IPv6 First Hop Security (FHS)

Enterprise Borderless Network

Last Updated: June 2013

First Hop Overview

In many modern networks, the Layer 2 domain is playing an increasingly important role, with large campuses, very large data centers, server virtualization, Overlay Transport Virtualization (OTV), Layer 2 mobility, etc., all resulting in larger Layer 2 domains. This change also brings with it an increasing number of challenges, such as security and scalability. In parallel with this change, IPv6 has been gaining momentum as the next generation IP, while the IPv4 address space continues to run out.

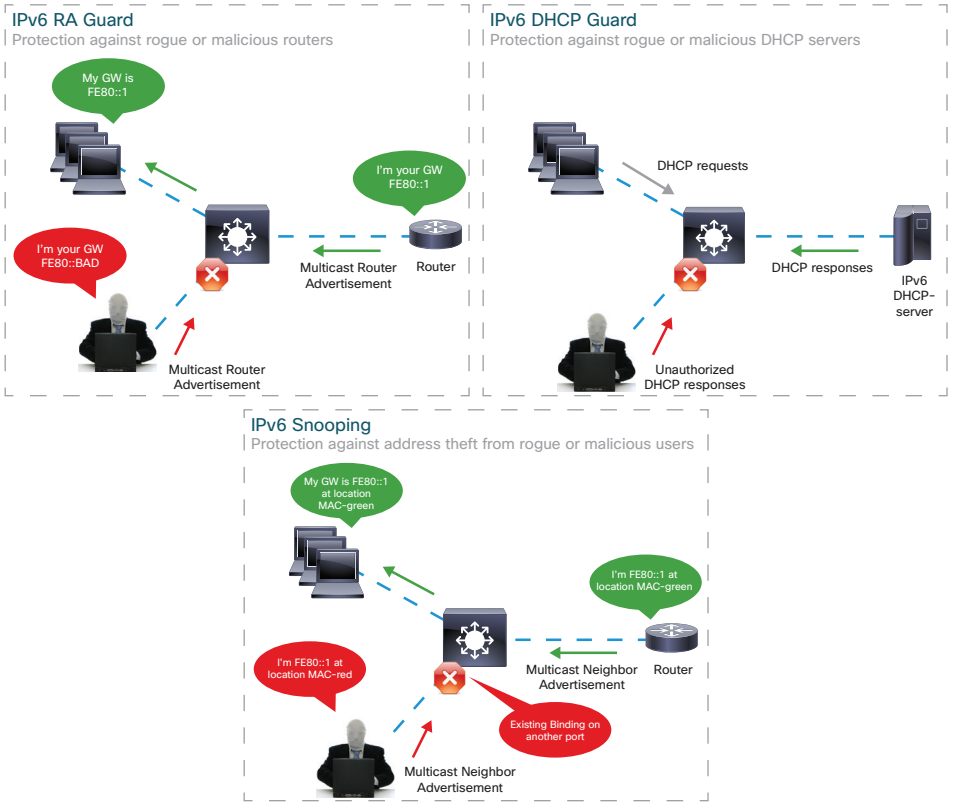
Layer 2 (and to some extent Layer 2/3) switches constitute the core of this Layer 2 domain, and their strategic position in the network provides a number of opportunities to secure this domain, and to optimize link operations. These devices are sometimes referred to as "first hops", specifically when they are facing end nodes. For many years, Cisco has been providing a suite of Catalyst Integrated Security Features (CISF) running on Catalyst switches, to secure and optimize Layer 2 (L2) operations for IPv4 networks. In order to provide the same level of end node protection on IPv6 or dual-stack networks, these L2 switches need to add a similar set of capabilities to address IPv6 link operations.

A myth and misconception that is frequently stated is that IPv6 is more secure than IPv4. This assertion stems from the original mandated use of IPSec in host-to-host communication, as specified in RFC 2401. Certainly, if IPSec is implemented, it would provide confidentiality and integrity between two hosts, but it still would not address any link operation vulnerabilities, attacks, and most of the Denial-of-Service (DoS) attacks. Furthermore, many consider IPv6 to be equivalent to IPv4, with the only difference being a larger address space, but this is not the case. In comparison with IPv4, IPv6 has an increased set of capabilities to simplify end-system auto-configuration, which includes the automated discovery of routers, neighbor resolution, duplicate address detection and neighbor unreachability detection. These enhancements bring along with them a different set of security vulnerabilities that must be addressed. Enter the IPv6 First Hop Security (FHS) solution, whose main role is to "secure and optimize IPv6 link operations."

What is First Hop Security?

