Discrete Logarithm Problem in finite fields and applications to cryptography:

Algorithms, Efficient Implementation and Attacks

by

Divyesh Bhagwanji Chudasama

A thesis submitted in fulfilment of the degree of Master Of Science in Internet Computing and Network Security

Loughborough University

14th September 2012

Abstract

This document contains lots of useful information on how to use luthesis and LaTeX in general to typeset your thesis. Please read it carefully.

This is the abstract. It could have been marked-up in an `abstract` environment, but then would not have appeared in the Table of Contents (ToC).

Acknowledgements

This is the ACKs chapter. It is quite hard to write!

Whilst we're here, it is important to point out that in your real thesis, you should probably keep each chapter in a separate `.tex` file. You bring these into your document using `\include{filename}` (without the `.tex` extension).

I would like to acknowledge Mark Withall, John Whitley and Iain Phillips for contributing code for and help with luthesis.

Contents

List of Figures

List of Tables

List of Corrections

Chapter 1

Introduction

The Internet enjoyed an unprecendented growth across the world in the last decade. According to Internet World Stats,[Reference them here] the number of Internet users increased from 16 million as at December 1995 to a staggering 2,280 million as at March 2012 representing a mammoth 14,250% increase in less than 17 years.

The table below samples the top 20 countries with the highest number of Internet users. These countries account for over 1.7 billion Internet users or 75% of the World's Internet usage and hence a good starting point to analyse and forecast future growth of Internet.

Table Legend.
Column 2. Name of the country
Column 3. Internet users as at year 2000
Column 4. Internet users at at March 2012
Column 5. Internet Penetration rate of the country.
Column 6. The average growth rate of Internet in the twelve years in question.

This table may mean different things to different people which include fertile business market, social networking potentials, e.t.c. However the report will highlight two major things:-

- The average growth of Internet users in the twelve years is around 4658%.
- The average Internet penetration rate for the twelve years in question is close to 50%.

The two major factors that have contributed to this unprecendented growth of the Internet are as follows:-

1. Cheaper and more powerful devices such as laptops, smart phones, e.t.c. Gordon E. Moores law[] which states that the number of transistors in circuits will double every two years, goes a long way in explaining this factor.

#	Country	Users (2000)	Users (2012)	Peneration(%)	Growth(%)
1	China	22,500,000	513,100,000	38.4	2280
2	U.S.A	95,354,000	245,203,319	78.3	257
3	India	5,000,000	121,000,000	10.2	2420
4	Japan	47,080,000	101,228,736	80.0	215
5	Brazil	5,000,000	81,798,000	42.2	1635
6	Germany	24,000,000	67,364,898	82.7	280
7	Russia	3,100,000	61,472,011	44.3	1982
8	Indonesia	2,000,000	55,000,000	22.4	2750
9	U.K	13,200,000	52,731,209	84.1	342
10	France	8,500,000	50,290,226	77.2	591
11	Nigeria	200,000	45,039,711	26.5	22519
12	Mexico	2,712,400	42,000,000	36.5	1548
13	Korea	13,200,000	40,329,660	82.7	211
14	Iran	200,000	36,500,000	46.9	14600
15	Turkey	2,000,000	36,455,000	46.3	1822
16	Italy	13,200,000	35,800,000	58.7	271
17	Phillipines	2,000,000	33,600,000	33.0	1680
18	Vietnam	200,000	30,858,742	34.1	15429
19	Spain	5,387,800	30,654,678	65.6	568
20	Pakistan	133,900	29,128,970	15.5	21754

Table 1.1: World Internet Usage Statistics

2. Gerry Butters law[] states that the amount of data coming out of an optical fiber will keep doubling and the cost decreasing by half every nine months.

The above mentioned laws coupled with the fact that some major countries will push the growth of Internet in the next few years.

1.1 Background

Two end hosts (e.g laptops, smart phones, web servers, sensor devices, e.t.c) communicating over the Internet require an Internet Protocol (IP) address to uniquely identify each other. There are two versions IP currently in use around the world, i.e, Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).
The predominant IP protocol version in use today is IPv4 and is described in RFC 791 []. IPv4 uses a 32-bit addressing scheme which limits its unique addresses to four billion two hundred and ninety four million, nine hundred and sixty seven thousand two hundred and ninety six possible IPv4 addresses.

$$\text{pow}(2,32) = 4,294,967,296$$

The massive growth of the Internet and the advent of technologies that will require IP addresses to function such as pervasive computing [], sensor networks

