CyberSecurity MALAYSIA

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

In conjunction with WIF-KL 2012

WIF KL WORLD INNOVATION FORUM KUALA LUMPUR

csm-ace 2012 CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION

CYBERSECURITY RISK & COMPLIANCE FOR ECONOMIC TRANSFORMATION

www.csm-ace.my

IPv6 Security Issues and Challenges

Dr. Omar A. Abouabdalla

(omar@ipv6global.my)

Head Technology Consultant

IPv6 Global Sdn Bhd

7 November 2012

IPv6 GLOBAL

IPv6

TO MIGRATE OR NOT TO MIGRATE?

- It's not an option.
- Either we migrate or we will be left behind.
- Malaysian government has mandated they will be IP native by end of 2015.
- Malaysian major trading partners including the U.S., China and India has already started aggressively migrating to IPv6. If we want to continue to be relevant, communicate and do business with these countries, we will have to migrate.

What's the problem?

- We have firewalls and Intrusion Detection Systems – so we're safe from outside attack.
- VPNs, SSH, etc. allow secure remote access.
- SSL/TLS protects web access – so phishing attacks don't work.
- Virus scanning is effective - so viruses are a thing of the past.
- Security patches applied – The patches never break

- complete built-in security.
- And cows can fly!

IPv4 to IPv6 Challenging Move

- The exhaustion of the finite pool of IPv4 addresses.
- IPv6 deployment is critical to safeguarding the future expansion of the internet.
- IPv6 deployment comes with its own set of challenges, and security issues.
- Networks need to be dual-stack during the transition phase.
- In most cases, settings will not be automatically copied between IPv4 and IPv6.
- Whenever you make a change for one protocol you have to do it for the other, which doubles the chances of making a mistake.

Some interesting aspects about IPv6 security

- We have much less experience with IPv6 than with IPv4.
- IPv6 implementations are much less mature than their IPv4 counterparts.
- Security products (firewalls, NIDS, etc.) have less support for IPv6 than for IPv4.
- The complexity of the resulting network will greatly increase during the transition/co-existence period:
  - Two internetworkin protocols (IPv4 and IPv6)
  - Increased use of NATs
  - Increased use of tunnels
- Lack of trained human resources.

Brief comparison between IPv6 and IPv4

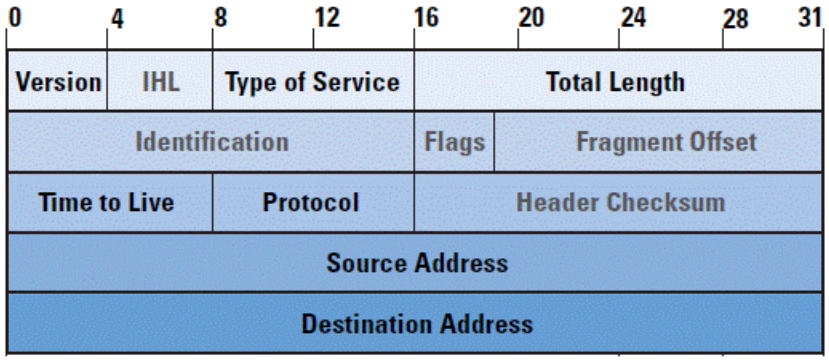
- IPv6 and IPv4 are very similar in terms of *functionality* (but not in terms of *mechanisms*)

	IPv4	IPv6
Addressing	**32 bits**	**128 bits**
Address Resolution	**ARP**	**ICMPv6 NS/NA**
Auto-configuration	**DHCP & ICMP RS/RA**	**ICMPv6 RS/RA & DHCPv6 (recommended)**
Fault Isolation	**ICMP**	**ICMPv6**
IPsec support	**Optional**	**Recommended (not mandatory)**
Fragmentation	**Both in hosts and routers**	**Only in hosts**

