Network Architecture and Man in the Middle

DYLAN FAHR

6/30/2016

**Table of Contents**

**Executive Summary**

**……………………………………………………………………….…. 2**

**MPLS vs SD-WAN**

**………………………………………………………………..…….. 3 - 5**

**Router Specifications**

**………...………………………………………………..…………... 6 - 7**

**Ping Mapping and Results**

**……………………………………………………………….......... 8 - 15**

**Man in the Middle Attack …………………………………………...………………………. 16 - 25**

**Conclusion**

**………………………………………..………………………….. 26 - 27**

**Executive Summary**

This experiment serves to demonstrate and analyze various aspects of the working of a network, what solutions are available, how they are connected to by outside users, how they interact on the local level, and how they can be manipulated through the use of virtualization. With the analysis of various network solutions, we are able to gauge differences between the two and how they relate to industries and their network infrastructure. The specifications of a personal router help describe the network infrastructure on the local level. A ping map is utilized to help understand how network connections change from site to site. A man in the middle attack is used is help understand how virtualization can be used to disrupt the network without the network detecting it.

Operating Systems Used:

* Host: Windows 10 64 bit
* Virtual Machines: Windows 7 x64 (Client) Windows 2012 Server (Server) Kali Linux (Attacker)

Virtual Machine Software:

* VMware Workstation Pro 12

Software Used:

* FileZilla (Client connect to Server)
* FTP (server)
* IP bulk lookup tool (ping)

Hardware:

* NETGEAR N750 Wireless Dual Band Gigabit Router

Misc. Software:

* Microsoft Excel (For graphing and table creation of ping results)

Conclusion:

In conclusion, the strength of a network depends on all the components involved. What can be gathered from the comparison of the SD-WAN and MPLS network solutions is how each have different advantages and disadvantages towards providing an ideal network environment for an enterprise. The analysis of the router helps bring the overview of a network and what is involved on a personal level. The mapping of IP addresses from ping tests from a machine shows how an enterprise network can change and help aid traffic. Finally, the man in the middle attack helps demonstrate how virtualization can be utilized to disrupt the network and steal packets without the network detecting it or destroy the flow of traffic. Altogether, what can be gained from this experiment is a better gage and understanding of how a network works both on an enterprise and local level and how virtualization can play a part in it.

**MPLS vs SD-WAN**

There are two different network solutions that are available to enterprises and provide various advantages to the business. The network solutions, MPLS and SD-WAN, are utilized in order to create and maintain a strong, secure and reliable network for the enterprise. Both have their advantages and disadvantages within the realm of network solutions. These advantages and disadvantages can be utilized in order to help make a decision of which network is suited best for a real world enterprise scenario.

MPLS stands for Multiprotocol Labeling Switching, this protocol allows for fast and reliable network connections. The protocol operates by forwarding packets to the switching level of the network, effectively bypassing the router level and allowing for quicker addressing and forwarding of packets. By utilizing this protocol and bypassing the router layer, the protocol allows for the packet delivery to be more reliable and direct from user to user throughout a network.

With the direct connection of packets utilized by this protocol, packet loss over the network is very minimal between the users, but is susceptible to network congestion by having multiple users using the same MPLS network as the core medium. By having multiple packets being send and received over a shared MPLS network, the odds of network congestion and packet loss increase. While packet loss is minimal over a MPLS network of a small number of users, the odds do increase as more are connected and sending / receiving packets over the network. This is namely due to the infrastructure of the protocol which enables the packets to be directly sent to the switch layer of the network, which bypasses the routing layer, whose job is to help connect to various networks and sort packets accordingly. While bypassing this level does grant higher speeds and connection dependability, it does make the network prone to congestion and packet loss over it.

The MPLS protocol does ensure great user-to-user connectivity over the network and has a layer of security that is guaranteed by the addressing protocol issued to each packet by the switch layer. This security helps ensure that the correct packet is sent over the network and helps to eliminate packet loss, but like stated before, this does become an issue as more users are connected and utilize the MPLS network and lead to network congestion.

SD-WAN is a networking solution that is dependent on the software of the network and the machines involved. Instead of solely utilizing the hardware platforms of the network and the machines connected to it, the SD-WAN utilizes the software on the machines to help aid connection and enable more secure and reliable connection throughout the network and the users involved.

By utilizing a set of encrypted tunnels for communication and packet transfer over the network, the SD-WAN bypasses the hardware levels of the network and ensures the packets are sent and received by the desired users of the network and ensure reliability and security of the network. In the case of network congestion and packet loss, SD-WAN utilizes the FEC (Forward Error Correction) tool to help aid network congestion and identify the lost packet and try to recover the packet and send it to its receptive recipient over the network. This solution, along with others, helps address the packet loss issue that is common over networks due to congestion and other factors. With the use of encrypted tunnels for connection of packets throughout the network, security is guaranteed and provided to all the users. Additionally, it should be noted, that additional security solutions, or the use of VPNs can also be added upon the network and used alongside the SD-WAN setup. With site-to-site connectivity, SD-WAN is very reliable and quick and cost effective as well. In order to help configure a line of connection within the network or in order to add a new one, one can be added or changed according to the provider of the internet over the network and by utilizing the software of the machines connected to the network, the cost and work of manually connecting each machine is minimal and rather relies on the software of the user.

The cons of the SD-WAN network solution are that it is not as fast or direct as the MPLS protocol. Since the SD-WAN network relies on the software of the machines connected to the network, if a user connected to the network lacks the appropriate software or if there is an issue with the software itself, the connection of the network starts to suffer.

A scenario to which the comparison can be made as to which network solution is preferred in its overall use and abilities, is an enterprise setting that has the users handling sensitive information. To be more specific with the scenario, a business enterprise that handles sensitive information, such as petroleum business that handles sensitive information regarding their clients and the products. Within this setting, the business relies on the network to connect all the employees and clients to each other in order to streamline connection and ensure clear and consistent communication across the connection. The network also needs to be heavily encrypted and secure in order to protect client and company information and ensure integrity that the information being sent over the network to and from the client and the business is the correct information and not in some way false or exposed by outside forces that may be malicious.

