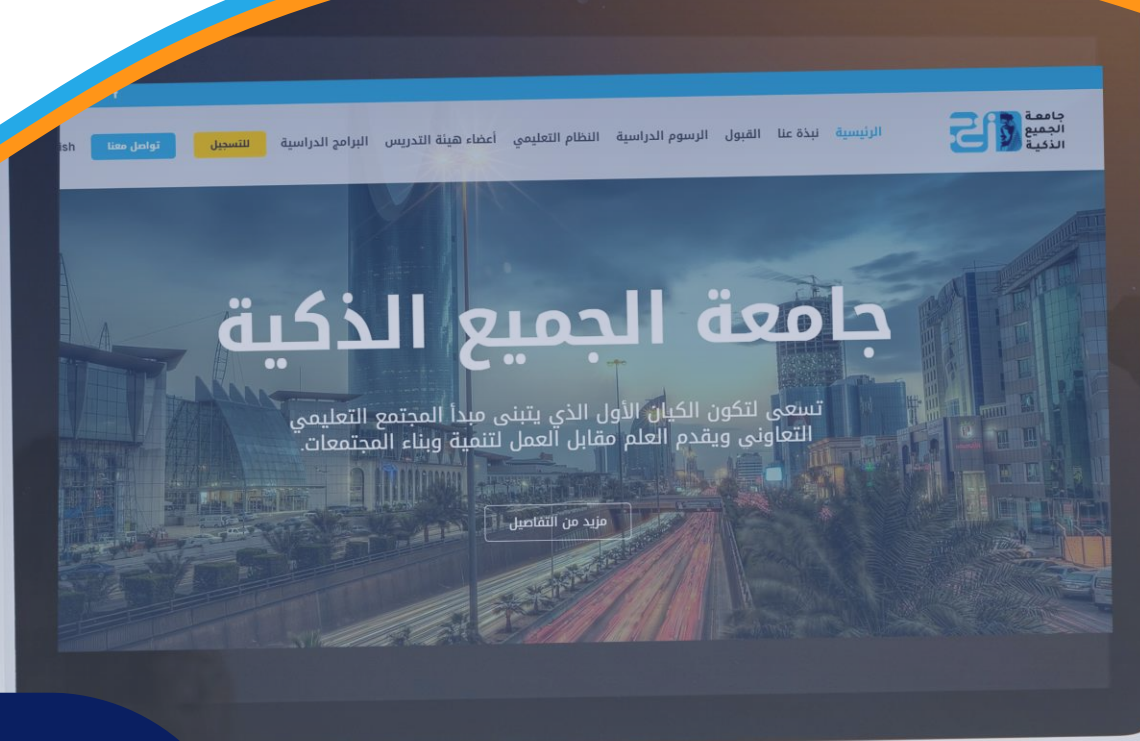




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



Network Security
Prepared by Dr. Mohammed Anbar
Lecture 3

IPv6 Security

Chapter 02

Learning Objectives:

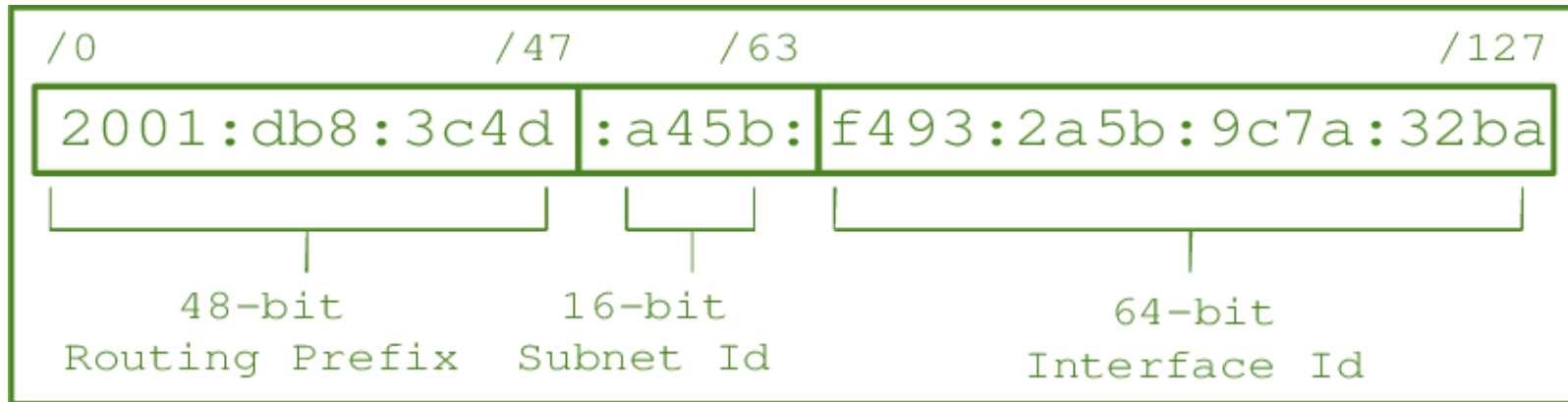
- Explain basic concepts of Internet Protocol version 6 (IPv6),
- Differentiate between IPv6 and IPv4,
- Explain basic concepts of IPv6 Security,
- Explain the Neighbor Discovery Protocol (NDP) ,
- Understand the NDP-based Attacks.

