

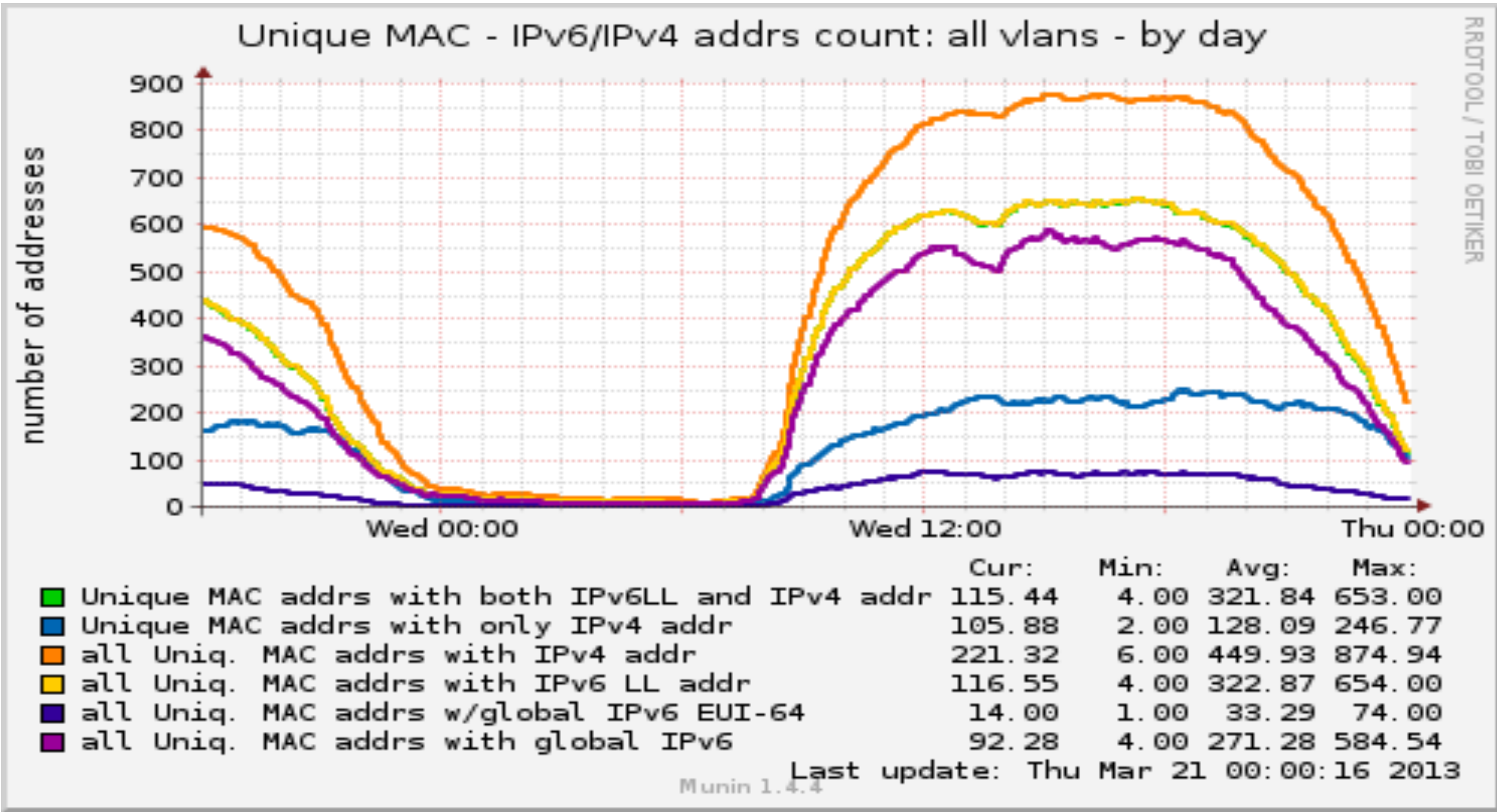


# IPv6 WiFi: опыт внедрения

Andrew Yourtchenko - Cisco



# Сегодня 60-70% WiFi устройств поддерживают IPv6



Источник: NOC stats MPLS & IPv6 World Congress Conference, Paris, 2013

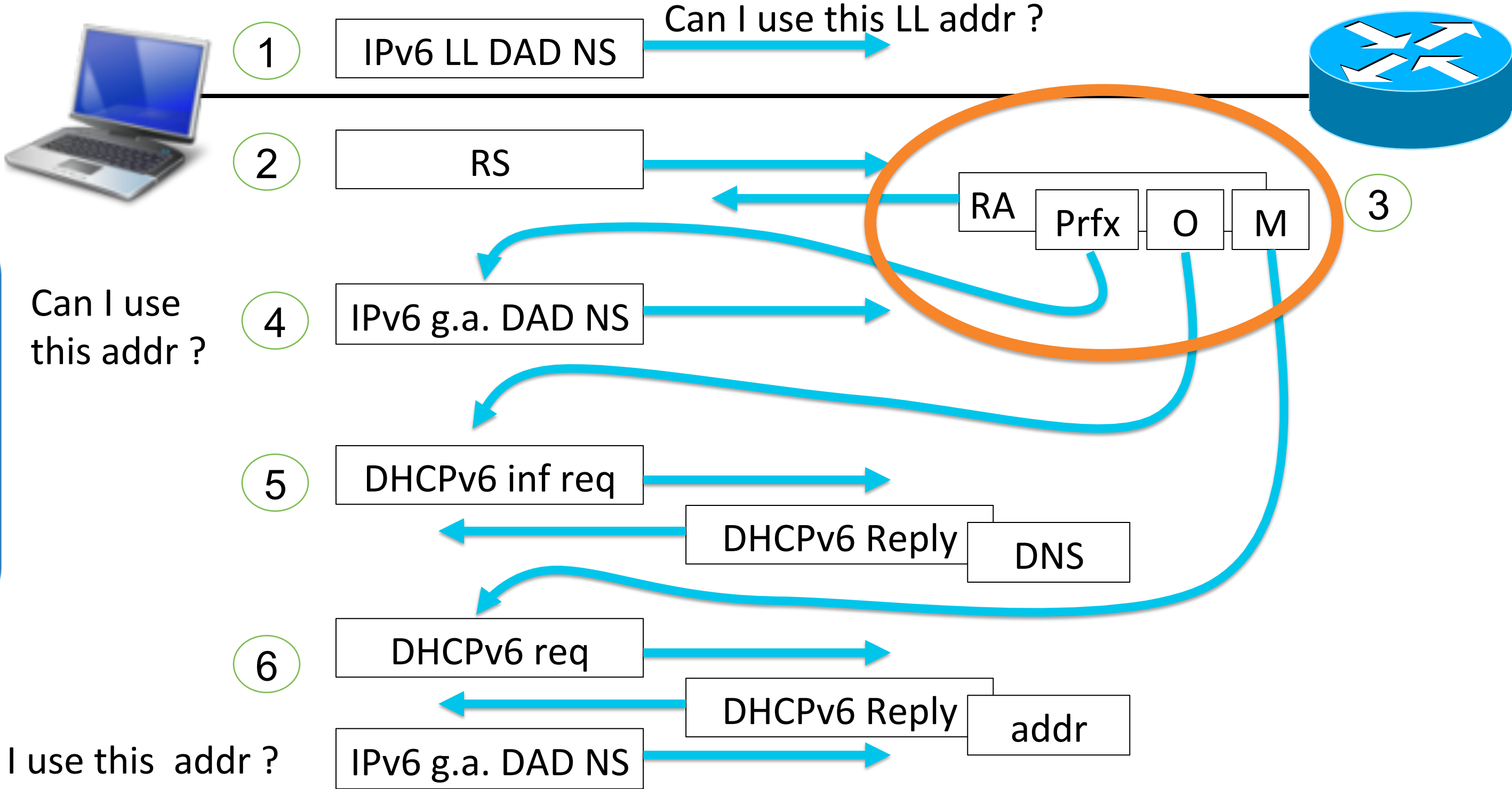
# Сеть конференции CiscoLive Europe

- 250-300 точек доступа (Access Points)
  - большая площадь покрытия
  - несколько тысяч одновременных подключений
- Динамичный жизненный цикл
  - Подготовка на месте – 4-5 дней
  - Срок эксплуатации – 5 дней
- WiFi - критичный и заметный компонент
  - «прозрачный» роуминг в движении
  - Простота в эксплуатации и настройке

