Pratique, aprenda, conquiste.

Proz
Viva sua profissão!

Disciplina | Internet e Redes

Téc. em Desenvolvimento de Sistemas

Aqui começa a sua jornada

Vamos nessa?

Disciplina | Internet e Redes

Téc. em Desenvolvimento de Sistemas

SUMÁRIO

Internet e Redes

Introdução

A evolução constante da tecnologia da informação tem desempenhado um papel crucial no desenvolvimento e na expansão de redes de computadores em diversos setores. Este material didático foi cuidadosamente elaborado para oferecer um panorama abrangente e atualizado do mundo das redes de computadores e sua crescente integração com a cloud computing. Destinado a estudantes, profissionais de TI e entusiastas da área, esta apostila aborda desde os fundamentos até os aspectos mais complexos das redes de computadores, garantindo uma base sólida de conhecimento para aqueles que buscam se aprofundar neste campo.

O primeiro tema introduz "Redes de Computadores e Cabeamento Estruturado", um pilar fundamental para a compreensão das infraestruturas de rede. Este módulo explica como as redes são construídas e interconectadas, enfatizando a importância de um cabeamento estruturado eficiente para a otimização da performance de uma rede.

Avançando para o segundo tópico, abordamos "Protocolo de Rede", uma peça chave para a comunicação entre dispositivos em uma rede. Este capítulo detalha os protocolos que regem o envio e recebimento de dados, essenciais para a integridade e segurança da informação.

O terceiro tema, "Topologia de Rede", mergulha nas diversas formas em que as redes podem ser organizadas. Compreender essas topologias é vital para o planejamento e implementação de redes eficientes e confiáveis.

Nos temas quatro e cinco, a discussão se volta para "IPv4, Máscara de Rede e Gateway" e "IPv6". Estes capítulos são dedicados a entender os sistemas de endereçamento IP, cruciais para a identificação de dispositivos em uma rede.

No sexto tema, exploramos os "Padrões Ethernet", uma tecnologia amplamente utilizada em redes locais. Este módulo fornece um entendimento detalhado das especificações e operações do Ethernet.

Os temas sete e oito cobrem o "Protocolo TCP e UDP" e "Dispositivo de Rede e Comandos Básico de Rede", respectivamente. Eles oferecem uma visão profunda sobre os protocolos de transmissão de dados e as ferramentas essenciais para a gestão e solução de problemas em redes.

Nos três últimos temas, a apostila se concentra em "Conceitos e modelos de serviços em Cloud", "Arquitetura e Implementação e Cloud" e "Padrões e Práticas em Cloud Computing". Estes capítulos são fundamentais para entender como as redes de computadores estão evoluindo com a integração de tecnologias de nuvem, refletindo as tendências atuais e futuras da indústria.

Este material é mais do que uma simples introdução às redes de computadores; é um guia abrangente que prepara o leitor para os desafios e oportunidades no mundo da tecnologia da informação, com ênfase especial na integração com a cloud computing. Seja você um iniciante ou um profissional buscando atualização, esta apostila é um recurso valioso para aprimorar seu conhecimento e habilidades na área.

TEMA 01

Redes de Computadores e Cabeamento Estruturado

Habilidades

- Projeto de Rede
- Cabeamento Estruturado
- Configuração de Dispositivos de Rede
- Resolução de Problemas de Rede
- Segurança de Rede
- Monitoramento e Gerenciamento de Rede

Figura 1: Rede de Computadores Fonte: https://www.camara.leg.br/noticias/659429-projeto-cria-mecanismos-de-checagem-e-correcao-para-evitar-conteudo-falso-na-internet/

Introdução a Redes

Redes de computadores é um conjunto de estrutura física (hosts) e lógica (protocolos), no qual permite que dois ou mais computadores sejam capazes de compartilhar informações entre si, ou seja, se tiver dois ou mais computadores conectados e trocando informações entre si, ali está composta uma rede de computadores.

A comunicação entre os computadores pode ser realizada por diversos meios físicos como:

- Par metálico;
- Coaxial;
- Fibra óptica;
- Transmissão por micro-ondas;
- Satélites de comunicação.

Confira o vídeo: https://www.youtube.com/watch?v=gjrOX2iYM3M

Quando um computador se encontra inserido em uma rede de computadores, ele adquire a capacidade de acessar não apenas as informações que são diretamente direcionadas a ele, mas também as informações residentes em outros computadores interligados na mesma rede. Esse intercâmbio de informações possibilita uma maior fluidez na comunicação e compartilhamento de dados entre os diversos dispositivos conectados à rede.

Um dos marcos pioneiros no desenvolvimento das redes de computadores remonta ao ano de 1969, quando o exército dos Estados Unidos implementou a ARPANET, uma precursora da Internet. O propósito principal da ARPANET era estabelecer uma infraestrutura de comunicação descentralizada, imune a eventuais ataques de bombardeio ou outros tipos de destruição. Nesse contexto, a ênfase residia na ausência de um ponto central de controle, em que cada ponto de conexão, também conhecido como "nó", estivesse interligado com outros nós de maneira intricada.

Dessa forma, cada nó da rede possuía múltiplas alternativas para transmitir dados, de

modo que, caso uma dessas rotas fosse comprometida ou destruída, outras opções permaneceriam disponíveis para a transmissão de informações.

Em resumo, uma rede de computadores possibilita o compartilhamento de recursos físicos e lógicos entre seus dispositivos interconectados. Esses recursos podem abranger uma ampla gama de elementos, tais como dados, comunicação de voz, impressoras, troca de mensagens via e-mail e diversos outros tipos de informações e serviços.

O que constitui uma rede de computadores?

Para que uma rede de computadores possa operar eficazmente, é imperativo que existam tanto dispositivos de hardware quanto software capazes de orquestrar a comunicação entre os diversos elementos que compõem a rede.

No contexto de uma rede, os clientes desempenham um papel crucial. Um cliente é um dispositivo pelo qual os usuários podem acessar os recursos disponíveis na rede. Tais dispositivos podem assumir diversas formas, incluindo estações de trabalho (computadores pessoais), tablets, notebooks, smartphones e uma ampla gama de outros dispositivos que são habilitados para aproveitar os recursos da rede. Em essência, os clientes são os pontos de acesso aos serviços e informações que a rede disponibiliza.

Por outro lado, temos os servidores, cuja função primordial é compartilhar recursos e serviços com os clientes da rede. Existem inúmeros tipos de servidores, sendo os mais conhecidos os servidores DHCP, DNS, de arquivos, web, e-mail, imagens, FTP, entre outros. Cada tipo de servidor desempenha um papel específico na gestão e distribuição dos recursos da rede, garantindo que os clientes possam acessá-los de maneira eficiente e segura.

As placas de rede, também conhecidas como Network Interface Cards (NICs), são dispositivos físicos essenciais que possibilitam a conexão entre os computadores na rede. As placas de rede mais comuns são aquelas compatíveis com os padrões Ethernet e Token Ring

(Rede em anel). Elas funcionam como as pontes que permitem a transmissão de dados entre os dispositivos conectados à rede, desempenhando um papel fundamental na comunicação efetiva.

No que diz respeito aos protocolos, esses representam conjuntos de regras que regulam a comunicação entre dispositivos distintos na rede. Diversos protocolos são empregados para facilitar essa comunicação, cada um com sua função específica. Por exemplo, protocolos como SMTP, IMAP e POP3 são dedicados à troca de e-mails, enquanto o ICMP, responsável pelo "ping", é utilizado para gerenciar o estado da comunicação entre computadores. Cada protocolo possui um propósito claro e desempenha um papel crucial na operação harmoniosa da rede.

Além disso, o cabeamento desempenha um papel central na infraestrutura da rede. Os cabos físicos representam os meios pelos quais os computadores são interconectados na rede, permitindo a transmissão de dados. Esses cabos são submetidos a padrões internacionais rigorosos que regulam sua qualidade, largura de banda e outros atributos técnicos. Um cabeamento adequado é essencial para garantir a conectividade confiável e a eficiência da rede.

Por último, mas não menos importante, temos o hardware de rede, que varia de acordo com o tipo de conexão e desempenha um papel crucial na otimização da comunicação dentro da rede. Dispositivos como switches, hubs e roteadores são exemplos desse hardware. Os switches, por exemplo, permitem a segmentação da rede, aumentando a eficiência da transmissão de dados, enquanto os roteadores desempenham um papel fundamental no encaminhamento de dados entre diferentes redes. O hardware de rede é a espinha dorsal que sustenta o funcionamento harmonioso de uma rede de computadores.

Para que servem as redes de computadores?

As redes de computadores desempenham um papel fundamental em nossa sociedade contemporânea, simplificando e aprimorando significativamente nossas atividades cotidianas. Quando utilizadas com discernimento e eficiência, essas redes se revelam recursos de extrema importância para a realização de nossas tarefas, além de possuírem a notável capacidade de conectar pessoas, cidades e culturas em uma única infraestrutura, um único clique, contribuindo assim para a crescente globalização que permeia todas as esferas de nossa

existência.

Compartilhar arquivos, um aspecto muitas vezes subestimado, representa uma das facetas mais cruciais das redes de computadores. A capacidade de armazenar um arquivo em um servidor remoto por meio da rede pode parecer trivial à primeira vista. No entanto, o cerne da questão aqui não reside apenas na eficácia do armazenamento, mas sim na habilidade de compartilhar esses arquivos de forma eficiente. A possibilidade de localizar e acessar uma cópia específica de um arquivo, sem a necessidade de se deslocar da estação de trabalho, ou mesmo de realizar cópias de segurança em diferentes locais, é um recurso inestimável. Isso não apenas aumenta a produtividade, mas também promove uma gestão mais eficaz dos recursos de armazenamento.

O compartilhamento de impressoras é outra vantagem substancial proporcionada pelas redes de computadores. Isso se traduz em redução de custos significativos em relação aos ativos de rede. Ao invés de adquirir uma impressora para cada computador, é possível instalar uma única impressora em um computador centralizado, permitindo que todos os dispositivos na rede a utilizem. Esse compartilhamento eficaz não apenas economiza recursos financeiros, mas também contribui para uma abordagem mais sustentável em relação ao uso de dispositivos de impressão.

Outra aplicação valiosa das redes é o compartilhamento de serviços e programas. Os computadores interconectados têm a capacidade de acessar programas ou serviços que residem em um servidor específico, eliminando assim a necessidade de instalações redundantes em várias máquinas. Essa prática não só otimiza o uso de recursos computacionais, mas também garante que todos os usuários estejam utilizando a mesma versão atualizada de um programa ou serviço, o que contribui para a padronização e eficiência operacional.

Além disso, o compartilhamento de acesso à internet é um dos pilares das redes de computadores. Ao ter um ponto de acesso à internet centralizado, é possível compartilhar a conexão com a web entre todos os dispositivos na rede. Isso se torna especialmente crucial, pois justifica o custo de uma conexão de alta velocidade quando compartilhada entre vários usuários. Essa prática é essencial para o acesso a serviços da web, comunicação por e-mail e diversas outras atividades online. Com apenas um computador servindo como ponto de

acesso à internet, todos os demais dispositivos na rede têm a capacidade de desfrutar de conectividade à web.

Em resumo, as redes de computadores são verdadeiros catalisadores da eficiência, produtividade e conectividade em nossa sociedade moderna. Elas não apenas facilitam nossas tarefas diárias, mas também promovem a coesão entre pessoas, comunidades e culturas em uma rede interconectada, moldando um mundo cada vez mais globalizado em todas as esferas de nossa vida.

História da Internet?

A Internet representa, sem dúvida, uma das mais extraordinárias inovações da nossa era contemporânea. Trata-se do veículo de comunicação mais veloz e eficaz, capaz de estabelecer conexões instantâneas que transcendem fronteiras geográficas, amalgamando virtualmente os habitantes do planeta numa espécie de "tribo" global. Inegavelmente, a Internet se configura como um elemento central em nossas vidas, tanto no ambiente de trabalho quanto no nosso tempo de lazer.

A magnitude da Internet é evidenciada pelo fato de que a maioria de nós passa uma parcela significativa de nossos dias conectados a ela. Seja na execução das tarefas laborais, no entretenimento ou na busca incessante por informações, a rede mundial de computadores está sempre presente. Num simples clique, somos capazes de acessar uma miríade de conteúdos, seja um filme, uma imagem, uma faixa musical ou uma notícia. Praticamente qualquer forma de entretenimento ou conhecimento que possamos conceber encontra-se ao nosso alcance na vastidão da Internet.

É importante ressaltar que a Internet nos confere a capacidade de obter informações em tempo real e, ao mesmo tempo, de nos comunicarmos instantaneamente com pessoas de qualquer parte do mundo. Essa interconexão global transcende barreiras geográficas e temporais, possibilitando um fluxo ininterrupto de dados e comunicação.

Afinal, o que é a Internet? Trata-se de uma intricada rede de conexões que abrange todos os computadores da Terra, permitindo que eles se comuniquem uns com os outros de maneira instantânea e eficiente. Essa teia interligada de informações e recursos transformou radicalmente a forma como vivemos, trabalhamos e nos relacionamos, moldando o cenário contemporâneo de maneiras profundas e inimagináveis.

A Internet é uma invenção que revolucionou a forma como o mundo se comunica,

compartilha informações e realiza negócios. Embora não seja exato afirmar que ela tem 50 anos, uma vez que seu desenvolvimento foi um processo gradual e contínuo, podemos traçar uma cronologia de eventos significativos que culminaram na Internet que conhecemos hoje:

Década de 1960 - O Início:

- 1962: J.C.R. Licklider propõe a ideia de uma "Rede Intergaláctica de Computadores" em suas memórias.

- 1969: A ARPANET (Advanced Research Projects Agency Network), uma rede de comutação de pacotes financiada pelo Departamento de Defesa dos Estados Unidos, é estabelecida como a precursora da Internet. Foi o primeiro exemplo de uma rede que utilizava o protocolo TCP/IP, o que se tornaria o padrão para a comunicação na Internet.

Década de 1970 - Surgimento da Arquitetura TCP/IP:

- 1972: O protocolo ARPANET adota o TCP/IP (Transmission Control Protocol/Internet Protocol), a base da comunicação na Internet.
- 1973: O primeiro pedido de comentário (RFC), um documento que descreve padrões e protocolos, é publicado.
- Década de 1980 - Expansão e Comercialização:
- 1983: A ARPANET muda para usar exclusivamente o protocolo TCP/IP, marcando o nascimento da Internet como a conhecemos hoje.
- 1985: A National Science Foundation (NSF) lança a NSFNET, uma rede de alta velocidade que interconecta instituições acadêmicas nos Estados Unidos.
- 1989: Tim Berners-Lee, um cientista britânico, propõe o conceito da World Wide Web (WWW).

- Década de 1970 - Surgimento da Arquitetura TCP/IP:
- 1972: O protocolo ARPANET adota o TCP/IP (Transmission Control Protocol/Internet Protocol), a base da comunicação na Internet.
- 1973: O primeiro pedido de comentário (RFC), um documento que descreve padrões e protocolos, é publicado.

Década de 1980 - Expansão e Comercialização:

- 1983: A ARPANET muda para usar exclusivamente o protocolo TCP/IP, marcando o nascimento da Internet como a conhecemos hoje.
- 1985: A National Science Foundation (NSF) lança a NSFNET, uma rede de alta velocidade que interconecta instituições acadêmicas nos Estados Unidos.
- 1989: Tim Berners-Lee, um cientista britânico, propõe o conceito da World Wide Web (WWW).

Década de 1990 - Popularização:

- 1990: Tim Berners-Lee desenvolve o primeiro navegador web e servidor web, criando a base para a WWW.
- 1993: O primeiro navegador web amplamente utilizado, o Mosaic, é lançado.
- 1995: A NSF encerra a NSFNET, abrindo a Internet para uso comercial e popularização em todo o mundo.

Década de 2000 - A Era das Redes Sociais e Aplicativos:

- 2004: O Facebook é lançado, marcando o início da explosão das redes sociais.
- 2007: A Apple lança o iPhone, popularizando os smartphones e o acesso à Internet móvel.
- 2008: A Bitcoin, uma moeda digital, é proposta por uma pessoa (ou grupo) sob o pseudônimo de Satoshi Nakamoto.

Década de 2010 - A Era das Redes Sociais e Aplicativos:

- 2010: O Instagram é lançado.
- 2016: O jogo Pokémon Go se torna um fenômeno global, mostrando o potencial da realidade aumentada em aplicativos móveis.
- 2019: O 5G começa a ser implantado em várias partes do mundo, prometendo uma conectividade ainda mais rápida.

Década de 2020 - Continuidade da Evolução:

- 2020: A pandemia da COVID-19 acelera a adoção de trabalho remoto, ensino online e telemedicina, destacando ainda mais a importância da Internet.
- 2021: O lançamento de satélites de Internet por empresas como SpaceX e OneWeb promete levar a conectividade a áreas remotas do mundo.

Esta cronologia abrange marcos importantes na evolução da Internet ao longo dos anos, mas é importante notar que a história da Internet continua a ser escrita à medida que novas tecnologias e inovações emergem. A Internet é uma ferramenta em constante evolução que

continua a moldar e transformar a sociedade global.

Figura 2: Cabeamento Estruturado. Fonte: https://www.timeteleinfo.com.br/

Imagine que você tem a incumbência de projetar uma rede para uma empresa de pequeno/médio porte, na qual se encontra 100 pontos de rede, não seria de qualquer forma que você iria montar a rede dessa empresa, não é mesmo?

Pense assim é muito diferente você montar uma rede em sua residência e montar uma rede em seu ambiente de trabalho (como essa do exemplo) é mais difícil de se projetar, sejam essas redes residenciais ou comerciais, empresas de pequeno ou grande porte, existem normas mais detalhadas a serem realizadas, e nós chamamos esse conjunto de regras de Cabeamento estruturado.

Podemos definir cabeamento estruturado como uma infraestrutura de cabos de rede organizados em ambientes residenciais, empresariais ou escolares, que consiste em um número de elementos padronizados (estruturados) pelas normas (ANSI/TIA/EIA-568-B).

O padrão de cabeamento estruturado é projetado conforme as normas e instalado fornece uma infraestrutura de rede que permite a entrega de um desempenho dos equipamentos já prevista pelos seus fabricantes, assim terá a flexibilidade necessária para acomodar às mudanças de equipamentos (layout), aumento de pontos de rede e ser compatível com várias possibilidades de novas tecnologias.

Em síntese, o cabeamento estruturado tem como objetivo agregar e incluir várias tecnologias/aplicações, no qual diversas opções de conexões tenham a possibilidade de estar interligados, através de apenas uma infraestrutura, ou seja, um sistema que se agrega a um hardware, pois o objetivo de se aplicar uma infraestrutura de cabeamento estruturado em uma

empresa, é transmitir informações através de uma infraestrutura de computadores, que permite uma redução de custos e evita grande problemas.

Conceitos de Cabeamento Estruturado

No ano de 1991 as normas EIA/TIA-568, indicou a primeira versão da padronização de cabos e fios para telecomunicações em prédios comercias, no qual o objetivo era:

a. Elaborou um padrão de cabeamento de telecomunicações, no qual todos os fornecedores deveriam segui-las;

b. Organizar um sistema de cabeamento em ambientes externo ou interno, no qual todos os fornecedores devessem se enquadrar;

c. Indicar parâmetros técnicos de performance para diferentes sistemas de cabeamento, baseando-se em sua regra de negócio ou aplicações.

Assim, os prédios possuíam cabeamento para voz, dados, sistemas de controle, eletricidade, segurança, cada qual com uma padronização proprietária.

Na época assim como hoje as empresas possuem todas as aplicações de rede ou em sua grande maioria como cabos de:

- Voip (Telefone via IP);
- Dados;
- Sistemas de controle (ERP);
- Eletricidade;
- Segurança.

Não podemos esquecer que cada um seguia seu próprio padrão, alguns prédios eram cabos e fios em toda parte, não tinha um padrão a ser seguido, partes da empresa funcionavam com cabo coaxial, par trançado, cabo blindado, enfim a única regra era funcionar, mas esse cenário ocasionava uma série de problemas, no qual ajudou a desestimular a essa prática e incentivar o cabeamento estruturado.

Hoje o cabeamento estruturado está na norma EIA/TIA-568A, no qual é descrito em seis subsistemas:

1. **(Horizontal Cabling - HC) - Cabeamento Horizontal:** Compreendido pelas conexões da sala de telecomunicações (TR) até a área de trabalho (WA).

2. **(Backbone Distribution - BC) - Cabeamento Backbone:** Pode ser chamado de

cabeamento vertical, e se interliga ao cabeamento horizontal, e sua transmissão é realizado por meios físicos (fios e cabos), entre seus mais variados níveis desde interligar salas e prédios e até Backbone.

Todos os cabos são padronizados e autenticados pela norma EIA/TIA 568A para ser utilizados em Backbone:

a. Cabo UTP - Par Trançado (100 Ohms 22 ou 24 AWG):

- 800 metros de cabo para voz (20 a 300 MHz);
- 90 metros de cabo para dados (Cat. 3,4 e 5).

b. **Cabo STP - Par trançado Blindado (150 Ohms):**

- 90 metros de cabos para dados.

c. **Fibra Óptica multimodo de 62,5/125 m:**

- 2.000 metros de cabos para dados.

d. **Fibra Óptica monomodo de 8,5/125 m:**

- 3.000 metros de cabos para dados.

Obs.: As recomendações básicas para obter a melhor performance é que as instalações não podem coexistir onde possam ter interferências eletromagnéticas e o aterramento deve seguir os padrões EIA/TIA 607.

3. **(Work Area – WA) - Área de Trabalho:** De acordo com o padrão EIA/TIA 568A o cabeamento até as estações de trabalhos tem que ter a possibilidade de maleabilidade e possíveis trocas de lugares, sem prejudicar o cabeamento, ou que impeça de alguma forma a conexão com a rede local, os itens que compõem esse subsistema são:

a. Computadores;

b. Telefones;

c. Jumpers de Fibra;

d. Cabos;

e. Cordão Modular (Telefone);

f. Jumpers de Fibra Óptica;

g. Adaptadores de Rede (Placa de Rede, Placa Wi-Fi entre outros).

4. **(Telecommunications Room – TR) - Sala de Telecomunicações:** É o lugar onde tem como objetivo alocar todos os cabos e equipamentos do seu ambiente de trabalho, tendo em mente que podem ou não alocar dispositivos ativos de rede, é o ponto de encontro de todos os cabeamentos verticais e Horizontais, assim como alguns equipamentos como por exemplo Patch Panel.

