IPv6

11th March 2019
at

Information Technology Center

Network Operation Center
(LEARN)

128 bit address space

3FFE:08EB:1F2F:0000:0000:0000:00A9:1432

8 groups of 16-bit hexadecimal numbers separated by ":"

For easy handling, leading zeros can be removed

3FFE:8EB:1F2F::A9:1432

:: = all zeros in one or more group of 16-bit hexadecimal numbers

IPv6 Address Types

Unicast

- Identifies a single node, and traffic destined to a unicast address is forwarded to a single node.

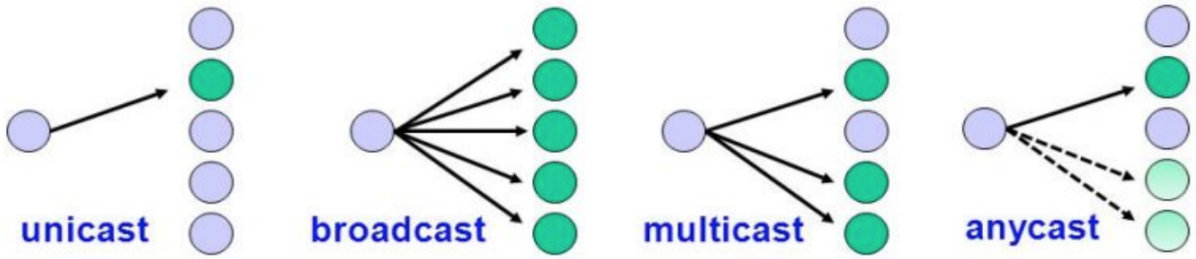
Multicast

- Identifies a group of nodes, and traffic destined to a multicast address is forwarded to all the nodes in the group.

Anycast

- Identifies a group of nodes, and traffic destined to an anycast address is forwarded to the nearest node in the group.