# Общие принципы дизайна

- Один сегмент: IPv4- /16, IPv6- /64
  - Простота управления адресным пространством
  - Отсутствие L3-роуминга (только L2)
- Ограничение multicast-трафика
- Безопасность IPv6 Neighbor Discovery

# Обзор – новое подключение IPv6



# Multicast Router Advertisement в WiFi сети конференции

```
22:15:25.308623 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:15:25.309215 IP6 fe80::217:dfff:fe76:fc40 > 2a02:88fe:de30:501:5fe:13a0:afad:c700: ICMP6, neighbor
22:16:20.061204 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:16:33.030970 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:16:36.123642 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:16:42.808234 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:16:46.881731 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:16:50.850732 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:00.235141 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:04.324473 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:07.242607 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:13.411358 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:16.440376 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:19.469278 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:22.498330 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:25.527292 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:28.642138 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:31.689689 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:34.927601 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:38.318309 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:17:41.403313 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:18:26.249138 IP6 andrews-macbook-air.local > ff02::2: ICMP6, router solicitation, length 8
22:18:26.253591 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:18:27.485346 IP6 andrews-macbook-air.local > ff02::2: ICMP6, router solicitation, length 8
22:18:28.406047 IP6 andrews-macbook-air.local > ff02::2: ICMP6, router solicitation, length 8
22:18:29.344763 IP6 fe80::217:dfff:fe76:fc40 > ff02::1: ICMP6, router advertisement, length 64
22:18:29.357259 IP6 andrews-macbook-air.local > ff02::2: ICMP6, router solicitation, length 8
```

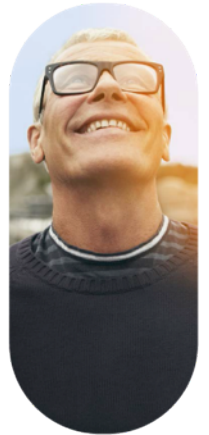
# Multicast Router Advertisements: RA throttling

The screenshot shows the Cisco Controller configuration interface. At the top, the Cisco logo is on the left, and navigation tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, and SECURITY are on the right. The CONTROLLER tab is selected. On the left side, a navigation menu lists various configuration categories: Controller, General, Inventory, Interfaces, Interface Groups, Multicast, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, IPv6 (with sub-items Neighbor Binding, RA Throttle Policy, and RA Guard), and mDNS. The RA Throttle Policy item is highlighted. The main content area is titled 'RA Throttle Policy > Edit' and contains the following configuration options:

- Enable RA Throttle Policy:
- Throttle Period (10-86400 seconds):
- Max Through (0-256):  No Limit
- Interval Option:
- Allow At-least (0-32):
- Allow At-most (0-256):  No Limit



