What’s on my network and what does it do?

This document is designed to provide you with an overview of a basic network layout and provide information about the role of each device or service.

Access Point – An access point is what your customers will attach to with their Wi-Fi enabled devices. There are many types of access points, but it is important at this time that your access points are dual band and use at least the N protocol. The newest protocol is AC, but it has yet to be finalized and devices that are providing early access to this protocol are expensive. There are also A, B, and G protocols. These are older than the N protocol, but if you purchase an N or AC protocol access point they are backward compatible. The dual band functionality enables devices to connect at the highest possible data rate for their device. Most new smartphones and laptops will take advantage of the higher data rates. Your access points should have full gigabit Ethernet ports to provide the highest available bandwidth back to your core network.

Active Directory – This Microsoft service allows you to provide user authentication and provide the ability to lock down computers. Your PCs should require a username and password to gain access. This is an initial security measure to protect the PC from access by those who should not have access. Group Policy can also be set up to protect your computers from changes being made or only allowing specific applications to run under a specific login. By not locking down your PCs, you run the risk of illicit software being installed that could capture other users’ data.

Content Filter – A content filter is mandatory for all libraries in the State of Pennsylvania, and is required to be able to receive federal funding or grants. The content filter will allow you to block categories of content that you do not want accessible within your building or by certain age groups. In addition to the ability to provide multiple levels of filtering, staff should have the ability to disable filtering when requested.

Customer (or Patron) management systems – These systems allow you to require users to log in with their barcode/password or a guest pass. The software allows you to track who is logging on to your equipment and what time, but does not track what your customers do while logged in. Some systems will also allow you to manage your Wi-Fi access in the same way.

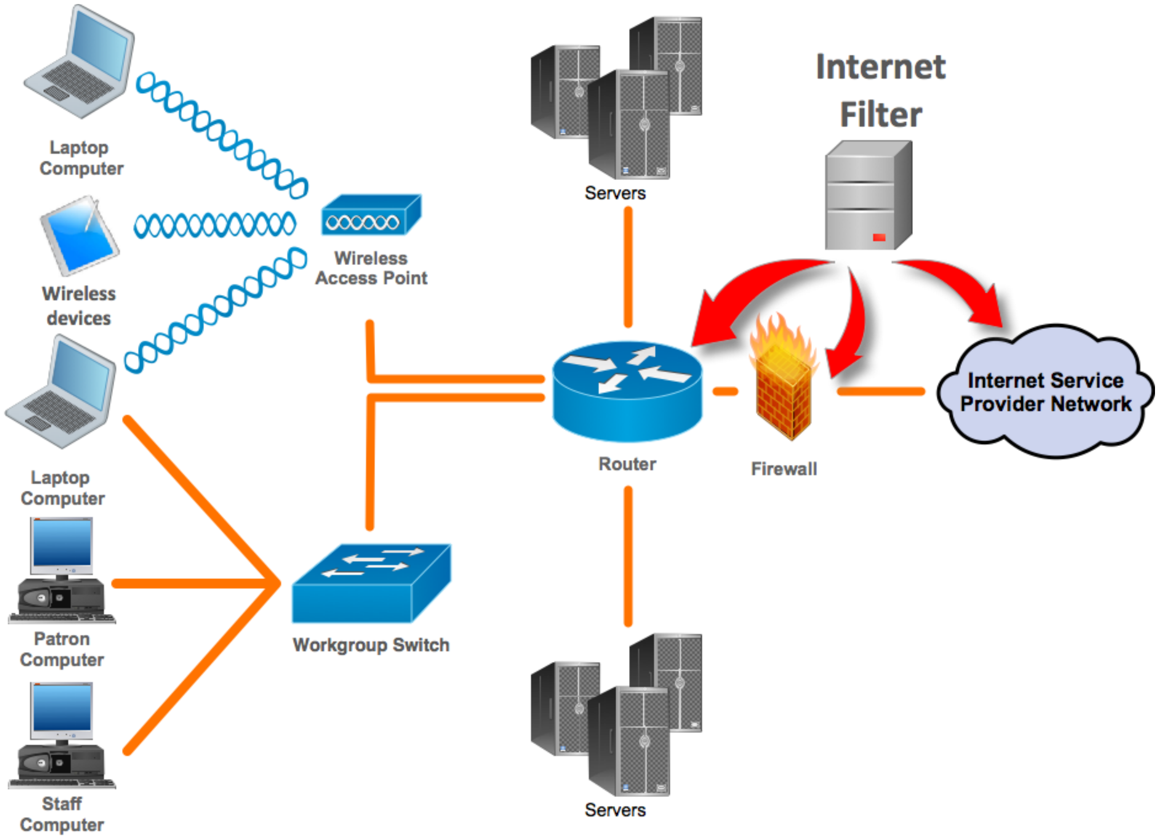
Firewall – A firewall typically sits between your network and the handoff from your Internet Service Provider (ISP). The primary role of this device is to protect your internal equipment from unauthorized external access. There are other services that this device can provide, such as content filtering, VPN (Virtual Private Network), and Antivirus/Antimalware. Depending upon the type of firewall, you can define separate network zones within your building. For instance, you would typically want to separate your staff traffic from your public traffic. Yes, your customers are trying to hack your staff machines—you have to always assume that the person sitting down at your computers or connecting to your Wi-Fi network are attempting to access your business hardware or data. It is okay to be paranoid when it comes to the security of your network.

