



Information Technology Protective Security Services

IPv6-to-IPv4 Transition And Security Issues

20 February 2008

Information Technology Protective Security Services

Block K, Information Technology & State Store Building,

Jalan Gadong, BE1110

Brunei Darussalam

TABLE OF CONTENTS

INTRODUCTION	3
Ipv4 Vs. Ipv6	3
Ipv4 Security Issues	3
Ipv6: The Features.....	4
IPsec	5
COMPARISON	6
TRANSITION CONSIDERATION IN IPV6.....	7
6to4 (Tunneling)	7
TRT (Translation)	8
Dual Stack Approach	9
CONCLUSION.....	10
REFERENCES	11

INTRODUCTION

IPv4 vs. IPv6

The current generation of IP, version 4, (IPv4), is roughly 20 years old. Since its inception in the 80's, it has supported the Internet's rapid growth during that time. It has been proven to be robust, easily implemented and interoperable. This is a tribute to its initial design. IPv4 uses a 32-bit address space, in which can accommodate about 4 billion unique addresses. While that sounds substantial, the practical number of usable addresses is actually much lower. The current Internet has grown much bigger than was anticipated. There are several problems such as impending exhaustion of the IPv4 address space, configuration and complexities and poor security at the IP level.

To overcome these concerns, in the early 90's, IETF (Internet Engineering Task Force (IETF), began developing a new IP protocol namely IPv6 (other name, Next Generation IP, IPng). It will use a 128-bit address space. In the other hand, it would support unique addresses well beyond the trillions. It can support **340, 282, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456** unique addresses! It will not only eliminate the shortcomings of IPv4, but also unlock new features and services.

IPv4 Security Issues

IPv4 was created with no security in mind. Because of its end-to-end model, IPv4 relies on the end-hosts to provide the appropriate security during communication. Below are some security threats on IPv4:

- Denial of Service Attacks (DOS): it is an attempt to make a computer resource unavailable to its intended users. One common method involves flooding the target host with requests, thus preventing valid network traffic to reach the host
- Viruses & Worms distribution: these malicious code/programs can propagate themselves from one infected or compromised hosts to another. This distribution is aided by the small address space of IPv4
- Man-in-the-middle attacks (MITM): an attacker is able to read, insert and modify at will messages between two hosts without either hosts knowing that their

communication has been compromised. This is because IPv4's lack of suitable authentication mechanisms

- Fragmentation attacks: Different Operating system has their own method to handle large IPv4 packets and this attack exploits that method. For example the "ping of death" attacks. This attack uses many small fragmented ICMP packets which when reassembled at the destination exceed the maximum allowable size for an IP datagram which can cause the victim host to crash, hang or even reboot
- Port scanning and reconnaissance: this is used to scan for multiple listening ports on a single, multiple or an entire network hosts. Open ports can be used to exploit the specific hosts further. Because of the small address space, port scanning is easy in IPv4 architecture
- ARP Poison: ARP poison attack is to send fake, or 'spoofed', ARP messages to a network. The aim is to associate the attacker's MAC address with the IP address of another node. Any traffic meant for that IP address would be mistakenly sent to the attacker instead

Many techniques or method had been developed to overcome the abovementioned security issues. For instance, the use of 'IPSec' to aid the use of encrypted communication between hosts, but this is still optional and continues to be the main responsibility of the end hosts.

IPv6: The Features

Backward compatibility:

The main objective for successful transition is to allow IPv6 and IPv4 hosts to interoperate. A second objective is to allow IPv6 hosts and routers to be deployed in the Internet in a highly diffuse and incremental fashion, with few interdependencies. The third objective is easy transition for end- users, system administrators, and network operators.

The IPv6 transition mechanisms are a set of protocol mechanisms implemented in hosts and routers, with some operational guidelines for addressing and deployment, designed to make the transition to work with as little disruption as possible. These will ensure that IPv6 hosts can interoperate with IPv4 hosts in the Internet up until the time when IPv4 addresses run out.

The IPv6 transition mechanisms provide a number of features, including:

- Incremental upgrade and deployment. Individual IPv4 hosts and routers may be upgraded to IPv6 one at a time without requiring other hosts or routers to be upgraded at the same time. New IPv6 hosts and routers can be installed one by one.
- Minimal upgrade dependencies. The DNS server must first be upgraded to handle IPv6 address records before upgrading hosts.
- Easy Addressing. For IPv4 hosts or routers being upgraded to IPv6, they may continue to use their existing address. So no new address assignment needed.
- Minimal operational upgrade cost and training expenses. Little or no preparation work is needed in order to upgrade existing IPv4 systems to IPv6, or to deploy new IPv6 systems.

