Survey and Study of Next Future Problems in IPV4 and IPV6 Created By Different Unreliable Network Issues

[1]Rahul Nagar, Mtech (Research Scholar)

[2]Mr. Asif Ali, Assistant Professor, Department Of Computer Science Engineering, AL-FLA University,Fridabad,Haryana

ABSTRACT

This research paper based on the study of IPV4 and IPV6 related next future problems .We've been at the time, computers were big, expensive, and rare. IPv4 had provision for 4 billion IP addresses, which seemed like an enormous number compared to the number of computers. Unfortunately, IP addresses are not use consequently. There are gaps in the addressing a company might have an address space of 254 (2^8-2) addresses, and only use 25 of them. The remaining 229 are reserved for future expansion. Those addresses cannot be used by anybody else, because of the way networks route traffic. The Internet Engineering Task Force (IETF) recognized this problem in the early 1990s and came up with two solutions: Classless Internet Domain Router (CIDR) and private IP addresses. Prior to the invention of CIDR, you could get one of three network sizes: 24 bits (16,777,214 addresses), 20 bits (1,048,574 addresses) and 16 bits (65,534 addresses). Once CIDR was invented, it was possible to split networks into sub networks. So, for example, if you needed 5 IP addresses, your ISP would give you a network with a size of 3 bits which would give you 6 IPaddresses. So that would allow your ISP to use addresses more efficiently. So in this solve the above related problem But the problems for your ISP drives them nuts. All of these problems went into the consideration of the next version of the Internet.

Keyword: *Internet Engineering Task Force (IETF), CIDR, IP addresses, SCADA (Systems Control and Data Acquisition)*

1. Introduction:

The IPv4 Security is a legitimate concern for any type of network. With SCADA being critical to our infrastructure, it is important to be thinking and learning all you can about security during every step of the process. By connecting control systems to the internet, operators opened it to the world where attacks are happening every day, and on a scale that has never been possible. An attack targeted at a critical infrastructure facility that attempts to disrupt service, insert false information, or create lasting physical damage is where the nation is really at risk. The potential risk is not only there – the attacks have already begun and are rapidly escalating. Driven by advances in information system technologies used around the world. The transition of most organization and companies to IPV6 has begun and will continue for years to come. SCADA (Systems Control and Data Acquisition) are gradually shifting to IPV6. IPV6 was designed to overcome the limitations of IPV4 of which is that IPV4 only allows for 4 billion nodes on the internet.

2. History and Background of the Study

The previous work done by the different studied. The rate of internet is growing, and it will actually run out of available internet by 2012. With about a huge number of diverse users of internet, it needs a room to grow. With SCADA as a crucial system in this generation and plays an important role in most big companies and even nations infrastructure it is just vital to put emphasis in the study of its security. With the benefits of IPV 6 it will dramatically increase the address space from 32 to 128 bits. This will allow for every person on the planet to be designated millions of IP addresses. That is anticipated to be enough space to accommodate the expansion of the internet to include every device in the world from here forward. The list of improvement for IPV6 goes on. More flexibility support for mobile computing device, such as laptop, PDAs, cell phones, wristwatch computers, GPS tracking devices and any other brilliant technology yet to be developed. IPV6 supports automatic transparent address reconfiguration while a device is in use, which provides better support for secure communication.

3. Research Problem Statement

The various problems coming in this future related to the issues of IPV4 and IPV5 and some other unreliable network problems.

A) Cloud Based Network Issues in Ipv6 and IPV4

The cloud computing network issues in ipv6 and ipv4 focused on the study of that existing security fixes may only be applied to IPv4 support, yet most kernels will prefer IPv6 interfaces before IPv4 when engaging in such activities as DNS lookups in order to foster more rapid IPv6 deployment. Indeed, the dynamic between IPv6 and IPv4 could result in a doubling of traffic for each DNS lookup (with both AAAA and A records requested, or worse, each over IPv4 and IPv6). This could result in large amounts on unnecessary DNS traffic in order to optimize for user experience. OS and content vendors frequently put hacks in place to mitigate or optimize for this behavior (e.g., AAAA white listing), which creates added system load and state. Additionally, it should certainly be observed that with new IPv6 stacks being accessible new vulnerabilities are sure to surface. Dual-stacking during a long transitional coexistence period, and inter-dependences between routers, end systems, and network services such as the DNS are sure to serve as fertile ground for miscreants.

