

TECHNICAL CODE

INTERNET PROTOCOL VERSION 6 - SECURITY REQUIREMENTS

Developed by



Registered by



Registered date:

© Copyright 2023

MCMC MTSFB TC Gxxx:2023

Development of technical codes

The Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) ('the Act') provides for a Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirements for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)

MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
<http://www.mcmc.gov.my>

OR

Malaysian Technical Standards Forum Bhd (MTSFB)

MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8680 9950
Fax: +60 3 8680 9940
<http://www.mtsfb.org.my>

Contents

	Page
Committee representation.....	ii
Foreword	iii
0. Introduction.....	5
1. Scope	5
2. Normative references	6
3. Abbreviations	6
4. Terms and definitions	6
4.1 Address scanning	6
4.2 Anycast	6
4.3 Denial of Service (DoS) attack	6
4.4 Firewalls	7
4.5 Intrusion Detection and Prevention Systems (IDPS)	7
4.6 Multicast	7
4.7 Router Advertisement (RA)	7
4.8 Security audit	7
4.9 Security policy	7
4.10 Unicast	7
4.11 Unique Local Address (ULA)	7
4.12 Zero Configuration (Zeroconf)	7
5. Overview.....	7
5.1 Internet Protocol Version 6 (IPv6)	7
5.2 Neighbor Discovery Protocol	8
6. IPv6 security requirements.....	9
6.1 IPv6 security threats	9
7. IPv6 security control	18
8. IPv6 Security policies & checklist	20
8.1 IPv6 security policies	20
8.2 IPv6 security checklist	21
Annex A.....	24
Annex B.....	25
Bibliography	27

MCMC MTSFB TC Gxxx:2023

Committee representation

This technical code was developed by Numbering and Electronic Addressing Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

Digi Telecommunications Sdn Bhd

FNS (M) Sdn Bhd

Maxis Broadband Sdn Bhd

SIRIM Berhad

Telekom Malaysia Berhad

Universiti Kuala Lumpur

Universiti Sains Malaysia

DRAFT FOR PUBLIC COMMENT

Foreword

This technical code for the Internet Protocol version 6 - Security Requirements ('this Technical Code') was developed pursuant to Section 185 of the Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) by the Malaysian Technical Standards Forum Bhd (MTSFB) under the Numbering and Electronic Addressing Facilities Working Group.

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

DRAFT FOR PUBLIC COMMENT

(THIS PAGE IS INTENTIONALLY LEFT BLANKED)

INTERNET PROTOCOL VERSION 6 - SECURITY REQUIREMENTS

0. Introduction

The adoption of Internet Protocol version 6 (IPv6) has brought numerous benefits and features to the internet, but it has also introduced new security risks and challenges that organisations need to address. To ensure the confidentiality, integrity, and availability of their network resources, organisations might need to implement proper security controls, policies, and practices to prevent, detect, and respond to various types of IPv6 attacks.

In most cases where organisations deploy dual stack as a transition to IPv6, it is imperative for them to understand the security threats that are unique to IPv6 and take appropriate measures to ensure that their networks are secured and protected against threats from both Internet Protocol version 4 (IPv4) and IPv6. IPv6 was designed with security in mind and can be more secured than IPv4 with proper implementation & configuration. A set of guidelines and best practices can help organisations to enhance their IPv6 security posture and protect their networks from potential security threats.

1. Scope

This Technical Code provides guidance on IPv6 security mitigation control and best practices for securing IPv6 networks in Malaysian enterprises and service providers.

It provides clarity into Internet Protocol version 6 (IPv6) security threats and requirements for IPv6 security mitigations as guidance for critical security control adoptions. This is consistent with Malaysian Critical Security Controls (MYCSC) framework security control on network infrastructure management, to prevent attackers from exploiting network vulnerabilities. This Technical Code is intended for use by technical personnel, including network administrators and security professionals responsible for the design, implementation, and management of IPv6 networks in Malaysia.

Table 1. MYCSC framework

MYCIC controls	INS Control Theme			
	Infrastructure	Organisation	Environment	People
1. Inventory and control of enterprise assets	✓			
2. Inventory and control of software assets	✓			
3. Data protection	✓			
4. Secure configuration of enterprise assets and software	✓			
5. Account management	✓			
6. Access control management	✓			
7. Continuous vulnerability management	✓			
8. Audit log management	✓			
9. Email and web browser protections	✓	✓		
10. Malware defences	✓			
11. Data recovery	✓			
12. Network infrastructure management	✓			

MCMC MTSFB TC Gxxx:2023

13. Network monitoring and defence	✓			
14. Security awareness and skills training				✓
15. Service provider management				✓
16. Application software security	✓			
17. Incident response management		✓		✓
18. Penetration testing	✓		✓	✓
19. Threat intelligence	✓	✓		
20. Information security for use of cloud services	✓			
21. Physical security monitoring	✓		✓	
22. Information deletion			✓	
23. Data masking			✓	
24. Data leakage prevention			✓	
25. Web filtering			✓	
26. Secure coding				✓

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative reference (including any amendments) applies.

See Annex A.

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

See Annex B.

4. Terms and definitions

For the purposes of this Technical Code, the following definitions apply:

4.1 Address scanning

The process of attempting to discover IPv6 addresses within a network, often used for reconnaissance by attackers.

4.2 Anycast

A routing technique in which a single destination address is assigned to multiple interfaces, allowing traffic to be routed to the nearest interface.

4.3 Denial of Service (DoS) attack

An attack that is designed to disrupt the normal functioning of a system or network by overwhelming it with a flood of traffic or other resource-intensive activities.

4.4 Firewalls

A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

4.5 Intrusion Detection and Prevention Systems (IDPS)

A security system that monitors network traffic for signs of malicious activity and can take automated actions to block or mitigate threats.

4.6 Multicast

A routing technique in which a single packet is sent to multiple interfaces simultaneously, allowing traffic to be distributed to multiple destinations.

4.7 Router Advertisement (RA)

A message sent by a router to announce its presence and share information about the network topology.

4.8 Security audit

A systematic evaluation of a network's security posture to identify vulnerabilities and ensure compliance with security policies and regulations.

4.9 Security policy

A set of guidelines and procedures that define how a network is secured and how security incidents are managed.

4.10 Unicast

A routing technique in which a packet is sent to a single interface, allowing traffic to be routed to a specific destination.

4.11 Unique Local Address (ULA)

A type of IPv6 address that is designed for use within a local network and is not globally routable.

4.12 Zero Configuration (Zeroconf)

A set of protocols that enable IPv6 hosts to automatically configure themselves and communicate without the need for manual configuration.

These terms and definitions are not exhaustive but provide a starting point for understanding the key concepts and technologies discussed in this technical code.

