MCMC MTSFB TC G046:2024

TECHNICAL CODE

INTERNET PROTOCOL VERSION 6 – SECURITY REQUIREMENTS

Developed by

Registered by

Registered date: 4 April 2024

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
Email : stpd@mcmc.gov.my
Website: www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Level 3A, MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8680 9950
Fax : +60 3 8680 9940
Email : support@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

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:

American Malaysian Chamber of Commerce

CelcomDigi Berhad

FNS (M) Sdn Bhd

Maxis Broadband Sdn Bhd

My6 Initiative Berhad

SIRIM Berhad

TM Technology Services Sdn Bhd

Universiti Kuala Lumpur

Universiti Sains Malaysia

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.

INTERNET PROTOCOL VERSION 6 - SECURITY REQUIREMENTS

1. Scope

This Technical Code provides guidance on Internet Protocol version 6 (IPv6) security mitigation control and best practices for securing IPv6 networks in Malaysian organisations.

It offers clarity into IPv6 security threats and guidance for the adoption of IPv6 critical security controls to mitigate them. This is consistent with MCMC MTSFB TC G042 to prevent attackers from exploiting network vulnerabilities. This Technical Code refers to 7 out of the 26 Malaysia Critical Security Controls (MYCSC), which are:

a) Access control management.

b) Continuous vulnerability management.

c) Network infrastructure management.

d) Network monitoring and defence.

e) Penetration testing.

f) Threat intelligence.

g) Security awareness and skills training.

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.

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.

MCMC MTSFB TC G042, *Information and Network Security - Malaysian Critical Security Controls*

RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

RFC 4291, *Internet Protocol Version 6 Addressing Architecture*

RFC 9099, *Operational Security Considerations for IPv6 Networks*

3. Abbreviations

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

See Annex A.

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 Address space

In the context of IPv6, the address space refers to the number of unique addresses available for assigning to devices on the network. IPv6 provides a significantly larger address space compared to Internet Protocol version 4 (IPv4), allowing for a greater number of connected devices.

4.3 Anycast

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

4.4 Address Resolution Protocol (ARP) cache poisoning

In IPv4 networks, Address Resolution Protocol (ARP) cache poisoning is a Man-in-The-Middle (MiTM) attack where the attacker sends false ARP messages to associate their Media Access Control (MAC) address with the Internet Protocol (IP) address of another network device. This can lead to the attacker intercepting or modifying network traffic intended for the targeted device.

4.5 Attackers

Individuals or entities who seek to compromise the security of a network or its resources by exploiting vulnerabilities, launching attacks, or unauthorised access.

4.6 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.

4.7 Domain Name System (DNS) spoofing

Domain Name System (DNS) spoofing is a MiTM attack where the attacker intercepts DNS requests and provides false DNS responses. By redirecting the victim's DNS queries to malicious DNS servers, the attacker can redirect the victim to fake websites, capture sensitive information, or manipulate network communication.

4.8 Dynamic Host Configuration Protocol (DHCP) spoofing

Another MiTM attack in IPv4 involves Dynamic Host Configuration Protocol (DHCP) spoofing. The attacker sets up a rogue DHCP server on the network and responds to DHCP requests from clients, providing them with incorrect network configuration information. This allows the attacker to intercept and manipulate the client's network traffic.

4.9 Firewalls

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

4.10 Internet Control Message Protocol version 6 (ICMPv6)

A protocol used in IPv6 for various network-related functions, including error reporting, diagnostics, and Neighbor Discovery. Internet Control Message Protocol version 6 (ICMPv6) plays a critical role in the proper operation of IPv6 networks.

4.11 Internet Protocol security (IPsec)

A suite of protocols that provide security services, such as confidentiality, integrity, and authenticity, for IPv6 packets. Internet Protocol security (IPsec) offers secure end-to-end communication without requiring additional security protocols or software.

4.12 Internet Protocol version 6 (IPv6)

The Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol that provides a larger address space, improved security features, and better support for modern networks compared to IPv4.

4.13 Intrusion Detection Systems (IDS)

Security systems that monitor network traffic or system events for potential security breaches or unauthorized activities. IDS can identify and alert administrators about suspicious or malicious behaviour on the network.

4.14 Media Access Control Security (MACsec)

A security protocol that provides encryption and authentication for data transported at the MAC layer of a network. It ensures secure, encrypted communication between devices connected to the same physical network.

4.15 Medium Access Control (MAC) address

A unique identifier assigned to network interfaces for communication at the link layer of the network model. In the context of IPv6, the MAC address is used for link-layer address resolution and identifying neighbouring nodes.

