

Linux Network Diagnostics Project (Ubuntu CLI)

By:

Chontele Coleman

Overview

This Linux networking project demonstrates command-line proficiency using tools on Ubuntu 22.04. It includes identifying IP and interface information, testing connectivity, analyzing DNS and remote hosts, examining open ports and firewall status without relying on a graphical user interface (GUI).

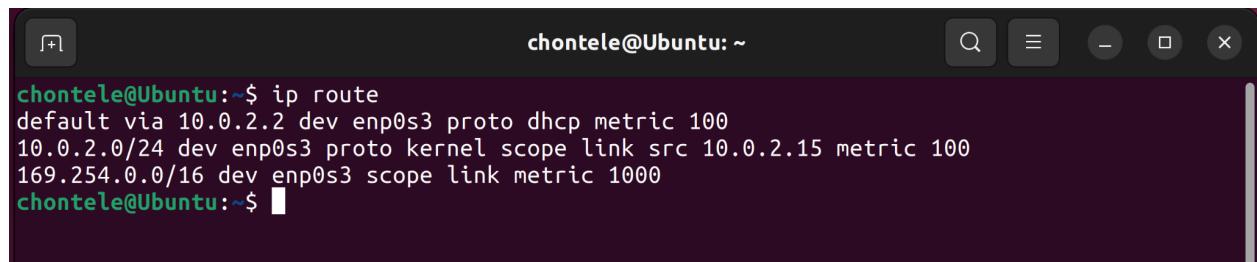
System Information & Interfaces

Commands executed:

ip a (lists network interfaces)

```
chontele@Ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    qlen 1000
    link/ether 08:00:27:6f:d3:33 brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
            valid_lft 86100sec preferred_lft 86100sec
        inet6 fd17:625c:f037:2:6e94:430b:f275:d5ad/64 scope global temporary dynamic
            valid_lft 86393sec preferred_lft 14393sec
        inet6 fd17:625c:f037:2:3e9c:2b60:aa55:4dee/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 86393sec preferred_lft 14393sec
        inet6 fe80::e09c:450a:cc83:7a7b/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
chontele@Ubuntu:~$
```

ip route (shows default gateway)



A screenshot of a terminal window titled "chontele@Ubuntu: ~". The window shows the command "ip route" being run and its output. The output displays three routing entries: a default route via interface enp0s3 with a metric of 100, a route to 10.0.2.0/24 via enp0s3 with a metric of 100, and a route to 169.254.0.0/16 via enp0s3 with a metric of 1000.

```
chontele@Ubuntu:~$ ip route
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
chontele@Ubuntu:~$
```

resolvectl status (shows DNS info)

```
chontele@Ubuntu:~$ resolvectl status
Global
  Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: stub

Link 2 (enp0s3)
  Current Scopes: DNS
    Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  Current DNS Server: 10.0.2.3
    DNS Servers: 10.0.2.3 fd17:625c:f037:2::3
    DNS Domain: lan
  . . . . .
```

hostnamectl (get hostname info)

```
chontele@Ubuntu:~$ hostnamectl
  Static hostname: Ubuntu
    Icon name: computer-vm
      Chassis: vm
    Machine ID: 3380e553b5cb4bb1b2f31515748d6f72
      Boot ID: 9a8c986c4ffd46009bc1136392ffef3f
  Virtualization: oracle
Operating System: Ubuntu 22.04.5 LTS
      Kernel: Linux 6.8.0-64-generic
    Architecture: x86-64
  Hardware Vendor: innotek GmbH
  Hardware Model: VirtualBox
```

Connectivity Testing

ping -c 4 <gateway_IP> (ping gateway)

```
chontele@Ubuntu:~$ ping -c 4 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=255 time=0.255 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=255 time=0.309 ms
64 bytes from 10.0.2.2: icmp_seq=3 ttl=255 time=0.297 ms
64 bytes from 10.0.2.2: icmp_seq=4 ttl=255 time=0.352 ms

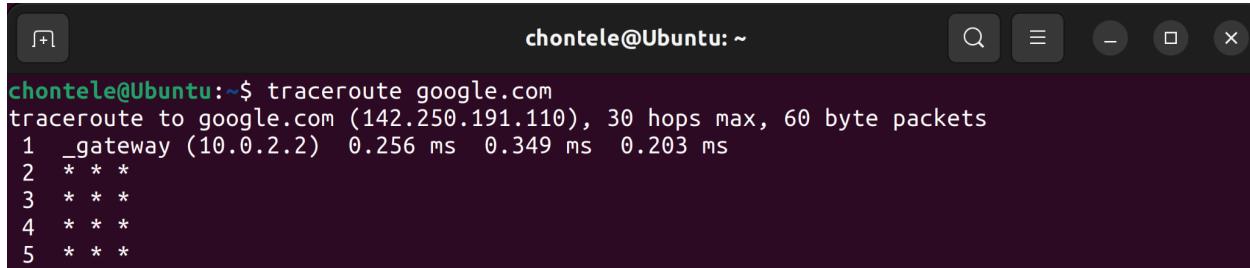
--- 10.0.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3088ms
rtt min/avg/max/mdev = 0.255/0.303/0.352/0.034 ms
```

