

Static and Default Routes

- Categories of routing table entries
 - Directly connected
 - Paths to remote networks
 - Host routes
 - Default route
- Directly connected routes
 - IP network/subnet for each active interface
- Static routes
 - Added manually by administrator
- Default route
 - Static route used if no other match
 - 0.0.0.0/0 or ::/0

Routing Tables and Path Selection

- Protocol
 - Source of the route
- Destination
 - Network/host address and prefix
- Interface
 - Outgoing interface
- Gateway/next hop
 - Address of next router along the path

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

C>* 10.0.0.2/32 is directly connected, lo, 00:06:52
S>* 10.0.1.0/24 [1/0] via 10.0.2.254, eth0, 00:02:26
C>* 10.0.2.0/24 is directly connected, eth0, 00:02:26
C>* 10.0.3.0/24 is directly connected, eth1, 00:06:51
S>* 10.0.4.0/24 [1/0] via 10.0.3.254, eth1, 00:06:49
```

Routing Table Example

Network	Interface	Source
10.0.1.0/24	G0	Static
10.0.2.0/24	G0	Connected
10.0.3.0/24	G1	Connected
10.0.4.0/24	G1	Static



Network	Interface	Source
10.0.1.0/24	G0	Connected
10.0.2.0/24	G1	Connected
10.0.3.0/24	G1	Static
10.0.4.0/24	G1	Static

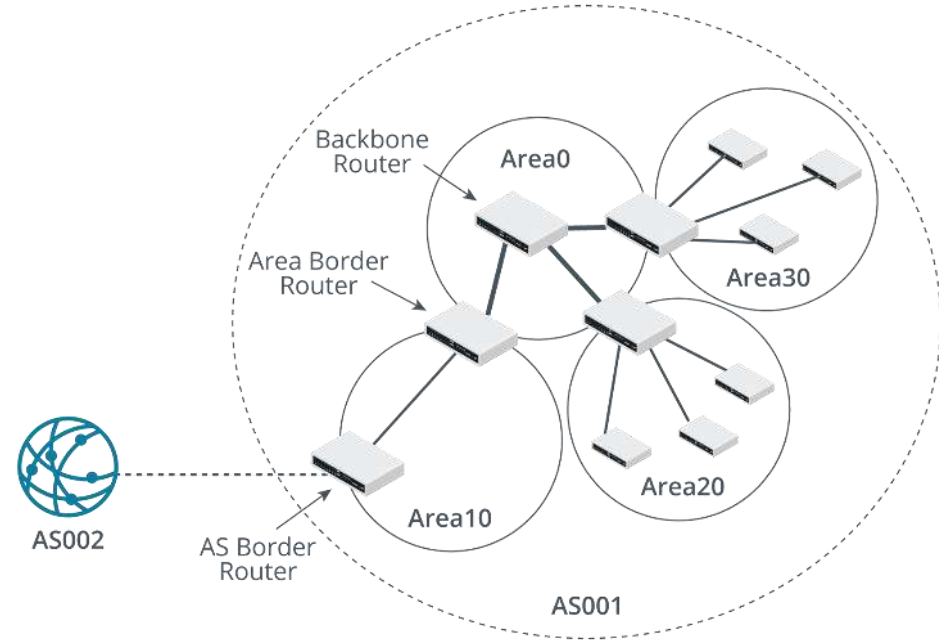
Network	Interface	Source
0.0.0.0/0	G0	Static
10.0.3.0/24	G0	Connected
10.0.4.0/24	G1	Connected

Dynamic Routing Protocols

- Build routing information base
- Share information with other routers (learned routes)
- Topology and metrics
 - Distance vector versus link state
 - Metrics assess similar routes for use of least-cost path in IP routing table
 - Algorithm determines nature of metrics
- Convergence
 - All routers agree on network topology

Open Shortest Path First

- Link state interior gateway protocol suited to complex private networks
- Group related networks by area hierarchy
- Supports classless addressing
- Runs over IP directly (protocol number 89) using multicasts



Border Gateway Protocol

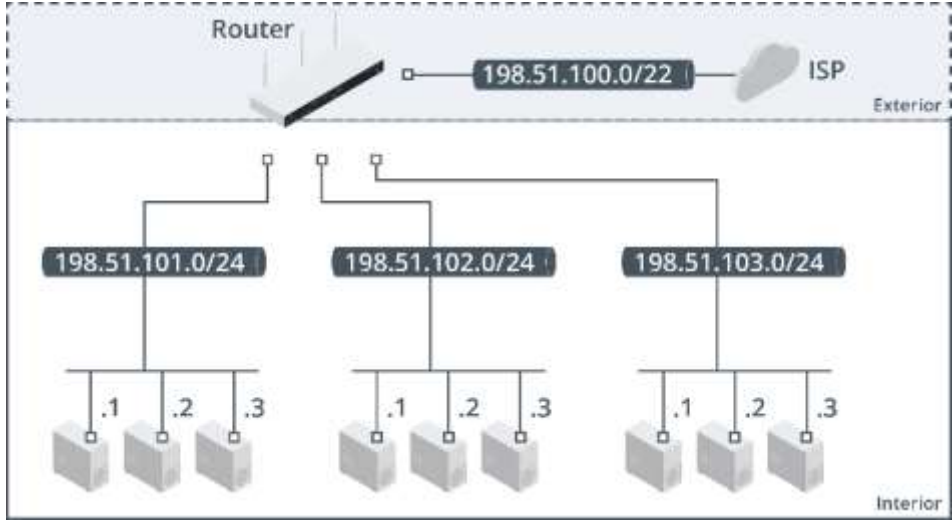
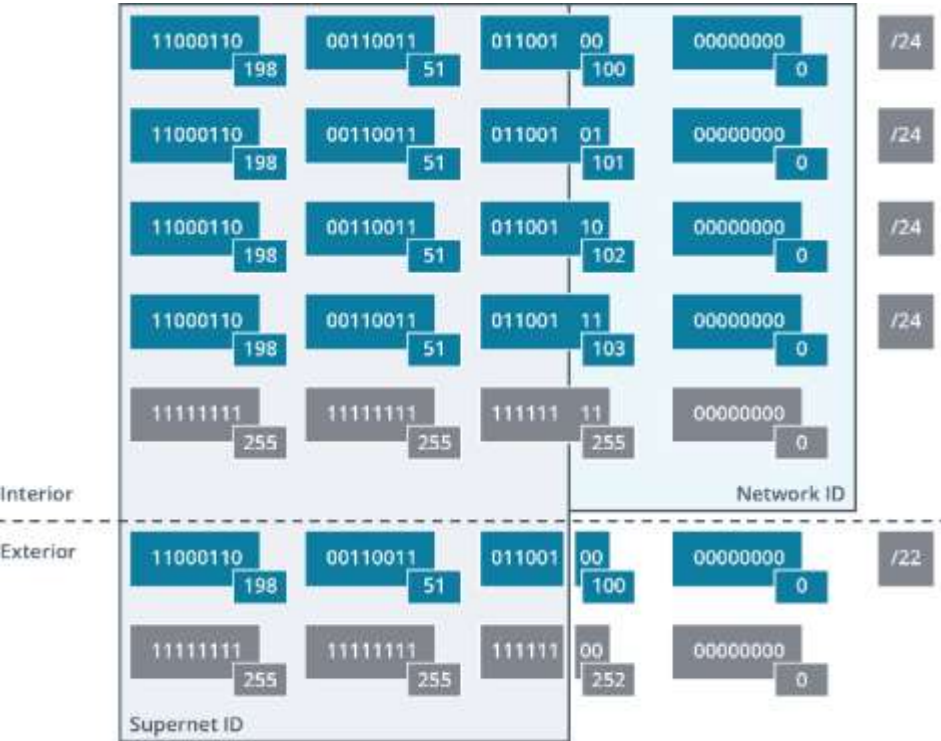