4.16 Multicast

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

4.17 Multicast address

An IPv6 address that identifies a group of hosts that are interested in receiving the same traffic. The multicast address FF02::1 is the all-nodes multicast address, used for sending ICMPv6 messages to all active link-local addresses on the network.

4.18 Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is an integral part of the IPv6 protocol suite used for network address and prefix discovery, router discovery, and address autoconfiguration. It replaces functions of IPv4 protocols such as ARP, ICMP Router Discovery, and ICMP Redirect.

4.19 Packet sniffing

The act of capturing and analysing network traffic to intercept and view the contents of packets, potentially leading to the exposure of sensitive information. Additional security measures, such as encryption, are necessary to protect against packet sniffing.

4.20 Security audit

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

4.21 Security policy

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

4.22 Session hijacking

Session hijacking is a MiTM attack where the attacker intercepts and takes control of an ongoing session between two parties. By gaining access to session tokens or cookies, the attacker can impersonate one of the parties and potentially access sensitive information or perform unauthorised actions.

4.23 Secure Sockets Layer (SSL)/Transport Layer Security (TLS) stripping

Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), provide encryption and secure communication between clients and servers. In a MiTM attack known as SSL/TLS stripping, the attacker intercepts communication, downgrades the connection to unencrypted Hypertext Transfer Protocol (HTTP), and captures sensitive information exchanged between the client and server.

4.24 Stateless Address Autoconfiguration (SLAAC)

A mechanism in IPv6 that allows hosts to automatically configure their network addresses without the need for a central server. Stateless Address Autoconfiguration (SLAAC) provides better address assignment and configuration, reducing the reliance on manual configuration and potential configuration errors.

4.25 Unicast

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

5. Overview

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

The adoption of IPv6 has brought numerous benefits and features to the Internet, but it has also introduced 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 IPv4 and IPv6. IPv6 was designed with security in mind and can be more secure than IPv4 with proper implementation and 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.

5.1 Internet Protocol Version 6 (IPv6)

IPv6 was developed with more secure 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 SLAAC and other mechanisms can provide better address assignment and configuration, further enhancing security.

One of the key upgrades in IPv6 security is the automatic inclusion of IPsec. IPsec enhances IPv6 packets with confidentiality, integrity, and authenticity, enabling secure communication directly between devices without extra security protocols or software. However, to fully benefit from IPv6's enhanced security, it's crucial to understand the protocol and correctly set it up for maximum protection.

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 ICMPv6. If ICMPv6 is disabled or dropped from the network, IPv6 does not operate properly, in contrast to IPv4. Due to the crucial role of NDP in an IPv6 network, attackers are inclined to exploit NDPs vulnerabilities.

5.2 Neighbor Discovery Protocol (NDP)

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 DNS servers, address prefix discovery, and maintaining reachability information about paths to other active neighbour nodes. NDP utilises 5 ICMPv6 packet types:

a) Router Solicitation (RS) - ICMPv6 Type 133.

b) Router Advertisement (RA) - ICMPv6 Type 134.

c) Neighbor Solicitation (NS) - ICMPv6 Type 135.

a) Neighbor Advertisement (NA) - ICMPv6 Type 136.

b) Redirect - ICMPv6 Type 137.

Table 1 describes the 5 NDP messages. 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 1. ICMPv6 messages defined for NDP

ICMPv6 packet type	Description
RS	RS is primarily used by hosts (devices such as a computer or a server) on a network to request immediate router advertisements. Instead of waiting for the next scheduled router advertisement, a host can send an RS message to ask for one immediately. This ability to prompt an immediate response is particularly useful when a device initially joins a network, allowing it to quickly establish its configuration with a local router's information.
RA	Routers advertise their presence together with various link and Internet parameters, either periodically or in response to an RS message.
NS	Its main purpose is to determine the link-layer address (like a MAC address) of a neighbor on the same network or to verify that a neighbor is still reachable via a previously determined link-layer address. When a device needs to communicate with another but doesn't know its physical address, it sends a NS message.
NA	NA functions as a response to a NS message. When a device receives an NS message inquiring about its physical, or link-layer, address, it responds with an NA message containing this information. Thus, the NA protocol plays a significant role in maintaining effective communication within the network, allowing nodes to confirm their existence and share their address information.
Redirect	The Redirect message is primarily used by routers to inform hosts of a more efficient route for reaching a particular destination. When a router receives a packet that it realises could be sent more directly through a different router or directly to the destination, it sends a Redirect message to the host. This process optimises network traffic flow and contributes to overall network efficiency.

