TCP/IP Cheat Sheet

This cheat sheet is a collection of common Internet facts and information. This document, along with a little experience with TCP/IP networking, will help with Internet Connectivity *course assignments. This is not a tutorial, nor is it an academically complete introduction to networking. It is just a cheat-sheet, exactly as suggested by the title.*

Q: What do I need to know about TCP / IP networking for the *Internet Connectivity* class?
A: Just a few things:

- concepts of IP address, network mask, subnet mask, and their allocation;
- Ethernet MAC address;
- basics of popular network protocols: IP, TCP, UDP, ICMP, FTP;
- basics of popular networking tools such as FTP, telnet, ping, nslookup, tracert.

Q: What is an Ethernet MAC address?
A: The Media Access Control (MAC) address, which is also called the ethernet hardware address, is a 48-bit number that is a unique characteristic of a physical network interface (Ethernet NIC). Hosts and routers cache a table of IP-to-Physical address translation used by address translation protocol (ARP). You can display the current IP-to-MAC table on your PC by entering command

```
arp –a
```

in the DOS session box in Windows NT or Win 95/98.

Q: What is an IP address?
A: An Internet address or IP address is a digital code that identifies a computer (host) location on the Internet. The current standard is IP address version 4 (IPv4), which is a 32 bit long number represented in the form of four octets (eight-bit or one-byte fields) separated by dots. Each octet is displayed as a decimal number in the range of 0-255. Examples of valid IP addresses:

```
205.245.172.72
10.1.0.22
```

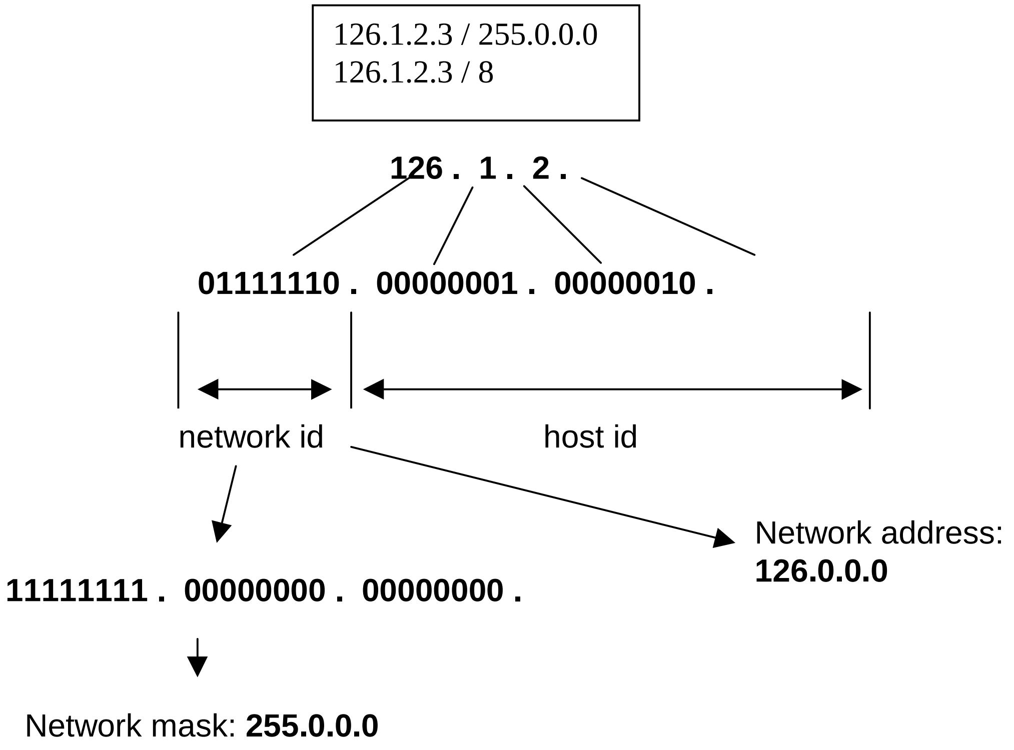
An IP address on the Internet or in a local network must be unique so network packets destined for the host with that address can find it. However, this uniqueness is not created at the hardware level, as in LONWORKS networks with the Neuron ID, but is rather like a unique domain/subnet/node ID allocation in LonWorks networks. This means that it is possible to create a bad network with several PCs having the same IP address. This happens sometimes, introducing a faulty network that is notoriously difficult to troubleshoot.