5. **(Equipment Room -ER) - Sala de Equipamentos:** É neste espaço que são alocados os ativos da rede, é área definida para guardar os equipamentos de rede como por exemplo:

a. Switch;

b. Roteadores;

c. PABX (Telefonia);

d. Patch Panel;

e. Servidores;

f. Distribuidores Ópticos.

Obs.: A diferença da Sala de Equipamento para o Armário de Telecomunicações é simplesmente é a diversidade de equipamentos que cada uma comporta, sendo assim a sala de equipamentos pode até atribuir alguns ou todos elementos de um Armário de Telecomunicação.

6. **(Entrance Facility – EF) - Entrada do Edifício**: É a área que é feita a conexão dos cabos externo e do cabeamento de sua rede interna (local de Trabalho), no qual disponibiliza alguns serviços (Internet e PABX). As definições desse subsistema são orientadas pela norma EIA/TIA 569.

Benefício do Cabeamento Estruturado

Pequena, Média ou Grandes empresas, que possuem dispositivos de rede, computadores e outros equipamentos que necessitam estar funcionando em rede, precisam manter a sua respectiva infraestrutura organizada, por isso, que foi inventado um padrão/ideia chamado cabeamento estruturado.

Um padrão no qual seguido adequadamente permite que a empresa possua um cabeamento mais organizado, tendo a disponibilidade de expansão dos dispositivos de rede e tem a facilidade de agregar novas tecnologias, compreenda os benefícios de se obter cabeamento estruturado em seu local de trabalho:

1. **Fácil Gestão:** Tendo em vista que já está implantando o padrão de cabeamento estruturado, não tem a necessidade de manter uma equipe enorme para cuidar da infraestrutura, pois quando a rede está centralizada em um único lugar o gerenciamento se torna eficaz e ágil, sendo assim terá um menor número de profissionais cuidando da mesma rede.

2. **Retorno Sobre Investimento - ROI:** Quando temos uma única estrutura que consiga integrar voz, vídeo e dados em uma rede, esta consegue reduzir os valores de manutenção e consequentemente qualquer alteração que possa ser aplicada na rede, pode ser feita com agilidade, poupando dinheiro e tempo.

3. **Rede de T.I com disponibilidade para ampliações:** Com novas tecnologias sendo lançadas praticamente todos os dias, a rede precisa estar preparada para essas possíveis mudanças, o profissional de T.I deve sempre pensar na expansão da rede, caso em um futuro a empresa queira implantar um ERP (Sistema de Gestão Empresarial), uma sala de videoconferência ou uma atualização mais ousada, e a empresa estiver operando como determina o sistema de cabeamento estruturado, a empresa poderá trabalhar com calma, pois saberá que seu sistema não irá ficar antigo em tão pouco tempo e não irá parar com tanta facilidade.

4. **Maleabilidade do Sistema:** Quando temos uma infraestrutura que todo o cabeamento está interligado a um ponto central, sendo que pode transportar os dados em diversas maneiras, podendo ter uma maior maleabilidade caso haja mudança para um novo local.

5. **Esteticamente:** O cabeamento estruturado proporciona muitos benefícios, e a parte estética é algo que todo patrão se importa em sua empresa, ninguém quer ver cabo pendurado, amarrado, solto, com vários padrões, dando até a possiblidade de estender uma roupa, óbvio que esse último item é brincadeiras, mas quem dera se os demais fossem também, tem muitas empresas que não importa como está empregada a distribuição de cabos em suas localidades, só se importam se está funcionando ou não, e empresas que adotam o sistema de cabeamento estruturado tem o privilégio de ver sua empresa funcionando de uma maneira adequada sem exposição de qualquer fio de rede ou similar.

RESUMO

As redes de computadores desempenham um papel crucial na conectividade global, permitindo a comunicação e o compartilhamento de informações em todo o mundo. O cabeamento estruturado é a base essencial para o funcionamento confiável dessas redes, envolvendo o projeto e a instalação de infraestruturas físicas que suportam a transmissão de dados. O projeto de rede é a primeira etapa crítica, exigindo a compreensão das necessidades da organização e a escolha adequada de topologias, protocolos e equipamentos.

O cabeamento estruturado, por sua vez, aborda a criação de uma infraestrutura organizada de cabos e conexões, otimizando o desempenho e facilitando futuras expansões. A configuração de dispositivos de rede é fundamental para garantir que os componentes da rede funcionem juntos de maneira eficiente, requerendo conhecimento em roteadores, switches e firewalls.

A resolução de problemas de rede é uma habilidade crucial, pois falhas podem ocorrer e afetar a produtividade. A segurança de rede é essencial para proteger os dados e recursos da organização contra ameaças cibernéticas, exigindo a implementação de políticas de segurança e firewalls. O monitoramento e gerenciamento de rede envolvem a supervisão constante do tráfego e da performance, com o uso de ferramentas para identificar e corrigir problemas em tempo real.

Em resumo, as redes de computadores e o cabeamento estruturado são fundamentais para a conectividade moderna, e profissionais dessa área devem dominar habilidades que vão desde o projeto até a segurança e o monitoramento das redes, garantindo a funcionalidade e a proteção dos recursos de TI das organizações.

ATIVIDADE DE FIXAÇÃO

1. O que é um sistema de cabeamento estruturado e por que é importante em redes de computadores?

2. Explique a diferença entre topologia física e topologia lógica em uma rede de computadores.

3. Quais são os principais componentes de um cabo Ethernet? Como a categoria do cabo afeta o desempenho da rede?

4. Descreva o processo de crimpagem de um conector RJ-45 em um cabo Ethernet. Quais são as etapas críticas desse processo?

5. O que é um endereço IP? Explique a diferença entre endereços IP estáticos e dinâmicos.

6. Quais são as vantagens e desvantagens de uma rede sem fio em comparação com uma rede com fio?

7. Explique o propósito de uma VLAN (Rede Local Virtual) e como ela pode melhorar a segmentação da rede.

8. Como um switch difere de um hub em uma rede de computadores? Quais são os benefícios de usar switches?

9. Quais são os principais protocolos de segurança utilizados para proteger redes de computadores? Descreva brevemente como funcionam.

10. Imagine que uma empresa está experimentando latência excessiva em sua rede. Quais poderiam ser as possíveis causas desse problema e como você começaria a diagnosticá-lo?

TEMA 2

Protocolo de Rede

Habilidades

- Compreensão de Protocolos em Camadas
- Análise de Pacotes
- Configuração de Protocolos de Rede
- Gerenciamento de Protocolos de Roteamento
- Segurança de Protocolos
- Resolução de Problemas de Protocolo

Figura 3: Protocolo de Rede. Fonte:
https://cacs.org.br/linguas/quais-sao-linguas-mais-faladas-no-mundo/

Introdução a Protocolos

Afinal, o que é um protocolo? Os protocolos é uma tecnologia que permite a comunicação entre os computadores, ou seja, se tiver duas pessoas que falam em idiomas diferentes, não há possibilidade de ter uma comunicação nesse ambiente.

Para haver comunicação necessita ter um tradutor, para que possa estabelecer uma comunicação entre essas pessoas, a função do protocolo é a mesma do tradutor, ele possibilita a comunicação entre os computadores.

Protocolos é um conjunto de regras, e métodos que devem ser seguidos para enviar e receber informações em uma rede, é a forma que possibilita a comunicação entre os computadores.

Existem variados protocolos para executar distintas tarefas na rede como, para enviar e receber arquivos (FTP), testar a conectividade de rede (ICMP), acessando a internet para enviar e receber informações é enviando uma sucessão de protocolos como:

1. ARP;
2. HTTP;
3. FTTP;
4. TCP;
5. ICMP;
6. IP;
7. SMTP;
8. Telnet;
9. UDP;
10. NNTP.

Confira o vídeo: https://www.youtube.com/watch?v=h_qeUwWGyTE

Funções dos Protocolos?

Como sabemos o protocolo é um conjunto de regras, que se caracterizam ser mais regido por tópicos que os determinam, os tópicos são esses:

- **(Sintaxe):** É o padrão dos dados e a forma sequenciada em que os dados são demonstrados, ou seja, esses padrões que determinam a função do byte a byte, é como uma "gramática" do "idioma" utilizado na comunicação;
- **(Semântica):** Representa um padrão dos dados (Sintaxe), para dar um significado à mensagem;
- **(Timing):** Estabelece uma velocidade de transmissão dos "pacotes" (pedaços da mensagem), ele pretende definir uma rapidez/velocidade concebível de comunicação no qual possa ser sustentado em todas as partes que está se mantendo a comunicação.

O protocolo tem funções predeterminada para obter a comunicação entre os hosts:

1. **(Endereçamento):** Determina qual o destino da mensagem, para enviar uma carta necessita ter um destinatário para que a carta chega ao seu destino, o endereçamento tem o mesmo papel para qual seu host quer se comunicar;

2. **(Sequência e Numeração):** Identifica as mensagens por meio de um número sequencial;

3. **(Estabelecer a conexão):** Constitui um canal lógico entre as duas pontas (Túnel) para estabelecer a troca das mensagens;

4. **(Controle de erros):** Idêntica e corrigi os erros durante a comunicação;

5. **(Retransmissão):** Se o sinal (ACK) não é recebido no destinatário, ou quando a mensagem não é recebida em seu destino;

6. **(Confirmação de recebimento):** Envia uma confirmação para cada pacote recebido (ACK);

7. **(Conversão de Código):** Faz um ajuste dos códigos de acordo com as particularidades do destinatário.

A grande maioria dos hosts e hardware de rede não falam a mesma língua, ou seja, se não houver um protocolo para fazer a (tradução) entre os hosts, não haverá comunicação.

Cada protocolo é definido um padrão, existem basicamente dois tipos de padrão:

- **Facto:** São padrões que são usados pela comunidade, principalmente por fabricantes quando lançam novos produtos, mas que ainda não foram aprovados por um comitê reconhecido, como ISO ou ANSI. Um exemplo é o protocolo IP;
- **Jure:** São usadas pelos fabricantes quando lançam novos produtos, porém ainda não tem aprovação pelos comitês reconhecidos.

Os protocolos são reconhecidos pelos comitês regularizadores, um exemplo claro é o modelo OSI, passam pelas especificações pelo comitê avaliador RFC (request for change).

Compartilhamento de Recursos na rede?

Em uma rede de computadores seja ela local ou global, temos a possibilidade de

compartilhar recursos entre os hosts que estão conectados na rede, mesmo que essa rede não tenha acesso a internet, temos a possibilidade de compartilhar impressoras, arquivos, pastas, etc.

Se a rede local estiver conectada com a internet, as possibilidades de compartilhamento nas redes de computadores aumentam, pois podemos trocar informações com qualquer host que esteja localizado no globo e conectado com a internet.

Compartilhar Internet e serviço entre os hosts, modificou a maneira do mundo em se comunicar, vai de conversa on-line para videoconferência (envio de vídeo em tempo real), a internet nos possibilita resolver as nossas pendências do dia a dia, fazendo transações bancárias, compra e vendas de produtos ou serviços, utilizar as redes sociais para se conectar com as pessoas diferentes.

Tudo isso é possível, pois os protocolos permitem diferentes serviços nas redes de computadores, o importante é estudar e compreender como funciona os principais protocolos na rede.

RESUMO

Os protocolos de rede desempenham um papel fundamental na comunicação e no funcionamento da internet e de redes de computadores em geral. Uma habilidade essencial na área de redes é a compreensão dos protocolos em camadas, que são conjuntos de regras que definem como os dispositivos em uma rede se comunicam. Os protocolos em camadas, como o modelo TCP/IP, dividem a comunicação em etapas, tornando-a mais organizada e eficiente.

A análise de pacotes é outra competência vital, pois permite aos profissionais de redes examinarem o tráfego de rede em busca de problemas, identificando erros, congestionamentos e até mesmo ameaças de segurança. A configuração de protocolos de rede é necessária para definir as regras de operação de dispositivos e serviços, garantindo que a comunicação ocorra de forma adequada.

O gerenciamento de protocolos de roteamento é importante para direcionar o tráfego pela rede da maneira mais eficiente, garantindo que os dados cheguem ao destino corretamente. A segurança de protocolos é essencial para proteger os dados sensíveis de ataques cibernéticos, sendo crucial entender como implementar criptografia e autenticação.

Por fim, a resolução de problemas de protocolo é uma habilidade crítica para solucionar questões de conectividade, lentidão na rede ou falhas de comunicação. Em suma, dominar essas habilidades relacionadas a protocolos de rede é essencial para garantir o funcionamento confiável e seguro das redes de computadores na era digital.

ATIVIDADE DE FIXAÇÃO

1. O que são protocolos de rede e por que são essenciais para a comunicação entre dispositivos em uma rede de computadores?

2. Explique o que é um modelo de referência em camadas, como o modelo OSI, e como ele auxilia na compreensão dos protocolos de rede.

3. Descreva o funcionamento básico do Protocolo de Controle de Transmissão (TCP) e do Protocolo de Internet (IP). Como esses protocolos trabalham juntos para fornecer comunicação confiável?

4. O que é o DNS (Sistema de Nomes de Domínio) e como ele funciona para traduzir nomes de domínio em endereços IP?

5. Explique a diferença entre os protocolos UDP (User Datagram Protocol) e TCP em termos de confiabilidade de transmissão de dados. Em que situações cada um é mais adequado?

6. Qual é a função do protocolo ARP (Address Resolution Protocol) em uma rede? Como ele permite que dispositivos encontrem o endereço MAC correspondente a um endereço IP?

7. O que é NAT (Network Address Translation) e qual é o seu papel na conservação de endereços IP em redes privadas?

8. Descreva como o protocolo DHCP (Dynamic Host Configuration Protocol) funciona para atribuir automaticamente endereços IP e outras configurações de rede a dispositivos em uma rede local.

9. Quais são os benefícios da implementação do protocolo de segurança TLS/SSL em uma conexão de rede? Como ele ajuda a proteger a confidencialidade e a integridade dos dados transmitidos?

10. Como os protocolos de roteamento, como OSPF (Open Shortest Path First) e BGP (Border Gateway Protocol), influenciam o tráfego de dados em uma rede? Qual é a diferença entre roteamento interno e roteamento externo?

11. O que é um Firewall e como ele utiliza protocolos para filtrar e controlar o tráfego de rede?

TEMA 03

Topologia de Rede

Habilidades

- Identificação de Topologias de Rede
- Projeto de Topologia de Rede
- Implementação de Topologia de Rede
- Diagnóstico e Solução de Problemas de Topologia
- Redundância e Tolerância a Falhas
- Topologias Híbridas e Virtuais

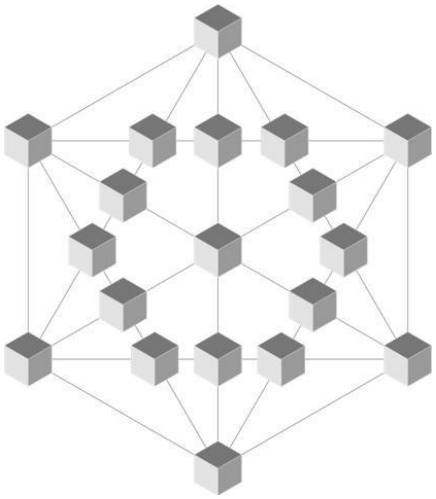


Figura 5: Topologia de Redes. Fonte: https://www.pngwing.com/pt/search?q=arte+-+rede

O que é Topologia de Redes?

Topologia é um sistema no qual demonstra como os hosts estão conectados na rede. Principalmente a estrutura da rede, e é demonstrado tanto fisicamente ou logicamente. Existem alguns modelos no qual se pode sistematizar a conexão de cada host na rede. Encontram-se dois tipos de topologias de rede:

Topologia Física: Demonstra de fato como os hosts estão dispostos e conectados no ambiente físico (Layout Físico). A posição de cada host, a forma que os cabos estão conectados, nós denominamos de topologia de rede, que tem como objetivo de auxiliar em vários pontos críticos, como a maleabilidade, velocidade na transferência dos dados e segurança.

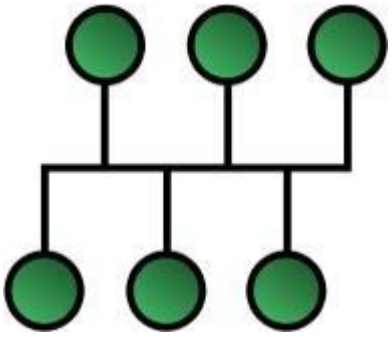
Topologia Lógica: Demonstra a forma como os dados são transmitidos na rede, ou a

forma como esses dados passam de um host a outro, sem se preocupar com a conexão física dos hosts, a forma como os dados são transmitidos na rede podem ser controladas por switches e roteadores.

Benefícios e desvantagens de cada Topologia:

Barramento

Todos os hosts estão conectados ao mesmo meio físico (barramento), embora os dados não "circulem" dentro de cada um dos nós, ou seja, se um computador estiver "escrevendo" aos outros computadores escutam e coletam os dados que é destinado para ele. Se um computador estiver enviando um sinal na rede e outro computador estiver tentando fazer o mesmo, ali se caracteriza uma colisão na rede, e se esse fato ocorrer terá que recomeçar a conexão.



Fonte: https://pt.wikipedia.org/wiki/Rede_em_barramento

Benefícios:

- Utilizam-se poucos cabos;
- Sua instalação é simples, seus meios físicos são economicamente barato;
- Simples e relativamente confiável;
- Sua topologia é simples e de certa forma confiável;
- E se necessário permite a ampliação da rede sem complicações.

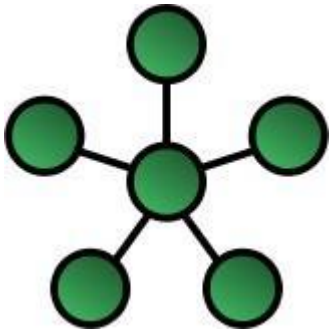
Desvantagens:

- A comunicação entre os hosts pode ficar lenta se o tráfego na rede aumentar;
- Problemas são difíceis de isolar;
- Caso ocorra um problema, o mesmo é difícil de identificar e isolar;

- Se por algum motivo houver uma falha no cabo de rede, a rede de sua empresa não irá funcionar.

Estrela

Atualmente é a topologia mais utilizada, esta topologia usa o meio físico de par trançado com um centralizador de rede (Switch e Roteador), este se encarrega de fazer a comunicação entre os hosts, isso facilita a detecção dos problemas, ou seja, se um computador não estiver ligado na rede o LED (Luz) do concentrador ficará desligado indicando que há um problema no host.



Fonte: https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens

Benefícios:

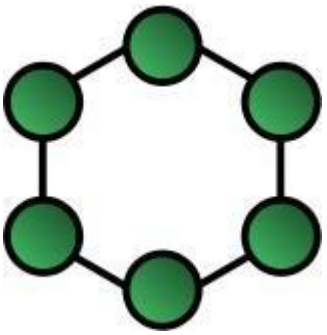
- Facilita a instalação e configuração dos computadores na rede;
- A gerencia dos equipamentos é centralizado;
- Caso um computador esteja com falha, o mesmo não paralisa a rede.

Desvantagem:

Se o centralizador da rede apresentar falha, o mesmo ocasiona a paralisação na rede.

Anel:

Estes hosts são conectados em série, no qual se caracteriza em um círculo formado (anel), estes dados são propagados em uma única direção de host a host até chegar em seu destino, ou seja, se uma estação transmitir uma mensagem, terá que retransmitir para todas as estações até chegar em seu destino, esta mensagem somente o host poderá retirar da rede quem transmiti ou recebe a mesma.



Fonte:https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens

Benefícios:

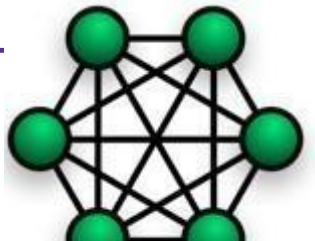
- Os hosts conseguem acessar a rede de uma maneira uniforme;
- O crescimento dos hosts não altera o desempenho da rede.

Desvantagens:

- Se um desses hosts falhar, poderá impactar toda a rede;
- Difícil isolar os Hosts.

Malha:

Esta é uma das topologias muito utilizada, pois é facilita a instalação e a configuração dos hosts. É como se todos os nós estivessem entrelaçados entre si, pois são diversos caminhos possíveis por onde os dados podem trafegar até o destino.



Fonte: https://www.oficinadanet.com.br/artigo/2254/topologia_de_redes_vantagens_e_desvantagens

Benefícios:

- Maior abundância e confiabilidade;
- Agilidade de reconhecimento nas falhas que possa ocorrer na rede.

Desvantagem:

Alto custo na implantação.

No vasto cenário das redes de computadores, onde informações fluem como correntes elétricas e dados atravessam o espaço à velocidade da luz, a topologia de rede desempenha um papel fundamental. Ela é a estrutura que define como os dispositivos se conectam, se comunicam e colaboram em um ecossistema digital cada vez mais interconectado.

Definindo a Topologia de Rede:

A topologia de rede é a disposição física ou lógica dos dispositivos em uma rede. É como o esqueleto que dá forma e direção a todo o sistema. Ela determina como os dispositivos estão interligados, quais caminhos os dados percorrem e como a comunicação é estabelecida. As diferentes topologias influenciam diretamente a eficiência, a escalabilidade, a redundância e a tolerância a falhas da rede.

Variedade de Topologias:

Existem várias topologias de rede, cada uma com suas próprias características e aplicabilidades. A topologia estrela, por exemplo, é amplamente utilizada devido à sua simplicidade e facilidade de manutenção. Nela, todos os dispositivos se conectam a um ponto central, como um switch ou hub. Por outro lado, a topologia em malha oferece alta redundância, pois cada dispositivo está conectado diretamente a todos os outros. A topologia em anel é menos comum, mas ainda possui utilidade em certos cenários.

Projeto Inteligente:

O projeto de topologia de rede é um exercício de equilíbrio e previsão. Profissionais de redes

devem considerar cuidadosamente as necessidades da organização, a quantidade de dispositivos, a capacidade de expansão e até mesmo os custos associados. Uma topologia bem projetada é escalável, eficiente e atende às demandas de comunicação presentes e futuras.