- The dramatic increase in the number of devices connected to the Internet has resulted in the allocation of many Internet Protocol versions 4 (IPv4) addresses, but the number of available address spaces is rapidly diminishing.
- The Internet Engineering Task Force (IETF) has been working on IPv6 specifications to overcome these address limitations.
- IPv6 provides much larger address spaces of 340 undecillion addresses to meet this demand.
- IPv6 is an enhanced version of IPv4 created to coexist with IPv4 and address unforeseen IPv4 design faults while also offering better internetworking capabilities.

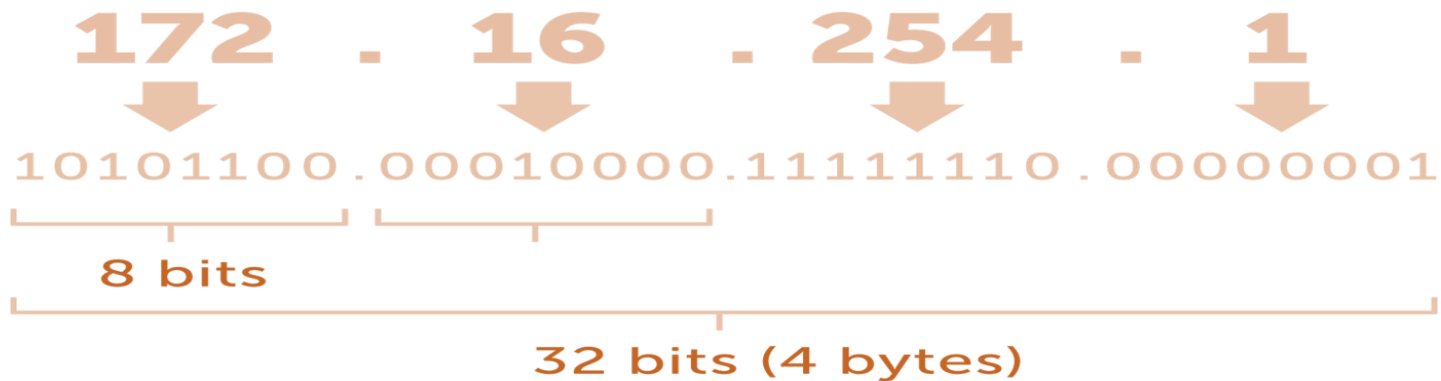
- In many parts of the world, IPv6 technology is currently being used, providing express end-to-end device addressability. In the end, IPv6 might become a requirement for institutions, although security issues are still of utmost importance.
- IPv6 and IPv4 are both network layer protocols, with many similar network layer vulnerabilities.
- IPv6 contains a new protocol, Neighbor Discovery Protocol (NDP), that replaces Address Resolution Protocol (ARP) in Internet Protocol version 4 (IPv4), router discovery, and redirect. If implemented without any security mechanism, NDP contains vulnerabilities.
- IPv6 is slightly better than IPv4 in terms of security, but IPv6 is not necessarily more secure than IPv4

