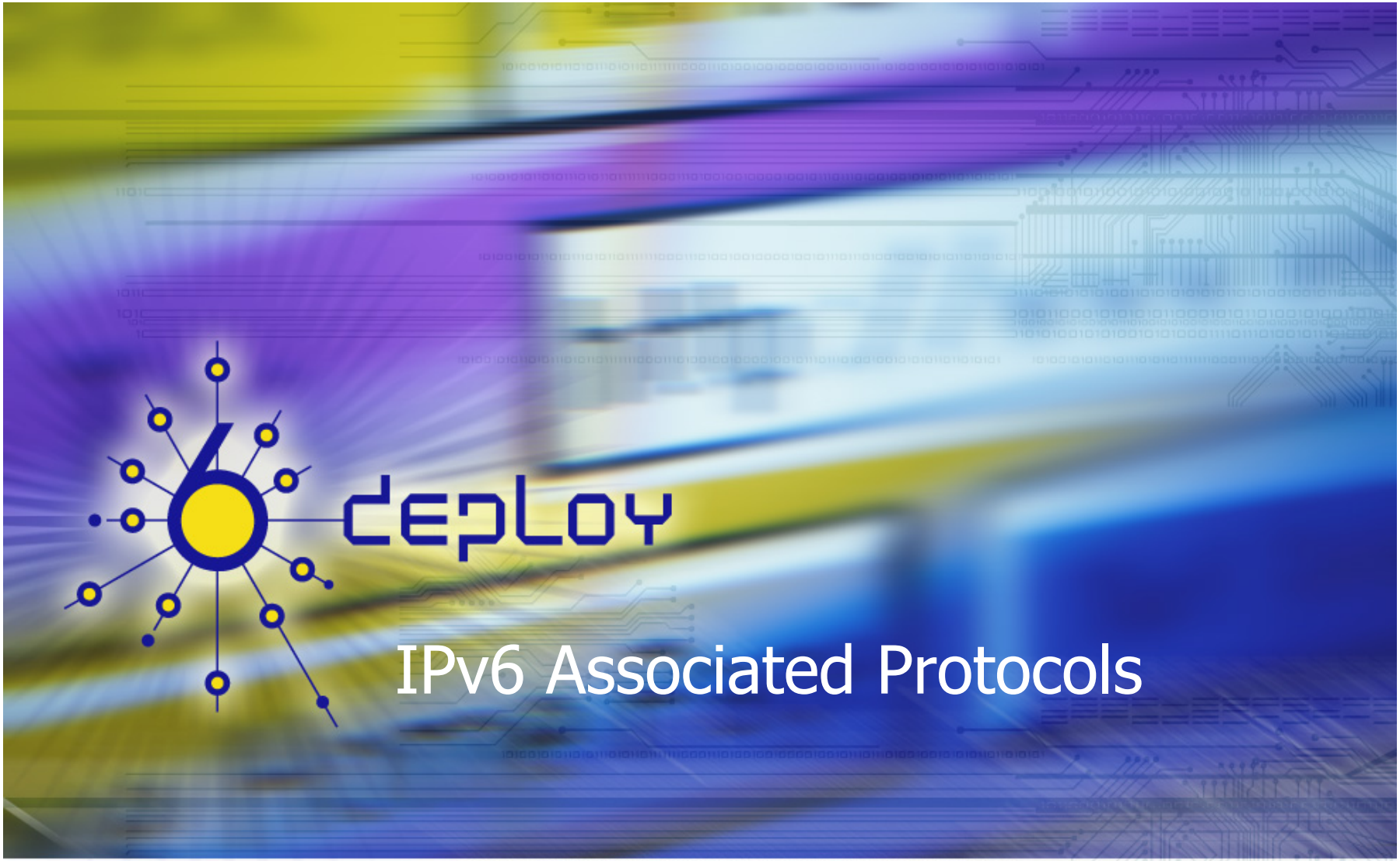


IPv6 Associated Protocols

Athanassios Liakopoulos (aliako@grnet.gr)

