Research Documentation

Secure Redundant Network

Aaron Morrissey

C00239014

Supervisor: James Egan

Contents

Abstract

A distributed hospital network is severely flawed and is showing signs of poor performance. I am asked to take on the role as a network engineer consultant to try and rectify this issue by providing better choices of protocols and technologies to be implement that I have learned about through research, testing and comparative analysis. The main priority must always be the security and integrity of the network. I researched and reviewed papers on past security failure incidents and flaws in protocols to gain a better understanding of the weak points within a network which allowed me to find a number of solutions.

Introduction

For this project I was asked to take on the role as a network engineer consultant for the purpose of improving an existing distributed hospital network. The network it seems contains many weaknesses and flaws such as weak LAN and WAN infrastructure, a lack of security, reliability, redundancy, controllability and fast connection resulting in very poor performance and quality of service. As a consultant my objective is to attain a better understanding of the various types of technologies and protocols than can be implemented within a network topology and from there compare and contrast them in terms of security, throughput, packet loss etc. in order to evaluate which is the best course of action when creating an overall better and highly improved network. However, even though having high standard values is ideal, the vital point of this document is focused on having a heavy emphasis on integrity/security methods and how they are to be implemented rather than other components such as delivery speed. An example of this is TCP versus UDP, UDP being made to be faster but at the same less reliable.

Comms & Network Protocols & Key Terms

In order to proceed with the creation of a virtual topology we must first learn, revise and study the numerous networking and routing protocols and to examine/test/compare the network traffic for each one of them in order to better determine which among them would be the better choice.

TCP

Transmission Control Protocol is used for communication and exchange of messages between numerous devices within a network and takes an approach that is more focused on reliability message delivery than it is on delivery speed.

UDP

User Datagram Protocol is quite similar to TCP in the sense that it is used to transmit data, that being said it differs in regards to where TCP is more focused on reliability, UDP is more focused on delivery speed, packets being sent and is more tolerant of packet loss.

IGP & EGP

Interior gateway protocols, as the name suggests, are protocols used inside a local network and only applies to the as far as the border router. Unlike its counterpart, Exterior gateway protocols are designed for exchanging routing information between two neighbouring hosts rather than internally.

Classful & Classless

A classful protocol is one that excludes the subnet mask when performing an update. This type of protocol focuses more on identifying whole networks instead of singular addresses and requires a greater amount of bandwidth due to it performing routing updates at regular intervals. Opposite of classful, a classless protocol is one that does include a subnet mask when commencing routing updates. The type of protocol has the ability to communicate with other devices that are located in separate networks and is more focused on transferring more in-depth information at much higher levels. Classless protocols also offer the benefit of less bandwidth used as it only performs updates when changes have been made.

RIP

Routing Information Protocol is responsible for determining which path a packet should be sent on by using a router routing table that is sent to every other connected router which is triggered every 30 seconds.

OSPF

Open Shortest Path First is a link-state (IGP) Interior Gateway Protocol (Mostly seen within a company's private LAN) and one of the worlds most used protocols, its main purpose is to navigate the best path from the source to the destination address prioritizing the shortest path first. It accomplishes this by maintaining a database of locally established networks and from there calculates a path based on the lowest cost and metric. [Source 2]

Autonomous System (AS)

An Autonomous System refers to a collection of devices (network) that all share the same IP-prefix and are governed by a single entity or organisation. The internet itself is made up of these autonomous systems and are connect through the use of the border gateway protocol.

BGP

Border Gateway Routing protocol is a dynamic routing protocol that connects the entire internet. A router that is using BGP contains a routing table and uses this information by looking at all the available paths it could travel and from there it calculates the best possible path to the destination by jumping from one autonomous system to another.

EIGRP

Enhanced Interior Routing Protocol is a more advanced version of IGRP and is used to automate routing decisions and configurations. It uses four different metrics to determine the best path to transmit packets, these being delay, reliability, load, and bandwidth.

MPLS

Multiprotocol Label Switching refers to data forwarding technology that increase's the speed and overall control of the flow of network traffic. This is accomplished by directing data through pathways based on labels rather than having to rely on routing table lookups at each stop.

QoS

Quality of Service defines certain technologies that function within a network with the goal of guaranteeing being able to run efficient high-priority applications as well as network traffic under limited capacity. In short, it is essentially responsible for reducing packet loss, latency, jitter as well as overseeing the control and management of the network's resources.

VPN

A Virtual Private Network is the process of creating a protected network connection when using a public network. They are used for their highly beneficial perks such as the level of integrity it offers a user by encrypting their internet traffic as well as protecting their identity.

IPsec

IPsec specify a group of protocols that's primary function is to achieve a high level of security at the IP layer for communications between devices and are often used in the creation of VPN's.

Tunnelling

Tunnels are utilized as a method for a user to securely transport data from one network to another, normally between private one, by first having the data encapsulated and sent over a public network.

VLAN's

VLAN's are the product of segmenting a Local Area Network into subnetworks that consist of a group of devices that are normally designed for different teams or departments allowing for a more structured topology.

VoIP

Voice Over Internet Protocol refers to a technology that offers the user the ability to make voice calls using broadband internet connection rather than having to rely on a normal phone line. A user can make calls directly from a computer with the addition of things such as host spots that allow a person to use VoIP wirelessly. [Source 5]

SNMP

To put it in general terms, Simple Network Management Protocol refers to a networking protocol that's main function is to monitor, obtain information and manage devices on a network.

Comparison of Communication & Routing protocols

TCP vs UDP

When discussing which protocol is the best choice to be implemented into a network, even knowing that the main priority of this specific network is security and redundancy, comparing them side by side still presents a challenge when determining which one is better suited to the job as each of them offer their own advantages but also their own individual short comings. In this case trying to determine what would the better option be, to allow TCP over UDP or the other way around when trying to develop a network with both LAN and WAN infrastructures, redundancy, increased security, faster connection, etc.

TCP is a communication protocol that takes a more reliable approach when it comes to the transmission of packets. It has the advantages of having an ordered reliable delivery system and being able to retransmit packets when it's been noticed that some have gone missing. It accomplishes this through a process known as the three-way-handshake, simply put, the source sends out a request to initiate communication with another device, the other device lets the source know its request has been acknowledged, the source receives the acknowledgment and a stable communication is created between the two. Thus, it's much better for cases where you need to download files, send emails or view webpages.

