Introduction to IPv6 Protocol
part 2

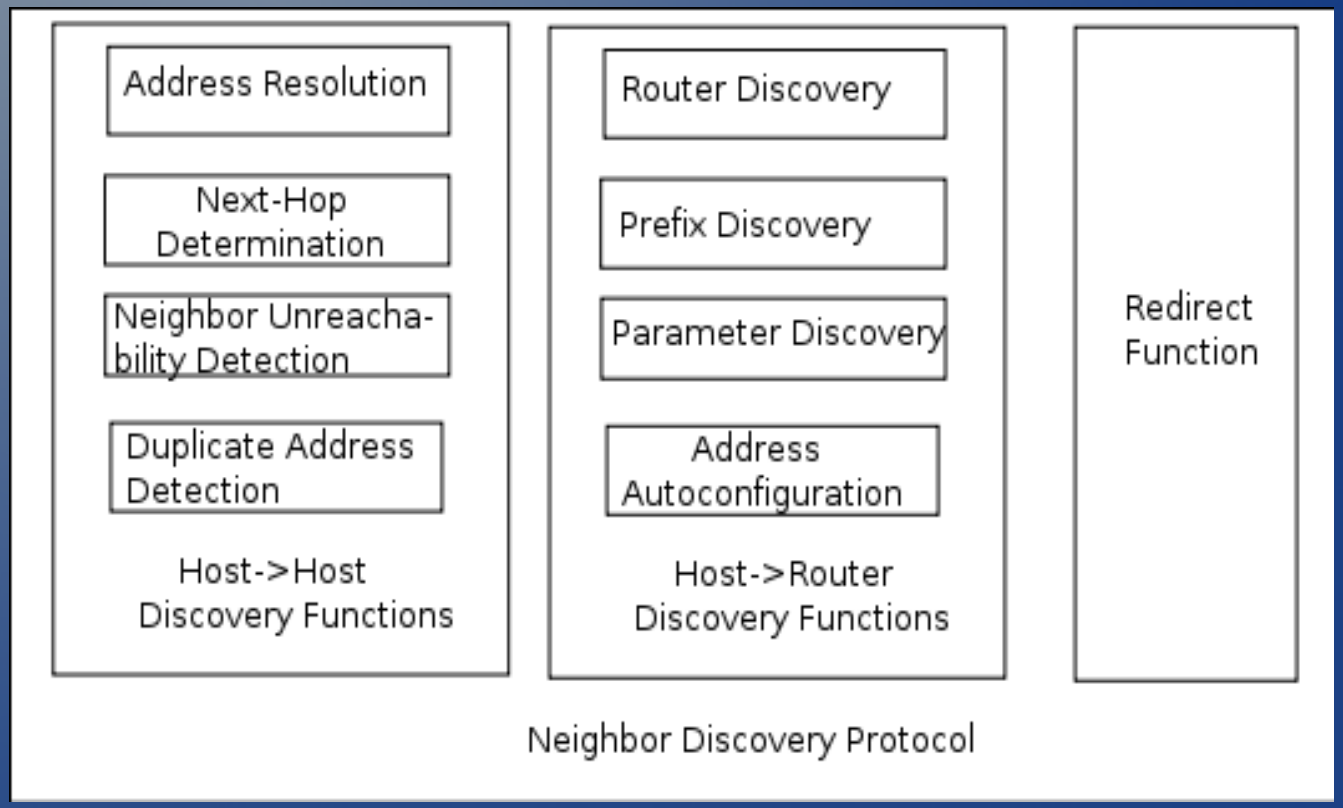
George Kargiotakis (kargig@void.gr)
oss-unipi: Event #27

Topics

- IPv6 Neighbor Discovery Mechanisms
- IPv6 Local Network Protection
- IPv6 Security Considerations
- IPv6 Linux

IPv6 ND (1/X)

- Neighbors = 2 devices on the same local network
- Based on ICMPv6 → Replaces ARP + ICMP on IPv4



IPv6 ND Host-to-Host (1/X)

- **Next-Hop Determination**: The method for looking at an IP datagram's destination address and determining where it should next be sent (Destination Cache).
- **Address Resolution**: The process by which a device determines the layer two address of another device on the local network from that device's layer three (IP) address. Replaces ARP in IPv4 (Neighbor Cache).
- **Neighbor Unreachability Detection**: The process of determining whether or not a neighbor device can be directly contacted.
- **Duplicate Address Detection**: Determining if an address that a device wishes to use already exists on the network.