Chapter 02

IPv6 and IPv4 packet format



IPv4 address in dotted-decimal notation



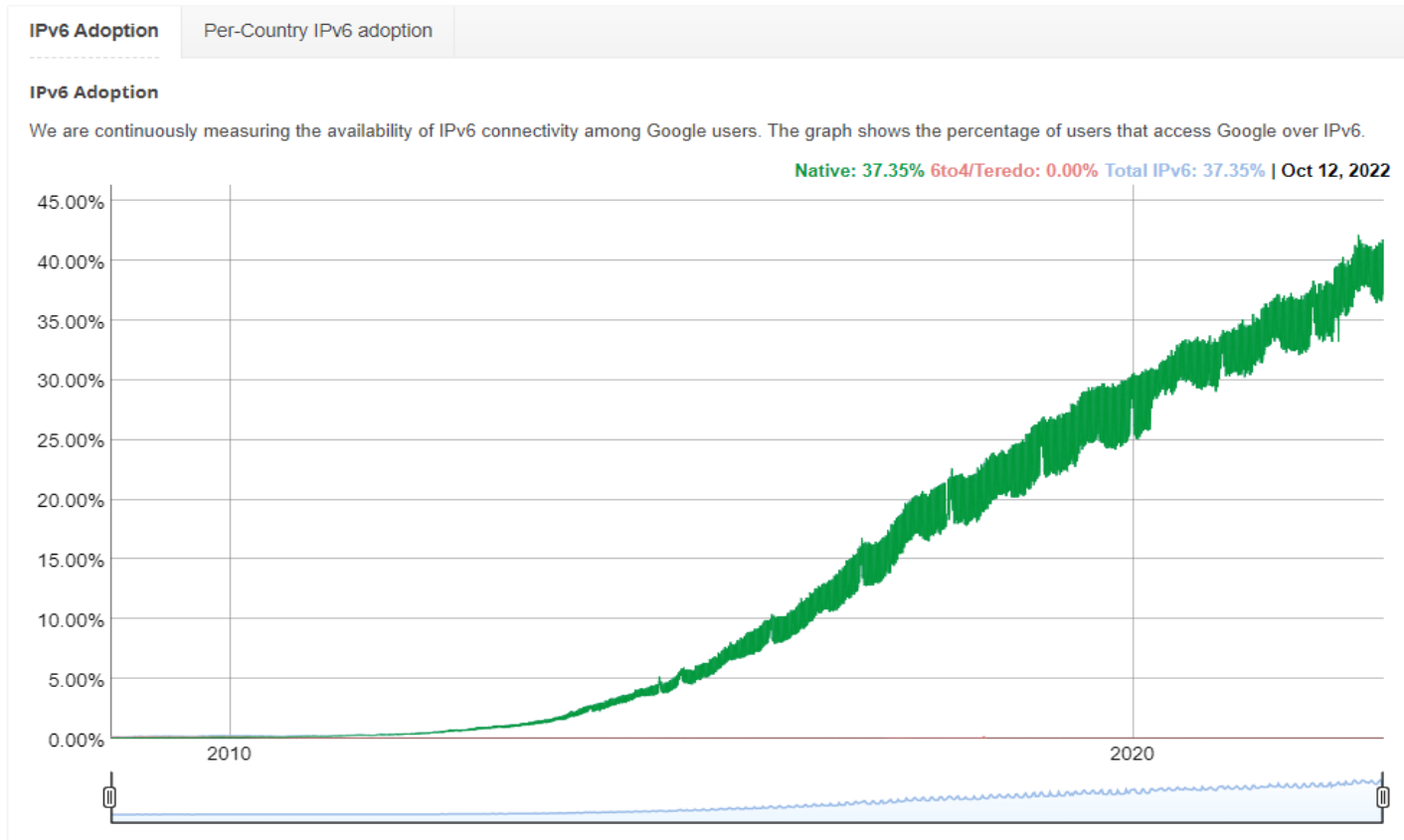
Chapter 02

IPv6 vs IPv4

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	$2^{32} = \sim 4,294,967,296$	$2^{128} = \sim 340,282,366,920,938,463,463,374,607,431,768,211,456$

Chapter 02

IPv6 Adoption



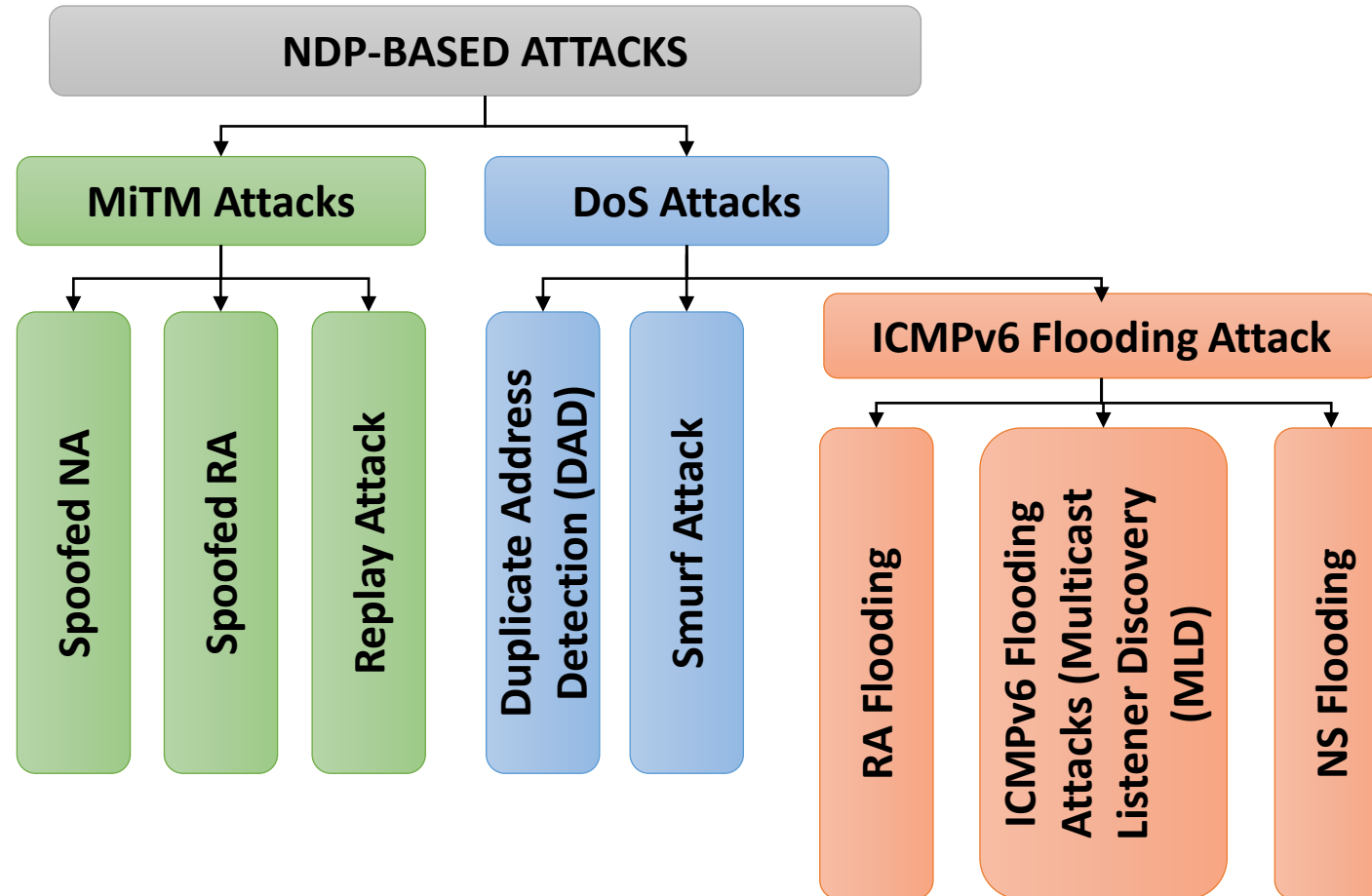
<https://www.google.com/intl/en/ipv6/statistics.html>