IPSec

IPv4 offers IPSec support, but it is optional. Support for IPSec in IPv6 implementations is not an option but a requirement.

IPSec consists of a set of cryptographic protocols that provide for securing data communication and key exchange.

IPSec uses two wire-level protocols:

- *Authentication Header (AH)* - provides for authentication and data integrity
- *Encapsulating Security Payload (ESP)* - provides for authentication, data integrity, and confidentiality

In IPv6 networks, both the AH header and the ESP header are defined as extension headers. Additionally, IPSec provides for a third suite of protocols for protocol negotiation and key exchange management known as the Internet Key Exchange (IKE). This protocol suite provides the initial functionality needed to establish and negotiating security parameters between endpoints. In addition it keeps track of this information to ensure secure communication at all times.

COMPARISON

The following table compares the key characters of IPv6 and IPv4:

Subjects	IPv4	IPv6	IPv6 Advantages
Address Space	4 Billion Addresses	2^{128}	79 Octillion times the IPv4 address space
Configuration	Manual or use DHCP	Universal Plug and Play (UPnP) with or without DHCP	Lower Operation Expenses and reduce error
Broadcast / Multicast	Uses both	No broadcast and has different forms of multicast	Better bandwidth efficiency
Anycast support	Not part of the original protocol	Explicit support of anycast	Allows new applications in mobility, data center
Network Configuration	Mostly manual and labor intensive	Facilitate the re-numbering of hosts and routers	Lower operation expenses and facilitate migration
QoS support	ToS using DIFFServ	Flow classes and flow labels	More Granular control of QoS
Security	Uses IPsec for Data packet protection	IPsec becomes the key technology to protect data and control packets	Unified framework for security and more secure computing environment
Mobility	Uses Mobile IPv4	Mobile IPv6 provides fast handover, better router optimization and hierarchical mobility	Better efficiency and scalability; Work with latest 3G mobile technologies and beyond.

TRANSITION CONSIDERATION IN IPv6

There are number of IPv6-to-IPv4 transition technologies are introduced to overcome the interoperability between IPv6 and IPv4 issues, mainly in the “IETF ngtrans working group”. The following focused on specific implementation:

- Tunneling
- Translation
- Dual-stack

Specific examples:

6to4 (Tunneling)

6to4 is a system that allows IPv6 packets to be transmitted over an IPv4 network without the need to configure communication tunnels. Routings are also in place that allows 6to4 hosts to communicate with hosts on the IPv6 environment. This is used when an end site or end user wants to connect to the IPv6 environment using their existing IPv4 connection.

6to4 is especially significant during the initial phase of IPv6 deployment to full, native IPv6 connectivity. However, it is intended only as transition mechanism and not permanent.

How it works

- Address block allocation – for any 32-bit global IPv4 address that is assigned to a host, a 48-bit 6to4 IPv6 prefix can be constructed for use by that host by pre-pending 2002 (in Hex) to the IPv4 address. For example:

IPv4 address:	202.142.131.202
IPv4 address in Hex:	C4: 8E: 83: CA
Append with IPv6 prefix:	2002:C48E:83CA::/48

- Encapsulation and Transmission – 6to4 encapsulates IPv6 packets inside IPv4 packets for transmission over an IPv4 network
- Routing between 6to4 and native IPv6 – to allow hosts and networks using 6to4 addresses to exchange traffic with hosts using ‘native’ IPv6 addresses, ‘relay routers’ have been established. This relay routers help the transmission of packets between IPv4 and IPv6 network possible

Security issues

Even if the 6to4 system properly implemented, it also pose security threats. Following are some of the threats:

- Denial-of-Service (DoS) attacks
- Reflection Denial-of-Service (DoS) attacks
- Service Theft, in which a malicious node/site/operator may make unauthorized use of service

The four main potential problems are:

- 6to4 routers not being able to identify whether relays are legitimate
- Wrong or impartially implemented 6to4 router or relay security checks
- 6to4 architecture used to participate in DoS or reflected DoS, making another attack harder to trace
- 6to4 relays being subject to “administrative abuse”

TRT (Translation)

Transport Relay Translator (TRT) enables IPv6-only host to exchange TCP, UDP traffic with IPv4-only host. It works similar to Network Address Translator where it translates (TCP, UDP) IPv6 to (TCP, UDP) IPv4, or vice versa.