- Classed as hybrid or path vector
- Usually deployed as an Exterior Gateway Protocol
- Supports routing on the Internet
 - Autonomous Systems (ASes) hide internal network complexity from Internet routers
 - Autonomous System Number (ASN)
 - BGP routers exchange AS path data between Autonomous Systems
- Supports classless addressing
- Runs over TCP on port 179

Administrative Distance

Source	AD
Local interface/Directly connected	0
Static route	1
BGP	20
EIGRP	90
OSPF	110
RIP	120
Unknown	255

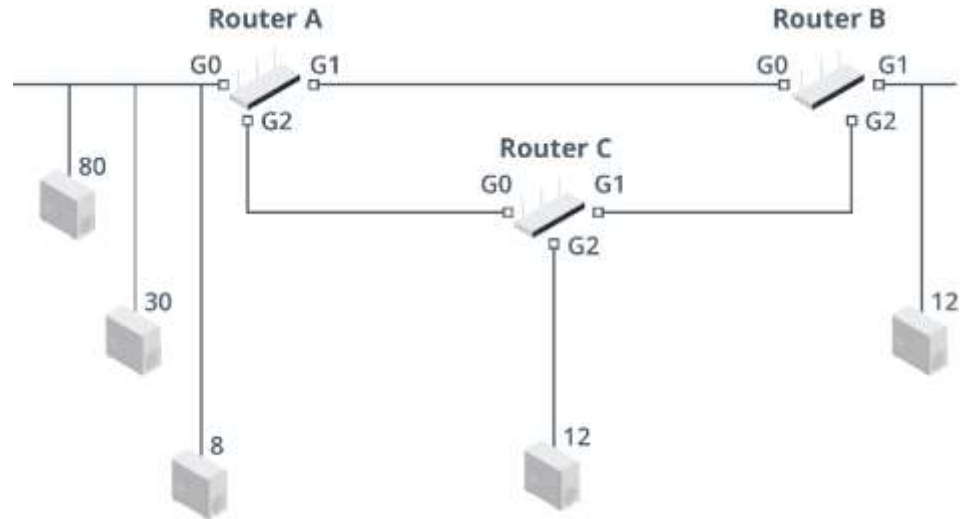
- Longer prefixes preferred for path selection
- Protocols add one route per destination prefix to global IP routing table
- Routing protocol uses metric to determine least-cost path
- Router uses administrative distance to prefer paths to same destination learned by different protocols

Classless Inter-Domain Routing



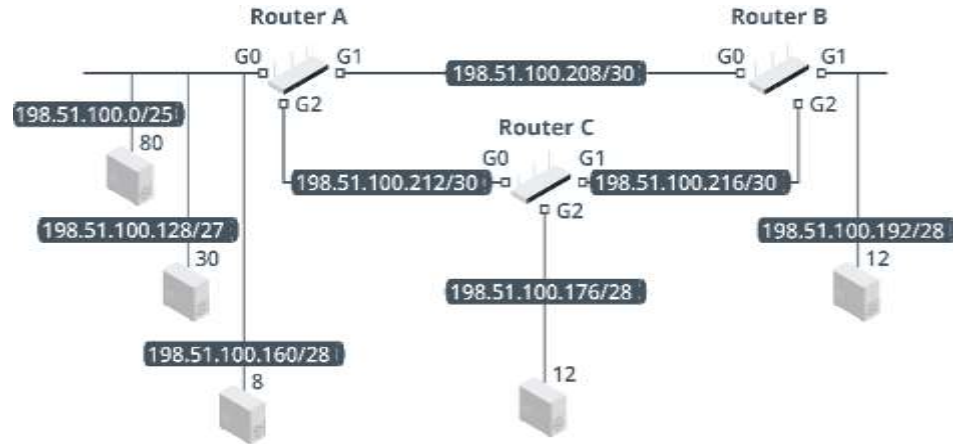
Variable Length Subnet Masks

- Use address space in IPv4 network more efficiently
- Rather than use the same mask for all subnets, use different mask lengths according to host numbers per subnet

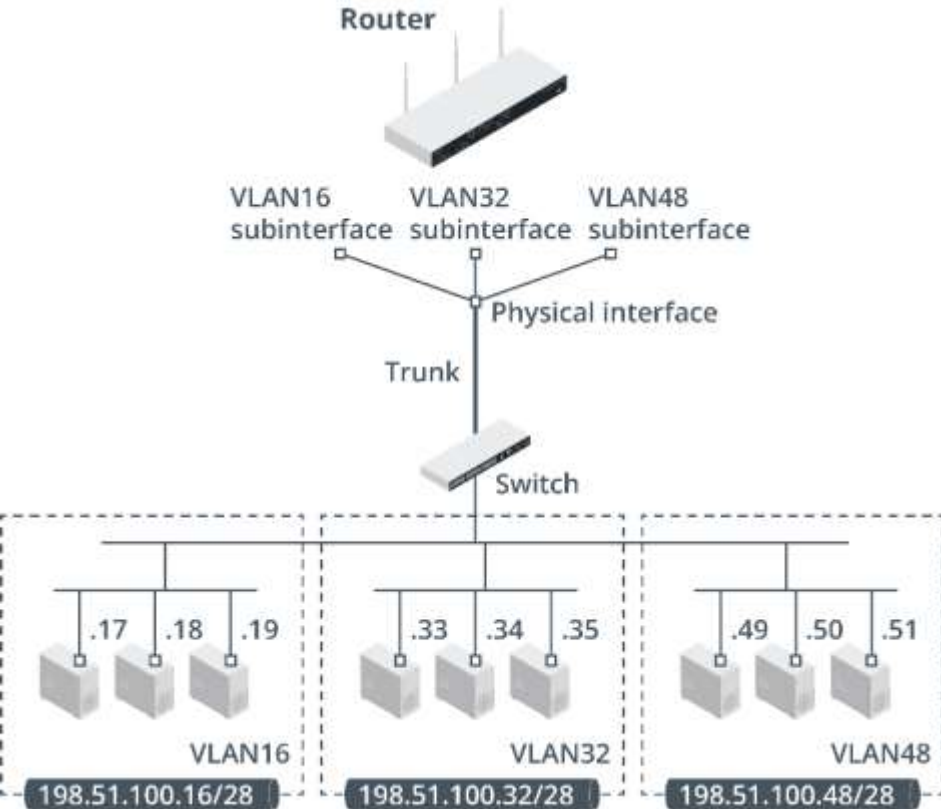


VLSM Design

Office/Subnet	Required Number of IP Addresses	Mask Bits	Actual Number of IP Addresses	Prefix Addresses
Main Office 1 (Router A)	80	7	126	/25
Main Office 2 (Router A)	30	5	30	/27
Main Office 3 (Router A)	8	4	14	/28
Branch Office (Router B)	12	4	14	/28
Branch Office (Router C)	12	4	14	/28
Router A - Router B	2	2	2	/30
Router A - Router C	2	2	2	/30
Router B - Router C	2	2	2	/30



Internal Routers



- Implement subnets and internal borders/areas
- Subinterfaces
 - Split single physical connection to per-VLAN subinterfaces
- Layer 3 switches
 - Hardware optimized to forward between VLANs

tracert and traceroute

- traceroute
 - UDP probes to identify each hop in a path
 - Increments TTL with each iteration
 - Outputs number of hops, the IP address of the ingress interface of the router or host, and time taken in milliseconds (ms)
- tracert
 - Windows
 - Uses ICMP

