IPv6 First Hop Security—Protecting Your IPv6 Access Network

What You Will Learn

This paper provides a brief introduction to common security threats on IPv6 campus access networks and will explain the value of using First Hop Security (FHS) technology in mitigating these threats. An overview of the operational principle of FHS is provided together with some examples on how to enable FHS on Catalyst® 6500, 4500, and 3750 Series Switches.

The target audience for this paper is network architects and network operation engineers.

Why First Hop Security for IPv6?

There are a growing number of large-scale IPv6 deployments at enterprise, university, and government networks. For the success of each of these networks, it is important that the IPv6 deployments are secure and are of a service quality that equals that of the existing IPv4 infrastructure.

Network users have an expectation that there is functional parity between IPv4 and IPv6 and that on each of these protocols security and serviceability concerns are similar. From the network operator perspective there is a similar assumption that both IPv4 and IPv6 are secure environments with a high degree of traceability and quality assurance.

This situation in the first instance comes down to a new set of technology paradigms. Threats for example are very much tied to the topology of a network infrastructure, and IPv6 brings in specific changes from a topology perspective:

- More end nodes allowed on the link (up to 2^{64})
- Bigger neighbor cache on end nodes
- Bigger neighbor cache on default router
- These create more opportunities for denial-of-service (DoS) attacks

In addition to the topological aspects there are threats closely related to the protocols in use:

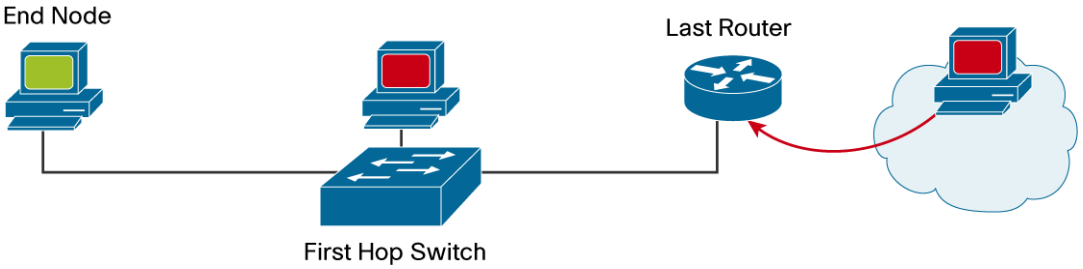
- Neighbor Discovery Protocol (NDP) integrates all link operations in charge of determining address assignment, router discovery, and associated tasks like redirect.
- Dynamic Host Configuration Protocol (DHCP) has a smaller role in address assignment compared to IPv4.
- Noncentralized address assignment creates true challenges for controlling address misusage.

Due to the uptake in IPv6 technology and the intrinsic differences between IPv4 and IPv6 outlined above, it is very important to have both a secure IPv4 environment and a secure IPv6 environment. It will be useful to understand where IPv6 is used for the various aspects and how best to secure the IPv6 infrastructure when connecting systems and devices to a network link.

Where to Secure Link Operations

When analyzing where best to secure the link operations, these can be divided into three different locations within the network. Security enforcement can happen at the end nodes, at the first hop within the network, and at the last hop (see Figure 1).

Figure 1. Link protection protagonists



At the End Node

This security model, a distributed model where the end nodes take care of themselves, does not provide any link operation with bottlenecks or single points of failure. This security model does not need central administration or operation as it is assumed that each node takes care of itself. The ultimate level of security in this model is accomplished by a SeND (RFC 3971) deployment.

This model is especially good for threats coming directly from the link; however, it provides poor protection against threats from offlink devices. Another consideration for this model is that, due to its distributed nature, a degree of complexity and heavy provisioning of end nodes is involved that spreads over the complete networking domain that is being secured.

At the First Hop Switch

This model is based upon a centralized model run by a centralized security administration. The burden of security enforcement of the previous model is pushed toward the first hop device, making this model a better scalable model as fewer devices are affected by the security tasks involved. This model makes the transition from a nonsecure link operation to a secure network easier as fewer components will have to be touched, monitored, and reconfigured.

While this model is a very convenient model for the network operator and the actual end user, it will be useful only in certain topologies in which all end users go through a network operator aggregation device capable of securing the link operations. This model increases the intelligence and the awareness that first hop networking devices need to have about the actual end nodes attached.

At the Last Router

The only option available here is the centralized model, which is good for securing against threats coming from outside of the link that is being protected. A property of this model is that the attached link is protected as well as all the downstream network elements.

This model must be combined with the first hop switch model to defeat threats that come from inside when, for example, a device has been compromised and is affecting the Internet network infrastructure. It requires the last hop router to learn about end nodes.

