

MÓDULO REDES/LINUX I

Curso de Redes / Infraestrutura

Versão: 2026

Professor: Marcos Brandão

Objetivo da Aula

Praticar comandos de rede utilizados na administração de servidores Linux Debian, entendendo:

- funcionamento da rede no Linux;
- identificação de IPs;
- roteamento;
- DNS;
- conectividade;
- monitoramento de portas;
- diagnóstico de problemas de rede.

1. Identificação de rede do servidor

hostname

Mostra o nome do servidor.

```
hostname
```

Resultado esperado

```
srv-rede01
```

Explicação

O hostname identifica o servidor na rede.

Muito utilizado em:

- SSH;
- monitoramento;

- inventário.
-

hostname -I

Mostra o IP do servidor.

```
hostname -I
```

Resultado esperado

```
192.168.0.10
```

Explicação

Exibe rapidamente os IPs configurados.

ip a

Mostra interfaces e endereços IP.

```
ip a
```

Resultado esperado

```
2: ens18: <UP,BROADCAST,RUNNING>  
inet 192.168.0.10/24
```

Explicação

Principal comando de rede no Linux moderno.

Mostra:

- interfaces;
 - IPv4;
 - IPv6;
 - MAC Address;
 - status da interface.
-

ip link

Mostra interfaces de rede.

ip link

Resultado esperado

2: ens18: <BROADCAST,MULTICAST,UP>

Explicação

Exibe:

- nome da placa;
 - estado UP/DOWN;
 - MAC Address.
-

2. Testes de conectividade

ping

Testa comunicação com outro host.

ping google.com

Resultado esperado

64 bytes from ...

Explicação

Verifica:

- acesso à internet;
 - resolução DNS;
 - latência;
 - conectividade.
-

ping 8.8.8.8

Teste usando IP diretamente.

ping 8.8.8.8

Explicação

Se funcionar por IP e não por nome:

- problema é DNS.
-

Parar o ping

CTRL + C

3. Informações de roteamento

ip route

Mostra tabela de rotas.

ip route

Resultado esperado

```
default via 192.168.0.1 dev ens18
```

Explicação

Mostra:

- gateway padrão;
 - redes locais;
 - interfaces usadas.
-

route -n

Comando antigo de roteamento.

Instalar:

```
sudo apt install net-tools -y
```

Executar:

route -n

Explicação

Exibe rotas numericamente.

4. DNS no Linux

cat /etc/resolv.conf

Mostra DNS configurado.

```
cat /etc/resolv.conf
```

Resultado esperado

```
nameserver 8.8.8.8
```

Explicação

Arquivo responsável pelos servidores DNS.

nslookup

Consulta DNS.

Instalar:

```
sudo apt install dnsutils -y
```

Uso:

```
nslookup google.com
```

Resultado esperado

```
Address: 142.250.x.x
```

Explicação

Verifica:

- resolução de nomes;
 - funcionamento do DNS.
-

dig

Consulta DNS avançada.

```
dig google.com
```

Explicação

Ferramenta profissional para:

- troubleshooting;
 - análise DNS;
 - registros MX/TXT/A/CNAME.
-

5. Verificação de portas e serviços

ss -tulnp

Mostra portas abertas.

```
ss -tulnp
```

Resultado esperado

```
LISTEN 0 128 0.0.0.0:22
```

Explicação

Mostra:

- portas TCP/UDP;
 - serviços escutando;
 - processos associados.
-

netstat -tulnp

Versão antiga do comando.

```
netstat -tulnp
```

Explicação

Ainda muito usada em ambientes legados.

lsof -i

Mostra conexões abertas.

Instalar:

```
sudo apt install lsof -y
```

Executar:

```
lsof -i
```

Explicação

Exibe:

- conexões;
 - portas;
 - processos usando rede.
-

6. Testes de portas e conectividade

telnet

Testa conexão em portas específicas.

Instalar:

```
sudo apt install telnet -y
```

Uso:

```
telnet google.com 80
```

Resultado esperado

Connected to google.com

Explicação

Muito usado para:

- testar serviços;
 - verificar firewall;
 - validar portas abertas.
-

nc (netcat)

Ferramenta avançada de rede.

Instalar:

```
sudo apt install netcat-openbsd -y
```

Teste:

```
nc -zv google.com 443
```

Resultado esperado

Connection successful

Explicação

Muito usada por administradores e pentesters.

