
Networkforyou
Welcome
To
Network for you
IPV6 FHS
Networkforyou

IPv6 First Hop Security Features:

- IPv6 FHS (First Hop Security) are different features that secure IPv6 on L2 links.
- First "hop" might make you think about the first router but that's not the case. These are all switch features, in particular, the switch that sits between your end devices and the first router.

RA (Router advertisements) Guard:

- Any device on the network can transmit router advertisements and hosts don't care where it comes from.
- They will happily accept anything. With RA guard, you can filter router advertisements.
- You can create a simple policy where you only accept RAs on certain interfaces or you can inspect RAs and permit them only when they match certain criteria.
- Router advertisements can be used by hosts to automatically configure their own IPv6 address and set a default route using the information they see in the RA.
- Hosts automatically select a router advertisement and they don't care where it came from. This is how it was meant to be but it does introduce a security risk since any device can send router advertisements and your hosts will happily accept it.
- An attacker can send rogue router advertisements to redirect the traffic, or you can send so many RAs that it causes a DOS since your hosts will be too busy configuring their IPv6 prefixes.
- The IPv6 RA guard feature can filter router advertisements and runs on switches.
- This can be as simple as "don't allow RAs on this interface" or complex with policies where router advertisements are only permitted when it matches certain criteria.

DHCPv6 Guard:

- Similar to DHCP snooping for IPv4 .
- We inspect DHCP packets and only permit them from trusted interfaces.
- You can also create policies where you only accept DHCP packets for certain prefixes or preference levels.
- **IPv6 DHCPv6 Guard is one of the IPv6 FHS (First Hop Security) mechanisms and is very similar to IPv4 DHCP snooping.**
- This feature inspects DHCPv6 messages between a DHCPv6 server and DHCPv6 client (or relay agent) and blocks DHCPv6 reply and advertisements from (rogue) DHCPv6 servers.
- DHCPv6 messages from clients or relay agents to a DHCPv6 server are not affected.

ND Inspection:

- IPv6 ND Inspection is one of the IPv6 first-hop security features.
- It creates a binding table that is based on NS (Neighbor Solicitation) and NA (Neighbor
- Advertisement) messages.
- The switch then uses this table to check any future NS/NA messages.
- When the IPv6-LLA combination does not match, it drops the message.
- This only applies to NS/NA messages , it doesn't drop any actual data packets that have a spoofed IPv6 or MAC address.

Source Guard:

- IPv6 Source Guard is one of the IPv6 FHS (First Hop Security) features.
- It filters inbound traffic on L2 switch ports that are not in the IPv6 binding table.
- The binding table stores the following information: a. IPV6 address b. MAC address c. VLAN d. Interface ID
- Source Guard only looks at information found in the binding table, and it doesn't fill the binding table.

IPv6 First Hop Security (FHS) features are a set of security features that can be implemented on Layer 2 switches to help protect IPv6 networks from a variety of attacks.

These features include:

RA Guard: This feature helps to prevent unauthorized routers from sending Router Advertisement (RA) messages on the network. RA messages are used to provide information about the IPv6 network, such as the prefix, the default gateway, and the preferred router. By blocking unauthorized RA messages, RA Guard can help to prevent unauthorized access to the network.

DHCP Guard: This feature helps to prevent unauthorized DHCPv6 servers from sending DHCPv6 messages on the network. DHCPv6 messages are used to provide IPv6 addresses and other configuration information to hosts on the network. By blocking unauthorized DHCPv6 messages, DHCP Guard can help to prevent unauthorized access to the network.

Binding Table: The binding table is a table that is maintained by the switch to store information about the IPv6 addresses and ports of the hosts on the network. This information is used by the other FHS features to help protect the network.

ND Inspection/Snooping: This feature helps to prevent unauthorized Neighbor Discovery (ND) messages from being sent on the network. ND messages are used by hosts to discover each other and to learn about the topology of the network. By blocking unauthorized ND messages, ND Inspection/Snooping can help to prevent unauthorized access to the network.

Source Guard: This feature helps to prevent unauthorized hosts from sending packets on the network. Source Guard works by filtering packets based on the source address of the packet. If the source address of the packet is not found in the binding table, the packet is dropped.

These features can be used together to provide a comprehensive security solution for IPv6 networks. By implementing these features, network administrators can help to protect their networks from a variety of attacks.