International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015
ISSN 2091-2730

Wired vs Wireless Using Advanced Network

M.SRIVIDYA Mrs. N.VIJAYARANI

[1]M.phil Full Time Research Scholar, Department of Computer Science

[2]Assistant Professor, Department of Computer Science & Applications

Vivekanandha College of Arts and Science for Women (Autonomous), Namakkal, Tamilnadu, India msrividya21@gmail.com

vijiyaranimca@rediffmail.com

Abstract- As technology advances in society the need for wired and wireless networking has become essential. Each of these types of networking has their advantages and disadvantages according to security. Wired networking has different hardware requirements and the range and benefits are different. Wireless networking takes into consideration the range, mobility, and the several types of hardware components needed to establish a wireless network. As you read on you will understand different types of configurations of networks and the security measures that need to be taken to ensure a secure network.

Keyword- Wi-Fi, mobility, local area network technology, Ethernet cables, broadband, fiber-optic, Wired Equivalent Privacy

INTRODUCTION

Organizations rely heavily on the ability to share information throughout the organization in an efficient and productive manner. Computer networks have allowed for this technology and are now a part of almost every business. An organization has two options when it comes to setting up a network. They can use a completely wired network, which uses networking cable to connect computers, or they can use a wireless network, which uses radio frequencies to connect computer. Wireless networks have allowed organizations to become more mobile; therefore, organizations are now using a combination of both wired and wireless networks.

They basic hardware layout for the two types of networks are fairly similar but for an organization to go wireless it requires a few more hardware components. Although networks provide convenience they do open the organization up to security and privacy risks. If a company is faced with a security they are ways that they can fix and prevent future security risks. As you read on, you will learn how the network has become an essential part of today's organizations.

Hardware Components

Before one can begin to setup a network they must first be sure they have a network interface card, commonly referred to as a NIC. A NIC is a device that connects a computer or other device to a network. For computers, the NIC is usually installed in an expansion slot and has a chip that handles the physical and data-link layers of network communications.

To establish your network you will need a few key components. If you plan to access the internet you will start your network off with a cable modem. This type of modem is designed to operate using your existing cable lines. Cable internet has a high bandwidth and can support most, if not, all applications you will be using. The second component is a router. A router is a device that routes data from one network to another network. A router is connected to at least two networks, commonly two networks or a network and its ISP's network. A router allows for everyone on the network to access the internet.

The next component that you will need to setup a network is a hub or sometimes a switch. A hub is a device that connects the cables from computers and other devices such as printers in a network. Traditionally, hubs are used for star topology networks, but

they are often used with other configurations to make it easy to add and remove computers without bringing down the network. A hub can be either active or passive; simply forwarding messages or amplifying or refreshing the data. A switch is a device similar to a hub that enables the connection of multiple computers, access points, and other network enabled devices. The difference between a hub and a switch is that a switch filters the data that passes through it and a hub does not.

These components have all been modified and are capable of establishing wireless networks. A router can be purchased with wireless capability but a more efficient way of adding wireless to your network is to simply add wired access points. An access point will bride a wired network with a wireless network and can be hard wired in to your existing system. This option allows for the mobility of a wireless network.

Another key component is a print server. A print server is used to connect printers to a network to allow for network printing. The server will act as a buffer; storing the messaging and printing them in order of the queue. This device can drastically reduce the cost of networking because now everyone can use the same printer without having a printer attached to every computer.

wired networks

Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology.

A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100 Mbps or higher. Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network interface card, or NIC). Ethernet adapters can be internal (installed in a computer) or external (housed in a separate case). Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter (Microsoft). There are three basic network topologies that are most commonly used today. (Homenthelp.com)

The star network, a general more simplistic type of topology, has one central hub that connects to three or more computers and the ability to network printers. This type can be used for small businesses and even home networks. The star network is very useful for applications where some processing must be centralized and some must be performed locally. The major disadvantage is the star network is its vulnerability. All data must pass through one central host computer and if that host fails the entire network will fail.

