

Fundamentos de redes de computadores

Cassiano Peres

DIO Tech Education Analyst



Objetivo Geral

Neste curso vamos falar sobre redes de computadores, um tema fundamental no assunto de cibersegurança.

Pré-requisitos

Conhecimento prévio no assunto torna a assimilação do conteúdo mais rapidamente, mas caso não há, não é excludente.

Percurso

Etapa 1

Conceitos de redes de computadores

Etapa 2

Componentes de redes de computadores

Etapa 3

Protocolos de redes de computadores

Percorso

Etapa 4 Endereços de IP

Etapa 5 Privacidade com Proxy e VPN

Etapa 1

Conceitos de redes de computadores

Introdução

Nesta aula vamos falar sobre redes de computadores, seus conceitos, protocolos e como funcionam.

Redes de computadores

Redes de computadores referem-se a dispositivos de computação **interconectados** que podem **trocar** dados e **compartilhar** recursos entre si.



Redes de computadores

Esses dispositivos em rede usam um sistema de regras, os **protocolos** de comunicação, para transmitir informações por meio de tecnologias físicas ou sem fio.



Composição da rede

- **Nós:** equipamento conectado à rede (computador, hub, switch, terminal, etc);
- **Links:** meio de transmissão que conecta dois nós, podendo ser físico ou sem fio.
- **Arquitetura:** define as especificações para os componentes físicos da rede, organização funcional, protocolos e procedimentos.

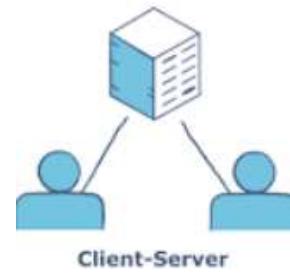
Tipos de arquiteturas de redes

O design de uma rede de computadores é enquadrado em duas grandes categorias:

- Cliente servidor;
- Ponto a ponto (P2P).

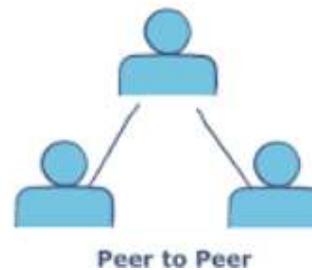
Arquitetura cliente servidor

Nessa arquitetura os nós podem ser **servidores** ou **clientes**. Os servidores fornecem recursos como memória, capacidade de processamento ou dados aos nós clientes.



Arquitetura ponto a ponto

Nesta arquitetura os computadores conectados têm capacidades e privilégios iguais, sem um servidor central para coordenação. Cada dispositivo na rede de computadores pode atuar como cliente ou servidor.



Topologias de redes

A disposição de nós e links é chamada de topologia de rede, podendo ser configurados de maneiras diferentes para obter resultados distintos.

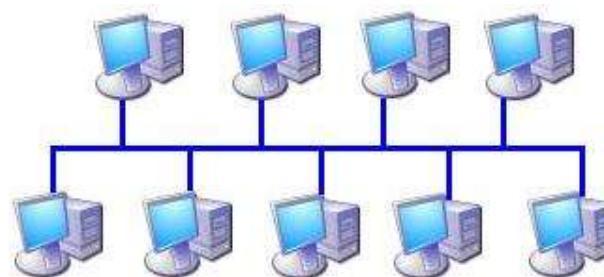
Topologias de redes

A disposição de nós e links é chamada de topologia de rede, sendo configurados de formas diferentes para obter resultados distintos.

- Barramento
- Anel
- Estrela
- Malha

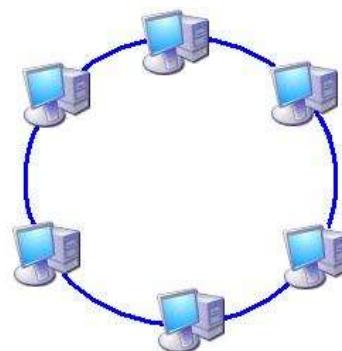
Topologia em barramento

Cada nó está vinculado a apenas um outro nó. A transmissão de dados pelas conexões de rede ocorre em uma direção.



