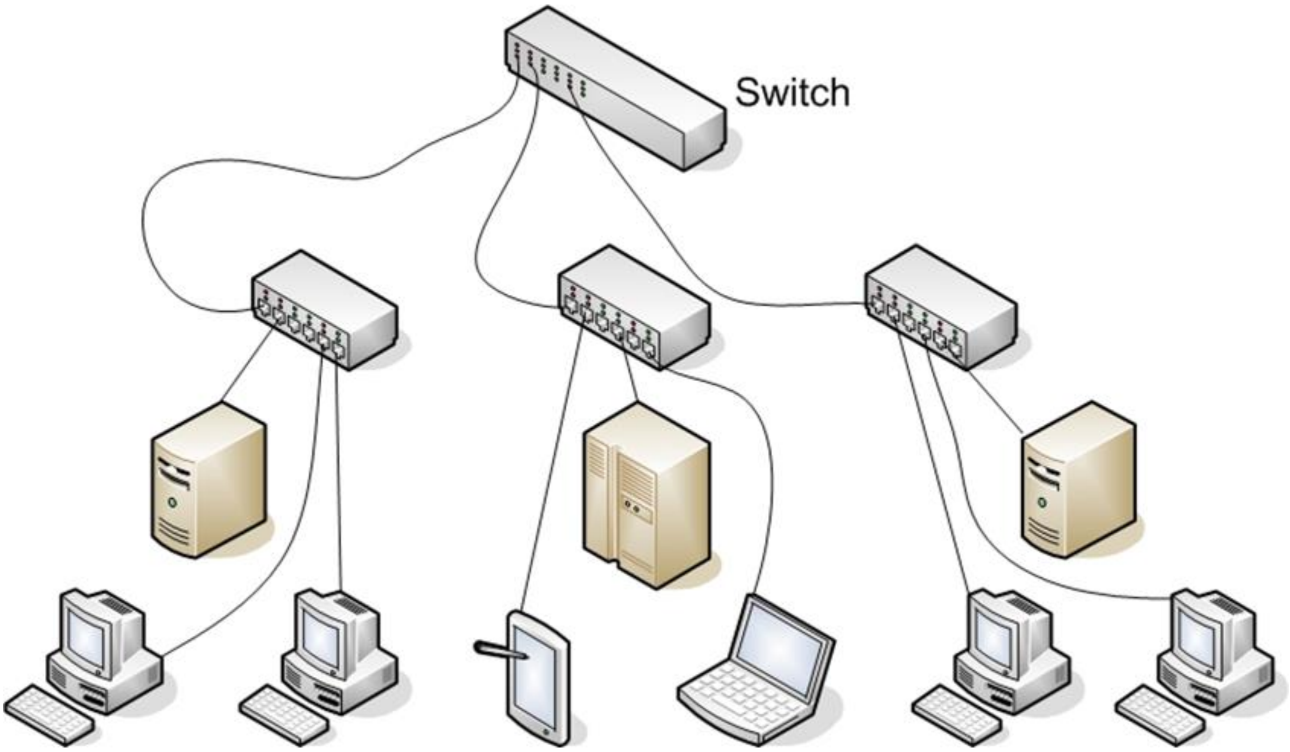
1.1 Network Basics

Before diving into how to protect a network, exploring what networks are, would probably be a good idea.

For many readers this section will be a review, but for some it might be new material. Whether this is a review for you, or new information, having a thorough understanding of basic networking before attempting to study network security is critical. Also, be aware this is just a brief introduction of basic network concepts.

A network is simply a way for machines / computers to communicate.

On a physical level, it consists of all machines that you want to connect and the devices that you use to connect them. Individual machines are connected either with a physical connection (a category 5 cable going into a network interface card, or NIC) or wirelessly. To connect multiple machines together, each machine must be connected to a hub or a switch. These hubs / switches must be connected together. In larger networks, each subnetwork is connected to the others by a router.

