SÃO
PAULO
TECH
SCHOOL

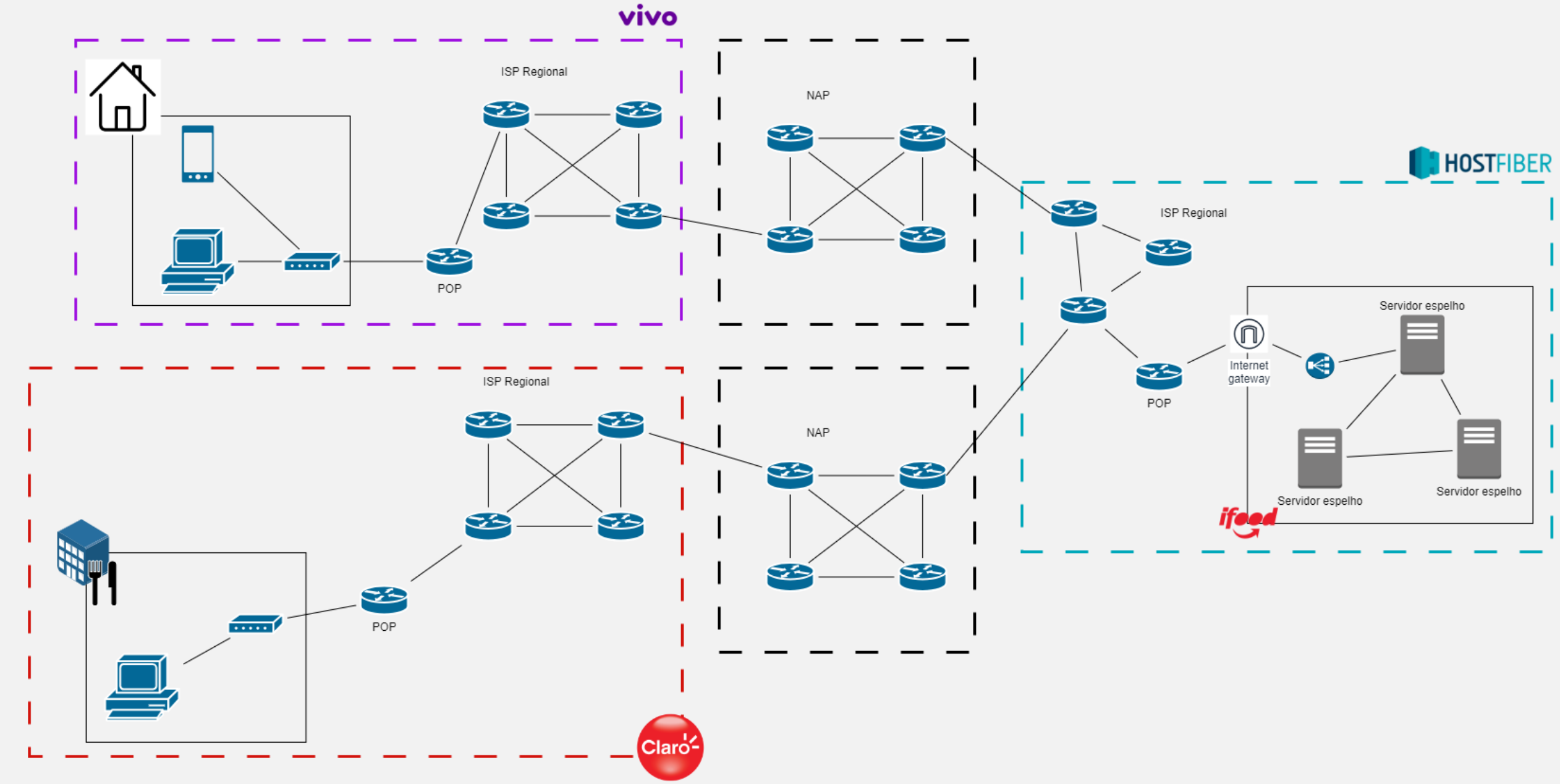
Computação e sistemas distribuídos em nuvem

IPV4 e IPV6

Diego Brito

diego.brito@sptech.school

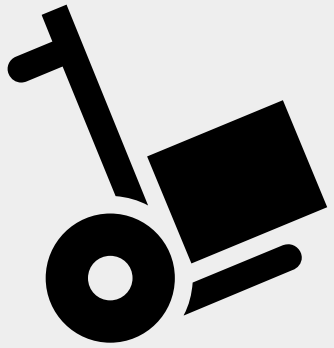
Revisão atividade iFood


vivo
ISP Regional
POP
NAP
HOSTFIBER
ISP Regional
POP
Internet gateway
Servidor espelho
Servidor espelho
Servidor espelho
ifood
ISP Regional
POP
NAP
Claro

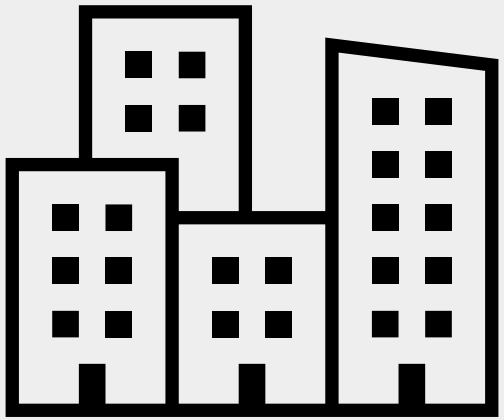
Endereçamento

Como é entregue um pacote?