Q: For what are IP addresses used?
A: IP addresses provide source/destination addresses for packets sent on a network.

Q: What is a network mask?
A: A network mask allows one to subdivide the flat 32-bit address space into chunks of addresses, so that each chunk can be allocated to one of a large number of computers. The concept is simple. Take the 32-bit IP address written as a sequence of bits:

xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

and announce that the first n bits will be used for the network address, and the last (32-n) bits will be used for the host identification in that network. Then create the network mask as a 32-bit number with 1's in the first n bits, and 0's in the last (32-n) bits. Finally, convert this mask in the familiar notation of four octets separated by dots, so it looks like an IP address.
Example:
Take IP address, 126.1.2.3, and apply to it a network mask corresponding to n=8. As the figure below demonstrates, the first octet is used as a network ID, and the last three octets as the host ID, with network mask 255.0.0.0.



Q: Are all addresses in the network equally valid?
A: Yes, with the exception of host ID made of all 0's and all 1's. All 0's are reserved for the network address, and all 1's are reserved for the network broadcast address.

Q: Can I arbitrarily assign a network mask to my IP address?
A: Usually the answer is 'no'. To prevent chaos with network mask allocation, it was agreed upon using the so-named "natural mask" picked from one of the four "address classes" A through D.

Class A includes all addresses with the first bit equal to '0'. Class A networks have network mask of 255.0.0.0, and the first octet of the IP address in the range 1-127. Each Class A network has 16777216 IP addresses.

Class B includes all addresses with the first two bits equal to '10'. Class B networks have network mask of 255.255.0.0, and the first octet of the IP address in the range 128-191. Each B class network has 65536 IP addresses.

Class C includes all addresses with the first three bits equal to '110'. Class C networks have network mask of 255.255.255.0, and the first octet of the IP address in the range 192-223. Each C class network has 256 IP addresses.

Class D is a special class for multicast addresses. For this class it is enough that you are aware of its existence, since we are using IP addresses from the Class A through C only.

Don't forget, in each network the number of useable IP addresses is two less that the total number of addresses, since one IP address is reserved for broadcast, and one for the network itself. For example, in the C class network you actually will have only 254 useable IP addresses. Subnetting will further reduce this amount, see Q&A on subnetting below.

Q: What is "address class", or "network class"?
A: See the Q&A about network mask allocation above.

Q: What is a subnet mask?
A: A subnet mask is used it to subdivide IP addresses in a class A, B, or C network to smaller chunks to accommodate the needs of departments, branches etc. The concept is the same as the network mask. Take the 32-bit IP address written as a sequence of bits:

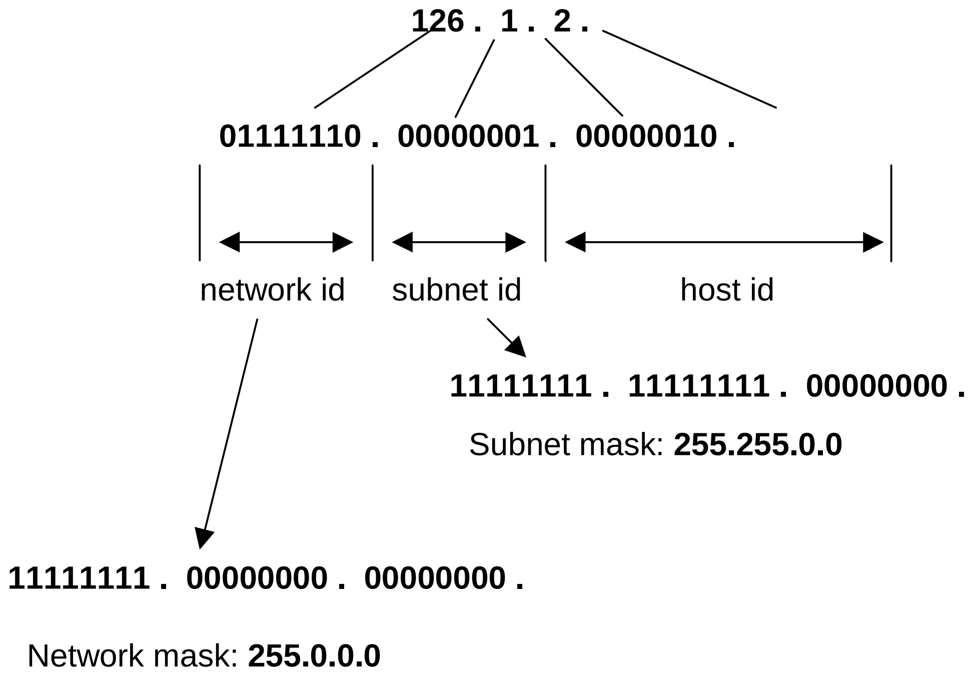
```
xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
```

leave the first n digits alone as specified by the network mask, and announce that the next m bits (or the first m bits of the host ID part) will be used for the subnet address, while the last (32-m-n) bits will be used for the host identification in that network. The subnet mask will be a 32-bit number with (n+m) 1's and (32-m-n) 0's presented in the form of four octets separated by dots, so it looks like an IP address.

Example:
Take the same IP address/network mask as above (126.1.2.3 / 255.0.0.0), and apply an 8-bit subnet mask (255.255.0.0). Now you have a network #126, subnet #1, and host ID #2.3.

Note that there is no natural subnet mask, similar to the natural network mask (IP address class based on the first 4 bits), subnetting is a purely internal issue of a particular network and is not governed by any universally accepted convention. You cannot guess a subnet mask based on the IP address, as you can easily guess the network mask. A subnet mask is something that your IT or IS department will provide to you.

IP address/network mask: 126.1.2.3 / 255.0.0.0 or 126.1.2.3 / 8
IP address/subnet mask: 126.1.2.3 / 255.255.0.0 or 126.1.2.3 / 16



Q: How large is a subnet with a particular mask?
A: Determine how many bits are left for the host ID in the 32-bit address or how many bits are 1's in the subnet mask. Here is a simple algorithm:

- Convert each octet of the subnet mask into the number of '1' bits using this table:

Octet value	Bits
128	1
192	2
224	3
240	4

248	5
252	6
254	7
255	1

- Add all bits (some number m).
- Subtract that number from 32 (n = 32-m).
- Convert the result using the formula:
  N = 2^n

Don’t forget that the number of usable IP addresses is always less by two.

Example:
How many IP addresses are there in a subnet a mask 255.255.255.224? First convert it to bits:

Bits: 8 + 8 + 8 + 3 = 27
Numbers of bits left for host IDs: 32-27 = 5.
Number of hosts = 2^5 = 32

Q: Why is a network mask useful?
A: You may argue that a network mask is just a way to organize IP address allocation. It also has a profound influence on the routing efficiency, since in most cases it also brings some order and structure in the way packets are routed, making routing protocols simpler. The same applies to subnets on your intranets.

Q: How are IP addresses allocated? Can I assign one of my own?
A: IP addresses are allocated for organizations by InterNIC, the Internet Network Information Center. An organization may further re-assign chunks of an address to its customers by means of subnetting. Customers’ IS departments will further subnet those for different departments.

