IPv6 migration challenges and Security

ITU Regional Workshop for the CIS countries

Recommendations on transition from IPv4 to IPv6 in the CIS region ,

16-18 April 2014

Tashkent , Republic of Uzbekistan

Desire.karyabwite@itu.int

IEE/TND
International Telecommunication Union

Contents

- Introduction
- IPv6 Addressing
- IPv6 Address Management
- Migration Challenges
- IPv6 security guideline
- Conclusion

Introduction

- IPv6 was originally specified in the mid-1990's to address a then-urgent need to supplement the rapidly diminishing IPv4 address space
- More and more enterprises were supplementing their internal networks to support the TCP/IP protocol suite in order to enable connection to the global Internet
- IPv4 address space availability is diminishing throughout the world. Every Regional Internet Registry (RIR) has issued notifications that IPv4 space availability is limited and will be exhausted within "a few years."

IPv6 Addressing

The management of various currently used naming and addressing resources

	Name	Address
Internet	Domain name	IP address
Fixed telephony	E.164 number	Q.708 ISPC
Mobile telephony	E.164 number	E.212 IMSI

Key features of IPv4 and IPv6

		IPv4	IPv6
Packet Format	Size of IPv6 header	Variable size	Constant size
	Optional headers	Optional headers	Extension headers and options
Addressing	Addressing spaces	Lack of address spaces	Large address spaces
	End-to-end communications	No	Yes
	Types of addresses	Unicast, multicast and broadcast	Unicast, multicast and anycast
	Scopes of addresses	Local and global	Link-local, local and global
	Address configuration to an interface	A address	Multiple addresses
	Address allocation to an equipment	Multiple interface/addresses	Multiple interfaces/addresses
	Address Autoconfiguration	Using private addresses	Using public addresses

		IPv4	IPv6
	Hierarchical addressing	–	Yes
	Address Renumbering	–	Yes
QoS	Management of service conflicts	Type of Service field	Traffic class field
	Identification of traffic flows	None	Flow label field
	Recognition of control/expedite data	None	Hop-by-Hop extension header
Security	AH header	Optional	Mandated
	ESP header	Optional	Mandated
Mobility	Detection of new networks	–	RA messages
	Generation of new addresses	–	Autoconfiguration
	Mobility headers	–	Mandated
	Option header: Destination option, routing, etc.	Optional	Mandated

IPv6 Address Management

Address Capacity

The most striking difference between IPv4 and IPv6 is the tremendous expansion of IP address space size. Whereas IPv4 uses a 32-bit IP address, IPv6 uses 128 bits.

- A 32-bit address system provides a maximum of 2^{32} addresses or 4.2 billion addresses.
- A 128-bit address system provides 2^{128} addresses or 340 trillion trillion trillion addresses

IPv6 Addressing Format

IPv4 addresses are represented in dotted decimal format where the 32-bit address is divided into four 8-bit segments, each of which is converted to decimal, then separated with "dots."

IPv6 addresses are represented using hexadecimal. The 128 bit IPv6 address is divided into eight 16-bit segments, each of which is converted to hexadecimal, then separated by colons.

Each hexadecimal "digit" represents four bits per the mapping of each hex digit (0-F) to its four-bit binary mapping.
Each hex digit corresponds to four bits with possible values of:

0 = 0000	4 = 0100	8 = 1000	C = 1100
1 = 0001	5 = 0101	9 = 1001	D = 1101
2 = 0010	6 = 0110	A = 1010	E = 1110
3 = 0011	7 = 0111	B = 1011	F = 1111

Two forms of abbreviation are permitted when writing IPv6 addresses

1) Leading zeroes within a quad-hex section, i.e., between colons, may be dropped.
e.g

could be abbreviated

4C62:E849:5F62:AB41:0:0:0:801.