5. Overview

This section is an overview about IPv6 and Neighbor Discovery Protocol (NDP).

5.1 Internet Protocol Version 6 (IPv6)

IPv6 was developed with more secured features compared to its predecessor IPv4. It provides a much larger address space, which enables more devices to be connected to the internet and making it more difficult for attackers to scan and probe the network. Additionally, the use of Stateless Address

Autoconfiguration (SLAAC) and other mechanisms can provide better address assignment and configuration, further enhancing security.

One of the most significant improvements in IPv6 security is the built-in support for Internet Protocol security (IPsec), which offer confidentiality, integrity, and authenticity to IPv6 packets. This allows for secure end-to-end communication between devices without the need for additional security protocols or software. However, despite the improved security features of IPv6, it is important to know the protocol, properly implement and configure it to ensure maximum security.

While IPv6 does provide improved security features, it is still vulnerable to certain types of attacks, such as Denial-of-Service (DoS) attacks and packet sniffing. It is important to implement additional security measures, such as firewalls and intrusion detection systems, to protect against these types of threats.

IPv6 depends heavily on NDP, which appears in the network in the form of Internet Control Message Protocol version 6 (ICMPv6). If ICMPv6 is disabled or dropped from the network, IPv6 does not operate properly, in contrast to IPv4. The importance of the NDP protocol in the IPv6 network is that it catches attackers' attention on NDP vulnerabilities that they can exploit.

5.2 Neighbor Discovery Protocol

NDP is a supporting protocol used with IPv6. It operates in the link layer of the Internet model and is responsible for the address auto configuration of nodes, discovery of other nodes on the link, determining the link-layer addresses of other nodes, duplicate address detection, detecting available routers and Domain Name System (DNS) servers, address prefix discovery, and maintaining reachability information about paths to other active neighbour nodes. NDP defines five ICMPv6 packet types for the purpose of Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor Advertisement (NA), and Network Redirects (NR).

Table 2 shows the ICMPv6 messages defined for NDP. By default, all IPv6 hosts joined with the multicast address group FF02::1 and other groups. The looking up of a MAC address of the target host in an IPv6 network can be performed by sending an ICMPv6 packet to the multicast address FF02::1. The sent packet will reach all active link-local addresses on the network. Exchanging ICMPv6 messages on top of the IPv6 protocol is crucial for IPv6 communication. However, this communication can be abused by sending fake, carefully crafted response messages for DoS, traffic re-routing, or other malicious purposes.

Table 2. ICMPv6 messages defined for NDP

ICMPv6 packet type	Description
RS (Type 133)	Nodes can use RS messages to locate routers on the same link. When a node receives an RS message and it is not the intended recipient, it will immediately generate a RA message instead of waiting until its next scheduled transmission time. This behaviour applies to nodes that forward packets that are not addressed to them.
RA (Type 134)	Routers advertise their presence together with various link and Internet parameters, either periodically or in response to an RS message.
NS (Type 135)	Nodes in a network use NS message to discover or verify the link-layer address of a neighbour. This can be done to ensure that the neighbour is still reachable using a cached link-layer address.
NA (Type 136)	NAs used by nodes to respond to the NS message.
Redirect (Type 137)	Routers have the ability to notify hosts for a better first hop router to a destination.

6. IPv6 security requirements

IPv6 concerns and security requirements covers on:

- a) security threats
- b) security control
- c) security policies and checklist

6.1 IPv6 security threats

IPv6 security threats can be broadly categorised into two main categories:

- a) Man-in-the-Middle (MiTM)
- b) Denial-of-Service (DoS)

6.1.1 Man-in-the-Middle (MiTM)

MiTM is an attack during the access gaining phase in which the attacker positions himself in the middle of the data communication between two parties. This attack is useful for conducting further attacks, such as sniffing and session hijacking. In IPv4, MiTM can be performed in various ways, such as Address Resolution Protocol (ARP) cache poisoning or Dynamic Host Configuration Protocol (DHCP) spoofing. ARP in IPv6 is replaced by the ICMPv6 NDP, while DHCP can be replaced by SLAAC. Common MiTM attacks are:

- a) Spoofed NA.
- b) Spoofed RA.
- c) Replay attack.
- d) IPv6 Tunnelling Attacks.
- e) Rouge Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Server Attack.

6.1.1.1 Spoofed NA

In a link local network, the communication between two nodes can be performed normally by exchanging two types of ICMPv6 messages, NS and NA. These two types of ICMPv6 messages are used to bind the MAC of the IPv6 address on the network but they are unsecured. No countermeasures are in place to prevent an attacker from generating an NA advertising his own layer-two address as belonging to other hosts on the link.

Figure 1 shows an example of a normal process of looking up the MAC of the IPv6 address on the network. Node A needs to communicate with Node B to perform data transmission. Thus, Node A sends ICMPv6 NS to a multicast address (FF02::1) specified by the target address. If the target node is present, it can be expected to be listening to the multicast address. Upon receiving the solicitation, it replies with an NA message to Node A with a solicited (S) flag enabled. Node A receives the advertisement and knows that IPv6 of Node B is on the Node B MAC address.

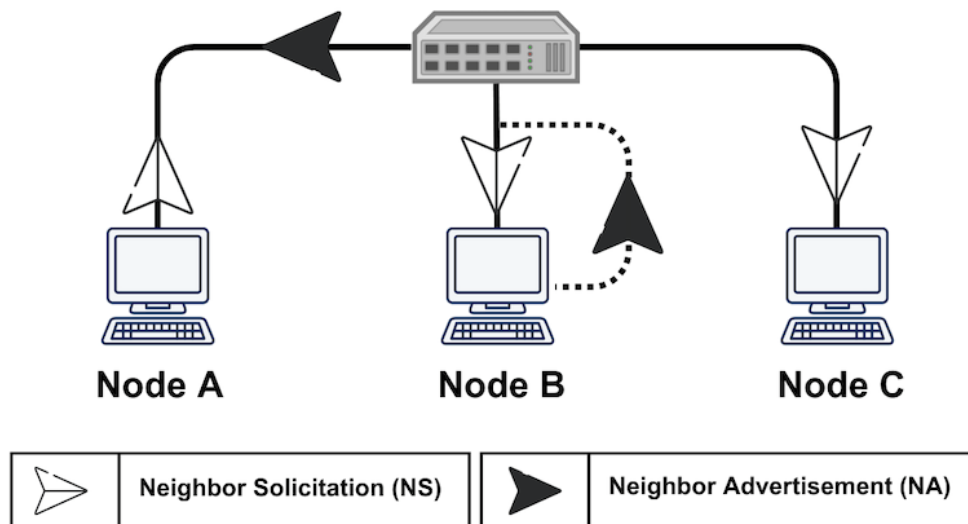


Figure 1. Normal process of looking up the MAC of the IPv6 address on the network.