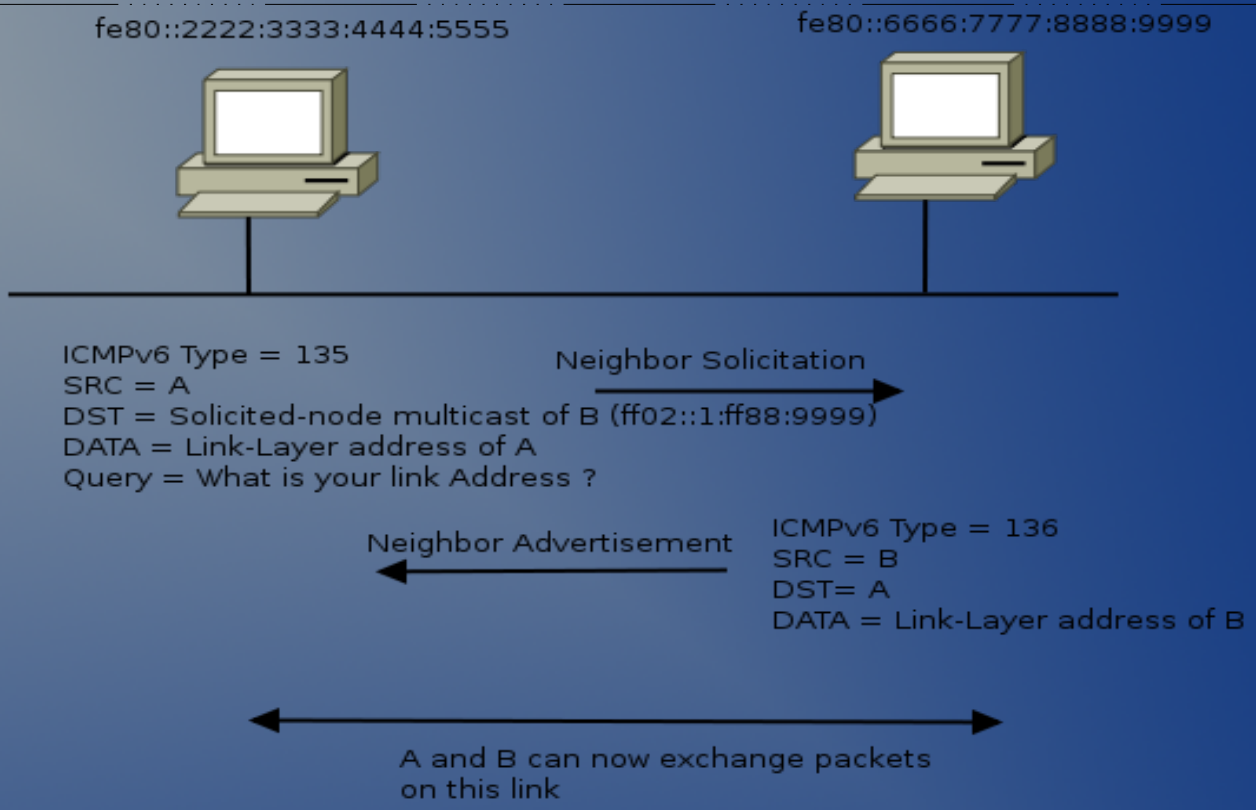
IPv6 Host-to-Router (1/X)

- **Router Discovery**: The method by which hosts locate routers on their local network.
- **Prefix Discovery**: Hosts use this function to determine what network they are on, which in turn tells them how to differentiate between local and distant destinations and whether to attempt direct or indirect delivery of datagrams (Prefix Cache).
- **Parameter Discovery**: The method by which a host learns important parameters about the local network and/or routers, such as the maximum transmission unit of the local link.
- **Address Autoconfiguration**: Hosts can automatically configure themselves, by information provided by a router.