6DEPLOY IPv6 Training, Skopje, June 2011

Copy ... Rights

- This slide set is the ownership of the 6DEPLOY project via its partners
- The Powerpoint version of this material may be reused and modified only with written authorization
- Using part of this material must mention 6Deploy courtesy
- PDF files are available from www.6deploy.org
- Looking for a contact ?
- Mail to : martin.potts@martel-consulting.ch

Associated Protocols

Neighbor Discovery for IPv6 (1)

- IPv6 nodes (hosts and routers) on the same physical medium (link) use Neighbor Discovery (NDP) to:
  - discover their mutual presence
  - determine link-layer addresses of their neighbors
  - find neighboring routers that are willing to forward packets on their behalf
  - maintain neighbors' reachability information (NUD)
  - not directly applicable to NBMA (Non Broadcast Multi Access) networks)
    - ➔ NDP uses link-layer multicast for some of its services.

Neighbor Discovery for IPv6(2)

- Protocol features:
  - Router Discovery
  - Prefix(es) Discovery
  - Parameters Discovery, e.g. link MTU, Max Hop Limit, etc
  - Address Autoconfiguration
  - Address Resolution
  - Next Hop Determination
  - Neighbor Unreachability Detection
  - Duplicate Address Detection
  - Redirect
  - *DNS servers*

NDP: Comparison with IPv4

- The IPv6 Neighbor Discovery protocol corresponds to a combination of the IPv4 protocols:
  - Address Resolution Protocol (ARP)
  - ICMP Router Discovery (RDISC)
  - ICMP Redirect (ICMPv4)
- Improvements over the IPv4 set of protocols:
  - Router Discovery is part of the base protocol set
  - Router Advertisements carry link-layer addresses and prefixes for a link, and enable address autoconfiguration
  - Multiple prefixes can be associated with the same link.
  - Neighbor Unreachability Detection is part of the base protocol set
  - Detects half-link failures and avoids sending traffic to neighbors with which two-way connectivity is absent
  - By setting the Hop Limit to 255, Neighbor Discovery is immune to off-link senders that accidentally or intentionally send ND messages.

NDP Messages (1)

- NDP specifies 5 types of ICMP packets :
  - **Router Advertisement** (RA) :
    - periodic advertisement or response to RS message (of the availability of a router) which contains:
      - list of prefixes used on the link (autoconf)
      - address configuration
      - a possible value for Max Hop Limit (TTL of IPv4)
      - value of MTU
  - **Router Solicitation** (RS) :
    - the host needs RA immediately (at boot time)

NDP Messages (2)

- **Neighbor Solicitation** (NS):
  - to determine the link-layer @ of a neighbor
  - or to check a neighbor is still reachable via a cached L2 @
  - also used to detect duplicate addresses (DAD)

- **Neighbor Advertisement** (NA):
  - answer to a NS message
  - to advertise the change of physical address

- **Redirect** :
  - Used by routers to inform hosts of a better first hop for a destination