# Безопасность Neighbor Discovery







# Демо: Windows 7 & "Rogue" RA

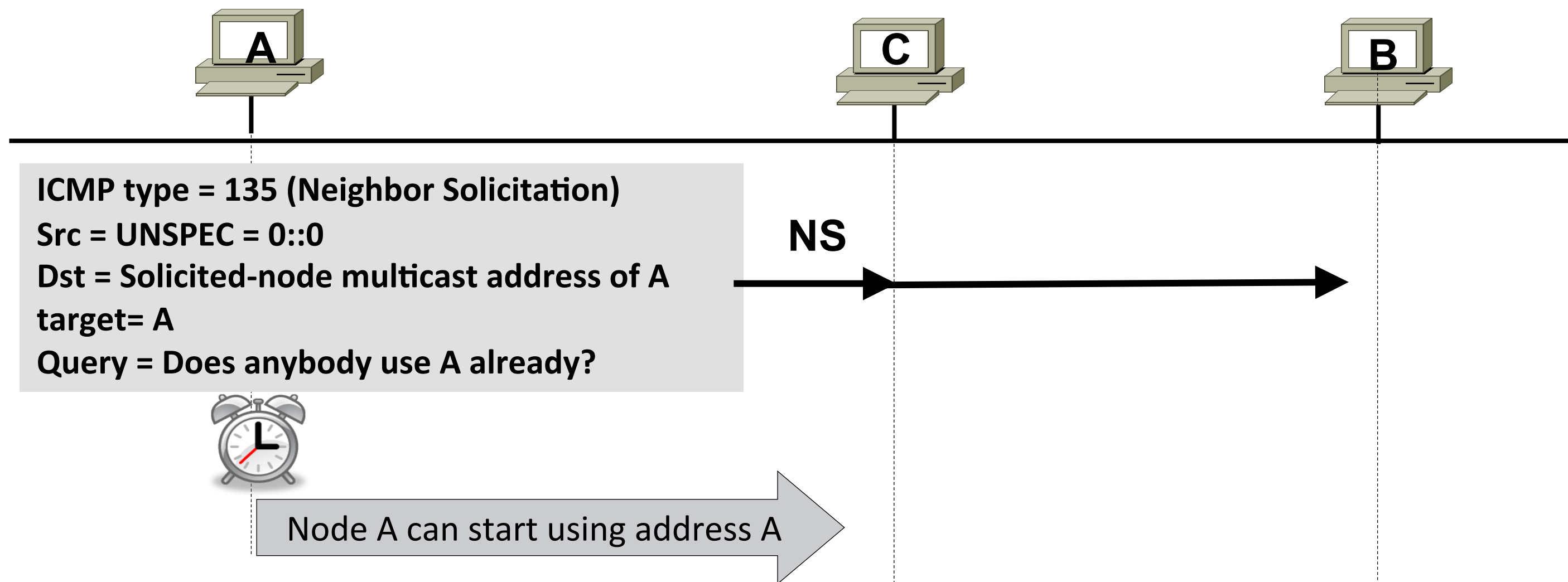


# WLC RA guard: запрет несанкционированных RA

The screenshot shows the Cisco WLC configuration interface. At the top is the Cisco logo and a navigation menu with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, and SECURITY. The CONTROLLER tab is selected. On the left is a sidebar menu with categories like General, Inventory, Interfaces, and a highlighted IPv6 section containing