Neighbor Discovery Protocol

Pierre-Marie de Rodat    Stephane Sezer

July 8, 2011
Plan

1. IPv6?
   - Addresses
   - Multicast
   - ICMP
   - EUI64

Neighbor Discovery Protocol

Pierre-Marie de Rodat, Stephane Sezer

IPv6?
- Addresses
- Multicast
- ICMP
- EU164

What is the use of NDP?
How does it work?
I can haz seuritie?
Conclusion
Plan

1 IPv6?
   • Addresses
   • Multicast
   • ICMP
   • EUI64

What is the use of NDP?
How does it work?
I can haz securitie?
Conclusion
Address format

128 bits

Network Prefix | Interface ID

XXXX | XXXX | XXXX | XXXX | XXXX | XXXX | XXXX | XXXX | XXXX

XXXX = 0000 through FFFF

$3.4 \times 10^{38} = -340,282,366,920,938,463,744,607,432,768,211,456$ IPv6 Addresses
Address scoping

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

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...

```
Layer-2 segment
fe80::dead:beef%em0
fe80::dead:beef%em1

Layer-2 segment
```

```
fe80::00c0:ffee%eth0
2001:db80::00c0:ffee
```
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, Stephane Sezer

IPv6? Addresses Multicast ICMP EUI64

What is the use of NDP?

How does it work?

I can haz securitie?

Conclusion
What is multicast?

- Reach a group of machines
- No broadcast in IPv6
What is multicast?

- Reach a group of machines
- No broadcast in IPv6
Multic和平 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

![Diagram showing multicast addresses on a local link]

- **ff02::1** All nodes on the local network segment 
- **ff02::2** All routers on the local network segment
Plan

1. IPv6?
   - Addresses
   - Multicast
   - ICMP
   - EUI64

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
What is it used for?

- **ICMPv6 is an integral part of IPv6**
- Used for error reporting, diagnostics, etc.
- NDP fits here
What is it used for?

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

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

**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 säkuritje?

Conclusion

**DOUBLE FACEPALM**

When the Fail is so strong, one Facepalm is not enough.
Plan

1. IPv6?
   - Addresses
   - Multicast
   - ICMP
   - EUI64

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

IPv6?
Addresses
Multicast
ICMP
EUI64

What is the use of NDP?
How does it work?
I can haz sekuritie?

Conclusion

Suffix construction from MAC address
Plan

2. What is the use of NDP?
   - Determination of the link-layer address of other nodes
   - Autoconfiguration of the address of nodes
   - DNS Configuration
Plan

2. What is the use of NDP?
   - Determination of the link-layer address of other nodes
   - Autoconfiguration of the address of nodes
   - DNS Configuration
Layer 3 to layer 2

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

Hey guys, who has <IP>?

Layer-2 segment

Ya, it’s me!
Layer 3 to layer 2

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

```
Hey guys, who has <IP>?
Ya, it’s me!
```

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
What is the use of NDP?

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

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

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

![Diagram of network with autoconfiguration process]

Hello, where am I?
Who's the gateway?
You're in 2001:dead:beef::/64,
You're in 2001:c0ff:ee00::/64,
Pass by 2001:c0ff:ee00::42.
Autoconfiguration

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

1. Hello, where am I? Who's the gateway?
3. You're in 2001:c0ff:ee00::/64, Pass by 2001:c0ff:ee00::42.
Autoconfiguration

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

Hello, where am I? Who's the gateway?

You're in 2001:c0ff:ee00::/64, Pass by 2001:c0ff:ee00::42.

Layer-2 segment
2 What is the use of NDP?
- Determination of the link-layer address of other nodes
- Autoconfiguration of the address of nodes
- DNS Configuration
A host also needs a list of recursive DNS servers to query,
and a search list.

RFC 6106
A host also needs a list of recursive DNS servers to query,

and a search list.

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

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

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

IPv6?
What is the use of NDP?
How does it work?
The Derridj part §
Link-layer address resolution
Address Autoconfiguration
I can haz securitie?
Conclusion
Message types

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

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

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

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

- 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
Link-layer address resolution

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

- 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.
Plan

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

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

- Complex to setup (not only with NDP)
SEND

- Non trivial to deploy
- Does not use IPsec
- Non trivial to deploy
- Does not use IPsec
Plan

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

- 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
RA guard

- 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
RA guard

- 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
RA guard

- 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
RA guard

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

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

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

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

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