Networking Refresher

IP Addresses

Why we use them, types, how they're designed

IPv4 format

128	64	32	16	8	4	2	1	To-tal
1	1	1	1	1	1	1	1	255
1	1	0	0	0	0	0	0	192
1	0	1	0	0	0	0	0	168

192.168.1.1 == 11000000.10101000.00000001.00000001

PRIVATE IP ADDRESS
(are not used anywhere on public internet, reserved for private LANs)

Network Class	Network Numbers	Network Mask	No. of Networks	No. of Hosts per Network
CLASS A	10.0.0.0	255.0.0.0	126	16,646,144
CLASS B	172.16.0.0 to 172.31.0.0	255.255.0.0	16,383	65,024
CLASS C	192.168.0.0 to 192.168.255.255	255.255.255.0	2,097,151	254
LOOPBACK (localhost)	127.0.0.0 to 127.0.0.7	255.255.255.0	-	-

MAC Addresses

Media Access Controller, burnt into the NIC

First 3 pairs of the MAC address are identifiers
(00:0c:29):0a:42:05

TCP, UDP and the Three-Way Handshake

TCP connection based protocol:

- FTP
- SSH
- HTTP/S

UDP connectionless protocol:

- VoIP
- DNS
- Streaming

Three-Way Handshake

SYN > SYN ACK > ACK

Common Ports and Protocols

TCP

- FTP (21)
- SSH (22)
- Telnet (23)
- SMTP (25)
- DNS (53)
- HTTP/S (80/443)
- POP3 (110)
- SMB (139 + 445)
- IMAP (143)

UDP

- DNS (53)
- DHCP (67, 68)
- TFTP (69)

• SNMP (161)

The OSI Model

Layer 7 - Application - HTTP, SMTP
Layer 6 - Presentation - WMV, JPEG, MOV
Layer 5 - Session - Session management
Layer 4 - Transport - TCP/UDP
Layer 3 - Network - IP addresses, routing
Layer 2 - Data Link - Switching, MAC addresses
Layer 1 - Physical - data cables, cat6

Subnetting

Netmask/Subnet mask/Subnet - Cheatsheet

The Cyber Mentor's Subnetting Sheet								
	Subnet x.0.0.0							
CIDR	/1	/2	/3	/4	/5	/6	/7	/8
Hosts	2,147,483,648	1,073,741,824	536,870,912	268,435,456	134,217,728	67,108,864	33,554,432	16,777,216
	Subnet 255.x.0.0							
CIDR	/9	/10	/11	/12	/13	/14	/15	/16
Hosts	8,388,608	4,194,304	2,097,152	1,048,576	524,288	262,144	131,072	65,536
	Subnet 255.255.x.0							
CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Hosts	32,768	16,384	8,192	4,096	2,048	1,024	512	256
	Subnet 255.255.255.x							
CIDR	/25	/26	/27	/28	/29	/30	/31	/32
Hosts	128	64	32	16	8	4	2	1
Subnet Mask (Replace x)	128	192	224	240	248	252	254	255

Notes:	*Hosts double each increment of a CIDR *Always subtract 2 from host total: Network ID - First Address Broadcast - Last Address

Important!

Subtract 2 from host total:

1. Network ID - First address
2. Broadcast - Last address

Examples:

IP range	Subnet	Hosts	Network ID	Broadcast
192.168.1.0/24	255.255.255.0	254	192.168.1.0	192.168.1.255
192.168.1.0/28	255.255.255.240	14	192.168.1.0	192.168.1.15
192.168.1.16/28	255.255.255.240	14	192.168.1.16	192.168.1.31
192.168.0.0/23	255.255.254.0	510	192.168.0.0	192.168.1.255
192.168.2.0/23	255.255.254.0	510	192.168.2.0	192.168.3.255
192.168.0.0/22	255.255.252.0	1022	192.168.0.0	192.168.3.255
192.168.1.0/26	255.255.255.192	62	192.168.1.0	192.168.1.63
192.168.1.0/27	255.255.255.224	30	192.168.1.0	192.168.1.31