```
PS C:\Windows\system32> tracert 203.0.113.33

Tracing route to 203.0.113.33 over a maximum of 30 hops

  0  <1 ms    <1 ms    <1 ms   10.1.24.254
  1  <1 ms    <1 ms    <1 ms   10.1.128.253
  2   1 ms     *         1 ms   198.51.100.30
  3   1 ms     1 ms     1 ms   198.51.100.253
  4   2 ms     2 ms     1 ms   203.0.113.33

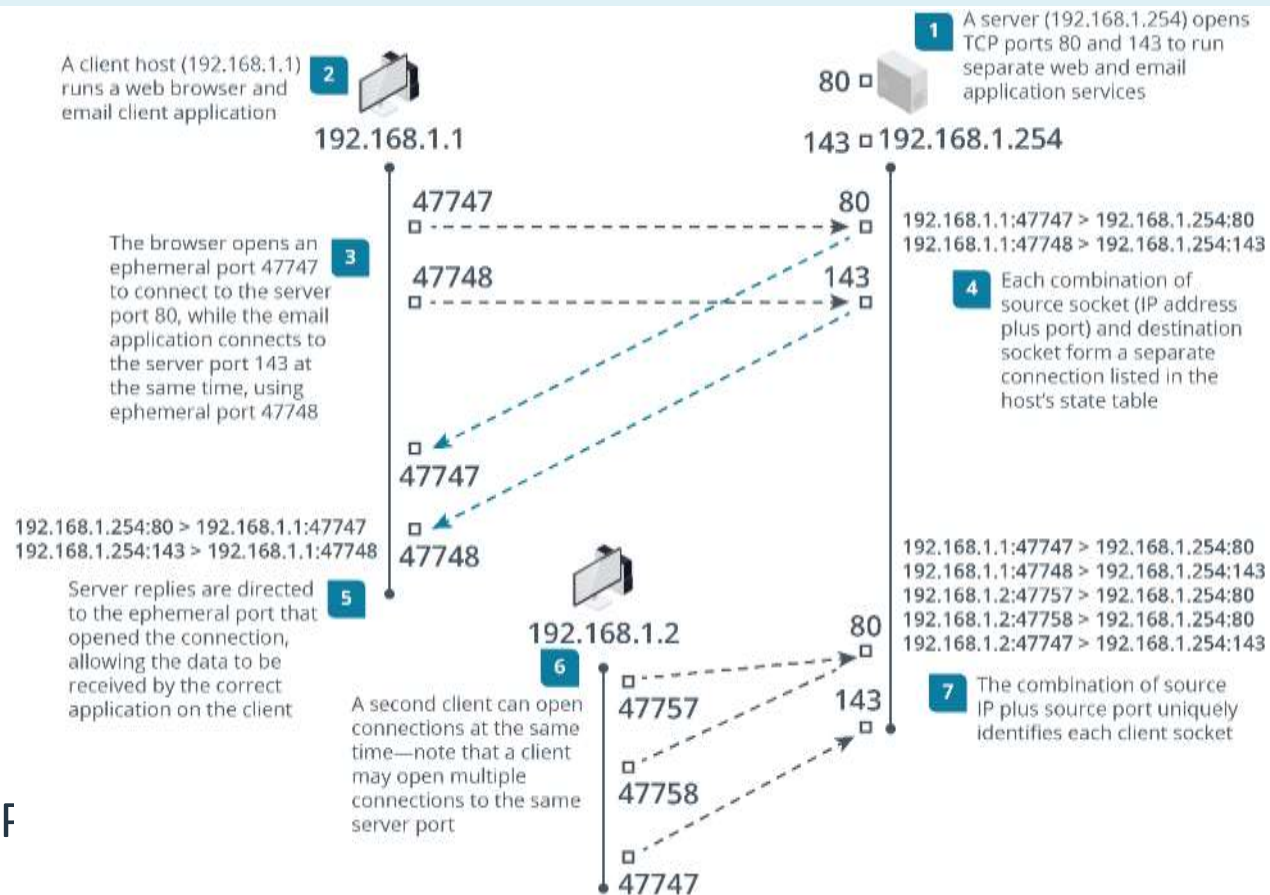
Trace complete.
```

Missing Route Issues

- Use ping and traceroute/tracert to identify where network path fails
- Check routing table
 - Missing static route
 - Dynamic protocol failure
- Device configuration review

Transport Layer Ports and Connections

- Identify individual applications as port numbers
- Socket
 - Source IP plus port bound to software process
- Connection
 - Client IP and port connected to server IP and port



Transmission Control Protocol

- Connection-oriented, guaranteed delivery
- Segments with header fields to track sequence and acknowledgements

TCP Handshake and Teardown

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\administrator>netstat -ano

Active Connections

 Proto Local Address           Foreign Address         State                   PID
----  -
TCP    0.0.0.0:135              0.0.0.0:0               LISTENING               652
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING                4
TCP    0.0.0.0:5985             0.0.0.0:0               LISTENING                4
TCP    0.0.0.0:47001            0.0.0.0:0               LISTENING                4
TCP    0.0.0.0:49664            0.0.0.0:0               LISTENING               428
TCP    0.0.0.0:49665            0.0.0.0:0               LISTENING               912
TCP    0.0.0.0:49666            0.0.0.0:0               LISTENING               864
TCP    0.0.0.0:49669            0.0.0.0:0               LISTENING              1996
TCP    0.0.0.0:49670            0.0.0.0:0               LISTENING               524
TCP    0.0.0.0:49703            0.0.0.0:0               LISTENING               516
TCP    0.0.0.0:49706            0.0.0.0:0               LISTENING               524
TCP    10.1.0.100:139           0.0.0.0:0               LISTENING                4
TCP    10.1.0.100:49764         10.1.0.192:3000         ESTABLISHED             4280
TCP    [::]:135                 [::]:0                  LISTENING               652
TCP    [::]:445                 [::]:0                  LISTENING                4
TCP    [::]:5985                [::]:0                  LISTENING                4
TCP    [::]:47001               [::]:0                  LISTENING                4
```

- Three-way handshake
 - Client SYN
 - Server SYN/ACK
 - Client ACK

User Datagram Protocol

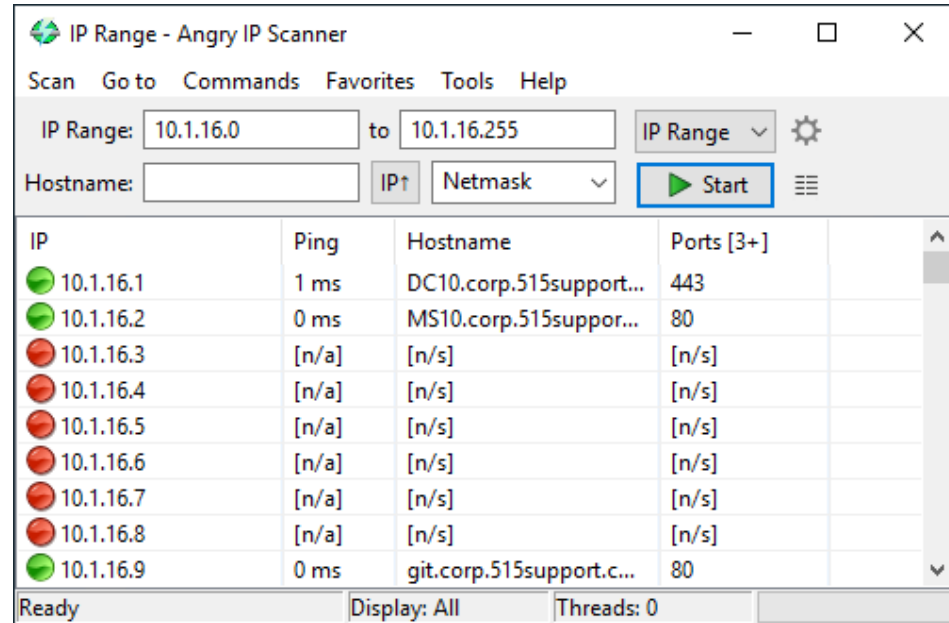
- Connectionless, non-guaranteed communication
- Fewer header fields required
- Used by protocols that can tolerate lost or out-of-order packets

