



INTERNET PROTOCOLS (ACCC4002_LON)

August Assessment
UNIVERSITY OF WALES TRINITY SAINT DAVID
Academic Year 2018/2019

Tawhid Ahmed
Student number: 1715006

Part 1 of assessment

Content	pag.
Table of contents.....	2
1. Introduction.....	3
2. Difference between IPv4 and IPv6.....	3
3. Uncast, anycast and multicast of IPv6.....	3
4. Possible vulnerability.....	3
4.1. Ddos.....	4
4.2. Men-in-middle.....	4
4.3. Spoofin.....	5
5. Conclusion.....	5
6. References.....	6

1 Introduction

Due to the rapid spread of internet due to the use of computers, smartphones, tablets, play stations, Smart TVs, vehicles and smart appliances connected to the network, Internet Protocol version 4 (IPv4) addresses are being depleted, this created towards the end of the years 70 and early 80s, such rapid growth was not expected. To address this problem The Internet Engineering Task Force (IETF) created version 6 of the Internet Protocol (IPv6) in the late 1980s. IPv6 was not adopted because companies have often decided to postpone investments for the transition. One of the reasons is that the activation of IPv6 requires the revision of procedures, the investment of a lot of money and time, but does not offer immediate economic advantages. Momentary solutions such as the use of NATs have allowed organizations to survive despite the decrease in IPv4 and to postpone the activation of IPv6. These solutions are expensive and hinder the development of the network.

2 Difference between IPv4 and IPv6

IPv4 addresses use 32-bit long addresses divided by dots into 4 bytes, each byte can go from 0 to 255 and the maximum available number of these is 4 294 967 296, in the writing of addresses it is possible to omit the initial zeroes. The ipv6 addresses compensate for the exhaustion of the addresses because they are longer, formed by 128 bits, these are composed of eight blocks each divided by two points, IPv6 makes use of a hexadecimal system, 64 bits of the addresses are dedicated to the interfaces while the others 64 are used for the header. The maximum number of this is (2^{128}) 79 228 162 514 264 337 593 543 950 336. In the writing of the address, it is possible to omit the initial zero, the doubling of the colon (:) can be used once in the format text of an address to indicate any number of 0 bits. IPv6 is still currently improving, so IPv4 is still used for security issues.

3 Unicast, anycast and multicast of IPv6

The transition from ipv4 to IPv6 takes years, various systems are foreseen to make the two systems exist between which tunnelling. IPv6 is thought to be safer because its specifications require the inclusion of IP Security (IPsec) technology and the elimination of NAT by making end-to-end communication safer. Many problems related to the security of IPv6 addresses are due to a wrong configuration or the incompleteness of the products, the vulnerabilities are identified and corrected from time to time. IPv6 addresses can be divided into different groups, such as unicast that includes the interface from a single host to another single host, the anycast interface that includes an interface from a host to a node as close as possible, and a multicast interface that includes a host interface that reaches multiple host interfaces.

4 Possible vulnerability

With the extensive use of the internet by users and various agencies, over the years malicious individuals developed various threats that could jeopardize the security and confidentiality of data. To maintain the integrity and confidentiality of the messages it is necessary to encrypt them in order not to be modified. The behaviour of malicious people are called cybercrimes, the most common are: the acquisition of unauthorized access, pretend to be another user to use licenses not their own, enter into a conversation between two other users, prevent communication between users, alter the software.

4.1 DDos

One of the most famous attacks are the DDoS acronym stands for Distributed Denial of Service, is to send many requests along with a site until it is unreachable. The main objectives of these attacks are companies or sites that provide a particular service to the computer, the simplest version is dos (Denial of Service), and it is an action that puts in a difficult position servers, distribution networks, data centres and connected computers that are filled with false requests for access that they cannot cope with. In cases of dos, the attack came from a single source, while in cases of the DDOS attack came multiple sources, this causes a longer and more effective block that goes from hours to several days. These attacks use botnets that would be a set of computers compromised by malware, which allow the attacker to take control and have certain actions performed. There are several types of DDoS, those that focus on speed by targeting TCP connections, where the botnet fills the server with connection requests. Another type of attack is fragmentation, in which incomplete requests are sent, the attacker uses most of the resources to decrypt requests. Then there are application attacks that point to important targets to destabilize the entire structure. To defend from it is important to use databases, web front-end clusters, firewalls or you can contact a specialized market author.