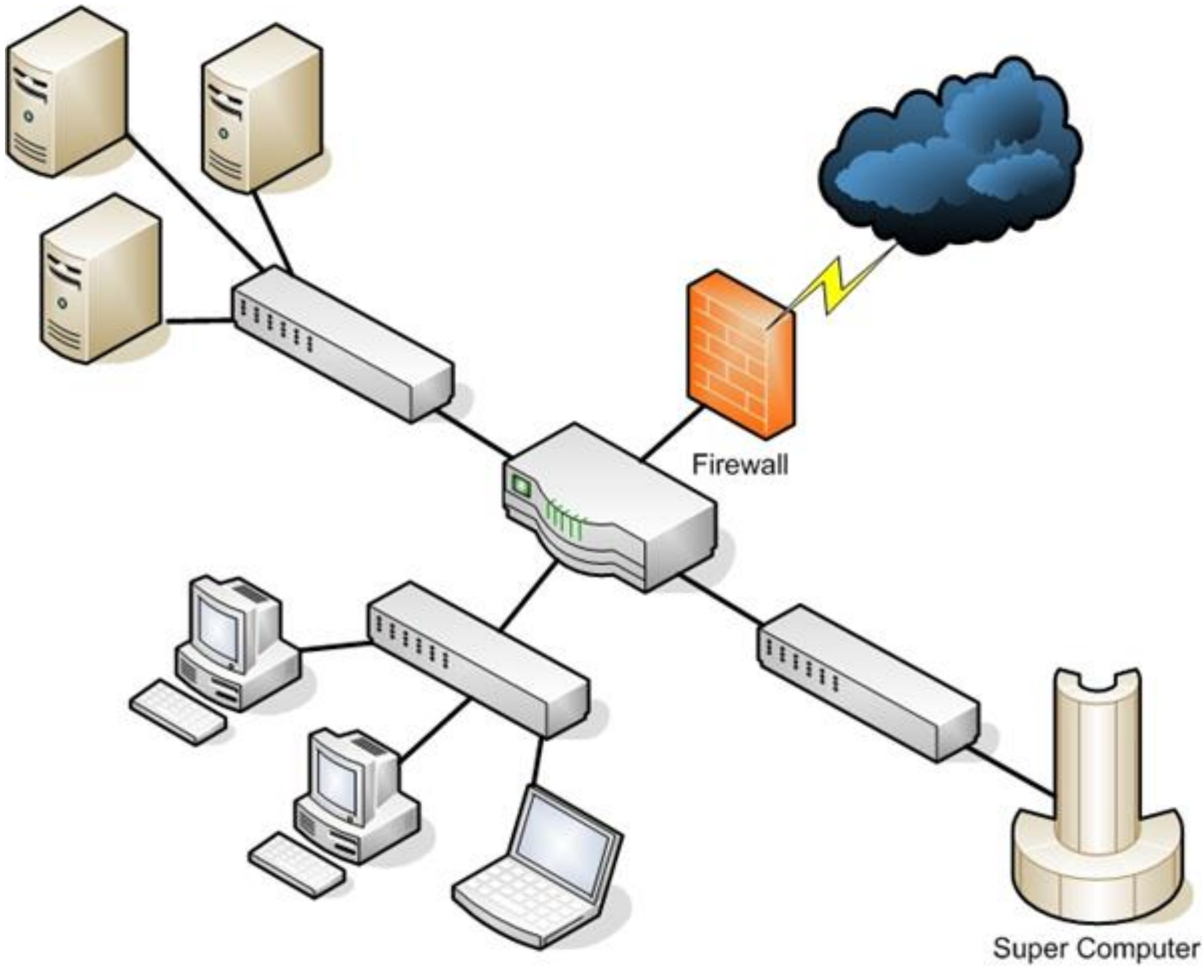


1.1.1 Basic Network Structure

Connection point(s) must exist between your network and the outside world. A barrier is set up between that specific network and the Internet, usually in the form of a firewall. The real essence of networks is to allow communication from one machine to another.

However, every path of communication has a possibility for a potential attack.

The first step in understanding how to defend a network is having a detailed understanding on how computers communicate over a network. Network interface cards, switches, routers, hubs, and firewalls are the fundamental physical pieces of a network. The way they are connected and the format they use for communication is the network architecture.



1.1.2 Data Packets

After you have established a connection with the network (whether it is physical or wireless), you need to send the data. The first part is to identify where you want it to be sent. All computers (as well as routers and switches), have an IP address that is a series of four numbers between 0 and 255 and is separated by periods, such as 192.168.0.1.