NO Broadcast Address



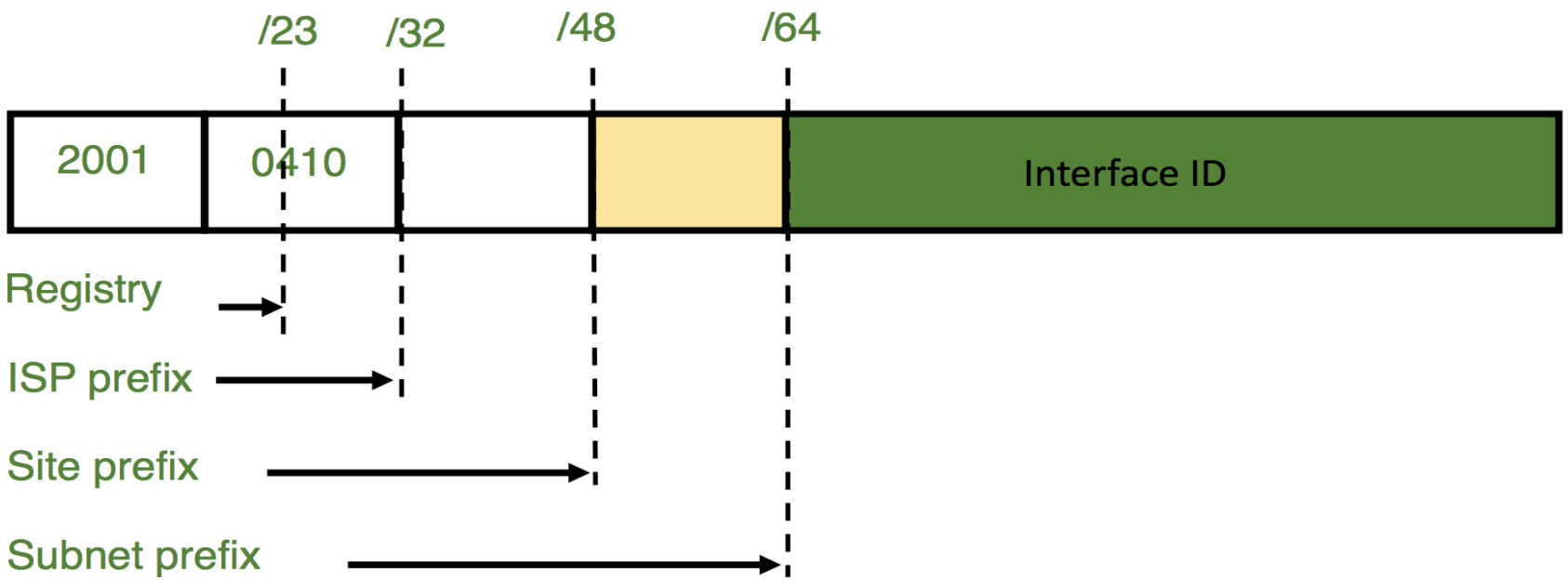
IPv6 Address Types in detail

IPv6 Address Type	Description
Global Unicast	Destined for a single recipient and can be routed on the public Internet
Multicast	Destined for members of a multicast group
Link Local	Valid only on a network segment
Unique Local	Cannot be routed on the public Internet
Loopback	The *localhost* address of a device
Unspecified	Does not specify a source address (all 128 bits in the IPv6 address set to zeros)
Solicited-Node Multicast	A multicast IPv6 address corresponding to a device's IPv6 address(es)

IPv6 Address Types - Values

Address Type	Binary Prefix	IPv6 Notation	IPv6 Address Range
Unspecified	00..0 (128 bits)	::/128	
Loopback	00..1 (128 bits)	::1/128	::1
Multicast	11111111	ff00::/8	ff00 - ffff
Link-local Unicast	1111111010	fe80::/10	fe80 - febf
Site-local Unicast [1)]	1111111011	fec0::/10	fec0 - feff
Unique Local Unicast	1111110	fc00::/7	fc00 - fdff
Global Unicast	(all others)		

IPv6 ISO Address Allocation Format



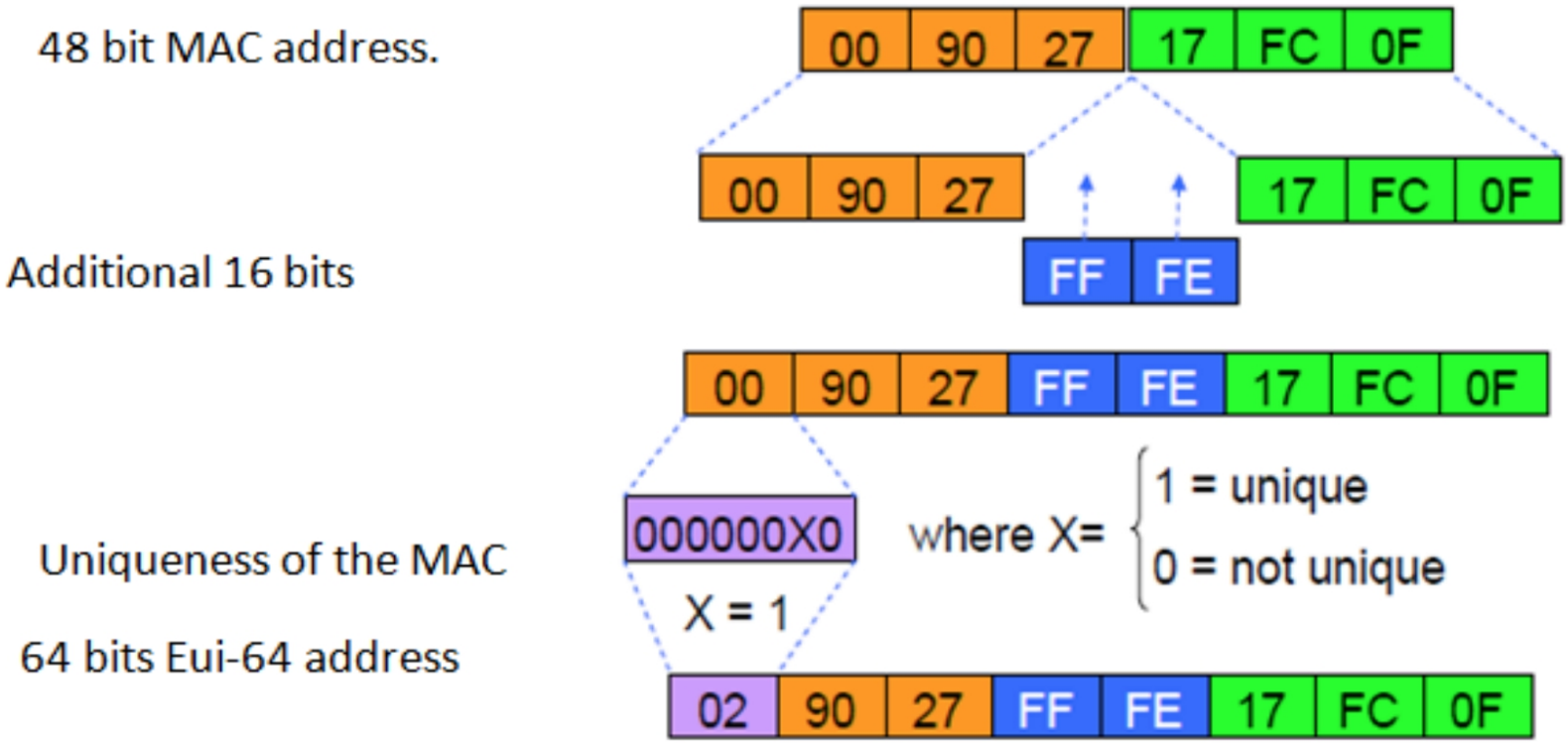
Eg:
LEARN Address Space -- 2401:DD00:0000:0000:0000:0000:0000:0000/32