01414-905



Correios

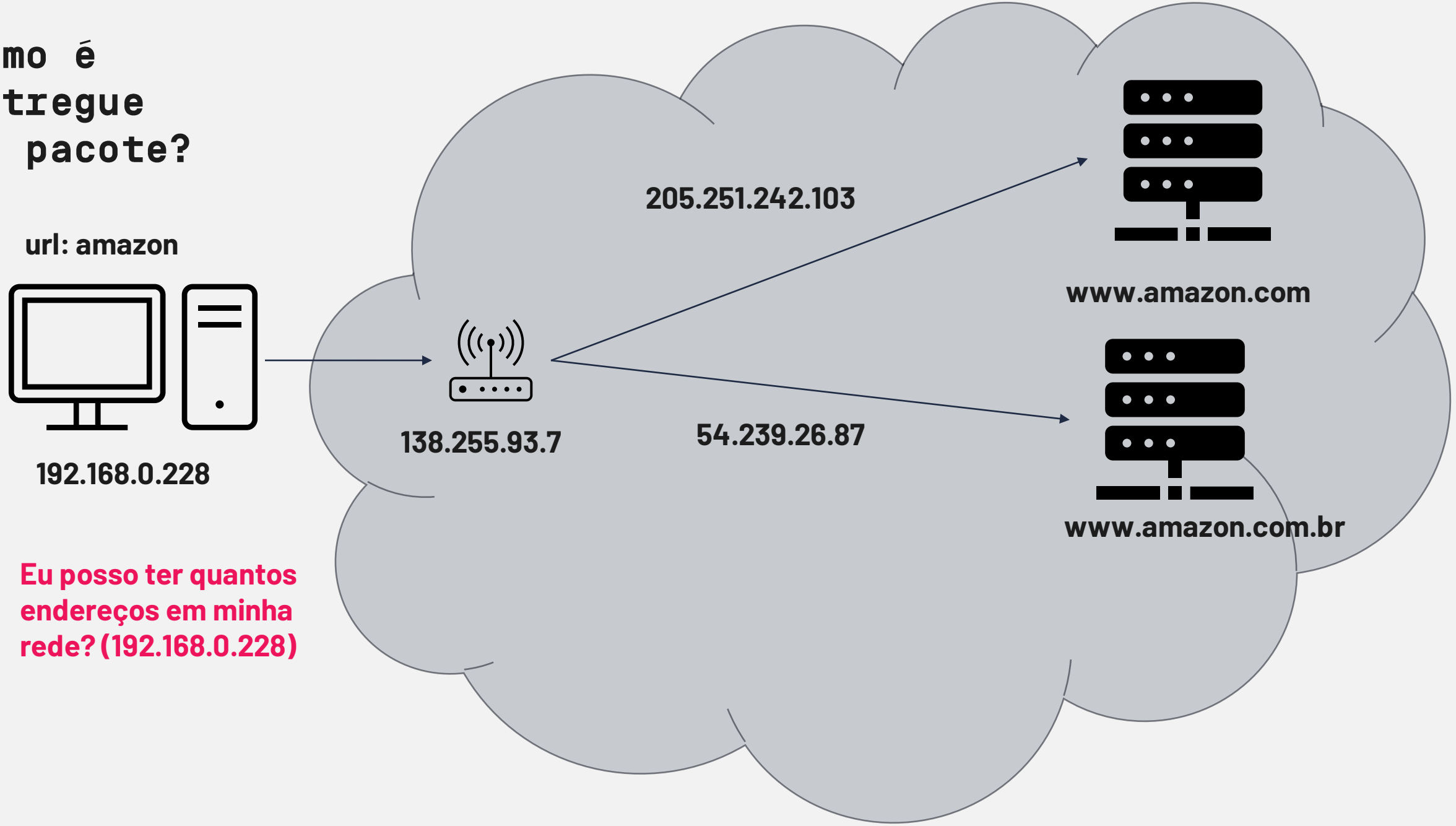


SÃO PAULO TECH SCHOOL

11º andar
sala professores

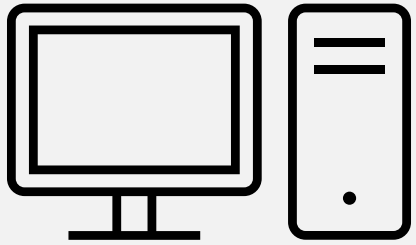
Quantos 11º andar existem nos prédios?
Quantas apartamentos 122 existem por ai?
Pode ter dois apartamentos 122 no mesmo prédio?