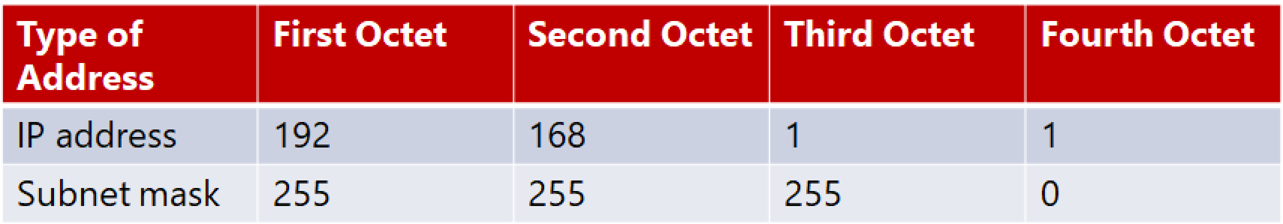
The second part is to format the data for transmission. All data is in binary form (1s and 0s). This binary data is placed into packets, roughly less than 65,000 bytes. The first few bytes consist of the header. This header states where the packet is going, where it came from, and how many more packets are coming as a part of this transmission. There is actually more than just one header, but for now we will discuss the header just as a single entity. Some attacks (IP spoofing, for example) try to change the header of packets in order to give false information. Other methods of attacks simply try to intercept packets and read the content (thus compromising the data).

A packet can have multiple headers. In fact, most packets will have at least three headers. The IP header has information such as IP addresses for the source and destination, as well as what protocol the packet is. The TCP header has information such as port number. The Ethernet header has information such as the MAC address for the source and destination. If a packet is encrypted with Transport Layer Security (TLS), it will also have a TLS header.

1.1.3 IP Addresses

The first major issue is to understand how packets reach their proper destination. Even small networks have many computers that could potentially be the final destination of any packet sent. The Internet has millions of computers spread out across the globe. How can you ensure that a packet arrives to its proper destination? This situation is no different than a letter not reaching its rightful destination. Let’s begin by looking at IP version 4 addressing due to the fact that it’s the most commonly used in today’s world. This section also briefly discusses IP version 6.

An IP version 4 address is a series of four three-digit numbers separated by periods (An example is 192.168.1.1.) Each of the three-digit numbers must be between 0 and 255. An address of 192.168.0.257 would not be a valid one. The reason for this rule is that these addresses are actually four binary numbers: The computer simply displays them to you in decimal format.

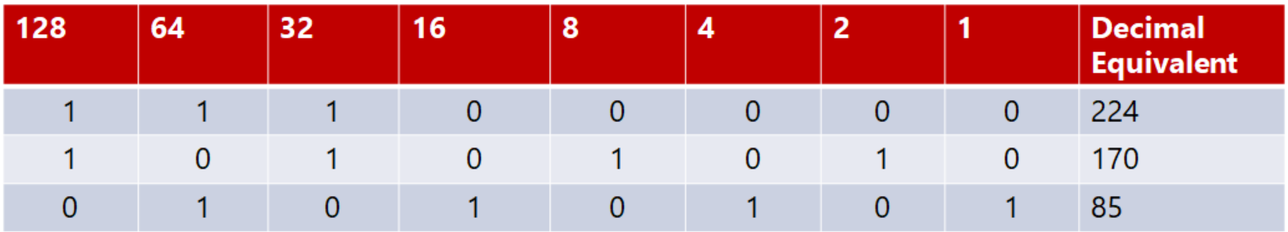


Type of Address	First Octet	Second Octet	Third Octet	Fourth Octet
IP address	192	168	1	1
Subnet mask	255	255	255	0

Table 1-1 IP version 4 Address

Recall that 1 byte is 8 bits (1s and 0s), and an 8-bit binary number converted to decimal format will be between 0 and 255. The total of 32 bits means that approximately 4.2 billion possible IP version 4 addresses exist.