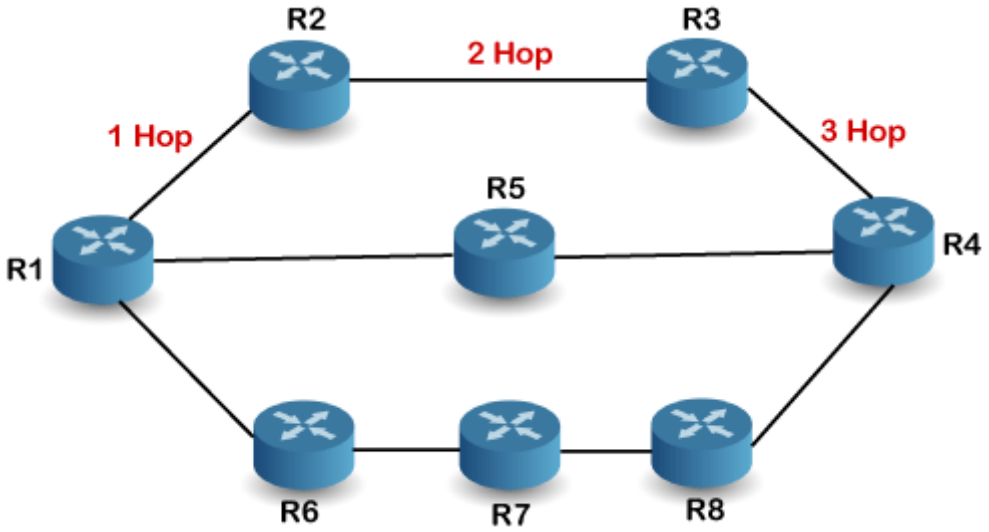
However, due to the steps TCP takes in order to ensure that reliability is established, it also means that a large amount of bandwidth within the network is being used up which isn't exactly ideal given that the hospital network is implementing real-time transmission protocols such as VoIP.

UDP on the other hand, as mentioned earlier, is much more focused around speed and data being continuously sent, delivering quality real-time communications, being much simpler as well as efficient to use and doesn't waste time with packet recovery or error checking.

Normally, if the network only wanted to be implementing services such as VoIP and SNMP (runs over UDP), the obvious solution would be to just go with UDP as its simpler, more efficient and produces less overhead, however, we also mean to implement services that run on TCP, not to mention that the document also states that there is a lack of redundancy and reliability so we must use both protocols in a healthy and optimal way.

OSPF vs RIP

RIP is an interior gateway distance vector routing protocol that, when transmitting packets, uses a hop count as its metric in order to determine the best path. Essentially, the hop count is the number of devices that the packets are transferred through from the source device to its destination (shorter the hop, better the path).



[Image 1]

RIP itself is easy to understand and configure and does not need to be updated every time the topology changes as it continually updates the full routing table every 30 seconds, however, it is only good for smaller networks. The hop count for RIP only allows for a max of 15 hops with anything over that being considered unreachable and due to the consistent router table updating every 30 seconds it causes bottlenecks and unnecessary waste of bandwidth.

OSPF is a classless interior routing protocol (carries the subnet mask in its updates) that's main purpose, similar to TCP, is to calculate the best (fastest in this case) path to a destination, however, this protocol is much more complex compared to TCP would be better suited to larger networks. Where TCP updates the contents routing tables every 30 seconds, OSPF multicasts any specific changes rather than the full routing table the moment they are noticed within the network.

In short, when determining between RIP and OSPF, OSPF is the better option that offers a number of significant features such as providing faster convergence time, updates any specific changes made within the network rather than the full table (efficiently using bandwidth), isn't limited to a number of hops like TCP (15 hops max), and is much more suited for larger networks and hierarchical organisations.

[Source 2][Source 7]

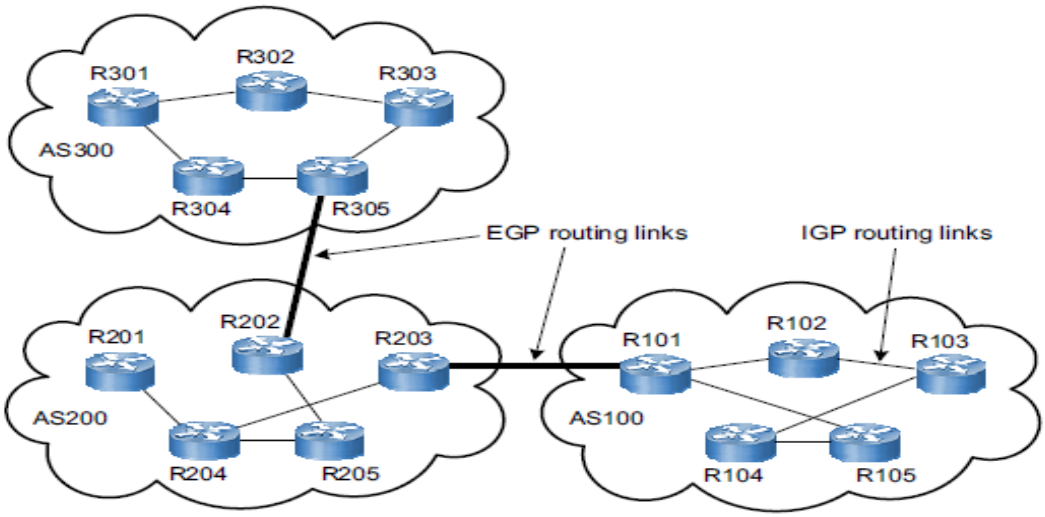
OSPF vs EIGRP

In regards to EIGRP, it is considered to be a classless hybrid protocol as it demonstrates certain characteristics seen in both link state and distance vector protocols (OSPF and RIP). It determines routing decisions by taking into consideration factors such as reliability, Maximum Transmission Unit, etc. with a default metric specifically focused on delay and bandwidth. Similar to OSPF, rather than sending an updated routing table at scheduled intervals, it only sends out the specific change to the network when it has been made, reducing the risk of bottling necking and freeing up bandwidth. Aside from a EIGRP router having its own routing table it also possesses a copy of every other routing table assigned to all other neighbouring router giving it a more in-depth view of the topology then the usual distance vector protocol. If, however, it is not possible to locate any route to a network it has learned from the table's it currently possesses, it will then initiate the process of sending queries out to all the routers until a suitable route can be found. Both protocols have a process where they send out "Hello" messages to neighbouring devices that basically function as a sort of heartbeat, broadcasting that it's still there. The difference being that after a certain time, if a router configured with OSPF doesn't hear that hello message after a certain time frame from another device it considers that neighbour device to be unavailable/dead, whereas with EIGRP it's the other way around where if the neighbours don't hear from it after a certain time, they consider it down.

When comparing EIGRP to all that was mentioned about OSPF earlier, it's clear to see that both are proficient at what they do, compared to where RIP falls off by being suited to smaller networks, and are both preferable for larger networks. That being said, in the case of which one is better it depends on what statistics and technologies you wish to prioritize, for example EIGRP has got OSPF beat as more in-depth research shows that it provides improved bandwidth control by looking at how much is available when calculating the rate at which it transmits updates, increased utilization of both memory and CPU and faster convergence time. On the other OSPF is consider the better choice when you wish for a network to be hosted in either a data-centre or cloud-based, has a much higher rate of scalability and a better option when implementing MPLS as it has traffic engineering

support. In this case the only way that a choice can be made between the two is after a comparison has been made when combining both of them with an EGP such as BGP.