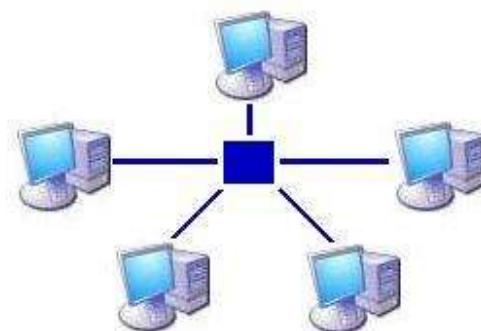
Topologia em anel

Cada nó está vinculado a dois outros nós, formando um anel. Os dados podem fluir bidirecionalmente. No entanto, a falha de um único nó pode desativar toda a rede.



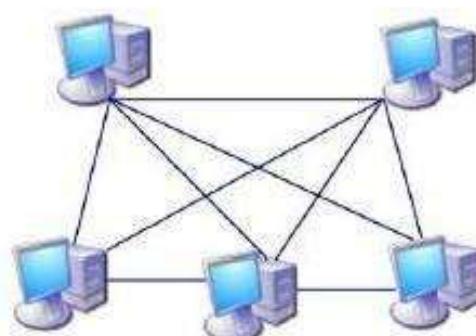
Topologia em estrela

Um nó de servidor central está vinculado a vários dispositivos de rede do cliente. Essa topologia tem melhor performance, pois os dados não precisam passar por cada nó.



Topologia em malha

Cada nó está conectado a muitos outros nós. Em uma topologia em malha completa, cada nó está conectado a todos os outros nós da rede.



Tipos de redes

- **LAN (Local Area Network)**: conecta dispositivos próximos, em um mesmo ambiente;
- **MAN (Metropolitan Area Network)**: para conectar as redes locais dentro de distâncias maiores;
- **WAN (Wide Area Network)**: rede de longa distância, conecta dispositivos dentro de países ou continentes;

Tipos de redes

- **SAN (Storage Area Network)**: armazenar dados da rede e fazer a comunicação entre um servidor e os demais dispositivos;
- **VLAN (Virtual LAN)**: reúne diversas máquinas de forma lógica e não física

Termos e conceitos

Endereço IP: número exclusivo atribuído a cada dispositivo conectado à rede;

Nós: equipamento que envia e/ou recebe dados em uma rede;

Portas: identifica uma conexão específica (protocolos);

Conclusão

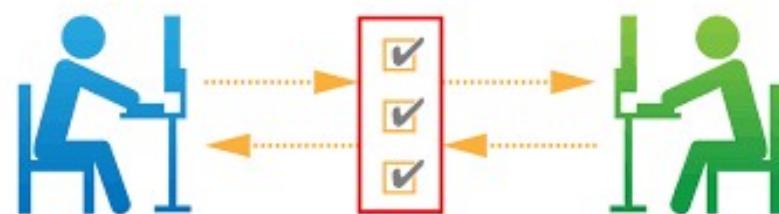
A compreensão dos fundamentos de redes de computadores é essencial dentro do contexto da segurança cibernética.

Etapa 2

Protocolos de redes de computadores

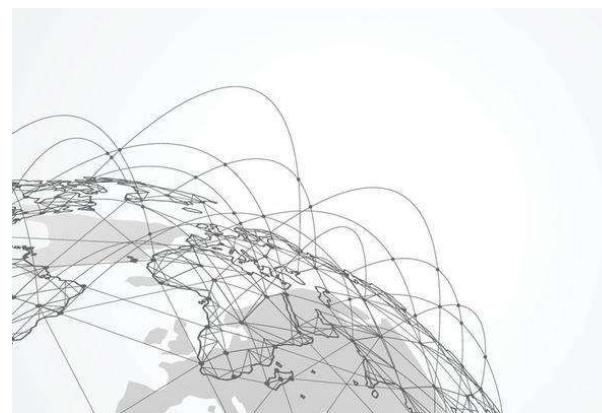
Introdução

Protocolos de rede são um conjunto de normas que permitem que máquinas conectadas em redes possam se comunicar entre si.