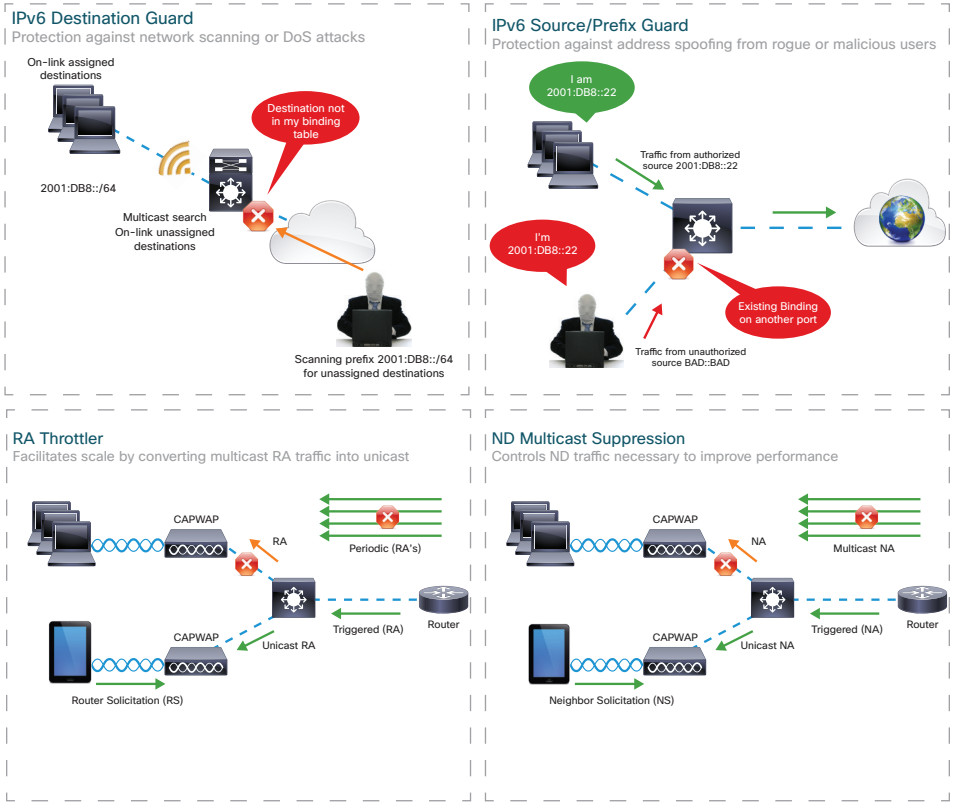
First Hop Security is a suite of features designed specifically to harden IPv6 link operation, as well as help with scale in large L2 domains. The base set of functionality provides solid protection from a wide host of rogue or mis-configured users, and this can be extended with additional features for different deployment scenarios, or attack vectors.

The FHS functionality is supported in Catalyst® 6500, 4500, 3850, 3750 and 2960 Series Switches, 7600 Series Routers and Cisco 5700 Series Wireless LAN Controllers.



FHS features can be classified in three feature categories (core, advanced and performance scalability) as follows:

- Core:
  - **RA Guard**–blocks unauthorized Router Advertisements (RAs)
  - **DHCP Guard**–blocks unauthorized DHCP servers
  - **IPv6 Snooping**–analyzes control/data switch traffic, detects IP address, and stores/updates them in a binding table.
- Advanced:
  - **Source/Prefix Guard**–validates source address or a prefix of IPv6 traffic sourced from the link
  - **Destination Guard**–validates the destination address of IPv6 traffic reaching the link
- Performance and scalability:
  - **RA Throttler**–facilitates scale by converting multicast RA traffic into unicast
  - **ND Multicast Suppress**–controls Neighbor Discovery (ND) traffic necessary for proper link operations and improves performance
- IPv6 FHS provides effective counter measures for the following types of attacks or misconfiguration errors that could result in DoS or information theft:
  - Router impersonation (MiM attacks)
  - Address theft
  - Address spoofing
  - Remote address resolution cache exhaustion (DoS attacks)
- These attacks can come from malicious or mis-configured users and could result in severe disruption to users of the Layer 2 domain and to the network in general. Many of the possible attack vectors are now known, with public tools readily available to exploit these vulnerabilities. With the transition to IPv6 picking up pace, it's now time for you to be aware of the vulnerabilities, understand how to mitigate against them, and to protect your network accordingly.



Why Cisco?

Cisco has the broadest support for IPv6, and IPv6 security in the industry. Cisco should be your valued business partner to help you securely deploy IPv6 to allow your organization to continue to thrive in the next wave of IP.

C45-707354-02 05/13