UoK Address Space -- 2401:DD00:0020:0000:0000:0000:0000:0000/48

Defining Interface ID

- Associate layer 2 address in the Extended Unique Identifier (EUI-64).
  - For the interface ID portion of the network, the seventh high-order bit of the EUI-64 format defines a local scope when set to 0 and a global scope (globally unique) when set to 1.
- Auto-generate a random address as defined in RFC 3041.
  - This mechanism was developed basically to limit the exposure of a globally reachable address and to increase privacy
- via DHCPv6.
- Manual configuration.
- Cryptographically generated addresses (CGAs) based on RFC 3972
  - This is done through a hash that includes a public key. This method of generating an interface ID provides added security and enables address authentication.

Extended Unique Identifier (EUI – 64)



Link-Local Address

- Meaningful only in a single link zone, and may be re-used on other links
- Link-local addresses for use during auto-configuration and when no routers are present
- Required for Neighbor Discovery process, normally automatically configured
- An IPv6 router never forwards link-local traffic beyond the link
- Prefix= FE80::/64

ICMPv6

- An integral part of IPv6 and MUST be fully implement by every Ipv6 node (RFC 2463)
- Report delivery or forwarding errors
- Provide simple echo service for troubleshooting
- Neighbor Discovery (ND): 5 ICMP messages
- Multicast Listener Discovery (MLD): 3 ICMP messages

ICMPv6

Message Number	Message Type	Code Field
128	Echo Request	RFC 4443. Used for the ping command
129	Echo Reply	
130	Multicast Listener Query	RFC 2710. Used for multicast group management
131	Multicast Listener Report	
132	Multicast Listener Done	
133	Router Solicitation	RFC 4861. Used for neighbor discovery and autoconfiguration
134	Router Advertisement	
135	Neighbor Solicitation	
136	Neighbor Advertisement	
137	Redirect Message	
200 and 201	Private Experimentation	RFC 4443
255	Reserved for expansion of ICMPv6 informational messages	RFC 4443