ICMPv6 and Neighbor Discovery Protocol

This section introduces the Internet Control Message Protocol Version 6 (ICMPv6). In comparison with IPv4, IPv6 has an increased set of capabilities to simplify end-system autoconfiguration while at the same time running service detection by means of ICMP. Because of these new ICMP capabilities, the importance of ICMP for IPv6 is much higher than it ever was for IPv4.

One of the new functionalities within ICMPv6 is the Neighbor Discovery Protocol, which in its base specification is a nonauthenticated protocol. NDP is an application and operates above ICMPv6. NDP makes heavy usage of multicast packets for on-the-wire efficiency.

The functional applications of NDP include:

- Router discovery
- Autoconfiguration of addresses (stateless address autoconfiguration [SLAAC])
- IPv6 address resolution (replaces Address Resolution Protocol [ARP])
- Neighbor reachability (neighbor unreachability detection [NUD])
- Duplicate address detection (DAD)
- Redirection

What Is SeND?

Secure Neighbor Discovery is a protocol that enhances NDP with three additional capabilities:

- **Address ownership proof**
  - Makes stealing IPv6 addresses “impossible”
  - Used in router discovery, DAD, and address resolution
  - Based upon Cryptographically Generated Addresses (CGAs)
  - Alternatively also provides non-CGAs with certificates
- **Message protection**
  - Message integrity protection
  - Replay protection
  - Request/response correlation
  - Used in all NDP messages
- **Router authorization**
  - Authorizes routers to act as default gateways
  - Specifies prefixes that routers are authorized to announce “on-link”

While SeND provides a significant uplift to the IPv6 neighbor discovery technology by introducing the above enhancements, it does not, for example, provide any end-to-end security and provides no confidentiality.

It is important to understand that SeND is **not** a new protocol and still remains a protocol operating on the link. Secure Neighbor Discovery is just an “extension” to NDP and defines a set of new attributes:

- **New network discovery options**

  CGA, Nonce[1], Timestamp, and RSA

  Purpose: These options provide a security shield against address theft and replay attacks.
- **New network discovery messages**

  CPS (Certificate Path Solicitation), CPA[2] (Certificate Path Advertisement)

[1] In order to prevent replay attacks, two new neighbor discovery options, Timestamp and Nonce (a random number), are introduced. Given that neighbor and router discovery messages are in some cases sent to multicast addresses, the Timestamp option offers replay protection without any previously established state or sequence numbers. When the messages are used in solicitation-advertisement pairs, they are protected with the Nonce option.

[2] Certification paths, anchored on trusted parties, are expected to certify the authority of routers. A host must be configured with a trust anchor to which the router has a certification path before the host can adopt the router as its default router. Certification path solicitation and advertisement messages are used to discover a certification path to the trust anchor without requiring the actual router discovery messages to carry lengthy certification paths. The receipt of a protected router advertisement message for which no certification path is available triggers the authorization delegation discovery process.

Purpose: Identifying valid and authorized IPv6 routers and IPv6 prefixes of the network segment. These two messages complement the already existing NDP messages (NS, NA, RA, RS, and Redirect).

- **New rules**

  Purpose: These rules describe the preferred behavior when a SeND node receives a message supported by SeND or not supported by SeND.

SeND technology works by having a pair of private and public keys for each IPv6 node in combination with the new options (CGA, Nonce, Timestamp, and RSA). Nodes that are using SeND cannot choose their own interface identifier because the interface identifier is cryptographically generated based upon the current IPv6 network prefix and the “public” key. However, the CGA interface identifier alone is not sufficient to guarantee that the CGA address is used by the appropriate node.

For this purpose SeND messages are signed by usage of the RSA public and private key pair. For example if node 1 wants to know the MAC address of node 2, it will traditionally send a neighbor solicitation request to the node 2 solicited node multicast address. Node 2 will respond with a corresponding neighbor advertisement containing the MAC address to IPv6 address mapping. Node 2 will in addition add the CGA parameters (which include among others the public key) and a private key signature of all neighbor advertisement fields. When node 1 receives this neighbor advertisement it uses the public key to verify with the CGA address the private key signature of node 2. Once this last step has been successfully completed, the binding on node 1 of the MAC address and CGA address of node 2 can be successfully finalized.

Note that the above mechanism is simply an explanation to verify the correct relationship between a node MAC address and its CGA IPv6 address. SeND does not check any of the node’s privileges to be allowed, or not allowed, on the network. If this is required, other means of infrastructure protection will be required (such as 802.1x).