- IPv6 is intended for end-to-end encryption, man-in-the-middle attacks should become much more challenging if IPv6 is widely used.
- IPv6 also supports more-secure name resolution. The Secure Neighbor Discovery (SEND) protocol adds a security extension to the Neighbor Discovery Protocol (NDP), which handles the discovery of other network nodes on a local link.
- NDP is not secure by default, so it can be vulnerable to malicious intrusion. SEND secures NDP with a cryptographic method that is independent of IPsec.
- IPv6 provides two security headers that can be used separately or together: the Authentication Header (AH) and Encapsulating Security Payload (ESP).
- Authentication Header provides data-origin authentication and protection against replay attacks, while ESP delivers connectionless integrity, data origin authentication, protection against replay attacks, and limited traffic flow confidentiality, as well as privacy and confidentiality through encryption of the payload.

- NDP is a supporting protocol used with IPv6. It operates in the link layer of the Internet model (RFC 1122).
- IPv6 depends heavily on NDP, which appears in the network in the form of ICMPv6. If ICMP is disabled or dropped from the network, IPv6 does not operate, 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.
- 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.

ICMPv6 Packet Type	Description
RS (Type – 133)	Hosts inquire with RS messages to locate routers on an attached link. Nodes that forward packets not addressed to them generate RSs immediately upon receipt of this message, rather than at their next scheduled time
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)	Neighbor Solicitations are used by nodes to determine the link-layer address of a neighbor, or verify that a neighbor is still reachable via a cached link-layer address
NA (Type – 136)	Neighbor Advertisement are used by nodes to respond to an NS messages.
Redirect (Type – 137)	Routers may inform hosts of a better first hop router for a destination.

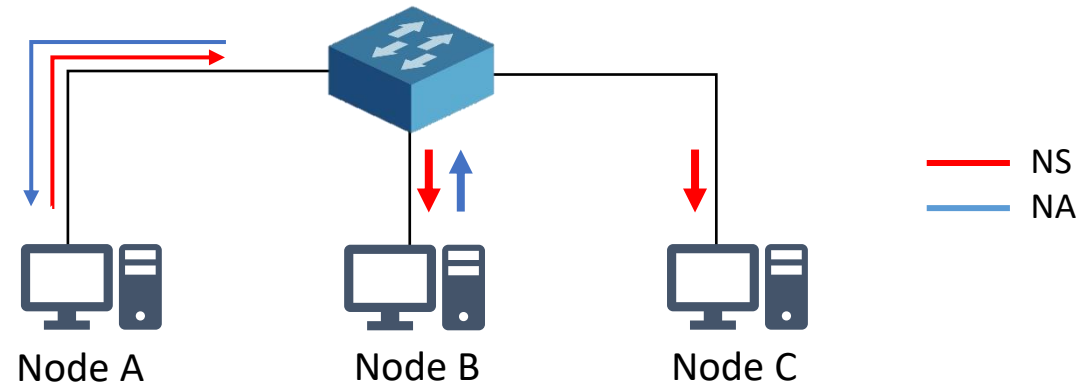


- MiTM is an attack during the access-gaining phase in which the attacker positions himself/herself in the middle of the data communication between two parties.
- MiTM attack is useful for conducting further attacks, such as sniffing and session hijacking.
- In IPv4, MiTM can be performed in various ways, such as Address Resolution Protocol (ARP) cache poisoning or Dynamic Host Configuration Protocol (DHCP) spoofing.
- ARP in IPv6 is replaced by the ICMPv6 neighbor discovery process, while DHCP can be replaced by an alternative process, stateless auto-configuration.

