IP/TCP Header Cheat Sheet

Each Block Represents 1 byte (8 bits) and double wide blocks count as 2 bytes etc...

Everything before the Dest. IP address is the IP header (Bold Text) and everything after is the TCP header (Italicized). Produced by Chris Davis.

4|5 IP vers.|IHL	**00** TOS	**00 28** Packet length	**eb 66** IPID	**40 00** Flags/Fragmentation	**40** TTL	**06** Encoding	**b4 ab** Checksum
oa oa oa 80 Src IP Address	**d0 6d b5 c6** Dest. IP address	*b9 50* Src Port	*00 50* Dest. Port				
6c e5 9f 79 Sequence Number	*61 d8 31 a9* Acknowledgement Number	*50* TCP/HL	*11* Flags	*75 40* Window Size			
9a d8 Checksum	*00 00* Urgent Pointer	TCP Options or Start of Payload	Payload--->				

|-----1 byte-----|----1 byte----|------------2 bytes---------|--------------------------4 bytes---------------------------|

1. IP version. The first four bits (1 hex) represents either ipv4 or ipv6. IHL is the IP header length and compose the second 4 bits (1 nibble) of block 1. An IHL of 5 would mean that the IP header length is 20 bytes (5 x 4). If the IHL is a length of 6 then the IP options field will be 4 bytes after the ip Checksum.

2. TOS stands for Type of service and has to do with prioritizing traffic. In this instance 00 means no prioritizing.

3. Packet size simply refers to the entire size of the packet so that the router know how much space in the buffer to allocate. I.e. --" 00 28" in hex would be 40 bytes.

4.IPID - Simply the identifier for the packet so the receiving end knows how to organize the data.

5. Fragmentation - This field refers to how the packets are fragmented. A value of "4"000 is Dont Fragment. "2 "Must Fragment. "8" Reserved. "0" is last frag packet.

6. TTL - Time to live. In this case, "40" in hex would be a TTL of 64.

7. Encoding - Refers to the IP encoding of this packet. In this instance, there is a value of "06" which simply means TCP. 01 is ICMP. 11 is UDP. 02 is IGMP. 09 is IGRP. 2f is GRE. 32 is ESP. 33 is AH. 39 is SKIP. 58 is EIGRP. 59 OSPF. 73 for L2TP.

8. Checksum of the IP header to validate the header hasn't been changed.

9. Source IP address

10. Destination IP address

11. Source Port

12. Destination Port

13. The TCP Sequence number used by the transport layer to order data.

14. The Acknowledgment field is used to acknowledge receipt of data.

15. The TCP/HL is the TCP header length and "50" in hex would just be "5" as we ignore the 0 in this instance. So a value of "5" means the TCP header length is 5x4=20 bytes.

16. TCP Flags Field. This has 2 hex (8 bits). Depending on the bits that are turned on, it represents either CWR,ECN-Echo, URG, ACK, PSH, RST, SYN, or FIN. This bits are aligned as follows: | C | E | U | A | P | R | S | F | In this instance, the Hex characters are "11" which would equate to 17 in decimal and would have the following bits in this order: | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | We can deduce that the ACK, FIN flags are set.

17. The TCP windows size field is used to show the number of bytes that can be transferred to the dest before an ACK should be sent.

18. The TCP header Checksum is used to validate the integrity of the TCP header field.

19. Urgent pointer field is used to identify the location of urgent data within the packet. In most cases it will be 00 00.

20. The TCP options Field represented in the graph is 4 bytes but can actually be 0-40 bytes. This field will often not exist and depends on the TCP/HL (refer to 15). Since the TCP header length was only 20, the TCP header ended after the urgent pointer and there is no TCP options in this example. This would start the payload if there was one. There is often not a TCP options field . Options are:

0 End of Options **1** No operation (pad) **2** Maximum segment size **3** Window scale **4** Selective ACK ok **8** Timestamp

IPv4 Subnetting

packetlife.net

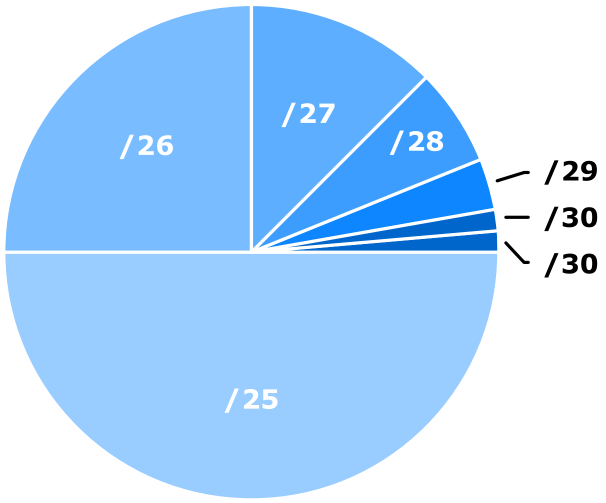
Subnets

CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1,024	0.0.3.255
/21	255.255.248.0	2,048	0.0.7.255
/20	255.255.240.0	4,096	0.0.15.255
/19	255.255.224.0	8,192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/9	255.128.0.0	8,388,608	0.127.255.255
/8	255.0.0.0	16,777,216	0.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255
/6	252.0.0.0	67,108,864	3.255.255.255
/5	248.0.0.0	134,217,728	7.255.255.255
/4	240.0.0.0	268,435,456	15.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255

Decimal to Binary

Subnet Mask		Wildcard	
255	1111 1111	**0**	0000 0000
254	1111 1110	**1**	0000 0001
252	1111 1100	**3**	0000 0011
248	1111 1000	**7**	0000 0111
240	1111 0000	**15**	0000 1111
224	1110 0000	**31**	0001 1111
192	1100 0000	**63**	0011 1111
128	1000 0000	**127**	0111 1111
0	0000 0000	**255**	1111 1111

Subnet Proportion



Classful Ranges

A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 255.255.255.255

Reserved Ranges

RFC 1918	10.0.0.0 - 10.255.255.255
Localhost	127.0.0.0 - 127.255.255.255
RFC 1918	172.16.0.0 - 172.31.255.255
RFC 1918	192.168.0.0 - 192.168.255.255

Terminology

CIDR
Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX

VLSM
Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes

by Jeremy Stretch