[] e.t.c means that the address space provided by IPv4 would not be suitable for the continued growth of the Internet. As a long term solution term, the Internet Engineeting Task Force (IETF) developed a next generation Interner Protocol version and called it IPv6. IPv6 is described in RFC 2460 [reference this] was published in December 1998 and uses a 128-bit addressing. This can be represented as follows:

$$\text{pow}(2,128) = 340,282,366,920,938,463,463,374,607,431,768,211,456$$

Apart from the unimaginable address space IPv6 boasts, it has the following benefits:-

- IPv6 is a better optimized IP protocol because it takes all the IPv4 best practices but removes the obsolete IPv4 characteristics.
- IPv6 offers Stateless address autoconfiguration (SLAAC) which enables an IPv6 end host to automatically configure itself when it is connected to an IPv6 network using Internet Control Message Protocol version 6 (ICMPv6) router discovery messages.
- IPv6 is designed to be extensible and offers support for new options and extensions.
- Internet protocol security (IPSec) is a mandatory feature in IPv6, even though it has been back-engineered, it is just an optional feature in IPv4 networks.
- IPv6 routers allow entire subnets to move to a new router connection point without renumbering unlike IPv4.
- IPv6 end hosts can optionally handle packet limits of 4,294,967,295 octets in its payload compared to IPv4's limits of just 65,535 octets. This is called Jumbograms and it greatly improves performance over high MTU links.

1.1.1 Analysis of the IPv6's Slow Adoption

The designers of IPv6 on the heels of its numerous benefits envisioned a dual-stack deployment of the new protocol so that by the time the IPv4 address space is exhausted, IPv6 would be the predominant IP protocol used in the world. However IPv6 has been struck with the "Chicken and Egg" problem where Internet Service Providers (ISPs) and content providers are blaming each other over the non-adoption of IPv6. The content providers are claiming that they cannot connect their content to the Internet on IPv6 because they lack IPv6 connectivity

options. While the ISPs on the other hand do not want to deploy IPv6 if their subscribers are not asking for it because most of the content in the world is on IPv4.

One of the best and least complicated ways to transition a network from IPv4 to IPv6 is by using dual-stack[] deployments. Dual-stack deployments have however been plagued with the dual-stack brokenness problem. This problem arises when IPv6 deployments choose bogus or unreliable IPv6 connections over working IPv4 conncections which results in long delays and the user can not do anything about it until the IPv6 connection has timed out before the IPv4 connection is tried.

These two issues among others where the major highlights of last year's World IPv6 Day which has the Internet Society as the major driving force while large providers such as Google, Yahoo, Facebook, Akamai and CNN participated. The various participants tested their IPv6 connectivity for the entire day, here is a summary of what transpired from a few participants:-
Google. Lorenzo Colitti [] presented the companies figures for the day in question as observed IPv6 traffic was about 0.3 % and dual-stack brokennes wasn not observed and the observation they saw in that respect was an 80-90% reduction in Chrome's dual-stack brokenness.
Yahoo. Igor Gashinsky presenting Yahoo's statistics had the following for the day in question: IPv6 peak traffic observed was about 0.229% and an average of 0.168%. He also stated that the dual-stack brokenness remained the same at approximately 0.022%.
Facebook. Donn Lee's[] Facebook report stated that their IPv6 capable users was about 0.2% and the dual-stack brokenness of users was approximately 0.02% which was an improvement on the 0.03% they had before the world IPv6 day.

We draw two major conclusions from the presenstation of representatives of the world's top providers:-
Dual-stack brokenness has reduced from the figures reported
A full transition to IPv6 is not likely in the short to meduim term.

1.1.2 IPv4 Address Exhaustion Crisis

Internet Assigned Numbers Authority (IANA) on 3rd February 2011 announced the depletion of its pool of public IPv4 addresses and the long anticipated IPv4 address exhaustion struck reality. With the IPv4 address depletion, the Regional Internet Registries (RIRs) will only be allocating a maximum of /22 prefix (1024 IPv4 addresses) to any organization applying for new IPv4 addresses. Already the Asia-Pacific Network Information Center (APNIC) has already started enforcing this policy as a way to ensure an efficient use of its remaining /8 block. This policy

will enable newcomers to enter the IPv4 market. However the wide concensus is that transitioning to IPv6 is the best solution to IPv4 address exhaustion crisis.

With devices getting cheaper for end users and ISPs not having access to a huge amounts of IPv4 addresses to service subscribers, they have turned their attention to mechanisms that can share a single IPv4 address between multiple subscribers.

Sharing a single public IPv4 address amongst multiple subscribers come with alot of issues that ISPs need to be aware of becoming any commitments to a specific mechanisms.

1.2 Aims and Objectives

The aim of this report is three-fold which are as follows:-

- Document first's year research work
- Literature review of the various address sharing mechanisms and their security issues
- Integrate the address sharing mechanisms into Autonetkit[].