ping -c 4 8.8.8.8 (ping Google DNS)

```
chontele@Ubuntu:~$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=32.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=26.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=27.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=27.6 ms

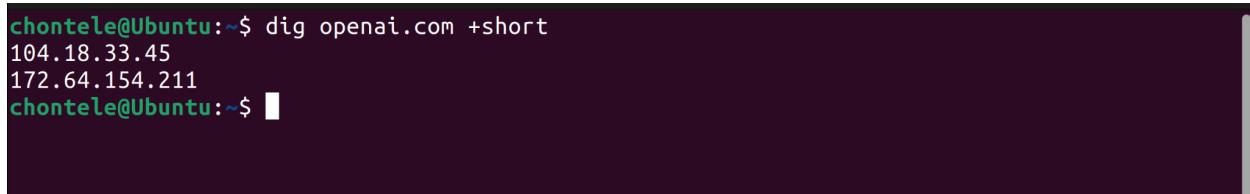
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 26.730/28.378/32.123/2.184 ms
```

traceroute google.com (Traceroute of google.com)



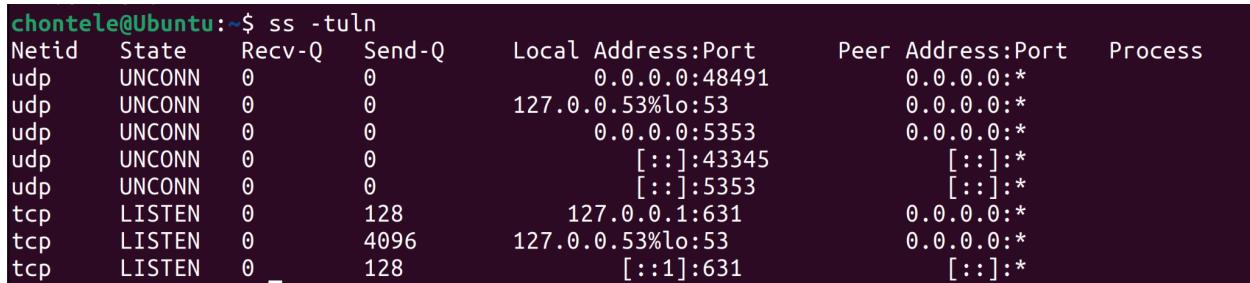
```
chontele@Ubuntu:~$ traceroute google.com
traceroute to google.com (142.250.191.110), 30 hops max, 60 byte packets
1 _gateway (10.0.2.2)  0.256 ms  0.349 ms  0.203 ms
2 * * *
3 * * *
4 * * *
5 * * *
```

dig openai.com +short (resolve domain IP)



```
chontele@Ubuntu:~$ dig openai.com +short
104.18.33.45
172.64.154.211
chontele@Ubuntu:~$
```

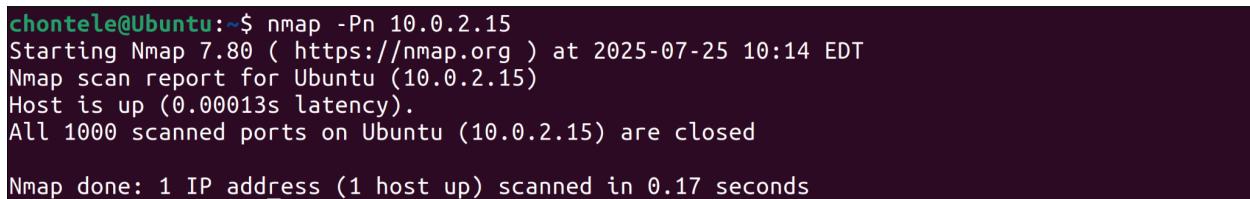
ss -tuln (checks locally open TCP ports)



Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
udp	UNCONN	0	0	0.0.0.0:48491	0.0.0.0:*	
udp	UNCONN	0	0	127.0.0.53%lo:53	0.0.0.0:*	
udp	UNCONN	0	0	0.0.0.0:5353	0.0.0.0:*	
udp	UNCONN	0	0	[::]:43345	[::]:*	
udp	UNCONN	0	0	[::]:5353	[::]:*	
tcp	LISTEN	0	128	127.0.0.1:631	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.53%lo:53	0.0.0.0:*	
tcp	LISTEN	0	128	[::1]:631	[::]:*	