Como é entregue um pacote?



Eu posso ter quantos endereços em minha rede? (192.168.0.228)

Regras da rede IPv4



192.168.0.228

192.168.0.228

4 octetos (4 blocos de 8 bits)

00000000.00000000.00000000.00000000

...

11111111.11111111.11111111.11111111

O que representa uma faixa de Ips entre

000.000.000.000 255.255.255.255

Totalizando 4.294.967.295 endereços IPs

101

122

Esses apartamentos estão no mesmo andar?

NÃO

101

122

00 a 99 andares

0 a 9 apartamentos

SIM

101

122

0 a 9 andares

00 a 99 apartamentos

Máscara de rede

Uma máscara de sub rede, conhecida como subnet mask ou netmask, é um número de 32 bits usado em um IP para separar a parte correspondente à rede pública, à sub rede e aos hosts.

As máscaras de sub rede decimais são convertidas em números binários que são todos uns à esquerda e todos zeros à direita.

Classe	Bits iniciais	Início	Fim	Máscara de sub-rede padrão	Notação CIDR
A	0	1.0.0.1	126.255.255.254	255.0.0.0	/8
B	10	128.0.0.1	191.255.255.254	255.255.0.0	/16
C	110	192.0.0.1	223.255.255.254	255.255.255.0	/24

Cálculo de hosts

IPv4:

192.168.0.228

Máscara de sub-rede:

255.255.255.0

255 = 8 bits

255.255.255.0 = 24 bits

Ou seja, 24 bits definem a rede, e 8 bits definem os hosts, dando um range de IP de **192.168.0.0** até **192.168.0.255**

Dando um total de 254 hosts

```
C:\>ipconfig
```

```
Adaptador de Rede sem Fio Wi-Fi:

   Sufixo DNS específico de conexão. . . . . :
   Endereço IPv6 de link local . . . . . : fe80::f3d0:c427:5825:5bf4%16
   Endereço IPv4. . . . . . . . . . . . . . : 192.168.0.228
   Máscara de Sub-rede . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . : 192.168.0.1
```

Os IPs **192.168.0.0** e **192.168.0.255** são reservados.

O **192.168.0.0** especifica a rede, enquanto que o **192.168.0.255** é o IP de ***broadcast***, endereço especial que cada computador em uma rede "escuta" em adição a seu próprio endereço. Este é um endereço onde os datagramas enviados são recebidos por todos os computadores da rede.

Chegando nos **254 hosts** nesta rede

IP Calculator / IP Subnetting (jodies.de)

Máscara /24:

255 . 255 . 255 . 0

Definição de rede: 192.168.0.0

Início: 192.168.0.1

Término: 192.168.0.254

Broadcast: 192.168.0.255

11111111. 11111111 . 11111111 . 00000000

24 bits para definir rede

8 bits para definição de hosts

2^24 = 16.777.216

2^8 = 256

Cálculo de host [atividade]

1. Utilizando o mesmo IP do slide anterior, calcule quantas sub rede e hosts teriam se a máscara fosse /23?
2. Utilizando o comando ipconfig(Windows)ou ifconfig(Linux) calcule a quantidade de hosts suportados na sua conexão atual.

Máscara /23 ?

255 . 255 . 254 . 0

Definição de rede: 192.168.0.0

Início: 192.168.0.1

Término: 192.168.0.254 ?

Broadcast: 192.168.0.255 ?

1111111. 1111111 . 1111111**0** . **00000000**

23 bits para definir rede

9 bits para definição de hosts

2^23 = 8.388.608

2^9 = 512

Calculadora de Sub redes

Primeira Sub-rede:

- **Endereço de Rede: 192.168.0.0/24**
- **Intervalo de IPs: 192.168.0.1** até **192.168.0.254**
- **Endereço de Broadcast: 192.168.0.255**

Segunda Sub-rede:

- **Endereço de Rede: 192.168.1.0/24**
- **Intervalo de IPs: 192.168.1.1** até **192.168.1.254**
- **Endereço de Broadcast: 192.168.1.255**

Sub redes

Segmentação de rede:

Notações CIDR e Máscara de Rede

CIDR (ClassLess Inter-Domain Routing)

Ex.: 192.168.1.0/24

Máscara de Rede:
Assemelhasse a um endereço IP, ou seja, é

dividida em 4 octetos que vai de 0 -255;

EX.: 255.255.255.0

Através de conjunto de Bits identificar qual porção representa a Rede e qual representa o Host;