Protocolos de redes

Funcionam como uma linguagem universal para que dispositivos distribuídos ao redor do mundo possam se comunicar de forma padronizada.



Modelos de camadas

Os modelos de camadas definem regras e orientações para que haja a intercomunicação entre os dispositivos de redes, independente dos modelos ou fabricantes.

Modelos de camadas

Os modelos de camadas definem regras e orientações para que haja a intercomunicação entre os dispositivos de redes, independente dos modelos ou fabricantes.

Modelos de camadas

Na transmissão, cada camada realiza seu trabalho e o entrega para a camada inferior.

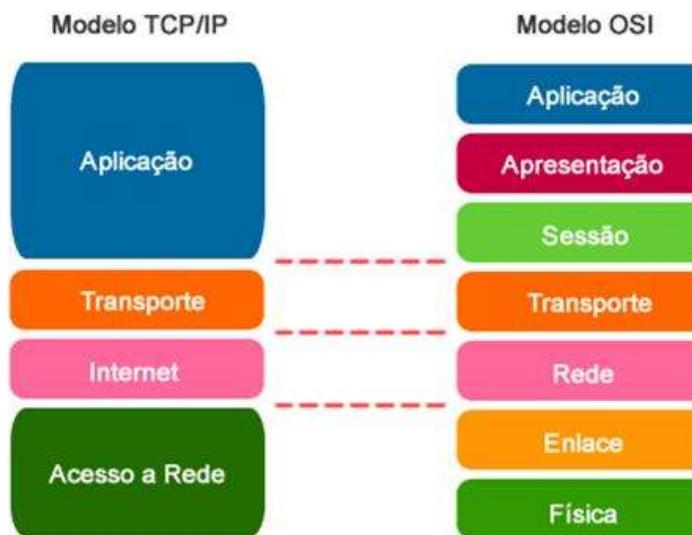
Modelos de camadas

O agrupamento em camadas facilita a análise do processo de comunicação por:

- Delimitar as funções das regras de comunicação (protocolos), dos serviços e das interfaces;
- Servir como referência de comparação entre protocolos ou serviços de pilhas diferentes.

Modelo de camadas

Existem dois modelos de camadas utilizados atualmente, os modelos OSI e TCP/IP.



Modelo OSI

Divide divide as funções em 7 camadas:

- Aplicação
- Apresentação
- Sessão
- Transporte
- Rede
- Enlace
- Física



Modelo OSI

- Decomposição dos componentes da rede em partes que são menores
- Padronização dos componentes presentes na rede
- Comunicação entre diversos tipos de hardware e software
- Evita que alterações em uma camada afetem as configurações de outra

Modelo TCP/IP

o modelo TCP/IP possui quatro camadas:

- Aplicação;
- Transporte;
- Internet;
- Acesso a rede.

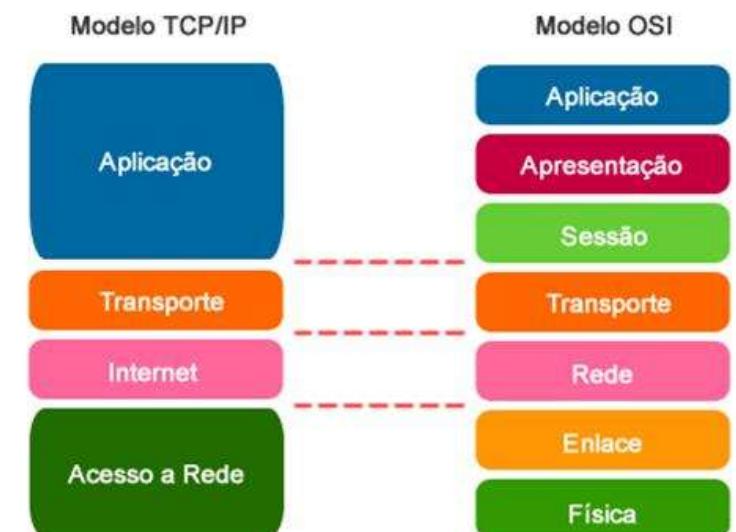


Modelo TCP/IP

No início, o modelo OSI foi o primeiro a ser utilizado, sendo base para nomenclaturas e para as redes, atualmente o modelo TCP/IP tem sido mais utilizado em todo o mundo tanto nas redes que são internas como também nas externas.