Remote Host Analysis

nmap -Pn <remote_host_IP> (scan remote host ports)



```
chontele@Ubuntu:~$ nmap -Pn 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-25 10:14 EDT
Nmap scan report for Ubuntu (10.0.2.15)
Host is up (0.00013s latency).
All 1000 scanned ports on Ubuntu (10.0.2.15) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

whois example.com (get whois info)

```
chontele@Ubuntu:~$ whois example.com
Domain Name: EXAMPLE.COM
Registry Domain ID: 2336799_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.iana.org
Registrar URL: http://res-dom.iana.org
Updated Date: 2024-08-14T07:01:34Z
Creation Date: 1995-08-14T04:00:00Z
Registry Expiry Date: 2025-08-13T04:00:00Z
Registrar: RESERVED-Internet Assigned Numbers Authority
Registrar IANA ID: 376
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: A.IANA-SERVERS.NET
Name Server: B.IANA-SERVERS.NET
DNSSEC: signedDelegation
DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A86764247
C
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-07-25T14:17:32Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

nslookup example.com (Performs DNS lookup)

```
chontele@Ubuntu:~$ nslookup example.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   example.com
Address: 96.7.128.175
Name:   example.com
Address: 96.7.128.198
Name:   example.com
Address: 23.192.228.80
Name:   example.com
Address: 23.192.228.84
Name:   example.com
Address: 23.215.0.136
Name:   example.com
Address: 23.215.0.138
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94c8
Name:   example.com
Address: 2600:1406:bc00:53::b81e:94ce
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f24
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f31
```

curl -I http://example.com (Display HTTP headers)

```
chontele@Ubuntu:~$ curl -I http://example.com
HTTP/1.1 200 OK
Content-Type: text/html
ETag: "84238dfc8092e5d9c0dac8ef93371a07:1736799080.121134"
Last-Modified: Mon, 13 Jan 2025 20:11:20 GMT
Cache-Control: max-age=1421
Date: Fri, 25 Jul 2025 14:27:29 GMT
Connection: keep-alive
```

Security/Listening Ports

Netstat -tulnp (view open ports)

```
chontele@Ubuntu:~$ netstat -tulnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name
tcp        0      0 127.0.0.53:53          0.0.0.0:*             LISTEN
tcp        0      0 127.0.0.1:631         0.0.0.0:*             LISTEN
tcp6       0      0 ::1:631                ::*:*                  LISTEN
udp        0      0 0.0.0.0:48128          0.0.0.0:*             -
udp        0      0 127.0.0.53:53          0.0.0.0:*             -
udp        0      0 0.0.0.0:5353          0.0.0.0:*             -
udp6       0      0 ::1:37669              ::*:*                  -
udp6       0      0 ::1:5353              ::*:*
```

sudo ufw status verbose (show firewall status)

```
chontele@Ubuntu:~$ sudo ufw status verbose
Status: inactive
chontele@Ubuntu:~$
```

sudo journalctl -u ssh (check recent auth logins)

```
Status: inaktiv
chontele@Ubuntu:~$ sudo journalctl -u ssh
-- No entries --
chontele@Ubuntu:~$
```

ss -ntu (list IPs with active connections)

```
chontele@Ubuntu:~$ ss -ntu
Netid      State    Recv-Q    Send-Q          Local Address:Port          Peer Address:Port    Process
udp        ESTAB     0          0          10.0.2.15%enp0s3:68          10.0.2.2:67
chontele@Ubuntu:~$
```

Log Output & Documentation

ip a > logs/ip_info.txt (save command output)

```
chontele@Ubuntu:~$ ip a > logs/ip_info.txt
chontele@Ubuntu:~$ ls
backups  Documents  Linux-user-manager  Music      Public   Templates   Videos
Desktop   Downloads  logs                 Pictures   snap     test_files
chontele@Ubuntu:~$ cd logs
chontele@Ubuntu:~/logs$ ls
ip_info.txt
```

<command> >> log.txt (append multiple logs)

```
chontele@Ubuntu:~/logs$ ping -c 4 8.8.8.8 >> network_checks.txt
chontele@Ubuntu:~/logs$ ls
ip_info.txt  network_checks.txt
chontele@Ubuntu:~/logs$ traceroute google.com >> network_checks.txt
chontele@Ubuntu:~/logs$ ls
ip_info.txt  network_checks.txt
chontele@Ubuntu:~/logs$ cat network_checks.txt
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=34.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=27.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=27.8 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=38.4 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 27.670/32.107/38.406/4.587 ms
traceroute to google.com (142.250.190.78), 30 hops max, 60 byte packets
1  gateway (10.0.2.2)  0.355 ms  0.308 ms  0.383 ms
```

