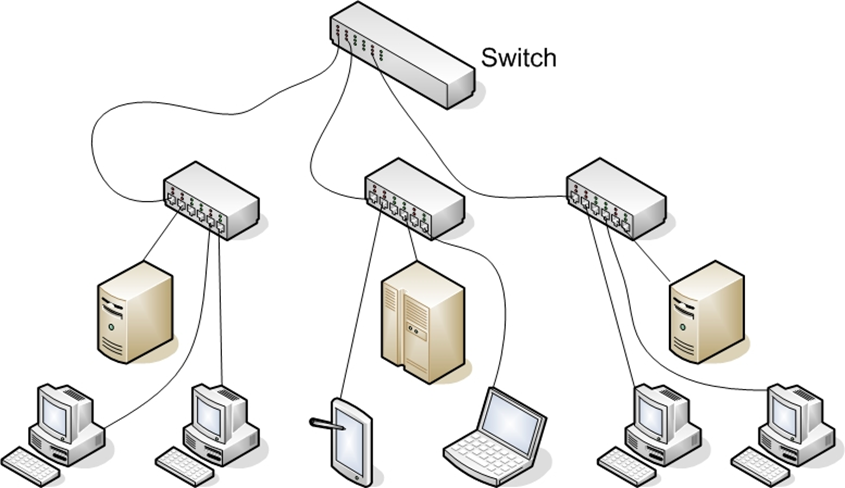
**Network Basics**

***A network is simply a way for communication between systems (computers).At the physical level, it consists of all the machines we want to connect and the devices that we 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. Hub and switches are used to connect multiple machines together and then those hubs / switches must connect together. In larger networks, each subnetwork is connected to the others by a router.***

******

**Basic Network Structure**

***Some connection point(s) must exist between your network and the outside world. Firewall acts as a barrier between that network and the Internet. Every path of communication is a possibility for an attack. We can only protect our network for the attacks when we will have the knowledge about how the computers communicate over the network . We must know about the concepts of NIC(Network Interface Card),switches,routers,hub and firewalls and the way they are connected and the format they use for communication is the network architecture.***

**Data Packets**

***After establishing a connection with the network (whether it is physical or wireless), we need to send data and the first part is to identify where we want to send it. 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 consist of formatting the data for transmission. All data is in binary form (1s and 0s). This binary data is put into packets, all less than about 65,000 bytes. The first few bytes are the header. That header tells where the packet is going, where it came from, and how many more packets are coming as part of this transmission. There is actually more than one header, but for now, we will just discuss the header 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.***

***IP header has information such as IP addresses for the source and destination, as well as what protocol the packet is.***

***TCP header has information such as port number.***

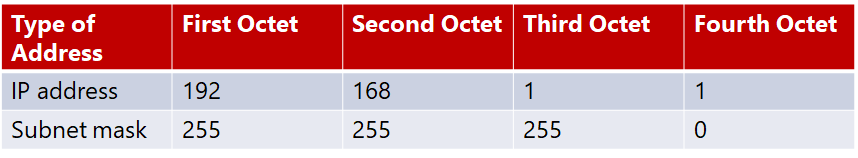
***Ethernet header has information such as the MAC address for the source and destination. If a packet is encrypted with Transport Layer Security (TLS), it will also have a TLS header.***

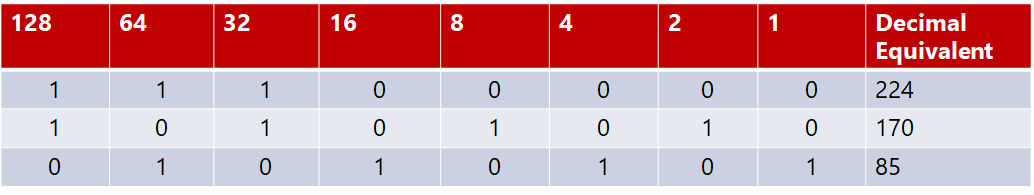
**IP Addresses**

***The first major issue to understand is how to get packets to 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***

***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 us in decimal format.***

**IP version 4 Address**

***NOTE: 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.  
  
Decimal-to-Binary Conversion Example***

******

***The first byte (or the first decimal number) in an address reveals about the network class that machine belongs to.***

***Five Network Classes***

|  |  |  |
| --- | --- | --- |
| ***Class*** | ***IP Range*** | ***Use*** |
| ***A*** | ***0-126*** | ***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*** | ***224-247*** | ***Reserved for multicasting*** |
| ***E*** | ***248-255*** | ***Reserved for experimental use.*** |