OSI vs TCP/IP

- OSI: 7 camadas - TCP/IP: 4 camadas;
- O TCP/IP mesclou as camadas 1 e 2 do OSI para a camada Aplicação.
- Há uma camada chamada de **Internet** em TCP/IP enquanto que a mesma é chamada de **Redes** no OSI.



Principais protocolos de redes

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

Principais protocolos de redes

- **Camada de Aplicação:** WWW, HTTP, SMTP, Telnet, FTP, SSH, NNTP, RDP, IRC, SNMP, POP3, IMAP, SIP, DNS, PING;
- **Camada de Transporte:** TCP, UDP, RTP, DCCP, SCTP;
- **Camada de Internet:** IPv4, IPv6, IPsec, ICMP;
- **Camada de acesso à rede:** Ethernet, Modem, PPP, FDDI.

Portas e protocolos

Ao realizar a comunicação entre dispositivos, por meio de protocolos, são utilizadas **portas** numeradas.

Portas e protocolos

Application	Protocol	Port Number
File Transfer Protocol FTP Client	TCP	20
File Transfer Protocol FTP Server	TCP	21
Secure Shell SSH	TCP	22
Telnet	TCP	23
Simple Mail Transport Protocol SMTP	TCP	25
Domain Name System DNS	UDP / TCP	53
Dynamic Host Configuration Protocol DHCP	UDP	67,68
Trivial File Transfer Protocol TFTP	UDP	69
Hypertext Transfer Protocol HTTP	TCP	80
Post Office Protocol 3 POP3	TCP	110
Simple Network Management Protocol SNMP	UDP	161
Hypertext Transfer Protocol Secure HTTPS	TCP	443

Conclusão

Nesta aula vimos fundamentos de redes de computadores que serão muito úteis e relembrados ao longo do curso.

Etapa 3

Endereços de IP

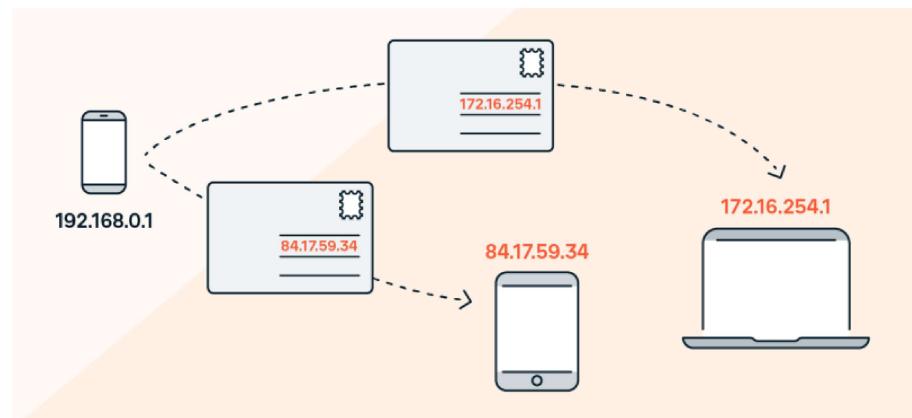
Introdução

Nesta aula vamos falar sobre IP, o identificador único de cada dispositivo conectado à rede.



Endereços de IP

Endereço IP é um endereço exclusivo que identifica um dispositivo na Internet ou em uma rede local.



