

Computer Networks - PL 4

\$ ip addr → exibe informações detalhadas sobre todas as interfaces de rede.

- nome da interface
- endereços IP atribuídos
- estado da interface

Interface lo : loopback, sempre com ip 127.0.0.1

Interface ens33 : interface Ethernet que conecta a rede do host

IP: 192.168.186.129 / 24

máscara de rede

\$ sudo ifconfig

- ↳ endereço IP;
- maskra de rede;
- broadcast;

User datagram Protocol (UDP)

→ Protocolo de comunicação do conjunto TCP/IP usado para enviar mensagens (datagramas) em redes IP.

→ Não exige estabelecer conexões ou caminhos antes da comunicação.

→ Portas de 16 bits : identificam aplicações dentro de um módulo.

↳ Permitem que várias aplicações na mesma máquina usem a rede sem confusão de dados.

Exemplo : Uma aplicação A (porta 1351) envia um datagrama para a aplicação E (porta 234) no endereço IP 192.168.1.3.

Funionalidades:

- Verificação de integridade;
- Sem garantias de entrega : não há confirmação de receção;
- Priorização para aplicações sensíveis ao tempo (prefere descartar pacotes a sofrer atrasos por retransmissão).

Limitações: Não oferece confiabilidade ou conexão de enxos.

Transmission Control Protocol (TCP)

- Fiduciário: implementa controlo de erros e retransmite dados que não chegam ou chegam corrompidos.
- Orientado a conexão: estabelece canais dedicados entre pares de aplicações;
 - garante a sequência dos dados e implementa controlo de fluxo.

Estabelecimento de conexão (Three-way Handshake):

1. SYN: o cliente A inicia a conexão enviando um pedido SYN com um número de sequência aleatório (N_A).
2. SYN-ACK: O servidor B aceita e responde com SYN-ACK, incluindo o seu número de sequência (N_B) e confirmado (ACK) o número de A ($N_A + 1$).
3. ACK: o cliente A finaliza enviando ACK para confirmar o número de B ($N_B + 1$).

Uso de portas:

- Utiliza portas de 16 bits para identificar aplicações em cada nó.
- Portas TCP e UDP são independentes, pois operam em diferentes camadas.

Vantagens:

- fiabilidade e retransmissão automática de dados;
- preservação da ordem dos bytes;
- controlo de fluxo para evitar sobrecarga dos dados;

Port Numbers

Porta: identifica unicamente um ponto de conexão para direcionar os dados a um serviço específico.

Porta de 16 bits: usada para cada protocolo de transporte (TCP, UDP) em combinação com o endereço IP de um host.

Tipos

- Well-known ports: nº abaixo de 1024, reservados para serviços essenciais (HTTP, F

Ephemeral ports: nº acima de 1024, usadas para conexões temporárias por aplicações

Função dos port numbers: facilitar o encaminhamento de pacotes para a aplicação correspondente no host

Dynamic Host Configuration Protocol (DHCP)

Protocolo que automatiza a atribuição de endereços IP em redes. Ele facilita a configuração de dispositivos (como computadores e impressoras) sem que o administrador precise configurar manualmente os endereços IP para cada dispositivo.

Processo de comunicação DHCP:

1. Cliente DHCP: quando um dispositivo (cliente) entra na rede, ele não sabe qual endereço usar. Então, ele envia uma solicitação chamada DHCP discover, que é enviada para o endereço broadcast (255.255.255.255). Este tipo de mensagem é recebida por todos os servidores DHCP na rede local.
2. Servidor DHCP: quando um servidor DHCP recebe a solicitação, ele responde com uma oferta de configuração, chamada DHCP offer. Esta resposta inclui um endereço IP que o servidor está disposto a fornecer ao cliente, junto dos outros parâmetros de rede, como máscara de sub-rede e gateway padrão.
3. Seleção da oferta: o cliente pode receber várias ofertas, mas escolhe uma delas e envia uma solicitação DHCP request para o servidor que fez a oferta escolhida.
4. Confirmação: o servidor DHCP então confirma a atribuição do endereço IP enviando uma DHCP ACK (acknowledgement) para o cliente. A partir desse momento, o dispositivo está configurado para usar o endereço IP atribuído.

→ Além disso, o servidor DHCP mantém um registo do endereço MAC do dispositivo (identificador único da interface da rede) e o IP atribuído. Isto garante que o servidor não atribua o mesmo endereço IP a dispositivos diferentes, evitando conflitos.