***The IP range of 127 is not listed in the above table. The IP address 127.0.0.1 designates the machine we are on, regardless the IP address assigned to our machine. This address is referred to as the loopback address and it is used in testing the machine and the NIC card.***

***These particular classes are important as they tell us what part of the address represents the network and what part 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 represent the node. And 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.***

***Private IP addresses are another issue to 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:***

* ***10.0.0.10 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. we can only have one 101. And within that building, if we refer office 101 it is immediately clear what we are talking about.***

***But there are other office buildings, many of which have their own office 101. we can think of private IP addresses as office numbers. They must be unique within their network, but there may be other networks with the same private IP. Public IP addresses are more like traditional mailing addresses. Those must be unique worldwide.   
  
When communicating from office to office we can use the office number, but to get a letter to another building we have to use the complete mailing address. It is much the same with networking. we can communicate within our network using private IP addresses, but to communicate with any computer outside our network, we have to use public IP addresses.***

***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.***

***Subnetting is splitting up a network into smaller portions. For example, if we have a network using the IP address 192.168.1.X (X being whatever the address is for the specific computer), then we have allocated 255 possible IP addresses.***

***More technically, 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. We also cannot just put in any number we want. The first value of a subnet mask must be 255; the remaining three values can be 255, 254, 252, 248, 240, 224, or 128. Our computer will take our network IP address and the subnet mask and use a binary AND operation to combine them.We already have an subnet mask even if we have not used subnetting .If we have a Class C IP address, then our network subnet mask is 255.255.255.0. If we have a Class B IP address, then our subnet mask is 255.255.0.0. And finally, if it is Class A, your subnet mask is 255.0.0.0.***

***The decimal value 255 converts to 11111111 in binary. So we 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. Now if we want fewer than 255 nodes in our subnet, then we need something like 255.255.255.240 for our subnet. If we convert 240 to binary, it is 11110000. That 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. That means we could have as many as 1111 (in binary) or 15 (in decimal) nodes on this subnetwork. This is the basic essence of subnetting.***

***Another approach is CIDR, or classless interdomain routing. Rather to define a subnet mask, we have the IP address followed by a slash and a number. That number can be any number between 0 and 32, which results in IP addresses like these:***

* ***192.168.1.10/24 (basically a Class C IP address)***
* ***192.168.1.10/31 (much like a Class C IP address with a subnet mask)***

***When we use this, rather than having classes with subnets, we have variable-length subnet masking (VLSM) that provides classless IP addresses. This is the most common way to define network IP addresses today.***

***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 often will buy a pool of public IP addresses and assign them to us when we log on. Therefore, an ISP might own 1,000 public IP addresses and have 10,000 customers. Because all 10,000 customers will not be online at the 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 us 2128 possible addresses (many trillions of addresses), so no chance exists of running out of IP addresses 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. So if the machine is configured for dynamically assigned addresses and cannot communicate with a DHCP server, it assigns 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::. So if our computer has this address, that means it could not get to 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.***

**Uniform Resource Locator (URL)**

***For most people, the main purpose for getting on the Internet is web pages (but there are other things such as e-mail and file downloading). If we had to remember IP addresses and type those in, then surfing the Net would be difficult. Fortunately, we do not have to. We type in domain names that make sense to humans and those are translated into IP addresses. For example, we might type in www.microsoft.com to go to Microsoft’s website.***

***Our ISP must translate the name we typed in (called a Uniform Resource Locator, or URL) into an IP address. The DNS (Domain Name Service) protocol handles this translation process. If that address is found, our 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 our browser’s request and communication will be established.***

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

***E-mail works the same way as visiting websites. Our e-mail client will seek out the address of our e-mail server. Then our e-mail client will use either POP3 to retrieve our incoming e-mail, or SMTP to send our outgoing e-mail. Our e-mail server will then try to resolve the address we are sending to. IMAP is now widely used as well. Internet Message Access Protocol operates on port 143. The main advantage of IMAP over POP3 is it allows the client to download only the email headers, and then the user can choose which messages to fully download. This is particularly useful for smart phones.***

**MAC Addresses**

***A MAC address is a unique address for a network interface card (NIC). Every NIC in the world has a 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. So, when we type in a web address, the DNS protocol is used to translate that 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.***

**Protocols**

***The different types of network communications are called protocols. A protocol is, essentially, an agreed method of communication. Each protocol has a specific purpose and normally operates on a certain port.***

|  |  |  |
| --- | --- | --- |
| ***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*** |

***All these protocols are part of a suite of protocols referred to as TCP/IP (Transmission Control Protocol/Internet Protocol).***