Implementação Precisa:

Após a fase de projeto, entra a implementação. Cabos são estendidos, dispositivos são configurados e a topologia ganha vida. A correta implementação é vital para garantir que a topologia projetada funcione conforme o planejado. Conectores e dispositivos são organizados, switches e roteadores são configurados e a rede se torna um ambiente de comunicação interligado.

Desafios e Resolução de Problemas:

Contudo, mesmo nas redes mais bem projetadas e implementadas, surgem desafios. Cabos podem falhar, switches podem congestionar e conexões podem ser interrompidas. A habilidade de diagnosticar e resolver problemas na topologia de rede é crucial. Profissionais precisam utilizar ferramentas de análise para identificar pontos fracos, reconfigurar dispositivos e, muitas vezes, redefinir a topologia para restaurar a integridade da comunicação.

Evolução Contínua:

Com o avanço da tecnologia, surgiram novas considerações na topologia de rede. Topologias virtuais, como as utilizadas em redes definidas por software (SDN), oferecem flexibilidade e agilidade incomparáveis. Além disso, as redes híbridas combinam diferentes topologias para atender às necessidades complexas das organizações modernas.

A topologia de rede é o alicerce sobre o qual a comunicação digital é construída. Desde redes locais (LANs) até redes globais da internet, ela desempenha um papel vital na conectividade que molda o mundo atual. Compreender as diferentes topologias, saber projetar e implementar eficientemente e possuir as habilidades para resolver problemas são marcos essenciais para qualquer profissional de redes que busca criar e manter redes confiáveis e eficazes.

RESUMO

A topologia de rede é um elemento fundamental na arquitetura e no funcionamento de sistemas de comunicação. Ela define a estrutura física e lógica pela qual os dispositivos em uma rede se conectam e se comunicam. Para entender a topologia de rede e aplicar suas várias habilidades, é necessário um profundo conhecimento sobre como os componentes de rede estão interligados e como isso afeta o desempenho e a confiabilidade da rede.

A identificação de topologias de rede é o ponto de partida. Isso envolve a análise das conexões físicas entre dispositivos, como cabos e switches, bem como a configuração lógica da rede, como endereços IP e sub-redes. Um entendimento claro das diferentes topologias, como estrela, barramento, anel e malha, é crucial para tomar decisões informadas no projeto de uma rede.

O projeto de topologia de rede é a próxima etapa crítica. Aqui, os profissionais de rede devem considerar requisitos específicos, como largura de banda, escalabilidade e redundância. Isso implica a seleção dos equipamentos de rede apropriados, a alocação de endereços IP, e a definição das políticas de segurança. O projeto também pode incluir a escolha entre topologias físicas e virtuais, dependendo das necessidades da organização.

A implementação da topologia de rede é a transformação do projeto em realidade. Isso envolve a instalação de dispositivos de rede, a configuração de roteadores e switches, e a atribuição de endereços IP aos dispositivos finais. A implementação requer habilidades técnicas para garantir que a topologia seja configurada corretamente e que todos os dispositivos estejam funcionando conforme o planejado.

O diagnóstico e solução de problemas de topologia são habilidades críticas para manter uma rede saudável. Quando ocorrem problemas, como quedas de conexão ou latência, é essencial identificar a causa raiz e implementar correções eficazes. Isso pode envolver a utilização de ferramentas de monitoramento de rede, análise de logs e colaboração com outros profissionais de TI.

A redundância e tolerância a falhas são conceitos-chave em topologia de rede. A redundância envolve a criação de caminhos alternativos de comunicação para garantir a continuidade do serviço em caso de falhas. A tolerância a falhas implica a capacidade de uma rede de continuar funcionando mesmo quando um ou mais componentes falham. Isso pode ser alcançado através de configurações de alta disponibilidade e backup.

Além disso, topologias híbridas e virtuais são cada vez mais comuns. Topologias híbridas combinam elementos de diferentes topologias físicas para atender a requisitos específicos, enquanto topologias virtuais são criadas em ambientes de rede virtualizados. A compreensão e a aplicação dessas abordagens flexíveis são essenciais para atender às demandas em constante evolução das organizações modernas.

Em resumo, a topologia de rede é um pilar fundamental da infraestrutura de comunicação, exigindo habilidades que abrangem desde a identificação e projeto até a implementação, diagnóstico de problemas, garantia de redundância e consideração de topologias híbridas e virtuais. O sucesso na gestão de redes requer um profundo conhecimento e experiência em todas

essas áreas para garantir um desempenho confiável e eficaz da rede.

ATIVIDADE DE FIXAÇÃO

1. O que é topologia de rede e por que ela é importante na configuração de redes de computadores?

2. Descreva a topologia de rede em estrela. Quais são suas vantagens e desvantagens em comparação com outras topologias?

3. Explique como funciona a topologia de rede em anel. Quais são os principais desafios dessa topologia em relação à escalabilidade e falhas?

4. Como a topologia de rede em malha difere das topologias em estrela e anel? Quais são as vantagens da topologia em malha em termos de redundância e confiabilidade?

5. Em uma topologia de rede em árvore, como os dispositivos são organizados? Qual é a relação entre a topologia de árvore e as topologias em estrela e hierárquica?

6. O que é uma topologia de rede híbrida? Dê exemplos de como diferentes topologias podem ser combinadas para atender às necessidades específicas de uma organização.

7. Explique como a topologia física e a topologia lógica podem diferir em uma rede de computadores. Dê exemplos de como uma rede pode ter uma topologia física diferente da topologia lógica.

8. Qual é o papel da topologia de rede na determinação dos caminhos que os dados percorrem entre dispositivos? Como essa determinação afeta o desempenho e a latência da rede?

9. Quais são os principais fatores que influenciam a escolha da topologia de rede para uma organização? Como a quantidade de dispositivos, o tráfego esperado e a escalabilidade afetam essa escolha?

10. Em uma rede definida por software (SDN), como a topologia é configurada e gerenciada? Quais são as vantagens e desafios de adotar uma abordagem SDN em relação às topologias tradicionais?

11. O que é uma topologia em estrela estendida (extended star)? Como essa topologia difere da topologia de estrela convencional?

TEMA 04

IPV4, Máscara de Rede e Gateway

Habilidades

- Configuração de Endereços IPv4
- Cálculo e Aplicação de Máscaras de Rede
- Entendimento de Sub-redes e VLSM
- Configuração de Gateway Padrão
- Resolução de Problemas de Conectividade
- Implementação de NAT

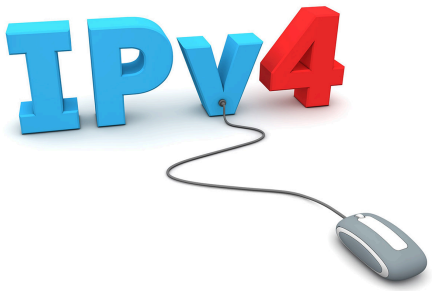
Figura 6: IPV4, Máscara de Rede e Gateway. Fonte: https://www.pngall.com/pt/gate-png

Confira o vídeo: https://www.youtube.com/watch?v=7OLSanO98-k

Introdução

Para eu obter a comunicação entre os hosts da minha rede, eu preciso da parte física (topologia, cabeamento) para que a rede tenha a possiblidade de ter uma comunicação entre os hosts, porém necessita ter a configuração lógica (IPV4, Máscara de Rede, Gateway e DNS), sem esses fatores não é possível estabelecer uma comunicação entre os hosts da rede.

O que é IPV4?



O protocolo IPV4, ou protocolo de versão 4, esta tecnologia permite que nossos hosts trafeguem na internet, todo host que estiver conectado (online) terá um código "99.48.224.242" por exemplo, que permite enviar e receber informações de outros hosts que estão conectados na rede.

Estes endereços IP, o IPV4, é formado por 04 blocos de 8 bits (8*4 = 32 bits), estes são exibidos por números de 0 a 255, por exemplo "200.145.36.25" ou "65.45.32.41".

Os endereços IPV4 que iniciam com "192.168", com "10" ou com "172.16" até "172.31", estes são "poupados" para redes locais, portanto não são utilizados na internet.

O IPv4 transfere endereços de protocolos de 32 bits. Sustenta mais ou menos 4,29 bilhões de IPs pelo mundo todo, o que nos tirou alcançar na crise atual: O sistema não suportará mais endereços do que isto.

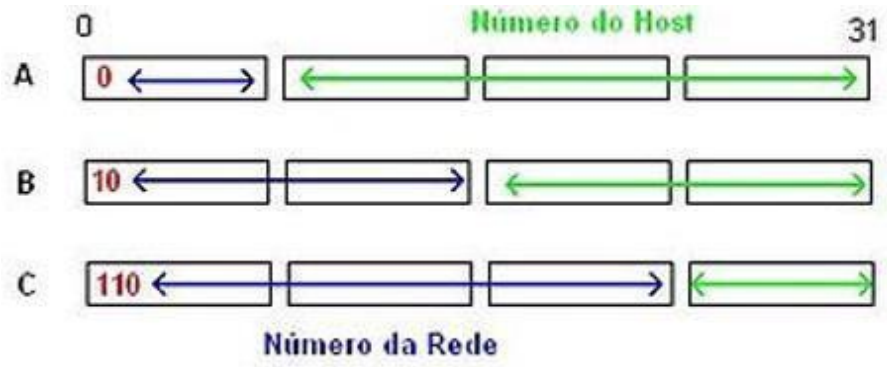
O IPV4 suporta por cerca de 4,29 bilhões de IPs por todo o mundo, o que infelizmente possibilitou essa crise atual por falta de IPs.

O que é Máscara de Rede?

Vamos imaginar que a máscara de rede é um bairro no qual possui várias residências (os IPs). Os IPs que utilizam uma determinada classe, pertence aquela classe, da mesma forma que se uma residência (IP), está presente no Bairro (Máscara de Rede) pertence a mesma, sendo que cada IP corresponde a uma máscara de rede:

Obs.: Os IPs possuem 4 octetos de binários que os totalizam em 32 bits.

- **Classe A:** 10.0.0.0 até 10.225.255.255 (255.0.0.0) - Utiliza apenas o primeiro octeto do IP que fica exclusivo para a máscara de rede e o restante para os hosts (11111111.00000000.00000000.00000000).
- **Classe B:** 172.16.0.0 até 172.31.255.255 (255.255.0.0) - Utiliza os dois primeiros octetos do IP que fica exclusivo para a máscara de rede e o restante para os hosts (11111111.11111111.00000000.00000000).
- **Classe C:** 192.168.0.0 até 192.168.0.0 (255.255.255.0) - Utiliza os três primeiros octetos do IP que fica exclusivo para a máscara de rede e o restante para os hosts (11111111.11111111.11111111.00000000).



O que é gateway?

O Gateway em geral é um host ou dispositivo de rede no qual se depara com duas redes. Podemos traduzir o termo gateway como "portão ou portal", é assim que essa tecnologia funciona, ele é um portão que libera o acesso ou não a outras redes. Essa tecnologia libera a passagem dos dados entre hosts (Tablet, telefone, computador, notebook entre outros). No qual pode ser instalado "políticas de acesso", que verificam a segurança dos dados do computador até a internet.

É como se fosse um portal que libera o acesso para o mundo externo (Internet), ele isola a rede doméstica com a internet.

Como havíamos dito o gateway é um portal que libera o acesso para a internet, por exemplo, eu tenho 04 computadores com 04 IPs diferente que estão na mesma máscara de rede, para não ter um modem ou qualquer outro dispositivo que conecte à internet em cada computador tem um gateway que compartilha a internet ou acesso para outra rede em todos os computadores da minha rede.

Por exemplo:

Comutador A:

IP: 192.168.1.100

Máscara de Rede: 255.255.255.0 Gateway: 192.168.1.1

Comutador B:

IP: 192.168.1.158

Máscara de Rede: 255.255.255.0 Gateway: 192.168.1.1

Comutador C:

IP: 192.168.1.200

Máscara de Rede: 255.255.255.0 Gateway: 192.168.1.1

Comutador D:

IP: 192.168.1.254

Máscara de Rede: 255.255.255.0 Gateway: 192.168.1.1

Configurando um cliente na rede

Existem duas formas para configurar um cliente na rede, o dinâmico onde só insere o cabo de rede e o Protocolo DHCP inclui todas as informações como IP, Gateway, DNS e Máscara de Rede, e a outra forma é estático onde você entra em (Painel de Controle – Redes e Internet – Central de Rede e Compartilhamento – Alterar as configurações do adaptador – botão direito do mouse em cima do ícone do adaptador – propriedade – Protocolo TCP/IPV4), chegando aqui você inseri manualmente as informações necessárias para se conectar na rede (IPV4, máscara de rede, Gateway e DNS.

IPv4, Máscara de Rede e Gateway: Os Pilares da Comunicação em Rede

Nos meandros da comunicação digital, onde dados fluem como elétrons por condutores virtuais, o IPv4, a máscara de rede e o gateway desempenham papéis fundamentais na garantia de que informações sejam encaminhadas com precisão e eficiência entre dispositivos em uma rede. Esses três elementos, juntos, formam a base do funcionamento das redes de computadores modernas, permitindo que dados sejam transmitidos de um ponto a outro, atravessando oceanos e continentes.

IPv4: Os Endereços Digitais Únicos

O IPv4 (Internet Protocol version 4) é o sistema de endereçamento padrão utilizado para identificar dispositivos em uma rede. Funciona como um equivalente digital de endereços postais. Um endereço IPv4 é composto por quatro grupos de números, variando de 0 a 255, separados por pontos. Cada dispositivo em uma rede tem um endereço IPv4 exclusivo, permitindo que os dados sejam enviados ao destinatário correto. No entanto, o esgotamento dos endereços IPv4 disponíveis é uma preocupação crescente, impulsionando a adoção do IPv6, que oferece um espaço de endereço muito maior.

Máscara de Rede: Segmentando Comunicações

Imagine uma cidade dividida em bairros, e cada bairro possui um código postal específico. Da mesma forma, a máscara de rede divide uma rede em segmentos menores, permitindo que dispositivos em cada segmento se comuniquem eficientemente. A máscara de rede é uma série de bits que, quando combinados com o endereço IP, definem qual parte do endereço identifica a rede e qual parte identifica os dispositivos individuais. Ao segmentar uma rede em sub-redes, a máscara de rede otimiza o uso de endereços IP e melhora o desempenho da comunicação.

Gateway: A Ponte entre Redes

O gateway, também conhecido como roteador, é o ponto de entrada e saída de uma rede para outras redes ou para a internet. Ele atua como uma espécie de porteiro digital, direcionando o tráfego de dados entre redes diferentes. Sem o gateway, a comunicação ficaria restrita apenas à rede local. Quando um dispositivo deseja se comunicar fora da rede local, ele envia os dados para o gateway, que encaminha os dados para a rede de destino. É o gateway que torna possível a comunicação entre diferentes redes e a navegação na internet.

A Sinfonia da Comunicação em Rede:

O IPv4, a máscara de rede e o gateway trabalham em conjunto para criar uma sinfonia de comunicação em rede. O endereço IPv4 identifica os dispositivos, a máscara de rede segmenta as redes e a comunicação, e o gateway permite que os dados fluam entre redes separadas. Esses elementos são essenciais para que o correio eletrônico seja entregue, os sites sejam carregados e os dados sejam trocados em redes locais e globais.

Desafios e Evolução:

Com o crescimento explosivo da internet e a proliferação de dispositivos conectados, os desafios associados ao IPv4 se tornaram evidentes, principalmente a escassez de endereços disponíveis. Isso levou ao desenvolvimento do IPv6, que oferece uma quantidade significativamente maior de endereços. A transição gradual para o IPv6 está em andamento para garantir a continuidade da comunicação em rede.

Em última análise, o IPv4, a máscara de rede e o gateway são os alicerces sobre os quais a internet moderna foi construída. Eles são as ferramentas que possibilitam a comunicação global, a troca de informações e o funcionamento das redes que sustentam nossas atividades diárias. Compreender o papel e a operação desses elementos é vital para qualquer pessoa envolvida em redes de computadores, pois eles são os elementos-chave que permitem a sinfonia contínua da comunicação digital.

RESUMO

O IPv4, Máscara de Rede e Gateway são conceitos fundamentais em redes de computadores. O IPv4, ou Protocolo de Internet versão 4, é o protocolo de comunicação usado para identificar e rotear dispositivos na Internet. Cada dispositivo conectado a uma rede possui um endereço IPv4 exclusivo, que é composto por quatro conjuntos de números separados por pontos, como 192.168.1.1.

A configuração de endereços IPv4 é uma habilidade crucial na administração de redes. Isso envolve atribuir endereços IP a dispositivos, garantindo que eles estejam na mesma faixa de endereços para se comunicarem efetivamente. Além disso, é importante entender a máscara de rede, que determina quais bits em um endereço IP são usados para identificar a rede e quais são reservados para identificar dispositivos dentro dela.

Ao calcular e aplicar máscaras de rede, os administradores de rede segmentam redes em sub-redes menores para otimizar o uso de endereços IP. Essa técnica, conhecida como VLSM (Variable Length Subnet Masking), permite uma alocação mais eficiente de endereços IP em uma rede.

O gateway, também conhecido como gateway padrão, atua como uma ponte entre redes. Configurar o gateway é essencial para permitir que dispositivos em uma rede local se conectem a outras redes, como a Internet. A configuração adequada do gateway é crucial para o roteamento eficiente de pacotes de dados.

Para manter uma rede funcionando sem problemas, é importante resolver problemas de conectividade. Isso inclui identificar e solucionar problemas de configuração de endereços IP, máscaras de rede, gateways e roteamento. A capacidade de diagnosticar e resolver problemas de conectividade é uma habilidade vital para administradores de rede.

Além disso, a implementação de NAT (Network Address Translation) é outra habilidade essencial. NAT permite que vários dispositivos em uma rede compartilhem um único endereço IP público para acessar a Internet. Isso ajuda a economizar endereços IP públicos e melhora a segurança da rede.

Em resumo, compreender o IPv4, a máscara de rede e o gateway é essencial para a configuração eficaz de redes. Isso inclui a capacidade de configurar endereços IPv4, calcular e aplicar máscaras de rede, entender sub-redes e VLSM, configurar gateways padrão, resolver problemas de conectividade e implementar NAT. Essas habilidades são fundamentais para garantir o funcionamento adequado e seguro de redes de computadores.

ATIVIDADE DE FIXAÇÃO

1. O que é um endereço IPv4 e como ele é estruturado? Explique a importância de ter um endereço IP exclusivo em uma rede.

2. Descreva a função da máscara de rede. Como ela é usada para segmentar uma rede em sub-redes?

3. Se um dispositivo possui o endereço IP 192.168.1.25/24, qual é o intervalo de endereços disponíveis para dispositivos na mesma sub-rede? Explique como você chegou a essa conclusão.

4. O que é um gateway em uma rede de computadores? Como ele permite a comunicação entre diferentes redes ou a internet?

5. Qual é a diferença entre um endereço IP público e um endereço IP privado? Quais são as implicações de usar cada tipo de endereço em uma rede local?

6. Suponha que você tenha uma rede com a máscara de sub-rede 255.255.255.224. Quantas sub-redes essa máscara pode criar e quantos hosts cada sub-rede pode acomodar?

7. Explique como a conversão de um endereço IP em um endereço MAC é facilitada pelo ARP (Address Resolution Protocol). Como o ARP permite que os dispositivos encontrem o endereço MAC correto?

8. Se um dispositivo na rede local deseja acessar um site na internet, qual é o papel do gateway nesse processo? Como o gateway direciona o tráfego para a rede externa?

9. O que é o NAT (Network Address Translation)? Como ele permite que vários dispositivos em uma rede compartilhem um único endereço IP público para acessar a internet?

10. Com a crescente demanda por endereços IP devido ao aumento do número de dispositivos conectados, como o IPv6 aborda essa limitação em comparação com o IPv4? Quais são as principais diferenças entre essas versões do protocolo IP?

11. Descreva o processo pelo qual um dispositivo, ao receber um pacote de dados, determina se o destinatário está na mesma sub-rede ou em uma sub-rede diferente. Como a máscara de rede é usada nesse processo?

TEMA 5

IPv6

Habilidades

- Configuração de Endereços IPv6
- Transição e Coexistência IPv4-IPv6
- Conhecimento dos Tipos de Endereços IPv6
- Endereçamento de Sub-Redes IPv6
- Segurança em Redes IPv6
- Implementação de IPv6 em Redes Locais e de Grande Escala

Fonte: https://www.entelco.com.br/blog/author/admin/page/79/

Para realizar a comunicação entre dois dispositivos na internet, é necessário que cada um possua em endereço único lógico na camada de rede, para isso foi criado o protocolo IPv4 que é utilizado no TCP/IP. O IPv4 possui o comprimento de 32bits, sendo permitido 2x32 (4294967296) de endereços em seu total.

Conforme o crescimento da internet e o aumento exponencial no número de dispositivos conectados a ela, foi identificado que surgiria um problema na falta de endereços IP a longo prazo.

Devido ao endereçamento Ipv4 possuir 32 bits de comprimento e junto ao fato de que cada endereço é único e não pode ser utilizado por mais de um dispositivo, ou seja, uma conexão de um dispositivo com a internet é feita por meio de um único endereço válido para comunicação. Foi então identificado a necessidade da criação de uma nova versão do protocolo IP, sendo então criado o IPv6 que veremos no capítulo seguinte

a. Endereços IPv6

Os endereços IPv6 foram criados com 128 bits de comprimento e nele é utilizado a

notação hexadecimal, para facilitar a leitura dos endereços. Esses 128 bits são distribuídos dentro de oito seções, cada uma possuindo então 2 bytes de comprimento. Para representação desses dois bytes na notação hexadecimal são necessários 4 dígitos, ou seja, o endereçamento IPv6 é representado na forma de 32 dígitos hexadecimais.

Ex.:

Fazendo a conversão: 128 bits = 16 bytes = 32 dígitos hexadecimais.

FFDC:4738:D423:8800:0000:57AB:BC99:3200

b. Tipos de endereços Ipv6

O protocolo IPv6 possui 3 tipos de endereçamento, são eles:

UNICAST - Os endereços IPv6 Unicast se caracterizam por identificar unicamente uma interface de rede. Por isso, um pacote enviado à um endereço IPv6 Unicast vai ser entregue à uma única interface em todo o escopo do endereçamento IPv6. São utilizados para permitir a comunicação entre dois nós exclusivos da rede, tais como PCs, Tablets, Telefones IP, etc.…

MULTICAST - Um endereço IPv6 Multicast é um endereço IP que designa um grupo de interfaces. Os pacotes enviados à um endereço multicast serão entregues a todos os endereços que compõe o grupo.