Q: Can you show me an example of IP allocation?
A: Here is a very basic example:

- Your ISP provider has a class B network allocated to it by InterNIC, 130.131.0.0. This means that they have all IP addresses in the range 130.131.0.0 through 130.131.255.255.
- The ISP provider further used an 8-bit subnet mask (255.255.255.0) and assigned your organization one subnet, or 256 IP addresses, in the range 130.131.160.0 through 130.131.160.255
- Your IS department decided to keep things simple and reserved the first 40 IP addresses for static allocation, in turn implemented a flat IP space subdivided a 2-bit subnet mask (255.255.255.192) and created four subnets for Accounting, Engineering, Sales, and Marketing departments. Each subnet has 64 IP addresses (62 usable.)

- Your IS department further subdivided each subnet, reserving the first 15 IP addresses for static allocation. A DHCP server (see definition of DHCP below) dynamically assigns the others.

Q: When is an IP addresses routable, or "real", and when is it non-routable?
A: Usually not every host on the intranet needs access to the Internet, e.g. network printers or file servers. In many cases a company will not grant all hosts direct access to Internet, and would rather have them to go through an NAT (see Q&A about NAT below.) In these cases, the hosts without direct access to Internet get special, non-routable, or not "real" IP addresses from special lots designated by InterNIC exclusively for that purpose. One of the ranges of non-routable addresses is the class B network 192.168.0.0. There are also others. A packet coming from a host with a non-routable address will not be passed to the Internet by a gateway or a router. The only way for such a host to access the Internet is if you have an NAT or a firewall box that can perform an address translation (see NAT).

Q: What is a loopback address?
A: A loopback address is a special IP address of 127.0.0.1 that allows you to run applications requiring configure TCP/IP, even if the host has no valid network interface (either no Ethernet adapter/PPP adapter, or no valid IP address and hence appearing unconfigured.) The operating system recognizes a packet destined for a loopback address as destined for the same host and turns it around. Such a packet never really shows up on the network.

Q: How can I find my IP address?
A: On Windows 95/98 you can run the utility winipcfg.exe from a DOS session. This utility has a nice GUI that displays useful information about your IP configuration, including IP address and network mask, DNS servers, if DHCP is on or off, default gateway, etc.
On Windows NT / 2000 you run the utility ipconfig.exe, again from a DOS session. This utility does not have a nice GUI, but it still has the information that you seek.

Q: What is a DHCP server?
A: A DHCP (Dynamic Host Configuration Protocol) server is a special application, running on some host, that allocates dynamic and static leases per client host request, and updates its DNS server and default gateway addresses. A DHCP server implements the DHCP protocol.

Q: What is a static or dynamic IP address? What is a static or dynamic allocation of IP address?
A: If you hardcode the IP address of your PC via the Network applet in the Control Panel, this is a static IP address. If you let the operating system query the network for a DHCP server to allocate a valid IP address by setting an option to turn DHCP on in the same Network applet, this is dynamic IP allocation.

A DHCP server usually has a pool of dynamically allocated addresses, plus a list of static IP addresses, assigned to particular hosts on the network. If your host is on the list of static IPs, it will get a static lease, i.e. it will get the same address every time it requests one. However, if your host is not on that list, it will receive an IP address from the pool of dynamically allocated ones. This is a dynamic lease, i.e. the address is ‘temporarily’ leased to your host, until the lease period (typically several days) expires. Once the lease expires, you will either get the same address, or a first available one from the pool of dynamic addresses.

Please note that in order for the *i*.LON 1000 to function properly as a router, you need a static IP address or a static lease.

Q: What is DNS?
A: DNS stands for Domain Name Service. DNS resolves (translates) Internet host names expressed in a user-friendly, readable format (like www.echelon.com) to the corresponding IP address (205.229.51.8) and performs the reverse translation. There are several ways to perform name resolution. All methods use a table, or a dictionary, which stores matches, "host name" - "IP address". This information can be local to the host, stored in files “hosts” or “lmhosts”, or external, stored in a DNS server (a special host on your Intranet or somewhere on the Internet.) Note that only static IP can be resolved by means of the files hosts or lmhosts.