Neighbor Binding Timers, RA Throttle Policy, and RA Guard. The main content area is titled 'IPv6 > RA Guard' and shows two configuration options: 'IPv6 RA Guard on WLC' set to 'Enabled' and 'IPv6 RA Guard on AP' set to 'Enable' in a dropdown menu. Below these is a section for 'RA Dropped per client:' followed by a table with headers 'MAC Address', 'AP Name', and 'WLAN'. The table is currently empty.

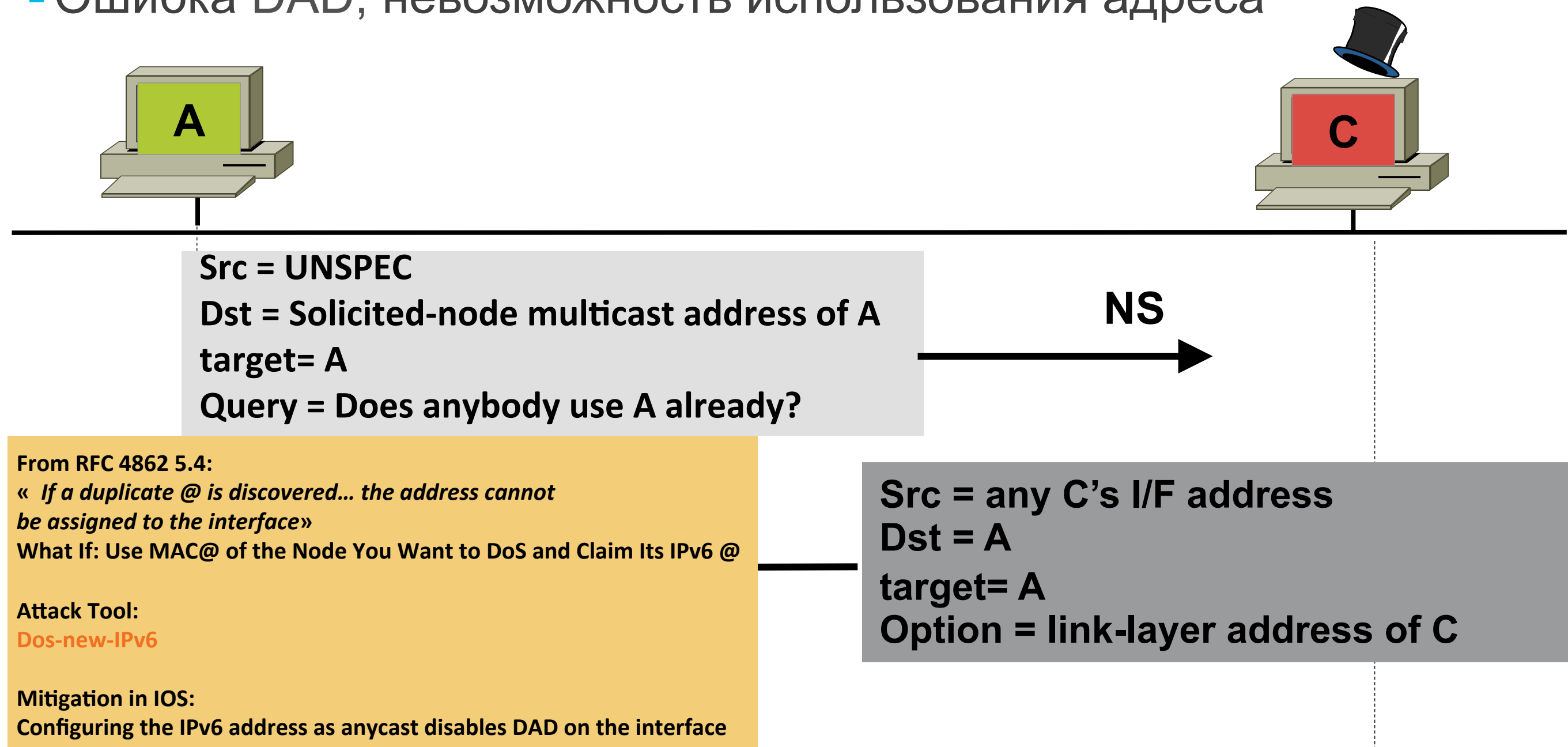
# Duplicate Address Detection: проверка уникальности