Um endereço multicast permite que uma cópia dos dados seja enviada à rede para que vários destinatários recebam os mesmos, ao invés de uma cópia para cada um dos destinos. Isto economiza, e muito o tráfego em uma rede, visto que não é necessária a duplicação do tráfego.

ANYCAST - Um endereço Anycast é utilizado para identificar um grupo de interfaces, mas diferente do Multicast, o pacote destinado à um endereço Anycast é entregue somente à interface mais próxima da origem, enquanto o Multicast entrega a todos os participantes do grupo.

Não existe um prefixo de endereço específico para identificar um endereço Multicast, ou seja, qualquer endereço Unicast aplicado à mais de uma interface automaticamente torna-se um endereço Anycast, com a única diferença de que a configuração deve explicitamente indicar que foi atribuído um endereço Anycast.

b. Cabeçalho do IPv6

O IPv6 introduz um novo formato de cabeçalho (Imagem 1). Se comparado ao anterior (Imagem 2), todos os campos do novo cabeçalho possuem tamanho fixo, totalizando 64 bytes. O fato dele possuir um tamanho fixo acelera bastante o processamento dos pacotes pelos roteadores, visto que não há necessidade de calcular a extensão de certos campos, e nem o tamanho do cabeçalho como um todo. Além disso, ocorreu uma redução dos números de

campos utilizados, por meio da exclusão de campos de pouca utilidade prática. Este fato também contribui para a diminuição do tempo gasto em processamento pelos roteadores.

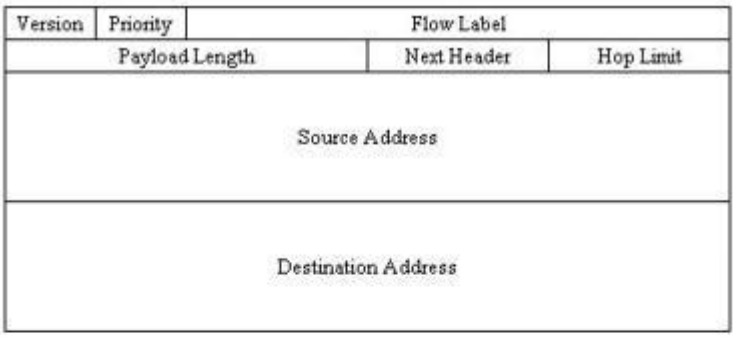


Imagem 1 – Cabeçalho IPv6

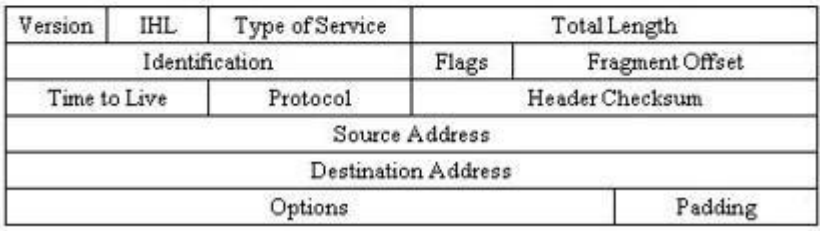


Imagem 2 – Cabeçalho IPv4

Dentre os campos que foram eliminados, dois que merecem destaque são os de Checksum e o de fragmentação.

A função do campo de Checksum era detectar erros que afetassem ao cabeçalho IP, sem detectar, no entanto, erros no restante do pacote. É fato que atualmente a maioria dos erros não é de transmissão, visto que os mecanismos de detecção de erros Ethernet e PPP são bastante eficientes, mas sim nos roteadores. Como os roteadores só alteram o campo Hop Limit (Time- to-live no IPv4), estes então terminam por recalcular o Checksum antes de retransmitir o pacote, o que pode causar a não detecção de possíveis erros. Além disso, vários roteadores, visando aumento de performance, não verificavam mais este campo, terminando assim por torná-lo totalmente supérfluo.

Quanto ao campo fragmentação, este foi excluído, pois decidiu-se que pacotes não serão mais fragmentados por roteadores. Caso um roteador receba um pacote com tamanho maior que o permitido, descartá-lo-á e enviará uma mensagem ao host que o enviou, comunicando o ocorrido. Este host deverá então retransmitir o pacote na forma de pacotes menores. Desta forma há um ganho de performance no roteamento, pois é eliminada a necessidade de um roteador fragmentar vários pacotes.

c. ICMPv6

ICMPv6 (Internet Control Message Protocol) é uma versão atualizada do protocolo ICMPv4 para ser utilizada em conjunto com o IPv6. Sua implementação, portanto, é obrigatória

em todos os nós da rede que utilizam IPv6 para se comunicar.

Embora esta versão possua as mesmas funcionalidades que a sua antecessora, como reportar erros no processamento de pacotes, realizar diagnósticos e enviar mensagens sobre as características da rede, ambas não são compatíveis e possuem diferenças significativas.

O ICMPv6 assume funções de outros protocolos, que existem isoladamente no IPv4. Tal mudança foi projetada com o simples intuito de reduzir a multiplicidade de protocolos, que é prejudicial por piorar a coerência e aumentar o tamanho das implementações. Os protocolos usados no IPv4, que não existem mais no IPv6, cujas funcionalidades foram agregadas pelo ICMPv6, são:

- **ARP (Address Resolution Protocol)**, cujo o objetivo é mapear os endereços físicos através dos endereços lógicos;
- **RARP (Reverse Address Resolution Protocol)**, que realiza o inverso do ARP, mapeando os endereços lógicos para endereços físicos;
- **IGMP (Internet Group Management Protocol)**, que atua com o gerenciamento de membros de grupos Multicast.

É importante notar que o ARP e RARP, no IPv4, são protocolos que podem ser descritos como operando entre as camadas 2 e 3 do modelo ISO/OSI. Em especial, eles não dependem de pacotes IP. O ICMPv6 é um protocolo de camada 3, mas é encapsulado em um pacote IP. Isso implica que firewalls operando na camada de rede, com o IPv6, podem bloquear funções extremamente básicas como a descoberta dos vizinhos e a autoconfiguração.

Uma outra diferença que se convém ressaltar é a utilização do ICMPv6 pelos subsequentes protocolos e funcionalidades:

- MLD (Multicast Listener Discovery), que opera com o gerenciamento dos grupos Multicast;
- NDP (Neighbor Discovery Protocol), que é responsável por identificar e conhecer características da vizinhança;
- Path MTU Discovery, que trabalha no processo de descoberta do menor MTU em comunicação entre dois nós;
- Mobility support, que cuida do gerenciamento de endereços de origem dos hosts dinamicamente;
- Autoconfiguração Stateless, que permite a aquisição de endereços globais sem o uso de DHCP.

Deve-se ter em mente que, de forma geral, o ICMPv6 é muito mais importante para o funcionamento do IPv6, do que o ICMP é para o funcionamento do IPv4.

IPv6: A Evolução Necessária para um Mundo Conectado

O crescimento exponencial da internet e a proliferação de dispositivos conectados trouxeram à tona um desafio fundamental: a escassez de endereços IP disponíveis no protocolo IPv4. Para atender às demandas de uma era digital em constante expansão, surgiu o IPv6 (Internet Protocol version 6), a próxima geração do protocolo IP. O IPv6 não é apenas uma atualização técnica; é uma transformação profunda que está moldando o futuro da comunicação online. Neste texto, exploramos o IPv6 em detalhes, desde suas características distintas até suas implicações na construção da internet do futuro.

O Limite do IPv4:

O IPv4, a versão anterior do protocolo IP, utiliza um espaço de endereço de 32 bits, o que resulta em um total de cerca de 4,3 bilhões de endereços. Parecia suficiente nas primeiras fases da internet, mas o aumento vertiginoso do número de dispositivos conectados, incluindo smartphones, tablets, dispositivos IoT e muito mais, rapidamente esgotou esse pool de endereços.

A escassez de endereços IPv4 é um gargalo que limita a expansão da internet e a conectividade global.

A Abordagem do IPv6:

O IPv6 surge como a solução para essa escassez de endereços. Utilizando um espaço de endereço de 128 bits, o IPv6 oferece uma quantidade quase inimaginável de endereços, na ordem de 340 undecilhões (3,4 x 10^38). Essa vasta reserva de endereços é praticamente inesgotável, o que significa que não só há endereços para todos os dispositivos atuais, mas também para as gerações futuras de dispositivos conectados.

Estrutura de Endereços IPv6:

Os endereços IPv6 são notavelmente diferentes dos endereços IPv4. Eles são representados em notação hexadecimal e são organizados em grupos de quatro dígitos separados por dois pontos, por exemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Além disso, o IPv6 introduz endereços especiais, como os endereços loopback (::1) e de link local (fe80::), que têm papéis específicos na comunicação.

Benefícios Além dos Endereços:

A expansão do espaço de endereços é apenas um aspecto das melhorias do IPv6. Ele também traz benefícios em termos de segurança, qualidade de serviço e eficiência de roteamento. A autoconfiguração de endereços permite que dispositivos conectados obtenham automaticamente um endereço IPv6 válido sem a necessidade de um servidor DHCP. Além disso, a integração de segurança é aprimorada por meio de extensões como o IPsec, que fornece criptografia e autenticação para comunicações mais seguras.

Desafios e Adoção:

A transição para o IPv6 não é uma tarefa simples. Requer a atualização de infraestruturas de rede, sistemas operacionais e aplicativos. No entanto, muitos governos, ISPs e empresas de tecnologia estão comprometidos com a adoção do IPv6 para garantir a continuidade da conectividade global. O World IPv6 Launch, em 2012, marcou um marco importante ao incentivar a implementação do IPv6 em uma escala global.

Conclusão: O Caminho para o Futuro

O IPv6 não é apenas uma atualização técnica; é um salto evolutivo que capacita a próxima geração de inovações digitais. Com sua capacidade praticamente ilimitada de endereçamento, melhorias em segurança e eficiência, o IPv6 está preparando o terreno para a expansão contínua da internet e o crescimento do ecossistema conectado. À medida que a adoção do IPv6 avança, o protocolo está abrindo portas para uma internet mais expansiva, mais segura e mais capaz, transformando a maneira como nos comunicamos, trabalhamos e vivemos em um mundo cada vez

mais conectado.

RESUMO

O IPv6, ou Internet Protocol version 6, é um protocolo de comunicação que representa a próxima evolução do IPv4, que estava rapidamente se esgotando devido à crescente demanda por endereços IP. Este novo protocolo traz consigo uma série de melhorias e desafios que os profissionais de rede precisam dominar para garantir o funcionamento eficiente e seguro das redes modernas.

Uma das habilidades fundamentais necessárias é a configuração de endereços IPv6. Ao contrário do IPv4, que utiliza notação decimal pontuada, o IPv6 utiliza uma notação hexadecimal e introduz um conjunto de regras específicas para configurar endereços, incluindo endereços unicast, multicast e anycast. Compreender essas regras é crucial para implantar o IPv6 com sucesso.

A transição e coexistência IPv4-IPv6 é outra área crucial. Muitas redes ainda dependem do IPv4, enquanto o IPv6 é gradualmente implementado. Isso exige a configuração de túneis, tradução de endereços e outros mecanismos para permitir que ambos os protocolos funcionem juntos até que o IPv6 seja amplamente adotado.

Conhecer os tipos de endereços IPv6 é essencial. Isso inclui endereços link-local, global unicast, site-local, entre outros. Cada tipo de endereço tem um propósito específico e é importante saber quando e como usá-los para otimizar o desempenho e a segurança da rede.

O endereçamento de sub-redes IPv6 é uma habilidade fundamental para criar uma estrutura de rede organizada e escalável. Isso envolve a alocação de blocos de endereços IPv6 e a configuração de prefixos de sub-rede para garantir que os dispositivos se comuniquem eficientemente.

A segurança em redes IPv6 é uma preocupação crítica. À medida que o IPv6 é adotado, surgem novas ameaças e desafios de segurança. Isso inclui a configuração adequada de firewalls, a autenticação de dispositivos e a proteção contra ataques de negação de serviço direcionados a endereços IPv6.

Por fim, a implementação do IPv6 em redes locais e de grande escala exige um planejamento cuidadoso e uma configuração precisa. Isso envolve a seleção de equipamentos compatíveis, a configuração de roteadores e switches, a migração de dispositivos existentes para o IPv6 e a realização de testes extensivos para garantir uma transição suave.

Dominar essas habilidades é essencial para os profissionais de rede que desejam enfrentar os desafios e aproveitar os benefícios do IPv6, preparando suas redes para um futuro cada vez mais orientado para o protocolo IPv6.

ATIVIDADE DE FIXAÇÃO

1. O que é IPv6 e como ele difere do IPv4?

2. Qual é o tamanho de endereço IPv6 em comparação com o IPv4?

3. Quais são as principais vantagens do IPv6 em relação ao IPv4?

4. Quais são os principais desafios na adoção do IPv6?

5. O que são endereços IPv6 globais únicos e como eles funcionam?

6. Quais são os diferentes tipos de endereços IPv6 e para que são usados?

7. Como um host IPv6 obtém seu endereço IP automaticamente?

8. O que é um túnel IPv6 e quando é usado?

9. Quais são as extensões de cabeçalho em um pacote IPv6 e para que servem?

10. Como as organizações podem migrar de uma infraestrutura IPv4 para IPv6 de forma eficaz?

TEMA 6

Padrões Ethernet

Habilidades

- Conhecimento dos Padrões Ethernet
- Seleção e Configuração de Cabos
- Negociação de Velocidade e Duplex
- Diagnóstico e Solução de Problemas
- Implementação de Redes em Conformidade
- Atualização e Migração de Padrões

Figura 7: Padrões Ethernet. Fonte: https://www.wallpaperflare.com/communication-concept-apple-updating-usb-port-network-wallpaper-wsyza

Introdução

Redes Ethernet é denominada por redes que utilizam cabos par trançados, para redes que não utilizamos cabos denominado rede Wireless/Redes sem fio, porem na história da informática as redes Ethernet tiveram vários aperfeiçoamentos por volta dos anos de 1970.

Existem três padrões importantes na rede Ethernet.

Confira o vídeo: https://www.youtube.com/watch?v=KIxPinooy9M

Características Gerais

10Base-T - 10 Megabit (Velocidade de Transmissão): Este padrão especifico utiliza cabos de par trançado, (Este "T" é de Twisted-pair), seu comprimento chega até 100 metros para possibilitar a transmissão de dados entre os hosts, pode se até utilizar um HUB para repetir o sinal, sendo assim permitindo alcançar distâncias maiores.

100Base-TX - 100 Megabit (Velocidade de Transmissão): Por volta de 1995 o padrão Fast Ethernet foi aprimorado para se adequar os padrões de transmissão, existem três tópicos que compõem o Fast Ethernet, o mais utilizado hoje em dia é o 100BASE-TX, no qual é constituído por um cabo de par trançado CAT5, empregado em mais de 80% das acomodações atuais.

1000Base-T - 1000 Megabit (Velocidade de Transmissão): Também denominado como GoC (Gigabit Over Copper), são chamados assim por utilizarem cabos de par trançado, os cabos de padrão 1000BaseT, utiliza com mais frequência o recurso de transmissão, portanto são mais críticos com interferência e cabos muito longo.

Obs.: Atualmente existem diversos padrões Ethernet que é de extrema importância conhecer, pois não existem padrões Ethernet somente para o cabo par trançado, mas também para fibra óptica entre outros.

Rede Ethernet

O padrão Ethernet é constituído por três princípios, nos quais reunidos definem de que forma os dados irão ser transmitido através do meio físico, sendo que sua missão é reunir os dados entregue por protocolo de alto padrão como TCP/IP, e implantar dentro de quadros que denominamos frames e envia-los pela rede:

MAC (Controle de Acesso ao Meio): Sua principal função é "montar" o quadro Ethernet que será enviado para a rede, no qual é responsável por inserir o endereço MAC de origem e Destino, o endereço MAC é o Endereço físico da Placa de Rede do seu host, este conceito está estipulado no protocolo IEEE 802.3 (Se os dados estiverem passando via meio físico) e o IEEE 802.11 (Se os dados estiverem passando por uma rede não cabeada, como por exemplo uma Rede Wireless).

Meio Físico ou Camada Física: Sua responsabilidade é transformar o quadro ethernet enviado pelo MAC em sinais elétricos (Se a rede utilizar meio físico) ou sinais eletromagnéticos (Se a rede não for cabeada).

LLC (Controle de Link Lógico ou Quadro Ethernet: O computador que irá receber os quadros consegue reconhecer o protocolo no qual ele deve entregar as informações de um quadro que o mesmo acabou de receber, ou seja ele é incumbido por incluir informações da camada de internet para originar os dados.

Endereçamento

O endereçamento de rede ou simplesmente endereço IP é um número binário (0 e 1) que especifica de maneira única um host conectado à uma rede TCP/IP.

Os endereços IPs é formado por 32 bits, no qual é separado por 04 grupos de 08 bits, esses grupos nos denominamos de octeto. Com cada grupo de octetos eu consigo chegar até 256 combinações distintas, para que esta configuração entre em um consenso os números utilizados são de 0 a 255, no qual retrata cada octeto, por exemplo é mais fácil utilizar a combinação de números (0 a 255) 75.96.200.151 do que usar números binários (0 e 1) para especificar um endereço de rede (1001011.1100000.11001000.10010111).

Se separarmos cada octeto de binário o cálculo será assim:

Pts	Octetos	Binários (grupo de 8 bits formado por 0 e 1)								Decimal
1°	01001011	0	1	0	0	1	0	1	1	75
		128	64	32	16	8	4	2	1	
2°	01100000	0	1	1	0	0	0	0	0	96
		128	64	32	16	8	4	2	1	
3°	11001000	1	1	0	0	1	0	0	0	200
		128	64	32	16	8	4	2	1	
4°	10010111	1	0	0	1	0	1	1	1	151
		128	64	32	16	8	4	2	1	

Pelo Endereço IP, temos a possibilidade de reconhecer a localidade e até mesmo o país que o host está conectado na internet.

1. Conhecimento dos Padrões Ethernet

O conhecimento dos padrões Ethernet é fundamental para qualquer profissional de redes. A Ethernet é a tecnologia de rede mais comumente usada em todo o mundo, e seus padrões estabelecem as diretrizes para a comunicação eficaz entre dispositivos em uma rede local (LAN). Isso inclui especificações para o cabeamento, protocolos de comunicação, taxas de transferência de dados e muito mais.

Os padrões Ethernet evoluíram ao longo do tempo, começando com o Ethernet de 10 megabits por segundo (Mbps) e progredindo para 100 Mbps, 1 gigabit por segundo (Gbps) e além. Além disso, existem padrões Ethernet específicos para conexões sem fio, como o Wi-Fi.

Um profissional de redes com conhecimento dos padrões Ethernet compreende as diferenças entre esses padrões, sabe como escolher o mais adequado para uma determinada situação e como implementá-lo com eficiência. Além disso, eles estão cientes das características de desempenho de cada padrão e podem otimizar a rede para atender às necessidades de largura de banda e latência dos usuários.

2. Seleção e Configuração de Cabos

A seleção e configuração de cabos desempenham um papel crucial na criação e manutenção de redes confiáveis e eficientes. Diferentes tipos de cabos são utilizados em redes, incluindo cabos de par trançado, cabos coaxiais e cabos de fibra óptica. Cada tipo de cabo tem suas características específicas e é adequado para diferentes cenários de rede.

Um profissional de redes precisa ser capaz de escolher o tipo certo de cabo com base nos requisitos da rede, como distância, largura de banda e ambiente. Eles também devem saber como configurar corretamente os conectores, emendas e terminações dos cabos para garantir uma conexão sólida e de alta qualidade.

Além disso, a capacidade de identificar e solucionar problemas de cabos, como quebras, interferências e perda de sinal, é essencial para manter o desempenho da rede. Isso inclui o uso de ferramentas de teste de cabos para verificar a integridade da conexão.

3. Negociação de Velocidade e Duplex

A negociação de velocidade e duplex é uma habilidade crucial para otimizar o desempenho da rede e garantir uma comunicação eficaz entre dispositivos. Velocidade se refere à taxa de transferência de dados entre os dispositivos, enquanto duplex se refere à capacidade de transmitir e receber dados simultaneamente.

Um profissional de redes precisa entender como a negociação de velocidade e duplex funciona e como configurá-la nos dispositivos de rede, como switches e placas de rede. Isso envolve a configuração das opções de auto-negociação e a seleção das velocidades e modos duplex apropriados para cada conexão.

A falha na configuração correta da negociação de velocidade e duplex pode levar a problemas de desempenho, como congestionamento de rede e colisões de pacotes. Portanto, é vital que os profissionais de redes compreendam essa habilidade para manter uma comunicação eficaz e evitar gargalos na rede.

4. Diagnóstico e Solução de Problemas

O diagnóstico e a solução de problemas são habilidades essenciais para qualquer profissional de redes. As redes são complexas e propensas a problemas, como falhas de conectividade, latência excessiva, perda de pacotes e muito mais.

Profissionais de redes habilidosos podem identificar rapidamente a origem dos problemas usando ferramentas de diagnóstico, como ping, traceroute, analisadores de protocolo e registros de eventos. Eles também compreendem os princípios de resolução de problemas em camadas, começando pela camada física (cabos, conectores) e progredindo até as camadas de aplicativos (softwares).

Além disso, a solução de problemas requer habilidades de resolução de problemas e pensamento lógico. Os profissionais de redes devem ser capazes de isolar problemas, tomar medidas corretivas eficazes e documentar suas descobertas para futuras referências.

5. Implementação de Redes em Conformidade

Implementar redes em conformidade com os padrões e políticas é fundamental para garantir a segurança e o desempenho da rede. Isso envolve a configuração adequada de dispositivos de rede, como firewalls, switches e roteadores, de acordo com as melhores práticas de segurança e conformidade regulatória.

Profissionais de redes precisam entender os requisitos de conformidade relevantes para suas redes, que podem variar dependendo da indústria e da localização geográfica. Eles devem ser capazes de implementar medidas de segurança, como criptografia, autenticação e controle de acesso, para proteger os dados e a integridade da rede.

Além disso, a conformidade inclui o monitoramento contínuo da rede para detectar qualquer atividade suspeita e tomar medidas corretivas imediatas. Isso pode envolver a análise de logs de segurança, a implementação de patches de segurança e a realização de auditorias regulares.

