Subnetting Quick Reference Guide

For Ethical Hackers

IP Address Types

IPv4 vs IPv6

Type	Format	Example	Address Space
IPv4	32-bit (4 octets)	192.168.1.1	~4.3 billion
IPv6	128-bit (8 groups)	2001:0db8:85a3::7334	Virtually unlimited

Private IP Ranges

Class	Range	Default Mask	CIDR
Class A	10.0.0.0 - 10.255.255.255	255.0.0.0	/8
Class B	172.16.0.0 - 172.31.255.255	255.255.0.0	/16
Class C	192.168.0.0 - 192.168.255.255	255.255.255.0	/24

CIDR Notation Chart

CIDR	Subnet Mask	Hosts per Subnet	Subnets Available
/8	255.0.0.0	16,777,214	1
/16	255.255.0.0	65,534	256
/24	255.255.255.0	254	65,536
/25	255.255.255.128	126	131,072
/26	255.255.255.192	62	262,144
/27	255.255.255.224	30	524,288
/28	255.255.255.240	14	1,048,576
/29	255.255.255.248	6	2,097,152
/30	255.255.255.252	2	4,194,304

Quick Calculations

Host Calculation Formula

- **Hosts per subnet** = 2^(32-CIDR) - 2
- **Number of subnets** = 2^(CIDR-original_mask)

Common Subnet Sizes

Need	CIDR	Hosts	Use Case
2 hosts	/30	2	Point-to-point links
6 hosts	/29	6	Small office networks
14 hosts	/28	14	Department networks
30 hosts	/27	30	Branch offices
62 hosts	/26	62	Medium networks
126 hosts	/25	126	Large departments
254 hosts	/24	254	Standard networks

Practical Examples

Example 1: Basic Subnetting

Network: 192.168.1.0/24 → Split into 2 subnets

Solution:

- New CIDR: /25
- Subnet 1: 192.168.1.0/25 (192.168.1.1 - 192.168.1.126)
- Subnet 2: 192.168.1.128/25 (192.168.1.129 - 192.168.1.254)

Example 2: Variable Length Subnetting

Network: 192.168.1.0/24 **Requirements:** 50 hosts, 25 hosts, 10 hosts

Solution:

- 50 hosts = /26 (62 available): 192.168.1.0/26
- 25 hosts = /27 (30 available): 192.168.1.64/27

- 10 hosts = /28 (14 available): 192.168.1.96/28

Essential Commands

Network Discovery

```bash
# Check your IP configuration
ifconfig            # Linux/Mac
ipconfig            # Windows

# Calculate subnet details
ipcalc 192.168.1.0/24    # Shows network info

# Scan network for active hosts
nmap -sn 192.168.1.0/24   # Ping scan
nmap -sn 10.0.0.0/8       # Scan large network
```

Binary Conversion Helper

Decimal	Binary	CIDR Bits
255	11111111	8 bits
254	11111110	7 bits
252	11111100	6 bits
248	11111000	5 bits
240	11110000	4 bits
224	11100000	3 bits
192	11000000	2 bits
128	10000000	1 bit
0	00000000	0 bits

Quick Tips for Ethical Hackers

Network Reconnaissance

- **Start with /24** networks for initial scans
- **Use /16** for broader discovery in private networks
- **Check /30** subnets for point-to-point connections
- **Look for /8** networks in large enterprise environments

Security Considerations

- **Smaller subnets** = Better traffic isolation
- **Larger subnets** = More broadcast traffic
- **/30 subnets** = Ideal for secure connections
- **Document subnet ranges** for network mapping

Common Mistakes to Avoid

- Forgetting to subtract 2 for network/broadcast addresses
- Overlapping subnet ranges
- Using subnet addresses as host IPs
- Not considering growth when planning subnets

Memory Tips

Powers of 2: 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024 **CIDR Shortcut:** Each bit doubles the subnets, halves the hosts **Quick Check:** Total hosts should always be (2^host_bits) - 2