- Проверка уникальности адреса перед его активизацией
- Требуема (MUST) при SLACC, рекомендована (SHOULD) by DHCP
- Запрос ND на случай если кто-то уже использует этот адрес



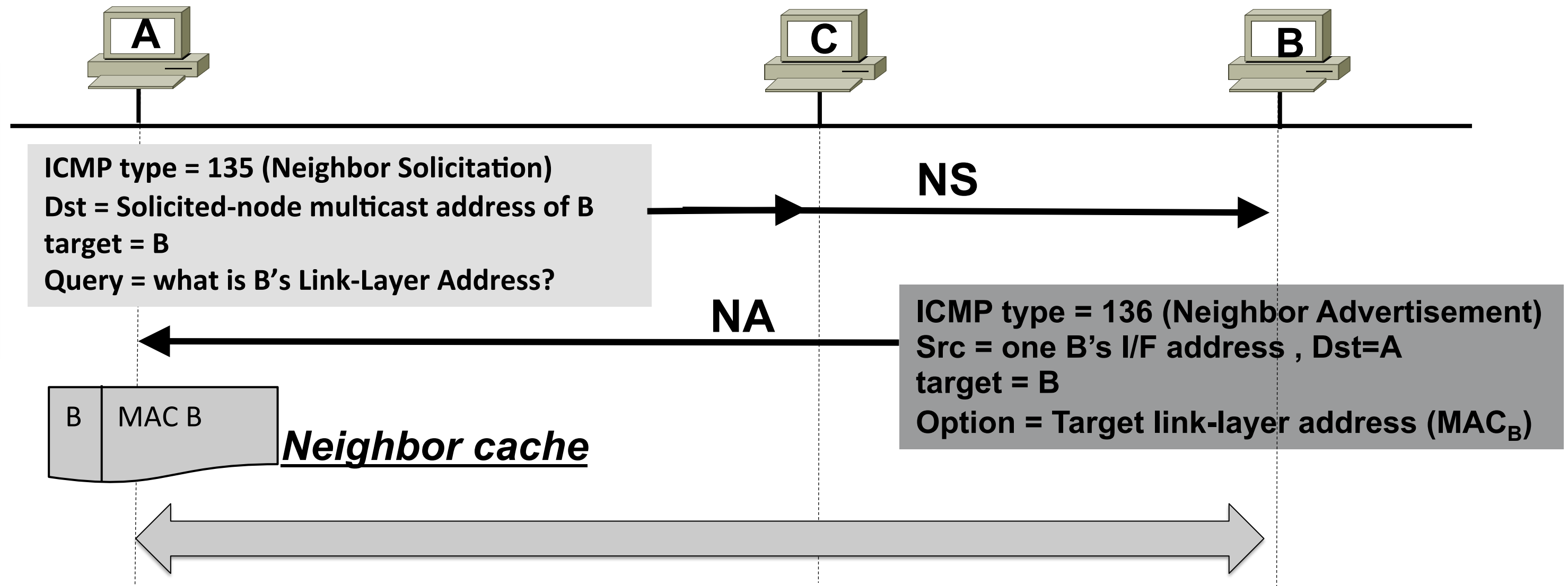
# Уязвимость в протоколе – блокировка работы