6. Atualização e Migração de Padrões

A tecnologia de redes está em constante evolução, e os profissionais de redes devem acompanhar as atualizações e migrações de padrões para manter suas redes atualizadas e eficientes. Isso inclui a transição de padrões mais antigos para novas tecnologias que ofereçam maior largura de banda, segurança e eficiência.

Profissionais de redes experientes devem estar cientes das últimas tendências em tecnologia de redes, como a migração para redes baseadas em nuvem, a implementação de IPv6 para substituir o IPv4 envelhecido e a adoção de protocolos de segurança mais robustos.

Além disso, eles devem ser capazes de planejar e executar migrações de padrões com o mínimo de interrupção para a operação da rede. Isso envolve a atualização de hardware e software, a migração de dados e a realização de testes rigorosos para garantir a integridade da rede após a migração.

RESUMO

Os Padrões Ethernet são um conjunto de diretrizes técnicas fundamentais que governam o funcionamento das redes de computadores. Para entender e aplicar esses padrões com sucesso, é essencial possuir um profundo conhecimento dos diferentes tipos de Ethernet, como 10BASE-T, 100BASE-TX, 1000BASE-T, e assim por diante. Além disso, é crucial compreender os protocolos de comunicação e as tecnologias subjacentes que sustentam esses padrões, como CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

A seleção e configuração dos cabos desempenham um papel crítico na implementação eficaz de redes Ethernet. O conhecimento das categorias de cabos, como Cat 5e, Cat 6, ou Cat 7, é fundamental para determinar a adequação de um cabo para uma determinada aplicação. A escolha correta do tipo de cabo, seu comprimento e a maneira como é conectado são aspectos cruciais para garantir uma transmissão de dados confiável e de alta velocidade.

A negociação de velocidade e duplex é outra habilidade vital no contexto da Ethernet. Os dispositivos Ethernet precisam se comunicar efetivamente sobre a velocidade de transmissão de dados (10/100/1000 Mbps) e o modo duplex (half-duplex ou full-duplex). Configurar essas configurações de forma adequada é essencial para evitar conflitos e garantir a melhor performance da rede.

O diagnóstico e a solução de problemas são habilidades críticas para manter uma rede Ethernet em funcionamento. Isso envolve a identificação e resolução de problemas de conectividade, interrupções na transmissão de dados, latência excessiva e outros problemas que podem afetar a operação da rede. Ferramentas como testadores de cabo e analisadores de protocolo são recursos valiosos para esse fim.

A implementação de redes em conformidade com os padrões Ethernet exige atenção meticulosa aos detalhes e a capacidade de seguir as especificações rigorosamente. Isso inclui a organização adequada dos cabos, a configuração correta dos dispositivos de rede, a implementação de políticas de segurança e a garantia de que todos os elementos da rede estejam em conformidade com os padrões Ethernet relevantes.

Por fim, a atualização e migração de padrões são habilidades necessárias para manter a rede atualizada com as tecnologias mais recentes. À medida que novos padrões Ethernet são desenvolvidos e adotados, é importante entender como migrar de padrões mais antigos para os mais recentes de forma eficiente, minimizando interrupções na operação da rede e aproveitando os benefícios das novas tecnologias.

Em resumo, os padrões Ethernet são a espinha dorsal das redes de computadores modernas, e uma compreensão profunda e habilidades abrangentes são essenciais para configurar, manter e aprimorar essas redes de maneira eficaz. Desde a escolha dos cabos até a solução de problemas e a migração de padrões, os profissionais de redes devem dominar essas habilidades para garantir o funcionamento suave e confiável das redes Ethernet.

ATIVIDADE DE FIXAÇÃO

1. O que é o padrão Ethernet e qual é a sua finalidade fundamental em redes de computadores?

2. Qual é a taxa de transmissão de dados do padrão Ethernet mais comumente utilizado em redes domésticas e de pequenas empresas?

3. Quais são as principais diferenças entre os padrões Ethernet 10BASE-T e 1000BASE-T?

4. O que é o padrão Ethernet Gigabit (1000BASE-X) e em que tipos de redes é mais comumente utilizado?

5. O que significa "half-duplex" e "full-duplex" em relação aos padrões Ethernet? Como eles diferem?

6. Quais são as características-chave do padrão Ethernet 10 Gigabit (10GBASE-T) e onde é amplamente implantado?

7. Qual é a diferença entre o padrão Ethernet e o padrão Fast Ethernet em termos de velocidade de transmissão de dados?

8. O que é o padrão Power over Ethernet (PoE) e como ele permite a transmissão de energia elétrica através de cabos Ethernet?

9. Qual é o padrão Ethernet mais recente e rápido atualmente disponível, e quais são suas especificações de velocidade?

10. Como o padrão Ethernet evoluiu ao longo dos anos para acomodar as crescentes demandas de largura de banda e melhorar a eficiência das redes de computadores?

TEMA 07

Protocolo TCP e UDP

Habilidades

- Identificar as principais diferenças entre TCP e UDP
- Configurar e gerenciar sockets TCP e UDP em aplicações
- Compreender o modelo de três vias do TCP para estabelecimento de conexões
- Diagnóstico de problemas de rede relacionados ao TCP e UDP
- Avaliar o desempenho de aplicativos usando TCP ou UDP
- Implementar medidas de segurança para proteger a comunicação TCP e UDP

Figura 8: Protocolo TCP e UDP. Fonte: https://projetocolabora.com.br/ods4/linguagem-simples/

Para obter uma comunicação é necessário que ambas as pessoas falem a mesma língua, não é diferente com os computadores, quando um computador necessita envia uma mensagem a outro, ambos precisam estar "conversando" na mesma linguagem, ou seja, é necessário ter um protocolo para obter a comunicação, como no mundo real existem várias línguas, para os computadores existem vários protocolos.

Nos tempos antigos para enviar uma mensagem para outros países, era necessário recorrer ao telegrama ou um telefone.

Atualmente os computadores necessitam ter protocolos para possibilitar a conexão entre si, entre diversos protocolos que existam hoje em dia, dois se destacam pela sua importância e usabilidade que são o TCP (Transmission Control Protocol) e o UDP (User Datagram Protocol).

O protocolo TCP

O protocolo TCP tem como característica ter uma transmissão confiável ponto-a-ponto, ou seja, se o {Computador (A) transmitir dados para o computador (B), será necessário enviar um ACK (Bit de Reconhecimento) para o computador (B), possibilitando a recuperação dos pacotes, rejeitando os pacotes duplicados e organizando os pacotes que forem chegando.

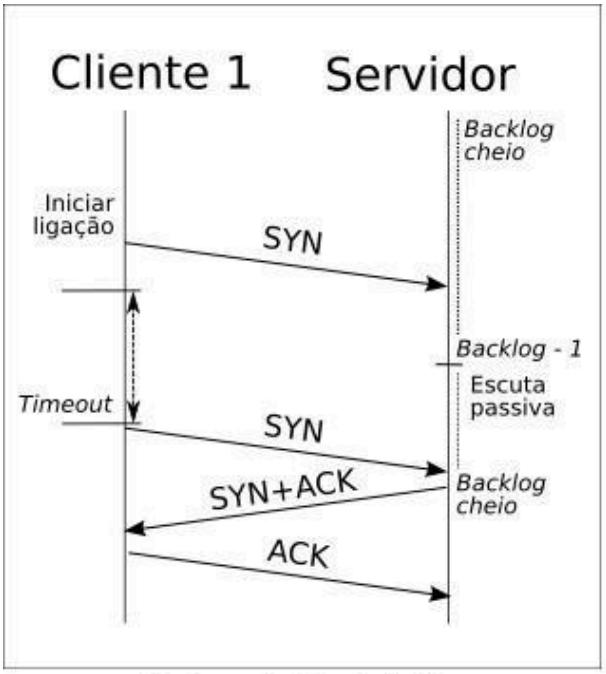
O TCP tem algumas características especificas como ordenar os pacotes, não possibilita o acumulo de pacotes na rede, e consegue transmitir ao mesmo momento a vários destinos diferentes, quando inicia uma conexão o também a fecha.

Quando estabelecemos a comunicação com o protocolo TCP com duas máquinas, quem envia os pacotes é denominado Cliente, e quem recebe os pacotes é chamado de Servidor, sendo assim a comunicação é estabelecida nos dois sentidos.

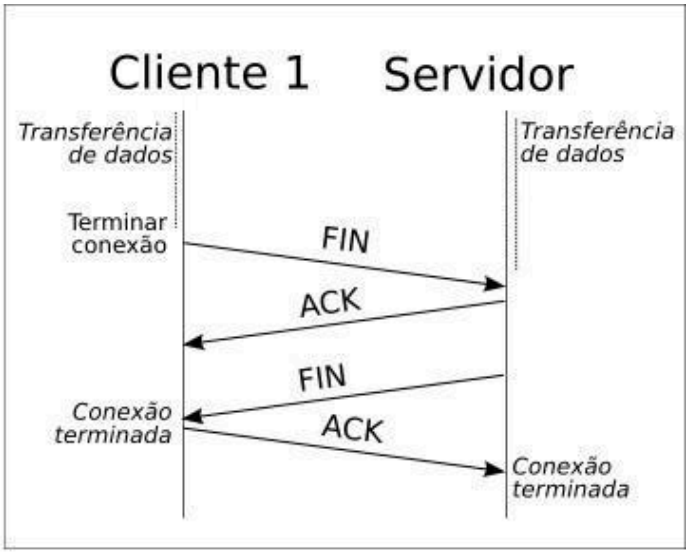
A comunicação do Protocolo TCP é realizada em três etapas:

- **1° Etapa:** O Cliente envia o SYN (Uma solicitação de conexão, no qual possui um sequencial de bytes para Cliente-Servidor);
- **2° Etapa:** O Servidor aceita o pedido de conexão (SYN), e envia um pacote aceitando o pedido (ACK), no qual possui um sequencial de bytes para Servidor-Cliente;
- **3° Etapa:** O Destino (servidor) transmite o ACK permitindo o SYN, então a troca de informações é efetuada entre esses hosts, quando se encerra a conexão, tanto o cliente ou servidor podem finalizar a conexão, um dos dois pode enviar o pacote FIN (Fim da conexão), quando se recebe o FIN a máquina envia um ACK aceitando o fim da conexão e algum tempo depois (milésimos de segundos) ele envia o FIN, finalizando de fato a conexão.

Obs.: Para cada pacote transmitido é inserido um checksum, que analisa se os pacotes estão danificados, ou perdidos durante a conexão, caso isso ocorra o protocolo retransmite os dados.



2- Conexão Estabelecida



1 - Conexão Finalizada

Protocolo UDP

O UDP é um protocolo que não é confiável, pois ele só envia os dados para o host de destino, por exemplo ele embala os datagramas e simplesmente envia, sem pedir confirmação de pacote ou verificar erros nos pacotes.

Este protocolo não dá garantias que o pacote será enviado até o seu destino, e muito menos que elas cheguem à ordem, pois não possui métodos para gerenciar os fluxos de dados.

Muitos pensam que por causa da falta de confiabilidade do protocolo UTP, que é melhor utilizar o TCP para obter a comunicação, entretanto vário serviço usufrui do protocolo UDP, pois é mais rápido o seu desempenho na rede.

O protocolo UDP é muito utilizado em serviço de multimídia (streaming e VOIP), pois se houver perda de dados não ocasiona delay na transmissão, se por acaso algum pacote for perdido, o mesmo não será perceptível para o usuário.

Portas TCP e Portas UDP

Existem várias portas TCP e UDP, e cada porta especifica um serviço na rede, de acordo com seu protocolo em questão.

Existem 65536 probabilidades de portas, isso porque são codificadas em 16 bits, por isso existe um órgão chamado IANA que parametriza essas portas e seus usos.

Porta de 0 a 1023 são as mais conhecidas, pois os administradores de rede ou usuário

com privilégio acessam os seus serviços. Já as portas de 1024 até 49151 são denominadas de portas registradas, e as portas de 49153 a 65535 são as portas dinâmicas ou privadas.

Abaixo uma tabela com os serviços/portas mais utilizadas hoje em dia:

Porta	TCP/UDP	Descrição / Serviço
20 /21	TCP	FTP
22	TCP/UDP	SSH
23	TCP/UDP	TELNET
25	TCP/UDP	SMTP
53	TCP/UDP	DNS
67/68	UDP	DHCP
80	TCP	HTTP
110	TCP	POP3
123	UDP	NTP
156	TCP/UDP	SQL
143		IMAP4
161	TCP/UDP	SNMP
179	TCP	BGP
443	TCP	HTTPS
1723	TCP/UDP	TUNEL PPTP
1863	TCP	MSN
3128	TCP	SQUID
3389	TCP	TERMINAL SERVER

Identificar as principais diferenças entre TCP e UDP:

TCP (Transmission Control Protocol) e UDP (User Datagram Protocol) são dois dos principais protocolos de transporte na pilha de protocolos da Internet. A principal diferença entre eles está na forma como lidam com a entrega de dados e na confiabilidade da comunicação.

O TCP é um protocolo orientado à conexão e fornece uma comunicação confiável. Isso significa que ele estabelece uma conexão antes de transmitir dados, verifica se os pacotes são entregues em ordem e garante que não haja perda de dados durante a transmissão. Ele é usado em situações em que a integridade dos dados é crucial, como em transferências de arquivos, navegação na web e emails.

Por outro lado, o UDP é um protocolo orientado a datagramas, o que significa que ele não estabelece uma conexão antes de enviar dados. Ele simplesmente envia os pacotes de dados para o destino, sem garantir a entrega ou a ordem dos pacotes. O UDP é mais rápido e eficiente em termos de latência, tornando-o ideal para aplicativos em tempo real, como videoconferência, streaming de áudio e jogos online.

Configurar e gerenciar sockets TCP e UDP em aplicações:

Configurar e gerenciar sockets TCP e UDP é fundamental para desenvolvedores de aplicativos que precisam de comunicação em rede. Sockets são interfaces de programação que permitem que aplicativos se comuniquem por meio de redes.

Para configurar e gerenciar sockets TCP, os desenvolvedores precisam estabelecer uma conexão utilizando funções como `socket()`, `bind()`, `listen()` e `accept()`. Eles também devem implementar a lógica de envio e recebimento de dados usando `send()` e `recv()`.

No caso de sockets UDP, os desenvolvedores criam sockets usando `socket()` e usam `sendto()` e `recvfrom()` para enviar e receber datagramas UDP. É importante lembrar que, ao contrário do TCP, não é necessário estabelecer uma conexão prévia.

O gerenciamento de sockets envolve a liberação adequada de recursos, tratamento de exceções e, em muitos casos, a implementação de mecanismos de timeout para lidar com a perda de pacotes.

Compreender o modelo de três vias do TCP para estabelecimento de conexões:

O modelo de três vias (three-way handshake) é fundamental para o estabelecimento de conexões TCP. Ele consiste em três passos sequenciais:

1. O cliente inicia a conexão enviando um segmento TCP com a flag SYN (synchronize) definida para o servidor. Isso indica o desejo de iniciar uma conexão.

2. O servidor recebe o segmento SYN, confirma a solicitação do cliente e responde com um segmento que possui as flags SYN e ACK (acknowledge) definidas. Isso significa que o servidor está disposto a estabelecer uma conexão e reconhece a solicitação do cliente.

3. O cliente recebe o segmento de resposta do servidor e confirma a conexão enviando um segmento com a flag ACK definida. Agora, a conexão está estabelecida e ambos os lados podem começar a trocar dados.

Esse processo garante que ambos os lados estejam cientes da intenção de estabelecer uma conexão e sincronizados para a comunicação subsequente. É um elemento fundamental para a confiabilidade do TCP.

Diagnóstico de problemas de rede relacionados ao TCP e UDP:

Diagnosticar problemas de rede relacionados a TCP e UDP é uma habilidade crítica para administradores de rede e desenvolvedores de aplicativos. Alguns dos problemas comuns incluem latência excessiva, perda de pacotes, congestionamento e configurações inadequadas.

Para diagnosticar esses problemas, é importante utilizar ferramentas como o `ping` e o `traceroute` para testar a conectividade e identificar pontos de falha na rede. Para problemas específicos de aplicativos, a análise de logs e o uso de ferramentas de monitoramento de rede são essenciais.

Além disso, entender os diferentes comportamentos do TCP e UDP é fundamental. O TCP lida automaticamente com retransmissões de pacotes perdidos, enquanto o UDP não o faz. Portanto, ao diagnosticar problemas com UDP, é necessário implementar lógica de recuperação de pacotes no aplicativo.

Avaliar o desempenho de aplicativos usando TCP ou UDP:

Avaliar o desempenho de aplicativos que usam TCP ou UDP envolve medir diversos aspectos, como latência, taxa de transferência e impacto na qualidade do serviço (QoS).

Para aplicativos que utilizam TCP, é importante avaliar a latência da conexão, pois o protocolo introduz alguma sobrecarga devido ao estabelecimento de conexão e ao controle de fluxo. A taxa de transferência também deve ser monitorada para garantir que atenda às necessidades da aplicação.

No caso de aplicativos UDP, a latência é crítica, especialmente para aplicativos em tempo real, como videoconferência e jogos online. Também é importante garantir que a taxa de transferência seja suficiente para a transmissão de dados em tempo real, sem atrasos perceptíveis.

Além disso, a QoS deve ser avaliada para garantir que a comunicação seja estável e livre de interrupções, independentemente de ser TCP ou UDP. Isso envolve o gerenciamento adequado da largura de banda e a priorização de pacotes.

Implementar medidas de segurança para proteger a comunicação TCP e UDP:

Implementar medidas de segurança para proteger a comunicação TCP e UDP é essencial para garantir a integridade e a confidencialidade dos dados transmitidos. Algumas das medidas comuns incluem:

- Criptografia: Usar protocolos como TLS/SSL para criptografar os dados transmitidos, garantindo que apenas os destinatários autorizados possam decifrá-los.

- Autenticação: Implementar mecanismos de autenticação, como senhas, tokens ou certificados, para garantir que apenas usuários autorizados tenham acesso à comunicação.

- Firewalls: Configurar firewalls para controlar o tráfego de entrada e saída, permitindo apenas o tráfego autorizado e bloqueando ameaças potenciais.

- VPN (Rede Privada Virtual): Usar VPNs para criar túneis de comunicação segura por meio de redes públicas, protegendo os dados de interceptação.

- Controle de acesso: Implementar políticas de controle de acesso para determinar quem pode iniciar ou participar de conexões TCP ou UDP.

- Monitoramento

de segurança: Utilizar ferramentas de monitoramento de segurança para detectar e responder a ameaças em tempo real.

A implementação adequada dessas medidas de segurança ajuda a proteger a comunicação TCP e UDP contra ameaças externas e garante que os dados sejam transmitidos com segurança.

RESUMO

O Protocolo de Controle de Transmissão (TCP) e o Protocolo de Datagrama de Usuário (UDP) são duas das principais tecnologias de comunicação utilizadas na internet. Identificar as principais diferenças entre TCP e UDP é fundamental para escolher o protocolo adequado para uma aplicação específica. Enquanto o TCP oferece uma conexão confiável e orientada a fluxo, garantindo que os dados sejam entregues na ordem correta e sem erros, o UDP é mais leve e rápido, porém menos confiável, já que não possui mecanismos de confirmação de entrega.

Configurar e gerenciar sockets TCP e UDP em aplicações é uma habilidade essencial para desenvolvedores de software e administradores de rede. Os sockets são os pontos de extremidade da comunicação e permitem que os dados sejam transmitidos entre dispositivos. Compreender o modelo de três vias do TCP para estabelecimento de conexões é crucial para garantir uma comunicação estável. Esse modelo envolve uma troca de mensagens entre cliente e servidor para estabelecer a conexão de forma segura.

O diagnóstico de problemas de rede relacionados ao TCP e UDP é uma habilidade crucial para manter a integridade da comunicação. Isso envolve a identificação de possíveis problemas, como perda de pacotes, congestionamento de rede ou falhas de roteamento, e a aplicação de soluções adequadas. Além disso, avaliar o desempenho de aplicativos usando TCP ou UDP é importante para garantir que a escolha do protocolo esteja alinhada com os requisitos de latência e confiabilidade da aplicação.

Implementar medidas de segurança para proteger a comunicação TCP e UDP é fundamental, especialmente em um cenário de ameaças cibernéticas crescentes. Isso inclui a criptografia dos dados transmitidos, autenticação de dispositivos e controle de acesso. Em resumo, dominar o TCP e o UDP envolve não apenas compreender suas diferenças e aplicações, mas também saber configurá-los, solucionar problemas de rede, otimizar o desempenho e garantir a segurança da comunicação. Essas habilidades são essenciais para profissionais de TI e desenvolvedores que trabalham com redes e aplicações online.

ATIVIDADE DE FIXAÇÃO

1. Qual é a principal diferença entre os protocolos TCP e UDP em termos de confiabilidade na entrega de dados?

2. Como o TCP garante a entrega ordenada de dados entre emissor e receptor?

3. Em que contexto ou cenários o TCP é preferível ao UDP na comunicação em rede?

4. Quais são as principais características do protocolo UDP e em que tipos de aplicativos ele é frequentemente utilizado?

5. Qual é o propósito da sequência de três vias (three-way handshake) no protocolo TCP e como ela é realizada?

6. Quais são as limitações do protocolo UDP em comparação com o TCP, e como essas limitações podem afetar aplicativos de tempo real?

7. Como o TCP lida com a retransmissão de pacotes perdidos e o controle de congestionamento?

8. Quando o uso de TCP pode levar a problemas de latência em aplicativos de alta sensibilidade ao tempo?

9. Qual é a diferença entre o modelo de comunicação orientada a conexão do TCP e o modelo de comunicação orientada a datagramas do UDP?