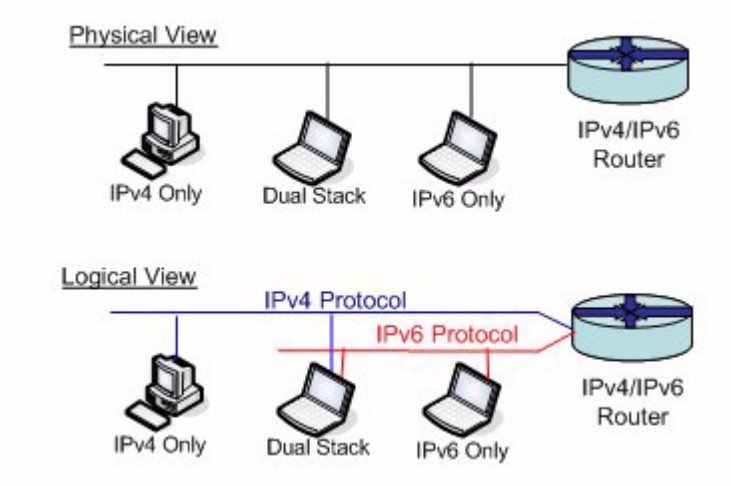
2) The use of a double colon to represent one or more consecutive sets of quad-hex zero strings.
e.g

could be abbreviated

4C62:E849:5F62:AB41::801

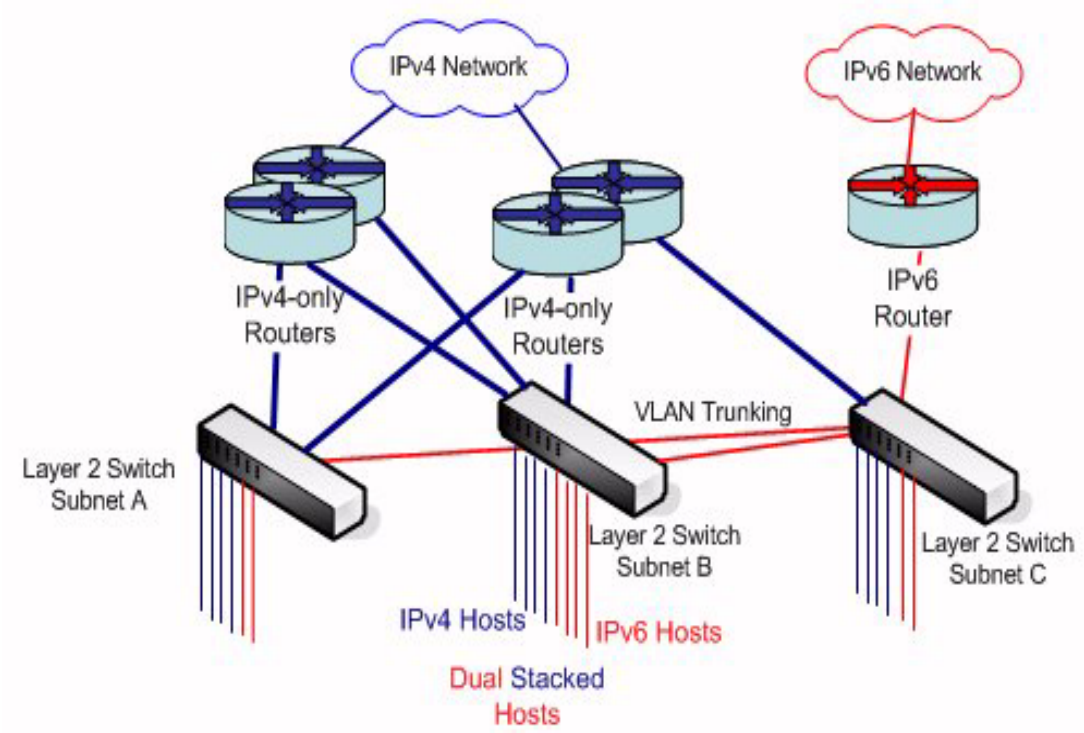
Migration Challenges

A variety of technologies are available to facilitate the migration to IPv6. These technologies are identified according to the following basic categories