Determina quantos Hosts poderemos ter em uma determinada rede

I. Facilitar gerenciamento
II. Melhorar performance
III. Controlar de tráfego
IV. Apoiar na segurança
V. Segmentar rede

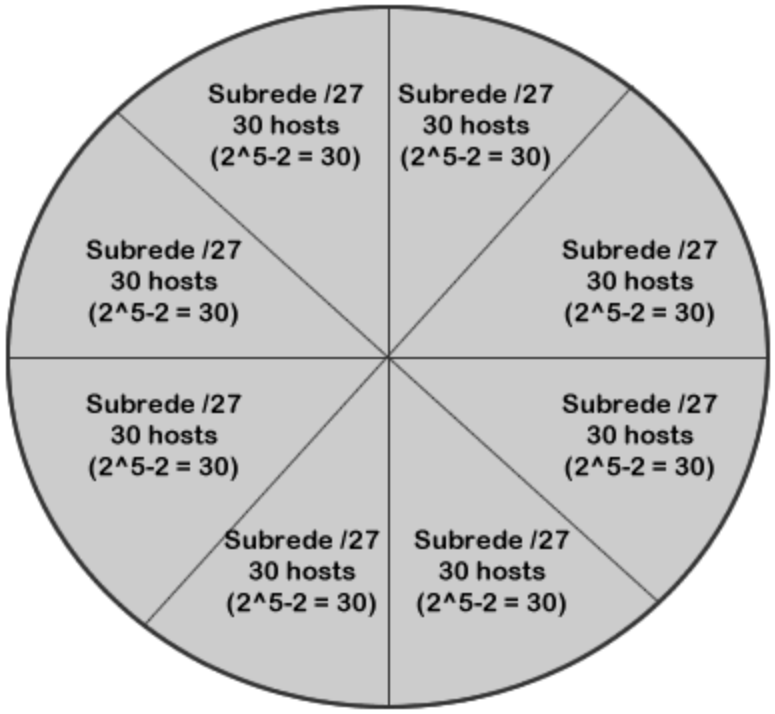
Segmentação de rede: VSLM

VLSM (Variable Length Subnet Masking) é uma técnica de subdivisão de redes em sub redes de tamanhos variáveis.

I. Permite otimizar o uso de endereços IP, minimizando o desperdício.

II. Tem como benefício melhor aproveitamento de endereços IP, evitando o esgotamento, flexibilizando a criação de sub redes de diferentes tamanhos e reduzindo do tráfego de broadcast ao dividir a rede em segmentos menores

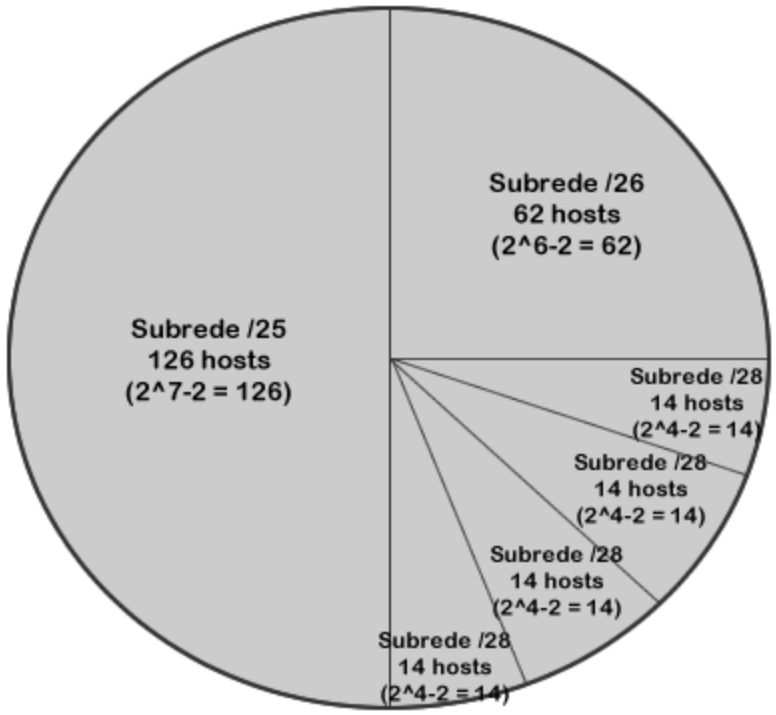
Segmentação de redes: VSLM



Rede Classe C /24 (254 hosts)

Com a utilização de sub-redes nós dividimos uma rede (classe A, B ou C) em várias sub-redes, cada uma delas com um tamanho fixo. Por exemplo, podemos dividir uma rede classe C em 08 sub-redes com a máscara /27.