- Атакующий отвечает на все NS запросы DAD
- Ошибка DAD, невозможность использования адреса

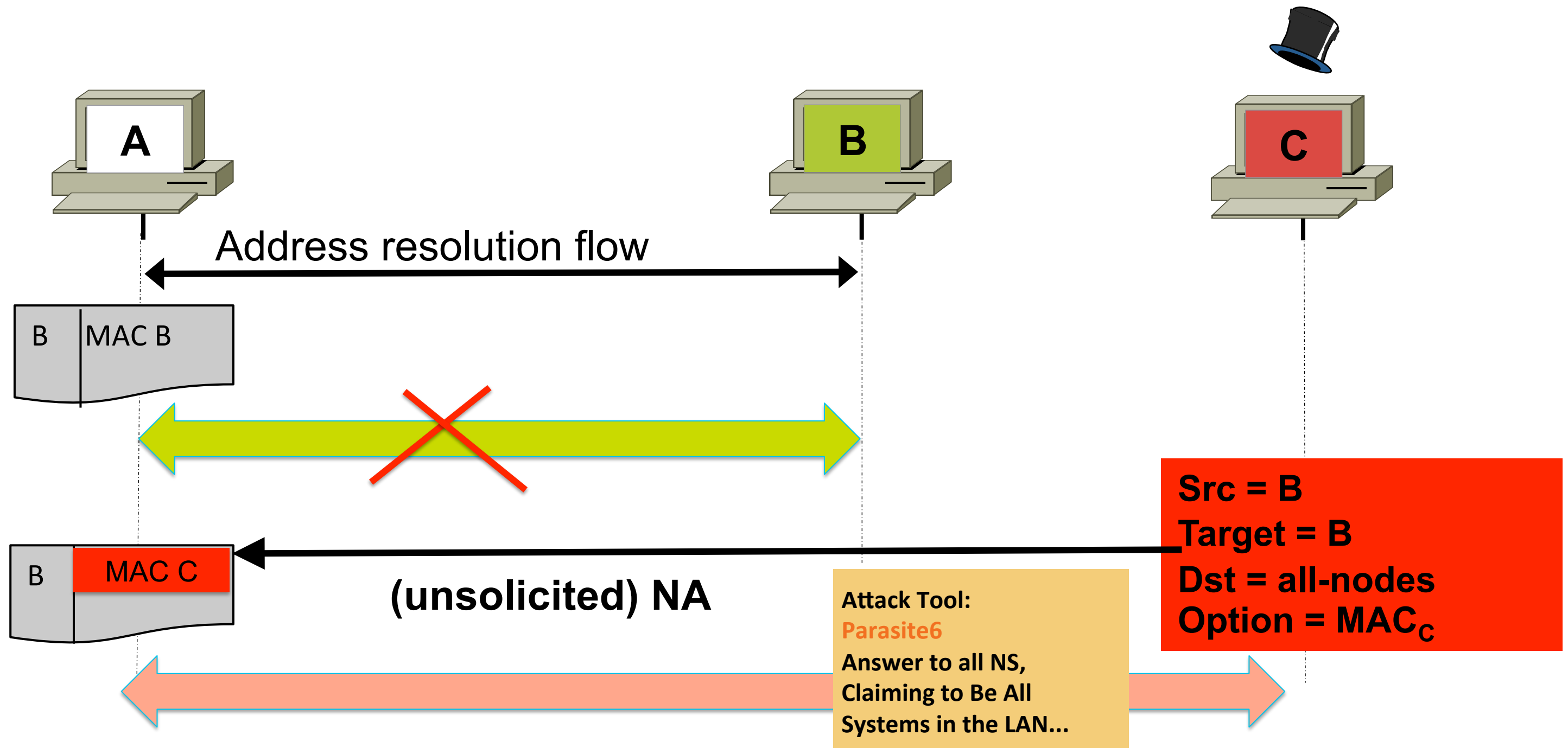


# IPv6 Neighbor Discovery: поиск Ethernet-адреса

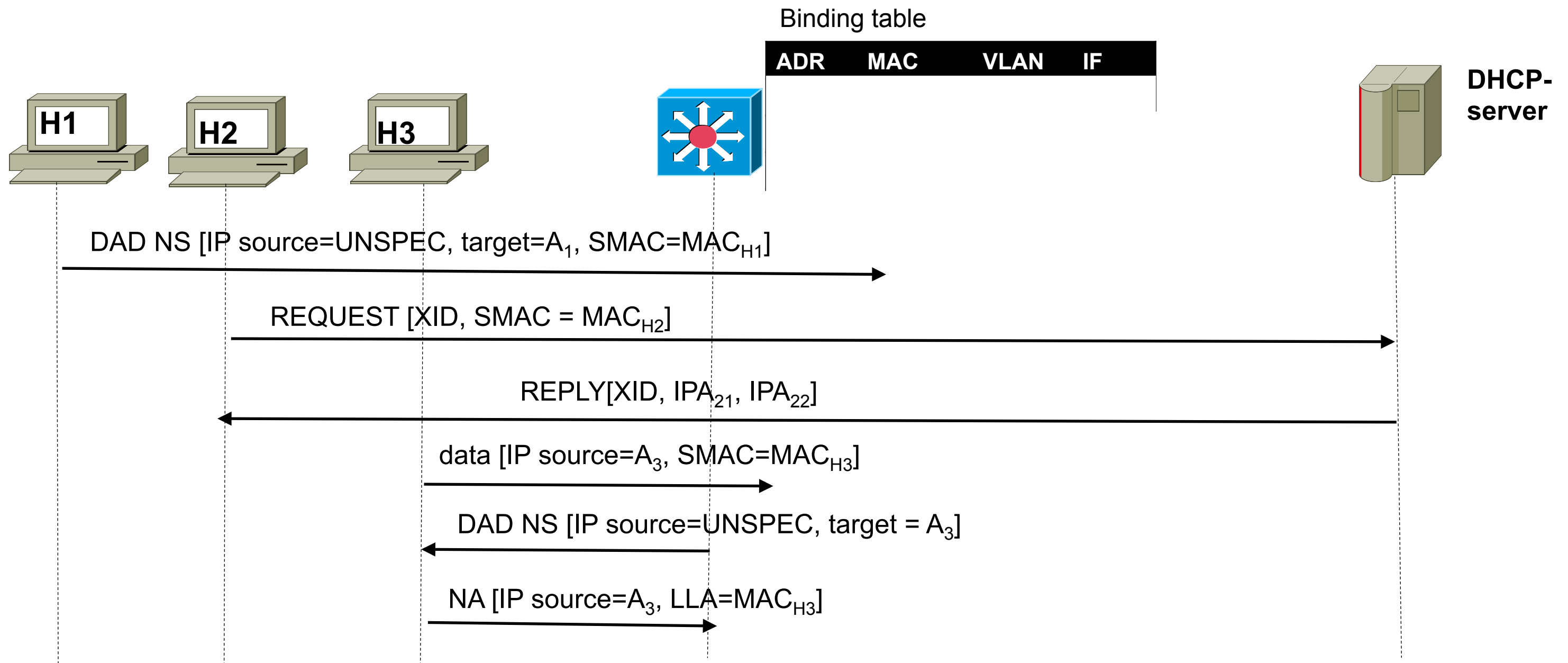
- Позволяет узнать Ethernet адрес узла сети по его IPv6 адресу
- Создает запись в таблице **neighbor cache**
- Поддерживает актуальность записи (NUD / обновления)
- Обновления обслуживаются по принципу “Last Come, First Serve (LCFS)”