Chapter 2

Background

D. Clark et al in RFC 1287 [] Towards the Future Internet Architecture is probably the first documented work to raise the concern of IPv4 address space exhaustion and discussed various ways of extending the IPv4 address space. They proposed three different directions to extend the IP address space which included giving different meaning to IPv4 address.

Another work similar to the current NAT called Dual Network Addressing (DNA) was documented in RFC 1335 was done by Crowcroft and Wang. The report proposed having two sets of IPv4 addresses, internal and external addresses. An internal address is to be used and unique only within private networks while the external address is unique to the entire Internet. Also proposed was External Address Sharing Service (EASS) which would be used to manage the sharing of external address.

An article in the January 1993 issue of ACM Computer Communication Review titled "Extending the IP Internet through Address Reuse"[] and later on published as RFC 1631[] explained the detailed concept behind Network Address Translators (NAT).

Network Address Translators (NAT) translate internal (called private from here) addresses to external (called public) addresses. NAT devices have played a major role in the past few decades due to the unprecendented growth of the Internet. Some of the benefits that made NAT deployment spread like wildfire since its inception include:-
NAT devices have helped meduim sized organizations to multiplex their entire network using limited IPv4 addresses
The major benefits of NAT devices were seen from day one, while their drawbacks were slowly and recently revealed.

Translation of internal addresses were later extended to include port numbers so as to be able to multiplex a bigger set of end hosts, a process that was termed Network Address and Port Translation (NAP-T)[]. The late standardization of

NAPT by the IETF[] led to vendors of the product implementing translators that behaved in different ways[].

The diagram above depicts a typical network topology with address sharing concept which will be used throughout this report. Below is a list of terms that will be re-occuring in all sections of the report:

- **End host**. A device with an IP address (IPv4 or IPv6) on the subscriber network
- **Customer Premises Equipment (CPE)**. A device at the subscriber network which processes traffic between the subscriber and the gateway
- **Subscriber**. Network behind the CPE device
- **Gateway**. Device that processes traffic between subscribers and the public Internet.
- **Access Network**. Network connecting CPE and gateway in ISP network
- **ISP Network**. Network of the Internet service provider

2.1 Network Address and Port Translators

The end hosts D1, D2 and D3 in the figure above route their traffic to the CPE in the access network. The CPE device forwards the traffic to the gateway in the ISP core network. The gateway device translates the private tuple (cite: IP address and port number) to a public tuple and creates a NAT mapping that will be added to its translation table so as to enable future packet exchange between the end host and the public Internet server. There are four ways a gateway translates private tuples into public tuples. These include:-

Static NAT. The gateway device will always translate to a specific IP address

Dynamic NAT. The gateway translates to the first available address from the pool of public IPv4 addresses.

Overloading NAT. Translates the end host addresses to the same public IPv4 address but different port numbers.

Overlapping NAT. This is

The following are the various flavours of port translations in use:-

Cone NAT. The concept behind this flavor is to have the NAT device maintain a one-to-one mapping between the internal (private IP and port) and the external (public IP and port). Whenever this mapping is in place, the external host can send a packet to the internal host.

Restricted Cone NAT. This technique is similar to Cone NAT except that an external server can only send a packet if the internal host had previously sent a packet to the external host. The internal end hosts are basically firewalled until they initiate a connection to the external host. This is sometimes called Address restricted cone NAT because the port number is not important in this NAT flavour.
Port Restricted Cone NAT. The concept here is similar to Restricted Cone NAT except that the port number is considered here. The external server here can only communicate with an internal host if it has the IP address and port number the internal host poked the NAT device with.
Symmetric NAT. Here different external address and port number are assigned to each external server and only that external address may send packets to the internal end host.

2.1.1 Requirements

The following are just a few requirements that NAT devices should have, detailed requirements are documneted in NAT UDP Unicast Requirements[], NAT TCP Requirements[], NAT Behavioral Requirements for ICMP [].

- **Hairpinning Behaviour**. Hairpinning is a behaviour that arises when two end host applications require the gateway device they are behind to relay their traffic. The gateway device can either use the internal tuple of the end hosts called *internal source IP address and port* or allocate an external tuple for the communication called *external source IP address and port*. Using the internal source IP address and port can cause conflicts when implementations are expecting the external source IP address and port. It is recommended that a gateway device must support hairpinning behaviour of type external source IP address and port so as to avoid implementation conflicts.

- **Application Level Gateways (ALGs)**. ALGs are used by protocols such as Session Initiation Protocol (SIP) [], BitTorrent [] and other protocols [][][] that embed IP address information in their payload to communicate with a server in the public Internet transparently. An ALG can request a state in the translation table of a gateway and pass the information to the application of the end host. The end host application can then modify its payload to contain the state to be created by the gateway device.To prevent ALGs from interfering with UNSAF methods, it is recommended that a network administrator should have the privilege of enabling or disabling ALGs.