Table 1-2 Decimal-to-Binary Conversion Example



128	64	32	16	8	4	2	1	Decimal Equivalent
1	1	1	0	0	0	0	0	224
1	0	1	0	1	0	1	0	170
0	1	0	1	0	1	0	1	85

The IP address of a computer highly informs you about that computer. The first byte (or the first decimal number) in an address reveals what network class the machine belongs to. Table 1-1 summarizes the five network classes.

Table 1-3 Five Network Classes

Class	IP Range	Use
A	**0-127**	**Used for large networks. All of them have been used**
B	**128-191**	**Large corporate and government networks. All of them have been used**
C	**192-223**	**Most common group of IP addresses.**
D	**224-239**	**Reserved for multicasting**
E	**240-255**	**Reserved for experimental use.**

The IP range of 127 is not listed in the above table. ***The IP address 127.0.0.1 designates to the machine you are on, regardless of the IP address assigned to your machine.***

This address is referred as the ‘loopback address’. This address is used to test the machine and the NIC card.

These particular classes are very important as they direct you to the part of the address that represents the network, and to the part that represents the node. For example, in a Class A address, the first octet represents the network and the remaining three represent the node. In a Class B address, the first two octets represent the network and the second two octets represent the node. Finally, in a Class C address, the first three octets represent the network, and the last represents the node. There are also some very specific IP addresses and IP address ranges you should be aware of.

The first, as mentioned previously is 127.0.0.1, or also called the loopback address. It is another way of referring to the network interface card of the machine you are on. Private IP addresses are another issue that one should be aware of. Certain ranges of IP addresses have been designated for use within networks.

These cannot be used as public IP addresses but can be used for internal.

Workstations and servers. Those IP addresses are:

- **10.0.0.0 to 10.255.255.255**
- **172.16.0.0 to 172.31.255.255**
- **192.168.0.0 to 192.168.255.255**

Sometimes people who are new to networking, have some trouble understanding public and private IP addresses. A good example is an office building. Within a single office building each office number must be unique. There can only be one ‘room 101’ within that building. This means that it is clear to everyone which room it is.

But there are also other office buildings, many of which have their own office 101. Simply view private IP addresses as office numbers. Even though the number should be unique, there may be other networks with the same private IP. Public IP addresses are more like traditional mailing addresses. They must be unique worldwide.

When communicating from office to office, you can use the office number. However, to send a letter to another building you have to use the complete mailing address. It is the same type of process that should be followed in networking. You can communicate within your network using private IP addresses, but to communicate with computers outside of your network must be through a public IP address.

One of the roles of a gateway router is to perform what is called network address translation (NAT). Using NAT, a router takes the private IP address on outgoing packets and replaces it with the public IP address of the gateway router so that the packet can be routed through the Internet.

We have already discussed IP version 4 network addresses. Now let’s turn our attention towards subnetting. Subnetting is simply the process of splitting up a network into smaller portions. For example, if you have a network using the IP address 192.168.1.X (X being whatever the address is for the specific computer), then you have allocated 255 possible IP addresses. What if you want to divide that into two separate subnetworks? This can be done through subnetting.

Technically speaking, the subnet mask is a 32-bit number that is assigned to each host to divide the 32-bit binary IP address into network and node portions. It does not accept random numbers. The first value of a subnet mask must be 255; the remaining three values can be 255, 254, 252, 248, 240, 224, or 128. The network IP address and the subnet mask will be accepted by the computer, which will then use a binary AND operation to combine them.

A subnet mask is present regardless of the fact that you might have never needed to use subnetting. If you have a Class C IP address, then your network subnet mask is 255.255.255.0. If you have a Class B IP address, then your subnet mask is 255.255.0.0. And finally, if it is Class A, your subnet mask is 255.0.0.0.

Now think about these numbers in relation to binary numbers. The decimal value 255 converts to 11111111 in binary. So you are literally "masking" the portion of the network address that is used to define the network, and the remaining portion is used to define individual nodes. If you want less than 255 nodes in your subnet, then you will need something such as 255.255.255.240 for your subnet. If you convert 240 to binary, it is 11110000. This means the first three octets and the first 4 bits of the last octet define the network. The last 4 bits of the last octet define the node. This means you could have as many as 1111 (in binary) or 15 (in decimal) nodes on this subnetwork. This is the basic essence of subnetting.