Common TCP and UDP Ports

TCP/UDP/53 DNS	UDP/123 NTP	UDP/67 DHCP-Server	UDP/68 DHCP-Client	UDP/546 DHCPv6- Client	UDP/547 DHCPv6- Server	TCP/80 HTTPS
TCP/25 SMTP	TCP/587 SMTPS	TCP/110 POP	TCP/995 POP3S	TCP/143 IMAP	TCP/993 IMAPS	TCP/443 HTTPS
UDP/5004 RTP	UDP/5005 RTCP	TCP/UDP/5060 SIP	TCP/UDP/5061 SIPS	TCP/1433 MS-SQL	TCP/1521 SQL*net	TCP/3306 MySQL
TCP/20 FTP-Data	TCP/21 FTP-Control	TCP/22 SSH/SFTP	TCP/23 Telnet	UDP/69 TFTP	TCP/3389 RDP	
UDP/514 Syslog	UDP/161 SNMP	UDP/162 SNMP-Trap	TCP/UDP/389 LDAP	TCP/636 LDAPS		TCP/445 SMB over TCP/IP

IP Scanners

- Perform host and topology discovery to maximize network visibility
 - Standalone tools
 - IP Address Management (IPAM)
- Determining “up” status
 - ping, arp, traceroute
 - Simple Network Management Protocol (SNMP)
 - Query DHCP/DNS



The screenshot shows the 'IP Range - Angry IP Scanner' application window. The interface includes a menu bar with 'Scan', 'Go to', 'Commands', 'Favorites', 'Tools', and 'Help'. Below the menu, there are input fields for 'IP Range' (10.1.16.0 to 10.1.16.255) and 'Hostname'. A 'Start' button is highlighted with a blue box. The main area displays a table of scan results with columns for IP, Ping, Hostname, and Ports. The status bar at the bottom shows 'Ready', 'Display: All', and 'Threads: 0'.

IP	Ping	Hostname	Ports [3+]
10.1.16.1	1 ms	DC10.corp.515support...	443
10.1.16.2	0 ms	MS10.corp.515support...	80
10.1.16.3	[n/a]	[n/s]	[n/s]
10.1.16.4	[n/a]	[n/s]	[n/s]
10.1.16.5	[n/a]	[n/s]	[n/s]
10.1.16.6	[n/a]	[n/s]	[n/s]
10.1.16.7	[n/a]	[n/s]	[n/s]
10.1.16.8	[n/a]	[n/s]	[n/s]
10.1.16.9	0 ms	git.corp.515support.c...	80

Nmap

Zenmap

Scan Tools Profile Help

Target: 10.1.16.0/24 Profile: Scan Cancel

Command: nmap -sn 10.1.16.0/24

Hosts Services

OS Host

- DC10.corp.515supp
- MS10.corp.515supp
- git.corp.515support
- 10.1.16.254

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sn 10.1.16.0/24 Details

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-04 02:45 Pacific Daylight Time
Nmap scan report for DC10.corp.515support.com (10.1.16.1)
Host is up (0.016s latency).
Nmap scan report for MS10.corp.515support.com (10.1.16.2)
Host is up (0.016s latency).
Nmap scan report for git.corp.515support.com (10.1.16.9)
Host is up (0.014s latency).
Nmap scan report for 10.1.16.254
Host is up (0.00s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 31.82 seconds
```

netstat

- Report local port status

- TCP versus UDP
- Local IP and port
- Remote IP and port
- State (Listening, Established, ...)

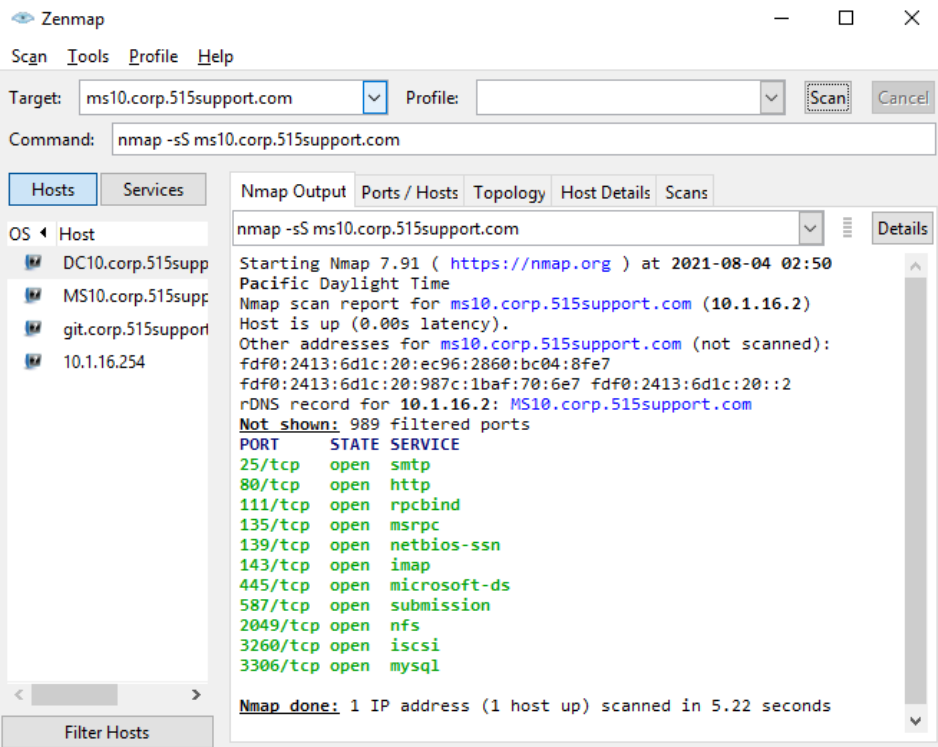
- Options

- Skip name resolution, show process, report statistics, ...
- Windows versus Linux syntax differences
- iproute2 ss and nstat commands replace netstat