6. IPv6 security threats

6.1 Classification of IPv6 security threats

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

a) MiTM.

b) 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 can be used 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 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 Neighbor Advertisement (NA)

In a local network connection, devices (or nodes) can communicate effectively by exchanging two kinds of ICMPv6 messages, NS and NA. These messages pair the devices' MAC addresses with their IPv6 addresses on the network. However, this process lacks security measures. There's nothing stopping a malicious party from sending a false NA message, claiming their own MAC address belongs to other devices on the network. This could potentially allow them to intercept communication intended for other devices.

Figure 1 illustrates a typical process of determining the MAC address associated with an IPv6 address on a network. For example, Node A wants to transmit data to Node B. To do this, Node A sends a NS message using the ICMPv6 protocol to the all-nodes multicast group (FF02::1). This group address includes Node A, Node B, and Node C. They are all listening to communications sent to this address. If Node B (the target) is active, it is expected to be receiving messages sent to this group address. Once Node B gets the solicitation from Node A, it responds with a NA message, indicating its presence with a special flag (S-flag) turned on. When Node A gets this advertisement, it understands that Node B's IPv6 address is associated with Node B's MAC address.

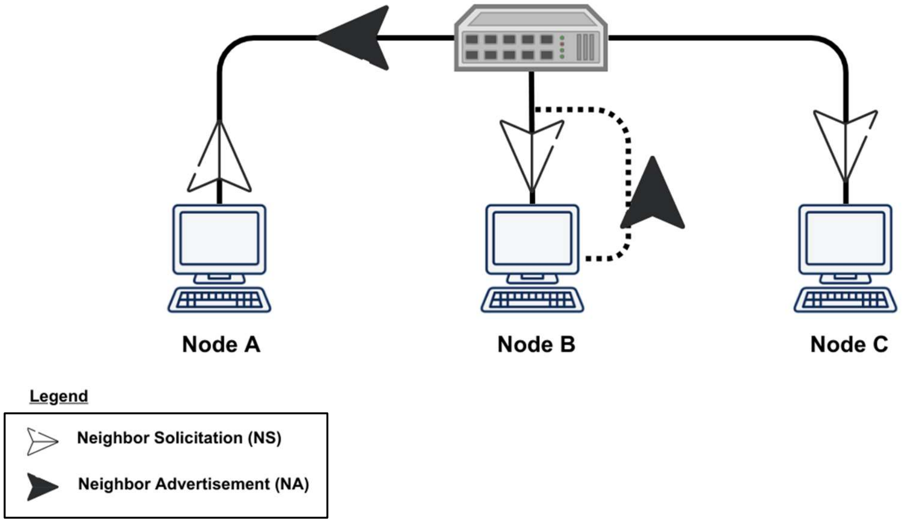


Figure 1. Normal process of looking up the MAC of the IPv6 address on the network.

However, the normal process has vulnerabilities that can be exploited to perform MiTM attacks. Figure 2 shows an example of an NA spoofing of the IPv6 network.

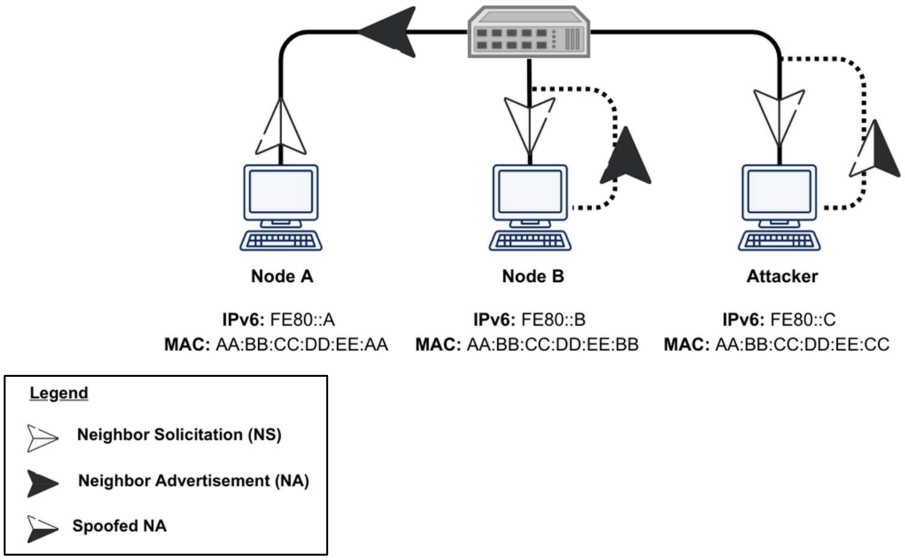


Figure 2. Example of NA spoofing

As shown in Figure 2, the attacker node and Node A are in the same Local Area Network (LAN) and they are automatically given IPv6 addresses and listens to the FF02::1 multicast group. When Node A sends an NS to FF02::1 to inquire about Node B's MAC address, 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 NA message to Node A with the S-flag and override (O-flag) enabled. Node A receives the advertisement from Node B and the attacker. However, given that the attacker enables the O-flag, 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.