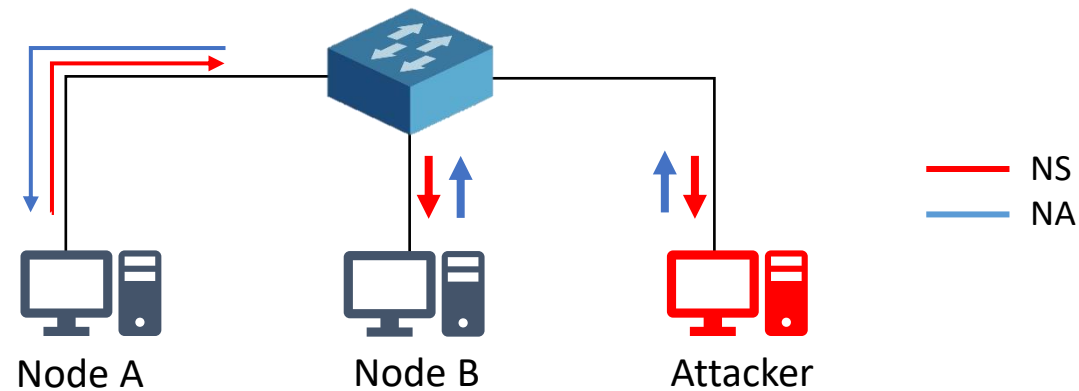
- In a link-local network, the communication between two nodes can be performed normally by exchanging two types of NDP messages, NS and NA.
- The two types of NDP messages are used to bind the MAC of the IPv6 address on the network. Unfortunately, these exchanges are completely unsecured.
- No countermeasures 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.

Chapter 02

MiTM Attacks: Spoofed NA (Cont.)



Normal process of looking up the MAC of the IPv6 address on the network



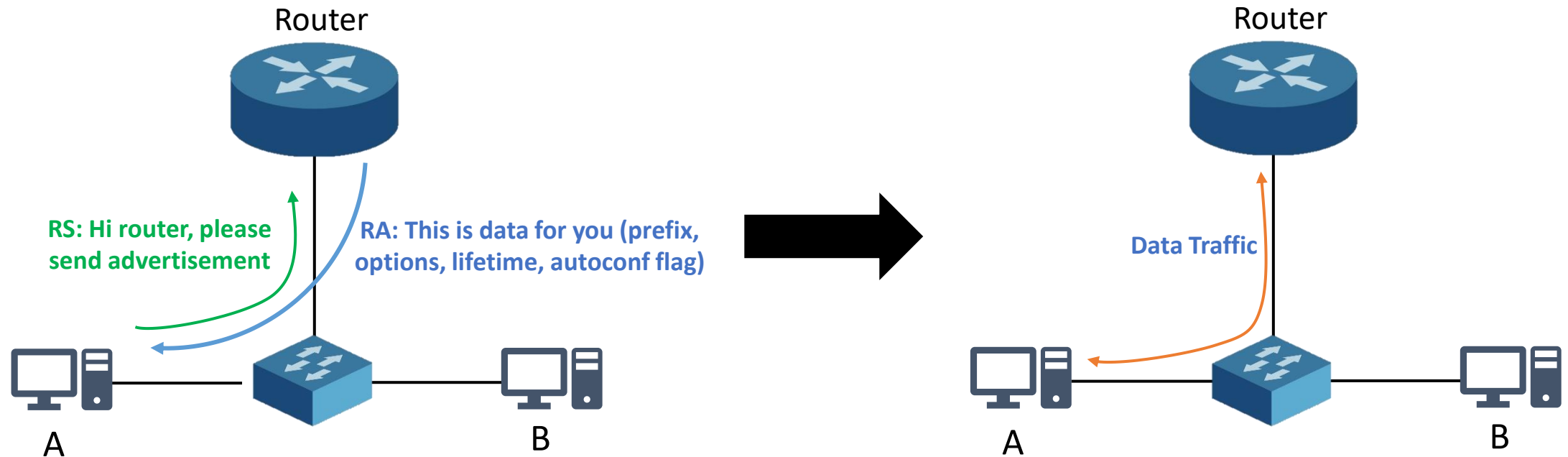
Example of spoofed

- 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.
- The IPv6 node can then prompt 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.