2.1.2 Issues

- **End-to-End Connectivity**. The Internet was built on the principle that any communication between two end host is a direct end-to-end communication. Having any additional device in between the two end hosts effectively breaks this principle and causes alot of probelms to the subscribers.

- **Impact on Applications**. Address sharing at the ISP network have so much impact on applications that the subscribers use, some example include:

  1. Applications that carry IP address and port information in their payload such as IPSec and VOIP
  2. Applications that use well-known ports and do not support port agility[], will also be impacted by address sharing solutions
  3. Applications that do not use any port number such as ICMP echo messages will require special handling.
  4. Applications that prohibit concurrent connection from the same source address will fail when multiple subscribers sharing an IP address attempt to use the application simultaniously.

  However there have been concerted to come up with techniques that mitigate some of the impacts stated such as UPnP-IGD[], NAT-PMP[], STUN [], Teredo [] and the most comprehensive for solving some of application impacts in NATs is documented in Interactive Connectivity Establishment (ICE) [].

- **State Maintenance**. The need for devices behind address sharing mechanisms to keep sending keep-alive messages periodically so that the session they have opened in the gateway does not close can greatly reduce battery performance.

NAT devices have slowed down the IPv4 address exhaustion over the years but the rate at which the global Internet is growing, it is no longer feasible for ISPs to allocate a single public IPv4 address to a subscriber. Therefore ISPs need to start sharing public IPv4 addresses among multiple subscribers, a technique called **ISP-level address sharing**.

2.2 ISP Address Sharing

The explosive growth of the Internet means that ISPs can not offer a single public IPv4 address to a single subscriber. The wide successes of NAT has sparked

alot of interests and discussions around ISP-level address sharing mechanisms. The proposed mechanisms come with alot of technical issues such as having the address sharing device in the ISPs core network which makes it a little bit more difficult for subscribers to manipulate when needed. These mechanisms propose multiplexing many subscribers from a pool of public IPv4 addresses. Lixia Zhang in "A retrospective view of network address translation" [] said it is likely some form of network address translation boxed will be with us forever. The actions of ISPs with regards to the deployment of address sharing mechanisms within their networks in the next few years will determine the future of the Internet.

The image below depicts the general scenario of multiplexing multiple subscribers on a single public IPv4 address.

In the image above, the various end hosts in the subscriber network can communicate with public Internet server by multiplexing from a pool of IPv4 addresses in the gateway device that is situated in the ISP network. A special purpose IPv4 addressing[] is needed between the CPE in the subscriber/access network the gateway in the access/ISP networ so as to avoid conflicts when using RFC 1918 addresses.

The following are some of the most important and re-occuring terms and concepts used throughout this report.

- **CGN vs A+P**.
- **Statelss vs Stateful**.
- **Routing vs Tunnelling**.
- **Signalling**.
- **Encouraging IPv6 Transition**.

The process in which the end hosts communicate with the gateway and the device's method of translation is what differentiates the various address sharing mechanisms.

2.2.1 Requirements

The following are some requirements deemed necessary for any IPv4 address solution to work properly. These set of requirements build on the NAT requirements we have already discussed in the previous section of this chapter.

- **Logging**. Sharing a single IP address among multiple subscribers come with a number of issues especially when trying to deal with abuse. Law enforcement officials will need more than the IP address of a malicious communication during their investigation. Additional information such as subscriber

identifier (internal source address and port or tunnel endpoint identifier) and timestamp will be needed for Law enforcement officials uniquely to identify a malicous subscriber. The major disadvantage of logging is that under heavy usage, a large storage volume of translations will be created that needs to be saved by the ISP. Address sharing mechanisms should have ways of logging data created during on-going communications.

- **Bulk port allocations**. Some applications require more than one port number for their communication, example of such applications include peer-to-peer application such as BitTorrent. For any outgoing communication, address sharing mechanisms should be able to allocate an external port, a scattered and/or consecutive port set. In order to avoid malicious attackers guessing a set of port numbers, it is recommended however that address sharing mechanisms employ scattered port set so as to provide security.

- **Port Rate Limitation**. Address sharing mechanisms should be able to limit the number of sessions, the number of filters, e.t.c. allocated per mapping and per subscriber. This is necessary so as to have an effective mitigation strategy against inter-subscirber Denial of Service attacks on the resources of the address sharing mechanism.

CGN Requirements [] contains a detailed explanation of the requirments of the various proposed ISP address sharing mechanisms. Sharing addresses at the ISP network is a work in progress and we expect that as more research is carried out on these mechanisms more requirements will be proposed.