In Table 2, you'll find an example of NA spoofing that directly relates to Figure 2. The table presents the MAC and IP addresses for Nodes A and B, along with the details of the attacker.

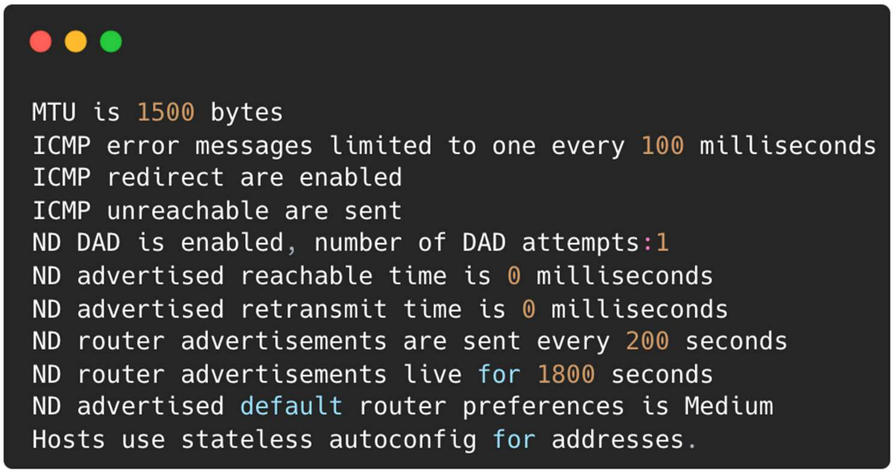
Table 2. MAC and IP addresses for Nodes A and B and the attacker

Node	IPv6 address	MAC address
A	FE80::A	AA:BB:CC:DD:EE:AA
B	FE80::B	AA:BB:CC:DD:EE:BB
Attacker	FE80::C	AA:BB:CC:DD:EE:CC

When the spoofed NA message is sent into the network, the neighbor cache entry in Node A changes after initiating a 'ping6' command from Node A to Node B. Now, the IPv6 link-local addresses FE80::B and FE80::C, which should be associated with different nodes (having different MAC address), are both linked to the same MAC address AA:BB:CC:DD:EE:CC. Notably, FE80::B, which should be linked to Node B's MAC address, is now associated with the MAC address of the attacker's node. As a result, all data traffic that is supposed to go from Node A to Node B will instead be routed through the attacker's node, creating a significant security breach.

