

Level 4

Internet Protocol

ACCC4002

Bogdan-Nicusor Halinga

Part 1:

IPv6 Threats

The Internet is one of the most important things now a days. First connection of Internet was on 29th of October 1969 at 22:30 between University of California, Los Angeles and Research Institute of Stanford. In 1979 ARPA decide to slip the network (one part for commercial use and the another one for army and security use). In 1983, TCP/IP become official the unique protocol of Internet and this help Internet expanding. In 1990, the Internet network had about 300000 computer and in 1992 1 million, then every year was doubling the number of computers. On the middle of 90s the Internet was very popular and increasing. The scientists start to worry about that in future we will finish the number of host available in IPv4.

1985	~ 1/16 of total space
1990	~ 1/8 of total space
1995	~ 1/4 of total space
2000	~ 1/2 of total space
Halfway through 2002	~ 2/3 of total space

Fig.1 IPv4 depletion.

The Internet Engineering Task Force (IETF) start in 1994 to develop and design new protocols and standard named IPv6. The mains changes between IPv6 and IPv4 are:

- Increased addresses space: IPv6 is based on 128-bit and IPv4 only 32-bit;
- Number of hosts: IPv4 has about 4 billion and IPv6 has 340 undecillions;
- IPv6 header was simplified.

Simplifying the design of IPv6 made it more vulnerable. The new futures of IPv6 likely generate new protocol attack. The most common attacks are: DOS, Man in the middle, Spoofy and Type 0 routing.

In IPv4 options were integrated in the basic header. In IPv6 they use it as an extension header and the extension are included when they are necessary. On this way the transmitting of packet is better because the packets become flexible. Being an extension, it is very vulnerable to many attacks, but the most common one is the type 0 routing header. "Some of the packet filtering system does not have the capability of processing routing header, therefore attacker first access the packet filtering system and gather all the related and secret information and later by using these information attacker use routing headers and generated malicious packet, then by using routing header attacker perform attack on internal network." (Manju Khari, Vulnerability of IPv6 Type 0 Routing Header and It's Prevention Algorithm).

Another type of attack is Spoofy. According with "Dictionary of the Internet", spoofing means "assuming the identity of an existing user in order to discover information associated with

that user or information that the user is allowed to access: a technique used by crackers. When the spoofing involves an Internet Protocol Address the process is known as IP spoofing.”

IP spoofing is the way through which an unauthorized person gains the access to our computers by manipulating IP packets. The attackers use IP spoofing for malicious and illegal activities. We can avoid this kind of attack monitoring networks for atypical activity, authentication all IPs, using network attacks blocker and deploy packets filtering.

DDoS (distributed denial of service) attack is a brute-force attempt to slow down or total crash a server. The hackers try to infect enough devices, usually with a trojan virus, then order them to attack. Each device start sending a flood of requests to the main server, overloading it. Usually, the companies or the main targets for this kind of attacks.

The mains reasons of these attacks are money, time and reputation. Because of overloading of server, the employees are not able to access network resources. Depending on the complexity of the attack, the server can be offline one day or even one month. All this time the company will lose money. A survey showed that one of five DDoS attacks can late days or even weeks. (Kaspersky Lab).

To avoid the DDoS attacks, the companies are guided to:

- Limit the number of login attempts
- Take a web-server configuration against DDoS attack
- Create an ISP firewall
- Move public resources to another IP
- Backup on cloud storage.

Man on the middle is another type of attack. These attacks are initiate by hackers, who intercept your browser history, email or social media details. On this way they can find a lot of information about you, like: credit or debit card details – they can do online shopping with your card, bank account details – they can send money from your account to their one, login details from different web sites – they will change the passwords and will require money to send you the new one, access your email – they can access your email and find important details about you, like holiday trips and they can sell the information to the house robber. Anyone can me a target of this kind of attack.

The hackers are using different methods. One of the most popular is to set up a bespoke Wi-Fi connection. Once you connected to their Wi-Fi connection, a hacker gains instant access to your device.

Another method of attack is named “session hijacking”. On this method the hacker gains control of your browser cookies and then he can steak range of data (log-in details, pre-filled web forms).

To protect us against these attacks we must use browser encryption software. According with www.statista.com, in United Kingdom in 2018, most of the people are using Google Chrome (47.19%), the second one is Safari (30.06%) and the third one is Internet Explorer (only 5.51%).