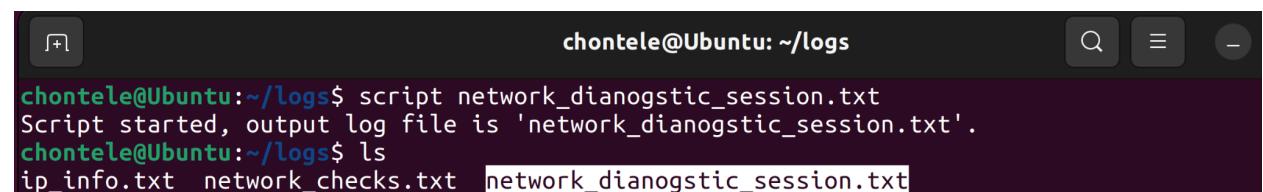
sudo journalctl -xe (view system logs)

```
chontele@Ubuntu:~/logs$ sudo journalctl -xe
[sudo] password for chontele:
Jul 25 12:25:19 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:19 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:19 Ubuntu gnome-shell[2541]: Bug in client with pid 2541: Buffer size (64x64) is n>
Jul 25 12:25:19 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:19 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:24 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:25 Ubuntu gnome-shell[2541]: Bug in client with pid 2541: Buffer size (64x64) is n>
Jul 25 12:25:25 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:25 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:29 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:29 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:29 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:29 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:29 Ubuntu gnome-shell[2541]: Bug in client with pid 2541: Buffer size (64x64) is n>
Jul 25 12:25:29 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:29 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:29 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:29 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:58 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:58 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:25:58 Ubuntu gnome-shell[2541]: Bug in client with pid 2541: Buffer size (64x64) is n>
Jul 25 12:25:58 Ubuntu gnome-shell[2541]: Bug in client with pid 3252: Buffer size (64x64) is n>
Jul 25 12:26:21 Ubuntu sudo[4401]: chontele : TTY=pts/0 : PWD=/home/chontele/logs : USER=root :>
```

dmesg | grep -i eth (view network logs)

```
chontele@Ubuntu:~/logs$ dmesg | grep -i eth
dmesg: read kernel buffer failed: Operation not permitted
chontele@Ubuntu:~/logs$ sudo dmesg | grep -i eth
[    1.853270] e1000 0000:00:03.0 eth0: (PCI:33MHz:32-bit) 08:00:27:6f:d3:33
[    1.853292] e1000 0000:00:03.0 eth0: Intel(R) PRO/1000 Network Connection
[    1.864543] e1000 0000:00:03.0 enp0s3: renamed from eth0
[ 103.964701] audit: type=1107 audit(1753458897.508:60): pid=601 uid=102 auid=4294967295 ses=42
94967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call" bus="system" path="/org/freedesktop/PolicyKit1/Authority" interface="org.freedesktop.DBus.Properties" member="GetAll" mask="send" name=:1.3' pid=2888 label="snap.snap-store/ubuntu-software" peer_pid=630 peer_label="unconfined"
[ 103.965314] audit: type=1107 audit(1753458897.508:61): pid=601 uid=102 auid=4294967295 ses=42
94967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call" bus="system" path="/org/freedesktop/PolicyKit1/Authority" interface="org.freedesktop.PolicyKit1.Authority" member="CheckAuthorization" mask="send" name=:1.3' pid=2888 label="snap.snap-store/ubuntu-software" peer_pid=630 peer_label="unconfined"
[ 104.075531] audit: type=1107 audit(1753458897.619:62): pid=601 uid=102 auid=4294967295 ses=42
94967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call" bus="system" path="/org/freedesktop/PolicyKit1/Authority" interface="org.freedesktop.DBus.Properties" member="GetAll" mask="send" name=:1.3' pid=2888 label="snap.snap-store/ubuntu-software" peer_pid=630 peer_label="unconfined"
[ 104.077414] audit: type=1107 audit(1753458897.621:63): pid=601 uid=102 auid=4294967295 ses=42
94967295 subj=unconfined msg='apparmor="DENIED" operation="dbus_method_call" bus="system" path="/org/freedesktop/PolicyKit1/Authority" interface="org.freedesktop.PolicyKit1.Authority" member=
```

script network_diagnostic_session.txt (full terminal session recording)



```
chontele@Ubuntu:~/logs$ script network_dianogstic_session.txt
Script started, output log file is 'network_dianogstic_session.txt'.
chontele@Ubuntu:~/logs$ ls
ip_info.txt network_checks.txt  network_dianogstic_session.txt
```

Final Outcome

This project validates essential Linux command-line networking skills, including:

- Identifying local and gateway IP configurations
- Testing and troubleshooting connectivity
- Performing DNS queries and remote scanning
- Using system tools to monitor ports, users, and logs