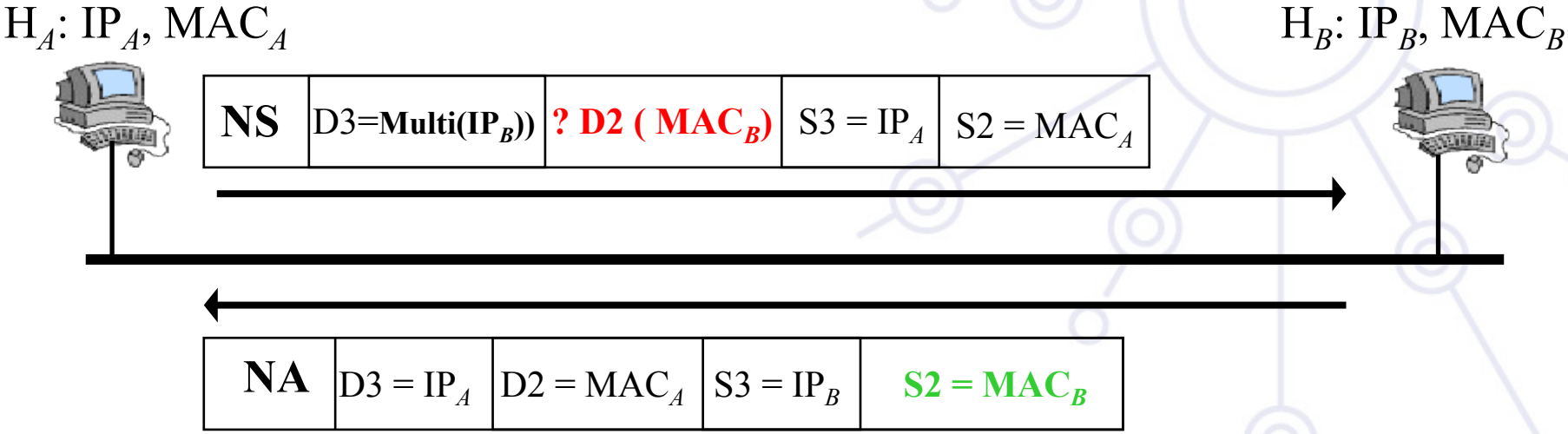
Address resolution

- Address resolution is the process through which a node determines the link-layer address of a neighbor given only its IP address.
- Find the mapping:
- Dst IP @ ➔ Link-Layer (MAC) @
- Recalling IPv4 & ARP
  - ARP Request is broadcasted
    - Request is sent to `ethernet address:`
      `FF-FF-FF-FF-FF-FF`
    - Request contains the src's link local address
  - ARP Reply is sent in unicast to the source
    - Reply contains the destination's link local address

Address resolution with NDP

At boot time, every IPv6 node has to join 2 special multicast groups for each network interface:

- All-nodes multicast group: `ff02::1`
- Solicited-node multicast group: `ff02::1:ffxx:xxxx`
  - derived from the lower 24 bits of the node's address



Address resolution (3) : multicast solicited address

- Concatenation of the prefix FF02::1:FF00:0/104 with the last 24 bits of the IPv6 address

Example:

- Dst IPv6 @: 2001:0660:010a:4002:4421:21FF:FE24:87c1
- Sol. Mcast @: FF02:0000:0000:0000:0000:0001:FF24:87c1
- Ethernet: 33-33-FF-24-87-c1

Associated Protocols

Path MTU discovery (RFC 1981)

- Derived from RFC1191 (IPv4 version of the protocol)
  - Path = set of links followed by an IPv6 packet between source and destination
- Link MTU = maximum packet length (bytes) that can be transmitted on a given link without fragmentation
- Path MTU (or pMTU) = min { link MTUs } for a given path
- Path MTU Discovery = automatic pMTU discovery for a given path

Path MTU discovery (2)

- Protocol operation
  - makes assumption that pMTU = link MTU to reach a neighbor (first hop)
  - if there is an intermediate router such that
    - link MTU < pMTU

    ➔ it sends an ICMPv6 message: "Packet size Too Large"
  - source reduces pMTU by using information found in the ICMPv6 message
  - …

=> Intermediate network element aren't allowed to perform packet fragmentation

Associated Protocols

Stateless Autoconfiguration

- Host should be plug & play
- Uses some of the Neighbor Discovery ICMPv6 messages
- When booting, the host asks for network parameters:
  - IPv6 prefix(es)
  - default router address(es)
  - hop limit
  - (link local) MTU

Stateless Autoconfiguration

- Only routers have to be manually configured
  - And/or can use the *Prefix Delegation* option
  - RFC 3633
- Hosts can get automatically an IPv6 address
  - BUT it isn't automatically registered in the DNS