The default periodic time for the RA

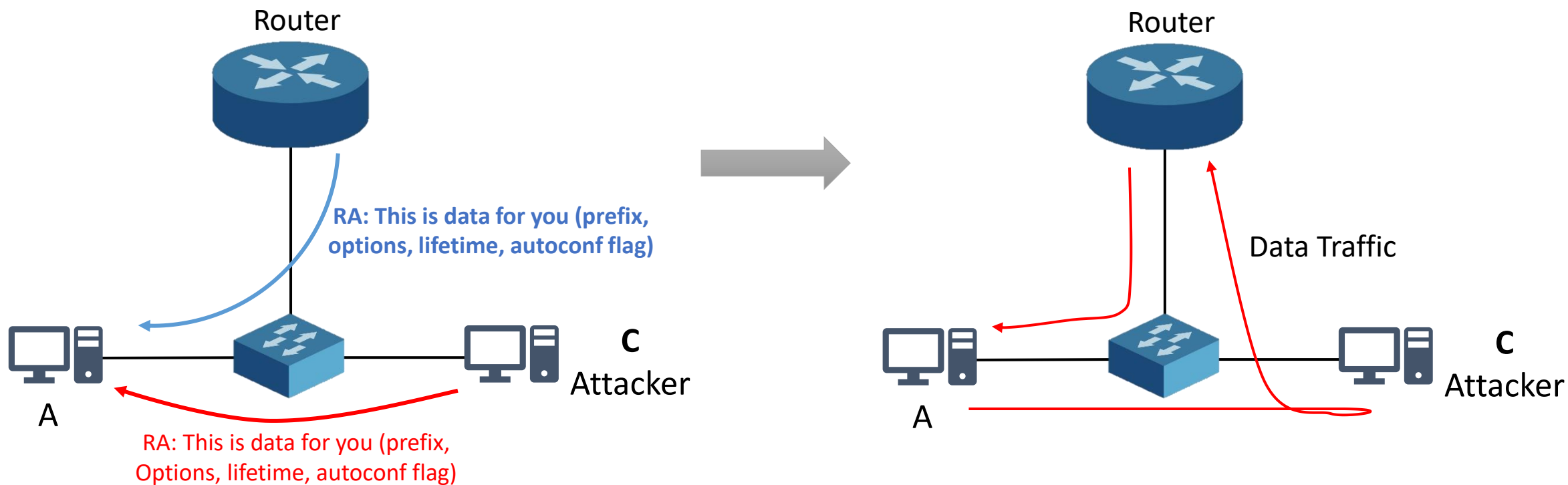
```
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 100 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

Router Advertisement



Chapter 02

MiTM Attacks: Spoofed RA (Cont.)



- A replay attack is a replay of any previous neighbor 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 is secure.
- There are three different attributes that secure communications must have secrecy, integrity, and authentication.

Below, are the recommendations to reduce the risk of Man in the Middle or to prevent it :

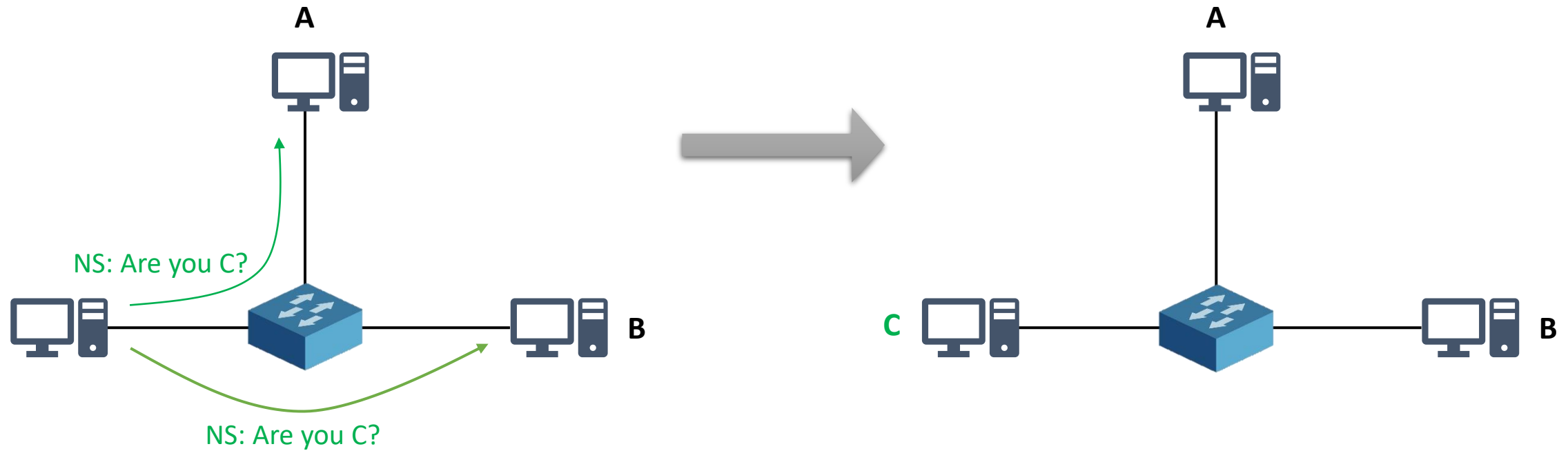
- You can monitor the neighbor cache entry and create an early alert mechanism when a suspicious change of cache occurs.
- You can use Secure Neighbor Discovery (SEND) in order to prevent a Man in the Middle attack, but it potentially increases your device load because of the encryption required.
- It is recommended to layer two devices such as a switch, with a router advertisement guard (RA guard) in order to block malicious incoming RA (IETF, 2011).

- IPsec on mobile IPv6, which is mandatory by default, prevents Man in the Middle from targeting mobile device.
- In addition, the create mechanism to give early alert about rogue DHCPv6 server detection. Multiple DHCPv6 servers may help to reduce the impact of Man in the Middle.
- It is also recommended to create a permanent entry for the default gateway address on the neighbor cache.

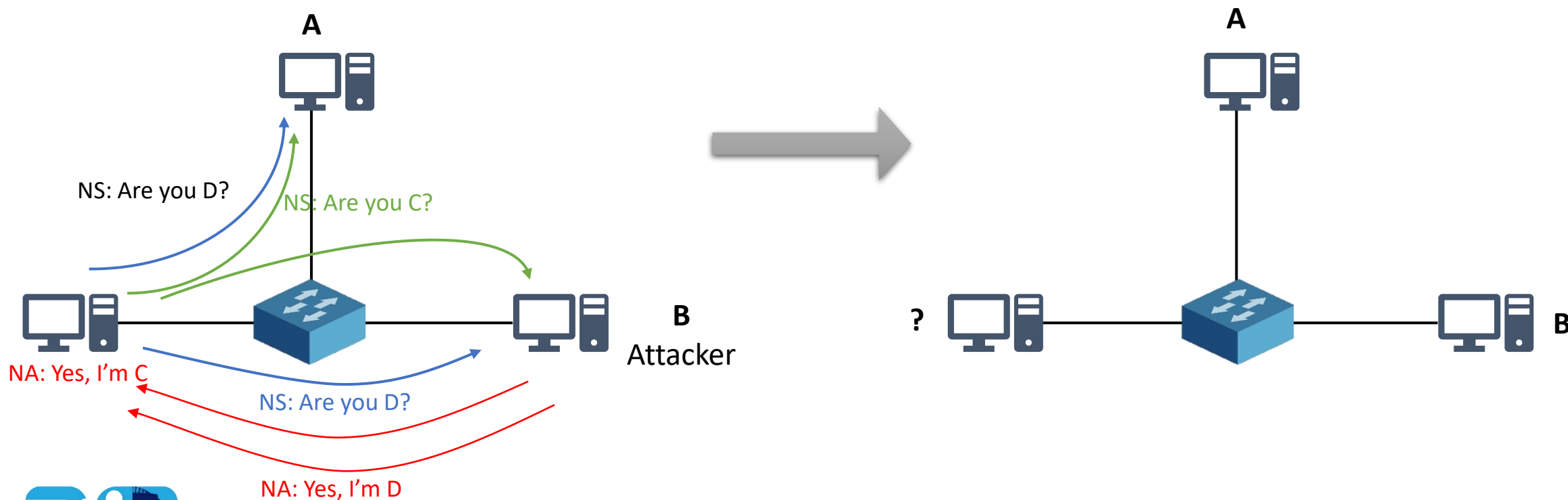
- In a DoS attack, the attacker makes an organization's network services or resources unavailable to legitimate users.
- A DoS attack on an IPv6 network can be launched by exploiting vulnerabilities in IPv6.
- Any deliberate effort to cut off a website or network from its intended users qualifies as a DoS attack.
- Such attacks have been successfully deployed against major online businesses, including Visa, Master card, Twitter, and WordPress.