This process also has vulnerabilities that can be used to perform MiTM Attacks. Figure 2 shows an example of an NA spoofing of the IPv6 network.

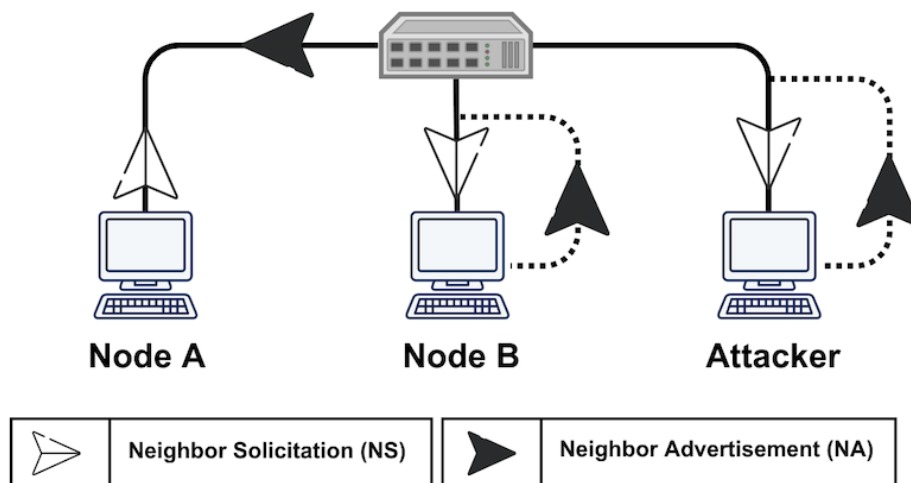


Figure 2. Example of NA spoofing

When an attacker joins the IPv6 network, it is automatically given an IPv6 address and listens to the FF02::1 multicast group. As shown in Figure 3, the attacker node and Node A are in the same LAN. When Node A sends an ICMPv6 NS to FF02::1 to inquire about Node B, Node B and the attacker node will receive an NS message from Node A.

Node B responds with NA to Node A with an S flag enabled. An attacker then responds with an ICMPv6 NA to Node A with the S and override (O) flags enabled. Node A receives the advertisement from Node B and the attacker. However, given that the attacker enables the O flags, it overwrites and creates a neighbour cache entry for Node A. Node A is deceived, thereby knowing that IPv6 of Node B is on the attacker's MAC address. Thus, all traffic between Nodes A and node B will go through the attacker node.

A practical example of NA spoofing is listed in Table 3. The table shows the MAC and IP addresses for Nodes A and B and the attacker.

Table 3. MAC and IP addresses for Nodes A and B and the attacker

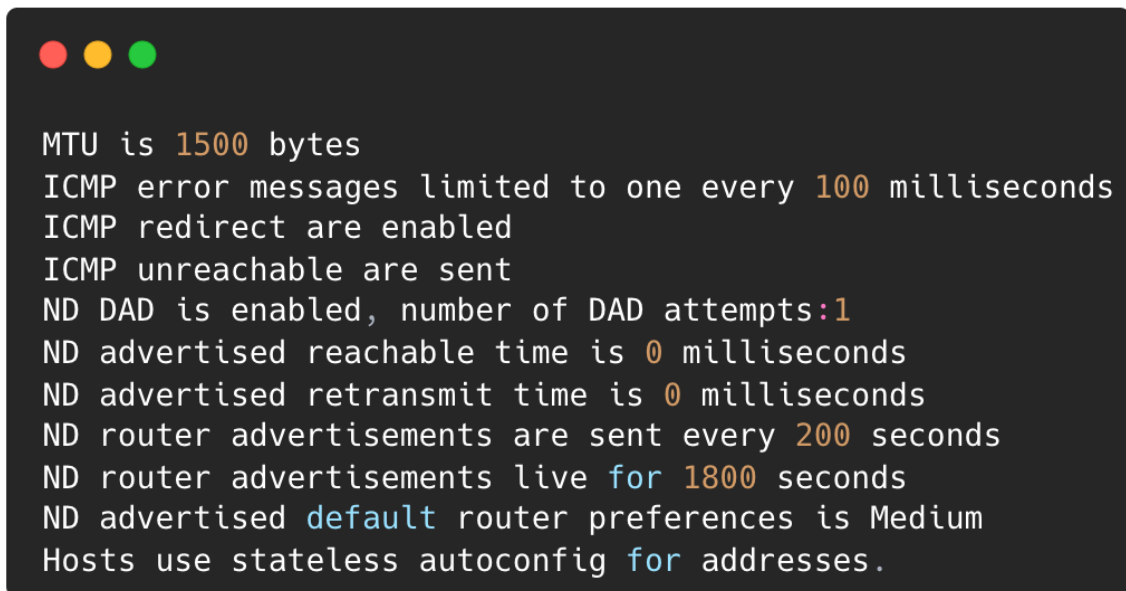
Node	IPv6 address	Mac Address
A	Fe80::3	aa:bb:cc:dd:ee:aa
B	Fe80::4	aa:bb:cc:dd:ee:11
Attacker	Fe80::5	aa:bb:cc:dd:ee:22

In the presence of a spoofed ICMPv6 NA in the network, the neighbour cache entry in node A after performing a ping6 command triggered from Nodes A to B is as follows: Fe80::5 link-layer address aa:bb:cc:dd:ee:22 Fe80::4 link-layer address aa:bb:cc:dd:ee:22. Notably, the Node B address is attached to the link-layer address of the attacker node. Therefore, all traffic from Nodes A to B goes through the attacker.

6.1.1.2 Spoofed RA

In an IPv6 local link network, a router announces its network prefix, lifetime, and configuration type periodically every 200 s by sending an RA to the FF02::1 multicast group. All nodes in the local link will receive the RA message and configure their routing table based on the RA and implant default gateway. Figure 3 shows the default periodic time for the RA message.

The IPv6 node can then promote the router to send an RA message by sending the RS to the FF02::2 multicast group. All routers in the network will receive the RS and respond by sending an RA to the FF02::1 multicast group, with all nodes receiving the RA and configuring their routing tables.



```

MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirect are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts:1
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preferences is Medium
Hosts use stateless autoconfig for addresses.

```

Figure 3. Default periodic time for an RA message

However, anyone can claim to be the router and send the periodic RA to the network. Thus, anyone can be the default gateway on the network.