Internet Control Message Protocol (ICMP)

Protocolo de nível ma suite de protocolos da Internet. É usado para enviar mensagens de erro e informações operacionais entre dispositivos de rede, como roteadores.

O comando PING usa mensagens ICMP de echo request e echo reply. Ele é usado para testar a conectividade entre dois dispositivos na rede, enviando um pacote ICMP para o destino e aguardando uma resposta para verificar se o dispositivo está ativo.

Domain Name System (DNS)

Sistema usado para identificar computadores na Internet e outras redes IP.

Traduz nomes de domínio legíveis em endereços IP numéricos.

Comandos como nslookup, host e dig são usados para realizar consultas ao DNS e obter o mapeamento entre nomes de domínio e endereços IP.

Create a host-only network in VMware

Uma host-only networking é uma tipo de rede virtual onde a comunicação acontece apenas entre a máquina host e a máquina virtual (VM), sem a necessidade de uma interface de rede física. Ou seja, a rede é isolada do mundo exterior, permitindo que as VM's comuniquem entre si e com a máquina host, mas sem acesso direto à rede externa (com Internet).

- Para configurar o endereço IP estático para a VM é necessário editar o ficheiro de configuração de rede NetPlan, que define como a rede é configurada no sistema. O objetivo é atribuir um endereço IP dentro de um intervalo pré-determinado à segunda interface de rede da VM.

SSH (Secure Shell)

Protocolo de rede utilizado para aceder de forma segura a um computador remoto através de uma rede insegura.

→ permite controlar um computador remoto de maneira segura e prática. Permite que

ssh myuser@server.example.com

nome de usuário da máquina remota (da conta à qual eu pretendo aceder)

endereço de rede IP da máquina remota

o utilizador execute comandos, transfira arquivos e realize outras operações...

SSH Key Pair

→ Utilizado para autenticação sem senha e acesso seguro a um servidor remoto. Em vez de usar uma senha para fazer login, pode-se usar um par de chaves criptográficas: uma chave privada (que mantém no computador) e uma chave pública (que coloca no servidor).

Gerar o par de chaves:

\$ ssh-keygen -t rsa -b 4096 → isto cria dois arquivos:
~/.ssh/id_rsa (chave privada)
~/.ssh/id_rsa.pub (chave pública)

Copiar a chave pública para o servidor:

\$ ssh-copy-id username@remotehost → para permitir o login sem senha,
ou copiar a chave pública para o servidor
\$ ssh -copy-id -i ~/.ssh/mykey user@host ↓ para testar se funcionou
\$ ssh -i ~/.ssh/mykey user@host → Após este comando, o servidor reconhecerá
ou a chave pública e permitirá o login sem senha.

\$ scp fileName username@remote host : /path/to/destination

↓
O comando scp (secure copy) permite copiar arquivos de forma segura entre computadores, usando o protocolo ssh.
(pode copiar arquivos do local para o remoto ou vice-versa)

Resumo: Pilha de protocolos TCP/IP

1. Internet Protocol (IP)

Responsável pelo roteamento dos pacotes de dados entre dispositivos em diferentes redes. O IP define o endereço de cada dispositivo na rede e garante que os dados sejam entregues ao destino correto.

Nível: camada de rede (layer 3).

2. ICMP (Internet Control Message Protocol)

Usado para enviar mensagens de erro e informações operacionais. Por exemplo, ele é utilizado pelo comando ping para verificar a conectividade entre dois dispositivos e gerar mensagens de erro quando um pacote não pode ser entregue.

Nível: camada de rede (layer 3).

3. ARP (Address Resolution Protocol)

Traduz endereços IP para endereços físicos (MAC addresses) necessários para a comunicação em uma rede local (LAN). O ARP é usado para encontrar o endereço MAC associado a um endereço IP dentro de uma rede local.

Nível: Camada de enlace (layer 2).

4. UDP (User Datagram Protocol)

Protocolo de comunicação sem conexão e não confidencial. O UDP envia pacotes (datagramas) de dados de uma forma simples e rápida, sem garantir a entrega ou a ordem dos pacotes. Isso torna-o adequado para aplicações que requerem baixa latência, como streaming de vídeo e jogos online.

Nível: Camada de transporte (layer 4).

5. TCP (Transmission Control Protocol)

Protocolo confidencial e orientado à conexão. O TCP garante que os dados sejam entregues de forma ordenada e sem erros. Ele estabelece uma conexão entre os dispositivos antes de transferir os dados e utiliza técnicas de controle de fluxo e retransmissão para garantir que a comunicação seja bem-sucedida.

Nível: Camada de transporte (layer 4)