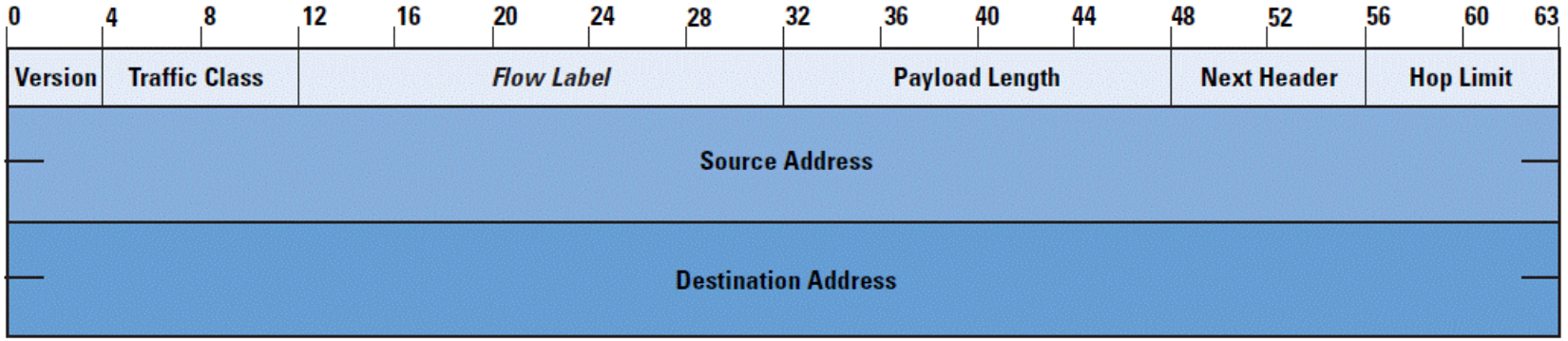
Brief comparison between IPv6 and IPv4

- Header formats:

IPv4 Header



IPv6 Header



Flow Label

- The three-tuple {Source Address, Destination Address, Flow Label} was meant to identify a communication flow.
- Currently unused by many stacks – others use it improperly
- Speficication of this header field, together with possible uses, is “work in progress” at the IETF.
- Potential vulnerabilities depend on the ongoing work at the IETF:
  - Might be leveraged to perform “dumb” (stealth) address scans.
  - Might be leveraged to perform Denial of Service attacks.

Hop Limit

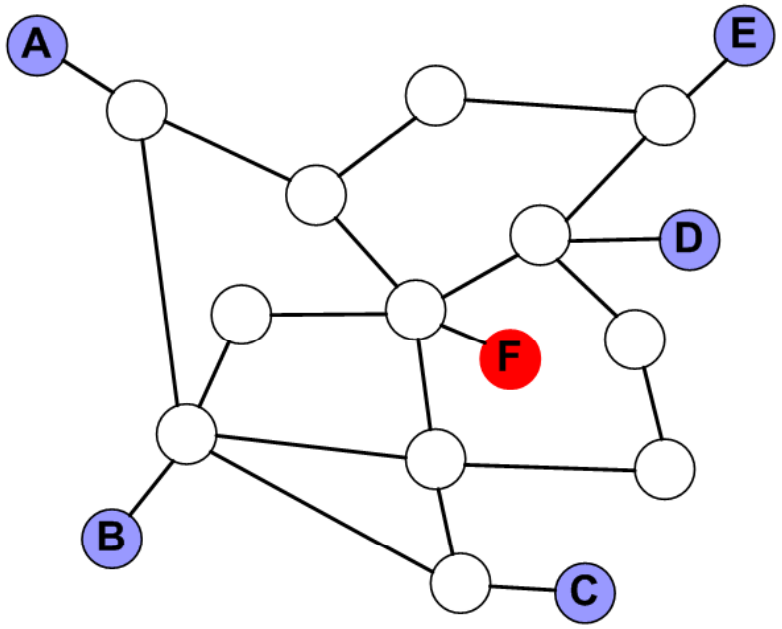
- Analogous to IPv4's "Time to Live" (TTL).
- Identifies the number of network links the packet may traverse.
- Packets are discarded when the Hop Limit is decremented to 0.
- Could be leveraged for:
  - Detecting the Operating System of a remote node.
  - Fingerprinting a remote physical device.
  - Locating a node in the network topology.

Hop Limit: Fingerprinting Devices or OSes

- Different Oses use different defaults for the “Hop Limit” (typically a power of two: 64, 128, etc.)
- If packets originating from the same IPv6 addresses contain very different “Hop Limits”, they might be originated by different devices. E.g.:
  - Packets from FTP server 2001:db8::1 arrive with a “Hop Limit” of 60
  - Packets from web server 2001:db8::2 arrive with a “Hop Limit” of 124
  - We infer:
    - FTP server sets the Hop Limit to 64, and is 4 “routers” away.
    - Web server sets the Hop Limit to 128, and is 4 “routers” away.
    - Detecting the Operating System of a remote node.