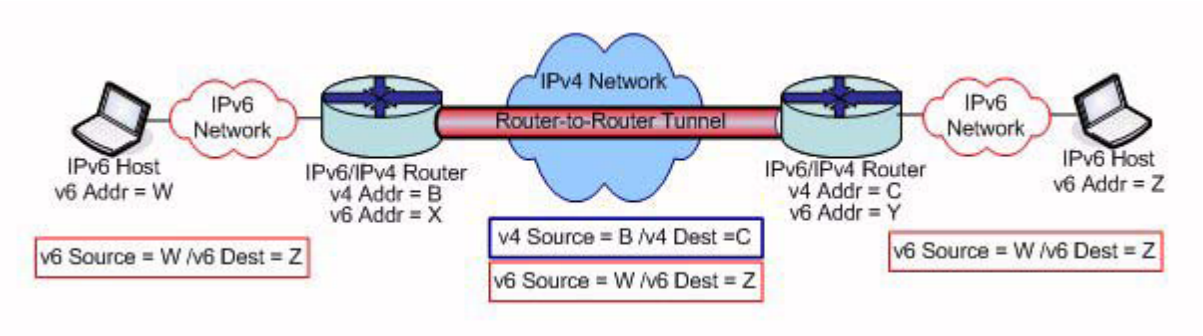
Dual-stacked Network Perspectives

a) Dual stack : support of both IPv4 and IPv6 on network devices. There will be a ***transition phase*** (expected to last for 10, 20 or even more years) when IPv4 and IPv6 will co-exist on the same machines (technically often referred to as "***dual stack***") and be transmitted over the same network links.

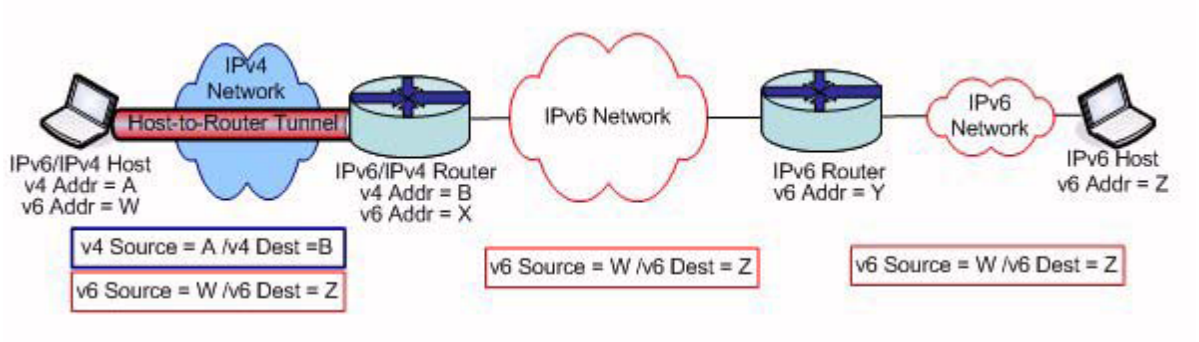


Dual-stacked VLAN Network

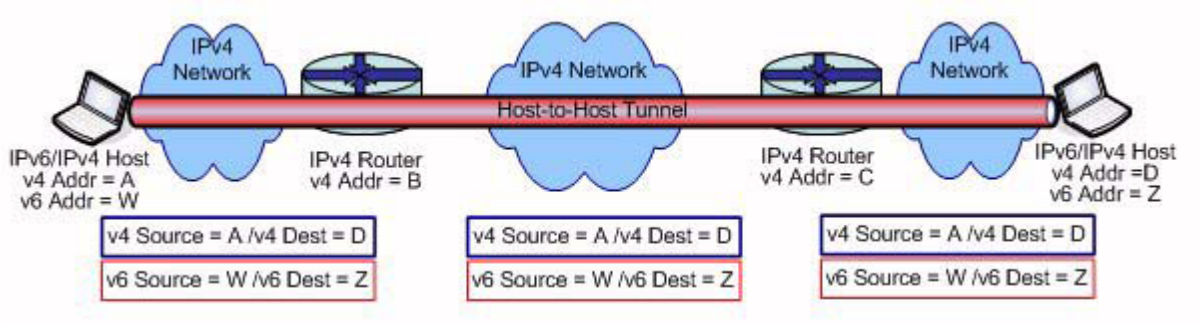
b) Tunneling : encapsulation of an IPv6 packet within an IPv4 packet for transmission over an IPv4 network. Technically referred to as "***tunnelling***", it allows IPv6 packets to be transmitted using IPv4 addressing and routing mechanisms and ultimately vice versa. This provides the technical basis for the step-by-step introduction of IPv6