B) Even IPSec Could Pose Problems When Tunneling To Other Networks

IP Security (IPSec) makes it possible to authenticate the sender, provide integrity protection, and optionally, encrypt IP packets to provide confidentiality of transmitted data. IPSEC was an optional feature for IPv4, but it’s mandatory with IPv6. In tunnel mode which essentially creates a VPN for network-to-network, host-to-network and host-to-host communications the entire packet is encapsulated into a new IP packet and given a new IP header. But a VPN connection with a network that’s beyond the originator’s control could result in security exposures or be used to exfiltrate data, etc. Because the negotiation and management of IPSEC security protections and the associated secret keys are handled by additional protocols (e.g., Internet Key Exchange IKE) and adds complexity, it isn’t likely IPSEC will be any more widely supported with IPv6 than it is with IPv4 initially. It will be some time before IPv6 is universally deployed and IPv4 devices decline. Until then, we will all be working to build on the protocol that enabled the Internet’s first 4 billion devices.

C) Technical Problems with IPv4

IPv4 has technical problems, and IPv6 is the solution. Unfortunately, deployment of IPv6 has been put off for too long had IPv6 been implemented years ago, the transition from the older standard to the newer one would have gone much more smoothly. In 1980, Internet Protocol version 4 addresses were defined as 32-bit numbers. This provided a total of 232 IPv4 addresses that’s 4 294 967 296, or 4.2 billion, addresses. This may have seemed like a lot of addresses back in 1980, but today there are many more than 4.2 billion network-connected devices on the planet. Of course, the number of devices connected to the Internet will only continue to grow. To make matters worse, some of these IPv4 addresses are reserved for special cases, so the Internet has fewer than 4.2 billion publically routable IPv4 addresses available to it. There aren’t anywhere near enough publically routable addresses available for every device on the Internet to have a unique one. One thing that’s helped is network-address translation (NAT), which most home networks use. If you have a router in your home, it takes a single publically routable IP address from your Internet service provider and shares it amongst the networked devices in your home. To share the single IPv4 address, it creates a local area network, and each networked device behind the router has its own local IP address.

D) How IPv6 Solves the Problems

To avoid the future exhaustion of IPv4 addresses, IPv6 was developed in 1995. IPv6 addresses are defined as 128-bit numbers, which means there are a maximum of 2128 possible IPv6 addresses. In other words, there are over 3.402 × 1038 IPv6 addresses – a much larger number. In addition to solving the IPv4 address depletion problem by providing more than enough addresses, this large number offers additional advantages – every device could have a globally routable public IP address on the Internet, eliminating the complexity of configuring NAT. IPv6 was finalized in 1998, 14 years ago. You might assume that this problem should have been solved long ago – but this isn't the case. Deployment has been going very slowly, in spite of how long IPv6 has been around. Some software is still not IPv6 compatible, although much software has been updated. Some network hardware may also not be IPv6 compatible – while manufacturers could release firmware updates, many of them would rather sell new, IPv6-ready hardware instead. Some websites still do not have IPv6 addresses or DNS records, and are only reachable at IPv4 addresses. Given the need to test and update software and replace hardware, IPv6 deployment has not been a priority for many organizations. With enough IPv4 address space available, it's been easy to put IPv6 deployment off until the future. With the imminent exhaustion of available IPv4 addresses, this concern has become more pressing. Deployment is ongoing, with "dual-stack" deployment easing the transition – modern operating systems can have both IPv4 and IPv6 addresses at the same time, making deployment smoother.

E) What's wrong with IPv4 and why we are moving to IPv6?