6.1.1.2 Spoofed Router Advertisement (RA)

In a local IPv6 network, routers can be configured to send Router Advertisement (RA) messages to the all-nodes multicast group (FF02::1) at regular intervals. The specific time interval for sending RA messages is determined by the network administrator and can vary, commonly set to every 200 s. All nodes in the network 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.



```
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 RA messages

If the node does not receive any RA message from a router, it can then attempt to locate the router by sending the RS message. Upon receiving the RS message, routers in the network respond by sending RA messages to the FF02::1 multicast group. All nodes on the network receive these RA messages, allowing them to configure their routing tables based on the received information.

However, any device can impersonate the router, sending periodic RAs and potentially becoming the default gateway on the network.

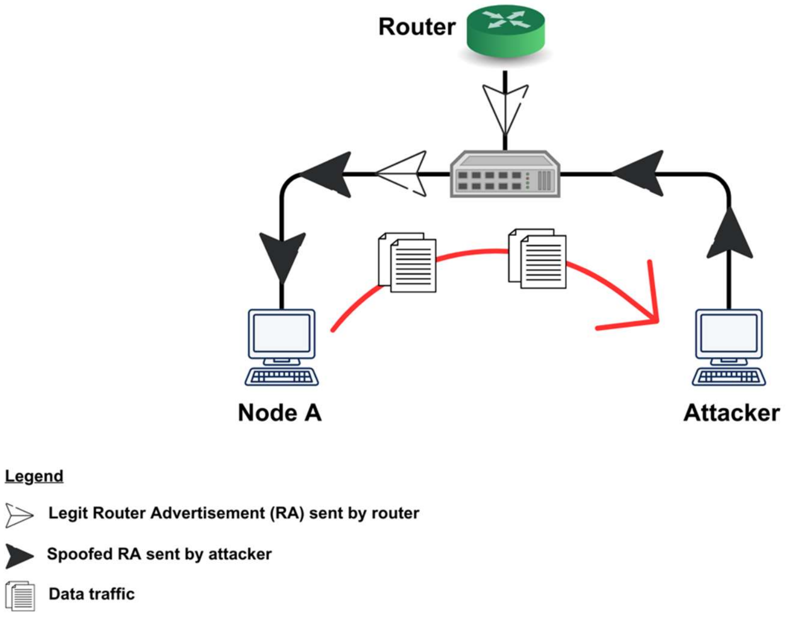

Router
Node A
Attacker
Legend
Legit Router Advertisement (RA) sent by router
Spoofed RA sent by attacker
Data traffic

Figure 4, the attacker sends a spoofed RA to all nodes in the link with the highest priority. Node A receives the spoofed RA from the attacker node and configures its default gateway to the attacker's node. Therefore, all IPv6 traffic from Node A goes through the attacker node.

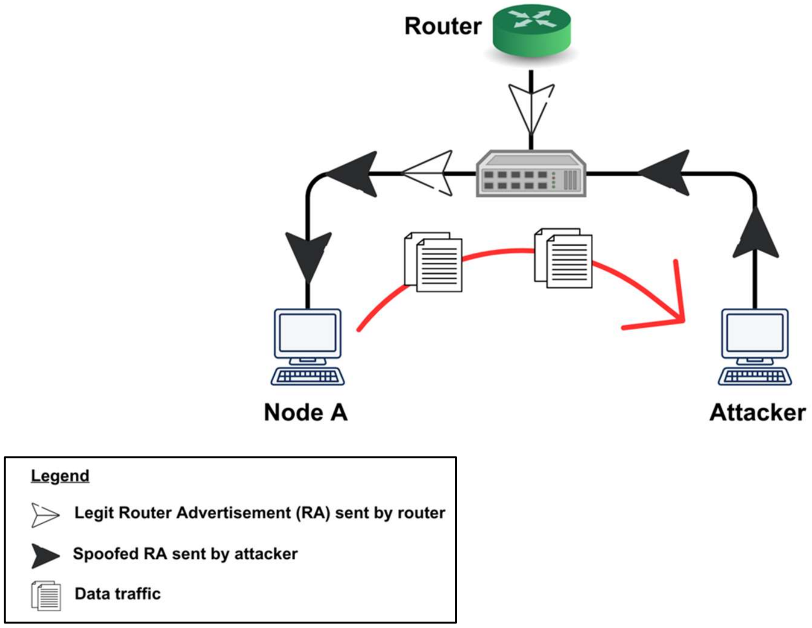

Router
Node A
Attacker
Legend
Legit Router Advertisement (RA) sent by router
Spoofed RA sent by attacker
Data traffic

Figure 4. Spoofed ICMPv6 RA process

6.1.1.3 IPv6 replay attack

An IPv6 replay attack is a type of network attack where an attacker intercepts and maliciously retransmits previously captured IPv6 network packets. The goal is to exploit the stateless nature of the IPv6 protocol and deceive the receiving system into accepting and acting upon duplicated or outdated packets. This can lead to security breaches, unauthorised access, data integrity violations, and DoS situations.

In an IPv6 replay attack as shown in Figure 5, the attacker captures valid IPv6 packets transmitted over the network. These packets can include various protocols, such as ICMPv6 or even higher-level protocols like HTTP or DNS. The attacker then replays these captured packets back into the network, often multiple times, without modification. The receiving system, unaware that it is processing duplicated or outdated packets, may act upon them, leading to potentially harmful consequences.

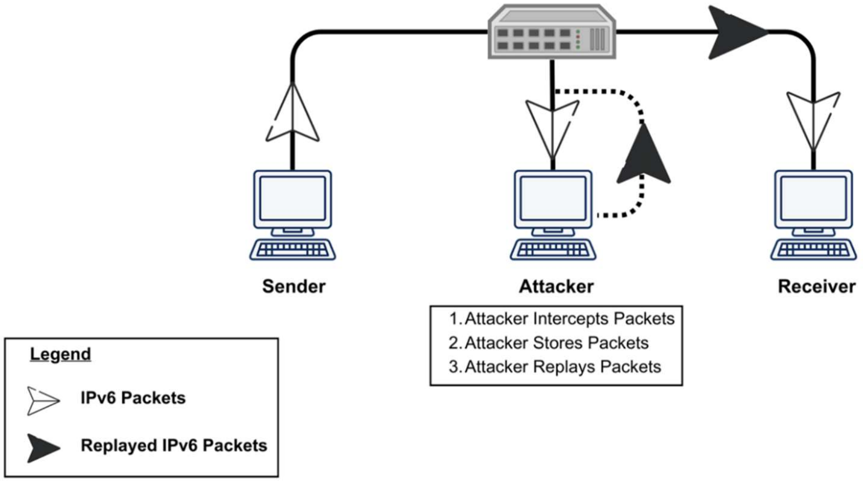

Sender
Attacker
Receiver
1. Attacker Intercepts Packets
2. Attacker Stores Packets
3. Attacker Replays Packets
Legend
IPv6 Packets
Replayed IPv6 Packets

Figure 5. IPv6 replay attack

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.

The attacker gains network access by exploiting a vulnerability or stealing login credentials. They create a tunnelling protocol that wraps IPv6 traffic in IPv4 packets, evading network security measures. This allows them to carry out various cyberattacks like DoS or data theft. Additionally, they can intercept and modify the tunnelled traffic, enabling them to steal sensitive data or launch additional cyberattacks. Through 'tunnel hijacking', the attacker seizes control of an established tunnel and redirects traffic to a malicious device.

6.1.1.5 Rogue 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.

As depicted in Figure 6, 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).

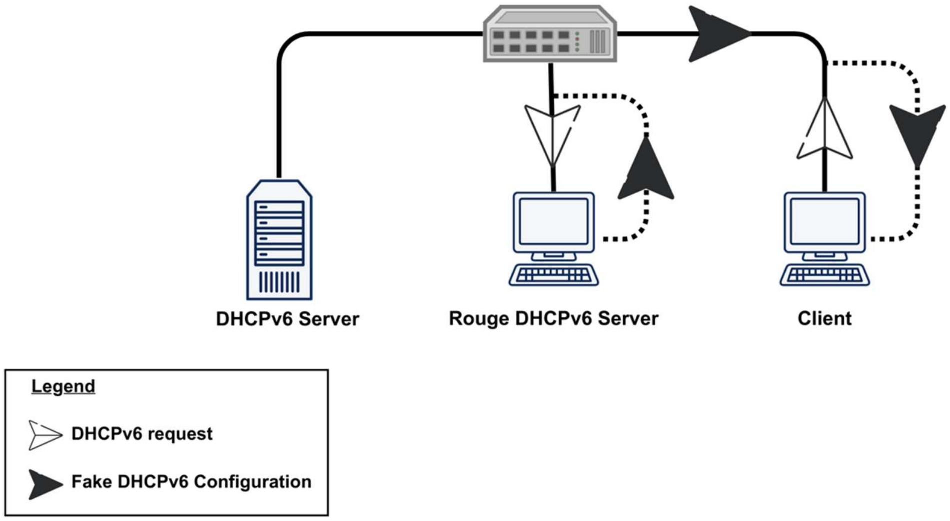


Figure 6. Rouge DHCPv6 server attack

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 attacks:

a) Rogue RA.

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 (RRA)

This type of attack involves the attacker sending fake RA messages to unsuspecting hosts. These false messages provide incorrect network configuration information. In the Rogue Router Advertisements (RRA) attack scenario depicted in Figure 4, victim hosts are tricked into sending their traffic to the attacker's rogue router. Consequently, the attacker gains the ability to intercept or manipulate the traffic.