Router-to-Router Tunnel

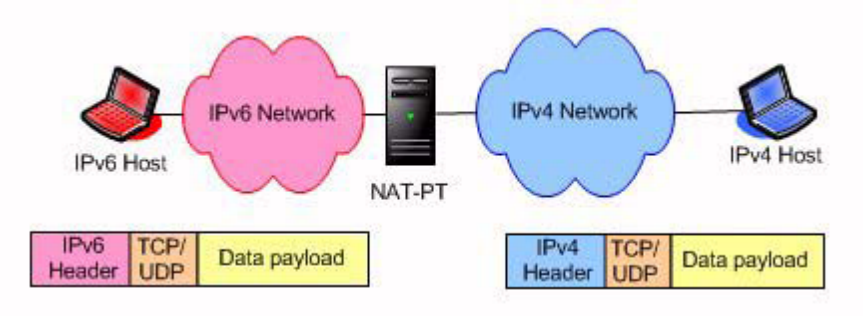


Router-to-Host Tunnel Configuration

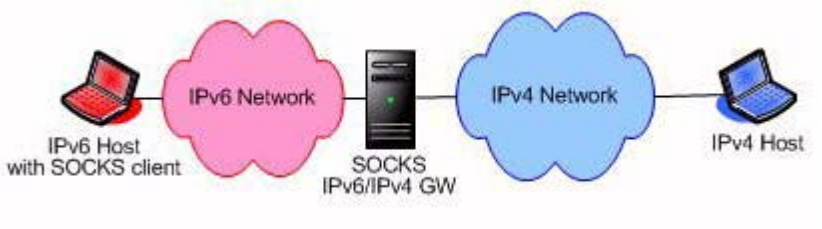


Host-to-Host Tunnel Configuration

c) Translation : address or port translation of addresses such as via a gateway device or translation code in the TCP/IP code of the host or router



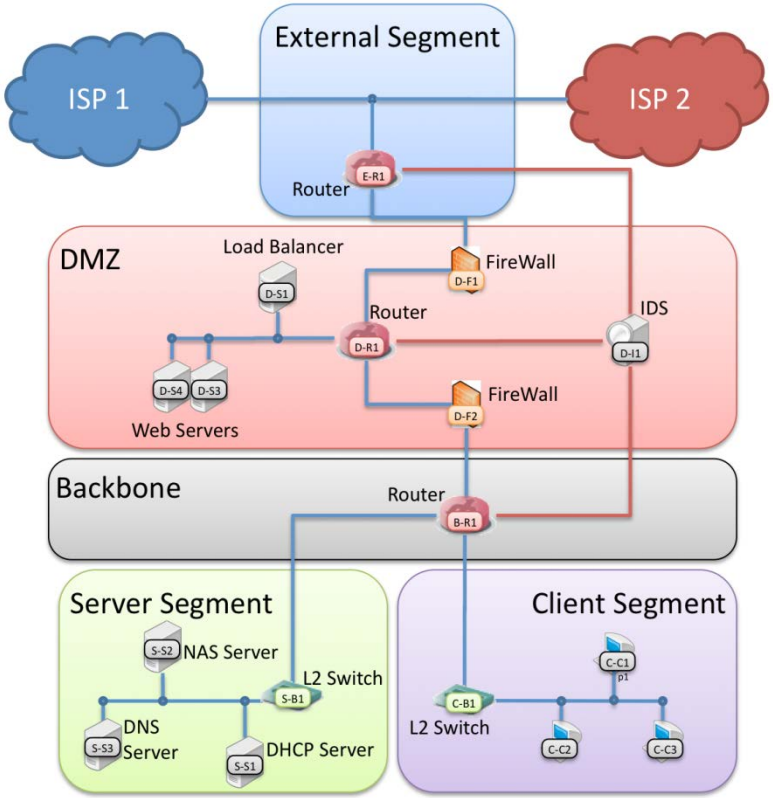
NAT-Port Translation Deployment (NAT-PT Deployment)