4.2 Men-in-middle

Man in the middle is a threat in which the bad people can intercept and manipulate our Internet traffic, putting themselves between the customer and the router, pretending to be both parties. Man-in-the-wifi exists in which the Wi-Fi network is compromised; the most common are open public networks like those of hotels and airports. The bad people can be fooled by making a fake copy of the Wi-Fi node, or they can monitor Internet traffic through cookies. Man-in-the-mobile where the target is to infect mobile phones to intercept message traffic. Man-in-the-browser predicts the installation of a malware that is able to change online transactions. Man-in-the-lot provides data collection from objects connected to the network such as a thermostat, TV, washing machines and others. Man-in-the-app in which the goal is to hack the app to take the data we have provided. To deal with these problems we can use small measures such as not using open public networks to perform transactions, ensure the encrypted version of the web, change the default password of Wi-Fi, update anti-virus, enable two-factor identification for our accounts, do not visit sites when the browser warns us of insecurity.

4.3 Spoofin

Spoofing allows falsifying digital identity to penetrate a network. This allows the ill-intentioned the ability to intercept data, spread false information. There are different types of spoofing, MAC Spoofing which would be the falsification of the MAC address, ARP Spoofing technique used by malicious people who sends ARP messages to connect their MAC address to the IP of another host to interface all the traffic. IP Spoofing consists in the creation of an IP packet in which the sender's IP address is falsified. One of these is to prevent packages from being sent from an interface where the source IP is not what is expected, but if the source interface for a packet is not the same one that would be chosen by the router for the forwarding the response packet then this package is discarded. This technique is called uRPF (Unicast Reverse Path Forwarding). Spoofing UDP falsification of a UDP datagram consists in entering the desired information and falsifying the header. Spoofing TCP, you have to create a SYN package with the falsified IP address and this is sent to a server before it is possible to send data the server will try to complete the handshake answering with a SYN / ACK package. This package will report the falsified IP address, so it will not be returned to the attacker who will not be able to reply with the third and last package (the ACK package). To complete this attack it is necessary to send an ACK packet to the server which not only reports the fake IP address again but also the sequence number that the server has inserted into the SYN / ACK packet. Email Spoofing It consists of falsifying the sender's address in an email. Used for spreading Spam emails, Malware. WEB spoofing this concerns the falsification of a web server to make a user believe to be connected to a certain server while connected to a malicious server. DNS Spoofing is a cyber-attack that involves the interception of direct queries to the DNS server and the sending of a fake reply, different from the one that would have given the real DNS server, typically in order to divert traffic to malicious servers. Referrer Spoofing consists of falsifying the referrer in an HTTP request, in order to prevent a site from obtaining accurate information on the web page previously visited by the user. Caller ID Spoofing Consists of falsifying the caller ID in a VoIP call. To prevent this, packet filtering can be used. By acting on the options of the router and possibly the firewall of the network, you can set a few stakes that will block the flow of data packets from unknown sources or you can defend against spoofing attacks by manually assigning the IP address.

5 Conclusions

We have seen what is an IPv6 and what are its main features by comparing it with IPv4 and finding the main differences, we have analysed the various types of IPv6 as unicast, anycast and multicast. The main vulnerabilities and attacks due to DDoS, man-in-middle and Spoofing have been analysed with their own security systems.

References

Bontà, Irene. (2008). "Il protocollo IPv6 e progetto di una rete aziendale." [Accessed: 26th August 2018]
http://netlab-mn.unipv.it/thesis/BSc/DDeVecchi_Thesis.pdf

Favalli, Lorenzo. (2004) "Il protocollo IPv6: considerazioni sulla sicurezza." [Accessed: 26th August 2018]
http://netlab-mn.unipv.it/thesis/BSc/DDeVecchi_Thesis.pdf

Srivatsa, Mudhakar, and Ling Liu. (2004) *Computer Security Applications Conference*.
<https://www.cc.gatech.edu/projects/disl/SGuard/dht-security/p2p-security.pdf> [Accessed: 26th August 2018]

www.cisco.com [Accessed: 26th August 2018]

