
Revisão do Tópico 205 – Configurações de Rede

205.1 – Configurações Básicas de Rede

Comando ifconfig

Uso e Principais Opções

ifconfig : Exibir apenas as interfaces ativas (UP/RUNNING)
ifconfig -a : Exibir todas as interfaces de rede, inclusive as inativas
ifconfig eth0 : Exibir as informações de uma interface específica

ifconfig eth0 192.168.1.10 up : Definir um IP e subir a interface
ifconfig eth0 192.168.1.10 netmask 255.255.255.0 : Definir IP e Máscara em uma interface
ifconfig eth0 down : baixar uma interface

ifconfig eth0:0 10.0.0.10 netmask 255.255.255.0 : Definir um IP adicional à uma interface
ifconfig eth0:sub1 172.16.30.1 : Definir um IP adicional à uma interface
ifconfig eth0 add 10.0.0.10 netmask 255.255.255.0 : Definir um IP adicional à uma interface

ifconfig eth0 hw ether 00:00:00:00:00:00 : Definir um MAC Address específico para uma interface

---

Comando route

Uso e Principais Opções

route -n : Exibe as rotas ativas, sem resolver os nomes

route {add|del} [-net|-host] alvo [interface]

route add default gw 192.168.1.1 : Define o IP gateway. Pode ser incluído o “dev eth0” ao final.
route del default : Remover a rota padrão.

route add -net 172.16.10.0 netmask 255.255.255.0 gw 192.168.1.10 dev eth0 : Adicionar uma rota à rede 172.16.10.0, pelo gateway/roteador 192.168.1.10, utilizando a interface eth0
route add -net 172.20.0.0/16 gw 192.168.1.1

route del -net 172.20.20.0/24
route del -net 10.0.0.0 netmask 255.255.255.0 : Remover a rota

---

Comando ip

Uso e Principais Opções

ip link show : Exibe o estado de cada interface
ip link show eth0 : Exibe o estado de uma interface específica

ip address show : Exibe as interfaces com seus respectivos IPs
ip -6 address show : Exibe apenas os IPs IPV6 de cada interface
ip address flush dev eth0 : Limpa as definições de IP
ip address add 10.0.0.10/24 dev eth0 : Define um novo IP à interface

ip route show : Exibe as rotas
ip route add 172.16.10.0/24 via 192.168.1.50 : Adiciona uma rota
ip route del 172.30.30.0/24
ip route add default via 192.168.1.1
ip route del default

ip neigh show : Exibe a tabela ARP (IP x MAC Address)

ARP = Address Resolution Protocol

Protocolo utilizado para resolver endereços da camada de Internet (IP) em endereços da camada de enlace (MAC).

Comando arp

Função: Exibir e maninhar a tabela de registros ARP

Uso e Principais Opções:

arp : Exibe a tabela IP x MAC atual
arp -n : Não resolve nomes
arp -d 192.168.1.10 : Remove a referência da tabela
arp -s 192.168.1.10 00:00:00:00:00:00 : Adiciona uma referência específica manualmente
arp -f /arquivo : Adiciona manualmente as referências contidas no arquivo especificado. Se nenhum arquivo for informado, será utilizado o /etc/ethers

Comando arpwatch

Função: Monitorar e enviar alarmes ao administrador de sistema sobre mudanças nas referências da tabela ARP.

Uso e Principais Opções

arpwatch -d : Modo debug

arpwatch -e email@email : Envia alarmes a um e-mail específico
arpwatch -i eth0 : Especifica a interface a ser monitorada

Configurações de Redes Wireless

Comando iw

Função: Usado para configurar os dispositivos wireless. Suporta apenas o padrão 802.11.

Uso e Principais Opções:

iw dev wlan0 link : Exibir os status da interface e conexão wireless
iw dev wlan0 scan : Exibir as rede acessíveis pela interface
iw dev wlan0 connect "Access Point" 2432 : Estabelecer uma conexão a um SSID

Comando iwlist

Função: Scanear e listar as redes wireless disponíveis

Uso e Principais Opções:

iwlist wlp2s0 scanning

Comando iwconfig

Função: Configurar uma interface de rede wireless. Associar uma interface a uma rede wireless Equivalente ao ifconfig.