[Source 10][Source 12]



[Image 2]

BGP (External Gateway Protocol) combined with IGP's

So far, we've talked about three types of interior gateway protocols, RIP, OSPF and EIGRP and how they are used to transmit and exchange data through routers within a single autonomous system. In this topology we also want to implement BGP in order to connect the various autonomous systems that will consist of four hospital sites. The main objective here is to take the previous IGP's that were looked at (RIP, OSPF, EIGRP) and combine them with BGP to see which combination is best suited to be the networks routing protocol by monitoring their performance based on certain statics such as:

Convergence time

- Convergence time refers to how quickly a group of routers can reach a state of convergence after a change has been made within a topology.
- When measuring the convergence time, EIGRP on its own displays the fastest convergence time, however, when combined with BGP it's is more or less the same value when compared with OSPF/BGP and RIP/BGP making it quite difficult to choose the best one based on convergence time alone.

Throughput

- Throughput, in general terms, is the measurement of units (or in this case packets) that are able to pass through a process within a certain time period. The greater the quantity of packets that have passed through, the more efficient the process.
- The throughput measurements indicate that the OSPF/BGP protocol delivers the highest value of packet transmission, which itself is surprising as my expectations

were for EIGRP/BGP protocol to offer the highest transmission but in reality, it only hosts the second.

Packet Loss

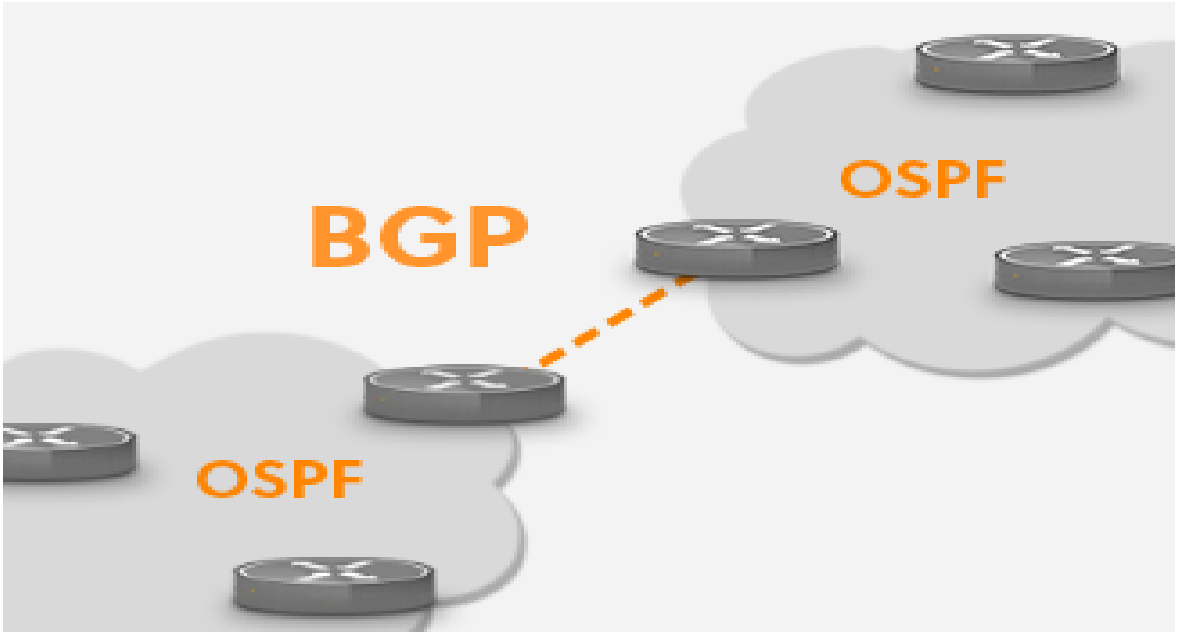
- Packet loss, as the name suggests, occurs when packets of data that are being transmitted across a network fail to reach their destination. The fewer packets lost each transmission, the better.
- When looking at the rate of packet loss between the protocols, OSPF/BGP boasts the best value of packet loss when compared to the others.

Jitter

- Jitter is an event within a network that normally occurs due to congestion and route changes and results in there being a time delay during the process of sending data packets, especially in regards to audio and video quality.
- When comparing the jitter measurements of the protocols to one another, there isn't really that big of a difference with them all being relatively decent, that being said, OSPF/BGP has a slightly better value than the others.

In conclusion it seems that OSPF in combination with BGP offers the best jitter, convergence, packet, throughput value and overall quality of service when compared to all the other protocols, thus this will be the choice of protocol to be implemented into our network resulting in an overall higher quality of service especially in regards to VoIP.

[Source 1] [Source 2][Source 8][Source 9][Source 11]



[Image 3]

Security & Flaws

So far, we have discussed the types of routing protocols that we wish to be implemented into the network, covering which ones are considered the best choice and why they should be used, however, we have yet to discuss the main priority of this project, that being the field of security. With our protocols chosen and the topology of the network more or less figured out, the question must be asked “how to guarantee, provide and maintain a high level of security and integrity for this network?”. In order to accomplish this, we must look at and examine a modern-day networks security standards, the most common types of attacks and flaws they suffer from, specific short-comings of our own network in regards to technologies such as BGP or SNMP, research similar cases related to our own network and research final strategies and practices that can be implemented in order to overcome these flaws and overall provide a more secure network.

Network Security Standards today

In recent years the crafting and complexity of organisational networks has become monstrous in size (especially given the circumstances of an increased level of distributed workforce the past two years) as the field of technology continues to be ever evolving, bringing with it new strategies and more efficient practices for building networks while at the same time presenting more opportunities for new and dangerous methods of attacks to be discovered.

In short, it is simply not enough anymore for organisations to relay on simple methods such as applying a firewall or only configuring security for edge devices, that are the bridge-point between a secure and untrusted network, doing so only results in a single point of failure for the network. In fact, as radical as it might sound, a network admin should be living with the mindset that even when protective measurements have been implemented, there is still a point of weakness yet to be discovered and exploited.