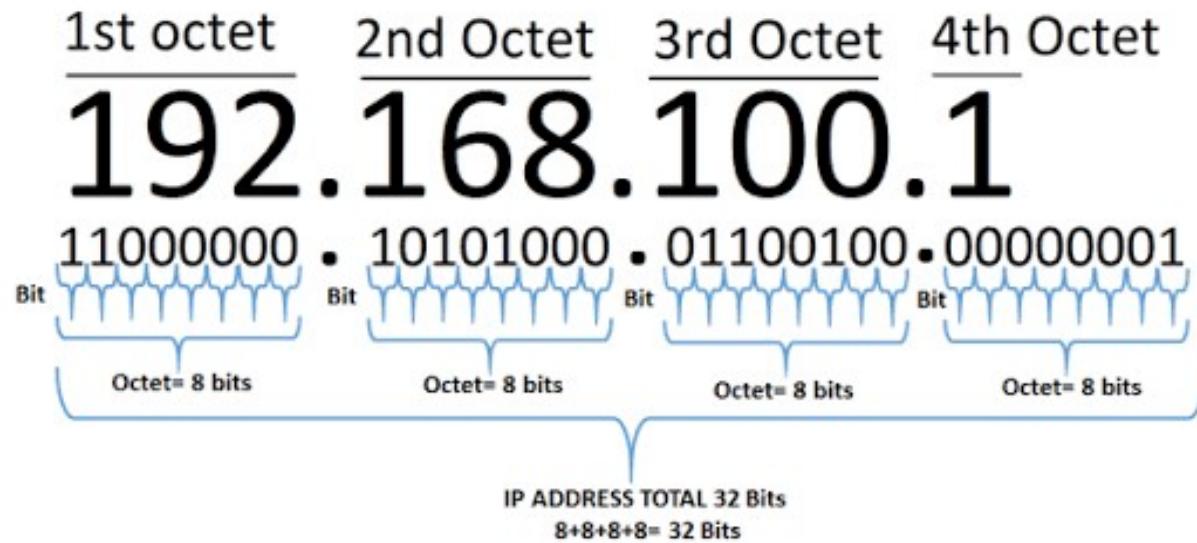
Endereços de IP

IP vem do inglês "*Internet Protocol*" que consiste em um conjunto de regras que regem o formato de dados enviados pela Internet ou por uma rede local.

O que é IP?

Um endereço IP é uma sequência de números separados por pontos, representado por um conjunto de quatro números conhecidos como **octetos**, como por exemplo **192.158.1.38**.

O que é IP?



Máscara de rede

A máscara de rede tem 32 bits, assim como o endereço IP, tendo como finalidade mascarar uma parte do endereço IP, assim, todo endereço IP tem uma máscara correspondente, servindo para identificar qual parte do endereço é da **rede** e qual é a do **host**.

Máscara de rede

HOSTS	REDES	CIDR	MÁSCARA DE SUB-REDE
1	256	/32	255.255.255.255
2	128	/31	255.255.255.254
4	64	/30	255.255.255.252
8	32	/29	255.255.255.248
16	16	/28	255.255.255.240
32	8	/27	255.255.255.224
64	4	/26	255.255.255.192
128	2	/25	255.255.255.128
256	1	/24	255.255.255.0

Classes de IP

As principais são a **classe A**, **classe B** e **classe C**.

Com base nos primeiros bits (**prefixo**) de um endereço IP, podemos determinar a qual a classe pertence um endereço IP.

Máscara de rede

- Classe de endereçamento A: 255.0.0.0
- Classe de endereçamento B: 255.255.0.0;
- Classe de endereçamento C: 255.255.255.0.

Classes de IP

Originalmente, o espaço de endereçamento IP foi dividido estruturas de tamanho fixo designadas de "**classes de endereço**".

Classes de IP

Classe	Primeiro octeto	Parte da rede (N) e parte para hosts (H)	Máscara	Nº Redes / hosts por rede
A	1-127	N.H.H.H	255.0.0.0	126 redes 16,777,214 hosts por rede ($2^{24}-2$)
B	128-191	N.N.H.H	255.255.0.0	16,384 redes (2^{14}) 65,534 hosts por rede ($2^{16}-2$)
C	192-223	N.N.N.H	255.255.255.0	2,097,150 redes (2^{21}) 254 hosts por rede (2^8-2)
D	224-239	Multicast	NA	NA
E	240-255	experimental	NA	NA

Classes de IP

IPv4 Address Format (Dotted Decimal Notation)