```
lamp@lamp:~$ netstat -tue
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN
tcp    0      0 localhost:mysql        0.0.0.0:*               LISTEN
tcp    0      0 localhost:domain      0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:ssh           0.0.0.0:*               LISTEN
tcp    0      0 localhost:33060        0.0.0.0:*               LISTEN
tcp    0      1 172.16.0.201:52492     172.16.0.254:domain    SYN_SENT
tcp6   0      0 [::]:http             [::]:*                  LISTEN
tcp6   0      0 [::]:ssh               [::]:*                  LISTEN
udp    0      0 172.16.0.201:43367    172.16.0.254:domain    ESTABLISHED
udp    0      0 172.16.0.201:42410    172.16.0.254:domain    ESTABLISHED
udp    0      0 172.16.0.201:47084    172.16.0.254:domain    ESTABLISHED
udp    0      0 localhost:domain      0.0.0.0:*               ESTABLISHED
udp    0      0 172.16.0.201:bootpc   0.0.0.0:*               ESTABLISHED
```

```
lamp@lamp:~$ netstat -i
Kernel Interface table
Iface:  MTU  RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0    1500  4069   0     0     0    8134   0     0     0   0 BMRU
lo      65536  5322   0     0     0    5322   0     0     0   0 LRU
```

Remote Port Scanners



The screenshot shows the Zenmap interface with the following details:

- Target:** ms10.corp.515support.com
- Command:** nmap -sS ms10.corp.515support.com
- Hosts List:**
 - DC10.corp.515supp
 - MS10.corp.515supp
 - git.corp.515support
 - 10.1.16.254
- Nmap Output:**