Today, organisations should have numerous layers of security before any outside traffic can enter their secure network, ACL’s (Access Control List’s) being applied to devices throughout the network determining what type of traffic gets passed through what ingress and egress points, disabling unused ports or interfaces that might be used as a point of entry, implementation of two-way-authentication and encryption of communication lines so as to try mitigating man-in-the-middle attacks etc. This type of awareness shouldn’t just be seen from an external threat point of view, in fact, in recent years there has been an increase of internal threats whether it be caused by social engineering or employees with malicious intent. Circumstance’s such as these should be more than enough to motivate network admins to implement practices such as restricting the accessibility of any device to users, utilization of authenticating access determined by a user’s clearance level through the instalment of Privilege levels or Role-based CLI’s, records and accounts of activities that occurred during device access and auditing purposes etc. This is but a fraction of the measure’s organisations today takes in order to ensure the safety and integrity of their

network, if not at the very least prepare it as much as possible for when, not if, attacks occur.

In conclusion, when asked to explain the security standards of an organisations network in modern times, it can essentially be seen as a complex and thought-out structure, one with numerous safeguards stacked on top of another, thus, the desired outcome of this project is to establish a high level of integrity and security for our network by applying as many safe guards as we can while at the same time trying to impede and limit as much operational backlog as possible.

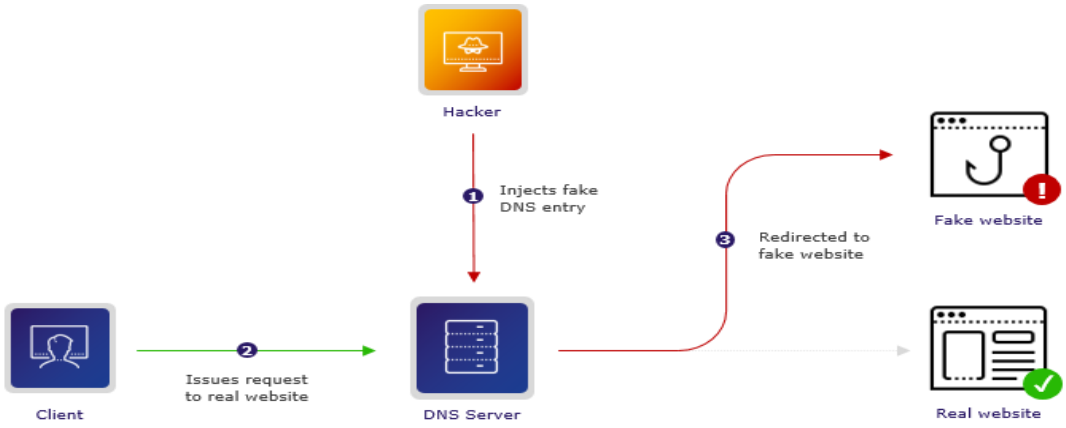
Common attacks/flaws

As mentioned earlier, in today's time's the threat and risk of network attacks and breaches are more prevalent than they ever have been. Companies and organisations are exposed on a daily basis to malefactors, both external and internal, with the intent of stealing, harming or blackmailing through creative and malicious practices. Being able identify and pin-point these specific attacks provide a network administrator the opportunity to recognizes what the attack is doing, what vulnerability it took advantage of within the network in the first place and how to mitigate and prevent future occurrences. Some of the most frequent and popular attacks seen in our current climate consist of variant redirection and man-in-middle attacks such as:

- Phishing **(Subject to change)** - this sort of attack is directly aimed at trying to attain a victims user data such as their usernames/passwords, banking information, credit card numbers etc. This is accomplished by an attacker crafting a fraudulent (but genuine looking) text message or email containing a malicious link and sending it the victim. The victim is tricked into clicking the link, thinking it genuine, and results in malware being installed, credentials being stolen by the user entering them into a fake login page etc. One of the reasons why this method is so often used is because it is a type of social engineering attack meaning that the security breach will always be the fault of human error and in an organisation with a larger workforce, the probability of it occurring skyrockets. There is also a variant of this sort of attack called Spear phishing, it essentially sets out to accomplish the same task but the difference being that the attacker crafts the message to the specific organisation, job or victim that they are targeting, appearing much more believable to the user. **[**Source 15]

- DNS Poisoning (Spoofing) – very similar to the attack described above, this is a type of attack that focuses on redirecting traffic towards malicious phishing websites and fake servers. The difference being, where phishing relies mostly on requiring its victims being redirected to a website by clicking on a link, DNS poisoning cuts this requirement out by impersonating a legitimate website that the user would visit by themselves. It accomplishes this by the process of spoofing a valid DNS and tampering with its directory so that it points the domain name that a user enters to

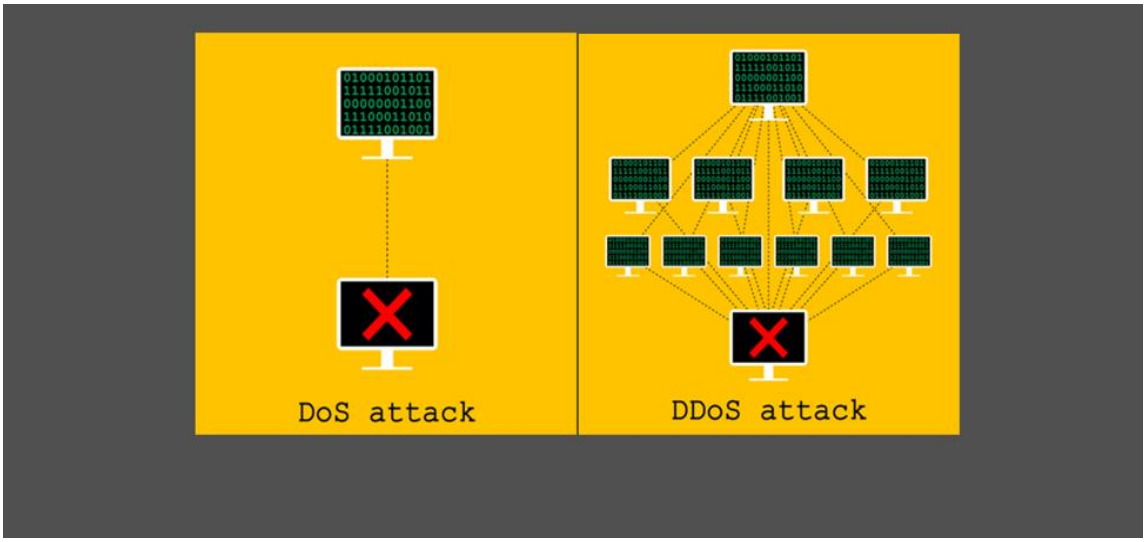
the false website. These types of attacks can be particularly aggravating to deal with as if done right it can be near impossible to tell the difference between the authentic and fake web page. [Source 16]



[Image 4]

Not all attacks these days are solely based on attaining a person's private data, but rather to simply inhibit a person or organisation from gaining access to a site or network.

- Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) attacks – as the name might suggest, the whole purpose of these types of attacks is to make it impossible of a user to gain access to a machine or network in various ways, whether it be flooding a system with response's so that it is inevitably brought down by being unable to process so much traffic at once or tampering with configurations so that the so-called updated path to a site leads to a dead end.