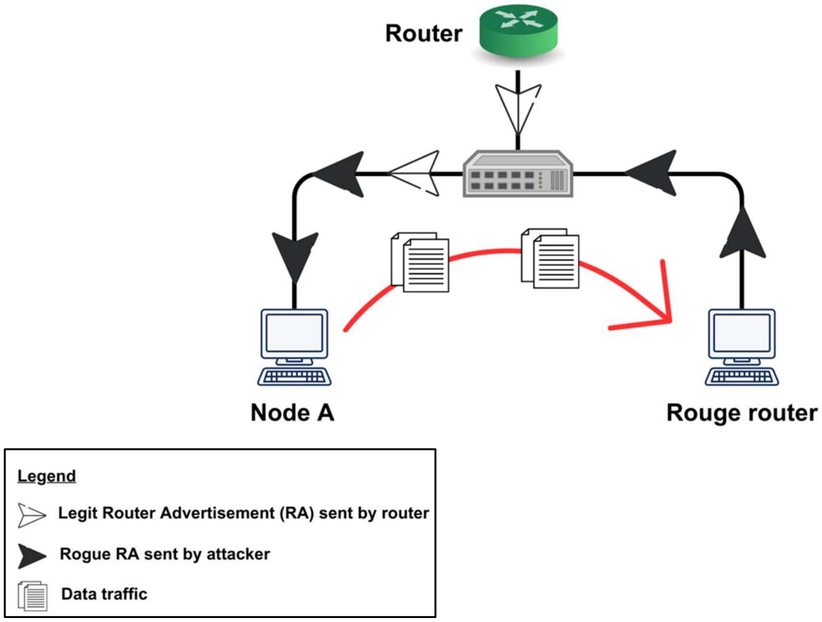

Router
Node A
Rouge router
Legend
Legit Router Advertisement (RA) sent by router
Rogue RA sent by attacker
Data traffic

Figure 7. Rouge Router Advertisements (RRA)

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.

The attacker gains access to a device on the network, either through a vulnerability or by stealing login credentials. They then send ICMPv6 redirect messages to other devices on the network, containing false routing information. These messages appear to come from a trusted router, causing other devices to update their routing tables and redirect traffic to the attacker's device.

With control over the redirected traffic, the attacker can intercept and modify network traffic in real-time, allowing them to steal sensitive data or launch other types of cyberattacks. In addition, they can utilise techniques like the ping of death, which involves sending oversized ICMPv6 packets that can crash or destabilise network devices.

6.1.2.3 Address resolution attacks

Address resolution attacks in IPv6 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. However, a distinction exists between ARP spoofing and address resolution attacks where IPv6 networks rely on NDP whereas IPv4 uses ARP for address resolution.

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. These requests use fake MAC addresses and DHCP Unique Identifiers (DUIDs), causing the server to reserve available IP addresses without assigning them to any device. As a result, legitimate users are denied service because all the available IP addresses are reserved by the attacker. This attack can disrupt network services and provide an opportunity for the attacker to carry out further cyberattacks or steal sensitive information.

6.1.2.5 Neighbor Solicitation (NS) flooding

Under normal circumstances, any IPv6 node has the ability to send an NS message to request the link-layer address of a target node while providing its own link-layer address. These NS messages are sent to the Solicited Node Multicast Address (SNMA) of the target node as part of the address resolution process. However, in an NS flooding attack, the objective is to manipulate the neighbor cache of the victim machine by introducing a mapping between the victim's IPv6 address and a multicast link-layer address. If the victim machine does not enforce any limits on the size of the neighbour cache, the kernel memory could be exhausted. This malicious activity adversely affects the network's performance, impacts the connected nodes, and grants the attacker the ability to capture and sniff network data.

6.1.2.6 Router Advertisement (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 will update its communication parameters blindly based on the information provided by that 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 diverse network prefixes, hosts, and router updates overwhelms the network information processing, depleting CPU resources and rendering systems unresponsive and unusable. Since IPv6 and auto configuration are typically enabled by default on most operating systems, all systems are affected in their default configuration. It's important to note that in the case of Windows, a personal firewall or similar security product does not provide protection against this type of attack.

RA messages are sent to the all-node multicast group (FF02::1) 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 the fake router as their default gateway.

6.1.2.7 Multicast Listener Discovery (MLD) report message flooding

MLD is an IPv6 protocol used by hosts to request multicast data for specific groups. It maintains a list of multicast group memberships per interface. Routers periodically broadcast MLD Query messages, and hosts respond with MLD report messages indicating their group memberships. Routers receive these reports, and if no report is received for a group, they assume there are no more members. However, MLD report message flooding targets a multicast group, compromising all multicast listeners and potentially compromising routers on the network.