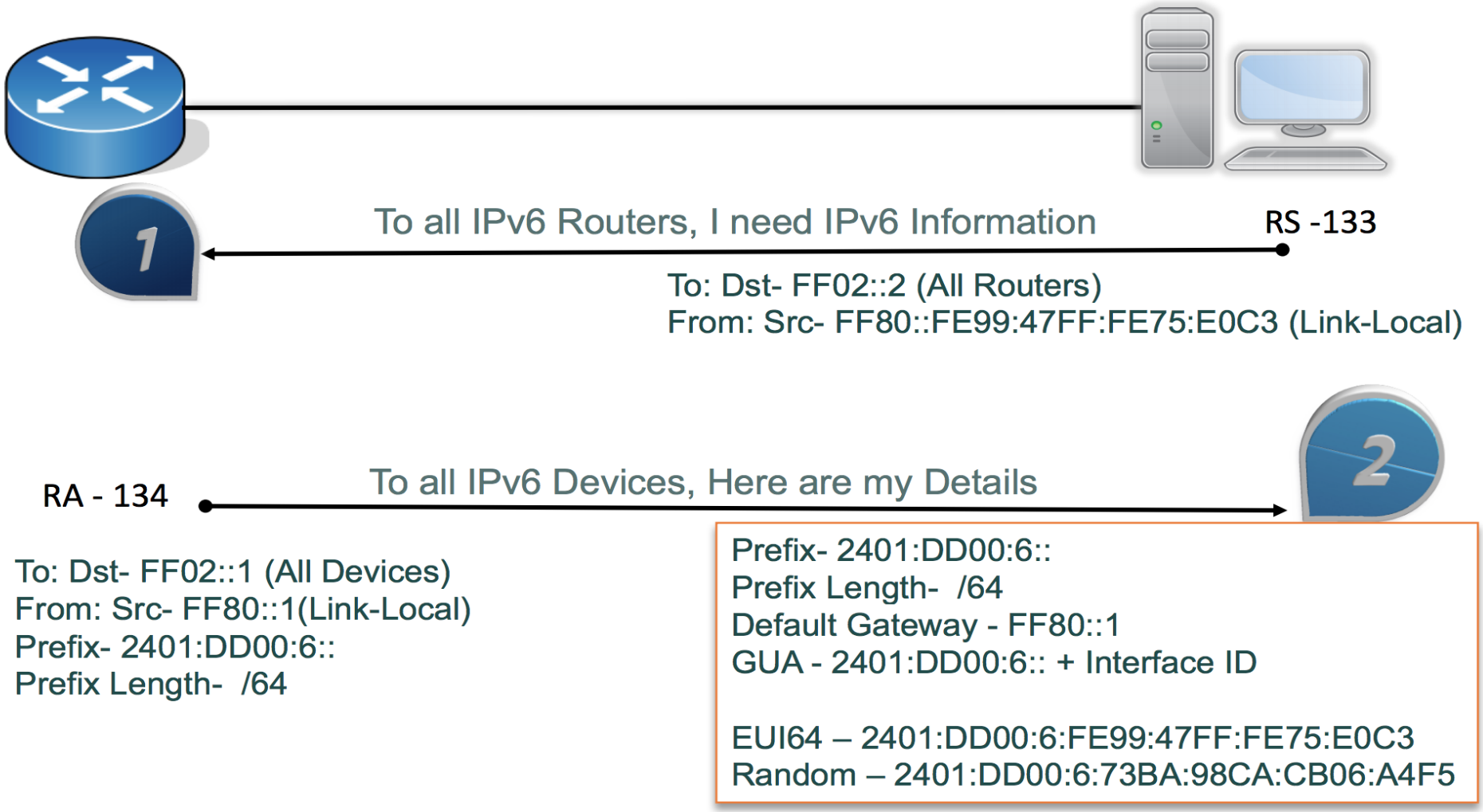
Address Auto-Configuration

- Stateful Auto-Configuration
  - method in which a host or router is assigned its entire 128-bit IPv6 address with the help of DHCP.
- SLAAC – Stateless Address Auto Configuration
  - method in which the host or router interface is assigned a 64-bit prefix, and then the last 64 bits of its address are derived by the host or router with help of EUI-64 process

Sateless Address Auto-Configuration – SLAAC

- No Need of DHCP Server
  - Step1 : A newly connected device will send an ICMPv6 Router Solicitation(133) to the network requesting network prefix from Routers.
  - Step 2: Router will reply with a Router Advertisement(134) containing required details
  - Step 3: New host will generate its Global Unicast Address using prefix sent and the Interface ID generated using EUI-64 or Random.