SeND Deployment Challenges

While the construction of a CGA address is a rather lightweight action because it “only” requires hosts to be crypto-capable (generate RSA key pairs, RSA sign NDP messages, and RSA verify messages). On the other hand, the SeND capability for router authorization is a much more heavyweight technology because it relies upon Certificate Authority (CA) implementation for hosts to trust routers. Also for routers to be trusted, they need some PKI implementation so that they can get a certificate from the CA and for obtaining and maintaining the certificate chain in case of hierarchical CAs. It is a pragmatic assumption that many hosts will not be deployed with CA certificates due to the complexity involved. Another challenge to deploy SeND is the bootstrapping of the trust relationship. To access the Certificate Revoke List (CRL) and the time server, the host would need to access these devices through a router it does not trust yet. A way to work around this challenge is to preprovison the host with certificates and ship them to users.

Securing at the First Hop

The first hop for an end node is very often a Layer 2 switch. By implementing the right set of security features this switch has a potential to solve many of the caveats attached to a SeND deployment and increase the link security model. The first hop switch is strategically located to learn about all its neighbors, and hence the switch can easily either allow or deny certain types of traffic, end-node roles, and claims. In its central position, the first hop switch can fulfill a number of functions. It will inspect the ND traffic and provide information about Layer 2/Layer 3 binding and monitor the use of ND by host to spot potentially abnormal behaviors. Ultimately, the switch can block undesired traffic such as rogue Router Advertisement (RA), rogue DHCP server advertisement, and data traffic coming from undesired IP addresses or prefixes.

Example of First Hop Security Configuration of Catalyst 6500, 4500 and 3750 Series

When IPv6 is implemented on the LAN network, certain switch ports are known to have only traditional end-node user devices attached. It can be safely assumed that these end-node user devices will not serve as either a router or DHCPv6 server. It is strongly recommended that the switches be configured in such a way that both RAs and DHCPv6 server packets are filtered on these end-node user ports to protect the network link operations.

To achieve this goal the following port access control list (PACL) can be implemented:

```
ipv6 access-list ACCESS_PORT
    remark Block all traffic DHCP server -> client
    deny udp any eq 547 any eq 546
    remark Block Router Advertisements
    deny icmp any any router-advertisement
    permit any any
!
interface gigabitethernet 1/0/1
    switchport
    ipv6 traffic-filter ACCESS_PORT in
```

PACLs have been available on the Catalyst 3750 Series since 12.2(46)SE, on the Catalyst 4500 Series since 12.2(54)SG, and on Catalyst 6500 Series since 12.2(33)SXI4.

On the Catalyst 6500 and 4500 Series a macro command creates the needed PACL to block RA:s

```
interface gigabitethernet 1/0/1
   switchport
   ipv6 nd raguard
```

Conclusion

Securing the IPv6 link is a cooperative effort, and all protagonists should be involved. Experience proves, however, that the first hop switch is a key piece of this puzzle and certainly plays a central role in link security, just like it did for IPv4. Compared to IPv4, IPv6 offers a number of technologies, such as SeND, that make security more flexible to deploy and more efficient at catching malicious behavior, paving the way for more secure deployments.

While Cisco IOS® Software supports the full IPv6 SeND and CGA technologies, it is currently not universally implemented within the most common host operating systems. This makes it crucial for the first hop network components to take this limitation into account and secure the link operations by other means like simple PACL configuration.

For More Information

- IPv6 Guard
  - IPv6 RA-Guard: http://www.ietf.org/id/draft-ietf-v6ops-ra-guard-04.txt
- IPv6 Rogue RA Problem Statement
  - Rogue IPv6 Router Advertisement Problem Statement: http://tools.ietf.org/html/draft-ietf-v6ops-rogue-ra-00
- Neighbor Discovery
  - RFC 2461: “Neighbor Discovery for IP Version 6 (IPv6)”
  - RFC 2462: “IPv6 Stateless Address Autoconfiguration”
- Trust Model and threats
  - RFC 3756: “IPv6 Neighbor Discovery (ND) Trust Models and Threats”

- Address ownership proof :
  - RFC 3972: “Cryptographically Generated Addresses (CGA)”
  - RFC 3971: “SEcure Neighbor Discovery (SEND)”
- Router authorization:
  - RFC 3971: “SEcure Neighbor Discovery (SEND)”
- Certificates:
  - RFC 3280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”
  - RFC 3779: “X.509 Extensions for IP Addresses and AS Identifiers”
- Cisco Press
  - IPv6 Security
- By Scott Hogg and Eric Vyncke
- ISBN-10: 1-58705-594-5; ISBN-13: 978-1-58705-594-2; Published: Dec 11, 2008; Copyright 2009
- IOS support for SeND
  - Implementing IPv6 Secure Neighbor Discovery: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-602135-00 05/10