2.2.2 Issues

Ford et al[] have research on the various issues plaguing IPv4 address sharing. In the following section we give a short overview on some of the things the report documented.

- **Single Points of Failure**. The introduction of address sharing mechanisms in the ISP network to handle the multiplexing of public IPv4 addresses across multiple subcribers can create single points of failure in the network. ISPs should consider having multiple address sharing mechanisms to handle the multiplexing of the IPv4 address as a way to add redundancy.

- **Traceability**. Monitoring the users of a service will become more complex as address sharing become more prominent in the world we live. This will

greatly affect law enforcement officials and content providers trying to blacklist a user will need to use more information other than an end host's IP address.

- **Additional Latency**. Studies have such as ... have shown that having address sharing mechanisms between subscribers and the public Internet can significantly add latency to the end-to-end communication between two devices. Though some address sharing mechanisms perform significantly better than others, they fare considerably badly when compared to the traditional Internet.

- **Geo-location and Geo-proximity**. Content providers use IP addresses to locate the physical location of a subcriber. This information is used for various reasons which include advertising, licensing restrictions, emergency services, e.t.c. The advent of address sharing threatens this service because the node used by the ISP to multiplex the public IPv4 address amongst multiple subscribers can be in a different city than the subcriber.

Chapter 3

Literature Review

This chapter of the report will be split into two different sections: address sharing mechanisms and security issues.

The first section will be covering an in-depth analysis of the six major address sharing mechanisms introduced in the previous chapter. The analysis will start by looking at the evolution of the mechanism, its numerous features, advantages and disadvantages. A step-by-step look at the address sharing process will lead to an experimental implementation of the address sharing mechanism. The analysis of experimental work and what people think about each mechanism is how the report concludes.

The second section will of the chapter will be looking at the various network security issues that affect the operability of the various address sharing mechanisms. This section starts off by looking at some well-known network security issues that affect the various mechanisms. The report then lists some security issues specific to the mechanisms. For each security issue discussed, appropriate mitigation strategies will be given if available.

3.1 Address Sharing Mechanisms

3.1.1 NAT444

NAT444 is an IPv4 extension technology being considered by Service Providers to continue offering IPv4 service to customers while transitioning to IPv6. This technology adds an extra Carrier-Grade NAT ("CGN") in the Service Provider network, often resulting in two NATs. NAT444 [1] are transition mechanisms that will allow Service Providers to multiplex customers behind a single IPv4 address, which will allow many legacy devices and applications some IPv4 connectivity.

[1] RFC6333

3.1.1.1 Features

3.1.1.2 Process

Advatnages and disadvantages

3.1.1.3 Implementation Notes

3.1.2 Dual Stack Lite

Dual-Stack Lite enables a broadband service provider to share IPv4 addresses among customers by combining two well-known technologies: IP in IP (IPv4-in-IPv6) and Network Address Translation (NAT).
Dual-Stack-capable implements both v4 and v6 from network layer to application layer
Dual-Stack-provisioned has both v4 and v6 addresses on its interface(s).
Three main components of D-S Lite technology include :- B4, softwire and AFTR.

Access Model - Theres no TWICE NAT here, but tunnelling and NAT function. Communications between end users use the same address family, i.e, IPv4-IPv4 and IPv6-IPv6 only during each connection. There is no translation in this mechanism but tunnelling. IPv4 gets encapsulated (@CPENATtunnelling) in IPv6 and decapsulated(@CGNtunnelling and NAT) and then taken to the user with my public IPv4 address(not really but 192.0.0.0/29).. IPv6 to IPv6 communications go directly without any tunnelling

3.1.2.1 Features

CPE
This is the home gateway and provisioned with only IPv6 by the service provider. Does not operate any NAT functionality as that will be handled by the AFTR in the SP network. However i should still have my normal DHCP pool giving out RFC1918 address space to the hosts at home.
The DNS functionality is rather tricky here, so let me try to explain the best i can.. The router should adversities
1) Its the default route to the hosts that acquire the DHCP addresses from it.
2) Its the DNS server in the DHCP Option 6 (DNS Server)
3) Its DNS proxy to accept DNS IPv4 requests from hosts and send them using IPv6 to the SP DNS server..
-Each DNS request will create a binding in the AFTR. A large number of DNS requests may have a direct impact on the AFTRs NAT table utilisation.
-IPv6 communications reach out directly to other IPv6 hosts on the Internet.