Hop Limit: Locating a Node

- Basic idea: if we are receiving packets from a node and assume that it is using the default “Hop Limit”, we can infer the orginal “Hop Limit”
- If we have multple “sensors”, we can “triangulate” the position of the node



Source	Hop Limit
A	61
B	61
C	61
D	62

F is the only node that is:

- **4 “routers” from A**
- **4 “routers” from B**
- **4 “routers” from C**
- **3 “routers” from D**

Threats to be Countered in IPV6

- Scanning Gateways and Hosts for weakness
- Scanning for Multicast Addresses
- Unauthorised Access Control
- Protocol Weaknesses
- Distributed Denial of Service (DDos)
- Transition Mechanisms
- Worms/Viruses
  - There are already worms that use IPv6
    - e.g. Rbot.DUD

Scanning Gateways and Hosts

- IPv6 Subnet Size is much larger
  - More than 500 000 years to scan a /64 subnet@1M addresses/sec.
  - Scanning for backdoors impractical.
  - Scanning for proxies impractical.
  - Scan-based worms can not propagate.

Scanning Gateways and Hosts

- IPv6 Scanning methods are changing
  - Public servers will still need to be DNS reachable giving attacker some hosts to attack.
  - Administrators may adopt easy to remember addresses (::1,::2,::53, or simply IPv4 last octet).
  - Use of trivial EUI-64 derived addresses.
    - EUI-64 derived from interface MAC addresses.
  - By compromising routers at key transit points in a network, an attacker can learn new addresses to scan.
- Avoid using easy to guess addresses.

Scanning Multicast Addresses

- New Multicast Addresses - IPv6 supports new multicast addresses enabling attacker to identify key resources on a network and attack them.
  - E.g. Site-local all DHCP servers (FF05::1:3), mDNSv6 (FF05::FB), and All Routers (FF05::2)
- Addresses must be filtered at the border in order to make them unreachable from the outside.
- To prevent smurf type of attacks: IPv6 specs forbids the generation of ICMPv6 packets in response to messages to global multicast addresses that contain requests.

Security of IPv6 Addresses

- Cryptographically Generated Addresses (CGA) IPv6 addresses [RFC3972].
  - Host ID - part of address is an encoded hash.
    - Binds IPv6 address to public key
  - Used for SEcuring Neighbor Discovery [RFC3971].
  - Is being extended for other uses [RFC4581].
- Privacy addresses as defined [RFC 4941].
  - Prevents device/user tracking
  - Makes accountability harder

Unauthorised Access Control

- Policy implementation in IPv6 with Layer 3 and Layer 4 is still done in firewalls.
- Some design considerations:
  - Filter site-scoped multicast addresses at site boundaries.
  - Filter IPv4 mapped IPv6 addresses on the wire.

Action	Src	Sst	Src port	Dst port
permit	a:b:c:d::e	X:y:z:w::v	any	ssh
deny	any	any		

Amplification (DDoS) Attacks

- There are no broadcast addresses in IPv6
  - This would stop any type of amplification attacks that send ICMP packets to the broadcast address
  - Global multicast addresses for special groups of devices, e.g. link-local addresses, etc.
- IPv6 specifications forbid the generation of ICMPv6 packets in response to messages to global multicast addresses
  - Many popular operating systems follow the specification.
  - Still uncertain on the danger of ICMP packets with global multicast source addresses.