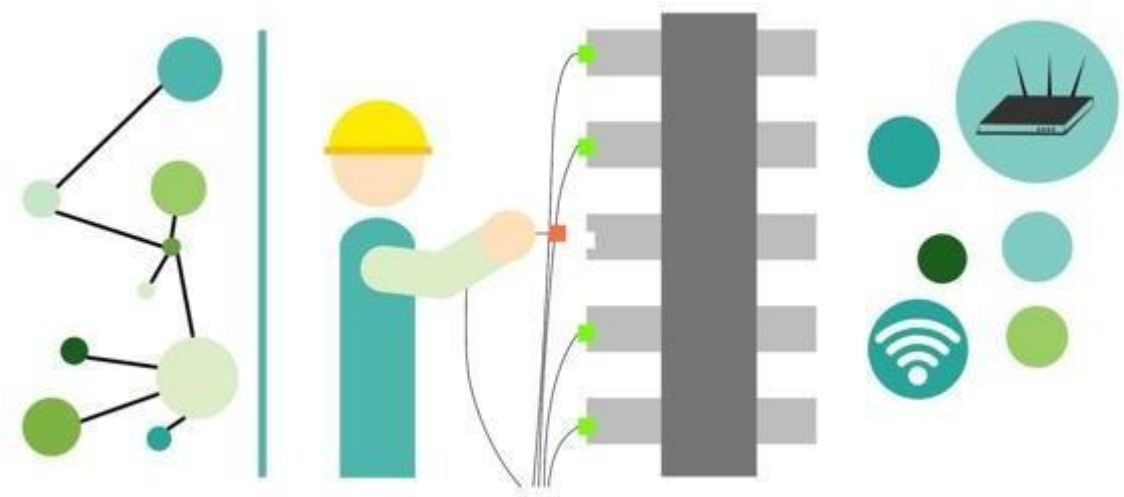
10. Quais medidas de segurança podem ser implementadas para proteger a comunicação via TCP e UDP e garantir a integridade e confidencialidade dos dados transmitidos?

TEMA 08

Dispositivo de Rede e Comandos Básico de Rede

Habilidades

- Identificar e Configurar Dispositivos de Rede
- Diagnosticar Problemas de Rede
- Gerenciar Tabelas de Roteamento
- Configurar ACLs (Listas de Controle de Acesso)
- Atualizar e Manter Firmware/Software de Dispositivos de Rede
- Interpretar Logs e Estatísticas de Rede



Fonte: https://pixabay.com/illustrations/network-infographics-cables-2389531/

Dispositivos de rede são ferramentas (equipamentos) que dispõe a possibilidade de ligar entre si, com o objetivo de compartilhar recursos, como uma rede residencial no qual tem o Modem (Que fornece a internet) que dê preferência é ligado ao um roteador (que compartilha a internet).

Confira o vídeo: https://www.youtube.com/watch?v=xuD1Hba-4fo

Dispositivos Ativos x Passivos na Rede

Passivo da Rede: São equipamentos de rede que são responsáveis por realizar a comunicação pelo meio físico, ou seja, são dispositivos que funcionam com sinais elétricos e não realizam uma análise de dados:

Alguns Exemplos:

- Pach Panel;
- Racks de Rede;
- Voice Panel;
- Cabos Metálicos;
- Cabos Ópticos;
- Conectores e Extensores;
- Patch Cable;
- Adapter Cable;
- Cable Link.

Ativo da Rede: Dispositivos que analisam e decidem sobre o modo como a informação atravessa o equipamento, afetando o funcionamento dos sistemas. Estes são responsáveis por

"decidirem" como os dados passam por seus equipamentos, de forma que influencia o funcionamento do sistema, seu objetivo é estabelecer uma comunicação entre o cliente e o servidor de uma maneira confiável e ágil, pois garantem que os serviços (portas) de rede funcionem como o esperado, porém para que esses equipamentos funcionem de forma correta você precisa adequá-los a realidade de seu ambiente de trabalho ou outro ambiente.

Alguns Exemplos:

- Switches;
- Hubs;
- Bridges;
- Modems;
- Roteadores;
- Placa de Rede (NIC);
- Firewall (equipamento);

- Chaveador KVM;
- Conversor de Mídia;
- Servidores;
- Access Points (Pontos de Acesso).

Equipamentos de Rede

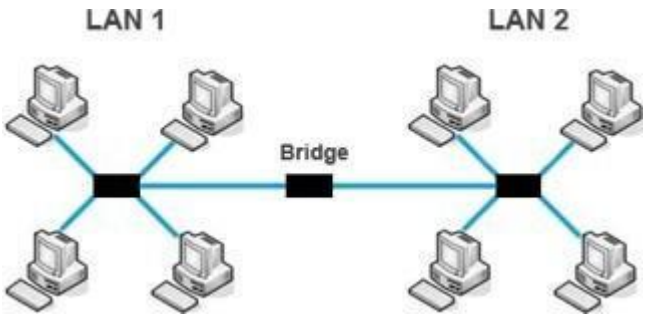
a. Hub

Este dispositivo funciona como um repetidor, ele simplesmente propaga a informação para todas as portas, menos para a qual enviou a mensagem, essa prática é denominada como Domínio de Colisão. Outro detalhe importante é que se dois computadores estiverem se comunicando o restante tem que esperar até a conexão entre eles finalizar, pois senão poderá ocorrer uma colisão de pacotes.

Fonte:
https://t1.gstatic.com/images?q=tbn:ANd9GcQtB_3nB3k61cmfnzXcOVPtuoKXnmO_GI6jQFS0tP3Z2ic8hizl

b. Bridge (Ponte)

Traduzido livremente como ponte, é uma ferramenta que tem como objetivo disponibilizar a comunicação entre duas redes diferentes, por exemplo, se eu estiver em uma rede apartada de outro computador, posso colocar um bridge para unir essas redes sendo assim possibilitando a troca de informação entre eles.



Fonte: https://antonioviana.wordpress.com/2009/11/20/dispositivos-de-ligacao-de-redes/

c. Switch

Esse dispositivo tem como objetivo de corrigir os erros de certos pacotes, e sistematizar o tráfego de informação na rede, pois evita o congestionamento ou as colisões dos arquivos, porque ele diferencia cada estação conectada por sua respectiva porta, então ele envia a informação diretamente ao destino possibilitando um tráfego de pacotes ágil e sem colisão.

:

Fonte : https://www.mercadolivre.com.br/switch-d-link-des-1210-52/p/MLB15798528

d. Roteador (Router)

Este é um dispositivo de rede que tem como objetivo de encaminhar os pacotes na rede, pois permite estabelecer uma comunicação entre diversos equipamentos de rede ou tecnologias aplicadas, também tem a disponibilidade de realizar o encaminhamento dos pacotes via rotas estáticas ou "Rotas Dinâmicas" depende muito do protocolo que vai utilizar.

Fonte:
www.niper.net/br/pt/products/routers/acx-series/acx2100-universal-metro-router.html

e. Placa de Rede

Conhecido como NIC (Network Interface Card), este dispositivo é responsável por possibilitar a comunicação entre os computadores da rede, ou seja, sua função principal é preparar, enviar e gerenciar as informações para a rede, e também "traduz" as informações que vem dos cabos e os transforma em bytes, para que o computador possa entender.

Fonte:
https://www.americanas.com.br/produto/3130334914/placa-de-rede-10-100-100-rj-45-pci-express-lotus

f. Roteador Wireless

Roteador Wireless (WiFi) tem como objetivo compartilhar a rede (INTERNET) para os diapositivos sem utilizar o meio físico.

Fonte: https://pgsconsultoriati.com/servicos/redesinfra-ti/seguranca-da-informacao/

g. Access Point

Tem como objetivo repetir o sinal, ou interligar redes wireless, ele serve como repetidor de sinal, e suas aplicações nos dias de hoje são considerável.

Fonte: https://www.bigdis2008.com/?category_id=5958767

h. Modem

Modem é um modulador de sinal, ou seja, é um dispositivo que visa converter sinais analógicos para digitais, ou vice-versa, isso possibilita que sejam transmitidos de forma coerente.

Fonte:
https://www.mercadolivre.com.br/terminal-gpon-tp-link-1-porta-gigabit-tx-6610-cor-preto-voltagem-110v220v/p/MLB24450029

Introdução sobre comandos básicos

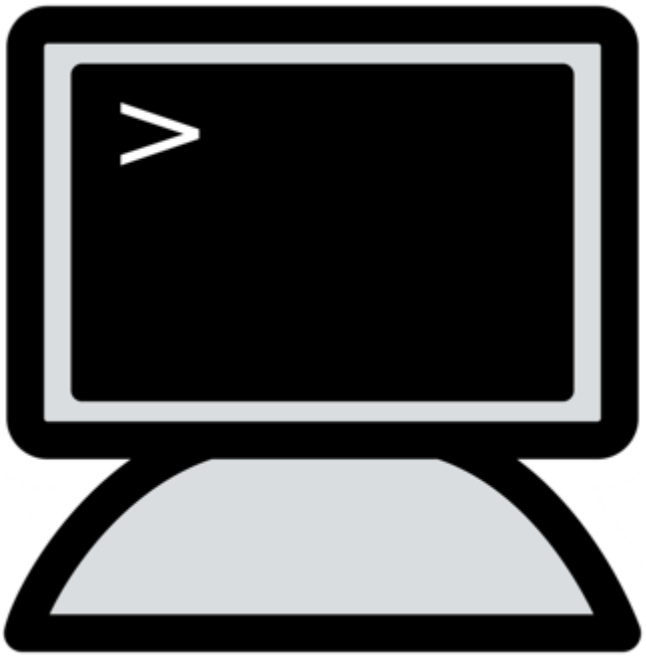


Figura 10: Comando Básico de Rede. Fonte:
https://www.codigofonte.com.br/dicas/um-comando-permite-que-voce-programe-seu-pc-com-windows-para-desligar-sozinho

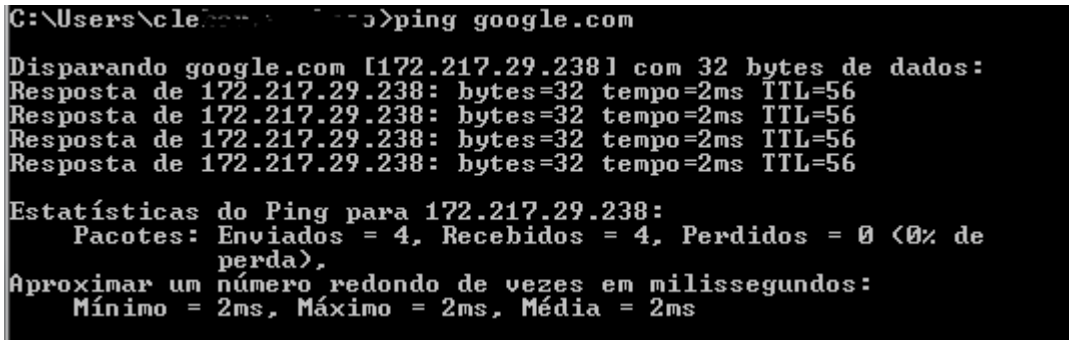
Introdução

Comando de rede tem como objetivo testar o serviço para verificar se está funcionando e identificar o problema, muito úteis no dia-a-dia, todos os sistemas operacionais tem um prompt de comando, o que varia são os comandos de Sistema operacional para outro, mas a funcionalidade do mesmo é "universal".

Os comandos que nós iremos ver agora é no Sistema Operacional Windows:

a. Ping

Com o ping podemos fazer uma medição de quantos milissegundos (ms), ou seja, mede o tamanho e o tempo para o pacote ser enviado e voltar, então quanto o menor for o valor de tempo indica uma maior velocidade.



Fonte: https://king.host/wiki/artigo/como-utilizar-o-comando-ping/

b. TraceRoute

Essa ferramenta possibilita descobrir qual o caminho que pacote (dados) faz desde sua origem até o destino, tem objetivo de verificar falhas de seus intermediários, também possibilita ver se há atrasos nas informações entre a origem e seus nós.

Só consegue verificar até 30 saltos até chegar ao destino.

Fonte: https://king.host/wiki/artigo/como-utilizar-o-comando-ping/

c. Ipconfig

Esta ferramenta demonstra a configuração do IPV4 e IPV6 de todas as placas de rede (IP, Gateway, Máscara de Rede e DNS), qual o adaptador da placa de rede, o MAC e o Domínio no qual está configurado.

- ipconfig /release = libera o ip;
- ipconfig /renew = renova o ip;
- ipconfig /flushdns = limpa o cache de DNS da máquina.

Fonte: https://www.mvteamcctv.com/pt/news/How-to-use-the-ping-command.html

d. NetStat

O comando Netstat exibe todas as portas e conexões pré-estabelecida.

NETSTAT

-a = Mostra todas as conexão e portas.

-e = Mostra as estatísticas Ethernet.

-n = Mostra os endereços e os números de portas (Decimal).

-p proto = Mostra as conexões para o protocolo especificado.

-r = Mostra o conteúdo da tabela do roteador.

-s = Mostra as estatísticas por protocolo.

-abnov = Mostra os processos que utilizam a conexão internet.

```
C:\Windows\system32>netstat -abnov

Conexões ativas

  Proto  Endereço local          Endereço externo        Estado           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING        740
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING        4
 Não é possível obter informações de propriedade
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING        1196
  CryptSvc
 [svchost.exe]
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING        440
 [wininit.exe]
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING        836
  eventlog
 [svchost.exe]
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING        944
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING        520
```

Fonte:
https://buildnetworks.blogspot.com/2019/09/como-configurar-o-fail2ban-com-asterisk.html

e. Route

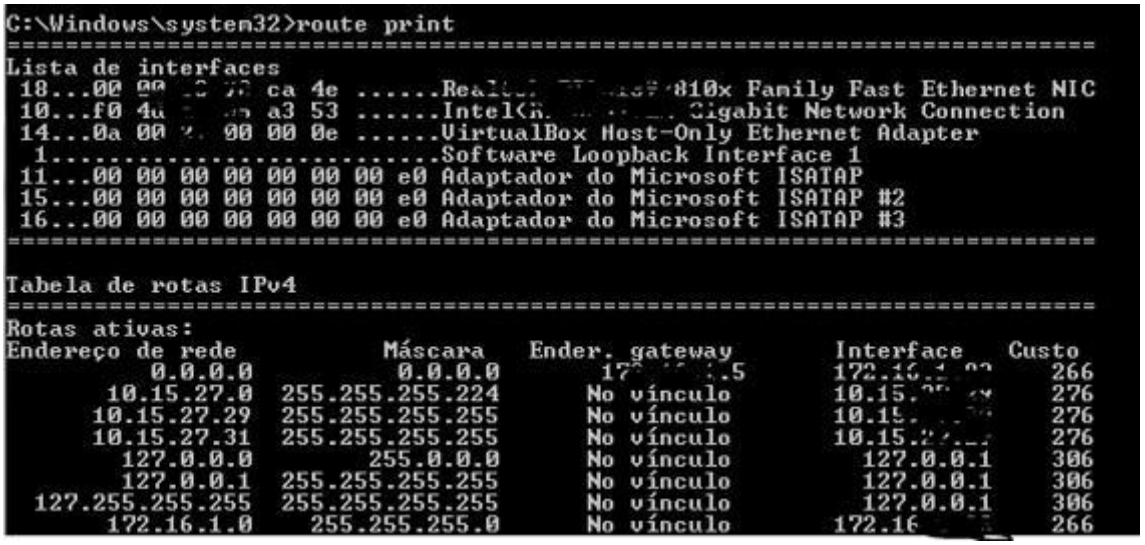
Mostra ou altera a tabela do roteador.

ROUTE

-f = deleta as tabelas do roteador.

-p = Aplica na tabela depois de reiniciar a máquina. PRINT = Mostra um itinerário.

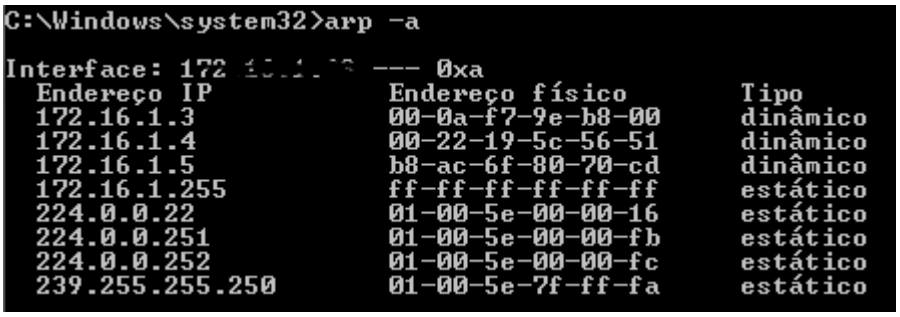
ADD = Acrescenta um itinerário.



Fonte:
https://www.geekzilla.com.br/tutorial-modificando-tabelas-de-roteamentowindows/

f. Arp

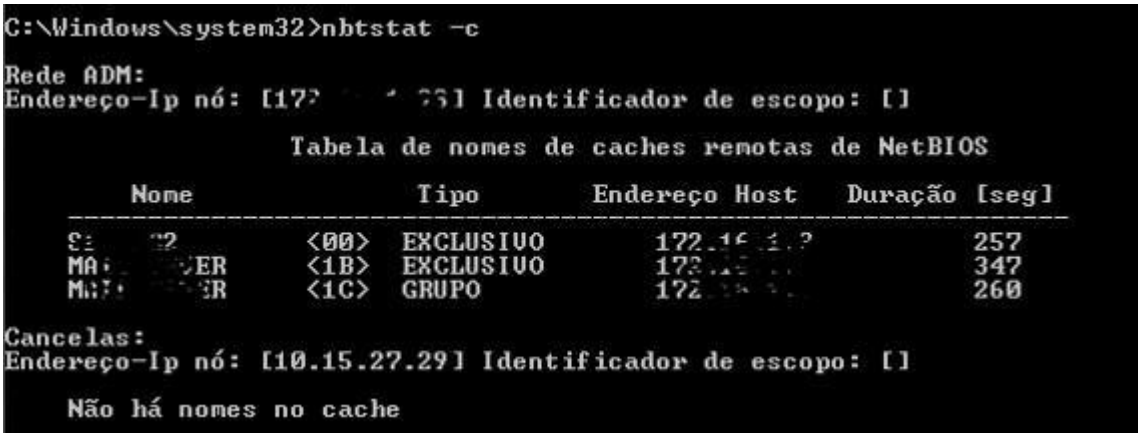
Resolve os endereços na rede em MAC, traduz os nomes e altera as tabelas do endereço IP.



Fonte:
https://www.geekzilla.com.br/tutorial-modificando-tabelas-de-roteamentowindows/

g. NbtStat

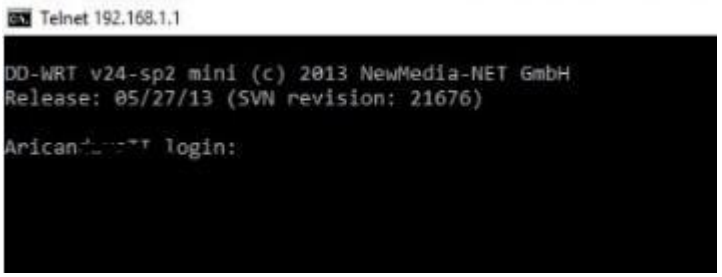
Atualiza o cache, e demonstra as estatísticas dos protocolos e suas conexões.


C:\Windows\system32>nbtstat -c
Rede ADM:
Endereço-Ip nó: [17
Identificador de escopo: []
Tabela de nomes de caches remotas de NetBIOS
Nome
Tipo
Endereço Host
Duração [seg]
<00> EXCLUSIVO
257
<1B> EXCLUSIVO
347
<1C> GRUPO
260
Cancelas:
Endereço-Ip nó: [10.15.27.29] Identificador de escopo: []
Não há nomes no cache

Fonte: https://www.tecmundo.com.br/tutorial/44083-como-recuperar-a-capacidade-completa-de-um-cartao-sd.htm

h. Telnet

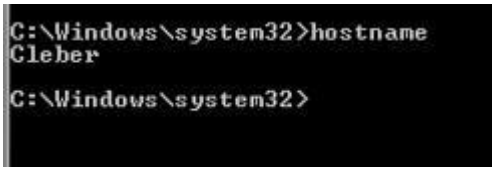
Esse serviço possibilita averiguar se o serviço TCP está "rodando" na máquina em questão, pode testar se a porta (serviço) em questão está funcionando ou não, e até mesmo entrar no equipamento caso o telnet esteja habilitado.



Fonte: http://excript.com/python/entrada-dados-python.html

i. Hostname

Demontra o nome da máquina.



Fonte: https://www.axtudo.com/solucao-nao-foi-possivel-encontrar-o-ambiente-de-recuperacao/

j. Nslookup

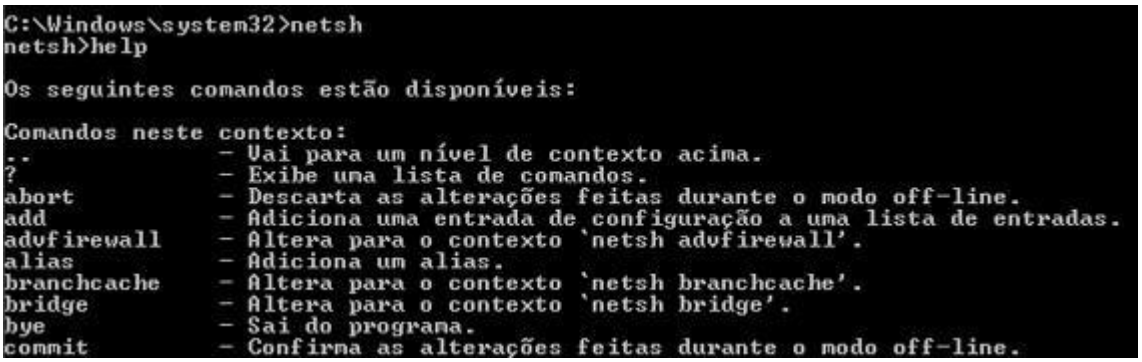
Essa ferramenta permite traduzir um nome de um host ou site em IPV4 ou IPV6 ou vice-versa.

Fonte:

https://www.dell.com/support/kbdoc/pt-pt/000138794/windows-server-reparo-do-banco-de-dados-do-active-directory-ap%C3%B3s-a-falha-do-controlador-de-dom%C3%ADnio

k. NetSh

Este comando Netsh é uma ferramenta que possibilita incluir ou excluir configurações de rede remotamente, ou executar script em modo BASH.



Fonte:
https://www.dell.com/support/kbdoc/pt-pt/000138794/windows-server-reparo-do-banco-de-dados-do-active-directory-ap%C3%B3s-a-falha-do-controlador-de-dom%C3%ADnio

RESUMO

Um dispositivo de rede é uma peça fundamental no ecossistema de comunicação moderno, permitindo a interconexão de diferentes sistemas e a transmissão de dados de forma eficiente. Para operar efetivamente nesse ambiente, é essencial possuir habilidades em identificar e configurar dispositivos de rede. Isso inclui a capacidade de reconhecer os diversos tipos de dispositivos, como roteadores, switches e firewalls, e configurá-los de acordo com as necessidades da rede, definindo endereços IP, máscaras de sub-rede e outras configurações essenciais.

