

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de Rodat Stephane Sezer

July 8, 2011

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

1 IPv6?

- Addresses
- Multicast
- ICMP
- EUI64

IPv6?

Addresses
Multicast
ICMP
EUI64

What is the use of
NDP?

How does it work?

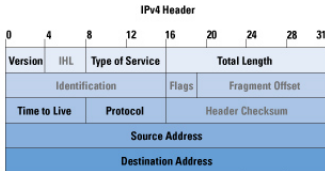
I can haz securitie?

Conclusion

The Derridj slide §

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer



IPv6?

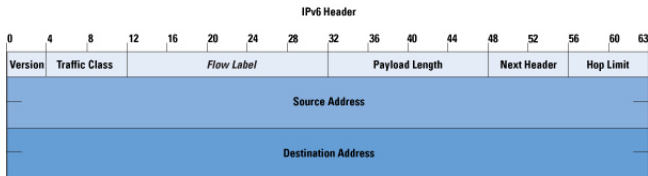
Addresses
Multicast
ICMP
EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion



Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

1 IPv6?

- Addresses
- Multicast
- ICMP
- EUI64

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

Address format

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

Addresses

Multicast

ICMP

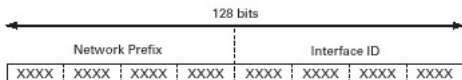
EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

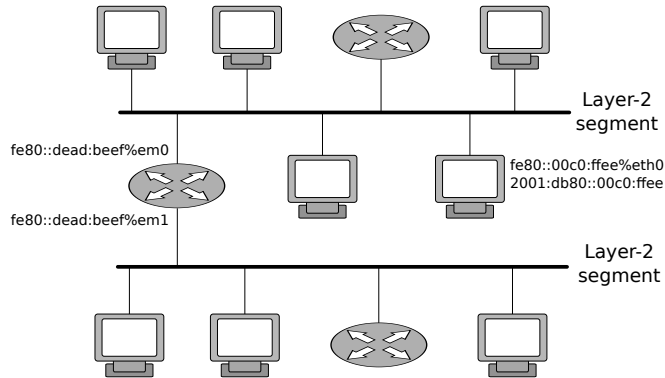
Conclusion



XXXX = 0000 through FFFF

$3.4 \times 10^{28} = \sim 340,282,366,920,938,463,374,607,432,768,211,456$ IPv6 Addresses

- Each address is assigned to an interface
- Each address has a scope
- Examples: link local, site local, global. . .



Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

Addresses

Multicast

ICMP

EUI64

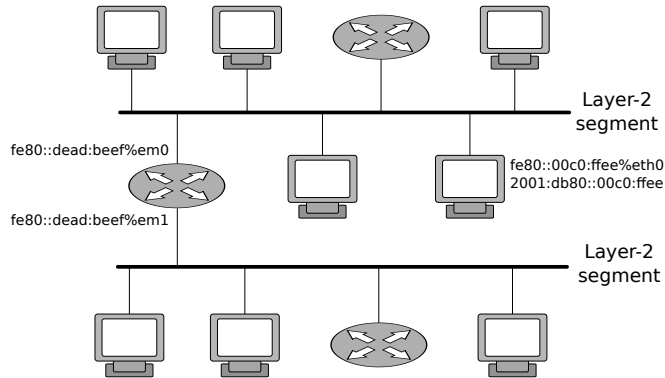
What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

- Each address is assigned to an interface
- Each address has a scope
- Examples: link local, site local, global. . .



Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stéphane
Sezer

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

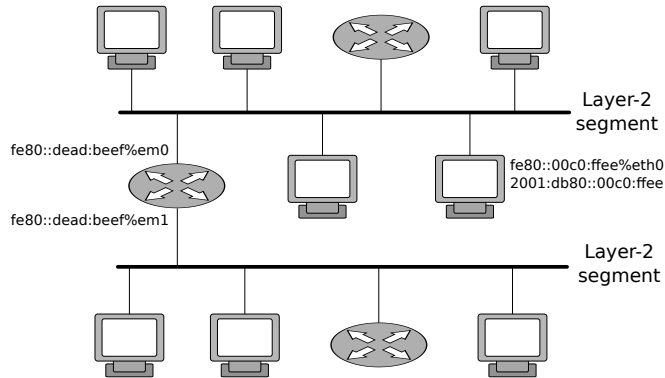
How does it work?

I can haz sekuritie?

Conclusion

Address scoping

- Each address is assigned to an interface
- Each address has a scope
- Examples: link local, site local, global. . .



Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stéphane
Sezer

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

1 IPv6?

- Addresses
- **Multicast**
- ICMP
- EUI64

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

I can haz securitie?