Figure 4 shows the spoofed ICMPv6 RA process. In Figure 4, the attacker sends a rogue RA to all nodes in the link with the highest priority. Node A receives the rogue RA from the attacker node and configures the default gateway on the routing table to the attacker node. Therefore, all traffic from Node A goes through the attacker node.

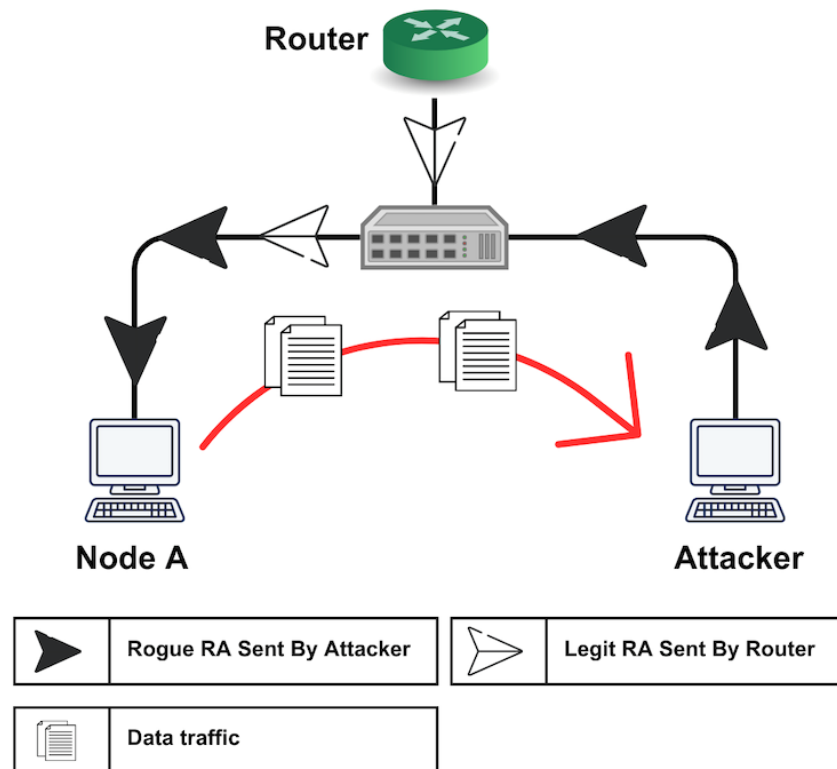


Figure 4. Spoofed ICMPv6 RA process

6.1.1.3 IPv6 replay attack

Replay attack is a replay of any previous neighbour or router discovery message to obtain network access. The attacker can capture the NDP message and send it again later. The attacker might also be modifying the content of the NDP message.

A replay attack occurs when a third party captures a command in transmission and replays it at a later time. By capturing the correct messages, an intruder might be able to gain access to a secure computer or execute commands that are normally encrypted and unreadable. It is often not necessary to decipher the command to use it. It is not difficult to capture the commands to be replayed. A user on a network can run a sniffer program and capture all packets that travel over the network. A user sends a computer command or transmission from one machine to another with the intention that the communication be secure. There are three different attributes that secure communications must have: secrecy, integrity, and authentication.

6.1.1.4 IPv6 tunnelling attack

IPv6 tunnelling attacks involve attackers exploiting weaknesses in IPv6 tunnelling mechanisms to bypass network security measures or access resources that should be protected. This can be used to steal sensitive information, launch further attacks, or disrupt network services.

Here is a list of how IPv6 Tunnelling Attacks are executed:

- a) The attacker gains access to a device on the network, either through a vulnerability or by stealing login credentials.
- b) The attacker sets up a tunnelling protocol to encapsulate IPv6 traffic within IPv4 packets, allowing the traffic to bypass security measures in place on the network.
- c) The attacker can use the tunnelling protocol to launch other types of cyberattacks, such as denial of service attacks or data theft.
- d) The attacker can also intercept and modify network traffic that is being tunnelled, allowing them to steal sensitive data or launch other types of cyberattacks.
- e) The attacker can use a technique called "tunnel hijacking" to take control of an existing tunnel and use it to redirect traffic to a malicious device.

A reported example of an IPv6 tunnelling attack is the Teredo attack, which involved attackers using Teredo tunnels to bypass network security measures and access resources on a protected network.

6.1.1.5 Rouge DHCPv6 server attack

Rogue DHCPv6 server attack is a type of network attack where an attacker sets up a fake DHCPv6 server on a network to provide false IPv6 addresses to devices on the network. A Rogue DHCPv6 server provides fake configuration information such as the IPv6 address of the default gateway, DNS server, and other network settings.

When a client device connects to a network and sends a DHCPv6 request for configuration information, the rogue DHCPv6 server intercepts the request and sends back fake configuration information. The client device then uses the fake configuration information to connect to the network, potentially exposing itself and the network to various security threats, such as MitM attacks, eavesdropping, and data theft.

To prevent Rogue DHCPv6 server attacks, network administrators can implement security measures such as DHCPv6 Shield, which monitors DHCPv6 messages to detect and block Rogue DHCPv6 servers. A similar mechanism has been widely deployed in IPv4 networks ('DHCP snooping').

6.1.2 Denial of Service (DoS)

These attacks occur when an attacker attempts to disrupt the normal functioning of a network or system by overwhelming it with traffic or by exploiting vulnerabilities. In IPv6, DoS attacks can exploit vulnerabilities in various protocols and mechanisms, such as NDP, ICMPv6, and routing protocols. These attacks can result in the degradation or interruption of network services, rendering them unavailable to legitimate users. The following are common DoS or DDoS attacks:

- a) Rogue router advertisements
- b) ICMPv6 redirect attack.
- c) Address resolution attack.
- d) DHCPv6 exhaustion attack.
- e) NS flooding.
- f) RA flooding.

- g) Multicast Listener Discovery (MLD) report message flooding.
- h) IPv6 fragmentation attack.
- i) Smurf attack.

6.1.2.1 Rogue Router Advertisements

RA DoS is a type of attack that targets the RA messages used by routers on an IPv6 network. The attack involves flooding the network with a large number of malicious RAs, causing network devices to run out of memory and crash.

A recent example of an RA attack is the RA DoS attack, which used a flood of malicious RAs to cause network devices to run out of memory and crash. This type of attack is like the Rogue Router Advertisement (RRA) attack, which involves an attacker sending fake RA messages to victim hosts, providing false information about the network configuration. As shown in Figure 4, the RRA attack can cause victim hosts to route their traffic to the attacker's rogue router, which can intercept or manipulate the traffic.