[Image 5]

Specific network shortcomings

In the previous paragraph we discussed attacks that are seen by organisations more often in today's times on a daily basis, which we will need to defend against within our own network. However, we also need to dissect and examine more unique flaws and vulnerabilities that effect this specific network which, if not fortified against, could be taken advantage of and used against us.

BGP

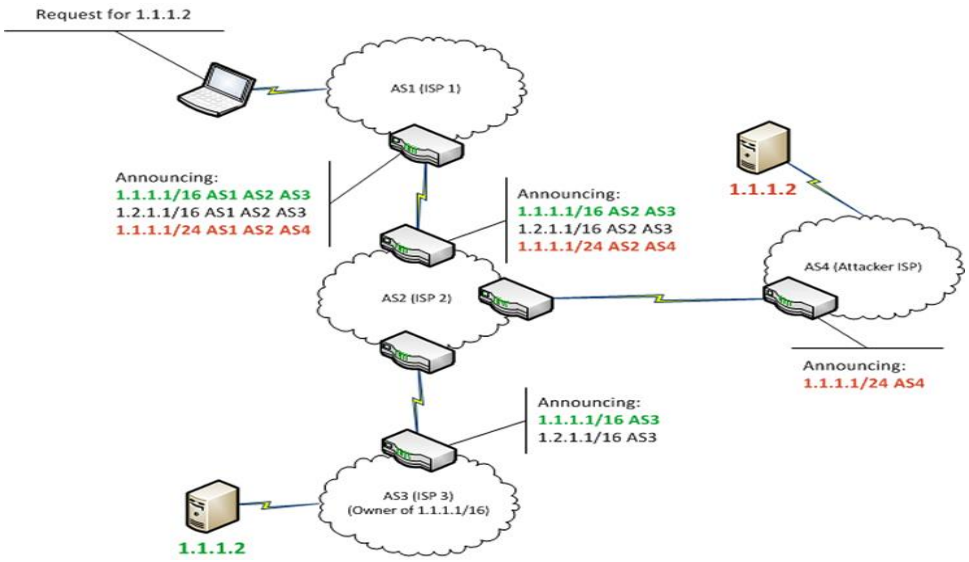
As was mentioned earlier, we wish to implement the BGP routing protocol as it allows for communication by enabling the internet to exchange routing information between autonomous systems, however, BGP has been known to suffer from a number of flaws and attacks and has caused some memorable incidents over the years, both intentional and intentional. These flaws and attacks consist of:

- AS-Path Poisoning – this type of flaw exploits the BGP's loop-prevention mechanism into denying traffic over a specific autonomous system. How an attacker might go about this is to start by adding both their own and the victims AS and AS Identifiers, the ASN (Autonomous System Number, used to identify ASs over the internet) and the AS Prefix length (same principle as ASN), to a BGP announcement (when a BGP device advertises its information to neighbouring BGP devices). This cause's the effect of making it seem like the victim's autonomous system was already reached, showing it to look like a loop in the AS-Path, so when the BGP announcement actually arrives at the AS it is then dropped as well as every single announcement afterwards if it contains the victims AS information resulting in no traffic being able to be routed over it.

- BGP Hijacking – this kind of attack involves a hijacker using their own AS in a malicious way in order to hijack a victims incoming traffic by redirecting it towards them, and in doing so, allowing the hijacker to completely take control of the traffic and the data within for whatever purpose they see fit before dropping it or deciding to continue forwarding it on to the victim. An attacker accomplishes this by either launching a sub prefix attack by making an announcement that will originate a more specific IP prefix (BGP prefers more specific routes) rather than the victim's prefix resulting in the victim's traffic being routed to the attacker or they can make an announcement that claims it has discovered a shorter path (a fake path) to the original destination and routing the traffic to the attacker.

- BGP Interception attack – this type of attack is similar to BGP hijacking but harder to detect and far more dangerous. Where both the methods of hijacking can be detected by a victim as the traffic itself has been disrupted and the volume of missing packets would usually go noticed, interception strives to make it seem like there has been no disruption within the network by establishing a valid path to the destination (victim) while simultaneously forwarding it through the attackers AS first. However, due to BGP preferring shorter paths, the reason it chose the attackers fake path in the first place, the traffic could be routed back to the attacker again initiating

a loop and could result in the traffic never reaching the victim. Unfortunately, as was mentioned earlier this can be undone with BGP's loop prevention mechanism with the cost of capturing a smaller percentage of the overall traffic.



[Image 6]

SNMP

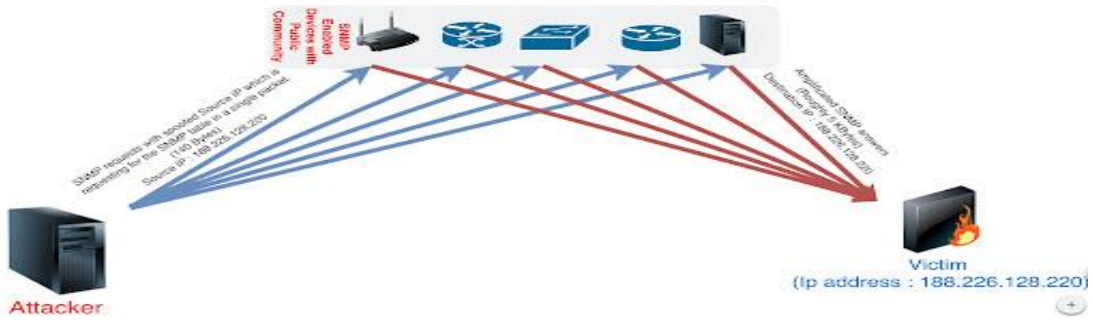
Simple Network Management Protocol, as was mentioned above, is a protocol that's main purpose is to manage and monitor devices on a network. However, when we take a more in-depth look it is clear to see that this protocol has numerous amounts of benefits to offer a network. It can provide an admin with a comprehensive list of information such as the faults and malfunctions that have occurred on system devices, the current status and well-being of devices and has the ability to remotely modify settings and configurations on an exorbitant number of devices connected to the network no matter their type or manufacturer as the protocol itself is supported on a large variety of hardware, all of this being capable from a single interface. It's able to accomplish these functions through the use of key components such as:

- SNMP Manager – used as a management station that runs SNMP management applications on various operating systems while actively making requests to SNMP agents to send updates.

- SNMP Agent – is the software that is monitored by SNMP in order collect data and information about high priority events that have occurred and sends it to the SNMP manager as per its request.

- Management information base (MIB) – in short, is a text file that contains information about devices that have been queried or under the control of SNMP (Manager making request of agent).