With this scenario, the SD\_WAN network solution is preferred due to its advantages with network reliability and security. By utilizing a connection dependent on the software used throughout the network, the information within the network remains within the network and can be monitored and adjusted as such to reach further means, including security. The SD-WAN utilizes encrypted tunnels overlay over the hardware connections of the network, and with the use of these encrypted tunnels, packets are quickly and securely sent from user to user. Along with this level of encryption and security, more security solutions can be implemented on top and help ensure a more secure network connection throughout. By bypassing the hardware levels of the network for connectivity of the network, an employee can easily join the network and send/ receive information easily and securely. With the SD-WAN network, the business’ network ensures security, reliability, efficiency, and integrity by making sure that only certain machines can be connected to the network, and with the added level of security, that only certain users have access to certain information. The secure information that is sent over the network is ensured to reach its desired location and communication is streamlined and made more reliable and secure.

**Router Specs:**

In order to further understand the strength of my network and all the factors involved, the makeup and technical specifications of the router in the network must be listed. By listing the internal makeup and technical specs of the router, one can have a better gauge of the network’s strength and reliability comes to be.

My router is a NETGEAR N750 Wireless Dual Band Gigabit Router, which helps broadcast and connect my network together and allows me to access the internet through my various devices. The router advertises its ability to provide up to 450 Mbps of wireless speed, a simultaneous dual band which help ensure top speeds and avoid interference from the network, four gigabit Ethernet ports, guest network access, broadband usage meter in order to help monitor and gage the network traffic, easy setup, and a secure connection. Upon further analysis, it becomes clearer as to why the router makes these claims in order to advertise itself.

The router is able to simultaneously broadcast the network signal at both 2.4 and 5 GHz, thus helping the broadcast become stronger and last longer with each device connected within the network. This simultaneous broadcast helps connect with all sorts of devices, including those with low broadcast signal, the lower broadcast power level helps pick them up and connect the device to the network. The router also has multiple SSID guest networks for devices to connect to if unable to connect to the main signal of the router. Each of the guest networks have their own security parameters in order to ensure a secure connection between the device and the network, as well as access restrictions so that the guest network connection cannot interfere with other guest networks or the main network or damage the security parameters of them.

The router also features an impressive amount of memory and performance based on its technical specifications. The router has 8MB of flash memory and 64 MB of actual RAM memory installed within. This helps guarantee fast and consistent connections to and from the router and allows it to handle multiple connections and interactions with the router. With a great amount of flash and RAM memory, the router is able to execute functions faster and help establish and maintain connections with multiple devices at once without tremendous pressure or damage to the router or the network traffic. The router also features 5 access points from it, 1 WAN and 4 LAN Gigabit Ethernet Ports. With these multiple ports open, multiple devices can be directly connected with the router and have full access to its security protocols and memory specs which helps execute functions and communication throughout the network much faster and securely.

The security features of the router as well is admirable and is significant towards the overall performance and reliability of the router to the network. The router features three levels of security protocols for wireless connections. The security protocols offered by the router are WPA, WPA2-PSK, and both 128-bit and 64-bit WEP. Both WPA and WPA2 are now standard security protocols for routers currently, but with additional security from WEP, the connection becomes more secure and protected from outside influences. The router also features pre-installed and active SPI and NAT firewalls. These firewalls help ensure that only certain connections are made and prevent outside influences upon the router that may be malicious in nature. Coupled with the firewall programs of the devices that are connected to the router within the network, the network and the devices connected, are granted better security and are ensured secure and reliable connections. Additionally, it should be noted that the router also advertises that it was built in programs and hardware which help include protocols that function as DoS attack prevention. With this added level of security, the router is better prepared for malicious attack from outside influences and able to maintain and secure network traffic within the network throughout the router. Overall, the security protocols and features of the router help make the Netgear router be more resilient to outside traffic and intrusion and maintain network traffic to make it more secure and reliable between connections of devices.

Overall, the NETGEAR N750 Wireless Dual Band Gigabit router is a sturdy, secure, and reliable router that is very useful within my network and helps provide a secure and reliable network environment for all devices connected. With the number of ports available to the router, multiple devices can have direct connection with the router and can utilize the rest of its built in features faster. The amount of memory and strength in broadcast signal, allows for a multitude of devices to connect both locally and wirelessly within range and allow their connection to the network to be fast and reliable with lower chances of overflow and traffic buildup or packet loss. The security protocols and features enabled within the router allow the network connections through the router to be more secure and for the correct packets and information to be sent through. With the WPA/WPA2 and WEP security protocols, wireless connections are granted an additional layer of security that can help prevent malicious intrusions from outside influences and can help aid the prevention in DoS attacks as well as brute force attacks upon the network. With all the security features within the router, all devices in the network can be guaranteed a safer and reliable connection to the router and other devices within the network.

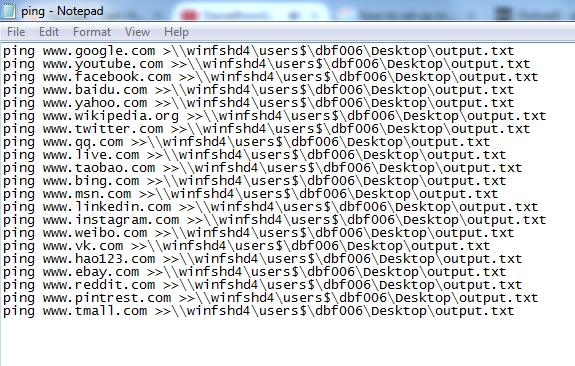
**Ping Mapping and Results:**

In order to better gauge and understand how devices connect and interact with networks, it must be observed and understood how the IP address changes during a ping commend to the network, and where the IP address comes from. By observing a trend of where the IP address sent from the network as a result of a ping command to it, one can see how a large and diverse network of a particular enterprise can give varying results and addresses back to the client. This demonstrates how dynamic the network is of particular companies and how they can handle network traffic by diversifying the information sent to and from the network across its multiple centers.