➢ Servers should be manually configured

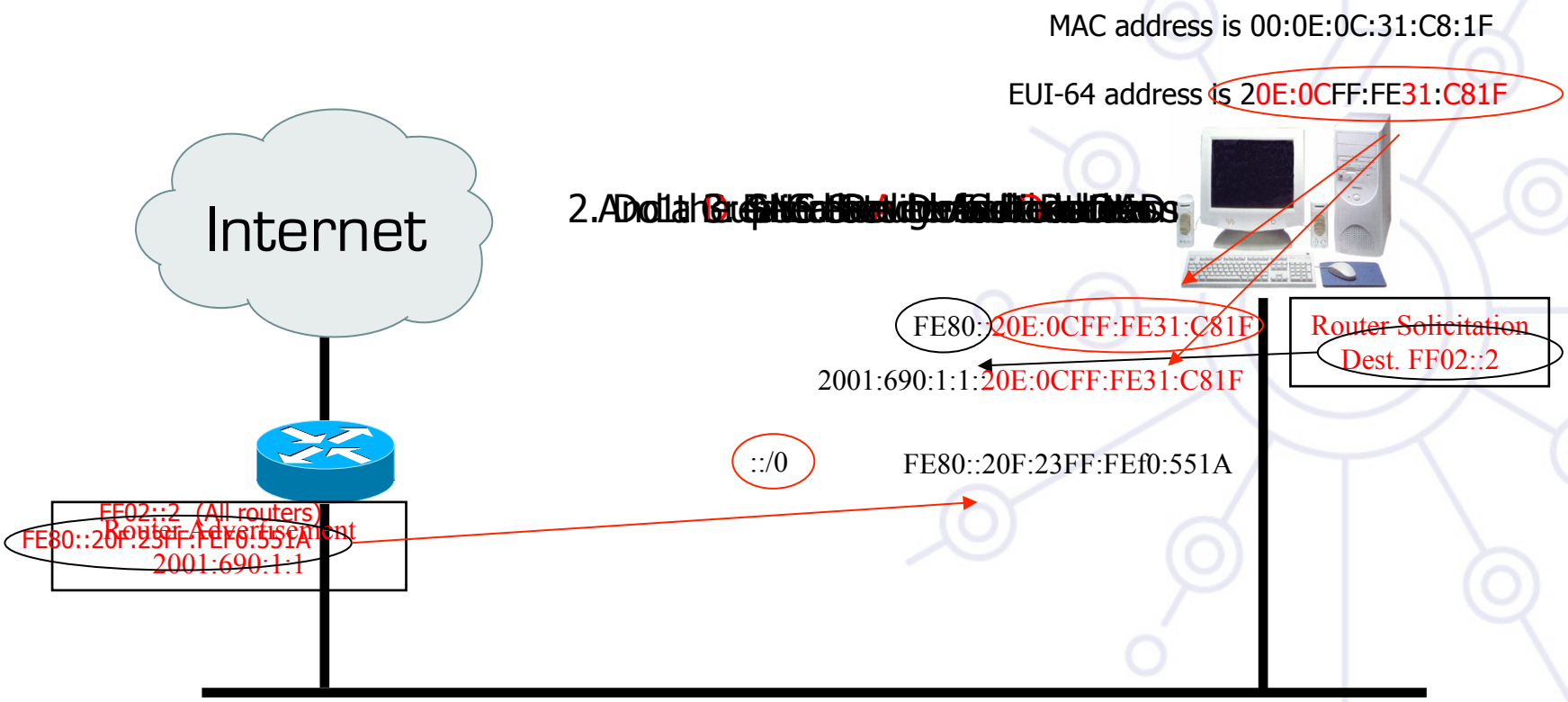
Stateless Autoconfiguration

- IPv6 Stateless Address Autoconfiguration is described in RFC 2462
- Hosts are listening for Router Advertisements (RA) messages, periodically sent out by routers on the local link
- RA messages coming from the router(s) on the link identify the subnet
- Allows a host to create a global unicast IPv6 address from:
  - Its interface identifier (EUI-64 address)
  - Link Prefix (obtained via Router Advertisement)
- Global Address = *Link Prefix* + *EUI-64 address*