Part 2 of assessment

IP addressing for School of Computerscience and Engineering

	Network	First usable	Last usable	Broadcast	Subnet mask
School of Applied Computing	172.18.0.0	172.18.0.1	172.18.7.254	172.18.7.255	255.255.248.0
School of Automotive Engineering:	172.18.8.0	172.18.8.1	172.18.11.254	172.18.11.255	255.255.252.0
School of Engineering	172.18.12.0	172.18.12.1	172.18.15.254	172.18.15.255	255.225.252.0
Line 1	172.18.16.0	172.18.16.1	172.18.16.2	172.18.16.3	255.255.255.252
Line 2	172.18.16.4	172.18.16.5	172.18.16.6	172.18.16.7	255.255.255.252

Address School of Applied Computing

	Network	First usable	Last usable	Broadcast	Subnet mask
Open Access lab	172.18.0.0	172.18.0.1	172.18.1.254	172.18.1.255	255.255.254.0
Lab308	172.18.2.0	172.18.2.1	172.18.2.254	172.18.2.255	255.255.255.0
ab301	172.18.3.0	172.18.3.1	172.18.3.126	172.18.3.127	255.255.255.128
Lab309	172.18.3.128	172.18.3.129	172.18.3.190	172.18.3.191	255.255.255.224
Lab 304	172.18.3.192	172.18.3.193	172.18.3.254	172.18.3.255	255.255.255.192
Lab306	172.18.4.0	172.18.4.1	172.18.4.62	172.18.4.63	255.255.255.192
Lab303	172.18.4.64	172.18.4.65	172.18.4.126	172.18.4.127	255.255.255.192
Lab302	172.18.4.128	172.18.4.129	172.18.4.190	172.18.4.191	255.255.255.192
A Test centre	172.18.4.192	172.18.4.193	172.18.4.222	172.18.4.223	255.255.255.224
Staff	172.18.4.224	172.18.4.225	172.18.4.254	172.18.3.255	255.255.255.224
Lab310	172.18.5.0	172.18.5.1	172.18.5.30	172.18.5.31	255.255.255.224

Address for School of Automotive Engineering

	Network	First usable	Last usable	Broadcast	Subnet mask
Lab301	172.18.8.0	172.18.8.1	172.18.8.62	172.18.8.63	255.255.255.192
Lab206	172.18.8.64	172.18.8.65	172.18.8.126	172.18.8.127	255.255.255.192
lab101	172.18.8.128	172.18.8.129	172.18.8.190	172.18.8.191	255.255.255.192
Lab205	172.18.8.192	172.18.8.193	172.18.8.254	172.18.8.255	255.255.255.192
Lab103	172.18.9.0	172.18.9.1	172.18.9.30	172.18.9.31	255.255.255.192
Lab102	172.18.9.32	172.18.9.33	172.18.9.94	172.18.9.95	255.255.255.192
staff	172.18.9.96	172.18.9.97	172.18.9.126	172.18.9.127	255.255.255.192
CAD lab	172.18.9.128	172.18.9.129	172.18.9.158	172.18.9.159	255.255.255.244

Address for School of Engineering

	Network	First usable	Last usable	Broadcast	Subnet mask
Lab202	172.18.12.0	172.18.12.1	172.18.12.126	172.18.12.127	255.255.255.128
Lab409	172.18.12.128	172.18.13.129	172.18.12.254	172.18.12.255	255.255.255.128
Lab203	172.18.13.0	172.18.13.1	172.18.13.62	172.18.13.63	255.255.255.128
Lab404	172.18.13.64	172.18.13.65	172.18.13.126	172.18.13.127	255.255.255.192
Lab410	172.18.13.128	172.18.13.129	172.18.13.158	172.18.13.159	255.255.255.192
Lab408	172.18.13.160	172.18.13.193	172.18.13.222	172.18.13.223	255.255.255.192
Lab205	172.18.13.224	172.18.13.225	172.18.14.30	172.18.14.31	255.255.255.192
lab201	172.18.14.32	172.18.14.33	172.18.14.62	172.18.14.63	255.255.255.224
staff	172.18.14.64	172.18.14.65	172.18.14.94	172.18.14.95	255.255.255.224