B4 - is implemented on a dual-stack-capable node that creates a tunnel to an AFTR.
1) Encapsulation The B4 element provides a multipoint-to-point(IPv4-in-IPv6) tunnel ending on a service provider AFTR.
2) Fragmentation should not happen to the IPV4 packet but should happen after the IPv6 encapsulation and obviously we have to reassemble the packets before decapsulating the IPv4 packet. This happens because the path MTU discovery is not a reliable method to deal with the reduction in effective MTU of the packet. The B4 is should not perform any fragmentation and/or re-assembly as that task will be handle by the AFTR and details explained in AFTR(2).
3) AFTR Discovery can be configured manually, via DHCPv6(M-I-T-M possible), out-of-band mechanism
4) DNS, the B4 element can easily serve IPv6 DNS requests to IPv6 users but not to IPv4 users. This makes it important for the B4 element to implement a DNS proxy that will serve IPv4 users.
5) Interface Initialisation, ¡coming soon¿
6) Well-Known IPv4 Address, IANA has reserved 192.0.0.0/29 in order to avoid conflicts with any other address.
192.0.0.0 is reserved subnet address
192.0.0.1 is for the AFTR element
192.0.0.2 is for the B4 element, however if SP has special config for this address, B4 element can use any other address within the 192.0.0.0/29 address space

AFTR - this element implements a combination of tunnel for decapsulating the IPv6 packet and IPv4-IPv4 NAT.
1) Encapsulation The AFTR provides a point-to-multipoint(IPv4-in-IPv6) tunnel ending at the B4 (@CPENAT) element. oneAFTR-to-manyB4elements
2) Fragmentation As stated above, fragmentation MUST happen after the encapsulation on the IPv6 packet. Here, if the packet size exceeds the tunnel MTU, it is handled as follows:-
- if original IPv4 packet DF bit flag is set, the AFTR discards the packet and sends an ICMP message of type=Unreachable with the code=packet too big and recommends MTU size field set to the size it can handle
- if original IPv4 packet DF bit flag is CLEAR, the AFTR encapsulates the IPv4 packet in IPv6 and then fragments the resulting IPv6 packet in such a way that will not exceed the path MTU to the tunnel exit-point. RFC2473:Section7.2
3) DNS packets not expected to pass through AFTR element because B4 element as described above performs DNS resolution over IPv6.
4) Well-Known IPv4 Addresses The AFTR just as stated above should use 192.0.0.1 reserved by IANA to configure v4-in-v6 tunnels. ICMP supported here.

5) Extended Binding Table There is need to keep a static and extended binding table on the AFTR element to include the IPv6 address of the incoming packets so as to disambiguate from responses. A reserve lookup will be aid the AFTR know how to reassemble(when necessary)IPv6 packets and encapsulating a packet coming back from the Internet.

3.1.2.2 Process

Gateway-Based (C.G.N)
An outbound message 10.0.0.1/10000 is sent to the D-S Lite route and B4 element encapsulates and forwards the packet over the softwire. The tunnel concentrator in the AFTR receives the datagram, decapsulates and sends it to the NAT where the packet is translated it to 192.0.2.1/5000.
An inbound message is received by the AFTR and looks it up in its translation table and translates the source address back to 10.0.0.1/10000. The packet is then forwarded to the softwire concentrator down to the D-S Lite route where the B4 decapsulates the packet and forwards it to the host. There are two interfaces configured on the AFTR that translates pairs of tuple(IP/port). The interfaces are as follows
Network: Translates IPv4 destination address and port to the softwire identifier and port.
Softwire: Translates softwire identifier and port to the IPv4 destination address and port.
When a packet is received on the AFTR network interface, the NAT translator looks up the IPv4-address/port in its translator table, changes the address/port to 10.0.0.1/10000 and forwards it to the softwire. The B4 receives the forwarded packets. decapsulates it and send it to the host. A softwire-ID(IPv6 address), IPv4 address, protocol and port is used to uniquely identify each host on the CPE and the IPv4, protocol and port number of the outgoing packet to the Internet is used for the mapping.

Host-Based (A+P)
An outbound message is sourced with a well-known non-route IPv4 address range reserved by IANA. The host device encapsulates the IPv4 datagram (192.0.0.2/10000) and sends it over the softwire tunnel to the AFTR. The tunnel concentrator in the AFTR receives the datagram, decapsulates and sends it to the NAT where the packet is translated it to 192.0.2.1/5000 and forwards it to the Internet.
An inbound message is received by the AFTR and forwards it to the NAT which looks it up in its translation table and translates the source address back to 192.0.0.2/10000. The packet is then forwarded to the softwire concentrator down

to the B4 inside the host which decapsulates the IPv4 packet and forwards it to the application.

Host-Based

The translation is the same as described above, the only difference is that the source host address must be in the range of the IANA reserved IPv4 address. Packets can be received from the different hosts sourced the same IANA IPv4 address range but different softwire tunnels. Just as in the above description, the softwire-ID(IPv6 address), IPv4 address, protocol and port is used to uniquely identify each individual host.