As well we must to browse only on secure web sites. How we can know which one is secure or nor? The secure website was a lock symbol on next to the URL address, if that lock is not there,

we can take a look on the prefix of URL address. Usually the URL starts with <http://>, but the secure websites will have <https://>. That “s” is from secure (Secure Hyper Text Transfer Protocol).

On the last we must to avoid to use the unsecure Wi-Fi connection or, if we use it, don't access important websites (like checking emails, do shopping, log in in different websites)

In conclusion, I can say that we don't have a perfect Internet protocols. Both, IPv4 and IPv6 are vulnerable. IPv4 was created in the '80s and is not fitted for all of us today and it has his vulnerabilities. Instead, IPv6, become be used since 1996 and become an Internet Standard on 14 July 2017. Since was only an idea, the scientists tried to improve the IPv6. Firstly, they tried to make it easiest to use then IPv4 and after they tried to improve the new vulnerabilities. On present they still try to improve it and make it more secure. I know that both all them will work together, maybe forever, but I think that IPv6 will be much better in the next years and will be the main Internet Protocol.

References

<https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#6.1.4.2> [accessed on August 23, 2018]

<https://usa.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work> [accessed on August 30, 2018]

<https://usa.kaspersky.com/resource-center/threats/ip-spoofing> [accessed on August 30, 2018]

<https://usa.kaspersky.com/resource-center/threats/man-in-the-middle-attack> [accessed on August 30, 2018]

<https://www.apnic.net/get-ip/faqs/what-is-an-ip-address/more-on-ip-addressing/about-ipv6/> [accessed on August 23, 2018]

<https://www.iplocation.net/ip-spoofing> [accessed on August 30, 2018]

<https://www.ipv6.com/general/ipv6-the-history-and-timeline/> [accessed on August 23, 2018]

Caicedo, Carlos E., James BD Joshi, and Summit R. Tuladhar. IPv6 security challenges

Ince, D., 2009 – A dictionary of the internet (2nd edition)

Khari, M., 2015 - Vulnerability of IPv6 Type 0 Routing Header and It's Prevention Algorithm (p.59)

Part 2:

IP addressing scheme

First step in designing the IP addressing scheme will be VLSM for the three schools and 2 networks between them. I choose VLSM instead of fixed submitting because the number of hosts is quite different and I don't want to waste too many addresses. The School of Applied Computing will have 711 devices to connect, the School of Engineering will have 406 devices to connect and School of Automotive Engineering will have 283 devices to connect. In total 1400 devices.

Because of big number of devices and labs and a future grow, I choose a private B class address – 172.20.0.0.

VLSM for the 3 buildings and 2 networks

5Name of school	Numbers pc (real number + future grow)	Network Address	Broadcast Address	First Usable	Last Usable	Subnet
School of Applied Computing	2048 (711 + future grow)	172.20.0.0/21	172.20.7.255	172.20.0.1	172.20.7.254	255.255.248.0
School of Engineering	2048 (406 +future grow)	172.20.8.0/21	172.20.15.255	172.20.8.1	172.20.15.254	255.255.248.0
School of Automotive Engineering	1024 (283 +future grow)	172.20.16.0/22	172.20.19.255	172.20.16.1	172.20.19.254	255.255.252.0
Network 1 (between School of Applied Computing and School of Engineering)	4	172.20.20.0/30	172.20.20.3	172.20.20.1	172.20.20.2	255.255.255.252
Network 2 (between School of Applied Computing and School of Automotive Engineering)	4	172.20.20.4/30	172.20.20.7	172.20.20.5	172.20.20.6	255.255.255.252