Subnetting only allows you to use certain, limited subnets. Another approach is CIDR, or classless inter-domain routing. Rather than defining a subnet mask, the IP address should be followed by a slash and a number. That number can be any number between 0 and 32, which results in IP addresses like the following below:

- 192.168.1.10/24 (basically a Class C IP address)
- 192.168.1.10/31 (very similar to a Class C IP address with a subnet mask)

Rather than having classes with subnets, using this method will give you variable-length subnet masking (VLSM) that provide classless IP addresses. This is the most common way to define network IP addresses in today's world.

You should not be concerned that new IP addresses are likely to run out soon. The IP version 6 standard is already available and methods are in place already to extend the use of IPv4 addresses. The IP addresses come in two groups: **public and private.**

The public IP addresses are for computers connected to the Internet. No two public IP addresses can be the same. However, a private IP address, such as one on a private company network, has to be unique only in that network. It does not matter if other computers in the world have the same IP address, because this computer is never connected to those other worldwide computers.

Network administrators often use private IP addresses that begin with a 10, such as 10.102.230.17. The other private IP addresses are 172.16.0.0–172.31.255.255 and 192.168.0.0–192.168.255.255.

Also, note that an ISP will often buy a pool of public IP addresses and assign them to you when you log on. Therefore, an ISP might own 1,000 public IP addresses and have 10,000 customers. This is because all 10,000 customers will not be online at the exact same time. The ISP simply assigns an IP address to a customer when he or she logs on, and the ISP un-assigns the IP address when the customer logs off.

IPv6 utilizes a 128-bit address (instead of 32) and utilizes a hex numbering method in order to avoid long addresses such as 132.64.34.26.64.156.143.57.1.3.7.44.122.111.201.5.

The hex address format appears in the form of 3FFE:B00:800:2::C, for example. This gives you 2128 possible addresses (many trillions of addresses), which means it is impossible to run out of IP addresses any time in the near future.

There is no subnetting in IPv6. Instead, it only uses CIDR. The network portion is indicated by a slash followed by the number of bits in the address that are assigned to the network portion, such as

- /48
- /64

There is a loopback address for IPv6, and it can be written as ::/128.

Other differences between IPv4 and IPv6 are described here:

- Link/machine-local.
- IPv6 version of IPv4's APIPA or Automatic Private IP Addressing. If the machine is configured for dynamically assigned addresses and fails to communicate with a DHCP server, it will assign itself a generic IP address. DHCP, or Dynamic Host Configuration Protocol is used to dynamically assign IP addresses within a network.
- IPv6 link/machine-local IP addresses all start with fe80::. If your computer has this address, this means it could not reach a DHCP server and therefore made up its own generic IP address.
- Site/network-local.
- IPv6 version of IPv4 private address. In other words, these are real IP addresses, but they only work on this local network. They are not routable on the Internet.

- All site/network-local IP addresses begin with FE and have C to F for the third hexadecimal digit: FEC, FED, FEE, or FEF.
- DHCPv6 uses the Managed Address Configuration Flag (M flag).
- When set to 1, the device should use DHCPv6 to obtain a stateful IPv6 address.
- Other stateful configuration flag (O flag).
- When set to 1, the device should use DHCPv6 to obtain other TCP/IP configuration settings. In other words, it should use the DHCP server to set things like the IP address of the gateway and DNS servers.

1.1.4 Uniform Resource Locator (URL)

For most people, the main purpose for surfing the net is to visit websites (amongst other things such as e-mail and file downloading). If you had to remember IP addresses and constantly type them in, then surfing the Net would be extremely difficult. Fortunately, you do not have to. You type in domain names that make sense to humans which are then translated into IP addresses. For example, you might type in www.microsoft.com to go to Microsoft’s website.

Your computer, or your ISP, must translate the name you typed in (which is called a Uniform Resource Locator, or URL) into an IP address. The DNS (Domain Name Service) protocol, which is introduced alongside other protocols later on, handles this translation process. Therefore, you are typing in a name that makes sense to humans, but your computer is using a corresponding IP address to connect. If that address is found, your browser sends a packet (using the HTTP protocol) to TCP port 80. If that target computer has software that listens and responds to such requests (like web-server software such as Apache or Microsoft Internet Information Services), then the target computer will respond to your browser’s request and communication will be established.