On Windows platform the file “hosts” is located in C:\Windows on Win95/98 box, or in %Windows%\System32\drivers\etc on Windows NT 4.0.

To test if your PC has a properly configured DNS enter a command ‘nslookup’ with a name of some available host in the DOS box. The name will be resolved to the corresponding IP address by the DNS if it is properly configured. You also must try to resolve the IP address back to the host name, failure to get a valid name will indicate a problem with reverse name resolution.

Please note that a properly configured DHCP server will also set your DNS server addresses.

Q: What is NAT?
A: NAT, or Network Address Translation prevents exposure of the IP address of an internal host to the outside world and typically swaps the IP address of an internal host to that of the machine running the NAT service. NAT is not currently compatible with LONWORKS/IP implementations.

Q: What is a gateway? What is a default gateway?
A: For clients in a TCP/IP network, a gateway is a router that connects two networks. You can usually assume:

- Packets sent to a host in the same subnet as your host will reach it without a gateway.

- If you have a specific gateway for a particular subnet/network, then packets sent to a host on that subnet will be automatically routed through that gateway.
- You have a default gateway for everything else. Packets sent to a network or subnet that doesn't have a specific gateway assigned to it will travel through the default gateway.

Q: What is a Firewall?
A: In short, a firewall is a special host with a special software and/or hardware that is used to restrict access to and from an internal network. The primary goal of a firewall is to prevent unauthorised access to a LAN from the Internet and to the Internet from the LAN. Basically, a firewall, working closely with a router program, filters all network packets to determine whether or not to forward them to their destination.

Q: What is WINS?
A: Windows Internet Name Services (WINS) manages the association of workstation names and locations with IP address without a user or administrator involved in each configuration change. WINS automatically creates a computer name-IP address mapping entry in a table, ensuring that the name is unique and not a duplicate of someone else's computer name. When a computer is moved to another geographic location, the subnet part of the IP address is likely to change. Using WINS, the new subnet information will be updated automatically in the WINS table. WINS complements the NT Server's Dynamic Host Configuration Protocol (DHCP), which negotiates an IP address for any computer (such as your workstation) when it is first defined to the network.

Q: What is IP?
A: IP (Internet Protocol) is a connectionless protocol, which means that there is no established connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. Because a message is divided into a number of packets, each packet can, if necessary, be sent via a different route across the Internet. Packets can arrive in a different order than the order they were sent. The Internet Protocol just delivers them. It is up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order.

Q: What is TCP?
A: TCP (Transmission Control Protocol) is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into packets that IP can manage and for reassembling the packets back into the complete message at the other end.

Q: What is UDP?
A: UDP (User Datagram Protocol) is a communication method that offers a limited amount of service when messages are exchanged between computers in a network that uses IP. UDP is an alternative to TCP and, together with IP, is sometimes referred to as UDP/IP. Like TCP, UDP uses IP to actually get a data unit from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets and reassembling it at the other end. Specifically, UDP does not provide sequencing of the packets when the data arrives. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order.

Q: What is ICMP?
A: ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses IP datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

Q: What is FTP? TFTP?
A: FTP (File Transfer Protocol) is a simple way to exchange files between computers on the Internet. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It is also commonly used to download programs and other files to your computer from other servers.

A typical FTP server may allow anonymous connections, but usually it allows connections based on a name and password. Authentication, i.e. user name and password, is sent to the FTP server using plain text, hence it may cause security problems (a hacker may intercept the packet with authentication, steal the user name and password, and break into the server.)

TFTP (Trivial File Transfer Protocol) is a network application that is simpler than the FTP but less capable. It is used where user authentication and directory visibility are not required. TFTP uses UDP rather than TCP.

Q: What is HTTP?
A: Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging information on the World Wide Web. Relative to the TCP/IP suite of protocols, which are the basis for information exchange on the Internet, HTTP is an application protocol.