Segmentação de redes: VSLM



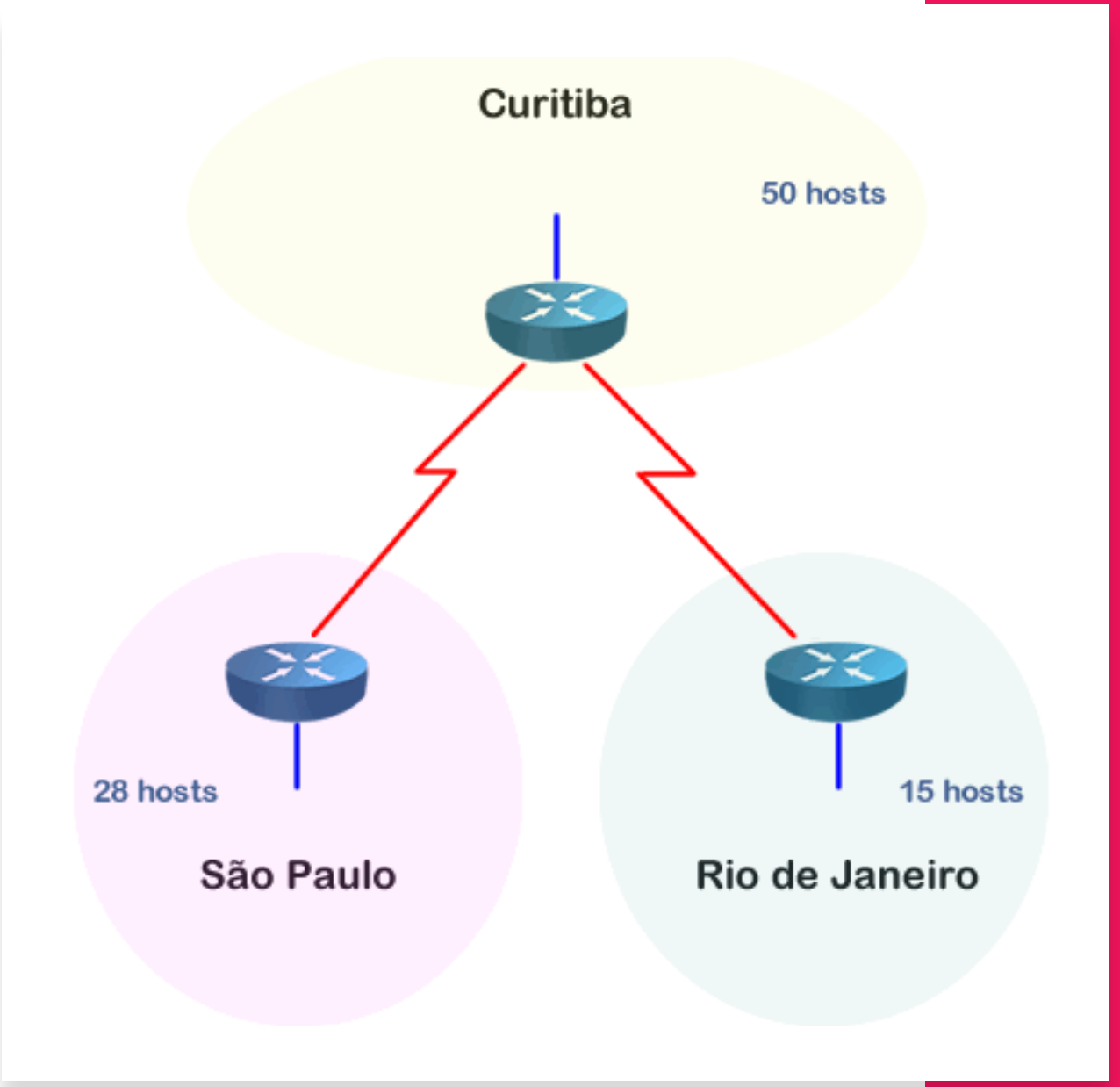
Rede Classe C /24 (254 hosts)
dividida com o uso do VLSM

Agora com o conceito de VLSM basicamente o que fazemos é dividir as sub redes em outras sub redes, cada uma com o tamanho necessário para satisfazer os requisitos de projeto. Simplificadamente podemos dizer que fazemos sub redes das sub redes

Exemplo prático: VSLM

- Suponha que você trabalhe como administrador de rede em uma empresa que tenha recebido o bloco de endereço IP 195.125.5.0/24 para endereçar três escritórios, conforme abaixo.