No entanto, problemas de rede são inevitáveis, e é crucial ter a habilidade de diagnosticá-los de forma eficaz. Isso envolve a análise de conexões falhas, latência excessiva ou perda de pacotes, identificando a causa subjacente do problema e tomando as medidas corretivas necessárias para restaurar o desempenho da rede.

O gerenciamento de tabelas de roteamento é outra habilidade vital na administração de redes. Isso inclui a configuração de rotas estáticas e dinâmicas para garantir que os dados sejam encaminhados eficientemente pela rede, além de lidar com situações de roteamento complexas e cenários de failover.

A configuração de ACLs (Listas de Controle de Acesso) é um elemento-chave da segurança de rede. Isso envolve a definição de políticas de acesso que determinam quais dispositivos ou usuários têm permissão para se conectar à rede e quais tipos de tráfego são permitidos ou bloqueados, protegendo assim a rede contra ameaças externas e internas.

Manter o firmware e o software dos dispositivos de rede atualizados é essencial para garantir o desempenho e a segurança contínuos. Isso inclui a aplicação de patches de segurança, atualizações de recursos e correções de bugs, garantindo que os dispositivos estejam em conformidade com as últimas diretrizes e regulamentações.

Por fim, a interpretação de logs e estatísticas de rede desempenha um papel crítico na monitorização e solução de problemas. Isso envolve a análise de registros de eventos, tráfego de rede e estatísticas de desempenho para identificar anomalias, tendências ou problemas emergentes, permitindo uma resposta proativa para manter a rede em ótimo estado de funcionamento.

Em resumo, as habilidades relacionadas a dispositivos de rede e comandos básicos de rede são cruciais para garantir o funcionamento eficiente, seguro e confiável das redes de comunicação modernas. Desde a configuração de dispositivos até a solução de problemas e a manutenção contínua, essas habilidades capacitam os profissionais de redes a enfrentar os desafios complexos do mundo conectado de hoje.

ATIVIDADE DE FIXAÇÃO

1. O que é um switch em uma rede de computadores e qual é a sua função principal?

2. Quais são as principais diferenças entre um hub e um switch em termos de operação e eficiência?

3. Explique o papel de um roteador em uma rede e como ele facilita a comunicação entre redes diferentes.

4. Qual é a função de um firewall em uma rede e como ele contribui para a segurança da rede?

5. Descreva o que é um modem e como ele permite a conexão à Internet por meio de uma rede de área ampla (WAN).

6. Como o comando `ping` é usado para testar a conectividade com um host remoto e o que os resultados do comando podem indicar?

7. Qual é a finalidade do comando `ipconfig` (ou `ifconfig` em sistemas Unix/Linux) e como ele pode ser usado para exibir informações sobre a configuração de rede de um computador?

8. Explique o que é o comando `tracert` (ou `traceroute` em sistemas Unix/Linux) e como ele ajuda a identificar a rota que os pacotes de dados percorrem para chegar a um destino.

9. O que faz o comando `netstat` e como ele pode ser utilizado para listar as conexões ativas e portas abertas em um sistema?

10. Qual é a finalidade do comando `arp` e como ele é usado para mapear endereços IP em endereços MAC em uma rede local?

TEMA 09

Conceitos e modelos de serviços em Cloud

Habilidades

- Seleção de Modelos de Serviços Adequados
- Compreensão dos Níveis de Abstração
- Implementação e Gerenciamento de Recursos em Nuvem
- Otimização de Custos em Nuvem
- Segurança em Nuvem
- Integração de Serviços em Nuvem

Fonte: https://fortenetwork.io/pt_br/forte-backup/

Conceito

Cloud computing é uma expressão que começou a ser utilizada por volta de 2008, porém os conceitos e ideias utilizadas já existem a bastante tempo. No Brasil conhecida como computação em nuvem, se refere em sua essência a utilização em qualquer localidade sendo somente necessário uma conexão com a internet, não dependendo de uma plataforma ou aplicação específica.

Nesse capítulo, iremos nos aprofundar neste ótimo conceito que trouxe diversas facilidades e avanços tecnológicos devido sua capacidade e barateamento de custos e utilização.

História, da Cloud Computing

O Cloud Computing é um termo relativamente novo, porem seu conceito é bastante antigo. Essa não foi uma tecnologia criada e testada em laboratório e então inserida no mercado, por esse motivo é identificar sua origem é um pouco difícil.

Existem indícios de que esse modelo de serviço foi proposto na primeira metade dos anos 60 pelo cientista da computação John McCartthy, conhecido mundialmente por ter inventado o termo “Inteligência Artificial” ou a “IA”. Na época ele defendeu sua proposta chamada “Time sharring” ou computação por tempo compartilhado, onde nela, um computador pode ser poderia ser utilizado simultaneamente por mais de um usuário para ser realizado uma determinada tarefa, sendo aproveitado o tempo ocioso entre cada processo.

Note que, dessa maneira é possível aproveitar melhor os recursos disponíveis no computador, na época esse era um dispositivo bastante caro, com isso os gastos seriam diminuídos pois seria pago somente o tempo de uso do computador. O que de certa forma é a ideia do uso dos recursos utilizados no Cloud Computing hoje em dia.

Nessa época, o físico Joseph Carl Robnett Licklider participante da ARPA (Advanced Research Projects Agency), estava pensando na ideia de utilização dos computadores que não fosse somente uma calculadora muito potente.

Nessa ideia Licklider foi um dos primeiros a pensar na utilização de computadores de maneira conectada, permitindo comunicação global e compartilhamento de dados. Esse pensamento foi determinante para posteriormente dar origem a ARPANET, essa sendo a porta para a criação da Internet como conhecemos hoje.

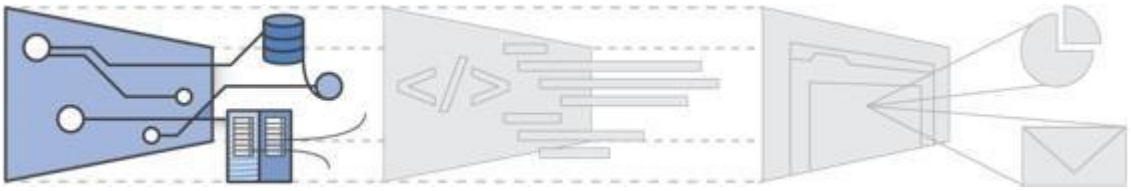
Várias tecnologias, conceitos e pesquisadores podem ser associados a esse assunto, porém ao juntarmos os trabalhos desses dois cientistas, pode-se ter uma grande ideia de como foi a origem e evolução da então conhecida posteriormente Cloud Computing.

a. Tipos de Serviços de Cloud Computing

No Cloud Computing são oferecidos os recursos de TI por meio de servidores em data centers conectados à internet. Em seus serviços a ideia é que possam ser dados e acessados de qualquer lugar do mundo e os recursos ficam disponíveis 24 horas por dia, sem necessidade de instalação de programas na máquina local, sendo possível o acesso somente pelo browser de internet.

Com isso, surgiram os seguintes tipos de serviços:

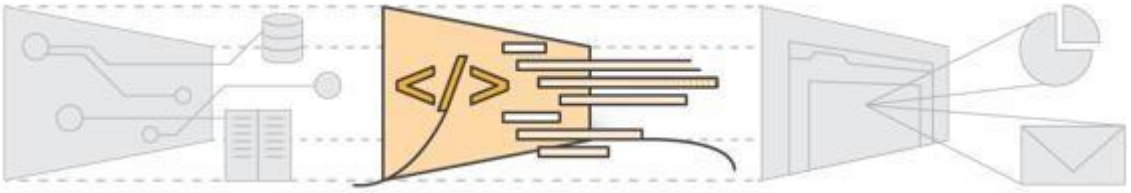
Infrastrucure as a Service (IaaS)



Legenda e Fonte?

Esse tipo de serviço oferece ao cliente toda infraestrutura necessária para que o mesmo utilize os servidores da melhor maneira que se encaixe em seu serviço, sendo possível a gerência que todos os recursos disponíveis.

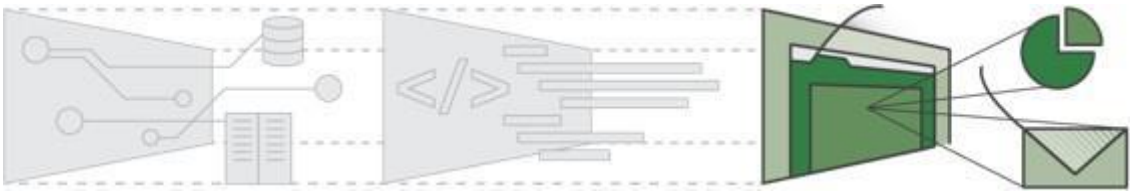
Platform as a Service (PaaS)



Legenda e Fonte?

A PaaS oferece as licenças de software, infraestrutura, manutenção, sistemas de comunicação e tudo o mais que for necessário para a publicação de um aplicativo/site. A liberdade de configuração e utilização vai depender do fornecedor de PaaS - se for mais ou menos flexível no quanto o usuário pode configurar da plataforma.

Software as a Service (SaaS)



Legenda e Fonte?

Ligado ao Cloud Computing primeiramente surgiram os serviços de Software as a service ou em português Aplicação como Serviço, o SaaS. Basicamente esse tipo de oferta de

serviço oferece uma aplicação (software) ao usuário, que não precisa adquirir de licenças de instalação nem mesmo é necessário ter um espaço físico com servidores dedicados para utilizar da aplicação.

b. Exemplos de aplicações em Cloud Computing

Hoje em dia temos muitas opções de programas/serviços que utilizam o Cloud Computing, iremos listar aqui alguns para vocês terem uma ideia de quais são.

Adobe Creative Cloud

Serviço de nuvem oferecido pela Adobe que inclui armazenamento, acesso a ferramentas da empresa e integração com outros produtos Adobe.

Fonte: https://www.iconarchive.com/show/flat-strokes-app-icons-by-hopstarter/Adobe-Creative-Cloud-icon.html

Google Apps

Pacote de produtos oferecidos pelo Google, que inclui ferramentas de edição de texto, criação de planilhas, apresentações, ferramenta de agenda, integração com e-mail próprio, entre outras funcionalidades.

Fonte: https://technewsbrasil.com.br/aplicativos-google-gratuitos-nao-tao-famosos/

Aprex

Conjunto de aplicativos online, o Aprex oferece soluções para profissionais e empresas, como: calendário, gerenciador de contatos, lista de tarefas, serviço de e-mail marketing, armazenamento de arquivos, apresentações, entre outras.

Evernote

O Evernote é um aplicativo para criação e armazenamento de notas. Ótima opção para reuniões e momentos de registrar ideias iniciais de um projeto. Inclui ferramentas de compartilhamento, edição, organização e localização de dados.

Fonte: https://pt.wikipedia.org/wiki/Evernote

OneDrive

Aplicativo de armazenamento em nuvem, o OneDrive é um produto da Microsoft. Por isso, outros produtos da empresa possuem integração com ele como, por exemplo, contas Outlook.com.

Fonte:
https://tecnoblog.net/responde/como-converter-imagem-em-texto-no-onedrive-ocr/

Dropbox

Outra opção de armazenamento em nuvem, o Dropbox possui vários recursos de compartilhamento de arquivos entre equipes e uma interface fácil e intuitiva.

Fonte: https://www.flaticon.com/br/icone-gratis/dropbox_733545

Office online

Os produtos do pacote Office da Microsoft com o funcionamento Cloud Computing: Word, Excel, PowerPoint, OneNote, Sway, E-mail, Calendário, Docs.com, e outros. Com esta aplicação, é possível criar e compartilhar documentos de qualquer lugar com conexão à internet.

Fonte:
https://techcommunity.microsoft.com/t5/microsoft-365-groups/jpg-artifacts-on-groups-logo-avatar/m-p/2159

c. Vantagens e desvantagens:

Como qualquer tipo de software ou hardware, existem vantagens e desvantagens a serem pesadas na hora de obter o que deseja, e com o Cloud Computing não é diferente, alguns pontos positivos são:

Tranquilidade:

Uma vez que todo o processamento de dados é feito na nuvem, o usuário não precisa se preocupar com problemas de compatibilidade de hardware/software e segurança.

Comodidade:

A vantagem mais óbvia. Em qualquer lugar ou hora é possível acessar os dados da

nuvem. Tudo o que é necessário é um dispositivo com acesso à internet.

Confiabilidade:

O acesso e processamento de dados não depende exclusivamente de um servidor, pelo que, em caso de falha o serviço não fica comprometido.

Capacidade de armazenamento virtualmente ilimitada

O usuário não precisa de se preocupar com o alojamento da informação porque esta não fica alojada no seu computador.

Temos também o outro lado da moeda, vejamos os pontos negativos a se destacar:

Dependência:

O acesso aos dados da nuvem depende obrigatoriamente de uma conexão à internet. Caso esta não exista não existem alternativas para contornar o problema.

Recuperação de dados:

Apesar da nuvem ser bastante confiável, falhas e erros são sempre possíveis. Caso a nuvem deixe de funcionar, todos os dados estão comprometidos e podem, eventualmente, ser perdidos.

Opções mais limitadas:

Esta é uma limitação técnica. Não é possível (pelo menos atualmente) desenvolver softwares muito complexo que processe a informação fora do computador local.

Vulnerabilidade:

A segurança informática é um tópico transversal em qualquer tema desta área. Aqui não é exceção. Todos os dados da nuvem estão vulneráveis a ataques hackers.

Conclusão

Seleção de Modelos de Serviços Adequados:

A seleção de modelos de serviços adequados em cloud computing é uma habilidade crucial para profissionais e organizações que desejam aproveitar ao máximo os benefícios da computação em nuvem. Existem três modelos de serviços predominantes: IaaS (Infraestrutura como Serviço), PaaS (Plataforma como Serviço) e SaaS (Software como Serviço).

A habilidade de selecionar o modelo correto começa com uma análise detalhada das necessidades do projeto ou da organização. O IaaS oferece controle total sobre a infraestrutura subjacente, permitindo a criação de servidores virtuais, redes e armazenamento personalizados. É ideal para projetos que exigem flexibilidade máxima e controle direto sobre o sistema operacional e aplicativos.

O PaaS oferece um ambiente de desenvolvimento e implantação, simplificando o ciclo de vida do software. É apropriado para equipes de desenvolvimento que desejam se concentrar na criação de aplicativos, sem se preocupar com a infraestrutura.

O SaaS, por outro lado, fornece aplicativos prontos para uso, hospedados na nuvem e acessados por meio de navegadores da web. É a escolha certa para organizações que buscam soluções prontas para uso, como serviços de e-mail, gerenciamento de relacionamento com o cliente (CRM) e colaboração online.

A habilidade de escolher o modelo de serviço certo também envolve considerar fatores como custo, escalabilidade, desempenho e requisitos de segurança. Um profissional competente em seleção de modelos de serviços em nuvem pode otimizar as operações, economizar custos e garantir que a tecnologia em nuvem atenda às metas de negócios.

Compreensão dos Níveis de Abstração:

A compreensão dos níveis de abstração em cloud computing é fundamental para tomar decisões informadas sobre como implementar e gerenciar recursos na nuvem. Cada modelo de serviço oferece um nível diferente de controle e responsabilidade.

No nível mais baixo de abstração, encontramos o IaaS, onde os usuários têm controle total sobre a infraestrutura virtualizada. Eles podem criar máquinas virtuais, redes, armazenamento e instalar sistemas operacionais e aplicativos. Isso oferece máxima flexibilidade, mas também exige um maior grau de gerenciamento e manutenção.

Em um nível intermediário de abstração, temos o PaaS. Aqui, os usuários se concentram na criação de aplicativos e não precisam se preocupar com a infraestrutura subjacente. O PaaS oferece um ambiente de desenvolvimento pré-configurado, acelerando o ciclo de desenvolvimento e implantação.

No nível mais alto de abstração, encontramos o SaaS, onde os usuários simplesmente acessam aplicativos prontos para uso pela internet. Não há necessidade de gerenciar infraestrutura, atualizações de software ou configurações de segurança. Isso torna o SaaS uma escolha conveniente para muitas organizações.

A compreensão desses níveis de abstração permite que profissionais e empresas escolham o modelo de serviço que melhor atende às suas necessidades de negócios, equilibrando controle, complexidade e conveniência.

Implementação e Gerenciamento de Recursos em Nuvem:

Implementar e gerenciar recursos em nuvem é uma habilidade essencial para aqueles que desejam migrar para a computação em nuvem. Isso envolve configurar servidores virtuais, redes, armazenamento e outros recursos de acordo com as necessidades do projeto ou da organização.

Na implementação, os profissionais devem ser capazes de provisionar máquinas virtuais, definir regras de firewall, configurar redes virtuais e armazenar dados de maneira eficiente. Isso requer um conhecimento sólido das ferramentas de gerenciamento em nuvem, como AWS, Azure ou Google Cloud, e a capacidade de escrever scripts para automação de tarefas.

O gerenciamento de recursos em nuvem envolve monitoramento constante, otimização de desempenho, aplicação de patches de segurança e dimensionamento adequado dos recursos. Profissionais competentes em gerenciamento de recursos em nuvem podem garantir que os recursos estejam disponíveis quando necessário, ao mesmo tempo em que controlam os custos.

Além disso, eles devem estar cientes das práticas recomendadas de segurança em

nuvem, como a configuração de políticas de acesso, criptografia de dados e auditorias regulares para proteger os recursos contra ameaças cibernéticas.

Otimização de Custos em Nuvem:

A otimização de custos em nuvem é uma habilidade fundamental para garantir que uma organização obtenha o máximo valor de seus investimentos em cloud computing. Os serviços em nuvem são geralmente faturados com base no uso, o que significa que os custos podem aumentar rapidamente se não forem monitorados e gerenciados de forma eficaz.

Profissionais de otimização de custos em nuvem devem ser capazes de identificar recursos subutilizados ou não utilizados e desativá-los para economizar dinheiro. Isso inclui desligar máquinas virtuais ociosas, reduzir o tamanho de instâncias quando possível e usar armazenamento de acordo com as necessidades reais.

Além disso, a habilidade de escolher os tipos de instâncias corretos e ajustar a capacidade de acordo com as demandas sazonais ou flutuantes é essencial para controlar os custos. Isso pode envolver a implementação de políticas de dimensionamento automático.

Outras práticas de otimização incluem a análise detalhada das faturas em nuvem, o uso de serviços de orçamento e alerta, e a consideração de opções de preços reservados ou de instâncias spot para economizar custos a longo prazo.

Profissionais habilidosos em otimização de custos em nuvem podem ajudar suas organizações a aproveitar ao máximo os benefícios da computação em nuvem, mantendo os gastos sob controle.

Segurança em Nuvem:

A segurança em nuvem é uma habilidade crítica para garantir que os recursos e dados armazenados em ambientes de nuvem permaneçam protegidos contra ameaças cibernéticas. Isso envolve a aplicação de práticas e medidas de segurança específicas para a nuvem.

Os profissionais de segurança em nuvem devem ser capazes de configurar políticas de controle de acesso, autenticação multifator, criptografia de dados em repouso e em trânsito, e

auditorias regulares para detectar e mitigar vulnerabilidades.

Além disso, eles devem estar cientes das melhores práticas de segurança em nuvem para garantir a conformidade com regulamentações de privacidade e proteção de dados, como o GDPR (Regulamento Geral de Proteção de Dados) ou o HIPAA (Lei de Portabilidade e Responsabilidade de Seguro Saúde).

A habilidade de monitorar e responder a eventos de segurança em tempo real, como intrusões ou atividades suspeitas, é essencial para proteger a infraestrutura em nuvem. Isso pode envolver o uso de ferramentas de segurança em nuvem, como sistemas de detecção de intrusão (IDS) e sistemas de prevenção de intrusão (IPS).

Profissionais competentes em segurança em nuvem são cruciais para garantir a confidencialidade, integridade e disponibilidade dos dados em ambientes de nuvem.

Integração de Serviços em Nuvem:

A integração de serviços em nuvem é uma habilidade necessária para garantir que diferentes serviços e aplicativos em nuvem possam se comunicar de maneira eficiente e interagir de forma coesa em um ambiente de nuvem.

Isso envolve a compreensão de APIs (Interfaces de Programação de Aplicativos) e protocolos de comunicação utilizados pelos serviços em nuvem. Profissionais de integração devem ser capazes de projetar e implementar soluções que permitam a troca de dados e informações entre sistemas em nuvem e locais.

Além disso, eles devem ser proficientes na configuração de serviços de autenticação e autorização, como o OAuth, para garantir que apenas aplicativos e usuários autorizados tenham acesso aos dados em nuvem.

A habilidade de integrar serviços em nuvem com sistemas existentes, como ERPs (Enterprise Resource Planning) ou CRMs (Customer Relationship Management), é fundamental para otimizar processos de negócios e garantir a consistência dos dados em toda a organização.

Profissionais de integração de serviços em nuvem desempenham um papel crucial na criação de ambientes de nuvem coesos e eficientes, permitindo que as organizações aproveitem ao máximo os recursos em nuvem e alcancem seus objetivos de negócios.

RESUMO

Os conceitos e modelos de serviços em nuvem desempenham um papel crucial na era digital, permitindo que organizações obtenham flexibilidade, escalabilidade e eficiência na entrega de serviços de TI. Para aproveitar ao máximo a computação em nuvem, é essencial possuir habilidades multifacetadas que abrangem desde a seleção de modelos de serviços adequados até a garantia da segurança e otimização de custos.

A escolha dos modelos de serviços adequados é o ponto de partida. Os principais modelos incluem Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS). A compreensão dos níveis de abstração associados a esses modelos é fundamental, pois influenciam a gestão e a personalização dos recursos em nuvem. Cada modelo oferece diferentes níveis de controle sobre a infraestrutura subjacente e requer habilidades distintas para sua configuração e operação.

A implementação e gerenciamento de recursos em nuvem exigem competências técnicas para configurar servidores virtuais, redes, bancos de dados e outros recursos. A capacidade de automatizar essas tarefas é crucial para manter a escalabilidade e a eficiência operacional. Além disso, a otimização de custos em nuvem é uma habilidade crucial para evitar gastos desnecessários, maximizando o ROI.