For the past 10 years or so, this has been the year that IPv6 will become wide spread. It hasn't happened yet. Consequently, there is little widespread knowledge of what IPv6 is, how to use it, or why it is inevitable.

4. What's wrong with IPv4?

We've been using IPv4 ever since RFC 791 was published in 1981. At the time, computers were big, expensive, and rare. IPv4 had provision for 4 billion IP addresses, which seemed like an enormous number compared to the number of computers. Unfortunately, IP addresses are not use consequently. There are gaps in the addressing. For example, a company might have an address space of 254 (2^8-2) addresses, and only use 25 of them. The remaining 229 are reserved for future expansion. Those addresses cannot be used by anybody else, because of the way networks route traffic. Consequently, what seemed like a large number in 1981 is actually a small number in 2014. The Internet Engineering Task Force (IETF) recognized this problem in the early 1990s and came up with two solutions: Classless Internet Domain Router (CIDR) and private IP addresses. Prior to the invention of CIDR, you could get one of three network sizes: 24 bits (16,777,214 addresses), 20 bits (1,048,574 addresses) and 16 bits (65,534 addresses). Once CIDR was invented, it was possible to split networks into subnetworks. So, for example, if you needed 5 IP addresses, your ISP would give you a network with a size of 3 bits which would give you 6 IPaddresses. So that would allow your ISP to use addresses more efficiently. Private IP addresses allow you to create a network where each machine on the network can easily connect to another machine on the internet, but where it is very difficult for a machine on the internet to connect back to your machine. Your network is private, hidden. Your network could be very large, 16,777,214 addresses, and you could subnet your private network into smaller networks, so that you could manage your own addresses easily. You are probably using a private address right now. Check your own IP address: if it is in the range of 10.0.0.0 – 10.255.255.255 or172.16.0.0 – 172.31.255.255 or 192.168.0.0 – 192.168.255.255, then you are using a private IP address. These two solutions helped forestall disaster, but they were stopgap measures and now the time of reckoning is upon us. Another problem with IPv4 is that the IPv4 header was variable length. That was acceptable when routing was done by software. But now routers are built with hardware, and processing the variable length headers in hardware is hard. The large routers that allow packets to go all over the world are having problems coping with the load. Clearly, a new scheme was needed with fixed length headers. Still another problem with IPv4 is that, when the addresses were allocated, the internet was an American invention

5. IPv6 and Its Features

The IETF unveiled the next generation of IP in December 1995. The new version was called IPv6 because the number 5 had been allocated to something else by mistake. Some of the features of IPv6 included.

1. 128 bit addresses (3.402823669×10^{38} addresses)

2. A scheme for logically aggregating addresses

3. Fixed length headers

4. A protocol for automatically configuring and reconfiguring your network.

Let's look at these features one by one:

Addresses-The first thing everybody notices about IPv6 is that the number of addresses is enormous. Why so many? The answer is that the designers were concerned about the inefficient organization of addresses, so there are so many available addresses that we could allocate inefficiently in order to achieve other goals. So, if you want to build your own IPv6 network, chances are that your ISP will give you a network of 64 bits (1.844674407×10^{19} addresses) and let you subnet that space to your heart's content. **Aggregation**-With so many addresses to use, the address space can be allocated sparsely in order to route packets efficiently. So, your ISP gets a network space of 80 bits. Of those 80 bits, 16 of them are for the ISPs sub networks, and 64 bits are for the customer's networks. So, the ISP can have 65,534 networks. However, that address allocation isn't cast in stone, and if the ISP wants smaller networks, it can do that (although probably the ISP would probably simply ask for another space of 80 bits). The upper 48 bits is further divided, so that ISPs that are "close" to one another have similar network addresses ranges, to allow the networks to be aggregated in the routing tables. **Fixed length Headers**-An IPv4 header has a variable length. An IPv6 header always has a fixed length of 40 bytes. In IPv4, extra options caused the header to increase in size. In IPv6, if additional information is needed, that additional information is stored in extension headers, which follow the IPv6 header and are generally not processed by the routers, but rather by the software at the destination. One of the fields in the IPv6 header is the flow. A flow is a 20 bit number which is created pseudo-randomly, and it makes it easier for the routers to route packets. If a packet has a flow, then the router can use that flow number as an index into a table, which is fast, rather than a table lookup, which is slow. This feature makes IPv6 very easy to route.