In order to conduct this experiment, 21 sites were chosen from [www.alexa.com](http://www.alexa.com) among the list of the top 500 sites visited globally. These sites included, [www.google.com](http://www.google.com), [www.youtube.com](http://www.youtube.com), [www.facebook.com](http://www.facebook.com), and [www.yahoo.com](http://www.yahoo.com), among many others.

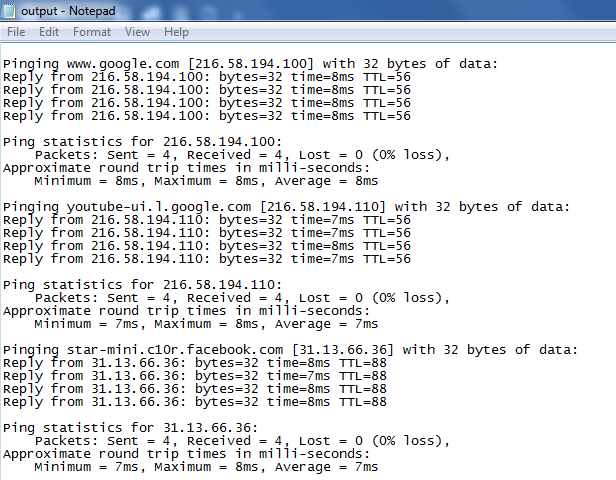
To detect the IP addresses sent from the sites and help find where they are geographically located, a mass ping command had to made. By pinging the sites in mass, the results can be received faster and analyzed quickly than if it were to be done one by one. In order to do this command, a .bat file had to be made for the host system. The .bat file was composed in Notepad and consisted of commands that required the site to be pinged and for the output to be sent to a text file so it could be read and analyzed. Figure 1.1 helps demonstrate what the code of the .bat file looked like.

**Figure 1.1**



After the .bat file was executed, the sites were pinged with information sent from the host system to the network servers of the sites. The sites were able to receive the packets and responded by sending back packets from their own IP address. A text document was created as a result of the .bat program which further details the response from the sites and the IP address sent (Figure 1.2).

**Figure 1.2**

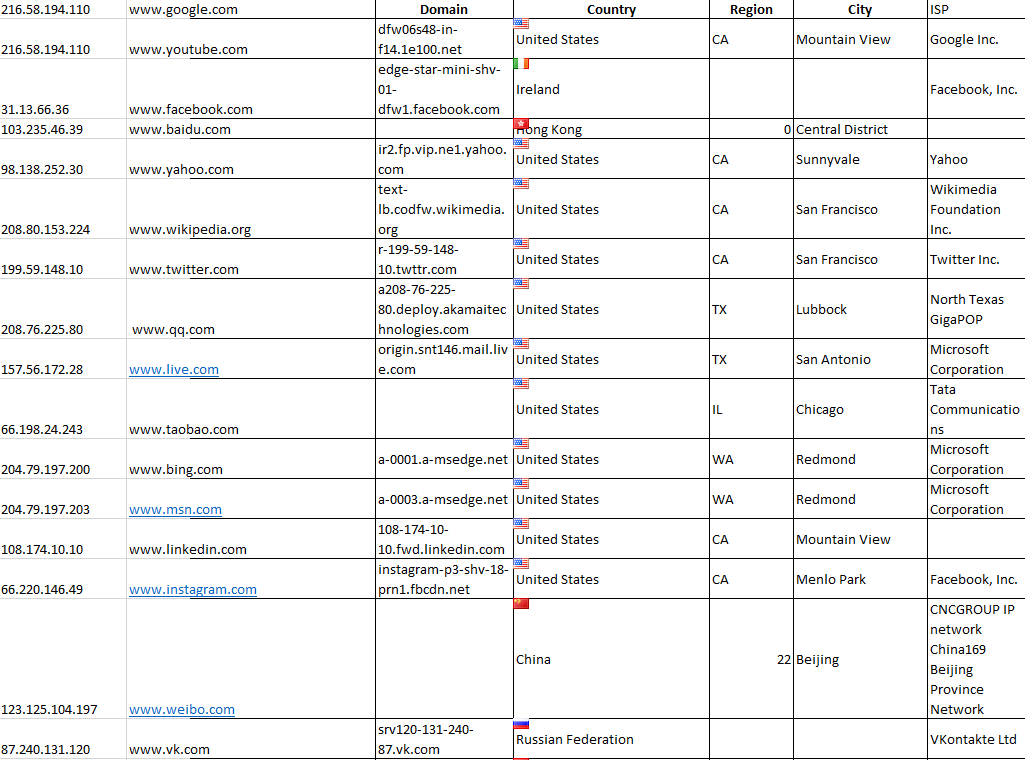


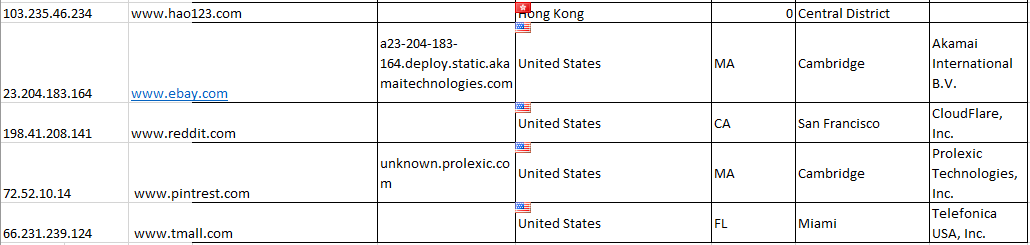
The IP addresses gathered from the output text file created by the .bat program, is then inserted within a bulk IP address geographic locator. The locator is a php program that is openly available online, called IP bulk lookup tool. The toll takes in the input of multiple IP addresses and then geo-locates the source of the IP address, and helps list the domain site of the IP, the country, state, and city of the server which broadcasts the IP address. These results are then gathered and put into an excel file in order to properly display the results of the tool.