Deployment Considerations

1) AFTR Service Distribution and Horizontal Scaling - Tunnel endpoints can be placed anywhere within the service provider network and this enables them to group users sharing the same AFTR. These groups can be further divided or merged with other groups at nay point in time. AFTR should not require per-user configuration but per group configuration so that when the group of users increase over time they can still be managed quite well.

2) Horizontal Scaling This enables the service provider start with a few AFTRs and increase them when more capacity is needed.

3) High Availability - D-S Lite has a very simple implementation especially on the customer side as only a tunnel and a default route to the B4 is needed to get IPv4 connectivity. ¡UPDATE¿

4) Logging - The AFTR should be able to log NAT bindings or ways to keep track of IP-ports. This is to enable better troubleshooting when theres a problem and for law enforcement authorities.

Network Considerations

1) Tunnelling Must be done in accordance to RFC2473 and RFC4213.. Update this appropriately

2) Multicast Considerations Update this as well

NAT Considerations

1) NAT Pool The AFTR can have different NAT pools but they MUST NOT overlap. Users can be assigned to different pools. Te AFTR having two interfaces can enable it have disjoint NAT pool assigned to it. A policy at the AFTR can specify a set of B4s use NAT pool 1 and another different set of B4s to use NAT pool 2.

2) NAT Conformance The AFTR must implement behaviour stated in chapter():section() (NAT ICMP, TCP and UDP Behavior)

3) ALGs It is impossible for AFTR to implement every current and future ALG because ALGs consume resources and AFTR supports a large number of B4 elements and hence implementing many ALGs may considerably affect the AFTR.

4) Sharing Global IPv4 Addresses To increase IPv4 utilisation, just like in our NAT444, the AFTR shares a single public IPv4 address among multiple users. The AFTR suffers the same issues as in other Carrier Grade NATs as discussed in chapter():section()
5) Port Forwarding / Keep Alive The Port Control Protocol being standardised by the IETF will enable applications to negotiate with the AFTR to open ports and negotiate keep alive values in order to avoid keep-alive traffic. (*** reference the IETF PCP-proposals here).

3.1.2.3 Implementation Notes

3.1.3 NAT64

NAT64 allows IPv6-only clients to contact IPv4 servers using unicast UDP, TCP, or ICMP. One public address will be assigned to NAT64 translator to share IPv4 addresses among IPv6-only clients. When used in conjunction with DNS64, no changes required in v6 client or v4 server. enable per peer-to-peer comm. techniques.
The two mechanisms NAT64 and DNS64 allow an IPv6-only client to initiate communication with the current large IPv4-servers.

3.1.3.1 Features

NAT64
The NAT64 device has two main parts

Address Translation Mechanism: the NAT64 map IPv6 transport addresses to IPv4 transport addresses and vice versa. In order to do this, the NAT64 device must have two pools of addresses.
IPv6 Pool: This is one or more IPv6 prefixes assigned to the NAT64 translator itself. This prefix(es) is used by the NAT64 to construct
IPv4-converted IPv6 addresses as defined in RFC6052(concatenating prefix w/ IPv4 address being mapped and a suffix)
IPv4 Pool: This is a set of IPv4 addresses usually assigned by a local administrator. This is typically small and dynamically allocated to contending parties.

Protocol Translation Mechanism: Translation done according to RFC 6145(Look into this)
v4 hosts translated to v6 addresses by using RFC6052 and the v6 prefix assigned to to the stateful NAT64 for this purpose.
v6 hosts translated to v4 addresses by using configuring mappings according to RFC 3022

DNS64

This is a mechanisms for synthesising AAAA records from A records. The generated synthetic IPv6 address is generated from the IPv4 address and the IPv6 prefix assigned to the NAT64 device as explained above.

NAT64 is complaint with NAT recommendations stated earlier in this report and also compatible with NAT traversal techniques such as RFC5245 and others.
- Without preexisting state in the NAT64(port forwarding), only IPv6-6 nodes can initiate communications with IPv4 nodes.
- IPv4 nodes can initiate communication only when one of the following is achieved
- Statically configured mappings exists for the IPv6 node
- The IPv6 node recently initiated a session to an IPv4 node and also if the v6 node has used a NAT-traversal technique such as the one mentioned above.
- NAT64 allows multiple IPv6-only nodes to share an IPv4 address to the IPv4 Internet.
- NAT64 device must obviously have at least two interface, IPv6 connected to the IPv6 network and IPv4 interface connected to the IPv4 network.

Access Model Packets generated from the IPv6 side of the network is routed to the NAT64 device where the packet gets translated and forwarded to the IPv4 network to the IPv4 receiver and reverse and sending back packets from the IPv4 network back to the IPv6 client. NAT64 devices require state which contains bindings of the IPv6 address and transport layer information to an IPv4 address and transport layer information. This binding can either be statically configured or created when IPv6-only nodes initiate communication and the translation/binding established. Once the binding has been established, packets flowing in both directions get translated.