A segurança em nuvem é uma prioridade constante. Profissionais precisam garantir que os dados e os aplicativos estejam protegidos contra ameaças cibernéticas. Isso envolve a implementação de práticas de segurança, como autenticação, autorização, criptografia e monitoramento constante. A integração de serviços em nuvem também é uma habilidade-chave, pois permite que aplicativos e sistemas se comuniquem e funcionem de maneira eficiente em ambientes híbridos ou multicloud.

Em resumo, os conceitos e modelos de serviços em nuvem são fundamentais na transformação digital das organizações. Dominar as habilidades de seleção de modelos adequados, compreensão dos níveis de abstração, implementação e gerenciamento de recursos, otimização de custos, segurança e integração de serviços é essencial para aproveitar ao máximo os benefícios da computação em nuvem e atender às crescentes demandas das empresas modernas.

ATIVIDADE DE FIXAÇÃO

1. O que é computação em nuvem e como ela se diferencia dos modelos de computação tradicionais?

2. Explique o conceito de "modelo de serviço" em nuvem e dê exemplos de modelos de serviço comuns.

3. Quais são os três principais modelos de serviço em nuvem, e como eles se diferenciam em termos de responsabilidades do provedor e do cliente?

4. Qual é a principal característica do modelo IaaS (Infraestrutura como Serviço) e quando ele é mais adequado?

5. Descreva o modelo PaaS (Plataforma como Serviço) e como ele pode acelerar o desenvolvimento de aplicativos.

6. Quais são os principais benefícios e desafios do modelo SaaS (Software como Serviço) para empresas e usuários finais?

7. O que é a abordagem de nuvem híbrida e como ela combina diferentes modelos de serviço?

8. Explique o conceito de "escalabilidade" em nuvem e como os modelos de serviço podem afetar a escalabilidade de uma aplicação.

9. Quais são os fatores-chave que uma organização deve considerar ao escolher o modelo de serviço em nuvem mais adequado para suas necessidades?

10. Como a escolha do modelo de serviço em nuvem pode afetar os requisitos de segurança e conformidade de uma organização?

TEMA 10

Arquitetura e Implementação e Cloud

Habilidades

- Design de Arquitetura em Nuvem
- Implementação de Infraestrutura como Código (IaC)
- Orquestração de Contêineres e Kubernetes
- Segurança em Cloud
- Otimização de Recursos em Nuvem
- Monitoramento e Solução de Problemas em Nuvem

Figura 1 Arquitetura e Implementação e Cloud. Fonte
:https://www.istockphoto.com/br/vetor/conceito-de-servi%C3%A7o-de-computa%C3%A7%C3%A3o-em-nuvem-de-armazenamento-de-tecnologia-de-gm1221331398-357950188

O que é essa tal de arquitetura Cloud?

Nada mais, nada menos que a integração de diversos componentes tecnológicos na configuração e estruturação de um ambiente cloud corporativo, que responda aos requisitos e às necessidades de negócio, equilibrando custos, riscos e benefícios.

Na prática, arquitetura cloud envolve a avaliação das tecnologias disponíveis, assim como configuração de uma série de ferramentas, explanando os impactos sobre a organização e, por fim, custos. Assim como a arquitetura predial, a arquitetura cloud é como se fosse a planta da construção, no caso é a nossa planta de estruturas tecnológicas.

Vantagens

Arquitetura Cloud permite que as empresas reduzam ou até mesmo eliminem seu uso com infraestrutura, no servidor e no armazenamento locais, sendo assim reduzindo gastos som equipamentos.

De modo geral, o meio corporativo que adot a arquitetura de nuvem transferem os recursos de TI para a nuvem pública, o que elimina a demanda de servidores e armazenamento locais e reduz a necessidade de espaço físico, refrigeração e energia para data centers, substituindo-os por despesas mensais com TI, ou seja, não se gasta com equipamentos físicos e sim com aluguel ou mensalidades de espaços virtuais (em Cloud).

Essa mudança de despesas de capital para despesas operacionais é um dos principais motivos da popularidade da computação cloud na atualidade.

Existem três modelos principais de arquitetura de nuvem que estão levando as organizações para a nuvem. Cada um deles tem os próprios benefícios e recursos importantes.

Falamos deles no Tema anterior

Software como serviço (SaaS)	**Plataforma como serviço (PaaS)**	**Infraestrutura como serviço (IaaS)**

Vale destacar que existem vários outros modelos de arquitetura cloud, vou deixar alguns exemplos aqui e aguçar sua curiosidade sobre o tema:

Function as a Service (*Faas*),

Everything as a Service (*Xaas*),

Content as a Service (*CaaS*),

Energy Storage as a Service (*ESaaS*),

Database as a Service (*BdaaS*),

Backup as a Service (*BaaS*),

Game as a Service (*GaaS*),

Robots as a Service (*RaaS*),

Veja alguns dos motivos para aderir:

- Acelerar o fornecimento de novos apps,
- Reutilização da arquitetura nativa da nuvem, como o Kubernetes, assim moderniza suas aplicações e otimizar todo processo de desenvolvimento,
- Conformidade,
- Maior transparência de recursos,
- Arquitetura de nuvem híbrida para permitir o dimensionamento em tempo real dos aplicativos conforme a mudanças de escopo,
- Cumprimento de metas,

Como funciona a arquitetura de Cloud?

Assim como na arquitetura predial que tem diversos tipos de plantas, padrões, processos de produção e criação, nós também temos vários modelos de arquitetura, tais como arquiteturas públicas, privadas, híbridas e multi-cloud.

Veja uma comparação entre eles:

Arquitetura pública: Geralmente são ambientes de nuvem criados em uma infraestrutura de TI que não é de propriedade do usuário final. Alguns dos maiores provedores de nuvens públicas são: Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure. Toda aquele cloud que tem um ambiente particionado e redistribuídos para vários locatários, caracteriza-se público. A cobrança de taxas deixou de ser uma característica primordial no cloud público. Alguns provedores, como a Massachusetts Open Cloud, permitem que os locatários as usem gratuitamente.	**Arquitetura privada**: Nuvem privada nada mais é que um cloud proprietário e gerenciada de forma privada, geralmente no próprio servidor local da empresa. Porém, a nuvem privada também pode ir além e incluir diversos locais de um servidor ou espaço alugado em instalações de localizações geograficamente diversas. Essa exclusividade tem um custo, é mais elevado que as soluções de nuvem pública, mas uma arquitetura de nuvem privada é mais personalizável e pode oferecer segurança de dados de maneira rigorosa em relação a pública.
Arquitetura híbrida: um cloud híbrido combina a eficiência operacional da cloud pública com os recursos de segurança de dados da nuvem privada. As nuvens híbridas ajudam a consolidar recursos de TI e permitem que as empresas migrem cargas de trabalho entre ambientes, dependendo de seus requisitos de segurança de dados e de TI.	**Arquitetura multi-cloud**: a arquitetura multi-cloud é aquela que usa vários serviços de computação em nuvem pública. Uma das vantagens de um ambiente multi-cloud é a flexibilidade maior para escolher e implantar os serviços de computação em nuvem que é a mais flexível em atender aos mais variados tipos de escopo. Outra vantagem é não contar apenas com um único provedor de serviços, o que reduz os custos e diminui a probabilidade de dependência de provedor. Além disso, a arquitetura multi- cloud pode ser necessária para executar aplicativos em contêineres baseados em microsserviços, em que os serviços necessitem de várias nuvens.

Pontos essenciais na arquitetura Cloud:

Virtualização: são criadas com base na virtualização de servidores, armazenamento e redes. Os recursos virtualizados são uma representação baseada em software, virtual, ou até mesmo um recurso físico, como servidores ou armazenamento. Essa camada de abstração permite que várias aplicações utilizem os mesmos recursos físicos, o que aumenta a eficiência de servidores, armazenamento e rede.

Infraestrutura: Existem servidores reais, E Toda a infraestrutura conta com os mesmos itens de um servidor tradicional, persistindo dados e equipamentos de rede, tais como switches e roteadores.

Middleware: O middleware atua como uma "camada" capaz de mediar entre várias tecnologias de software para que as informações mesmo que de fontes diferentes, sejam transferidas sem que suas diferenças de protocolo, plataforma, arquitetura, SO interfiram no processo.

Gerenciamento: Essas ferramentas monitoram continuamente o desempenho e a capacidade do ambiente de nuvem. A partir de um único console, as equipes de TI podem rastrear o uso, implantar novos aplicativos, integrar dados e garantir a recuperação de acidentes.

Software de automação A entrega de serviços críticos de TI por meio de automação e políticas predefinidas pode reduzir significativamente as cargas de trabalho de TI, simplificar a entrega de aplicativos e reduzir custos. Em uma arquitetura de nuvem, a automação é usada para facilitar o dimensionamento vertical dos recursos do sistema para acomodar picos nas demandas de poder de processamento, implantar aplicativos para atender às demandas flutuantes do mercado ou garantir a governança em ambientes de nuvem.

Design de Arquitetura em Nuvem:

O design de arquitetura em nuvem é um processo crítico para o sucesso de qualquer projeto de computação em nuvem. Envolve a criação de uma estrutura sólida e escalável que atenda aos requisitos de negócios, mantendo a eficiência, a segurança e o desempenho. Uma arquitetura em nuvem bem projetada considera vários fatores:

- Escalabilidade: Deve ser capaz de lidar com aumentos significativos na carga de trabalho sem degradação do desempenho. Isso geralmente envolve a distribuição de recursos em várias regiões geográficas ou zonas de disponibilidade.

- Alta Disponibilidade: A arquitetura deve ser projetada para minimizar o tempo de inatividade e garantir a continuidade dos serviços, mesmo em caso de falha de hardware ou software.

- Segurança: Deve incluir medidas de segurança robustas, como grupos de segurança, VPNs, criptografia, autenticação de dois fatores e monitoramento de segurança constante.

- Desempenho: Deve garantir que os aplicativos e serviços tenham um desempenho adequado, levando em consideração fatores como latência de rede e dimensionamento correto dos recursos.

- Custo: Deve equilibrar os requisitos de desempenho com os custos envolvidos, otimizando o uso de recursos em nuvem.

Uma arquitetura em nuvem bem projetada também deve levar em consideração os serviços em nuvem específicos que serão utilizados, como AWS, Azure ou Google Cloud, e escolher os componentes apropriados de acordo com as necessidades do projeto. O processo de design de arquitetura deve ser iterativo e adaptativo, acompanhando as mudanças nas demandas de negócios e na tecnologia em nuvem.

Implementação de Infraestrutura como Código (IaC):

A implementação de infraestrutura como código (IaC) é uma prática fundamental na computação em nuvem, que envolve a criação e a gestão de recursos em nuvem por meio de código, em vez de configuração manual. Isso proporciona várias vantagens:

- Automatização: IaC permite automatizar a criação, configuração e implantação de recursos em nuvem, reduzindo erros humanos e economizando tempo.

- Reprodutibilidade: O código IaC pode ser versionado e reproduzido em diferentes ambientes, garantindo consistência e facilitando a replicação de infraestrutura.

- Escalabilidade: Facilita o dimensionamento automático de recursos em nuvem de acordo com a demanda, adaptando-se às flutuações de carga de trabalho.

- Auditoria: Toda a infraestrutura é documentada no código, permitindo um rastreamento preciso de mudanças e uma auditoria fácil.

- Colaboração: Equipes de desenvolvimento e operações podem colaborar de forma eficaz usando código IaC, reduzindo silos organizacionais.

Ferramentas populares, como Terraform, AWS CloudFormation e Azure Resource Manager, permitem que os engenheiros criem e gerenciem recursos em nuvem usando código declarativo. Isso significa que eles descrevem o estado desejado da infraestrutura e deixam a ferramenta cuidar da implementação detalhada.

Orquestração de Contêineres e Kubernetes:

A orquestração de contêineres, com foco em Kubernetes, tornou-se essencial para implementações escaláveis e flexíveis em nuvem. Kubernetes é uma plataforma de código aberto que automatiza a implantação, o dimensionamento e a operação de aplicativos em contêineres. Essa tecnologia é especialmente adequada para aplicações distribuídas e microserviços. Aqui estão alguns aspectos-chave da orquestração de contêineres com Kubernetes:

- Implantação de Contêineres: Kubernetes facilita a implantação de contêineres em clusters de máquinas virtuais ou físicas, garantindo alta disponibilidade e escalabilidade.

- Gerenciamento de Recursos: Ele permite a alocação eficiente de recursos de computação, como CPU e memória, para aplicativos em contêineres.

- Balanceamento de Carga: Kubernetes oferece balanceamento de carga integrado, distribuindo o tráfego entre instâncias de aplicativos em contêineres.

- Atualizações e Escalonamento Automático: A plataforma suporta atualizações de aplicativos sem tempo de inatividade e dimensionamento automático com base na carga de trabalho.

- Monitoramento e Automação: Kubernetes pode ser integrado com ferramentas de monitoramento e automação para simplificar a operação e o diagnóstico de problemas.

Kubernetes é altamente flexível e pode ser implantado em várias nuvens ou em infraestruturas locais. A habilidade de projetar, implantar e gerenciar clusters Kubernetes é

valiosa para profissionais de cloud que desejam criar sistemas escaláveis e resilientes.

Segurança em Cloud:

A segurança em cloud é uma preocupação crítica, uma vez que os recursos e dados estão acessíveis pela internet. Garantir a proteção adequada é uma responsabilidade fundamental na implementação de soluções em nuvem. Aqui estão algumas das áreas mais importantes da segurança em cloud:

- Gerenciamento de Identidade e Acesso: Isso inclui o controle de acesso aos recursos em nuvem, garantindo que apenas usuários e aplicativos autorizados tenham permissão para acessá-los. O uso de autenticação multifator é comum para proteger contas de usuário.

- Criptografia: A criptografia é usada para proteger dados em repouso e em trânsito. Os dados armazenados em serviços em nuvem devem ser criptografados, e as comunicações devem ser seguras por meio de protocolos criptografados.

- Proteção contra Ameaças Cibernéticas: Isso envolve a implementação de firewalls, detecção de intrusões, monitoramento de segurança e resposta a incidentes para proteger os

recursos em nuvem contra ameaças cibernéticas.

- Compliance: A conformidade com regulamentações de segurança e privacidade, como GDPR ou HIPAA, é fundamental em muitos setores. Os profissionais de segurança em cloud devem garantir que os recursos em nuvem estejam em conformidade.

- Auditoria e Monitoramento: Monitorar constantemente a segurança dos recursos em nuvem e manter registros detalhados de atividades é essencial para detectar e responder a eventos de segurança.

Profissionais de segurança em cloud devem ter conhecimento abrangente das melhores práticas de segurança em cloud e habilidades para implementar medidas de proteção eficazes. A segurança em cloud é uma preocupação constante, dada a evolução das ameaças cibernéticas.

Otimização de Recursos em Nuvem:

A otimização de recursos em nuvem é uma prática que visa maximizar o valor dos investimentos em cloud computing, minimizando os custos e melhorando a eficiência operacional. Aqui estão algumas áreas-chave relacionadas à otimização de recursos em nuvem:

- Escolha de Instâncias: Os profissionais devem ser capazes de escolher os tipos e tamanhos de instâncias de máquinas virtuais apropriados para as cargas de trabalho, equilibrando desempenho e custos.

- Dimensionamento Automático: Implementar dimensionamento automático para aumentar ou diminuir o número de recursos em nuvem com base na demanda, economizando recursos quando não estão em uso.

- Desligamento de Recursos Ociosos: Identificar e desligar recursos em nuvem que não estão sendo utilizados para evitar custos desnecessários.

- Uso de Instâncias Spot ou Reservadas: Considerar a utilização de instâncias spot (recursos não garantidos, mas mais baratos) ou instâncias reservadas (contratos de longo prazo com desconto) para economizar custos a longo prazo.

- Análise de Custos: Realizar análises regulares das faturas em nuvem para identificar oportunidades de economia e otimização.

- Políticas de Gerenciamento de Custos: Implementar políticas organizacionais para controlar e otimizar os gastos em nuvem.

Profissionais de otimização de recursos em nuvem devem equilibrar o fornecimento de recursos suficientes para atender às demandas operacionais com o objetivo de manter os

custos sob controle.

Monitoramento e Solução de Problemas em Nuvem:

Monitorar e solucionar problemas em nuvem é uma habilidade fundamental para garantir que os sistemas em nuvem funcionem de forma confiável e eficiente. Isso envolve:

- Configuração de Monitoramento: Configurar ferramentas de monitoramento para rastrear o desempenho e a disponibilidade de recursos em nuvem, bem como gerar alertas em caso de problemas.

- Análise de Logs: Examinar logs e registros de eventos para identificar problemas, erros e anomalias que possam afetar o desempenho ou a segurança.

- Diagnóstico de Problemas: Identificar e isolar problemas, determinar suas causas raízes e implementar soluções eficazes.

- Resposta a Incidentes: Desenvolver procedimentos de resposta a incidentes para lidar com eventos de segurança, falhas de sistema ou outros problemas inesperados.

- Melhorias Contínuas: Usar dados de monitoramento para identificar oportunidades de otimização e implementar melhorias contínuas no desempenho e na eficiência dos sistemas em nuvem.

Profissionais de monitoramento e solução de problemas em nuvem devem ser hábeis em usar ferramentas de monitoramento, análise de dados e colaboração entre equipes de desenvolvimento e operações para garantir que os sistemas em nuvem atendam aos padrões de desempenho e disponibilidade esperados.

RESUMO

A arquitetura e implementação em nuvem revolucionaram a maneira como as empresas gerenciam seus recursos de TI, permitindo uma flexibilidade e escalabilidade sem precedentes. Nesse contexto, habilidades essenciais surgiram para profissionais de TI. O Design de Arquitetura em Nuvem é fundamental, envolvendo a criação de infraestruturas altamente disponíveis e eficientes na nuvem, levando em consideração fatores como balanceamento de carga, redundância e tolerância a falhas.

A Implementação de Infraestrutura como Código (IaC) tornou-se uma pedra angular, permitindo a automatização da criação e gestão de recursos na nuvem. Isso significa que as configurações podem ser codificadas e versionadas, garantindo consistência e facilitando a implantação repetível de infraestruturas complexas.

A Orquestração de Contêineres e Kubernetes é outra habilidade crucial, uma vez que as aplicações modernas frequentemente são empacotadas em contêineres para facilitar a implantação e o gerenciamento. O Kubernetes é a plataforma mais popular para gerenciar esses contêineres, permitindo a escalabilidade dinâmica e a orquestração eficiente de recursos.

A segurança em nuvem é uma preocupação constante. Profissionais de arquitetura e implementação em nuvem devem entender como proteger dados e recursos na nuvem, implementando políticas de acesso, monitorando ameaças e mantendo a conformidade com regulamentos de segurança.

A otimização de recursos em nuvem é uma habilidade econômica, garantindo que os recursos sejam usados de maneira eficiente para evitar desperdícios e reduzir custos. Isso envolve o dimensionamento automático de recursos, o uso de instâncias reservadas e a identificação de recursos subutilizados.

Por fim, o monitoramento e a solução de problemas em nuvem são essenciais para manter as operações funcionando sem problemas. Isso inclui a coleta de métricas e logs para identificar problemas potenciais, a implementação de alertas proativos e a resolução rápida de incidentes para minimizar o tempo de inatividade.

Em resumo, a arquitetura e implementação em nuvem requerem um conjunto diversificado de habilidades que abrangem desde o design de arquitetura até a solução de problemas em tempo real, tudo isso com foco na eficiência, segurança e escalabilidade. Profissionais com expertise nessas áreas são essenciais para o sucesso das operações em nuvem das empresas modernas.

ATIVIDADE DE FIXAÇÃO

1. O que é arquitetura em nuvem e por que é importante para projetos de computação em nuvem?

2. Quais são os principais fatores a serem considerados ao projetar a arquitetura em nuvem para um sistema de alta disponibilidade?

3. Como a escalabilidade é alcançada em ambientes de nuvem e por que é fundamental para sistemas modernos?

4. Quais são os benefícios da implementação de Infraestrutura como Código (IaC) na gestão de recursos em nuvem?

5. Como o Kubernetes ajuda na orquestração de contêineres e qual é o seu papel na arquitetura em nuvem?

6. Quais são as principais preocupações de segurança em cloud computing e como podem ser abordadas em uma arquitetura em nuvem?

7. Quais são os métodos comuns para otimizar custos em ambientes de nuvem e como você equilibra custos e desempenho?

8. Qual é a importância da auditoria e do monitoramento na arquitetura em nuvem e como essas práticas contribuem para a operação eficiente?

9. Como o conceito de "elasticidade" se aplica à arquitetura em nuvem e qual é a sua relevância para sistemas dinâmicos?

10. Quais são os desafios comuns enfrentados ao migrar sistemas legados para a nuvem e como uma arquitetura apropriada pode ajudar a superá-los?

REFERÊNCIAS

CARVALHO, Paulo Sérgio Licciardi Messeder de; CASALECHI, Alberto Sampaio Lima. Redes de Computadores: Uma Abordagem Prática. 2012. Novatec.

COLCHER, Sérgio; CARDOSO, Fábio Mendonça; ARAÚJO, Virgílio Almeida. Introdução à Internet: Conceitos, Tecnologias e Serviços. 2015. Elsevier.

COMER, Douglas E. Interligação em Redes com TCP/IP - Volume 1: Princípios, Protocolos e Arquitetura. 2007. Bookman.

FOROUZAN, Behrouz A. Comunicação de Dados e Redes de Computadores. 2013. Bookman.

KUROSE, James F.; ROSS, Keith W. Redes de Computadores e a Internet: Uma Abordagem Top-Down. 2021. Pearson.

MENDES, Patricia; RAMOS, Marco. Guia de Sobrevivência em Redes TCP/IP: Fundamentos, Protocolos, Diagnóstico e Administração. 2009. Novatec.

MORIMOTO, Carlos E. Redes: Guia Prático. 2009. Sulina.

PUJOLLE, Guy. Redes de Computadores: Dos Princípios às Aplicações. 2007. LTC.

TAFT, Andrew S.; MATTOSO, Marta; BOAVENTURA, Maurício, et al. Internet das Coisas: Fundamentos e Aplicações. 2016. Novatec.

TANENBAUM, Andrew S.; WETHERALL, David J. Redes de Computadores. 2016. Pearson.


Proz
Viva sua profissão!