Host-to-Host Tunnel Configuration

IPv6 security guideline

General topology of IPv6 network (including transition environment to IPv6 where there exist three different types of hosts: IPv4 only, IPv6 only and IPv4/IPv6-enabled)



Topology of IPv6 network

5 segments: external segment, DMZ, backbone, server segment and client segment

Client/Server devices

- **Threat 1:**

IPv6 hosts can automatically configure their addresses (e.g., global addresses) using Internet Control Message Protocol version 6 (ICMPv6) Router Advertisement (RA) messages. Since they also can choose a default router based on RA messages, RA messages can be used for man-in-the-middle attack. In other words, if a malicious node sends a forged RA message where the default router is set to itself to victim hosts, the malicious node is able to steal and watch all traffic of the victim hosts.

- **Measure 1:**

To minimize the security risk by forged RA messages, it is recommended that each host discards all of RA messages with an extremely short lifetime

Threat 2:

When IPv6 hosts configure their addresses using RA messages, they have to conduct Duplicate Address Detection (DAD) procedure to verify the uniqueness of the tentative addresses on a link.

During the procedure for detecting duplicate addresses, IPv6 hosts that have tentative addresses send Neighbor Solicitation (NS) messages on the link and a node already using the tentative address replies with a Neighbor Advertisement (NA) message. If there is no response, the tentative address can be assigned to the interface of IPv6 hosts. However, a malicious host on the link can prevent IPv6 hosts from obtaining their addresses: if a malicious host always replies NA messages against NS messages of other IPv6 hosts, they are unable to obtain their addresses

Measure 2:

If administrators check the number of IP addresses that each node has and set its limitation for every host, the security risk by the malicious DAD can be mitigated. To this end, administrators can use open source tools such as NDPMon. In addition, a switch is able to detect malicious DADs by controlling the pair of the MAC address of hosts and the physical port connected to the host

IPv6 Technical Verification Consortium

Activities of the Consortium

Consortium members inspect vulnerabilities of their IPv6-enabled products and solutions such as network devices (e.g., router, switch, NAT, load balancer), security appliances (e.g., IDS, IPS, Firewall) and network service equipment (e.g., proxy server, DHCP server, Web server, DNS server) with respect to the IPv6 security issues that have been studied in NICT (National Institute of Information and Communications Technology).

Consortium members also share all of the discovered vulnerabilities from the inspection with each other and devise countermeasures against them, so that the consortium can contribute to make more secure and stable IPv6-based networks. The direction of the activity is decided under consensus of all consortium members and its main goal is to make the future IPv6-based Internet more secure and stable

Conclusions

- ***Simplified packet format***

IPv6 headers are simplified from IPv4 headers. Some IPv4 header fields have been dropped or made optional to limit their bandwidth cost. They also have a constant size to reduce the common processing cost of packet handling.

- ***Expanded addressing scheme***

IPv6 addressing schemes have a large addressing space due to an increased size of the IP address fields to support more levels of addressing hierarchy, a much greater number of addressable nodes and interfaces, and a simpler autoconfiguration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. In addition, a new type of address called an "anycast address" is defined and is used to send a packet to any of a group of nodes.

- ***QoS***

A flow label and traffic class fields in IPv6 header are added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service. In addition, IPv6 hop-by-hop header with router-alert option will indicate the contents of IPv6 packets to support the selective processing of the intermediate nodes.

- ***Security support***

IPv6 supports built-in IPsec services such as authentication, data integrity and data confidentiality using authentication header (AH) and encapsulating security payload (ESP) extension headers. These enable end-to-end security services via global IP addresses even though intermediate nodes do not understand the IPsec headers.

- ***Mobility support***

IPv6 capabilities such as neighbour discovery, address resolution and reachability detection support the mobility services using destination option, routing and mobility extension headers.

Thank you for your Attention