Mitigation of IPv6 amplification

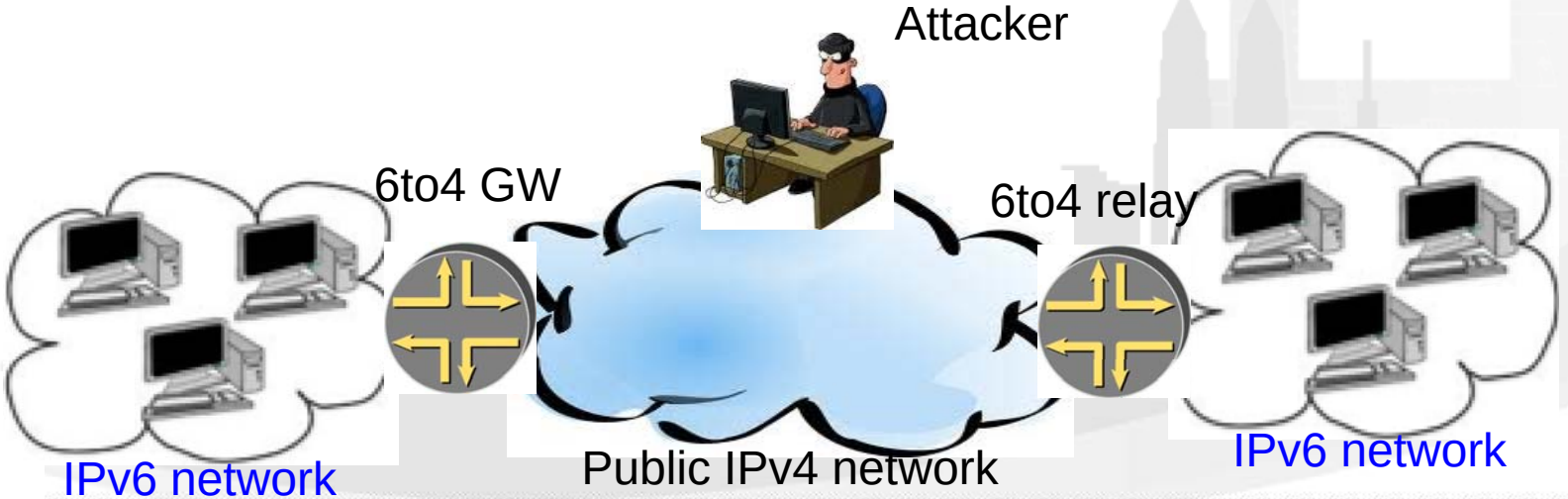
- Be sure that your host implementations follow the ICMPv6 specification [RFC 4443].
- Implement Ingress Filtering.
  - Defeating Denial of Service Attacks which employ IP Source Address Spoofing [RFC 2827].
- Implement ingress filtering of IPv6 packets with IPv6 multicast source address.

Mixed IPv4/IPv6 Environments

- Some security issues with transition mechanisms.
  - Tunnels often interconnect networks over areas supporting the “wrong” version of protocol.
  - Tunnel traffic often not anticipated by the security policies. It may pass through firewall systems due to their inability to check two protocols in the same time.
- Do not operate completely automated tunnels.
  - Avoid “translation” mechanisms between IPv4 and IPv6, use dual stack instead.
  - Only authorised systems should be allowed as tunnel end-points.

L3 – L4 Spoofing in IPv4 with 6to4

- Via 6to4 tunneling, spoofed traffic can be injected from IPv4 into IPv6.
  - IPv4 Src: IPv4 Address.
  - IPv4 Dst: 6to4 Relay
  - IPv6 Src: 2002:: Spoofed Source
  - IPv6 Dst: Valid Destination



IPv6 and IPsec

- General IP Security mechanisms that provides:
  - Authentication
  - Confidentiality
  - key management -requires a PKI infrastructure (IKEv2)
- Applicable to use over LANs, across public & private WANs, & for the Internet
- IPSec is not a single protocol. Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.
- IPSec is mandated in IPv6 – you can rely on for end-to-end security.

What is IPsec?

- Work done by the IETF IPsec Working Group
- Applies to both IPv4 and IPv6 and its implementation is:
  - Mandatory for IPv6
  - Optional for IPv4
- IPsec Architecture: RFC 2401
- IPsec services
  - Authentication
  - Integrity
  - Confidentiality
- IPsec modes: Transport Mode & Tunnel Mode
- IPsec protocols: AH (RFC 2402) & ESP (RFC 2406)