The results of the ping experiment are separated into 3 instances with a time span of 20 minutes apart in order to detect changes in IP addresses from the sites. A change in IP addresses can be observed in some cases and can be utilized to help understand the makeup of the network of these sites and help understand how it can be utilized to aide network traffic from site-to-site.

The first batch of results of the ping experiment shows the initial set of IP addresses of the sites that were pinged. These results will be used in comparison to the other ping results to help detect any changes in location of IP address. The results (Figure 1.3) reveal that both Google and YouTube shared the same IP address, domain, and server location. This is possibly due to Google’s acquisition and ownership of YouTube, which helps explain why the results are the same. Facebook’s IP originates from Ireland which is unique for the America-based social media company. This can possibly have explained due to the technology boom in Ireland and how several businesses have invested and built data centers and remote offices so as to take advantage of tax benefits and workforce solutions in Ireland. The foreign-based sites do broadcast an IP that is within the country of origin for the sites. These results will serve as the control group for the rest of the results and used to compare to detect any changes in location or IP address broadcasted.

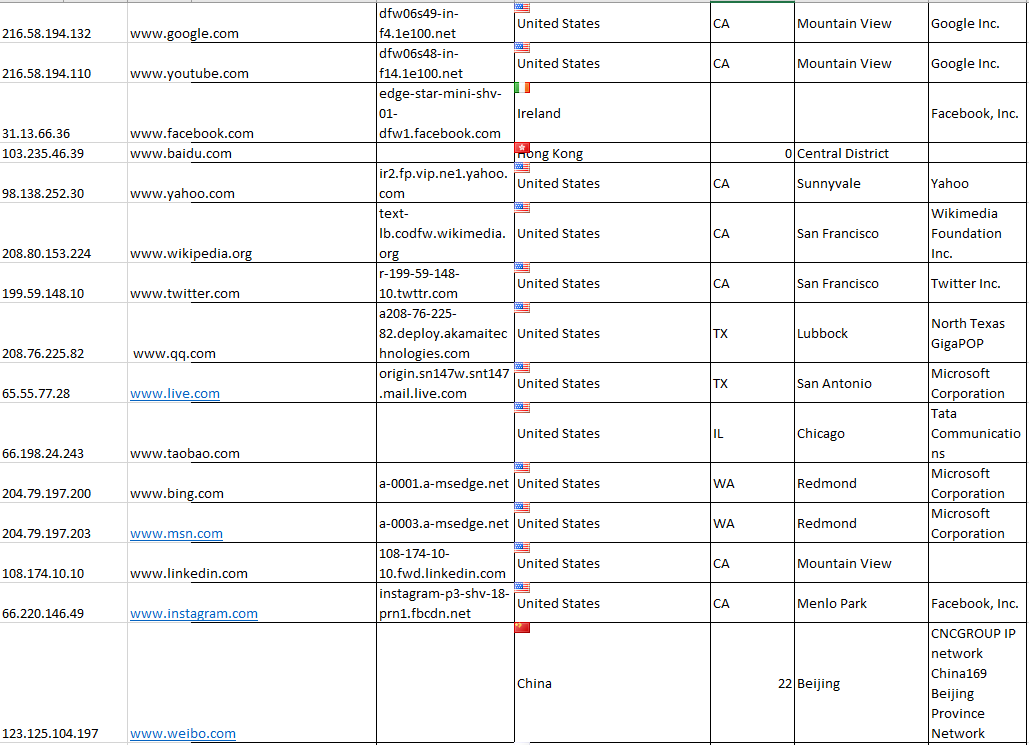
**Figure 1.3**

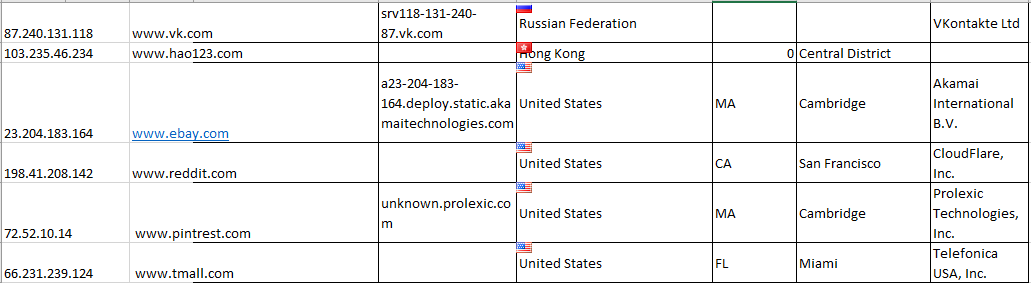




The second batch of results do detail the changes made in IP addresses and location of the source of the IP address. Some sites did broadcast a different IP address over the span of 20 minutes, while a majority broadcasted the same IP address (Figure 1.4). The geolocation is the same but some domains have been changed and the IP addresses as well. The IP addresses and domains of Google, QQ, VK, and Reddit sites did change over the span of 20 minutes. This change in IP address helps demonstrate the dynamic and ever changing nature of the network servers of these sites.