  - 1 escritório com 50 hosts em Curitiba
  - 1 escritório com 28 hosts em São Paulo
  - 1 escritório com 15 hosts no Rio de Janeiro



Exemplo prático: VSLM – Resolução

195.125.5.0/24 – máscara de rede 255.255.255.0
11111111.11111111.11111111.00000000 = /24
2^8 = 256 IPs

11111111.11111111.11111111.10000000 = /25
2^7 = 128 IPs

11111111.11111111.11111111.11000000 = /26
2^6 = 64 IPs

11111111.11111111.11111111.11100000 = /27
2^5 = 32 IPs

11111111.11111111.11111111.11110000 = /28
2^4 = 16 IPs

Curitiba = 50 IPs **/26 (255.255.255.192)**
195.125.5.0 – 192.125.5.63 (Host úteis .1 até .62)

São Paulo = 28 IPs **/27 (255.255.255.224)**
195.125.5.64 – 195.125.5.95 (Host úteis .65 até .94)

Rio de Janeiro = 15 IPs **/27 (255.255.255.224)**
195.125.5.96 – 195.125.5.127 (Host úteis .97 até .126)

Exemplo prático: VSLM - Resolução

Em uma rede de computadores, um endereço de enlace local é um endereço de rede que é válido apenas para comunicações dentro do segmento de rede (enlace) ou do domínio de broadcast que o hospedeiro está conectado.

Endereços de enlace local não são garantidos de serem únicos além de um único segmento de rede. Roteadores entretanto não enviam pacotes com endereços de enlace local.

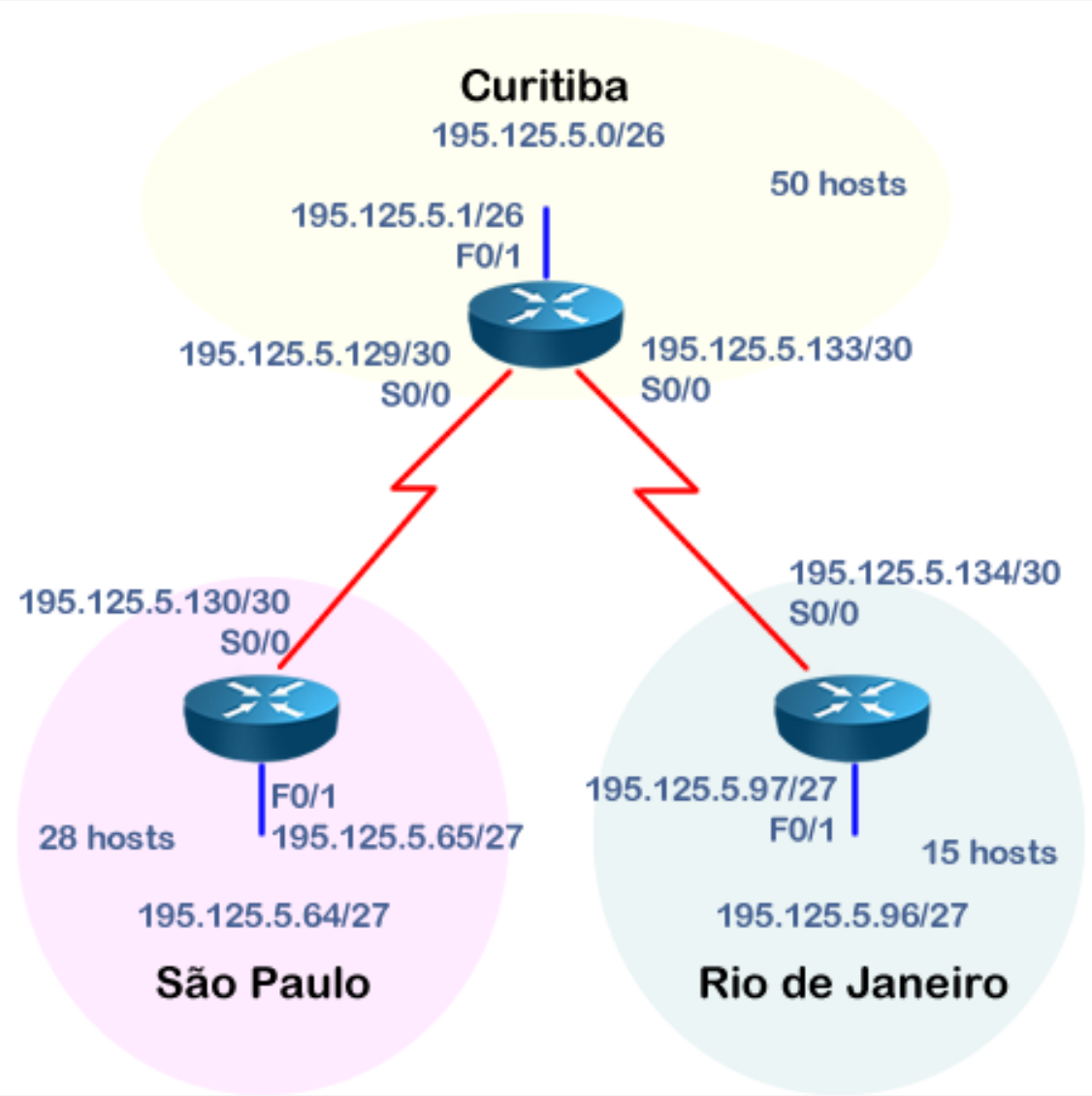
Primeiramente vamos calcular os endereços do enlace entre Curitiba-São Paulo. Precisamos apenas de 2 endereços de hosts (um para cada interface serial de cada roteador). **Logo, 2 bits para hosts é o suficiente e ficamos uma máscara /30**