On the other hand the bus network has no central computer and all computers are linked on a single circuit. This type broadcasts signals in all directions and it uses special software to identify which computer gets what signal. One disadvantage with this type of network is that only one signal can be sent at one time, if two signals are sent at the same time they will collide and the signal will fail to reach its destination. One advantage is that there is no central computer so if one computer goes down others will not be affected and will be able to send messages to one another.

The third type of network is the ring network. Similar to the bus network, the ring network does not rely on a central host computer either. Each computer in the network can communicate directly with any other computer, and each processes its own applications independently. A ring network forms a closed loop and data is sent in one direction only and if a computer in the network fails the data is still able to be transmitted.

Typically the range of a wired network is within a 2,000-foot-radius. The disadvantage of this is that data transmission over this distance may be slow or nonexistent. The benefit of a wired network is that bandwidth is very high and that interference is very limited through direct connections. Wired networks are more secure and can be used in many situations; corporate LANs, school networks and hospitals. The biggest drawback to this type of network is that it must be rewired every time it is moved.

WIRED VS WIRELESS IN THE ENTERPRISE:

He world around us is going wireless; we stream music and movies from our home PCs to any room in the house, we can play music from our phones on car stereos and we can go to any number of public places and hook up to the internet. But one place has stayed resolutely wired the enterprise. Yes, many offices these days will have Wi-Fi but often it is reserved for senior management or visitors. Even if it is available for all workers, the connection is rarely the most reliable

Benefits of wired connection

It is easy enough to see why enterprises want to remain wired – control and security, reliability and speed are the primary benefits of using physical connections. It is also relatively cost-effective, as the price of cabling – even at the lengths needed to cover an average office – is pretty cheap. One great advantage of having a wired infrastructure, which seems particularly relevant in today's mobile world, is the control it provides. If a physical connection is needed to access the corporate network, the business is in full control of whom and what gets online. While this has obvious security benefits of keeping unauthorized visitors out of your network, it also means your network will not be overloaded with non-business critical traffic.

Benefits of wireless connection

While a physical infrastructure may be good from a management point of view and offer cheap deployment, having all those wires running throughout a building can be costly and awkward to maintain. For example, if a business increases its workforce, all those new workers will need physical connections at their desk – connections that will need to be manually set up. Any breakages in the wired connection will also have to be manually fixed as there is no software solution to a broken Ethernet pin. With the explosion in mobile devices over the last few years – Apple alone has sold around 100 million iPads since the tablet was introduced in 2010 – many workers are bringing their own devices into the office. It is vital these employees have access to the corporate network to get the most out of them, and that means giving them wireless access. As well as being able to use their own devices, wireless infrastructure means freedom to move around the office, from desk to desk or meeting room to meeting room. A wireless network is also neater, getting rid of all those unsightly cables that usually run around an office.

Disadvantages of wireless connection

But while enabling workers to use their own devices at work connect up with the corporate network and move around the building brings obvious productivity benefits, it also causes huge headaches for the IT department from a security point of view. The threat of malware getting onto the corporate network via a compromised device is one particular issue. If the mobile or tablet is owned by the business, security is obviously easier to take care of – but employee-owned devices are another question, as most are not protected

A combination of wired and wireless is the way forward:

Prior to allowing workers to connect their personal device to the wireless network, it is important for a business to ensure employees are aware of the risks. Updating security policies to reflect changing ownership is one good step, but educating employees through initiatives such as workshops is vital. There are other threats to a wireless enterprise. Your network will now extend beyond the physical walls of the office, giving attackers another potential route into the business. All that critical corporate data is now flying

across the airwaves, and if your wireless network is not secured to the same extent as your wired infrastructure, it could very easily end up in the wrong hands. This means elements such as authentication, intrusion detection, prevention, reporting and security event management (SEM) must be included in the security set-up of a wireless infrastructure. It is also worth pointing out more simple measures – such as changing the default SSID and password to a more secure one – can be very effective.

Beyond the security implications there are other drawbacks to wireless connections. Speeds are much slower than with a wired connection and the signals can be affected by outside influences, such as walls and floors, as well as other electronic items. Another issue is the range offered by wireless access points. Not only can these be limited in terms of how far the signal travels but the signal can also fade the further away from it you are. This means to ensure full, reliable coverage across a building, a business must install plenty of access points, driving up the cost of the installation.