Stateless Autoconfiguration

- Usually, the router sending the RA messages is used, by hosts, as the default router
- If the RA doesn't carry any prefix
  - The hosts don't configure (automatically) any global IPv6 address (but may configure the default gateway address)
- RA messages contain two flags indicating what type of stateful autoconfiguration (if any) should be performed
- *Now it's possible to automatically send recursive DNS server(s) (RDNSS) address(es) using RA option (RFC6106)*
  - Also in include DNS Search List – DNS suffixes
- IPv6 addresses depends on NIC card

Stateless Autoconfiguration



Statefull Autoconfiguration DHCPv6

- Dynamic Host Configuration Protocol for IPv6
  - RFC 3315
  - stateful counterpart to IPv6 Stateless Address Autoconfiguration.

- According to RFC 3315 DHCPv6 is used when:
  - no router is found
  - Or if Router Advertisement message enables use of DHCP

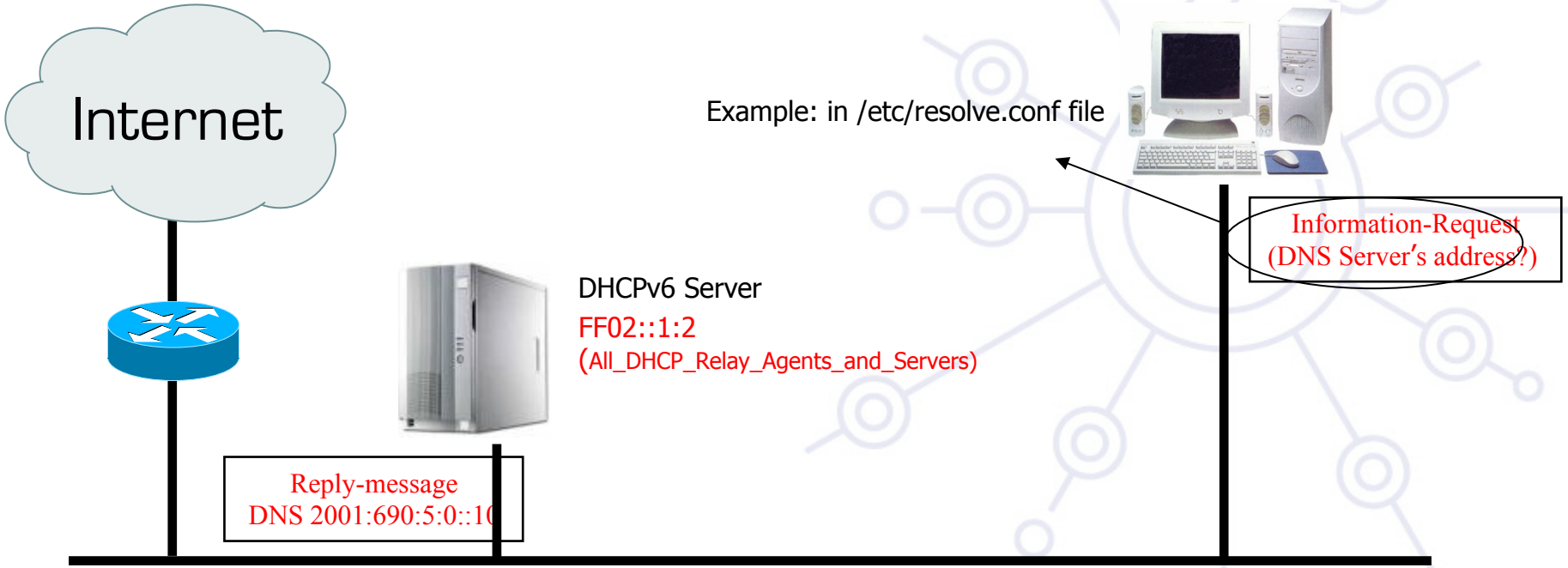
Statefull Autoconfiguration DHCPv6

- DHCPv6 works in a client / server model
  - Server
    - Responds to requests from clients
    - Optionally provides the client with:
      - IPv6 addresses
      - Other configuration parameters (DNS servers…)
    - Is listening on multicast addresses:
      - All_DHCP_Relay_Agents_and_Servers (FF02::1:2)
      - All_DHCP_Servers (FF05::1:3)
    - Memorizes client's state
    - Provides means for securing access control to network resources

Statefull Autoconfiguration DHCPv6 /3

- Client
  - initiates requests on a link to obtain configuration parameters
  - uses its link local address to connect the server
  - Sends requests to FF02::1:2 multicast address (All_DHCP_Relay_Agents_and_Servers)
- Relay agent
  - node that acts as an intermediary to deliver DHCP messages between clients and servers
  - is on the same link as the client
  - Is listening on multicast addresses:
    - All_DHCP_Relay_Agents_and_Servers (FF02::1:2)

Statefull Autoconfiguration DHCPv6



Conclusion

- The two types of configuration complement each other
  - Example: we can obtain the address from stateless autoconfiguration and the DNS server address from DHCPv6
- In dual-stack networks we can obtain DNS server addresses from DHCPv4/6 or RDNSS RA-options
- DHCPv6 clients aren't still available natively in all dperating systems.
  - So, we still need to install manually a client
  - Not transparent to users

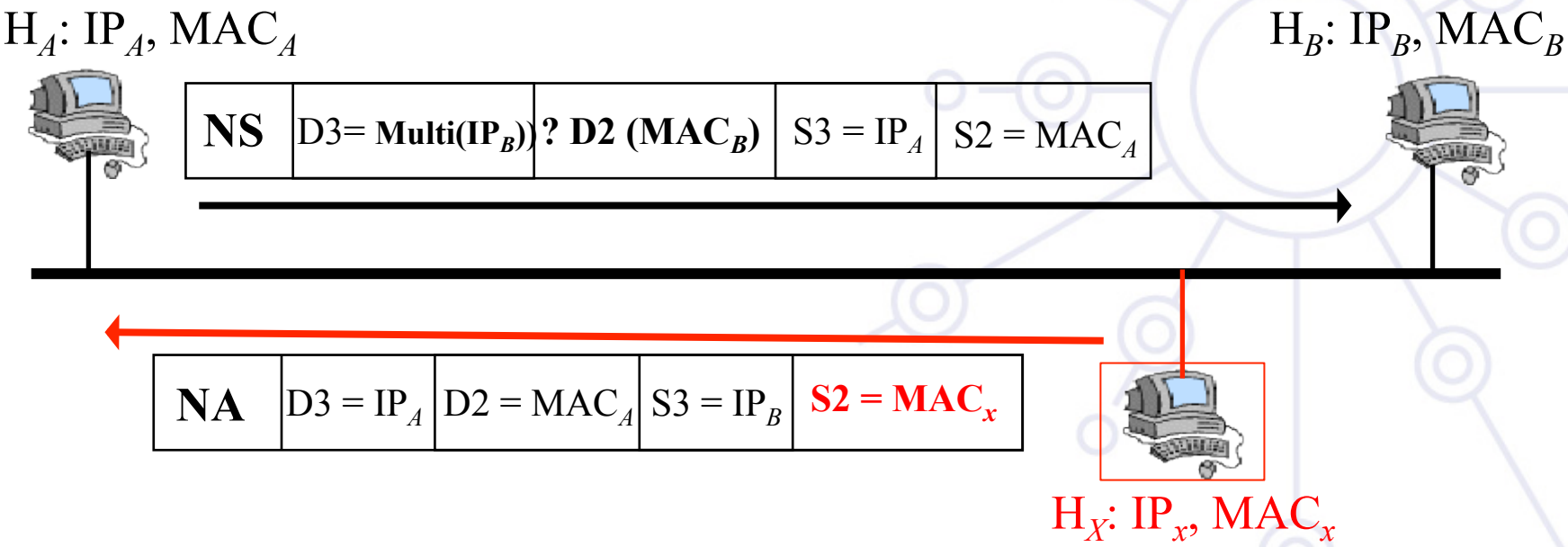

deploy
Questions?