IPsec Protocols, modes and combinations

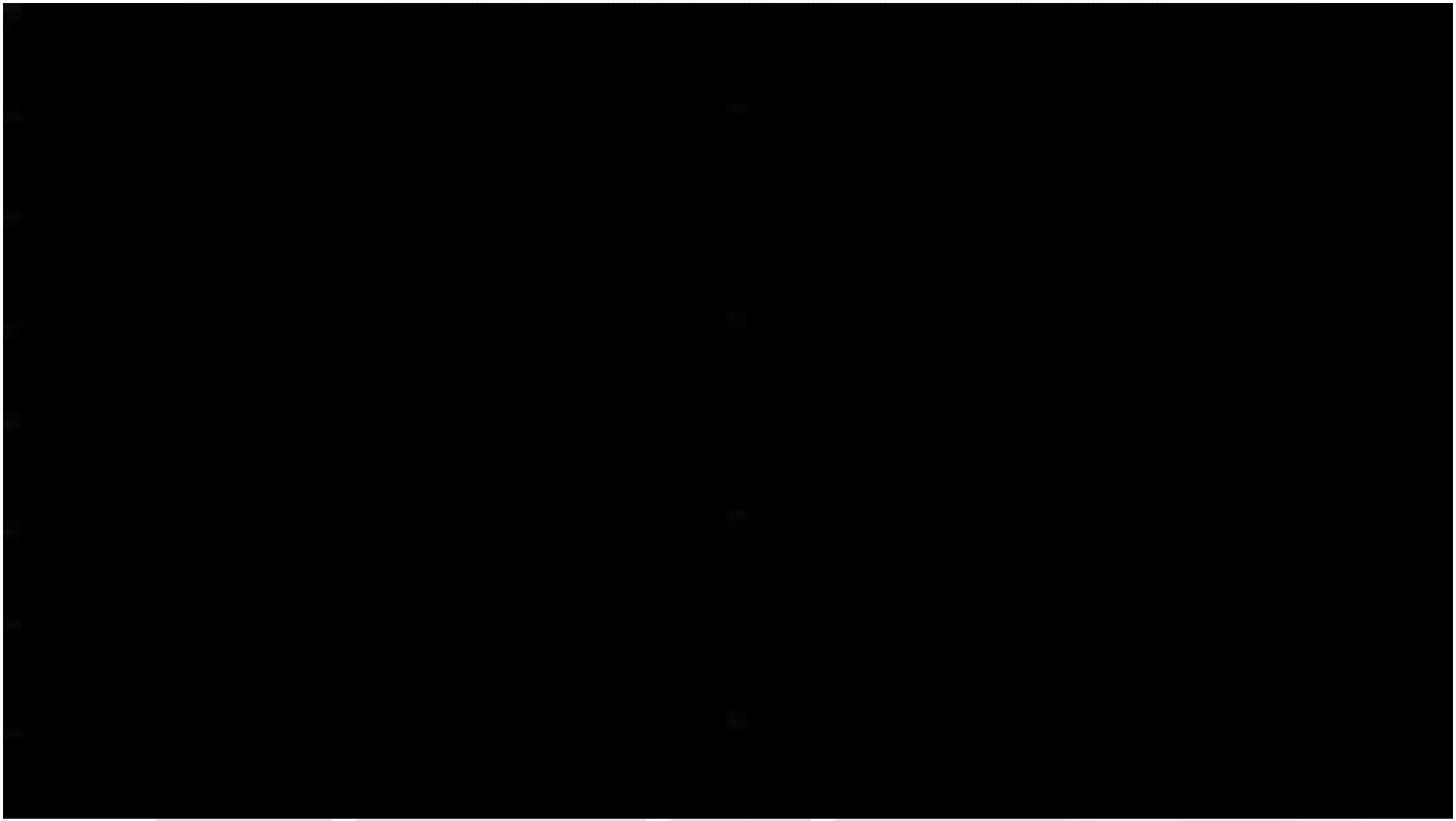
	Transport Mode	Tunnel Mode
AH	Authenticates IP payload and selected portions of IP header	Authenticates entire inner IP datagram (header & payload) and selected portions of the outer IP header
ESP	Encrypts IP payload	Encrypts inner IP datagram
ESP with Authentication	Encrypts IP payload and authenticates IP payload but not IP header	Encrypts and authenticates inner IP datagram

Some thoughts...

- While IPv6 provides similar features as IPv4, it uses different mechanisms. – and the evil lies in the small details.
- The security implications of IPv6 should be considered before it is deployed (not after!).
- Most systems have IPv6 support enabled by default, and this has implications on “IPv4-only” networks!
- Even if you are not planning to deploy IPv6 in the short term, most likely you will eventually do it.
- It is time to learn about and experiment with IPv6!

Summary

- IPv6 carries a number of advantages
  - Improved addressing
  - Improved security
  - Improved routing
- IPv6 advantages can be used against networks
  - Backdoors hidden
  - Communications channels hidden
  - Security mechanisms bypassed
- IPv6 is easier and cheaper to provide than prevent
- Time for ignoring IPv6 is past
- Time for understanding and using IPv6 is now



Acknowledgements

This presentation includes some material from these other sources:

- National Advanced IPv6 Centre (NAv6)
- 6Deploy


Thank you


Q
&
A

Who is IPv6 Global Sdn Bhd

IPv6 Global Sdn Bhd is an affiliate to Universiti Sains Malaysia's National Advanced IPv6 Center (NAV6). **NAV6 is a world leader in IPv6 R&D** and sit in IPv6 Council of several countries including China, India and Singapore. In 2005, the **Ministry of Information, Culture and Communication appointed NAV6 to spearhead the country's transition to be IPv6**. We aim to provide a complete one-stop centre for all IPv6 requirements and needs.

Contact information

Zulkifli Shahari
zul.shahari@ipv6global.my
0133305588

info@ipv6global.my or go to our website, www.ipv6global.my

IPv6 GLOBAL