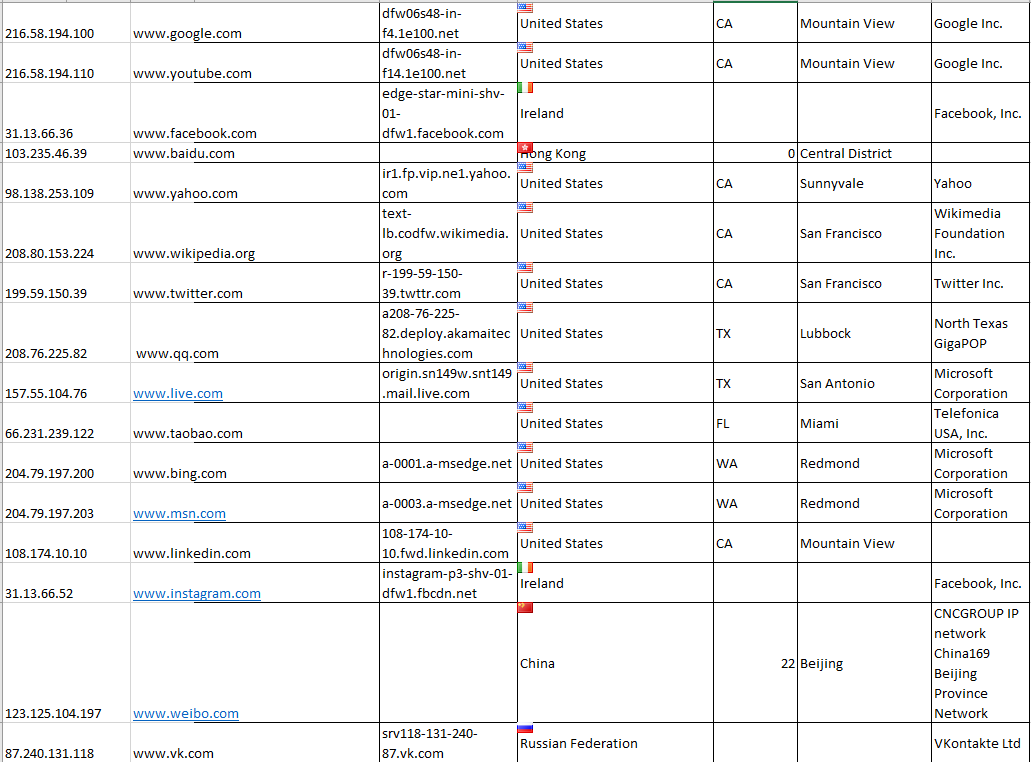
**Figure 1.4**

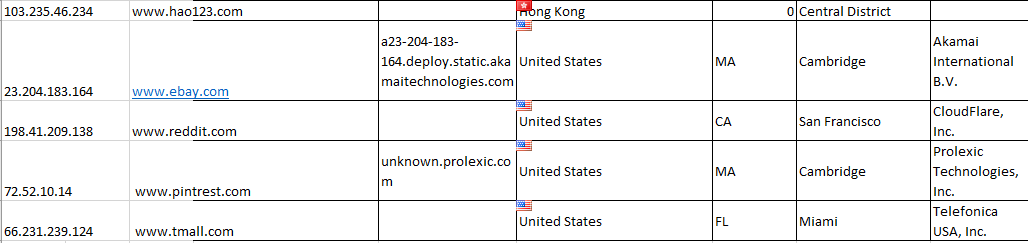




The third and last batch of results of the ping experiment further demonstrates the change in IP address and domain of the site. Figure 1.5 shows how the ping results of the experiment further changes and help display how dynamic and ever-changing the networks are for the sites. In this instance, the sites that changed domains and IP addresses are; Google, Yahoo, Twitter, Live, Taobao, Instagram, and Reddit. Like the previous instance, Google and Reddit were able to change their IP addresses, but now with more sites changing their IP addresses, it can be concluded that over greater periods of time, the IP addresses of the sites will completely change and be entirely different from the IP addresses sent prior. This further demonstrates the dynamic nature of these sites and how their servers are able to broadcast multiple signals.

**Figure 1.5**





What can be gathered from these results is that various enterprises are able to broadcast and send packets from various IP addresses in order to meet the high demands in information requested and send from users. The ability to have their servers dynamically change and host various domains and IP addresses can be utilized to better handle network traffic. The dynamic nature is helpful in handling in network traffic because, if a multitude of users are connecting to the servers and requesting and sending information to them, multiple IP addresses and the ability to dynamically change them, can assign various IP addresses to address each user and to handle the traffic through that particular connection. With multiple connection lines throughout the network, the traffic becomes more stream-line and manageable and less congested. With this advantage, these sites are able to meet the needs of their multiple users and able to streamline content to their clients. Overall this helps the business grow and meet the needs of their clients and helps grow their brand and reliability and integrity of it.

**Man in the Middle Attack:**

A Man in the Middle Attack was orchestrated and executed within a virtual environment to help understand the network infrastructure of an FTP server and a client machine, and how the connection between the two can be exploited by outside forces.

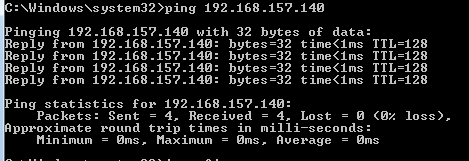
In order to commence the attack, a Windows 2012 Server virtual machine was created and within it, configured for FTP. The FTP site / server was made where the FTP site enabled access to a file within the Documents section of the Server computer, labeled TEST.txt (Figure 1.6). Once the FTP site was created, the firewall was turned off in order to allow a connection between the server and client virtual machines. With the firewall off, the server was ready to be connected and accessed by the client machine.