IPV4 e IPV6

IPv4	IPv6
Deployed 1981	Deployed 1998
32-bit IP address	128-bit IP address
4.3 billion addresses Addresses must be reused and masked	7.9x10²⁸ addresses Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18	Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration	Supports autoconfiguration

Ataques contra IP's

- Engenharia social
- Ciberstalking
- Download de conteúdo ilegal usando seu endereço IP
- Rastrear sua localização
- Ataque direto à sua rede
- Ataques em seu dispositivo

Conclusão

Nesta aula exploramos os endereços de IP, nas aulas seguintes será um conceito muito utilizado para conexão com computadores alvos nos testes.

Etapa 4

Privacidade com Proxy e VPN

// Título do Tema/Apresentação

Introdução

A privacidade na internet é algo que as pessoas estão cada vez mais levando a sério, buscando vários recursos para isso.

Introdução

Hoje em dia, muitos internautas compararam um proxy com uma VPN, perguntando-se o que deveriam usar ao navegar para se protegerem.



Introdução

As Redes Privadas Virtuais (VPNs) e os proxies são uma solução potencial porque adicionam uma camada extra entre um navegador e qualquer empresa de rastreamento de dados ou governo.

VPN

Uma VPN é uma rede privada que codifica os dados enviados para ou recebidos da Internet, permitindo acessar websites de forma segura e privada e usar programas e aplicativos, independentemente da rede utilizada.

VPN

How a VPN works



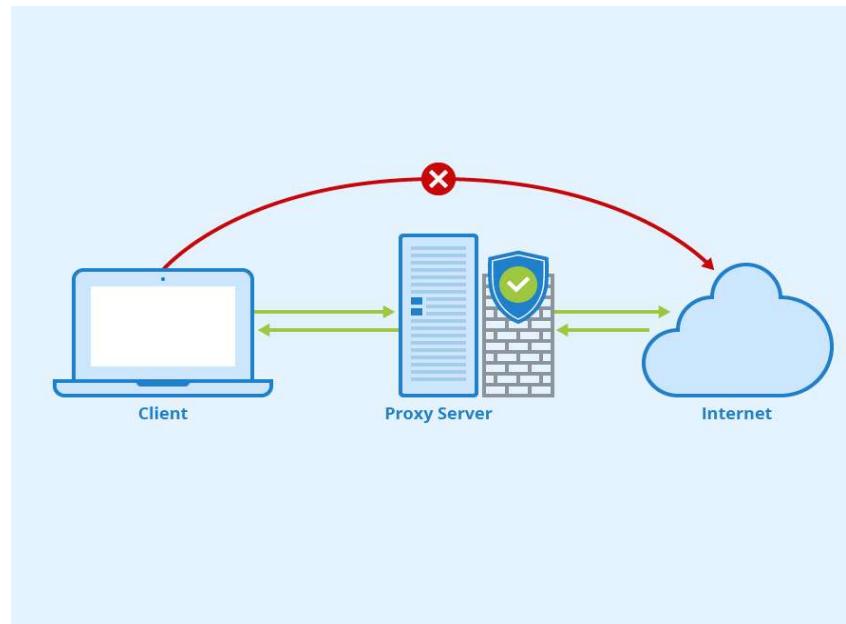
Vantagens da VPN

- Como a VPN criptografa a conexão, os hackers potenciais não podem “escutar” a transmissão para roubar dados vulneráveis;
- Também evita que um provedor ou empregador espie o tráfego, rastreando o tráfego do roteador.

Proxy

Um servidor proxy é normalmente um servidor público remoto acessado através de um aplicativo web ou programa desktop que acessa páginas web “em seu nome”.

Proxy



Proxy

- Na maioria das vezes a palavra *servidor proxy*, se refere a *servidor proxy HTTP*.
- Estes servidores proxy são servidores web que acessam uma página web pela Internet e depois encaminham os dados para o navegador.

Prática

Vamos configurar servidores de Proxy e VPN para navegarmos na internet.

Dúvidas?

- > Fórum/Artigos
- > Comunidade Online (Discord)