Uso e Principais Opções:

iwconfig essid “Rede Wireless X”
iwconfig key s:123456

205.2 – Configurações e Resolução de Problemas Avançados em Redes

Roteamento

Identificando Flags nas Tabelas de Rotas

- U: Rota ativa (UP)
- H: Alvo da rota é um host
- G: Gateway sendo utilizado
- R: Rota Reestabelecida por Roteamento Dinâmico
- D: Rota Instalada por Roteamento Dinâmico
- M: Rota Modificado por Roteamento Dinâmico
- ! : Rota Rejeitada

Alguns Daemons de Roteamento Dinâmico:

- **Routed**
- **GateD**
- BIRD
- Zebra
- Quagga

Para habilitar o roteamento de pacotes de uma rede para outra, o seguinte parâmetro deve ser configurado para 1 no kernel:

- /proc/sys/net/ipv4/ip_forward (IPv4)
- /proc/sys/net/ipv6/conf/all/forwarding (IPv6)

Testando o Acesso a Hosts

Comandos ping / ping6

O comando ping pode ser utilizado tanto para IPv4 quanto para IPv6, com o uso da opção -6. O ping6 é específico para IPv6.

O ping utiliza o protocolo **ICMP**, enviando um pacote de **ECHO_REQUEST** e aguardando o retorno do **ECHO_REPLY**

Comandos traceroute / traceroute6

Assim como o ping, o traceroute pode ser utilizado tanto para IPv4 quanto para IPv6, com o uso da opção -6. O traceroute6 é específico para IPv6.

O traceroute utiliza por padrão o **protocolo UDP** para realização dos testes. Utilizando a opção -I o ICMP será utilizado.

O comando também utiliza o campo **TTL (Time to Live)** do protocolo IP para testar as conexões. Caso um host não consiga alcançar o host seguinte, ele deve retornar um pacote **ICMP TIME_EXCEEDED**.

Comando netcat (nc)

Função: Utilizado para testar conexões em portas TCP e UDP

Uso e Principais Opções:

nc 192.168.1.10 80 : Testar a porta 80 no IP 192.168.1.10
nc -vz 192.168.1.10 50-100 : Testa as portas de 50 a 100 do IP informado. O -z faz com que a porta seja apenas verificada mas não é feita a conexão. O -v é o modo verbose.

nc -l -p 1234 : Abre no host local o processo para escuta (listenning) na porta 1234

Comando netstat

Função: Exibir as conexões de rede da máquina, tabelas de roteamento, estatísticas sobre as interfaces e etc.

Uso e Principais Opções:

- -r : Exibe a tabela de rotas
- -n : Não resolve nomes
- -a : Exibe tanto as conexões de sockets em listenning quanto as demais. Sem o -a (ou o -l), as conexões em listenning não são exibidas.
- -l : Exibe os sockets em estado listening
- -i : Exibe estatísticas por interface de rede
- -t : TCP
- -u : UDP
- -A inet/unix/etc : Especificar o tipo de conexão. -A inet = --inet
- -p : Exibe o PID/Processo responsável por cada socket
- -c : Atualiza continuamente
- -s : Exibe as estatísticas por protocolo

Comando ss

Função: É o comando que visa substituir o netstat. Possui as mesmas funções de investigação e análise de sockets e conexões abertas.

Uso e Principais Opções:

Muitas das opções são iguais ao netstat, com algumas exceções:

- -a : Exibe todos os sockets

- -n : Não resolve os nomes dos serviços
- -r : Resolve os nomes dos hosts. No ss, por padrão os nomes dos hosts não são traduzidos
- -l : Conexões em listenning
- -p : Exibe os processos
- -t : TCP
- -u UDP
-

Comando lsof

Função: Listar arquivos abertos. Como todo socket também possui um arquivo aberto no sistema, ele também pode ser usado para monitorar conexões.

Uso e Principais Opções:

lsof -i : Exibe os arquivos relacionados ao protocolo IP
lsof -i tcp : Apenas TCP
lsof -i :443 : Apenas porta 443
lsof -i @192.168.1.1:443 : Apenas de um IP específico em uma Porta específica

---

Comando tcpdump

Função: Realizar uma análise dos pacotes que trafegam pelas interfaces de rede.

Uso e Principais Opções:

- -c : Limita a quantidade de pacotes a ser capturados
- -D : Apenas lista as interfaces que podem ser analisadas
- -i : Especifica uma interface para ser capturada
- -q : Exibe os resultados em modo sucinto
- -t : Não mostra hora
- -v -vv -vvv : Ativa diferentes níveis de detalhamento
- -w : Escreve o resultado em um arquivo
- -r : Lê os dados de um arquivo

Filtros:
- dst host : Especificar o host destino
- src host : Especificar o host origem
- host : Especificar um host para origem ou destino
- dst port : Especificar uma porta destino
- src port : Especificar uma porta origem
- port : Especificar uma porta para origem ou destino
- dst net : Especificar uma rede destino
- src net : Especificar uma rede origem
- net : Especificar uma rede para origem ou destino
- dst portrange : Especificar um grupo de portas destino
- src portrange : Especificar um grupo de portas origem

- portrange : Especificar um grupo de portas para origem ou destino

Os filtros podem ser combinados com “and” e “or”. O not ou ! também pode ser uado para negar uma das opções.