IP Address – A number made up of four numbers separated by three dots (167.101.158.41) that uniquely identifies each device on the Internet or internal network. There are two types of IP addresses, private and public. Private IP addresses start with 10, 192.168, or 172.16, and are used for internal networks and cannot be routed or accessed through the Internet. Public IP addresses are those addresses that can be reached on the Internet such as web sites, your cable modem, or mail servers.

MAC Address - A Media Access Control address is a hardware identification number (00:0d:83:b1:c0:8e) that uniquely identifies every device on a network. The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card, and cannot be changed. You generally do not need to know what the MAC address is for each device, but it may be important when trying to troubleshoot a network issue.

Modem – If you have cable or DSL service, this is the device that connects your network to your broadband service and provides access to the Internet.

Network Map – A network map is a graphical representation of your network. It will show how data flows through your network to your broadband connection. The map does not show all of the PCs or servers on your network, but it should show all network device on your network and all zones. If you have separated your public traffic from your staff traffic, you would want to show these as separate network segments on your map. If you work with a consultant or vendor to set up or manage your network, they should provide you with a network map. The following image is an example of a basic network map. More advanced network maps may include IP address or MAC addresses for each network device so that troubleshooting may be easier when needed.



QoS – Quality of Service is a set of standards and mechanisms for ensuring high-quality performance for critical application. QoS is generally configured on a switch, router or firewall. A reason for doing this would be to ensure that ILS traffic receives priority on your network and is less likely to be slow or experience drops.

Router – A router may be used to route traffic on your network. Some networks no longer have a separate router since routing functionality is built into many other devices (firewalls or switches). If you are on a fiber (not FIOS) connection, your network provider may provide you with a router as the handoff point between their service and your network.

Switch – A switch aggregates many connections to one connection (could be more than one, but that is a more advanced discussion). You should be purchasing a switch that is at least gigabit or 10/100/1000Mbps capable. All of the latest computing devices are designed to work at gigabit speed. Switches generally accommodate 24 or 48 connections in a single box. Switches are either unmanaged or managed. An unmanaged switch provides no additional services other than aggregating the connections and generally less expensive. A managed switch can provide higher end functions such as monitoring, individual port control, QoS (Quality of Service) or VPN.

VPN – A Virtual Private Network uses a public network connection, such as the Internet, to provide remote offices or individual users with secure access to the organization's network. For example, if you are connecting a branch library back to a headquarters location through a public fiber network, you would set up a VPN to ensure that your data is encrypted and not accessible by a third party.