- The DAD process ensures that all the IP address assigned to the node segment is unique.
- The attacker falsely responds with a neighbor advertisement packet, informing the new node that it is already using that address.
- Upon receiving the NA, the new node generates another address and repeats the DAD procedure; the attacker again falsely responds with an NA packet.
- Eventually, the new node gives up without initializing its interface.

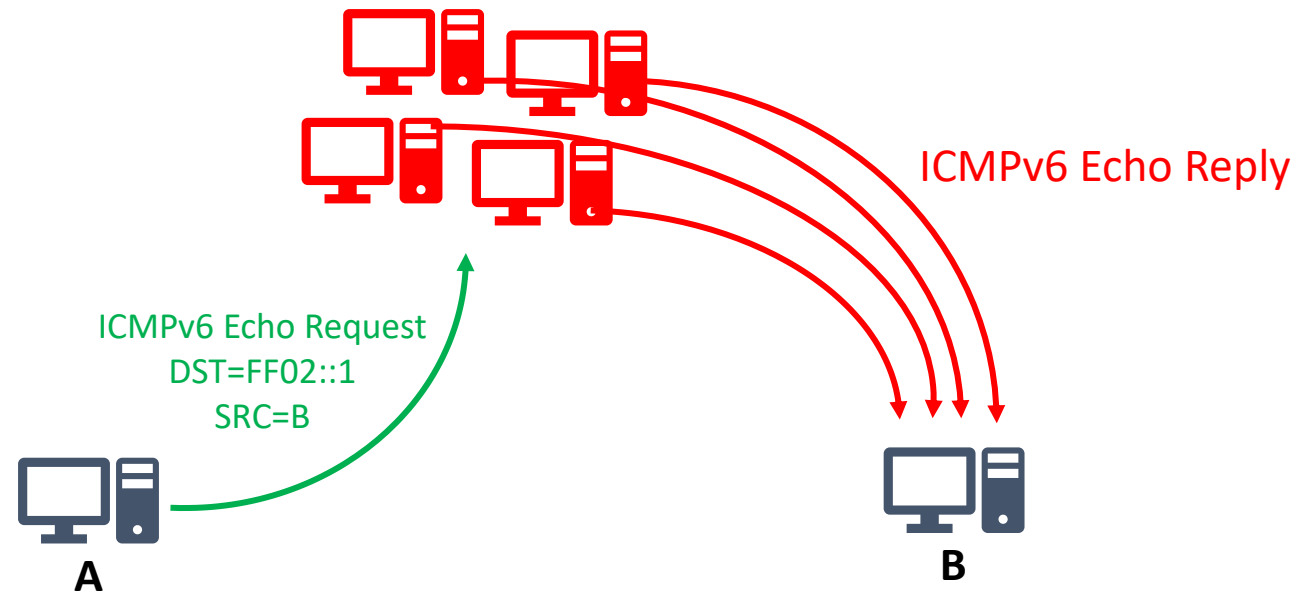
Duplicate Address Detection



Duplicate Address Detection



- A Smurf attack aims to flood the target machine with a large amount of traffic with the intention of keeping the target machine busy responding 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.



- 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 fake address prefix information to reroute legitimate traffic to prevent the victim from accessing the desired network.

- RA's message is sent to the 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.

- 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, and rendering the systems unusable and unresponsive.
- As IPv6 auto-configuration is 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.

Traffic generated IPv6 addresses by performing an RA

Time	Source IP	Destination IP	Protocol	Length
97.11189	fe80::218:7bff:fe86:189e	ff02::1	ICMPv6	118
97.1127	fe80::218:1eff:fe07:89a1	ff02::1	ICMPv6	118
97.12059	fe80::218:dcff:fe86:4745	ff02::1	ICMPv6	118
97.12208	fe80::218:dfff:fec3:55f8	ff02::1	ICMPv6	118
97.12348	fe80::218:6eff:feaf:14f7	ff02::1	ICMPv6	118
97.12462	fe80::218:deff:fec3:4e25	ff02::1	ICMPv6	118
97.12562	fe80::218:2cff:fe89:4981	ff02::1	ICMPv6	118
97.12662	fe80::218:1eff:fe61:9732	ff02::1	ICMPv6	118
97.12746	fe80::218:4cff:fe91:7c9b	ff02::1	ICMPv6	118
97.1283	fe80::218:79ff:fe0f:78c2	ff02::1	ICMPv6	118

Chapter 02

DoS Attacks: RA Flooding (cont.)