**Figure 1.6**



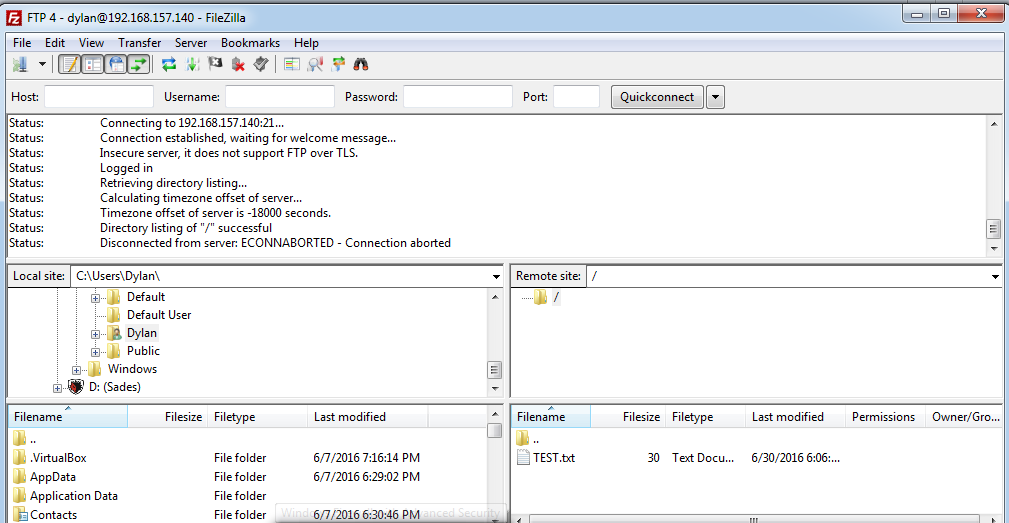
The client machine was a Windows 7 virtual machine, which has been used in prior experiments. In order to help connect to the FTP server, the client machine used a FileZilla client in order to directly connect to the IP address and user account of the FRP server. Additionally, in order to communicate and connect to the FTP server, the client’s firewall was also disabled in order for the two virtual machines to connect. The client machine was also tested through a ping command in order to test if a connection could be made from the client to the server (Figure 1.7).

**Figure 1.7**



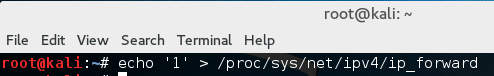
Through the FileZilla client, the client machine was able to directly connect to the host account of the FTP server and able to access the text file within the server (Figure 1.8). This successful connection through the FileZilla client demonstrates that the client machine is currently connected directly to the FTP server and will receive any information sent from it and vice versa. With the client and server finally connected, the Man in the Middle Attack could be then commenced between the two from the attacker machine.

**Figure 1.8**



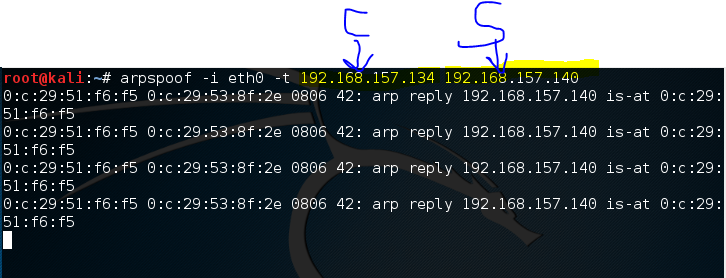
The attacking machine is a Kali Linux virtual machine with multiple programs and security suites that can be utilized to exploit various connections and other victim vulnerabilities and openings. To start the Man in the Middle attack, the attacker machine must utilize arpspoof suite in order to simulate the communication of the client to the server and vice versa, in order to implant the attacker machine within the line of communication between the two machines. In order to utilize the arpspoof suite and simulate the connection between the client and server, the native port of the attacker machine must be changed to port 1 in order to connect and monitor the connection of the client and server (Figure 1.9).

**Figure 1.9**

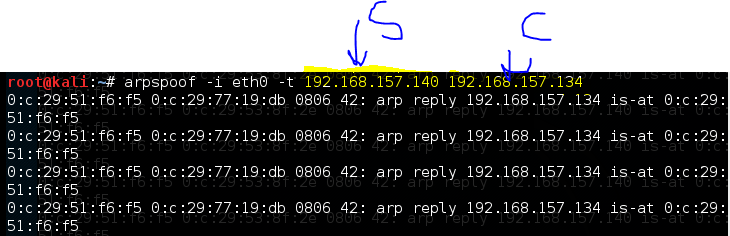


The first stage of the arpspoof stage of the attack is to mimic the connection of the client to the server and to spoof the packets sent between the two machines. The command for this attack is: arpspoof -i eth0 -t <client IP> <server IP>. With the execution of this command, the attacking machine mimics the signal of the client to the server and spoofs the packets sent between the two without the acknowledge of the two machines. The server machine is tricked to believe that the attacking machine is part of the network and represents the client machines, so as a result the server sends packets to the attacking machine thinking it is receiving packets and information from the client machine. Figure 1.10 helps demonstrate the command and the spoofing of the packets sent over the two machines. The “C” represents for the client IP address, “S” represents the server IP address.

**Figure 1.10**



Simultaneously, another console window is opened and a similar command is issued. This time the command simulates the connection from the server to the client machine. By doing this command and spoofing the packets sent from the server to the client, the client machine is fooled that the attacking machine is the server machine and receives packets sent back in response to the server. Figure 1.11 demonstrates how this spoofing attack is made and how the client sends packets to the attacking machine, thinking it is the server machine.

**Figure 1.11**

Now with the packets being spoofed and the connection of the server and client intercepted unknowingly by the attacking machine. The packets can be interpreted and information can be extracted into any means necessary. For the sake of the experiment, the images being viewed by the client computer can be streamlined and viewed by the attacking machine.