Comando nmap

Função: É um port scanner, ou seja, uma ferramenta capaz de fazer uma varredura de portas locais ou de hosts e redes remotas.

Uso e Principais Opções:

nmap 192.168.1.10 : Faz a varredura em um host específico
nmap 192.168.1.10/24 : Faz a varredura em todos os hosts de uma rede

Opções:
- -F : FastScan. Verifica um conjunto menor de portas
- -sV : Procura identificar mais detalhes relacionados à versão do serviço disponibilizado em cada porta
- -p : Analisa uma porta específica, ou um conjunto delas.
- -O : Identifica detalhes do Sistema Operacional através do Stack Fingerprint

205.3 – Resolução de Problemas em Redes

Configurações de Rede

Padrão Debian

Arquivo de Configuração das Interfaces e Gateway: **/etc/network/interfaces**

Exemplo:
auto enp0s3
iface enp0s3 inet static
address 192.168.1.210
netmask 255.255.255.0
gateway 192.168.1.1

Padrão RedHat

Arquivo de Configuração das Interfaces: /etc/sysconfig/network-scripts/ifcfg-*

Exemplo: ifcfg-enp0s3
DEVICE=enp0s3
BOOTPROTO=static
IDPADDR=192.168.1.210
NETMASK=255.255.255.0
ONBOOT=yes

O gateway deve ser configurado no arquivo: /etc/sysconfig/network:
GATEWAY=192.168.1.1

NetworkManager

Função: Serviço responsável por gerenciar de maneira dinâmica as interfaces de rede com ou sem fio e suas conexões com a rede.

Diretório Principal: /etc/NetworkManager/

Comando Principal: nmcli

Investigação de Eventos e Logs

No processo de investigação de falhas de redes, informações e registros devem ser analisados principalmente nos seguintes arquivos e comandos:

- dmesg
- /var/log/messages (RedHat)
- /var/log/syslog (Debian)
- Systemd Journal, pelo comando “journalctl”

Falhas de DNS

Em eventos de falhas de resolução de nomes, os seguintes arquivos de configuração devem ser analisados:

- /etc/resolv.conf - Configurações referentes ao serviço DNS, principalmente o(s) servidor(es) DNS que deverá(ão) ser utilizado(s), através do parâmetro "nameserver"
- /etc/hosts - Definições estáticas de IP e Nomes
- /etc/networks - Definições estáticas de Redes e Nomes
- /etc/hostname ou /etc/HOSTNAME - Nome da máquina

Comandos para análise de DNS:

- hostname : Nome da máquina
  - -d : Exibe o domínio
  - -f : Exibe o FQDN (Fully Qualified Domain Name), ou seja, o nome completo do host
- host : Ferramenta utilizada para verificar a resolução de nomes
  - -a : Verifica todos os registros relacionados a um nome
  - -t <tipo> : Verifica um tipo de registros específico
- dig : Ferramenta para realizar a verificação de DNS de um endereço
  - # dig www.lpi.org
  - # dig www.lpi.org @8.8.8.8 : Utiliza um servidor DNS específico
  - # dig lpi.org -t mx : Verifica apenas um tipo específico de registro, no caso MX

TCP Wrappers

Os arquivos de configuração /etc/hosts.allow e /etc/hosts.deny podem ser configurados para definir quem pode ou não utilizar serviços que utilizam as bibliotecas do TCP Wrappers

É importante notar que:

- Se não há nenhuma configuração em nenhum dos 2 arquivos, não há bloqueios
- Se há uma regra de liberação de um serviço para determinado IP no /etc/hosts.allow, o host.deny nem mesmo é consultado
- Se não há regras de liberação no hosts.allow, o hosts.deny é consultado

Exemplos para o /etc/hosts.allow:
ALL: 192.168.8.* EXCEPT 192.168.8.1 : Libera todos os serviços para a rede 192.168.8.0/24, exceto para o IP 192.168.8.1
telnetd: 192.168.8.10 192.168.8.50 : Libera o serviço telnet para os 2 IPs informados

Exemplos para o /etc/hosts.allow:
ALL: ALL : Bloqueia tudo o que não for liberado no hosts.allow
sshd: 192.168.1.* : Bloqueia o serviço SSH para a rede 192.168.1.0/24

Comando mtr

Função: O mtr (My Trace Route) combina as funções do ping com o traceroute em uma interface que faz a atualização constante das informações de acesso a um host específco.

Uso e Principais Opções:

mtr -n www.lpi.org