IP Addressing Quick Reference

Essential Concepts for Security+

Private vs Public IP Addresses

Private IP Ranges (MEMORIZE THESE!)

Class	Range	CIDR Notation	# of Addresses
Class A	10.0.0.0 – 10.255.255.255	10.0.0.0/8	~16 million
Class B	172.16.0.0 – 172.31.255.255	172.16.0.0/12	~1 million
Class C	192.168.0.0 – 192.168.255.255	192.168.0.0/16	~65,000

Key Facts:

- ✅ Used for internal networks (home, office)
- ✅ NOT routable on the internet
- ✅ Can be reused by different organizations
- ✅ More secure (not directly accessible from internet)

Most Common: 192.168.x.x (home networks)

Public IP Addresses

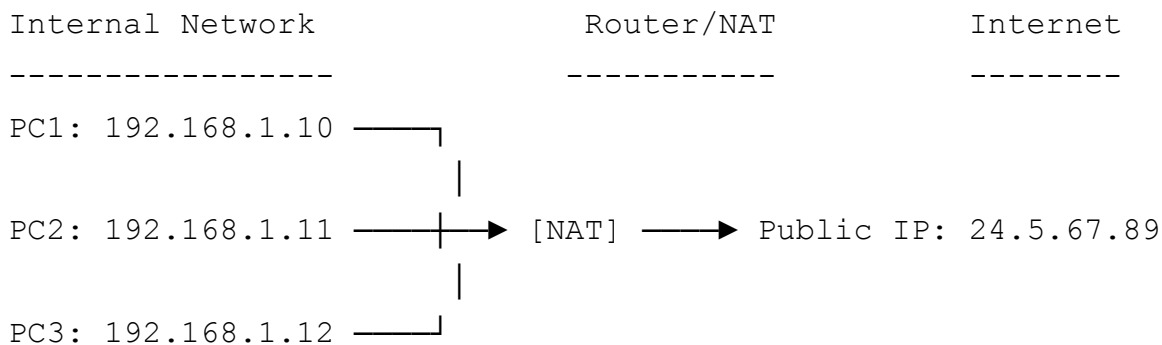**Examples:** 8.8.8.8, 142.250.80.46, 104.16.132.229

Key Facts:

- ✅ Unique worldwide
- ✅ Routable on the internet
- ✅ Assigned by ISPs
- ⚠️ Directly accessible from anywhere

NAT (Network Address Translation)

What It Does

Translates private IP addresses to public IP addresses (and vice versa)

Visual Diagram

```
Internal Network                  Router/NAT         Internet
-----------------                 -----------        --------
PC1: 192.168.1.10 ———┐
                     |
PC2: 192.168.1.11 ———┼——→ [NAT] ——→ Public IP: 24.5.67.89
                     |
PC3: 192.168.1.12 ———┘
```

Key Points

- All internal devices share ONE public IP
- NAT keeps a translation table (which internal IP goes with which connection)
- Provides some security through obscurity
- **NOT a firewall** - but offers security benefits

Security Benefits

- ✅ Hides internal network structure
- ✅ Attackers can't directly target internal IPs
- ✅ Conserves public IP addresses
- ⚠️ Does NOT inspect or filter traffic (that's a firewall's job)

Subnet Masks & CIDR Notation

Common Subnet Masks

CIDR	Subnet Mask	# of Usable IPs	Common Name
/8	255.0.0.0	~16 million	Class A
/16	255.255.0.0	~65,000	Class B
/24	255.255.255.0	254	Class C
/30	255.255.255.252	2	Point-to-point links

What It Means

- **/24** means the first 24 bits are the network portion
- **192.168.1.0/24** = all IPs from 192.168.1.0 to 192.168.1.255
- The first and last number (.0 to .255) are not available for hosts
    - .0 is typically for the network itself
    - .255 is typically for broadcast

Example

```
IP Address:     192.168.1.100
Subnet Mask:    255.255.255.0  (or /24)
Network:        192.168.1.0
```

- Network portion: 192.168.1
- Host portion: .100
- All devices with 192.168.1.x are on the same network

IPv4 vs IPv6

IPv4

Format: 192.168.1.1 (four octets, 0-255 each)

- **Size:** 32 bits
- **Total addresses:** ~4.3 billion
- **Problem:** Running out of addresses!
- **Example:** 192.168.1.100

IPv6

Format: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

- **Size:** 128 bits
- **Total addresses:** 340 undecillion (basically unlimited)
- **Benefits:** Built-in IPsec, no NAT needed
- **Format:** Hexadecimal with colons

Security+ Need-to-Know

- ✅ Recognize IPv6 format (colons, longer)
- ✅ Know IPv6 offers more security features
- ⚠️ Many networks run dual-stack (both IPv4 and IPv6)
- ⚠️ IPv6 can be exploited if enabled but not monitored

Special IP Addresses

Loopback Address

127.0.0.1 (IPv4) or **::1** (IPv6)

- Points to "this computer"
- Used for testing
- Example: "ping 127.0.0.1" tests your own network card

APIPA (Automatic Private IP Addressing)

169.254.x.x

- Self-assigned when DHCP fails
- Means: "I couldn't get an IP from DHCP"
- Only works on local network segment

Default Gateway

- The router's IP address on your network
- Where traffic goes to reach other networks
- Example: If you're on 192.168.1.x network, gateway might be 192.168.1.1

Broadcast Address

- Last IP in a range (e.g., 192.168.1.255 for /24 network)
- Sends to ALL devices on that network
- Can be exploited (smurf attacks)

Network Segmentation for Security

Why Segment?

Break one large network into smaller networks:

- ✅ Contain breaches (malware can't spread between segments)
- ✅ Apply different security policies
- ✅ Reduce broadcast traffic
- ✅ Principle of least privilege

Example

```
VLAN 10: Sales (192.168.10.0/24)
VLAN 20: Finance (192.168.20.0/24)
VLAN 30: IT (192.168.30.0/24)
VLAN 99: Guest WiFi (192.168.99.0/24)
```

Each VLAN is isolated - traffic must go through firewall to cross

---

Quick Self-Test

1. **Is 192.168.1.100 a private or public IP?**

   (Answer: Private)

2. **Can you ping 172.16.5.10 from the internet?**

   (Answer: No, it's a private IP - not routable)

3. **What does NAT do?**

   (Answer: Translates private IPs to public IPs)

4. **What does /24 mean?**

   (Answer: 255.255.255.0 subnet mask, 254 usable IPs)

5. **What is 127.0.0.1?**

   (Answer: Loopback address - refers to your own computer)

6. **Is NAT a firewall?**

   (Answer: No, but it provides some security benefits)

7. **What's a sign DHCP failed?**

   (Answer: Device gets 169.254.x.x IP address)

Security+ Exam Tips

High Priority:

- Memorize the three private IP ranges
- Understand NAT (what it is, what it does)
- Know /24, /16, /8 CIDR notation
- Recognize IPv6 format

Medium Priority:

- Special addresses (127.0.0.1, 169.254.x.x)
- Difference between IPv4 and IPv6
- Network segmentation benefits

Remember: Security+ won't make you do complex subnetting math. You just need to recognize IP types and understand security implications!