```
ICMPv6 110 Router Advertisement from c0:00:15:70:d6:8f

Cur hop limit: 64
Flags: 0x80
  1... .... = Managed address configuration: Set
  .0.. .... = Other configuration: Not set
  ..0. .... = Home Agent: Not set
  ...0 0... = Prf (Default Router Preference): Medium (0)
  .... .0.. = Proxy: Not set
  .... ..0. = Reserved: 0
```

Default preference flag in a legitimate RA message

```
ICMPv6 214 Router Advertisement from 00:0c:29:70:fe:0d

Cur hop limit: 255
Flags: 0x08
  0... .... = Managed address configuration: Not set
  .0.. .... = Other configuration: Not set
  ..0. .... = Home Agent: Not set
  ...0 1... = Prf (Default Router Preference): High (1)
  .... .0.. = Proxy: Not set
  .... ..0. = Reserved: 0
```

Preference field in a fake RA message

Chapter 02

DoS Attacks: RA Flooding (cont.)

List of IPv6 addresses generated by a single node with different prefixes

```
C:\WINDOWS\system32\cmd.exe
fe80::218:6dff:fece:6a06%4
fe80::218:c8ff:feef:8d08%4
fe80::218:ecff:fe46:c16a%4
fe80::218:14ff:fece:993c%4
fe80::218:abff:fea1:3fbaz%4
fe80::218:1bff:fe66:7ea9%4
fe80::218:43ff:feef:2877%4
fe80::218:8cff:fe90:ece%4
fe80::218:daff:fe44:8dae%4
fe80::218:60ff:fed2:3301%4
fe80::218:bff:fed0:423a%4
fe80::218:79ff:fe13:d4a9%4
fe80::218:caff:fe70:a097%4
fe80::218:ebff:fe5e:2e81%4
fe80::218:4aff:fef3:30e0%4
fe80::218:63ff:fe6e:cc53%4
fe80::218:36ff:fe27:96df%4
fe80::218:a3ff:fe8c:95e2%4
fe80::218:19ff:fe8a:efa1%4
fe80::218:30ff:fee7:a926%4
fe80::218:f8ff:fe64:3f55%4
fe80::218:93ff:fe1d:88a2%4
fe80::218:9dff:fe8a:f6dd%4
fe80::218:3cff:fef2:5c37%4
fe80::218:8eff:fe69:fb1%4
```

- 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.

- An NS flooding attack occurs, when a victim node is flooded with NS messages, thereby enforcing 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 messages, with the result that all hosts in the same link receive these NS messages and update their neighbor caches accordingly.

- Anbar, M., Abdullah, R., Saad, R. M., Alomari, E., & Alsaleem, S. (2016). Review of Security Vulnerabilities in the IPv6 Neighbor Discovery Protocol. In Information Science and Applications (ICISA) 2016 (pp. 603-612). Springer Singapore.
- Pilihanto, A. (2011). A Complete Guide on IPv6 Attack and Defense. Sans. org [online].

Thank you