Conclusion

What is multicast?

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

- Reach a group of machines
- No broadcast in IPv6

What is multicast?

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

- Reach a group of machines
- No broadcast in IPv6

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

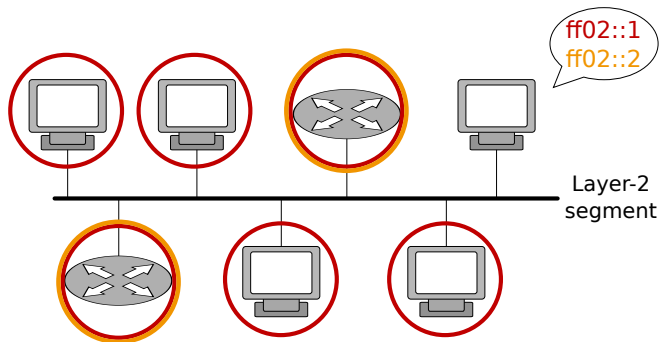
Conclusion

Multicast addresses on a local link

The ones we are interested in...

`ff02::1` All nodes on the local network segment

`ff02::2` All routers on the local network segment



Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

1 IPv6?

- Addresses
- Multicast
- **ICMP**
- EUI64

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

What is it used for?

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

- ICMPv6 is an integral part of IPv6
- Used for error reporting, diagnostics, etc. . .
- NDP fits here

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

What is it used for?

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

- ICMPv6 is an integral part of IPv6
- Used for error reporting, diagnostics, etc. . .
- NDP fits here

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

What is it used for?

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

- ICMPv6 is an integral part of IPv6
- Used for error reporting, diagnostics, etc. . .
- NDP fits here

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

1 IPv6?

- Addresses
- Multicast
- ICMP
- EUI64

IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

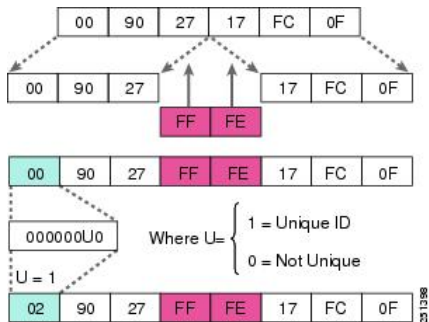
I can haz securitie?

Conclusion

Suffix construction from MAC address

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer



IPv6?

Addresses

Multicast

ICMP

EUI64

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

2 What is the use of NDP?

- Determination of the link-layer address of other nodes
- Autoconfiguration of the address of nodes
- DNS Configuration

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

DNS Configuration

How does it work?

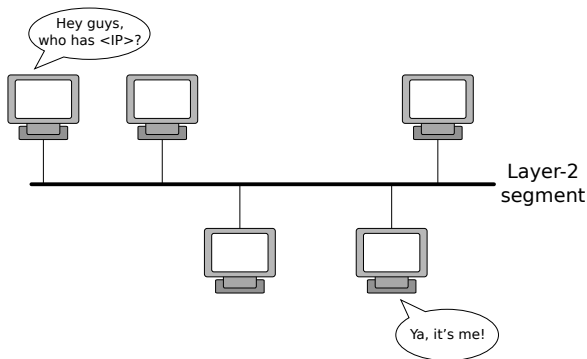
I can haz sekuritie?

Conclusion

2 What is the use of NDP?

- Determination of the link-layer address of other nodes
- Autoconfiguration of the address of nodes
- DNS Configuration

- When talking to a host on the same network
- Replaces ARP on an IPv6 network



Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

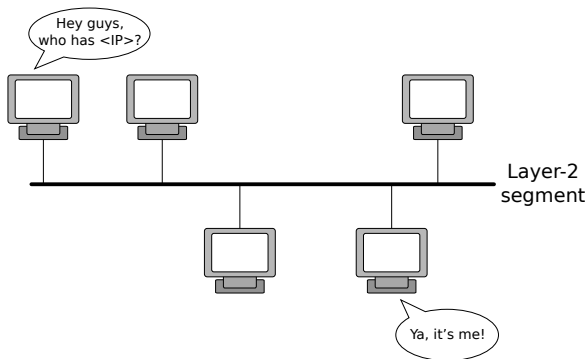
DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

- When talking to a host on the same network
- Replaces ARP on an IPv6 network



Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

2 What is the use of NDP?

- Determination of the link-layer address of other nodes
- Autoconfiguration of the address of nodes
- DNS Configuration

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

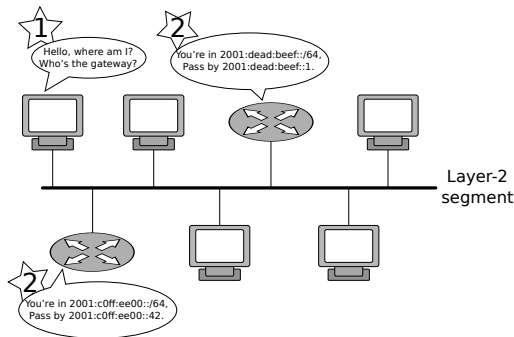
DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

- A machine connecting to a network,
- needs a prefix,
- and a suffix,
- and then... we have a full address.