Auto-configuration / Neighbour Discovery

- Neighbour Discovery
  - Suffers similar problems as ARP cache poisoning
- SEcure Neighbor Discovery (SEND) [RFC3971]
  - Applicable in environments where physical security is not assumed, e.g. wireless
  - Based on CGA
    - Linux implementation: DoCoMo's Open Source SEND Project
  - Certify routers with a trust anrchor, verify ownership of addresses, avoid replay attacks, etc
- DHCPv6 with authentication is also possible
- ND with IPsec is also possible

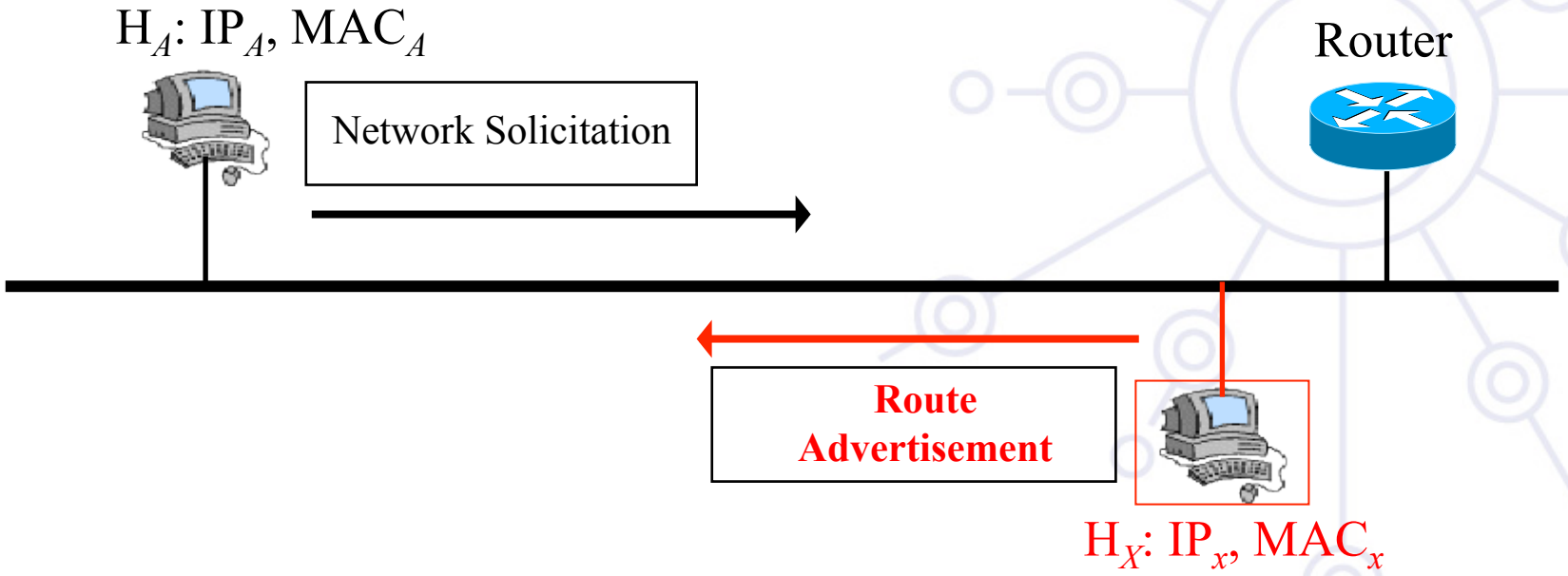
ND Attacks (1/3)