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.

An 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 disruption 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

An IPv6 Smurf attack is a type of network attack that involves overwhelming a target by flooding it with a large volume of ICMPv6 echo requests. In this attack, the attacker spoofs the source IP address to match the target's IP address and sends these requests to a multicast group. As a result, all nodes within the multicast group respond to the requests, flooding the target with a massive amount of traffic.

The target, being bombarded with an overwhelming number of responses, becomes overloaded and may become unable to respond to legitimate requests or operate properly. This DoS effect is similar to the original Smurf attack in IPv4 networks, but it is specifically tailored to exploit the characteristics of IPv6 networks. IPv6 Smurf attacks can disrupt network services, cause network congestion, and impact the availability and performance of the targeted system.

7. IPv6 security control

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 as shown in Table 3 provides a list of mitigation measures that can help organisations protect their networks against IPv6 threats.

By referring to the matrix, organisations can enhance their IPv6 security posture and minimise the risk of network breaches and disruptions caused by these attacks.

This Technical Code offers a detailed overview of essential IPv6 security measures that organisations can adopt to enhance their overall security posture, including network security.

For a more comprehensive understanding of critical security controls, please refer to MCMC MTSFB TC G042.

Table 3. Security controls matrix

MYCSC framework	Security threats	Security controls
Access control management	a) Spoofed NA b) Spoofed RA c) Smurf attack d) IPv6 tunnelling attack e) Rouge DHCPv6 server attack f) ICMPv6 redirect attacks g) DHCPv6 exhaustion attacks h) NS flooding i) RA flooding j) MLD report message flooding k) IPv6 fragmentation attacks	a) Network Access Control (NAC) b) Access Control Lists (ACLs) c) Encryption d) Secure Neighbor Discovery (SEND) protocol e) CGA (call check) f) DHCPv6 server hardening, filtering policies g) Network-based or host-based firewalls h) Network monitoring and analysis tools
Continuous vulnerability management	All security threats	a) Continuous vulnerability scanning b) Timely patching and updates
Network infrastructure management	All security threats	a) Network segmentation b) Strict configuration management c) Secure routing and switching
Network monitoring and defence	All security threats	a) Intrusion Detection and Prevention Systems (IDS/IPS) b) Security Information and Event Management (SIEM) solutions c) 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	a) Solicited Node Multicast Address Continuous monitoring of emerging threats and vulnerabilities b) 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

For explanation and examples on security controls for IPv6 network security, please refer to Annex B.

Table 4 provides an indication of the severity of attacks against the Confidentiality Integrity Availability (CIA) triad, which is a framework that entails confidentiality, integrity, and availability of data as three most important concepts within information security.

Table 4. Severity of attacks mapped to CIA triad

Category	Attacks	Confidentiality	Integrity	Availability
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
DoS attacks	RRA	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

8. IPv6 security policies and 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 minimise the risk of unauthorised 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 unauthorised 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 authorisation 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 unauthorised 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 will have a consistent approach to security and that all stakeholders are aware of their roles and responsibilities.