Neighbor Discovery Protocol

Pierre-Marie de Rodat, Stéphane Sezer

IPv6?

What is the use of NDP?

Determination of the link-layer address of other nodes

Autoconfiguration of the address of nodes

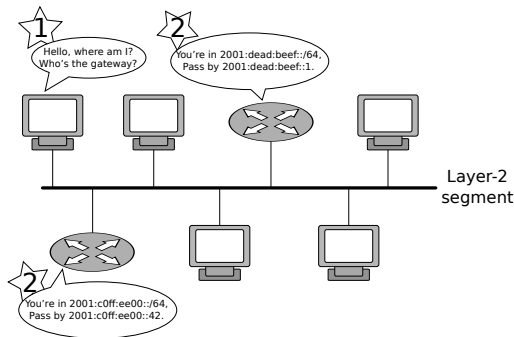
DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

- A machine connecting to a network,
- needs a prefix,
- and a suffix,
- and then... we have a full address.



Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

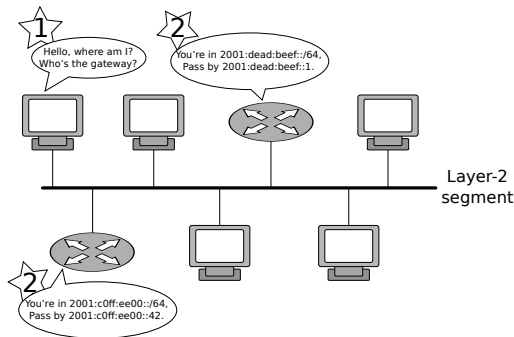
DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

- A machine connecting to a network,
- needs a prefix,
- and a suffix,
- and then... we have a full address.



Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

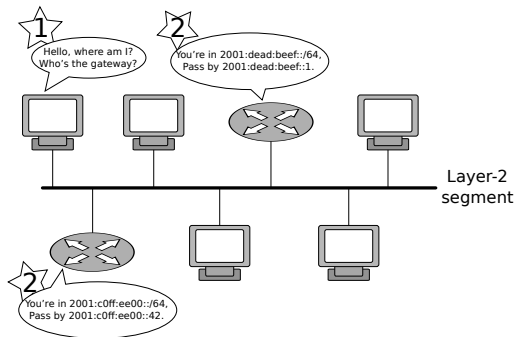
DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

- A machine connecting to a network,
- needs a prefix,
- and a suffix,
- and then... we have a full address.



Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

2 What is the use of NDP?

- Determination of the link-layer address of other nodes
- Autoconfiguration of the address of nodes
- DNS Configuration

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

- A host also needs a list of recursive DNS servers to query,
- and a search list.
- RFC 6106

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

- A host also needs a list of recursive DNS servers to query,
- and a search list.
- RFC 6106

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

- A host also needs a list of recursive DNS servers to query,
- and a search list.
- RFC 6106

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

Determination of the
link-layer address of other
nodes

Autoconfiguration of the
address of nodes

DNS Configuration

How does it work?

I can haz sekuritie?

Conclusion

- 3 How does it work?
 - The Derridj part §
 - Link-layer address resolution
 - Address Autoconfiguration

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

- 3 How does it work?
 - The Derridj part §
 - Link-layer address resolution
 - Address Autoconfiguration

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

- Router Solicitation/Router Advertisement (RS, RA)
- Neighbor Solicitation/Neighbor Advertisement (NS, NA)
- Route Redirection

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

- Router Solicitation/Router Advertisement (RS, RA)
- Neighbor Solicitation/Neighbor Advertisement (NS, NA)
- Route Redirection

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

- Router Solicitation/Router Advertisement (RS, RA)
- Neighbor Solicitation/Neighbor Advertisement (NS, NA)
- Route Redirection

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

- 3 How does it work?
 - The Derridj part §
 - **Link-layer address resolution**
 - Address Autoconfiguration