3.1.3.2 Process

Advantages and disadvantages

3.1.3.3 Implementation Notes

3.1.4 4RD

3.1.4.1 Features

3.1.4.2 Process

3.1.4.3 Implementation Notes

3.1.5 Lightweight 4over6

3.1.5.1 Features

3.1.5.2 Process

Advantages and disadvantages

3.1.5.3 Implementation Notes

3.1.6 Stateless TUN

3.1.6.1 Features

3.1.6.2 Process

Advantages and disadvantages

3.1.6.3 Implementation Notes

3.2 Security Issues

3.2.1 Traditional Network Security Issues

Introduction and general talk

3.2.1.1 Denial of Service

Overview

- **How it works**.
- **Impact**.
- **Implementation**.
- **Mitigation Strategies**.

3.2.1.2 Filtering

Overview

- **How it works**.
- **Impact**.
- **Implementation**.
- **Mitigation Strategies**.

3.2.1.3 Port Randomization

Overview

- **How it works**.
- **Impact**.
- **Implementation**.
- **Mitigation Strategies**.

3.2.1.4 Routing

Overview

- **How it works**.
- **Impact**.
- **Implementation**.
- **Mitigation Strategies**.

3.2.1.5 Fragmentation

Overview and what will I'll be talking about

- **How it works**.
- **Impact**.
- **Implementation**.
- **Mitigation Strategies**.

3.2.2 Address Sharing Security Issues

Overview and what will I'll be talking about

3.2.2.1 Mechanism Issues

Overview

- **Hair-pinning**.
- **End-to-End**.
- **Traceability** .
- .
- .

3.2.2.2 UPnP-IGD

Overview and what will I'll be talking about

- **How it works**.
- **Impact**.
- **Implementation**.
- **Mitigation Strategies**.

3.2.2.3 P.C.P

Overview and what will I'll be talking about

- **How it works**.
- **Impact**.
- **Implementation**.
- **Mitigation Strategies**.

Chapter 4

Methodology

4.1 Example

4.2 Challenges

4.3 Abstractions

4.4 Implementation

Chapter 5

Conclusions

5.1 Contributions

Here discuss your contributions and future work—and ensure you end on a positive note!

5.2 Recommendations

5.3 Future Works

Chapter 6

Project Plan

6.1 Year One

- **July**.
- **August**.
- **September**.
- **October**.
- **November**.
- **December**.
- **January**.
- **February**.
- **March**.
- **April**.
- **May**.
- **June**.

6.2 Year Two

- **July**. Second Year Organization.
- **August**.
- **September**. CCIE Routing and Switching, CCIE Security and major network security certifications and workshops.

- **October**. CCIE Storage, CCIE Service Provider and Linux certification.
- **November**. Setup of second year testbed and literature review for second year.
- **December**. Continuation of literature review, network security conferences, workshops and getting input from the community.
- **January**. Test Scenarios and metrics, experiments.
- **February**. Experiments, report, papers and posters writing.
- **March**. Experiments and result analysis. Report and paper writing.
- **April**. Report writing.
- **May**. Report writing.
- **June**. Third year organization and proof-reading report.

6.3 Year Three

- **July**. Holiday and literature review
- **August**. More literature review and practical experiments
- **September**. Gathering input form the community through conferences, workshops, events and other means
- **October**. Final year experiment setup: test scenarios, aims and objectives, considerations, challenges and goals
- **November**. Experiment and results
- **December**. Experiment and results
- **January**. Experiment and results
- **February**. Report writing and final experiments
- **March**. Report writing
- **April**. Report writing
- **May**. Report writing and proof-reading
- **June**. Proof-reading

```
\cleardoublepage
\phantomsection
\addcontentsline{toc}{chapter}{References}
```

Don't worry about the use of `\cleardoublepage`—it does The Right Thing(tm) when the document is single-sided. Also, the `\phantomsection` is required if you are using **pdflatex** and hyperref, as is *strongly recommended* for luthesis documents.

If you are using gcite—and therefore biblatex—the procedure for adding the bibliography is slightly different and you don't need to add the above commands. This is all explained in the gcite manual.

References

[1] Matthew Tylee Atkinson and Iain Phillips. gcite. http://www.ctan.org/tex-archive/macros/latex/exptl/gcite, 2007.

Appendix A

Example Appendix

You should avoid using these but for supporting evidence that is not directly related to the main body of the thesis—e.g. to store large tables of results, where in the main text you only want to tell the story of and give the flavour of the results. You may also like to include a list of your publications.