- Attacker sends fake NA messages
  - Attack node claims to be any system in the LAN
  - Sink or divert traffic



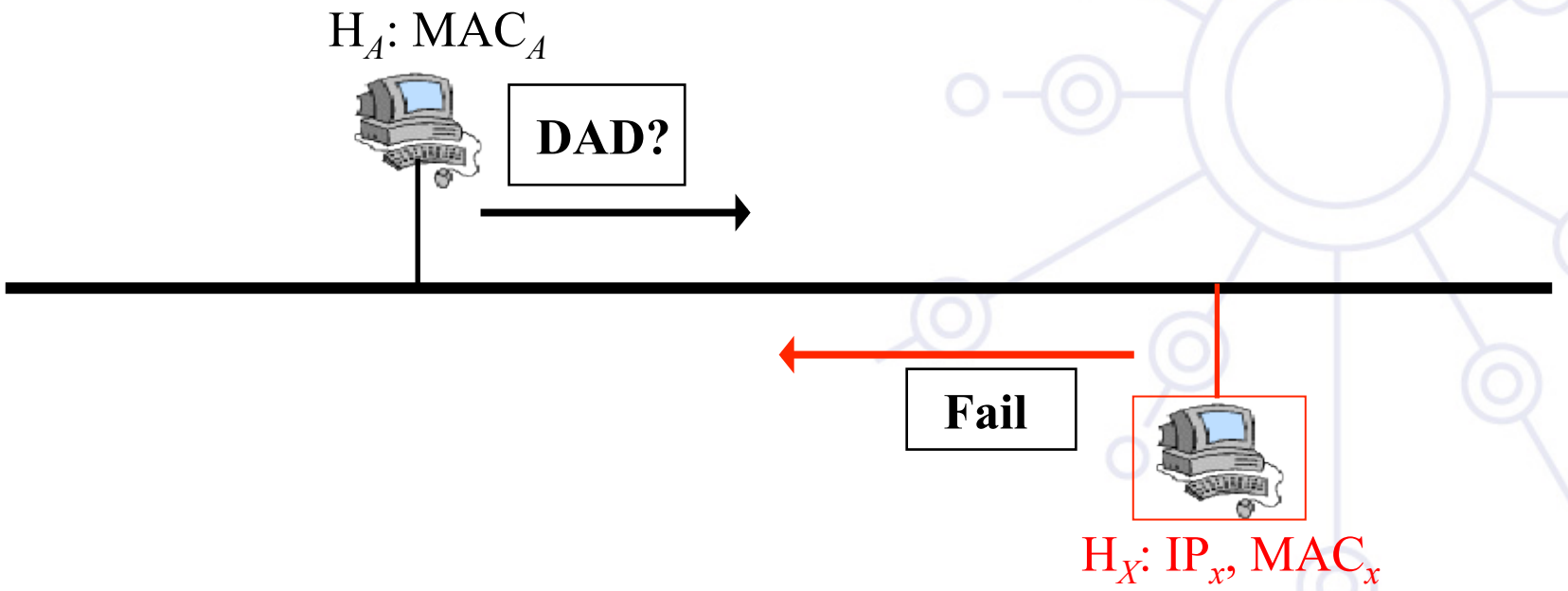
ND Attacks (2/2)

- Attack node sends fake RA
  - Attack node claims to be the router
  - Sink or divert traffic



ND Attacks (3/3)

- Attack node sends fake DAD replies
  - Attack node claims to have any IPv6 address checked via DAD
  - Prevent new nodes to set an IPv6 address



Some food for thought

- DHCPv6 clients aren't still available natively in all operating systems.
  - So, we still need to install manually a client
  - Not transparent to users
- How to populate reverse DNS entries in IPv6 Network?
  - A residential user may get /56 address block!
  - Possible problems with anti-spam filters