```
nmap -sS ms10.corp.515support.com

Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-04 02:50
Pacific Daylight Time
Nmap scan report for ms10.corp.515support.com (10.1.16.2)
Host is up (0.00s latency).
Other addresses for ms10.corp.515support.com (not scanned):
fdF0:2413:6d1c:20:ec96:2860:bc04:8fe7
fdF0:2413:6d1c:20:987c:1baf:70:6e7 fdF0:2413:6d1c:20::2
rDNS record for 10.1.16.2: MS10.corp.515support.com
Not shown: 989 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
587/tcp   open  submission
2049/tcp  open  nfs
3260/tcp  open  iscsi
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds
```

- Report port status from a remote host
- Scan types
 - Half-open, full connect, UDP, port range, ...
- Host and service fingerprinting

Protocol Analyzers

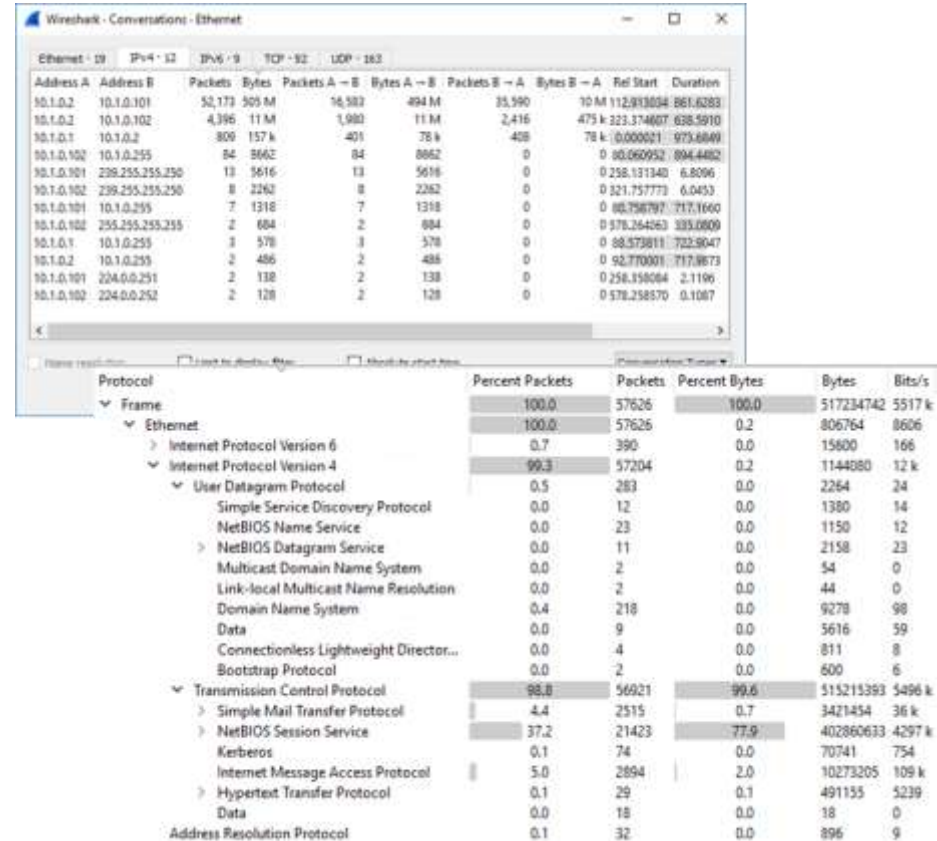
- Decode frames captured by sniffer

- Live capture or saved capture file (pcap)
- Parse header fields to reveal packet metadata

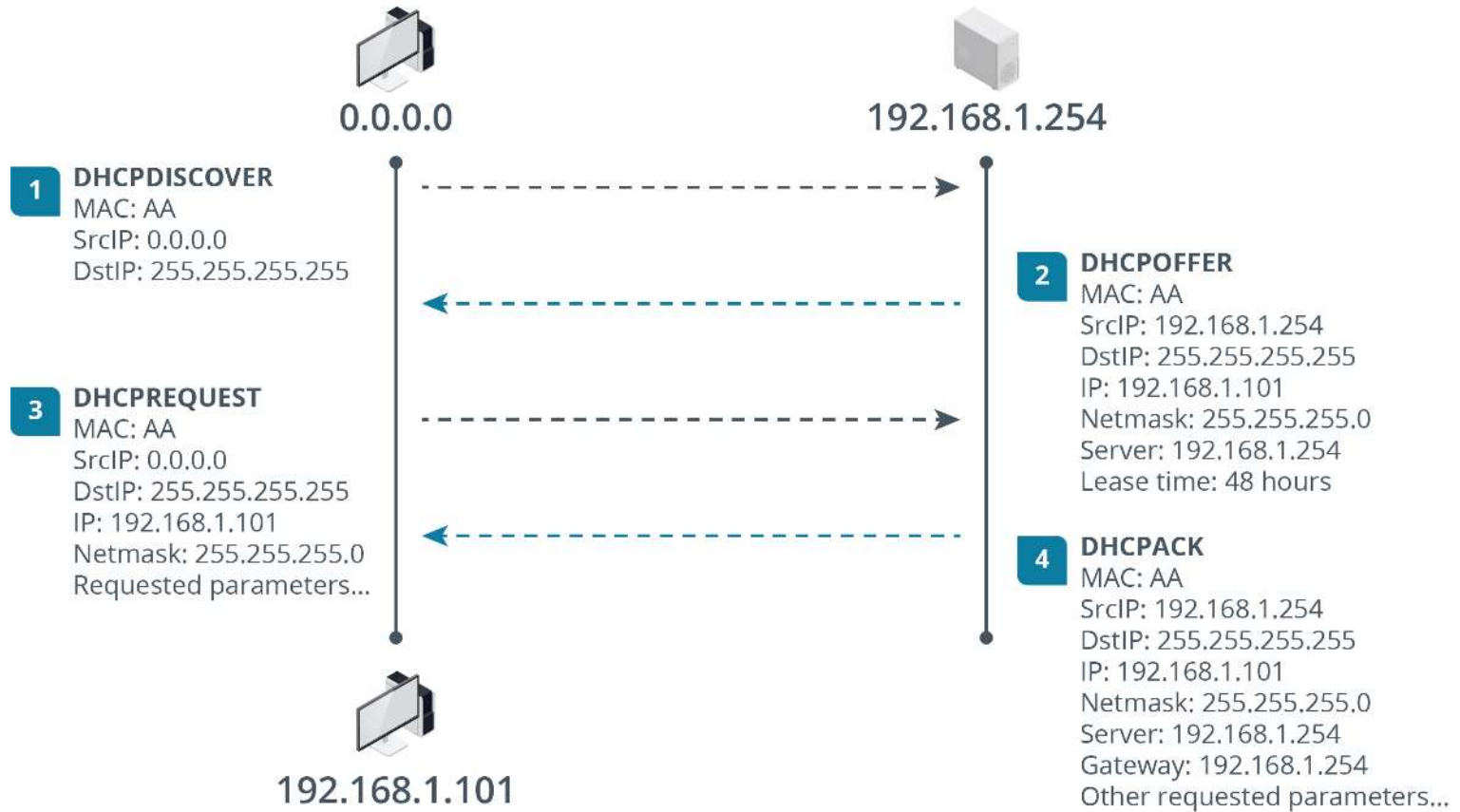
- Reconstruct TCP streams

- Analyze traffic statistics

- Per-host utilization
- Per-protocol utilization



Dynamic Host Configuration Protocol



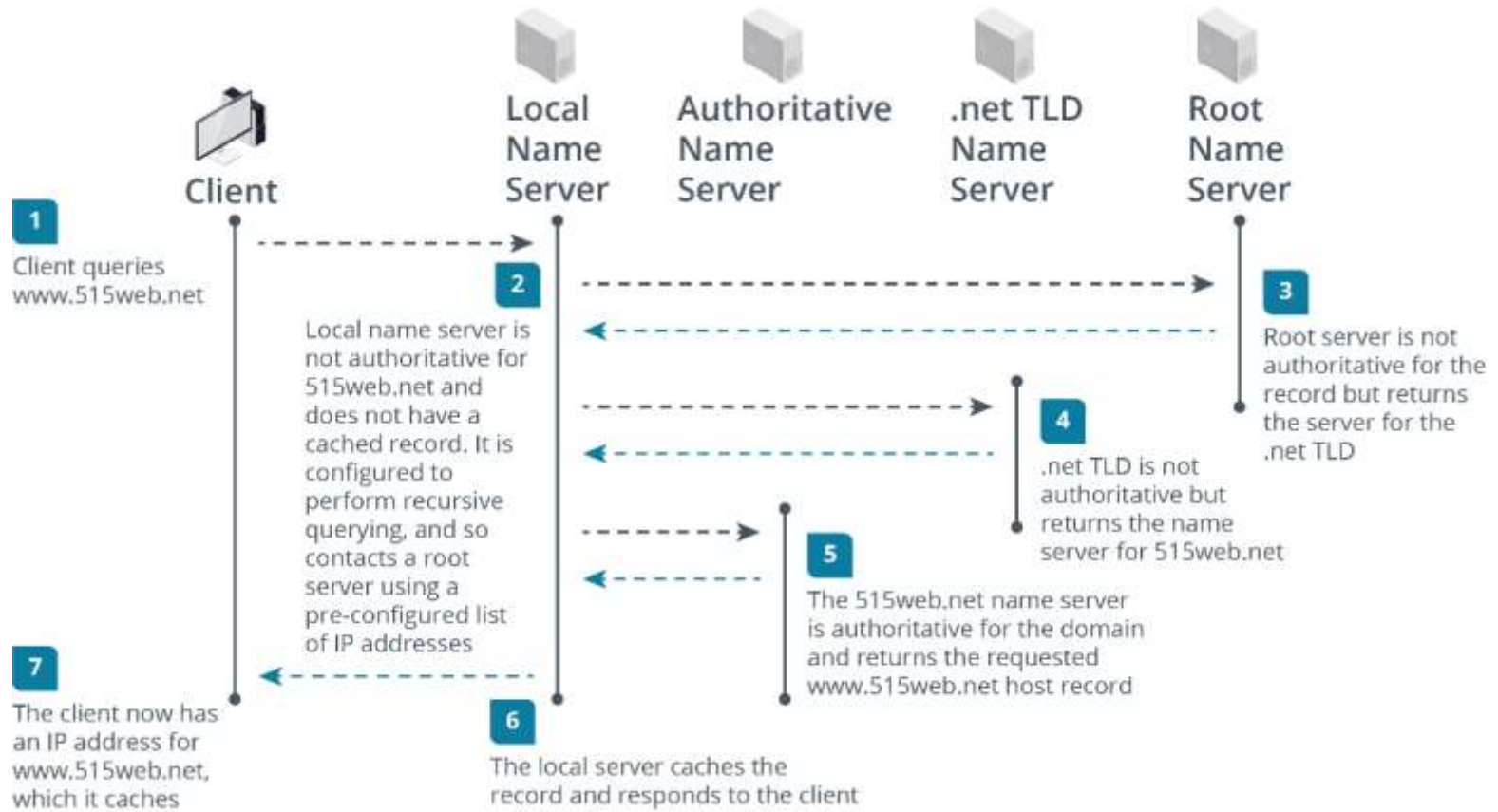
DHCP Reservations and Exclusions

- Static assignments and exclusions
 - Use IP addresses outside address pool
 - Exclude specific IP addresses from pool range
- MAC/IP reservation
 - Always allocate a device the same pre-selected IP
- Automatic allocation
 - Lease any IP address from the pool to the same client persistently

Host Names and Fully Qualified Domain Names

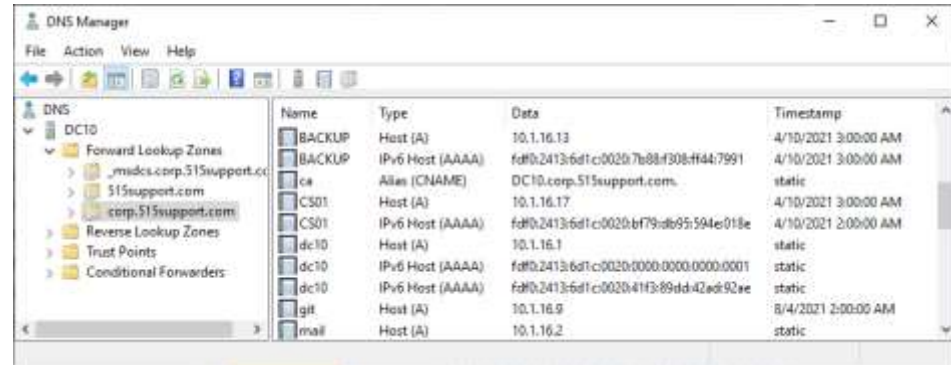