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

- Operation is quite similar to ARP
- A requests the MAC-address of B
→ Send a Neighbor Solicitation
- If B is available, it answers to A
→ Send back a Neighbor Advertisement

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

- Operation is quite similar to ARP
- A requests the MAC-address of B
→ Send a Neighbor Solicitation
- If B is available, it answers to A
→ Send back a Neighbor Advertisement

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

- Operation is quite similar to ARP
- A requests the MAC-address of B
→ Send a Neighbor Solicitation
- If B is available, it answers to A
→ Send back a Neighbor Advertisement

- 3 How does it work?
 - The Derridj part §
 - Link-layer address resolution
 - Address Autoconfiguration

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stéphane
Sezer

- On a regular basis or in response to a Router Solicitation, routers send Router Advertisements
- These RAs can contain: network's prefix (/64), default route, DNS servers, . . .
- A new host receive a RA, combine its information and EUI64 to create its own address and to configure itself
- The host then checks with a Neighbor Solicitation if the address was free

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

- On a regular basis or in response to a Router Solicitation, routers send Router Advertisements
- These RAs can contain: network's prefix (/64), default route, DNS servers, . . .
- A new host receive a RA, combine its information and EUI64 to create its own address and to configure itself
- The host then checks with a Neighbor Solicitation if the address was free

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

- On a regular basis or in response to a Router Solicitation, routers send Router Advertisements
- These RAs can contain: network's prefix (/64), default route, DNS servers, . . .
- A new host receive a RA, combine its information and EUI64 to create its own address and to configure itself
- The host then checks with a Neighbor Solicitation if the address was free

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stéphane
Sezer

- On a regular basis or in response to a Router Solicitation, routers send Router Advertisements
- These RAs can contain: network's prefix (/64), default route, DNS servers, . . .
- A new host receive a RA, combine its information and EUI64 to create its own address and to configure itself
- The host then checks with a Neighbor Solicitation if the address was free

IPv6?

What is the use of
NDP?

How does it work?

The Derridj part §

Link-layer address
resolution

Address Autoconfiguration

I can haz sekuritie?

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

- 4 I can haz sekuritie?
 - IPsec and SEND
 - RA guard
 - Weaknesses in implementations

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

- 4 I can haz sekuritie?
 - IPsec and SEND
 - RA guard
 - Weaknesses in implementations

- Complex to setup (not only with NDP)

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

- Non trivial to deploy
- Does not use IPsec

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

- Non trivial to deploy
- Does not use IPsec

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

- 4 I can haz sekuritie?
 - IPsec and SEND
 - **RA guard**
 - Weaknesses in implementations

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

- Implemented on some switches
- Blocks RA packets coming from unauthorized hosts
- Similar to some existing techniques to prevent ARP spoofing
- Can work in both stateless and stateful modes
- Eventually vulnerable to some kind of attacks

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

- Implemented on some switches
- Blocks RA packets coming from unauthorized hosts
- Similar to some existing techniques to prevent ARP spoofing
- Can work in both stateless and stateful modes
- Eventually vulnerable to some kind of attacks

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

- Implemented on some switches
- Blocks RA packets coming from unauthorized hosts
- Similar to some existing techniques to prevent ARP spoofing
- Can work in both stateless and stateful modes
- Eventually vulnerable to some kind of attacks

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

- Implemented on some switches
- Blocks RA packets coming from unauthorized hosts
- Similar to some existing techniques to prevent ARP spoofing
- Can work in both stateless and stateful modes
- Eventually vulnerable to some kind of attacks

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

- Implemented on some switches
- Blocks RA packets coming from unauthorized hosts
- Similar to some existing techniques to prevent ARP spoofing
- Can work in both stateless and stateful modes
- Eventually vulnerable to some kind of attacks

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

**Weaknesses in
implementations**

Conclusion

- 4 I can haz sekuritie?
 - IPsec and SEND
 - RA guard
 - **Weaknesses in implementations**

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

- “A local network is considered safe”
- Sometimes, you don't have the choice
- thc-ipv6 provides a nice set of tools

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

- “A local network is considered safe”
- Sometimes, you don't have the choice
- `thc-ipv6` provides a nice set of tools

Neighbor
Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

IPsec and SEND

RA guard

Weaknesses in
implementations

Conclusion

- “A local network is considered safe”
- Sometimes, you don't have the choice
- thc-ipv6 provides a nice set of tools

Questions?

Neighbor Discovery Protocol

Pierre-Marie de
Rodat, Stephane
Sezer

IPv6?

What is the use of
NDP?

How does it work?

I can haz sekuritie?

Conclusion

```
42sh$ gcc questions.c
gcc: No route to host.
42sh$ _
```