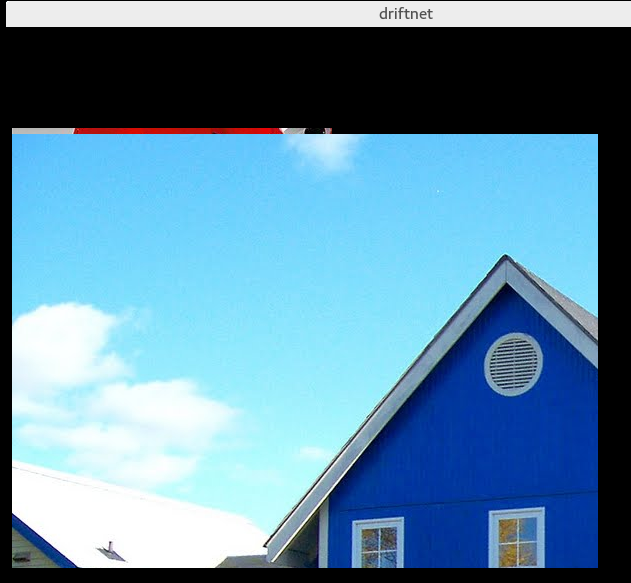
In order to view the images being viewed by the client machine, the packets sent between the machines is interpreted and rendered by the driftnet command. Driftnet instantiates and renders the image information within the packets of the network between the machines. Figure 1.12 lists the command executed in the attacking machine in order to execute the driftnet command.

**Figure 1.12**

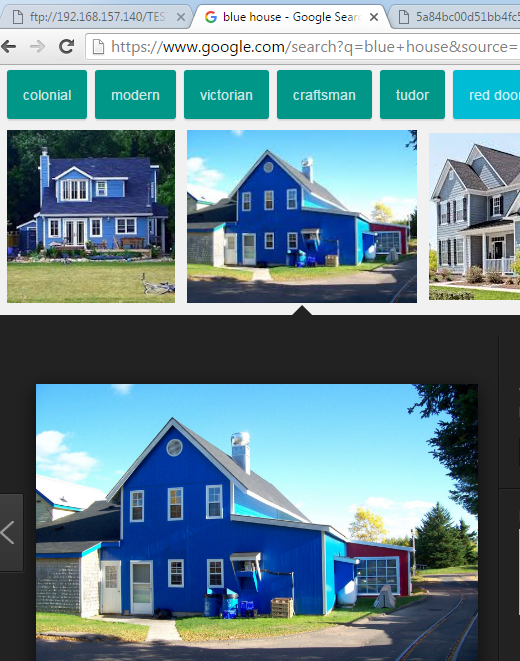


With the execution of the driftnet command, the images viewed by the client machine is rendered and made viewable in a separate window. In order to help display the process of this command and the results, screenshots are made both from the client machine and the attacker machine. Figures 1.13, 1.15 and 1.18 demonstrate the results of the driftnet command within the attacking machine. Figures 1.14, 1.16 and 1.17 demonstrate what is viewed within the client machine and essentially sent to the driftnet console window of the attacking machine.