Essential concepts of HTTP include (as its name implies) the idea that files can contain references to other files whose selection will elicit additional transfer requests. Any Web server machine contains, in addition to the HTML and other files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. Your Web browser is an HTTP client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator or URL) or clicking on a hypertext link, the browser builds an HTTP request and sends it to the Internet Protocol address indicated by the URL. The

HTTP daemon in the destination server machine receives the request and, after any necessary processing, returns the requested file.

Q: What is telnet?
A: Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. The Web, or HTTP protocol, and the FTP protocol allow you to request specific files from remote computers, but not to actually log on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific applications and data on that computer.

Q: What is ping?
A: Ping is a basic Internet program that lets you verify that a particular Internet address exists and can accept requests. Ping is a diagnostic tool to ensure that a host computer you are trying to reach is actually operating. For example, if a user cannot ping a host, then the user will be unable to FTP to send files to that host. You can also use ping with a host that is operating to see how long it takes to get a response back. Using ping, you can learn the number form of the IP address from the symbolic domain name. Loosely, ping means "to get the attention of" or "to check for the presence of" another party online. Ping operates by sending a packet to a designated address and waiting for a response.

Q: What is nslookup?
A: Name Server Lookup (nslookup) is the name of a program that lets an Internet server administrator or user enter a host name (for example, "echelon.com") and find out the corresponding IP address. It can also do reverse name lookup and find the host name for an IP address you specify. For example, if you entered "echelon.com", you would receive as a response our IP address, which happens to be “205.229.51.8”.
Or, if you entered "205.229.51.8", it would return "echelon.com". nslookup sends a domain name query packet to a designated (or defaulted) DNS server.

Q: What is tracert?
A: Tracert allows you to see if a destination host is reachable and examine the route taken to get to another host. It lists all routers on the way, with a propagation delay from one router to the next one in the chain.

Q: What does the acronym URL stand for, and how is a URL constructed?
A: The structure of a Uniform Resource Locator (URL) may be expressed as:

resource_type:additional_information

The possible resource types include `file`, `http`, `news`, `gopher`, `telnet`, `ftp`, and `wais`, among others; and each resource type relates to a specific server type. Since each server performs a unique function, each resource type requires different `additional_information`. For example `http` and `gopher` URLs will have a structure like:

resource_type://host.domain:port/pathname

The colon followed by an integer TCP port number is optional, and is used when a server is listening on a non-standard port.

Examples:
http://www.echelon.com/default.htm
http://www.redhat.com:1023/default.htm

Q: What is an IP port? What are valid ranges for the packet sender/packet receiver?
A: IP port is an ID that identifies the specific process to which a message is to be forwarded. A source IP port number is randomly chosen between 1024 – 65535. A destination IP port number is determined by the destination machine's configuration.

Q: What are the tools used by network administrators to troubleshoot a network?
A: Ping is used to determine if a host is reachable and determine channel delays. Tracert allows one to see if a host is reachable and examine the route taken to get to another host.

Q: What is a propagation delay? What is a typical propagation delay?
A: A propagation delay is the time that takes an IP packet to travel from the sender (source) host to the receiver (destination) host. The delay depends upon many factors, such as the number of routers that it needs to cross on its way, the load of the routers, change of packet size that may occur in some routers, and so on. For example, if a large IP packet needs to cross an ATM network, it will be broken into a sequence of smaller ATM packets at the ATM entry router, and then re-assembled when exiting the ATM network. Different IP packets may take different paths with different propagation delay. In a local IP network, the delay would be between 1ms and 50ms, and it is unlikely to have large variation over time.

A typical worst-case propagation delay between two hosts on the Internet is <500ms. This delay may vary over a wide range over time, since a packet travelling over Internet will traverse many routers, much more than found in a typical intranet, and the conditions of those routers vastly unpredictable.

Recommended reading

Windows NT TCP/IP Network Administration, by Craig Hunt, Robert Bruce Thompson, and Robert Denn, O’Reilly, 1998