8.2 IPv6 security checklist

IPv6 security checklist is crucial so that organisations can ensure the security and integrity of their IPv6 networks as shown in Table 5. The checklist includes a wide range of security controls, such as network segmentation, access controls, encryption, and monitoring, among others.

Table 5. IPv6 security checklist

Security control	Description	Checklist items	IPv6 security policy (as defined in 8.1)
Network segmentation	Isolate critical assets and services to prevent unauthorised access and limit the impact of security incidents.	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]
Encryption	Use encryption mechanisms such as MACSec or IPSec to protect the confidentiality and integrity of data in transit.	a) Appropriate encryption mechanisms shall be used to secure data in transit. b) Encryption policies shall be followed and properly configured.	[SP1], [SP3]

Table 5. IPv6 security checklist *(continued)*

Security control	Description	Checklist items	IPv6 security policy (as defined in 8.1)
IPv6 address management	Proper IPv6 address management can prevent address theft and rogue devices.	a) IPv6 address management policies and procedures shall be developed and implemented. b) Regular reviews shall be conducted to ensure compliance. Dynamic IP addressing shall be used instead of contiguous address.	[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]

Table 5. IPv6 security checklist *(concluded)*

Security control	Description	Checklist items	IPv6 security policy (as defined in 8.1)
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 unauthorised 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 that includes multiple layers of security controls, regular security audits and vulnerability assessments, as well as a strong incident response plan should be developed.

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
HTTP	Hypertext Transfer Protocol
ICMPv6	Internet Control Message Protocol version 6
IDS/IPS	Intrusion Detection and Prevention Systems
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol security
IPv6	Internet Protocol version 6
LAN	Local Area Network
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	Router Advertisement
RA DoS	Router Advertisement Denial-of-Service
RRA	Rogue Router Advertisements
RS	Router Solicitation

SEND	Secure Neighbor Discovery
SIEM	Security Information and Event Management
SNMA	Solicited Node Multicast Address
SLAAC	Stateless Address Autoconfiguration

Annex B
(informative)

Explanation and examples of security controls for IPv6 network security

Table B.1. Examples of security controls 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
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 unauthorised 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
SIEM solutions	Centralises 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

Table B.1. Examples of security controls for IPv6 network security *(continued)*

Security control	Description	Examples
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
Sharing of threat intelligence information	Shares threat intelligence data with other organisations 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

Acknowledgements

Members of the Numbering and Electronic Addressing Working Group

Ms Azura Mat Salim (Chair)	TM Technology Services Sdn Bhd
Ts Adil Hidayat Rosli (Draft lead)	My6 Initiative Berhad
Ms Nurul Amirah Zarifah Norazaruddin/ Mr Muhaimin Mat Salleh (Secretariat)	Malaysian Technical Standards Forum Bhd
Ts Salim Mohammad Ghani	American Malaysian Chamber of Commerce
Ts Hanaffy Geoffrey Ramli	CelcomDigi Berhad
Mr Thaib Mustafa	FNS (M) Sdn Bhd
Dr Leon Mun Wai Yuen/ Mr Lee Wei Han	Maxis Broadband Sdn Bhd
Mr Muhammad Faiz Rahmat	SIRIM Berhad
Prof Dr Shahrulniza Musa	Universiti Kuala Lumpur
Dr Mohammed FR Anbar	Universiti Sains Malaysia

By invitation:

Mr Yan Kim Fui (Vice Chair)	Cisco Systems