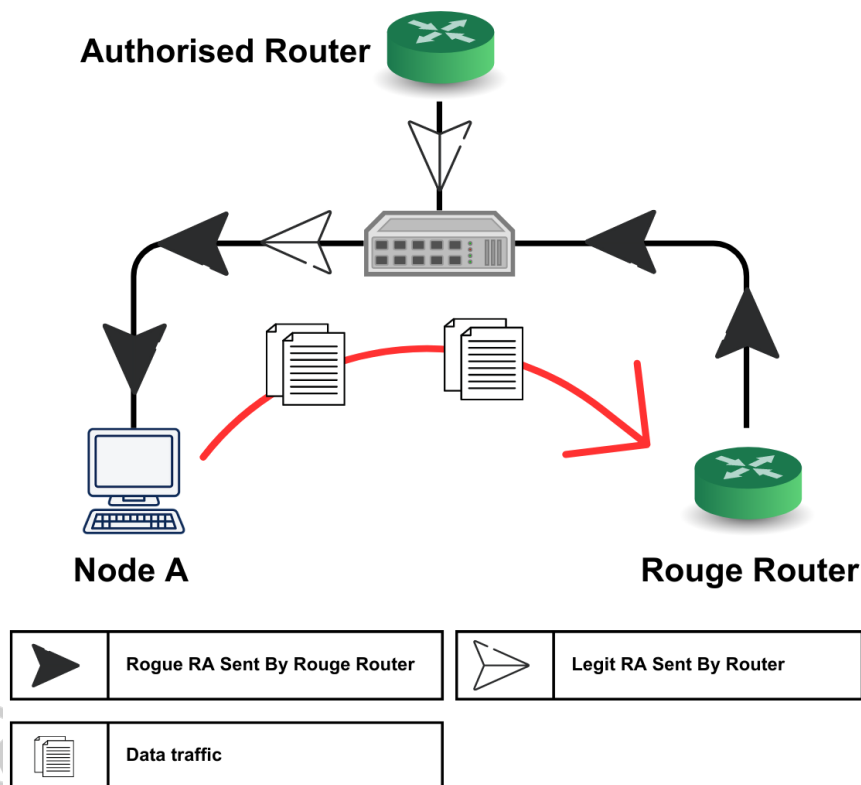


Figure 5. Rouge Router Advertisements

Here is a list of how the RA DoS attack is executed:

- a) The attacker sends a large number of RA messages to the network. These RAs are designed to flood the network with unnecessary traffic.
- b) The network devices receive the RAs and attempt to process them. However, the high volume of RAs causes the devices to run out of memory and crash.

- c) The network becomes unavailable as a result of the crash, causing disruption to network services and potentially exposing sensitive data to attackers.
- d) The attack can be repeated multiple times, causing additional disruption and damage to the network.

6.1.2.2 ICMPv6 redirect attacks

ICMPv6 redirect attacks involve attackers using malicious ICMPv6 redirect messages to redirect network traffic to a malicious device or network segment. This can be used to steal sensitive information, launch further attacks, or bypass security measures.

Here is a list of how ICMPv6 redirect attacks are executed:

- a) The attacker gains access to a device on the network, either through a vulnerability or by stealing login credentials.
- b) The attacker sends an ICMPv6 redirect message to other devices on the network, containing false routing information that redirects traffic to a malicious destination.
- c) The redirect message appears to come from a trusted router on the network, causing other devices to update their routing tables and redirect traffic to the attacker's device.
- d) The attacker can use a technique called MiTM to intercept and modify network traffic in real-time, allowing them to steal sensitive data or launch other types of cyberattacks.
- e) The attacker can also use a technique called ping of death to send oversized ICMPv6 packets that can cause network devices to crash or become unstable.

6.1.2.3 Address resolution attacks

Address resolution attacks are similar to ARP spoofing attacks in IPv4 networks. Attackers use this type of attack to redirect traffic to a malicious device by spoofing the MAC address of a device on the network. This can be used to steal sensitive information or launch other types of attacks.

One difference between ARP and address resolution attacks is that IPv6 networks use a different protocol for address resolution called NDP. NDP includes several features that help prevent address resolution attacks, such as Secure Neighbor Discovery (SEND) and Cryptographically Generated Addresses (CGA).

6.1.2.4 DHCPv6 Exhaustion Attacks

DHCPv6 exhaustion attacks involve attackers using a large number of DHCPv6 requests to exhaust the DHCPv6 server's pool of available addresses, leading to denial of service for legitimate users. This can be used to disrupt network services or launch other types of attacks.

A recent example of a DHCPv6 exhaustion attack is the DHCPv6 Starvation attack, which used a flood of malicious DHCPv6 requests to exhaust the available pool of IPv6 addresses on a network.

Here is a list of how DHCPv6 Starvation is executed:

- a) The attacker sends a large number of DHCPv6 requests to the DHCPv6 server, using fake MAC addresses and DHCP Unique Identifiers (DUIDs).
- b) The DHCPv6 server responds to each request with an available IP address, but because the requests are fake, the server reserves those addresses without actually assigning them to any device.

- c) The attacker continues to flood the DHCPv6 server with fake requests until all available IP addresses have been reserved, effectively preventing legitimate devices from obtaining IP addresses.
- d) Once the DHCPv6 server is overwhelmed, the attacker can launch other types of cyberattacks or steal sensitive information.

6.1.2.5 NS flooding

In a normal situation, any IPv6 node can send an NS message at any time to request a target node's link-layer address, while also providing its own link-layer address to the target node. NS messages are sent via multicast to the Solicited Node Multicast Address (SNMA) of the target node when the sending node is performing address resolution. An NS flooding attack aims to poison the neighbour cache at the victim machine, introducing a mapping from a victim IPv6 address to a multicast link-layer address. This has a negative impact on the performance of the network and of the attached nodes, and also allows an attacker to capture sniff network.

Traffic even in switched networks, as packets intended to travel from the target node to the victim IPv6 address are sent instead to a link-layer multicast address, thus allowing the attacker to receive a copy of such packets.

An NS flooding attack occurs, when a victim node is flooded with NS messages, thereby inducing the victim machine to create an entry (map IPv6 address - MAC address) in the neighbour cache of the victim machine. If the victim machine does not enforce any limits on the size of the neighbour cache, the kernel memory could be exhausted.

NS messages are sent to FF02::1 multicast group, with the result that all hosts in the same link receive these NS messages and update their neighbour caches accordingly.

6.1.2.6 RA Flooding

Routers in IPv6 can use the ND protocol to discover each other's presence and determine their link-layer addresses and prefix information. However, this also permits a malicious node to impersonate a network segment's default gateway. A receiving node does not validate router advertisements. Thus, any node that receives a fake RA updates its communication parameters blindly based on the RA. A malicious node can propagate bogus address prefix information to reroute legitimate traffic to prevent the victim from accessing the desired network.