Enlace Curitiba - São Paulo = 2 IPs **/30 (255.255.255.252)**
195.125.5.128 – 195.125.5.131 (Hosts úteis .129 até .130)

Enlace Curitiba – Rio de Janeiro = 2IPs **/30 (255.255.255.252)**
195.125.5.132 – 195.125.5.135 (Hosts úteis .133 até .134)

Exemplo prático: VSLM Resolução

Nesse ponto já temos todo o nosso esquema de endereçamento calculado. Perceba que a partir de um bloco contínuo de endereços classe C padrão (195.125.5.0) conseguimos fazer a divisão em blocos de endereços variáveis, otimizando a utilização dos endereços IP. Isso graças ao conceito de VLSM.



Atividade plano de endereçamento

Você está planejando expandir seu escritório e precisará acomodar novos funcionários em diversos departamentos.

Com um endereço IP base de **192.168.0.0/24** disponível, você deseja criar sub-redes otimizadas para o seguinte número de funcionários: **20** desenvolvedores, **4** de RH, **2** do financeiro, **10** de vendas e atendimento, e **5** do administrativo.

Quais mascaras de sub rede ou CIDR você usaria e porquê ?

Atividade plano de endereçamento

Além disso, você precisará definir os **intervalos de endereços para cada sub-rede** criada para assegurar que haja endereços IP suficientes para os hosts em cada departamento, sem sobrepor sub-redes e minimizando o desperdício de endereços IP.

Faixas de endereços IP recomendados para redes privadas

I. 10.0.0.0 a 10.255.255.255
II. 172.16.0.0 a 172.31.255.255
III. 192.168.0.0 a 192.168.255.255

IP Fixo vs DHCP

IP FIXO: IP Configurado diretamente no HOST (Equipamento de Rede)

I. Dificuldade no gerenciamento
II. Conflitos de IP na Rede
III. Aplicável para servidores e/ou serviços que não podem mudar de IP

DHCP: Dynamic Host Configuration Protocol. Trata-se de um protocolo utilizado em redes de computadores que permite a estes obterem um endereço IP automaticamente.

I. Facilita o gerenciamento
II. Ausência de Conflitos de IP na Rede
III. Aplicável para grandes redes que não precisam de IP fixo

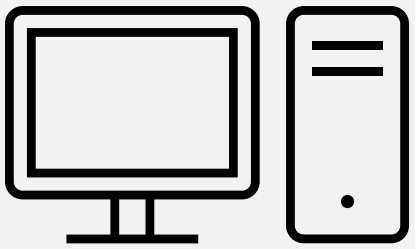
IPv4 vs IPv6

O Internet Protocol Version 6 (Protocolo de Internet Versão 6, em português) é a denominação da versão mais recente do padrão responsável por abrigar todos os endereços de dispositivos conectados à internet

No endereço IPv4 temos quatro grupos, ou octetos, nos quais podemos utilizar números para escrever o endereço. Cada octeto é um conjunto de oito bits. Logo, temos 32 bits disponíveis para escrever um endereço. Ou, aproximadamente, 4,2 bilhões de endereços.

Já com o IPv6, temos oito grupos, porém esses grupos não são divididos em oito bits cada, mas em 16 bits, separados por dois pontos(:). Portanto, temos 128 bits disponíveis para escrever nosso endereço. Logo, temos, aproximadamente, 340 undecilhões de endereços. Ou, 3,4 x 10^38 endereços.

IPv4 vs IPv6 Desvantagens IPv4



192.168.0.228

fe80::f3d0:c427:5825:5bf4

fe80::f3d0:c427:5825:5bf4

fe80:0000:0000:0000:f3d0:c427:5825:5bf4

Rápido esgotamento do espaço de endereço: Isso levou ao uso de conversores de endereço de rede (NATs) que mapeiam vários endereços particulares para um único endereço IP público. Os principais problemas criados por esse mecanismo são a sobrecarga de processamento e a falta de conectividade de ponta a ponta.

Falta de suporte a hierarquia: Por causa de sua organização de classe predefinida inerente, IPv4 não tem um verdadeiro suporte hierárquico. É impossível estruturar os endereços IP de uma forma que realmente mapeie a topologia de rede. Essa falha de design crucial cria a necessidade de grandes tabelas de roteamento para entregar pacotes IPv4 em qualquer local na Internet.

Configuração de rede complexa: Com o IPv4, os endereços devem ser atribuídos estaticamente ou usando um protocolo de configuração, como o DHCP. Em uma situação ideal, hosts não precisariam depender da administração de uma infraestrutura DHCP. Em vez disso, eles poderiam configurar a si mesmos com base no segmento de rede no qual estivessem localizados.