IPv6 ND Messages (3/X)

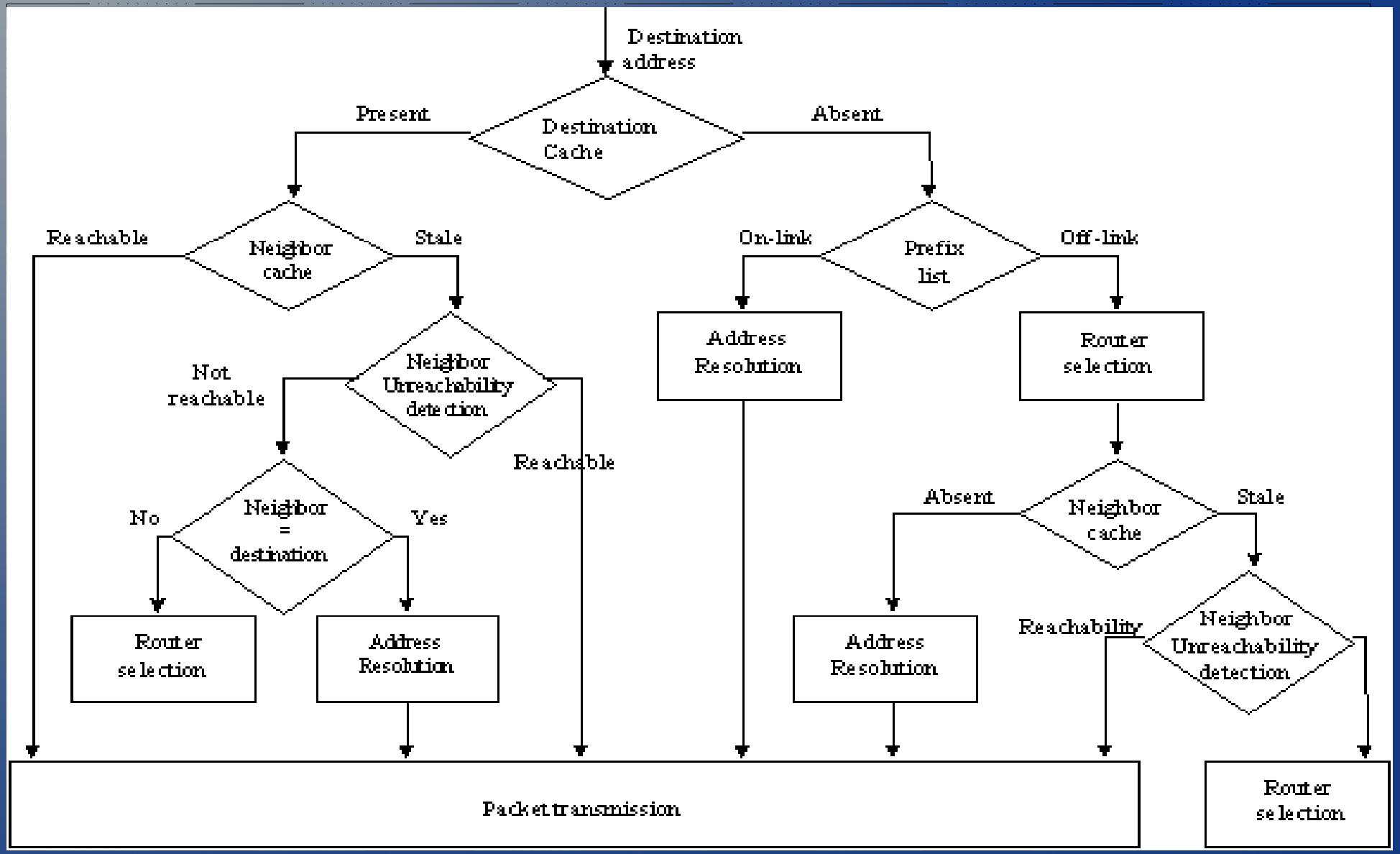
- Commonly used messages:
  - Router Advertisement (Type 134)
  - Router Solicitation (Type 133)
  - Neighbor Advertisement (Type 136)
  - Neighbor Solicitation (Type 135)
  - Redirect
- Benefits:
  - Formalize Address Resolution + Router Discovery (Security at layer 3 independent of IPsec → SeND)
  - Autoconfiguration
  - Dynamic Router Selection
  - Multicast