Flooding the local network with completely different network prefixes, hosts, and routers updates the network information based on the announced prefix, consuming all available CPU resources, rendering the systems unusable and unresponsive. As IPv6 and auto configuration are enabled by default in most operating systems, all are affected in their default configuration. For Windows, a personal firewall or similar security product does not protect against this attack.

RA's message is sent to FF02::1 multicast group so that all hosts on the same link will receive the announced fake prefixes; thus, these hosts will configure their default gateway based on the fake announced prefixes. There is a flag in IPv6 router advertisements that determines default router preference. First, by default, the legitimate router sends out RAs with the router preference flag set to Medium. The fake RAs will set the preference flag to High, forcing hosts to use it as their default gateway.

The attacker sends hundreds or thousands of RAs to all hosts on the same link, with the result that the nodes' resources (CPU and memory) are consumed, because these nodes continue generating a new IPv6 address for each announced prefix.

6.1.2.7 Multicast Listener Discovery (MLD) report message flooding

MLD is an IPv6 protocol that a host uses to request multicast data for a particular group. Using the information obtained through MLD, the software maintains a list of multicast group or channel memberships on a per interface basis. The devices that receive MLD packets send the multicast data that they receive for requested groups or channels out the network segment of the known receivers. The following describes the essential operation of MLD:

- a) One router periodically broadcasts MLD Query messages onto the link.
- b) Hosts respond to the query messages by sending MLD report messages indicating their group memberships.
- c) All routers receive the report messages and note the membership of hosts on the link.
- d) If a router does not receive a report message for a specific group for a period of time, the router assumes there are no more members of the group on the link.

MLD report message flooding aims to target a specific multicast group to compromise all multicast group listeners. The MLD report message flooding targeted (FF02::02) a multicast group, with the result that all routers on the link are listening to FF02::2; thus, these routers are compromised by the flooded traffic.

6.1.2.8 IPv6 fragmentation attack

IPv6 fragmentation attacks take advantage of vulnerabilities in IPv6 fragmentation and reassembly mechanisms to send packets that can cause network devices to crash or malfunction. Attackers can exploit fragmentation vulnerabilities to bypass security measures, execute buffer overflow attacks, or redirect network traffic.

A recent example of an IPv6 fragmentation attack is the BlackNurse attack, which used ICMPv6 Type 3 (Destination Unreachable) messages to flood network devices with fragmented packets, leading to network congestion and denial of service.

To mitigate IPv6 fragmentation attacks, network administrators can implement filtering policies to block packets with specific fragmentation header fields, disable IPv6 fragmentation if possible, and use network-based or host-based firewalls to filter ICMPv6 packets. Additionally, using network monitoring and analysis tools can help detect and prevent fragmentation attacks before they cause significant damage.

6.1.2.9 Smurf attack

A Smurf attack aims to flood the target machine with a large amount of traffic with the intention of keeping the target machine busy respond- in to the incoming requests. In an IPv6 network, a Smurf attack occurs when an attacker sends spoofed ICMP echo request packets to a multicast group (FF02::1) with the target machine as the source. All nodes receive the packets and respond to the spoofed source IP. Sufficiently many machines on the network receiving and responding to these packets will flood the target computer with traffic. This scenario can slow down the target computer to the point where it becomes impossible to work on.

However, despite these security features, IPv6 networks are still vulnerable to address resolution attacks. Attackers can use techniques such as ICMPv6 redirection attacks, rogue RAs, and router discovery attacks to compromise network devices and redirect traffic.

MCMC MTSFB TC Gxxx:2023

One reported example of an IPv6 address resolution attack is the SLAAC attack which involved attackers spoofing the IPv6 address of a network gateway to redirect network traffic to a malicious device.

Below is a detailed explanation of how the SLAAC attack is executed:

- a) The attacker sets up a rogue router on the network. This can be done using a compromised device, a virtual machine, or a dedicated router device.
- b) The attacker then spoofs the IPv6 address of the legitimate gateway on the network. This allows the attacker to impersonate the gateway and intercept traffic intended for it.
- c) The attacker sends out bogus router advertisements (RA) to other hosts on the network. The RA contains a new prefix and gateway address that redirect traffic to the attacker's device.
- d) The hosts on the network receive the RA and update their IP address configuration accordingly. This results in traffic intended for the legitimate gateway being redirected to the attacker's device.
- e) The attacker can then intercept and modify network traffic as desired, including stealing sensitive information, launching man-in-the-middle attacks, and redirecting traffic to other malicious devices.
- f) The attack can continue until the rogue router is detected and removed from the network. This can be difficult, as the rogue router can be configured to hide its presence and avoid detection.

7. IPv6 security control

IPv6 brings many benefits and features, but it also introduces new security risks and challenges. To secure IPv6 networks, it is essential to implement proper security controls that can prevent, detect, and respond to different types of attacks. The IPv6 Security Control Matrix provides a list of mitigation measures that can help organisations protect their networks against IPv6 threats that is listed section 6.

Table outlines the security controls matrix that organisations should implement to mitigate each type of attack. By using the matrix as a reference, organisations can improve their IPv6 security posture and reduce the risk of network breaches and disruptions caused by these attacks.

This Technical Code provides an in-depth overview of essential security measures that organisations can implement to improve their overall security posture, including network security.

For a more comprehensive understanding of critical security controls, please refer to the Information and Network Security - Malaysia Critical Security Controls (MYCSC). For the summary of security controls and best practices for IPv6 network security, please refer to Annex B.

Table 4. Security Controls Matrix

MYCSC framework	Security threats	Security controls
Access control management	<ul style="list-style-type: none"> • Spoofed NA • Spoofed RA • Smurf attack • IPv6 tunnelling attack • Rouge DHCPv6 server attack • ICMPv6 redirect attacks • DHCPv6 exhaustion attacks • NS Flooding • RA Flooding • MLD report message flooding • IPv6 fragmentation attacks 	<ul style="list-style-type: none"> • Network Access Control (NAC) • Access Control Lists (ACLs) • Encryption • SEND protocol • CGA • DHCPv6 Server Hardening, Filtering Policies • Network-Based or Host-Based Firewalls • Network Monitoring and Analysis Tools
Continuous vulnerability management	All security threats	<ul style="list-style-type: none"> • Continuous vulnerability scanning • Timely patching and updates
Network infrastructure management	All security threats	<ul style="list-style-type: none"> • Network segmentation • Strict configuration management • Secure routing and switching
Network monitoring and defence	All security threats	<ul style="list-style-type: none"> • Intrusion Detection and Prevention Systems (IDS/IPS) • Security Information and Event Management (SIEM) solutions • Real-time network monitoring and analysis
Penetration testing	All security threats	Regular penetration testing to identify vulnerabilities and assess security posture
Threat intelligence	All security threats	<ul style="list-style-type: none"> • Continuous monitoring of emerging threats and vulnerabilities • Sharing of threat intelligence information
Security awareness and skills training	All security threats	Regular training and awareness programs for employees to increase their knowledge and understanding of security best practices and procedure

Table provides valuable insights into the security measures that are commonly adopted to mitigate and identify IPv6 related attacks. One of the most effective security measures is implementing network segmentation, which isolates critical assets and services to prevent unauthorized access and limit the impact of security incidents. By following these security measures, organisations can enhance their IPv6 network security and protect their assets against potential attacks.