Legacy infrastructure and mixed environments

There are pros and cons to having a wireless and a wired enterprise and it is fair to say that wireless becoming the norm is still some way off. For example, there is too much legacy infrastructure in place to rip it out and replace it with a wireless set up. A combination of wired and wireless is the way forward, at least for now. That way a business can satisfy the needs of its mobile workers and ensure all security, control and reliability requirements are met.

Having a mixed environment does not need to mean a nightmare from a management point of view. Cisco, for example, recently unveiled its new Unified Access platform, which brings together wired and wireless connections in one switch. The 5760 Unified Access WLAN controller enables wireless connections to be managed on top of existing wired infrastructure.

Juniper Networks also integrates wireless LANs with existing wired infrastructure, giving businesses the best of both worlds. Managing both together means businesses can run the same policies across the wired and wireless infrastructure, meaning business will see the benefit of having both while, hopefully, reducing the negatives associated with either installation.

Wired vs Wireless Networking

Computer networks for the home and small business can be built using either wired or wireless technology. Wired Ethernet has been the traditional choice in homes, but Wi-Fi wireless technologies are gaining ground fast. Both wired and wireless can claim advantages over the other; both represent viable options for home and other local area networks (LANs).

Wired LANs: Wired LANs use Ethernet cables and network adapters. Although two computers can be directly wired to each other using an Ethernet crossover cable, wired LANs generally also require central devices like hubs, switches, or routers to accommodate more computers.For dial-up connections to the internet, the computer hosting the modem must run Internet Connection Sharing or similar software to share the connection with all other computers on the LAN. Broadband routers allow easier sharing of cable modem or DSL internet connections, plus they often include built-in firewall support.

Installation: Ethernet cables must be run from each computer to another computer or to the central device. It can be time-consuming and difficult to run cables under the floor or through walls, especially when computers sit in different rooms. In some new home builds, homeowners are installing CAT5 cable right up front to make the cabling process easier and to hide the cable runs. Your organization's mix of devices (such as the type of internet connection, whether your modem is internal or external) will have a direct impact on the cabling configuration for a wired LAN, but it will not make the configuration more complex. Once you have installed your hardware, the final steps for configuring your wired or wireless LAN are pretty much the same as the both rely on standard IP and network configuration options. Laptops and other portable devices often enjoy greater mobility in wireless home network installations.

Cost: Ethernet cables, hubs and switches are very inexpensive. Some connection sharing software packages, like ICS, are free; some cost a nominal fee. Broadband routers cost more, but these are optional components of a wired LAN, and their higher cost is offset by the benefit of easier installation and built-in security features.

Reliability: Ethernet cables, hubs and switches are extremely reliable, mainly because manufacturers have been continually improving Ethernet technology over several decades. Loose cables likely remain the single most common and annoying source of failure in a wired network. When installing a wired LAN or moving any of the components later, be sure to carefully check the cable connections.

Broadband routers are relatively new, multi-function devices which have suffered from some reliability problems in the past. They have however, matured over the past several years and as a result, their reliability has improved greatly.

Performance: Wireless LANs using 802.11b support a maximum theoretical bandwidth of 11 Mbps – roughly the same as that of old, traditional Ethernet. 802.11a and 802.11g WLANs support approximately one-half the bandwidth of fast Ethernet. In addition to that the further away you are from the original access point the greater the degradation of WI-FI signal. Should you increase the number of wireless devices which utilize the WLAN this will also have a negative impact on performance. Overall, the performance of 802.11a and 802.11g is sufficient for home internet connection sharing and file sharing, but generally not sufficient for home LAN gaming.

Although there is a performance disadvantage with wireless LANs, this is offset by the advantage o greater mobility. Mobile computers do not need to be tied to an Ethernet cable and can roam freely within the WLAN range. However, many home computers are larger desktop models, and even mobile computers must sometimes be tied to an electrical cord and outlet for power. This undermines the mobility advantage of WLANs in many homes.