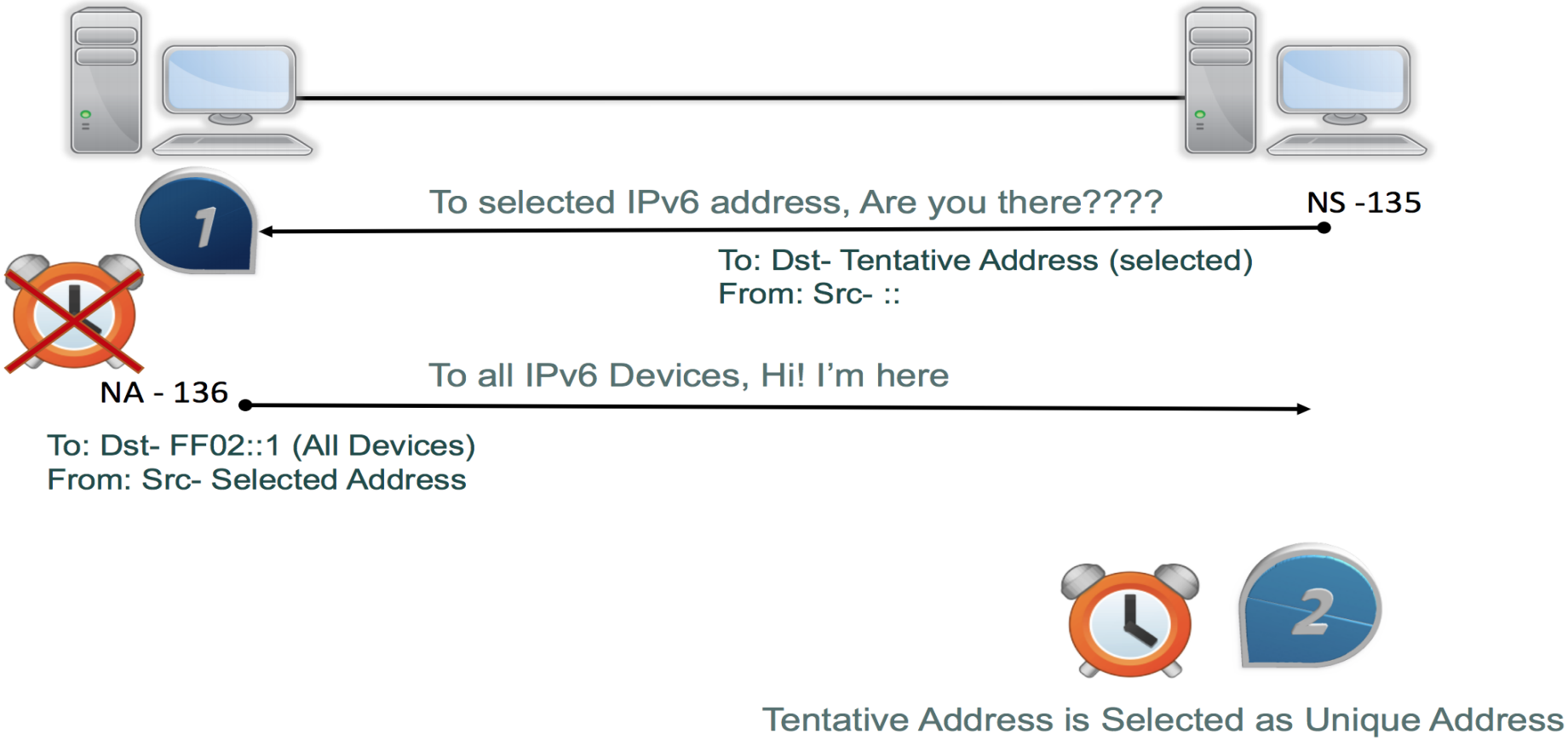
SLAAC


1
To all IPv6 Routers, I need IPv6 Information
RS -133
To: Dst- FF02::2 (All Routers)
From: Src- FF80::FE99:47FF:FE75:E0C3 (Link-Local)
2
RA - 134
To all IPv6 Devices, Here are my Details
To: Dst- FF02::1 (All Devices)
From: Src- FF80::1(Link-Local)
Prefix- 2401:DD00:6::
Prefix Length- /64
Prefix- 2401:DD00:6::
Prefix Length- /64
Default Gateway - FF80::1
GUA - 2401:DD00:6:: + Interface ID
EUI64 – 2401:DD00:6:FE99:47FF:FE75:E0C3
Random – 2401:DD00:6:73BA:98CA:CB06:A4F5

Duplicate Address Detection - DAD

- Since SLACC and Link Local addresses are configured automatically and no inventory like DHCP is recording the usage we need to confirm that the selected address is unique.
  - Step1 : Neighbor Solicitation (NS) is sent to own solicited node Multicast address
  - Step 2: If the new address is already in use, a Neighbor Advertisement is received through the multicast group FF02::1, if the NS gets timed out then the selected address will be marked as unique and it will be selected as the address