This method is how web pages are viewed. If you have ever received an Error 404: File Not Found, let’s analyse what exactly happened. Basically, your browser received back a packet (from the web server) with the error code 404, designating that the web page you requested could not be found. The web server can send back a series of error messages to your web browser, indicating different situations.

E-mail works the same way as visiting websites do. Your e-mail client will seek out the address of your e-mail server. Then your e-mail client will use either POP3 to retrieve your incoming e-mail, or SMTP to send your outgoing e-mail. Your e-mail server (probably at your ISP or your company) will then try to resolve the address you are sending it to. For example, if you send something to johndoe@gmail.com, your e-mail server will translate that e-mail address into an IP address for the e-mail server at gmail.com, sending your e-mail there. Note that newer e-mail protocols are also out there; however, POP3 is still the most commonly used.

IMAP is currently widely used too. **Internet Message Access Protocol operates on port 143. The main advantage of IMAP over POP3 is that it allows the client to download only the email headers, leaving the user to choose which messages to fully download. This is particularly useful for smart phones.**

1.1.5 MAC Addresses

MAC addresses are an extremely interesting topic. A MAC address is a unique address for a network interface card (NIC). Every NIC in the world has their own unique address that is represented by a six-byte hexadecimal number. The Address Resolution Protocol (ARP) is used to convert IP addresses to MAC addresses. This means that when you type in a web address, the DNS protocol is used to translate it into an IP address. The ARP protocol then translates that IP address into a specific MAC address of an individual NIC.

IEEE assigns the first three bytes (24 bits) of the MAC address to a vendor. This part of the address is known as ‘Organizationally Unique Identifier’ (OUI). The OUI helps professionals to determine the MAC address manufacturer. The remaining three bytes (24 bits) are assigned by the vendor. The MAC address is equal to 48 bits.

1.1.6 Protocols

Different types of communication exist for different purposes. These different types of network communications are called protocols. A protocol, is essentially an agreed method of communication. In fact, this definition is exactly how the word protocol is used in standard, non-computer usage. Each protocol has a specific purpose and normally operates on a certain port. The table below lists some of the most important protocols.

Protocol	Purpose	Port
FTP (File Transfer Protocol)	For transferring files between computers	20,21
SSH (Secure Shell)	A secure way to transfer files and remotely login to a system	22

Telnet	Remotely login to a system	23
SMTP (Simple Mail Transfer Protocol)	For sending emails	25
WhoIS	A command to query a target for information	43
DNS (Domain Name Service)	For translating URLs to IP addresses	53
TFTP (Trivial File Transfer Protocol)	Quick but less reliable FTP server	69
HTTP (Hypertext Transfer Protocol)	For displaying web pages	80
POP3 (Post Office Protocol v3)	Retrieves email	110
NNTP (Network News Transfer Protocol)	Used for network news group	119
NetBIOS	An old Microsoft protocol for naming systems on a local network	137,138,139
IRC (Internet Relay Chat)	Chat Room	194
HTTPS (Secure Hypertext Transfer Protocol)	Encrypted HTTP (SSL/TLS)	443
SMB (Server message Block)	Used by Microsoft Active Directory	445
ICMP (Internet Control Message Protocol)	Simple packets containing error messages, informational and control messages	No specific port

You should note that this list is not complete and hundreds of other protocols exist. All these protocols are part of a suite of protocols referred to as TCP/IP (Transmission Control Protocol/Internet Protocol).

The most important thing for us to realize here, is that the communication within networks takes place via packets, and those packets are transmitted according to certain protocols, depending on the type of communication that is occurring.

You might be wondering what exactly a port is. Please do not confuse this type of port with the connections on the back of your computer, such as a serial port or a parallel port. A port in networking terms is a handle or a connection point. It is a numeric designation for a particular pathway of communications.

All network communication, regardless of the port used, comes into your computer through the connection on your NIC. Think of a port as a channel on your TV. You most probably have one cable coming into your TV, but you can view many channels. You have one cable coming into your computer, but you can communicate on many different ports.