Security: If you accept that you should protect your home network like you protect your physical home, then the security issues surrounding wireless versus wired LANs becomes a moot point. While data travelling via a wireless LAN can be intercepted, WLANs do protect their data through Wired Equivalent Privacy (WP). Take additional security steps such as ensuring your home's internet-firewall is properly configured, and being alert to spoof emails and spyware. Do also be wary of who you give access to your home's network. No computer network is completely secure and homeowners but being forewarned is being forearmed.

Wireless Routers vs. Wired Connections

Wired connection speeds: Wired connections can achieve extremely fast speeds, which work well if you have a fast broadband or fiber-optic Internet connection, making wired options superior to wireless when it comes to speed. These speeds are almost always theoretical maximum speeds, so you will probably see a lower speed in actual performance, depending on the actual conditions.

Wired Options:

- **Ethernet:** These connections for home routers and computers typically support transmissions up to 100 megabits per second (Mbps).
- **Phone-line:** A phone-line connection between your network router and computer can allow for varying speeds from 1 Mbps to 128 Mbps, depending on the hardware you have available.
- **Power-line networking:** This option, which uses the existing power outlets and electrical wiring to transmit network signals, can be a cheap solution although it only supports speeds up to 14 Mbps.

Wireless connection speeds: Wireless networks are also typically rated with theoretical maximum speeds, so these numbers may not reflect actual performance. In general, you'll get slower performance from a wireless connection than from a wired connection. Wireless routers, laptops and other devices typically use one of the following signal standards.

Wireless Options:

- **802.11a:** Also known as "Wireless-A," this wireless standard can transfer at speeds up to 54 Mbps.
- **802.11b:** Wireless-B networks are slower, only transferring at 11 Mbps.
- **802.11g:** Wireless-G is backwards-compatible with wireless-B although an older device will obviously operate at the slower of the two speeds. Wireless-G devices can transfer at up to 54 Mbps.
- **802.11n:** Wireless-N promises transfer rates of up to 600 Mbps although actual reported performance is much lower, depending on other conditions and what type of hardware you're using.

Installation: A wired connection is rather simple to set up. All you need is a connecting cable from your computer to your router or modem. You may need to change some settings to get your computer to recognize the connection. Wireless networks take a bit more work to set up, and you'll need to place the router in a location where your computers will receive a clear signal. You'll also need to set up security settings and a network passkey, which you'll need for every single computer on the network. Depending on your wireless router and the operating system software running on each computer, you may have to install additional software or change the network settings to get the computers to recognize the connection.

Compatibility: Wired connections only require that your computer and network devices be compatible with a technology like Ethernet or HomePNA. Ethernet is the most widely used wired connection for desktops and laptop computers, requiring an actual Ethernet port. If you don't have the appropriate port, you might be able to install an Ethernet adapter card that adds the port to your computer. Wireless networks, in comparison, need no connection ports. Instead, you'll need wireless capability that uses a signal compatible with your wireless router's signal. This means that many different Wi-Fi devices can use the network as long as they use the right signal. If your computer doesn't have built-in wireless, you can add that capability by installing a wireless-network adapter through a USB port.

Wired vs. Wireless Networking

The biggest difference between these two types of networks is one uses network cables and one uses radio frequencies. A wired network allows for a faster and more secure connection and can only be used for distances shorter than 2,000 feet. A wireless network is a lot less secure and transmission speeds can suffer from outside interference. Although wireless networking is a lot more mobile than wired networking the range of the network is usually 150-300 indoors and up to 1000 feet outdoors depending on the terrain. (Homelanextream.com)

The cost for wired networking has become rather inexpensive. Ethernet cables, hubs and switches are very inexpensive. Some connection sharing software packages, like ICS, are free; some cost a nominal fee. Broadband routers cost more, but these are optional components of a wired network, and their higher cost is offset by the benefit of easier installation and built-in security features.

Wireless gear costs somewhat more than the equivalent wired Ethernet products. At full retail prices, wireless adapters and access points may cost three or four times as much as Ethernet cable adapters and hubs/switches, respectively. 802.11b products have dropped in price considerably with the release of 802.11g. (Homelanextream.com)

Wired LANs offer superior performance. A traditional Ethernet connection offers only 10 Mbps bandwidth, but 100 Mbps Fast Ethernet technology costs a little more and is readily available. Fast Ethernet should be sufficient for file sharing, gaming, and high-speed Internet access for many years into the future. (Wi-Fi.org) Wired LANs utilizing hubs can suffer performance slowdown if computers heavily utilize the network simultaneously. Use Ethernet switches instead of hubs to avoid this problem; a switch costs little more than a hub.