7. Monitoramento de rede

iftop

Monitoramento de tráfego em tempo real.

Instalar:

```
sudo apt install iftop -y
```

Executar:

```
sudo iftop
```

Explicação

Mostra:

- consumo de banda;
 - conexões ativas;
 - tráfego em tempo real.
-

nload

Monitor simples de banda.

Instalar:

```
sudo apt install nload -y
```

Executar:

```
nload
```

Explicação

Exibe:

- upload;
 - download;
 - velocidade instantânea.
-

8. Descoberta e diagnóstico de rede

arp -a

Mostra tabela ARP.

```
arp -a
```

Resultado esperado

192.168.0.1 ether xx:xx:xx

Explicação

Relaciona:

- IP;
 - MAC Address.
-

ip neigh

Equivalente moderno do ARP.

ip neigh

traceroute

Mostra caminho até destino.

Instalar:

```
sudo apt install traceroute -y
```

Uso:

```
traceroute google.com
```

Explicação

Mostra:

- roteadores intermediários;
 - saltos;
 - latência.
-

9. Firewall no Debian

ufw status

Verifica firewall.

```
sudo ufw status
```

Resultado esperado

Status: active

Liberar porta SSH

```
sudo ufw allow 22
```

Liberar HTTP

```
sudo ufw allow 80
```

Ativar firewall

```
sudo ufw enable
```

Ver regras numeradas

```
sudo ufw status numbered
```

10. Captura de pacotes

tcpdump

Captura tráfego de rede.

Instalar:

```
sudo apt install tcpdump -y
```

Capturar:

```
sudo tcpdump -i ens18
```

Explicação

Ferramenta extremamente importante para:

- análise;
 - troubleshooting;
 - segurança.
-

Filtrar porta

```
sudo tcpdump port 80
```

Filtrar ICMP (ping)

```
sudo tcpdump icmp
```

11. SSH e acesso remoto

Verificar SSH

```
systemctl status ssh
```

Resultado esperado

```
active (running)
```

Conectar via SSH

```
ssh usuario@192.168.0.10
```

Explicação

Principal método de administração remota Linux.

Ver conexões SSH ativas

```
who
```

12. Download e testes web

wget

Baixa arquivos.

```
wget https://site.com/arquivo.zip
```

curl

Faz requisições HTTP.

```
curl ifconfig.me
```

Resultado esperado

```
191.xxx.xxx.xxx
```

Explicação

Muito usado em:

- APIs;
 - automações;
 - troubleshooting web.
-

Exercícios Práticos

Exercício 1

Descobrir:

- IP do servidor;
- gateway;
- DNS configurado.

Comandos:

```
ip a  
ip route  
cat /etc/resolv.conf
```

Exercício 2

Testar conectividade:

```
ping 8.8.8.8  
ping google.com
```

Pergunta:

- Qual a diferença entre os dois testes?
-

Exercício 3

Verificar portas abertas:

```
ss -tulnp
```

Identificar:

- SSH;
 - Apache;
 - outros serviços.
-

Exercício 4

Instalar Apache:

```
sudo apt install apache2 -y
```

Verificar porta:

```
ss -tulnp | grep 80
```

Exercício 5

Capturar pacotes ICMP:

```
sudo tcpdump icmp
```

Em outro terminal:

```
ping google.com
```

Desafio Final

Cada aluno deverá:

1. Descobrir IP;
 2. Descobrir gateway;
 3. Descobrir DNS;
 4. Instalar Apache;
 5. Verificar porta 80;
 6. Liberar firewall;
 7. Testar conectividade;
 8. Capturar pacotes;
 9. Acessar via navegador;
 10. Explicar o funcionamento da comunicação.
-

Perguntas para revisão

1. Qual comando mostra IP?
 2. Qual mostra portas abertas?
 3. Qual verifica DNS?
 4. Diferença entre ping por IP e por nome?
 5. Para que serve o traceroute?
 6. O que faz o tcpdump?
 7. Para que serve o firewall?
 8. Como verificar conexões ativas?
-

Resumo dos comandos essenciais

ip a

ip route

ping

nslookup

dig

ss -tulnp

netstat

tcpdump

traceroute

ufw

curl

wget

iftop

nload

ssh