6. Big Problem in IPV

So if IPv6 is so much better than IPv4, why hasn't adoption been more widespread (as of May 2014, Google estimates that its IPv6 traffic is about 4% of its total traffic)? The basic problem is which comes first, the chicken or the egg? Somebody running a server wants the server to be as widely available as possible, which means it must have anIPv4 address. It could also have an IPv6 address, but few people would use it and you do have to change your software a little to accommodate IPv6. Furthermore, a lot of home networking routers do not support IPv6. A lot of ISPs do not support IPv6. I asked my ISP about it, and I was told that they will provide it when customers ask for it. So I asked how many customers had asked for it. One, including me. By way of contrast, all of the major operating systems, Windows, OS X, and Linux support IPv6 "out of the box" and have for years. The operating systems even have software that will allow IPv6 packets to "tunnel" within IPv4 to a point where the IPv6 packets can be removed from the surrounding IPv4 packet and sent on their way.

7. Conclusion

The conclusion of this paper based on study of IPv4 has served us well for a long time. IPv4 has some limitations which are going to present insurmountable problems in the near future. IPv6 will solve those problems by changing the strategy for allocating addresses, making improvements to ease the routing of packets, and making it easier to configure a machine when it first joins the network. However, acceptance and usage of IPv6 has been slow, because change is hard and expensive. The good news is that all operating systems support IPv6, so when you are ready to make the change, your computer will need little effort to convert to the new scheme. So if IPv6 is so much better than IPv4, why hasn't adoption been more widespread as of May 2014, Google estimates that its IPv6 traffic is about 4% of its total traffic The basic problem is which comes first, the chicken or the egg Somebody running a server wants the server to be as widely available as possible, which means it must have anIPv4 address. It could also have an IPv6 address, but few people would use it and you do have to change your software a little to accommodate IPv6. Furthermore, a lot of home networking routers do not support IPv6. A lot of ISPs do not support IPv6.the above defined the study focused on the problem of IPV4 and IPv6.

8. References

[1] Definition of fuzzing, http://en.wikipedia.org/wiki/Fuzzing.

[1] Global IPv6 Statistics Measuring the current state of IPv6 for ordinary users, S.H. Gunderson (Google),RIPE 57 (Dubai, Oct 2008) Security Issues and Preventive Measures for IPV6 on Systems Control and Data Acquisition.

[2] Das, Kaushik (2008). "IPv6 and the 2008 Beijing Olympics". IPv6.com. http://ipv6.com/articles/general/IPv6-Olympics 2008.htm. Retrieved 2008 08 15.

[3] The IETF Portal website; http://www.ipv6tf.org/news/newsroom.php.

[4]http://intelligrid.info/IntelliGrid_Architecture/Technology_Analysis/Anl_Comm_Recomm.

[6] Sean Convery and Darrin Miller, IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation(v1.0,CiscoWhitepaper.http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf.

[7] Donald Wallace (2003-09-01). "How to put SCADA on the Internet". Control Engineering. http://www.controleng.com/article/CA321065.html. Retrieved 2008-05-30. (Note: Donald Wallace is COO of M2M Data Corporation, a SCADA vendor.)

[8] Zhaoxia Xie, et al.; An Information Architecture for Future Power ystems and Its Reliability Analysis. IEEE Transactions on Power Systems, Vol. 17, No. 3, August 2002.

[9] Davies, E.; Krishnan, S.; and Savola, P.; IPv6 Transition/Co-existence Security Considerations, IETF Draft,October 2006.

[10] Zhaoxia Xie, et al.; An Information Architecture for Future Power Systems and Its Reliability Analysis. IEEE Transactions on Power Systems, Vol. 17, No. 3, August 2002.

[11] http://www.tecmint.com/ipv4-and-ipv6-comparison/.