Table provides an indication of the severity of attacks against the CIA Triad, which is a framework that entails confidentiality, integrity, and availability of data as three most important concepts within information security.

Table 5. Severity of Attacks Against the CIA Triad

Category	Attacks	Confidentiality	Integrity	Availability
Man-in-the-Middle (MiTM) attacks	Spoofed NA	Medium	Medium	Medium
	Spoofed RA	Medium	Medium	Medium
	IPv6 Replay Attack	High	High	Medium
	IPv6 Tunnelling Attacks	High	High	High
	Rogue DHCPv6 Server Attack	High	High	High
Denial of Service (DoS) attacks	Rogue Router Advertisements	Medium	Medium	High
	Address Resolution Attacks	Medium	High	High
	ICMPv6 Redirect Attacks	Medium	Medium	High
	DHCPv6 Exhaustion Attacks	Low	Low	High
	NS Flooding	Low	Low	High
	RA Flooding	Medium	Medium	High
	Multicast Listener Discovery Flooding	Low	Low	High
	IPv6 Fragmentation Attacks	Low	High	High
	Smurf Attack	Low	Low	High

In conclusion, securing IPv6 networks requires a comprehensive and proactive approach that involves implementing a variety of security controls. The IPv6 Security Control matrix provides a useful reference for organisations to select and prioritize the appropriate mitigation measures to protect their networks against common IPv6 attacks. However, it's worth noting that the security landscape is constantly evolving, and new threats may emerge in the future. Therefore, organisations should stay up-to-date with the latest security trends, technologies, and best practices and continuously assess and improve their IPv6 security posture to ensure the confidentiality, integrity, and availability of their network resources.

8. IPv6 Security policies & checklist

8.1 IPv6 security policies

Security policies are an important security control that can be used to ensure that organisations have a consistent approach to security. Security policies can cover a range of topics, including:

- a) **Secure configuration [SP1]:** IPv6-enabled devices shall be configured securely to minimize the risk of unauthorized access. This includes using strong passwords, disabling unused services, and disabling any unnecessary IPv6 features.
- b) **Network segmentation [SP2]:** Segmentation of the network shall be done to prevent unauthorized access to your management interfaces. You can do this by using firewalls, VLANs, or other network segmentation techniques.
- c) **Access control [SP3]:** Access to the management interfaces shall use authentication and authorization mechanisms. This can include using usernames and passwords, two-factor authentication, or certificate-based authentication.

- d) **Monitoring and logging [SP4]:** All management activities and network traffic related to IPv6 management shall be monitored and logged against unauthorized access or suspicious activity.
- e) **Regular updates and patches [SP5]:** IPv6-enabled devices and management tools shall be regularly updated with the latest patches and security updates to prevent vulnerabilities from being exploited.
- f) **Incident response [SP6]:** An incident response plan shall be developed and updated for IPv6 management security incidents. This plan shall include procedures for identifying and responding to security incidents, as well as communication procedures for notifying stakeholders and other relevant parties.

By implementing security policies, organisations can ensure that they have a consistent approach to security and that all stakeholders are aware of their roles and responsibilities.

8.2 IPv6 security checklist

With the increasing adoption of IPv6 globally and in Malaysia, it is crucial to ensure that their networks are secure and protected from potential security threats.

An IPv6 security checklist with a comprehensive set of security measures and best practices is crucial so that service providers and enterprises can follow to ensure the security and integrity of their IPv6 networks. The checklist includes a wide range of security controls, such as network segmentation, access controls, encryption, and monitoring, among others.

In developing the checklist, key security measures and best practices shall be outlined as a guidance for service providers and enterprises to secure their IPv6 networks, including firewall implementation, intrusion prevention, network segmentation, access controls, encryption, IPv6 address management, security monitoring and analysis, vulnerability assessments and penetration testing, and incident response planning. By following these guidelines, organisations can ensure that their IPv6 networks are secure and protected from potential security threats.

The following table serves as a guidance for service providers and enterprises to ensure the security and integrity of their IPv6 networks.

Table 8-1. IPv6 Security Checklist

Security Control	Description	Checklist Items	IPv6 Security Policy
Network Segmentation	Isolate critical assets and services to prevent unauthorized access and limit the impact of security incidents.	<ul style="list-style-type: none"> a) Network segmentation reviews shall be conducted regularly. The frequency of the activities shall be defined by the organisation's security policy. b) Policies and procedures shall be followed. 	SP1, SP2, SP3, SP4

MCMC MTSFB TC Gxxx:2023

Encryption	Use encryption mechanisms such as MacSec or IPSec to protect the confidentiality and integrity of data in transit.	<ul style="list-style-type: none"> a) Appropriate encryption mechanisms shall be used to secure data in transit. b) Encryption policies shall be followed and properly configured. 	SP1, SP3
IPv6 Address Management	Proper IPv6 address management can prevent address theft and rogue devices.	<ul style="list-style-type: none"> a) IPv6 address management policies and procedures shall be developed and implemented. b) Regular reviews shall be conducted to ensure compliance. The use of dynamic addressing shall be assigned instead of contiguous addresses. 	SP1, SP2, SP4
ICMPv6	ICMPv6 messages are used for network diagnostics and error reporting but can also be used for attacks such as flooding and redirection.	Filters and rate-limiting for ICMPv6 messages shall be implemented to prevent attacks.	SP1, SP3
Autoconfiguration	IPv6 has multiple autoconfiguration methods, such as stateless and stateful autoconfiguration, that can introduce security risks.	Controls and policies for autoconfiguration shall be implemented to prevent security risks.	SP1
Extension Headers	IPv6 introduces extension headers, which can be used for fragmentation, mobility, and security, but can also be used for attacks such as fragmentation attacks.	Controls and policies for extension headers shall be implemented to prevent attacks.	SP1
Multicast	IPv6 uses multicast for efficient communication, but multicast traffic can also be used for attacks such as flooding.	Controls and policies for multicast traffic shall be implemented to prevent attacks.	SP1, SP2, SP4
Transition Mechanisms	IPv6 transition mechanisms, such as dual-stack, tunnelling and translation can introduce security risks.	Controls and policies for transition mechanisms shall be implemented to prevent security risks.	SP1, SP4
Internet of Things (IoT)	The proliferation of IoT devices can introduce security risks, such as default or weak credentials and unpatched vulnerabilities.	Controls and policies for IoT devices shall be implemented to prevent security risks.	SP1, SP3, SP4, SP5