- Fully Qualified Domain Name (FQDN)
 - Host name + domain suffix
- Domain suffix
 - Domain name + Top Level Domain (TLD)
 - Subdomains
- Naming rules
 - Host name must be unique within domain
 - Labels separated by periods
 - Max length of 253 characters overall and 63 characters per label (excluding periods)

Name Resolution Using DNS



Host Address and Canonical Name Records

- IPv4 Host (A)
 - Host record to resolve a name to an IPv4 address
- IPv6 Host (AAAA)
 - Host record to resolve a name to an IPv6 address
- Canonical Name (CNAME)
 - Alternative name for a particular A or AAAA record



The screenshot shows the Windows DNS Manager interface. The left pane displays the hierarchy: DNS > DC10 > Forward Lookup Zones > corp.515support.com. The right pane shows a list of records with columns for Name, Type, Data, and Timestamp.

Name	Type	Data	Timestamp
BACKUP	Host (A)	10.1.16.13	4/10/2021 3:00:00 AM
BACKUP	IPv6 Host (AAAA)	fd8b:2413:6d1c:0020:7b88:f308:ff44:7991	4/10/2021 3:00:00 AM
ca	Alias (CNAME)	DC10.corp.515support.com.	static
CS01	Host (A)	10.1.16.17	4/10/2021 3:00:00 AM
CS01	IPv6 Host (AAAA)	fd8b:2413:6d1c:0020:bf79:db95:594e:018e	4/10/2021 2:00:00 AM
dc10	Host (A)	10.1.16.1	static
dc10	IPv6 Host (AAAA)	fd8b:2413:6d1c:0020:0000:0000:0000:0001	static
dc10	IPv6 Host (AAAA)	fd8b:2413:6d1c:0020:41f3:89dd:42ed:92ae	static
git	Host (A)	10.1.16.9	8/4/2021 2:00:00 AM
mail	Host (A)	10.1.16.2	static

nslookup

- Query a name server for resource records
- nslookup –Option Host Server
- Interactive mode
- PowerShell cmdlets