Duplicate Address Detection - DAD



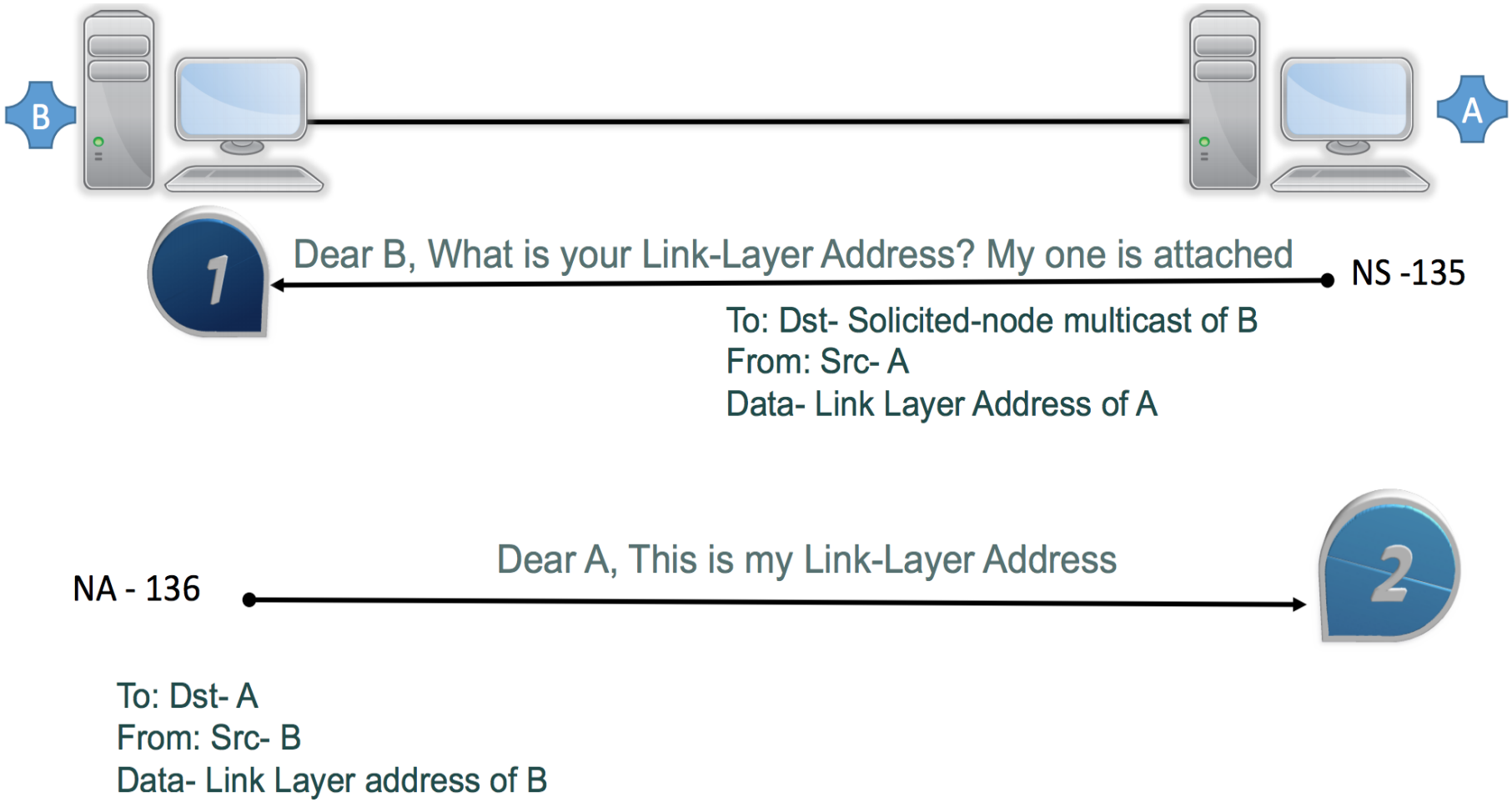
Stateful Auto Configuration – DHCPv6

- Problem with stateless:
  - Anyone can connect
  - Stateless auto-configuration only configures addresses; not “other configuration” information (DNS servers, domain search list, ...)
  - Stateless auto-configuration is “one-size fits all” Addresses can not be selectively assigned
  - Policies can not be enforced about clients allowed addresses
- So routers ask the new system to go DHCP server (by setting managed configuration bit)
- System multicasts to "All DHCP servers"
- DHCP server assigns an address

Neighbor Discovery Protocol - ND

- Node (Hosts and Routers) use ND to determinate the link-layer addresses for neighbors known to reside on attached links and quick purge cached valued that become invalid
- Hosts also use ND to find neighboring router that willing to forward packets on their behalf
- Nodes use the protocol to actively keep track of which neighbors are reachable and which are not, and to detect changed link-layer addresses
- Replace ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4

Neighbor Discovery Protocol - ND



Thank You

Senevi Herath, Network/Systems Manager, LEARN

Email: senevih@learn.ac.lk
noc@learn.ac.lk