However, for all its benefits, SNMP is not without its flaws, one of the major issues with the protocol is that when an agent receives a message request there isn't any way to verify that the message originally came from a management station in the first place. As such these messages could have been generated from an alternative station that has spoofed its IP address. From this spoofed address an individual (attacker) can send out a large volume of request messages to numerous device agents on the network that will in-tern respond with a constant stream of replies (SNMP is implemented using UDP so it doesn't require error-checking, packet recovery or authentication such as the TCP handshake, it only care's about continuously sending data). Eventually, due to the sheer volume of replies, it will cause the network to be brought down resulting in a denial of service, this is known as a SNMP reflection attack and can be taken even further when amplified, where the attack can produce a higher quantity of traffic resulting in a much more devastating and dangerous denial of service attack. [Source 19][Source 20][Source 21][Source 22]



[Image 7]

Related Cases

In regards to the specific flaws and attacks that were discussed above, it would be of benefit to reflect on some notable real-world incidents that occurred in recent years, showing their capabilities and the damages they could inflict if left unchecked. As an admin for this network, these cases also provide the opportunity to learn from them and how best to defend and prepare for them.

- YouTube block by Pakistan – in 2008 a Pakistan ISP was issued an order by the government to censor YouTube in an attempt to prevent Pakistani people from viewing an anti-Islamic film. Pakistan Telecom complied with this order and went about modifying the BGP entry for YouTube with the intent of directing users to a page informing them that YouTube would be blocked for them. However, the desired affect worked to well, the ISP announced the updated route to upstream providers who didn't verify but accepted the changes (communication relies on trust

and most networks will trust each other's information without testing it first) and triggered a chain affect for it to be passed on. This ultimately resulted in BGP entries around the world being updated so anyone who decided to visit YouTube that day would be directed to the network block. This denial of service lasted a total of two hours and is one of the better examples of BGP flaws. [Source 18]

- Facebook Disappearance – recently there was an incident which had the general public in uproar as a network issue had caused Facebook as well as its affiliated services Instagram and WhatsApp to be temporarily down for a total of six hours. It was noticed that Facebook's DNS records had become unavailable making it impossible to respond to user generated queries that were asking for Facebook.com IP address. The root of this issue originated from Facebook network engineers, who tried to implement configuration changes, ended up removing BGP routes from the global internet routing table.

Incidents of this magnitude truly demonstrate the consequences of misusing BGP, whether they be intentional or not, and shows how essential it is to secure BGP routing as even the slightest change in configuration could have devastating repercussions.

DDoS

- The Google Attack – Google announced that back in 2017 it had experienced the largest attempted DDoS attack it had ever seen to date. The attackers at the time had the goal of using a number of networks to spoof 167 Mbps to exposed DNS, SMTP and CLDAP servers, which numbered in the thousands, that would cause a flood of responses to be sent to Google with hopes that the volume of response would eventually cause a crash. Fortunately, it was announced that they were able to stop the attack before any real damage could be done, which if it couldn't would have disastrous effects for the company and prevent anyone from gaining access to google as well as most likely leading to general panic and a decrease in user trust.

Security Improvement & Practices

So far, when referring to security, we briefly discussed what the standards of an organisations security in modern times consists of, researched various types of attacks, both general and specific, and have also learned about a number of incidents caused by these attacks, in order to have a fair grasp on what they are capable of in a real-world scenario. With all this information that has been gathered we now have to conclude what improvements and practices can be implemented in order to further prevent any type of malicious attack on this network.

In this situation we consider that our system is newly setup with basic configurations and as such is highly vulnerable malicious, both internal and external threats, let us workout and

list all the possible improvements we could implement into our system by working outwards from a router.

Even though it's more likely to experience attacks from an outside source, internal threats are just a relevant, whether they be caused through social engineering or an employee with malicious intent. For starters we can fortify our device infrastructure in order make sure that unauthorized personnel can't gain access to our routers in an attempt to disable routing functions, discover and gain access to other systems located within the network or alter routing parameters, by securing administrative access. This can be accomplished through a number of beneficial tasks, by adding configurations to our routers, such as:

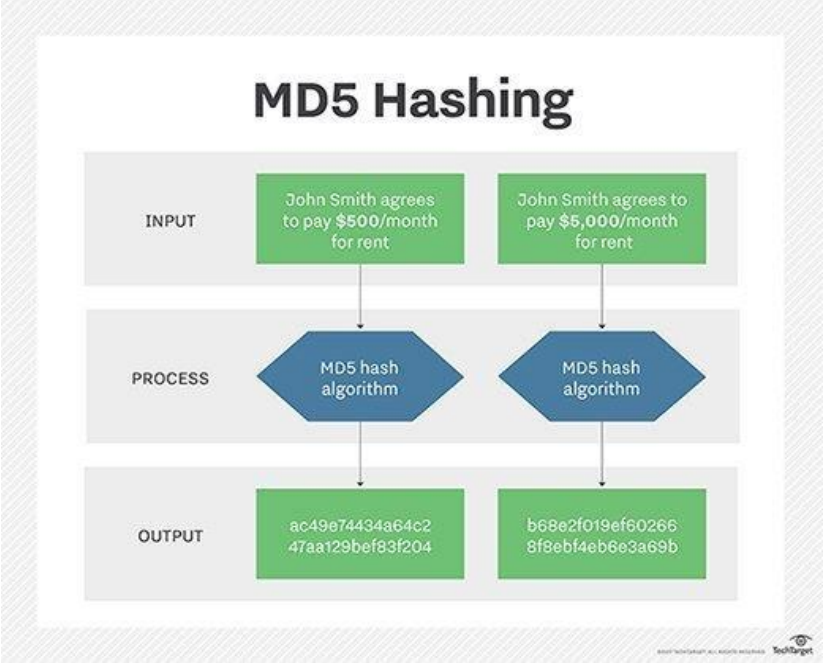
- Granting access only to those who have proven to be authenticated users or groups as well as implementing multi-factor authentication.
- Managing administrative credentials, making sure that every password is salted and hashed.
- Restricting access to unused ports, interfaces and services that could be used as a means of access (ACL's).
- Limit the actions and capabilities a user has based on their level of clearance within the company (Privilege level or Role-based configurations)
- Log entries of events where routers have been accessed as well as the activities that occurs on them such as updating routing configurations (through either SNMP or Syslog).

As was mentioned earlier the type of network we are trying to design is that of a distributed hospital and as such its virtual layout will mirror its physical, so once we are confident enough with our internal configurations, we need to consider configurations regarding external security factors such as safe communication from one machine to another over the internet as originally routeing protocols were not created with security in mind.