**Figure 1.13**



**Figure 1.14**



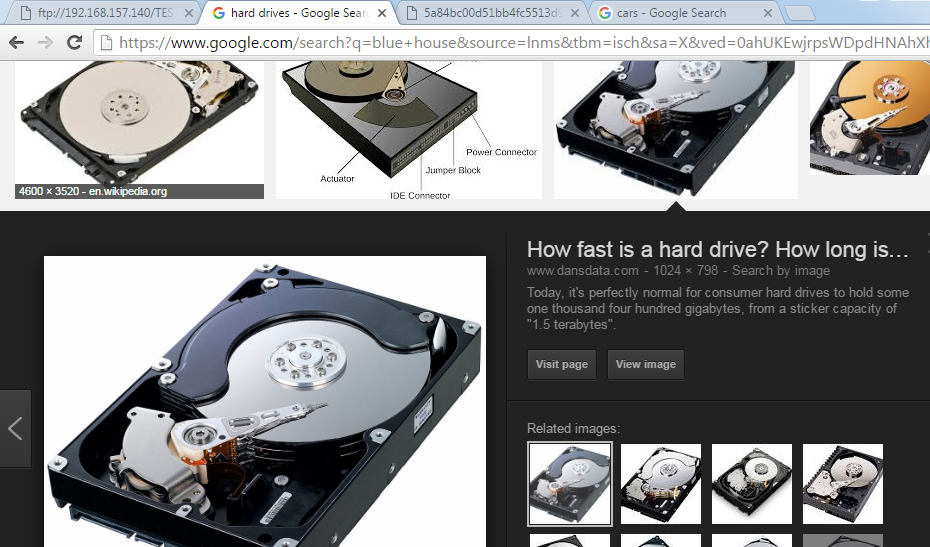
**Figure 1.15**



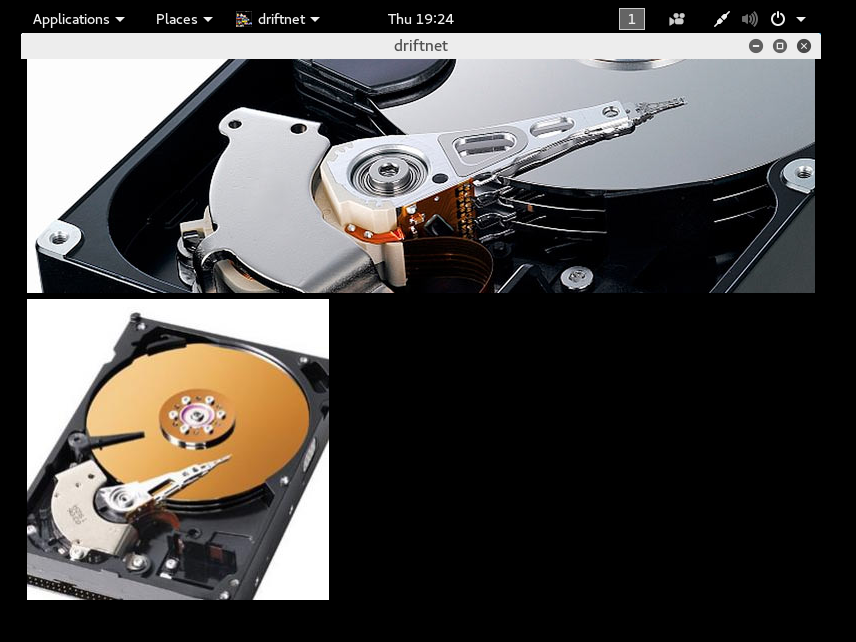
**Figure 1.16**



**Figure 1.17**



**Figure 1.18**



What can be gathered from this attack is how a network can be established and manipulated in order for an outside machine to connect and obtain information from the network. By establishing a simple FTP network connection between a client and server, an observation can be made towards an understand of not only how virtual machines communicate with each other, but how a server is made and how a client machine can connect and send information to and from the server. The arpspoofing helps simulate the signals of both machines and demonstrates how an outside machine can simulate these signals and fool the machines into thinking they are discussing with each other uninterrupted and for information to be intercepted by the attacking machine. By mimicking the signals, the machines send the packets to the attacker machine and information is sent without either the server or client knowing that a third machine connected. With the driftnet, a visual demonstration can be made how the information intercepted between the machines can be utilized to understand and manipulate it accordingly. By having it display and intercept images viewed by the client machine, it can be demonstrated how vulnerable the client is and how information can be easily accessed and used by the attacker machine. If the situation was different and the client were to be accessing sensitive information or be viewing information regarding personal accounts or even personal images, the attacking machine can access that information easily through the attack and view the exact same thing that the client is.

**Conclusion:**

In conclusion, the strength of a network depends on all the components involved, and how they all work in order to provide a strong and secure connection between devices / machines. A network is a diverse connection of devices / machines to which each is actively communicating with each other and depends on each other for information to be sent and received accordingly. The health and strength of a network can be gauged on multiple levels, including the number of users connected, the network traffic across the network and how it deals with that traffic, the security of the connections throughout the network, and how dynamic it can be. With these factors and more, it can be observed and recorded, the overall health of the network and possibly used in order to improve or attack the network, depending of the observer.

With the analysis and comparison of SD-WAN and MPLS, an observation can be made of what network solutions are made available and how they affect the overall health and performance of the network. With MPLS, the network directly connects through the switches and are able to quickly and seamlessly access information from users and servers throughout the connection. With this network solution, a faster and seamless connection can be made between machines and information can be directly sent and received across the network. With SD-WAN, the network becomes more software dependable and allows for the connections between users to be made easily and securely through the use of encrypted tunnels overlaying the hardware of the network and allowing only certain users with certain software requirements and credentials to have access across the network. With these network solutions, a comparison can be made and related towards a real world scenario where the network solutions can be fully executed within.

The analysis of the personal router allows a more in depth observation to be made on the overall health of the personal / local network. By observing and understanding the internal makeup of the router, a more complete analysis can be made on the local network. With its multiple ports, the Netgear router is able to directly connect to multiple devices and allow them to directly take advantage of the security features of the router. With its high memory and levels of encryption and security protocols, even wireless connections can be made securely and seamlessly. Altogether, with the security protocols and makeup of the router, coupled with the memory and broadcasting strength of the router, a more secure and complete local network can be made with the devices connected.

The ping test revealed on how businesses can dynamically change their IP address and domain in order to meet the ever amounting number of users connected to their network and the information requested and sent. The changing IP addresses and domains of the sites demonstrated how dynamic and ever changing the servers are. With this dynamic nature, more users can be connected and sent / receive information from the servers accordingly without mass network traffic or packets dropped as a result to congestion. It also gives a glimpse and understanding of the security of the networks. By dynamically assigning various IP addresses to the user in response to the user’s request, a connection can be made that is unique to the user and to the timeframe to which the connection is made. If an attack were to be made regarding the IP addresses of the client and the website’s server, it would be increasingly difficult since it is always changing. Thus, as a result the web sites provide a diverse and secure connection in order to meet the needs of its multitude of users it connects with.

The Man in the Middle Attack demonstrated how a connection between a client and server within a network can be accessed and manipulated by outside machines, without the detection from either the server or the client. The attack was made through a direct connection between the server and the client and demonstrated a FTP network between the two, which would be normally heavily secured, depending on the server and client involved. By mimicking the signals for the client and server, the attacker machine is able to trick the target machines into thinking that it is the destination machine for the packets sent and received. With the packets intercepted by the attacking machine, multiple commands can be made in order to interpret and decipher the information within the packets. In this experiment, the information within the intercepted packets was utilized in order to interpret and render images viewed by the client machine. Although no personal or incriminating images were intercepted in this experiment, it can be demonstrated how the packets intercepted can be interpreted and used to view sensitive information from the client and server. This is a huge security exploit and can be used in a multitude of ways to where the victim machines can be effected in a multitude of ways.

Overall, these experiments and analyses help detail and demonstrate the overall importance and strength of a network in relation to the devices involved and the components available and which security measures taken. With a greater number of users connected, an appropriate network solution must be chosen to where the connections are encrypted and made secure, yet able to transfer information throughout the network quickly and correctly. Additionally, the network should have hardware that is able to directly connect devices whether they are physically connected or wirelessly and enable the connections to be made reliably and securely throughout the network. By having a dynamic connection, similar to those that can be observed from ping results to major websites, multiple users can be connected and their information can be sent and received quickly and securely with less risk of network traffic congestion, packet loss, or outside influence. If the network to be compromised by an attacking computer, the attacker can mimic the signals of the server and the client and spoof information from the network without the knowledge of the machines involved. Altogether, the architecture and security of a network is very diverse and evolving according to the devices connected. With these experiments and analyses made in this report, one can have a better understanding of a network and how to possibly strengthen it or harm it accordingly, depending on the intention of the person.