Falta de autenticação interna e de confidencialidade: O IPv4 não requer suporte para nenhum outro mecanismo que fornece autenticação ou criptografia dos dados transmitidos. Isso muda com o IPv6. O protocolo IPsec é um requisito de suporte a IPv6.

Comandos de controle de rede [Windows]

Ipconfig: Fornecer informações básicas de configuração IP da rede em que você está conectado. Quando digitamos o comando **ipconfig**, ele exibe informações básicas como, adaptadores de rede, adaptadores de LAN Wi-Fi, endereço IPv4, gateway padrão, máscara de subnet.

ping: Identificar e Solucionar problemas de conexão de Rede, e/ou testar velocidade de resposta do Host. Quando digitamos o comando, "ping e o seu caminho no CMD", ele envia pacotes de dados para o Host, se tudo tiver ok, você receberá esses pacotes de volta, confirmando que o Host de destino testado, está ativo.

tracert: Obter informações das rotas, números de roteadores, contagem de conexões, até o destino. O comando **tracert** rastreará cada ponto da rota que o pacote de dados enviado percorrerá antes de chegar ao seu destino, sendo exibido informações sobre a; latência entre os dispositivos e o endereço IP de cada salto ao longo da rota.

pathping: Obter informações das rotas, números de roteadores, contagem de conexões, até o destino. O comando **pathping**, tem função semelhante a combinação de dois comandos; **ping** e **tracert**, no entanto ele exibe um relatório estatístico de perdas de pacotes e latência, tornando um comando mais completo, com mais detalhes

getmac: Fornece uma maneira fácil de encontrar o endereço MAC do seu dispositivo. Todos os dispositivos de hardware têm sua própria Identidade, no caso de dispositivos que se conectam a Rede, cada um deles têm seu próprio número de MAC, isso quando o equipamento está em conformidade com os padrões IEEE 802.

hostname: Fornece uma maneira simples de identificar o nome do Host atribuído ao seu dispositivo Windows.

nslookup: Obter informações sobre registros de DNS de um determinado domínio, Host ou um IP. Existem dois modos de trabalho para o comando **nslookup**. Modo Interativo e o Modo não Interativo. Para iniciar o Modo Interativo, digitamos a sintaxe **nslookup**, ele já entra no Modo Interativo, você pode digitar os parâmetros desejado, como no nosso exemplo, colocamos o parâmetro >www.google.com

netstat: Obter informações: Conexões ativas, protocolos de conexões TCP ou UDP, IP e Portas ativas ou inativas, IP ou FQDN de dispositivos Remotos, Conexões ativas ou inativas. O comando netstat permite listar conexões de redes ativas de entrada e de saída, e monitorar as portas de conexões, exibir estatísticas de protocolos, IPv4, IPv6, adaptadores de rede e roteamento em tempo real

systeminfo: Exibe informações completas sobre o seu PC

Comandos de controle de rede [Linux]

ip: Manipulação do roteamento para atribuir e configurar parâmetros de rede

traceroute: Identificar a rota tomada pelos pacotes para chegar ao host

tracepath: Obtém a unidade de transmissão máxima ao rastrear o caminho para o host de rede

ping: Frequentemente usado para verificar a conectividade entre o host e o servidor

ss: Obtém detalhes sobre soquetes de rede

dig: Fornece todas as informações necessárias sobre o servidor de nomes DNS

host: Imprime o endereço IP de um domínio específico e vísceras

hostname: Usado principalmente para imprimir e alterar o nome do host

curl: Transfere dados pela rede, suportando vários protocolos

mtr: Uma combinação de ping e traceroute é usada para diagnosticar a rede

whois: Obtém informações sobre domínios registrados, endereços IP, servidores de nomes

ifplugstatus: Detecta o status do link de um dispositivo Ethernet local

iftop: Monitora estatísticas relacionadas à largura de banda

tcpdump: Utilitário de detecção e análise de pacotes usado para capturar, analisar e filtrar o tráfego de rede

ettool: Permite que os usuários configurem dispositivos Ethernet

nmcli: Utilitário de solução de problemas para conexões de rede

nmap: Usado principalmente para auditar a segurança da rede

bmon: Um utilitário de código aberto para monitorar a largura de banda em tempo real

firewalld: Ferramenta CLI para configurar regras de Firewall

iperf: Utilitário para medir o desempenho e o ajuste da rede

speedtest-cli: Utilitário CLI de speedtest.net para verificar as velocidades da Internet

vnstat: Usado principalmente para monitorar o tráfego de rede e o consumo de largura de banda

Agradeço
a sua atenção!

Diego Brito

diego.brito@sptech.school

SÃO PAULO TECH SCHOOL