Let's assume that a so-called "known" neighbouring router is directing traffic towards our network, we must implement a way to prove that the data being sent to us is authentic by first authenticating the router itself otherwise we run the risk of foreign or spoofed devices compromising our network by means of receiving fraudulent routing updates and other nefarious actions. It is fortunate then, that the routers for this situation are configured with OSPF and BGP, both of which support Neighbour Authentication, specifically MD5 (although not considered the highest of standards in regards to protecting packets, it's still better than using plaintext).

How a router is actually able to verify if the packets it received are genuine or not is by authenticating their source through the use of exchanging authentication keys that are known to both routers, if the router that has sent the packets offers a key that corresponds with of the one the receiving router is holding then the packet is accepted. MD5 takes it a step further by sending a message digest with the packet instead of the actual key in order to ensure its integrity, otherwise if it was sent across the network in plaintext, an attacker could initiate a packet capture and view its contents.

[Source 23]



[

Image 8]

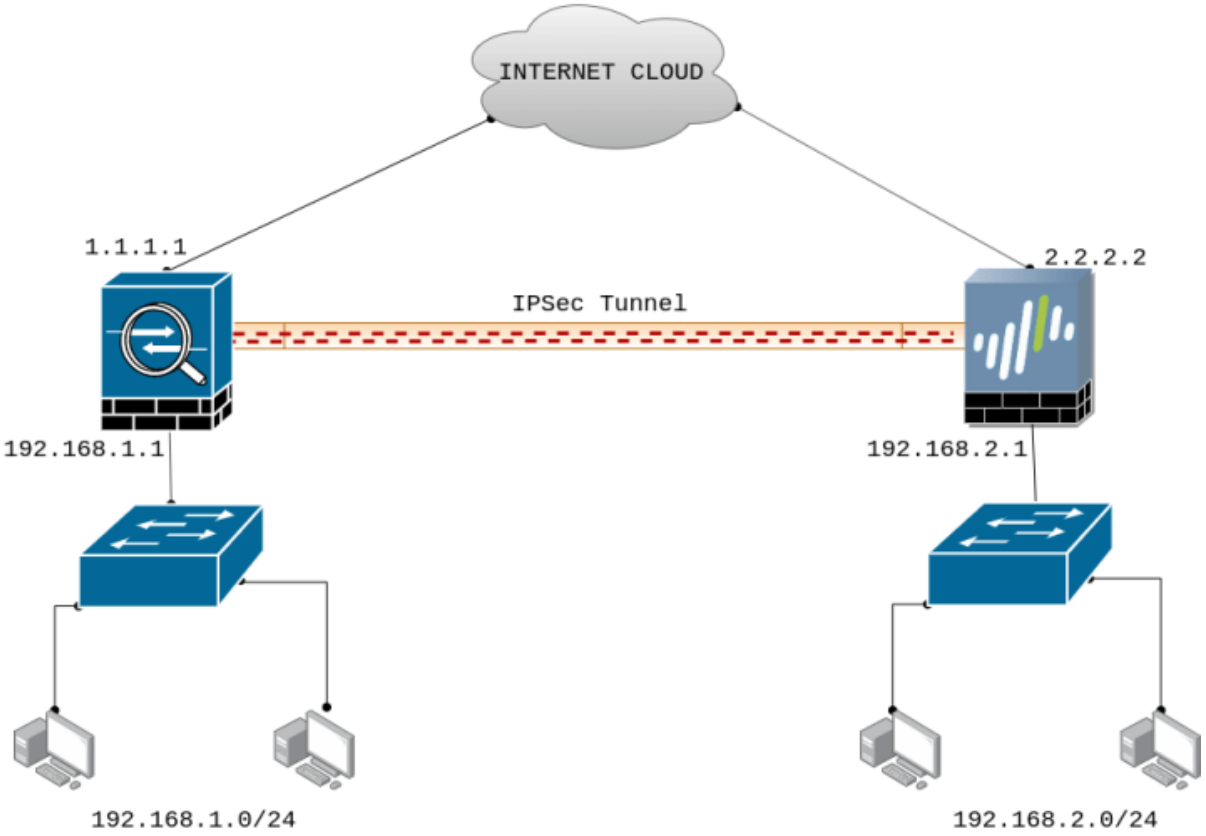
Given that BGP is such an integral part for this network's functionality, a lack of its security could lead to severe drawbacks (as mentioned earlier routing protocols weren't originally designed with security in mind), as such we must insist on implementing as many beneficial improvements as possible such as:

- Implementing control plane policing, prevent unauthenticated transfer of packets.
- Implement TCP MD5 message Digest
- TTL security
- Actively check and update data

One of the main reason's why a lot of BGP incidents can escalate within organisations (such as the Pakistan incident mentioned earlier) occur is due to their lack of prefix filters. Without these necessary components that are used to decide who is allowed to advertise and receive what prefixes, it opens up the opportunity for far-reaching negative effects from malicious attacks and misconfigurations. Take a situation where one of our routers is updating there routing table from an announcement they learned from their neighbour, soon after we realise that changes wish to make on our own router aren't being updated, through further in-depth research and backtracking we realise that the updates our router originally accepted from the neighbouring router contained an entry that specified the

denial of a prefix length belonging to our network and as a result of allowing our router to accept that we are thereby inhibiting ourselves.

Probably one of the most obvious method of securing communications that hasn't been discussed yet, is the creation of virtual private network (VPN) configured with IPsec. In short, a VPN is an encrypted communications line between devices over public networks and IPsec is the set of protocols used to set up said encrypted communications. Through the combination of these two assets, we are able to achieve the process of exchanging confidential data across a network.



[Image 9]

Conclusion

In conclusion, through research and testing we were able to gain extensive knowledge about how best to redesign our hospital network with the intended resulted to be a higher level of overall performance and security. Through comparative analysis of different routing protocols, we were able to conclude which combination was the best choice to be implemented in regards to factors such as convergence time, throughput, packet loss and jitter with protocols being OSPF/BGP. We were also able to increase the networks security standards by comparing certain flaws seen within some of the protocols we wish to

implement with those of real-world ones that lead to large scale incidents which allowed us further fortify the system.

Glossary

- Laptop/PC
- GNS3
- Cisco IOS images
- Virtual Machine

Bibliography

Images

Image 1

Static.javatpoint.com. 2021. [online] Available at: <https://static.javatpoint.com/tutorial/computer-network/images/rip-protocol.png> [Accessed 23 November 2021].

Image 2

Docs.vmware.com. 2021. [online] Available at: <https://docs.vmware.com/en/VMware-Smart-Assurance/10.1.0/npm-bgp-user-guide-101/images/GUID-CF9767BF-852D-4143-8847-85ECDE2DAEB2-low.png> [Accessed 23 November 2021].

Image 3

Noction.com. 2021. [online] Available at: <https://www.noction.com/wp-content/uploads/2014/12/bgp-ospf.png> [Accessed 23 November 2021].