Firewalls, Intrusion Prevention and Detection Systems	These security measures protect the network perimeter and can detect and prevent unauthorized access and attacks.	a) Firewall shall be configured for IPv6 network. b) Intrusion prevention and detection systems that are appropriate for the network environment should be implemented to ensure that policies and procedures are followed and that the systems are properly configured.	SP1, SP2, SP3, SP4, SP5, SP6
Security Monitoring and Analysis	Regular monitoring and analysis can detect and respond to security incidents.	a) Security monitoring and analysis mechanisms that are appropriate for the network environment shall be implemented. b) Incident response procedures shall be developed to enable a rapid and effective response to security incidents.	SP4, SP6
Vulnerability Assessments and Penetration Testing	These activities can identify potential security risks and gaps in security controls.	a) Vulnerability assessments and penetration testing shall be conducted regularly. The frequency of the activities shall be defined by the organisation's security policy. b) Remedial plans shall be developed and implemented based on the results of the assessments and tests.	SP4, SP5, SP6

It is important to note that this table is not meant to be exhaustive, and that each organisation's IPv6 network implementation and security needs may be different. Additionally, implementing these considerations alone may not be sufficient to ensure network security. A comprehensive security strategy should be developed that includes multiple layers of security controls, regular security audits and vulnerability assessments, and a strong incident response plan.

Annex A
(informative)

Abbreviations

ACLs	Access Control Lists
ARP	Address Resolution Protocol
CGA	Cryptographically Generated Addresses
CIA	Confidentiality, Integrity, and Availability
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
DUIDs	DHCP Unique Identifiers
ICMPv6	Internet Control Message Protocol version 6
IDS/IPS	Intrusion Detection and Prevention Systems
IP	Internet Protocol
IPsec	Internet Protocol security
IPv6	Internet Protocol version 6
MAC	Media Access Control
MiTM	Man-in-the-Middle
MLD	Multicast Listener Discovery
MYCSC	Network Security - Malaysia Critical Security Controls
NA	Neighbor Advertisement
NAC	Network Access Control
NDP	Neighbor Discovery Protocol
NR	Network Redirects
NS	Neighbor Solicitation
RA DoS	Router Advertisement Denial-of-Service
RS	Router Solicitation
SEND	Secure Neighbor Discovery
SIEM	Security Information and Event Management
SLAAC	Stateless Address Autoconfiguration

Annex B
(informative)

Summary of security controls and best practices for IPv6 network security

Security control	Description	Examples
NAC	Controls access to the network by verifying the identity of devices and users	802.1X, MAC authentication
Access Control Lists (ACLs)	Filters network traffic based on predefined rules to permit or deny access	IP-based ACLs, port-based ACLs
Encryption	Protects data by encoding it so it can only be read by authorised parties with the correct decryption key	SSL/TLS, IPsec
Secure Neighbor Discovery (SEND) protocol	Protects against attacks on NDP messages	Cryptographically generated addresses, SEND protocol
Cryptographically Generated Addresses (CGA)	Uses public key cryptography to create a unique IPv6 address	CGA-based addressing
DHCPv6 Server Hardening, Filtering Policies	Protects against rogue DHCP servers and prevents denial of service attacks	DHCPv6 server hardening, filtering policies
Network-Based or Host-Based Firewalls	Controls traffic flow by blocking or allowing traffic based on predefined rules	Network-based firewalls, host-based firewalls
Network Monitoring and Analysis Tools	Monitors network traffic for potential threats and provides real-time analysis	Network performance monitoring, packet sniffers
Continuous vulnerability scanning	Identifies vulnerabilities in the network and devices on an ongoing basis	Vulnerability scanning tools
Timely patching and updates	Ensures devices and software are up to date with the latest security patches and updates	Automated patch management tools
Network segmentation	Separates network traffic to improve security and performance	VLANs, network zoning
Strict configuration management	Enforces consistent configuration settings across devices to reduce security risks	Configuration management tools
Secure routing and switching	Implements secure routing and switching protocols to prevent unauthorized access	OSPFv3, BGP4+
Intrusion Detection and Prevention Systems (IDS/IPS)	Detects and prevents malicious activity on the network	Network-based IDS/IPS, host-based IDS/IPS
Security Information and Event Management (SIEM) solutions	Centralizes and analyses security event data from across the network to identify potential threats	Log management, correlation engines
Real-time network monitoring and analysis	Provides real-time visibility into network activity to identify and respond to potential threats	Network traffic analysis tools
Regular penetration testing to identify vulnerabilities and assess security posture	Tests network and system security by simulating real-world attacks	Penetration testing services
Continuous monitoring of emerging threats and vulnerabilities	Monitors emerging security threats and vulnerabilities to identify potential risks	Threat intelligence services

MCMC MTSFB TC Gxxx:2023

Sharing of threat intelligence information	Shares threat intelligence data with other organizations to improve security posture	Information sharing and analysis centres
Regular training and awareness programs for employees to increase their knowledge and understanding of security best practices and procedures	Educates employees on security policies and procedures to reduce human error	Security awareness training programs

DRAFT FOR PUBLIC COMMENT

Bibliography

- [1] RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*
- [2] RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*
- [3] RFC 1122, *Requirements for Internet Hosts -- Communication Layers*

DRAFT FOR PUBLIC COMMENT

Acknowledgements

Members of the Numbering and Electronic Addressing Working Group

Ms Azura Mat Salim (Chair)	Telekom Malaysia Berhad
Ms Nurul Amirah Zarifah Norazaruddin/	Malaysian Standards Forum Bhd
Mr Muhaimin Mat Salleh	
Dr Mun Wai Yuen/	Maxis Broadband Sdn bhd
Mr Lee Wei Han	
Dr Mohammed F.R Anbar	Universiti Sains Malaysia
Mr Muhammad Faiz Rahmat	SIRIM Berhad
Mr Hanaffy Geoffrey Ramli	Digi Telecommunications Sdn Bhd
Mr Thaib Mustafa	FNS (M) Sdn Bhd
Prof Dr Shahrulniza Musa	Universiti Kuala Lumpur

By invitation:

Mr Yan Kim Fui (Vice Chair)	Cisco Systems
Mr Adil Hidayat (Draft lead)	My6 Initiative Sdn Bhd
Nurah Muhammad	MYNIC Berhad