Wireless networks using 802.11b support a maximum bandwidth of 11 Mbps, roughly the same as that of old, traditional Ethernet. 802.11a and 802.11g LANs support 54 Mbps, that is approximately one-half the bandwidth of Fast Ethernet. Furthermore, wireless networking performance is distance sensitive, meaning that maximum performance will degrade on computers farther away from the access point or other communication endpoint. As more wireless devices utilize the 802.11 LAN more heavily, performance degrades even further. (Wi-Fi.org)

The greater mobility of wireless LANs helps offset the performance disadvantage. Mobile computers do not need to be tied to an Ethernet cable and can roam freely within the wireless network range. However, many computers are larger desktop models, and even mobile computers must sometimes be tied to an electrical cord and outlet for power. This undermines the mobility advantage of wireless networks in many organizations and homes.

For any wired network connected to the Internet, firewalls are the primary security consideration. Wired Ethernet hubs and switches do not support firewalls. However, firewall software products like Zone Alarm can be installed on the computers themselves. Broadband routers offer equivalent firewall capability built into the device, configurable through its own software.

In theory, wireless LANs are less secure than wired LANs, because wireless communication signals travel through the air and can easily be intercepted. The weaknesses of wireless security are more theoretical than practical. (Wi-Fi.org) Wireless networks protect their data through the Wired Equivalent Privacy (WEP) encryption standard that makes wireless communications reasonably as safe as wired ones.

No computer network is completely secure. Important security considerations for organizations tend to not be related to whether the network is wired or wireless but rather ensuring that the firewall is properly configured, employees are aware of the dangers of spoof emails, they are away of spy ware and how to avoid and that anyone outside the organization does not have unauthorized access to the network.

Wireless Network Security

Network security is a big concern for individuals and organizations because vital information is stored on the network and most critical process of the business are done through the network. If a network is to fail or security is compromised an organization could be completely crippled. For example, if Wal-Mart was to lose their cash register network than they would suffer a huge loss of business and would take, depending on the severity of the breach, several hours to days to fix. Also at risk is employee and client privacy. If an organization's network is hacked into they would have access to client databases as well as employee databases. The most important thing to keep in mind when it comes to wireless network security is keeping unauthorized users from accessing your network. The first step is to know your wireless network's range and to use specific software to grant access only to authorized users.

CONCLUSION

Wired and Wireless networks are very common in the workplace as well as in the home. Technology has been created to store, transmit and receive data through networks at very high rates of speed. Networks have become essential to completing daily business tasks and most business, those who rely heavily on information technologies, would be crippled without their networks. Advances in networking storage have allowed for organizations to use their networks not only for the sharing of resources but to store large pools of data to be used for data analysis. Companies can now store detailed profile information for customers at a very low cost. In the future, the speed of networks will increase as they have in past years. The cost of networks will continue to decline and using a network will be essential for every organization. As computing technology increases in power, and decreases in size, the price of creating a high-powered full featured network will decrease rapidly.

REFERENCES:

[1]http://www.homelanxtreme.com/wired-vs-wireless.htm

[2]http://www.vicomsoft.com/knowledge/reference/wireless1.html#6

[3]http://www.cert.org/tech_tips/home_networks.html#introduction

[4]http://www.pcstats.com/articleview.cfm?articleID=1489

[5]http://compnetworking.about.com/od/wirelesssecurity/

[6]http://www.infotelsystems.com/wireless%20networking%20outline.htm

[7]http://www.homenethelp.com/web/diagram/index.asp

[8]http://www.windowsecurity.com/articles/Wireless-Networks-Surpassed-Security-Wired-Networks.html

[9]http://whatis.techtarget.com/definitionsCategory/0,289915,sid9_tax1681,00.html

[10]http://www.wifi.org/OpenSection/wireless_vs_wired.asp?TID=2