Image 4

Keyfactor.com. 2021. [online] Available at: <https://www.keyfactor.com/wp-content/uploads/DNS-Spoofing-Attack.png> [Accessed 14 November 2021].

Image 5

2021. [online] Available at: <https://home.sophos.com/sites/default/files/2021-09/DoS-and-DDOS-Attacks.png> [Accessed 23 November 2021].

Image 6

Microcontrollertips.com. 2021. [online] Available at: <https://www.microcontrollertips.com/wp-content/uploads/2019/01/bgp-hacking.jpg> [Accessed 23 November 2021].

Image 7

Lh3.googleusercontent.com. 2021. [online] Available at: <https://lh3.googleusercontent.com/proxy/1PA8A4RyGF6SidS3iQ5F62uYtmNWf_JRN9oNJWFua91MptaEYX6lEjp_3iHMy0kEqmSYhJvfHqHxIGKn_OGiUiTQMz4jvgPV7UKvoEbF1g> [Accessed 23 November 2021].

Image 8

Cdn.ttgtmedia.com. 2021. [online] Available at: <https://cdn.ttgtmedia.com/rms/onlineImages/security-md5_hashing_mobile.jpg> [Accessed 25 November 2021].

Image 9

Encrypted-tbn0.gstatic.com. 2021. [online] Available at: <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQaxoxPvlHxU9c4YqT-dPHE20pZYyjwjYKYGA&usqp=CAU> [Accessed 26 November 2021].

Sites/Papers

Source 1

SearchNetworking. 2021. *BGP vs. OSPF: When to use each protocol*. [online] Available at: <https://www.techtarget.com/searchnetworking/tip/BGP-vs-OSPF-When-to-use-each-protocol> [Accessed 13 November 2021].

Source 2

OSPF?, W., 2021. *What is OSPF? | How it works? | Implementation And Application of OSPF*. [online] EDUCBA. Available at: <https://www.educba.com/what-is-ospf/> [Accessed 13 November 2021].

Source 3

Liu, D., 2021. *Cisco IOS Router Basics*.

Source 4

Blog. 2021. *OSPF vs BGP: Which Routing Protocol to Use?*. [online] Available at: <https://community.fs.com/blog/ospf-vs-bgp-routing-protocol-

choice.html#:~:text=The%20main%20difference%20between%20OSPF,routing%20operations%20performed%20between%20two> [Accessed 13 November 2021].

Source 5

2021. [online] Available at: <https://www.fcc.gov/general/voice-over-internet-protocol-voip> [Accessed 13 November 2021].

Source 6

Ieeexplore.ieee.org. 2021. *Voice over Internet protocol (VoIP)*. [online] Available at: <https://ieeexplore.ieee.org/abstract/document/1041060> [Accessed 13 November 2021].

Source 7

Ieeexplore.ieee.org. 2021. *A comparative study on RIP and OSPF protocols*. [online] Available at: <https://ieeexplore.ieee.org/abstract/document/7193275> [Accessed 13 November 2021].

Source 8

Ieeexplore.ieee.org. 2021. *A Case Study in Understanding OSPF and BGP Interactions Using Efficient Experiment Design*. [online] Available at: <https://ieeexplore.ieee.org/abstract/document/1630727> [Accessed 13 November 2021].

Source 9

Ieeexplore.ieee.org. 2021. *Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP*. [online] Available at: <https://ieeexplore.ieee.org/abstract/document/8319134> [Accessed 13 November 2021].

Source 10

Ieeexplore.ieee.org. 2021. *Dynamic Routing Protocol Implementation Decision between EIGRP, OSPF and RIP Based on Technical Background Using OPNET Modeler*. [online] Available at: <https://ieeexplore.ieee.org/abstract/document/5474509> [Accessed 13 November 2021].

Source 11

Ieeexplore.ieee.org. 2021. *Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in Ipv4 and Ipv6 Network*. [online] Available at:

<https://ieeexplore.ieee.org/abstract/document/6141697> [Accessed 13 November 2021].

Source 12

Blog. 2021. *What's EIGRP? What's OSPF? EIGRP vs OSPF Differences*. [online] Available at: <https://community.fs.com/blog/eigrp-vs-ospf-differences.html> [Accessed 13 November 2021].

Source 13

Ieeexplore.ieee.org. 2021. *MPLS and traffic engineering in IP networks*. [online] Available at: <https://ieeexplore.ieee.org/abstract/document/809383> [Accessed 13 November 2021].

Source 14

Hjp.at. 2021. *Hjp: doc: RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)*. [online] Available at: <https://www.hjp.at/doc/rfc/rfc4364.html> [Accessed 13 November 2021].

Source 15

Learning Center. 2021. *What is phishing | Attack techniques & scam examples | Imperva*. [online] Available at: <https://www.imperva.com/learn/application-security/phishing-attack-scam/> [Accessed 14 November 2021].

Source 16

Keyfactor. 2021. *What is DNS Poisoning? (aka DNS Spoofing)*. [online] Available at: <https://www.keyfactor.com/blog/what-is-dns-poisoning-and-dns-spoofing/> [Accessed 14 November 2021].

Source 17

Maxcrone.org. 2021. [online] Available at: <https://maxcrone.org/assets/docs/2021-02-01-secure-bgp-adoption.pdf> [Accessed 14 November 2021].

Source 18

Nast, C., 2021. *Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net*. [online] Wired. Available at: <https://www.wired.com/2008/02/pakistans-accid/> [Accessed 23 November 2021].

Source 19

2021. [online] Available at: <https://www.thousandeyes.com/learning/techtorials/snmp-simple-network-management-protocol> [Accessed 23 November 2021].

Source 20

Annalsofrscb.ro. 2021. *View of Evaluation of the Security Mechanisms in the Notification Systems and Event Registration for Network Management*. [online] Available at: <https://annalsofrscb.ro/index.php/journal/article/view/9225/6735> [Accessed 23 November 2021].

Source 21

Ieeexplore.ieee.org. 2021. *Advantages and Disadvantages of the Data Collection's Method Using SNMP*. [online] Available at: <https://ieeexplore.ieee.org/abstract/document/8934069> [Accessed 23 November 2021].

Source 22

Learning Center. 2021. *What is SNMP Reflection and Amplification | DDoS Attack Glossary | Imperva*. [online] Available at: <https://www.imperva.com/learn/ddos/snmp-reflection/> [Accessed 23 November 2021].

Source 23

Cisco. 2021. *This documentation has been moved - Neighbor Router Authentication: Overview and Guidelines [Support]*. [online] Available at: <https://www.cisco.com/en/US/docs/ios/sec_control_plane/configuration/guide/sec_neigh_rtr_authen_external_docbase_0900e4b180dc7d5a_4container_external_docbase_0900e4b1810e9980.html> [Accessed 25 November 2021].