VLSM of School of Applied Computing

Name of class room	Numbers pc (real number + future grow)	Network Address	Broadcast Address	First Usable	Last Usable	Subnet
Open Access	512 (250 + Future grow)	172.20.0.0/23	172.20.1.255	172.20.0.1	172.20.1.154	255.255.254.0
Lab 308	256 (140 + Future grow)	172.20.2.0/24	172.20.2.255	172.20.2.1	172.20.2.154	255.255.255.0
Lab 301	128 (60 + Future grow)	172.20.3.0/25	172.20.3.127	172.20.3.1	172.20.3.126	255.255.255.128
Lab 309	128 (50 + Future grow)	172.20.3.128/25	172.20.3.255	172.20.3.129	172.20.3.254	255.255.255.128
Lab 304	128 (45 + Future grow)	172.20.4.0.25	172.20.4.127	172.20.4.1	172.20.4.126	255.255.255.128
Lab 306	128 (40 + Future grow)	172.20.4.128/25	172.20.4.255	172.20.4.129	172.20.4.254	255.255.255.128
Lab 303	64 (36 + Future grow)	172.20.5.0/26	172.20.5.63	172.20.5.1	172.20.5.62	255.255.255.192
Lab 302	64 (30 + Future grow)	172.20.5.64/26	172.20.5.127	172.20.5.65	172.20.5.126	255.255.255.192
Test centre	64 (22 + Future grow)	172.20.5.128/26	172.20.5.191	172.20.5.129	172.20.5.190	255.255.255.192
Staff	64 (20 + Future grow)	172.20.5.192/26	172.20.5.255	172.20.5.193	172.20.5.254	255.255.255.192
Lab 310	64 (18 + Future grow)	172.20.6.0/26	172.20.6.63	172.20.6.1	172.20.6.62	255.255.255.192

School of Engineering

Name of class room	Numbers pc (real number + future grow)	Network Address	Broadcast Address	First Usable	Last Usable	Subnet
Lab 202	256 (80 + Future grow)	172.20.8.0/24	172.20.8.255	172.20.8.1	172.20.8.254	255.255.255.0
Lab 409	256 (80 + Future grow)	172.20.9.0/24	172.20.9.255	172.20.9.1	172.20.9.254	255.255.255.0
Lab 203	128 (65 + Future grow)	172.20.10.0/25	172.20.10.127	172.20.10.1	172.20.10.126	255.255.255.128
Lab 404	128 (45 + Future grow)	172.20.10.128/25	172.20.10.255	172.20.10.129	172.20.10.254	255.255.255.128
Lab 410	128 (45 + Future grow)	172.20.11.0/25	172.20.11.127	172.20.11.1	172.20.11.126	255.255.255.128
Lab 408	64 (28 + Future grow)	172.20.11.127/26	172.20.11.191	172.20.11.128	172.20.11.190	255.255.255.192
Lab 205	64 (25 + Future grow)	172.20.11.192/26	172.20.11.255	172.20.11.193	172.20.11.254	255.255.255.192
Lab 201	64 (20 + Future grow)	172.20.12.0/26	172.20.12.63	172.20.12.1	172.20.12.62	255.255.255.192
Staff	64 (18 + Future grow)	172.20.12.64/26	172.20.12.127	172.20.12.65	172.20.12.126	255.255.255.192

School of Automotive Engineering

Name of class room	Numbers pc (real number + future grow)	Network Address	Broadcast Address	First Usable	Last Usable	Subnet
Lab 301	128 (50 + Future grow)	172.20.16.0/25	172.20.16.127	172.20.16.1	172.20.16.126	255.255.255.128
Lab 206	128 (48 + Future grow)	172.20.16.128/25	172.20.16.255	172.20.16.129	172.20.16.254	255.255.255.128
Lab 101	128 (40 + Future grow)	172.20.17.0/25	172.20.17.127	172.20.17.1	172.20.17.126	255.255.255.128
Lab 205	128 (40 + Future grow)	172.20.17.128/25	172.20.17.255	172.20.17.129	172.20.17.254	255.255.255.128
Lab 103	64 (35 + Future grow)	172.20.18.0/26	172.20.18.63	172.20.18.1	172.20.18.62	255.255.255.192
Lab 102	64 (25 + Future grow)	172.20.18.64/26	172.20.18.127	172.20.18.65	172.20.18.126	255.255.255.192
Staff	64 (25 + Future grow)	172.20.18.128/26	172.20.18.191	172.20.18.129	172.20.18.190	255.255.255.192
CAD lab	64 (20 + Future grow)	172.20.18.192/26	172.20.18.255	172.20.18.193	172.20.18.254	255.255.255.192

IPv6 assigned to the servers are:

Server Name	IPv6 Address
DNS	fc00::
Email	fc00::1
Finance	fc00::2
Registry	fc00::3
File Server	fc00::4
Printer Server	fc00::5
MP	2001:0DB8::