Pros:

- Unlike other translation, TRT does not need extra modification on both initiating host nor on the IPv4-only destination hosts.
- TRT is free from taking care of path MTU and fragmentation and fragmentation issues

Cons:

- TRT supports bidirectional traffic only, thus can be an issue with the IPv6-to-IPv4 header converters that support unidirectional multicast datagram's.
- Like Network Address Translator it needs a stateful TRT system between the communicating peers

Security Consideration

- Similar to an SMTP open relay, TRT for traffic to IPv4 can be abuse by malicious user, which is similar to circumventing ingress filtering, or to achieve some other improper use. Access control can be implement to prevent such improper usage
- Improper TRT implementation may be subject to buffer overflow attack, but this kind of issue is implementation dependent.
- Due to the nature of TCP/UDP relaying service, it is not recommended to use TRT for protocols that use authentication based on source IP address (i.e., rsh/rlogin).
- A transport relay system intercepts TCP connection between two nodes. This may not be a legitimate behavior for an IP node.
- IPsec cannot be used across a relay. Thus defeat the security purpose of Implementing IPv6
- Use of DNS proxies that modify the RRs will make it impossible for the resolver to verify DNSsec signatures.

Dual Stack Approach

IPv6 was delivered with a lot of migration techniques but many were ultimately rejected and today a small set of practical approaches is left.

One technique, called dual stack, involves running IPv4 and IPv6 concurrently. End-hosts and network devices run both protocols, and if IPv6 communication is detected that is the favored protocol.

Common Dual-Stack Strategy

One common dual-stack migration approach is to make the transition from the network core to the network edge. This involves enabling two TCP/IP protocol stacks on the WAN core routers, then perimeter routers and firewalls, then the server-farm routers and finally the desktop access routers.

After the network supports IPv6 and IPv4 protocols, the process will enable dual protocol stacks on the servers and then the edge computer systems.

Security Issues on Dual-Stack

Enterprises that run dual-stack device will have to tackle the vulnerabilities of both protocols.

Dual-stack operation can raise other security problems if consistent security policies are not created for both IPv6 and IPv4 traffic. For example, if a firewall is not configured to apply the same level of screening to IPv6 packets as for IPv4 packets, the firewall may let IPv6 pass through to dual-stack hosts within the enterprise network, potentially exposing them to attack.

CONCLUSION

This paper discussed the brief introduction of IPv6-to-IPv4 and their comparison. As well as the different tools and techniques for IPv4-to-IPv6 transition and their security issues.

Transitioning technologies always poses security threats, for instance most security related products (firewall/IDS/IPS) have not been programmed to inspect IPv6 packets in depth thus can allow malicious packets to pass through by taking advantage on the encapsulation of IPSEC in IPv6. There are tools developed for creating covert channels that can pass undetected through most firewalls and intrusion detection systems such as "VoodooNet" or "v00d00n3t"

Based on our research we concluded that the transition to IPv6 network should be carefully planned. We need to carefully study the requirement for the transition and address the security related issues on the implementation.

Reference:

Title: IPv6: Dual-stack where you can; tunnel where you must

Author: Scott Hogg, Network World, 09/05/07

Link: <http://www.networkworld.com/news/tech/2007/090507-tech-uodate.html?page=1>

Title: IPv6 Security Issues

Author: Samuel Sotillo, East Carolina University

Link: http://www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf

Title: Security Implications of IPv6

Author: Michael H. Warfield

Link: <http://documents.iss.net/whitepapers/IPv6.pdf>

Title: 6to4

Link: <http://en.wikipedia.org/wiki/6to4>

Title: Technical and Economic Assessment of Internet Protocol, Version 6 (IPv6)

Author: IPv6 Task Force, U.S. Department of Commerce

Link: <http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/ipv6final3.htm>

Title: Cisco IOS IPv6 Services Integration and Co-Existence

Author: Patrick Grossetete, Cisco System, Cisco IOS IPv6 Product Manager

Link: www.ipv6.or.kr/ipv6summit/Download/3rd-day/Session-IV/s-4-1.ppt