```
C:\Users\Admin>nslookup -type=mx comptia.org 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
comptia.org      MX preference = 10, mail exchanger = comptia-org.mail.protection.outlook.com

C:\Users\Admin>nslookup -type=ns comptia.org 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
comptia.org      nameserver = ns2.comptia.org
comptia.org      nameserver = ns1.comptia.org

C:\Users\Admin>nslookup -type=mx comptia.org ns1.comptia.org
Server: UnKnown
Address: 209.117.62.56

comptia.org      MX preference = 10, mail exchanger = comptia-org.mail.protection.outlook.com

C:\Users\Admin>
```

```
toor@LX200:~$ dig +nocmd +noedns +noquestion 515support.com MX
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12449
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
515support.com.      6968      IN        MX        10 mail.515support.com.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Aug 04 10:08:20 BST 2021
;; MSG SIZE rcvd: 53

toor@LX200:~$ dig +nocmd +noedns +noquestion mail.515support.com
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57840
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
mail.515support.com. 7029      IN        A         198.51.100.29

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Aug 04 10:08:32 BST 2021
;; MSG SIZE rcvd: 53
```

- Domain Information Groper (dig)
- Shipped with BIND DNS server software
 - dig host
 - dig @ns1.isp.example host
 - dig @ns1.isp.example host all
 - dig @ns1.isp.example host MX
- Output parameters
 - +nocomments or +nostats