IPv6 ND Address Resolution (4/X)



- Efficiency due to using Solicited-node Multicast Addresses instead of broadcast
- Address Resolution only for “on-link” nodes

IPv6 ND Flow (4/X)



IPv6 Local Network Protection

GOAL	IPv4	IPv6
Simple Gateway between Internet and Private Network	DHCP	DHCPv6-PD + SLAAC
Simple Security	Filtering side-effect due to lack of translation state	ACL/Firewall
Local Usage Tracking	NAT State Table	Address uniqueness
End-System Privacy	NAT transforms device ID bit in the address	Privacy Extensions
Topology Hiding	NAT transforms subnet bits in the address	Untraceable addresses (IGP host routes/MIPv6 Tunnels)
Addressing Autonomy	Private Address Space	Large Address Space + ULA
Global Address Pool Reservation	Private Address Space	**WHAT ?**
Renumbering/Multihoming	Address translation at border	Lifetime per prefix / Multiple addresses per interface

IPv6 Common Attacks

- Address Resolution
  - Attacker claims victim's IP address
- Redirect
  - Attacker sends RA and redirects traffic heading to an off-link host elsewhere
- DAD (DoS)
  - Attacker replies to any victim's DAD requests

IPv6 Common Attacks

- First-Hop Router Attack
  - Attacker tricks victim into accepting itself as a default router canceling the previous one (lifetime=0). Steals all traffic.
- Address Configuration (DoS)
  - Attacker cancels previous default router prefix and sends new prefix to victim. Victim can't access the network due to spoofed prefix filtering by default router.
- DHCPv6 spoofing

IPv6 Migration Security

- Deny packets for transition techniques not in use
  - Deny IPv4 protocol 41 forwarding unless that is exactly what is intended – unless using 6to4 tunneling
  - Deny UDP 3544 forwarding unless you are using Teredo tunneling
- Avoid Dynamic Tunnels (6to4, Teredo, etc)
- Don't forget Link-Local addresses! (demo?)

IPv6 Security Overview

- IPv6 is no more or less secure than Ipv4
  - Experience is the issue
- IPv6 will change traffic patterns (p2p, MIPv6)
- IPv6 larger addresses makes worms and scanning less effective but there are still ways to find hosts
- Apply IPsec wherever possible
- LAN based attacks → Stronger physical security, Ethernet-port Security, NAC, 802.1X, SeND

IPv6 Linux

- Show IPv6 neighbors
  - ip -6 neighbor show
- Show IPv6 addresses
  - ip -6 address
- Show IPv6 routes
  - ip -6 route

IPv6 Linux

- Add neighbor
  - ip neighbor add 2001:db8::2 dev eth0 lladdr 00:11:22:33:44:55
- Add address
  - ip address add 2001:db8::1/64 dev eth0
- Add route
  - ip route add 2001:db8::10:1/64 dev eth0

IPv6 Linux

- Show destination cache
  - ip route show cache
- Show multicast listening addresses
  - ip maddr
- Log routing changes
  - rtmon file /tmp/rtmon.log
  - ip monitor file /tmp/rtmon.log

IPv6 Linux

- /proc/
  - /proc/net/snmp6
  - /proc/sys/net/ipv6/bindv6only
  - /proc/sys/net/ipv6/conf/[all,default,devX]/YYYY
    - accept_ra
    - autoconf
    - forwarding (0,1,2)
    - accept_redirects
    - disable_ipv6 (newer kernels)
    - router_solicitations
    - mtu
    - use_tempaddr (0,1,2)

IPv6 Linux

- Apache configuration
  - Listen 80
  - Listen [2001:db8::1]:80
  - NameVirtualHost [2001:db8::1]:80
  - <VirtualHost [2001:db8::1]:80>
- vsftpd
  - listen_ipv6=YES
  - sysctl -w net.ipv6.bindv6only=0 (don't forget!)
- Postfix
  - inet_protocols = ipv4, ipv6

The End

Thanks!

Any Questions ?