# Уязвимость в протоколе – кража адреса



# Защита: отслеживание адресов на уровне L2



# WLC 7.2 - FHS source-guard

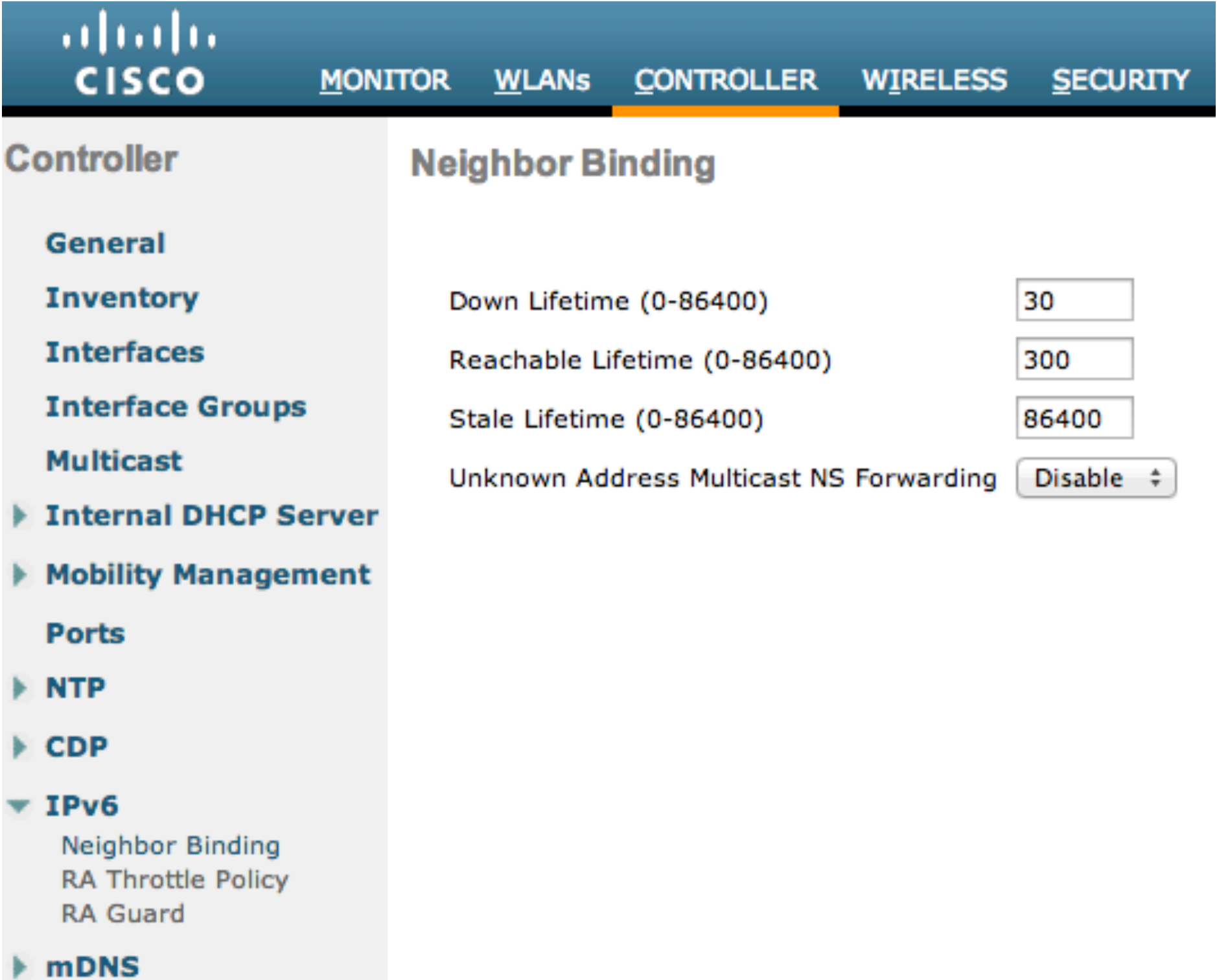
The screenshot shows the Cisco WLC 7.2 GUI. The browser address bar displays `https://172.17.1.20/screens/frameset.html`. The navigation menu includes **MONITOR**, **WLANs**, **CONTROLLER**, **WIRELESS**, **SECURITY**, **MANAGEMENT**, **COMMANDS**, **HELP**, and **FEEDBACK**. The **Monitor** section is active, showing a sidebar with **Summary**, **Access Points**, **Cisco CleanAir**, **Statistics**, **CDP**, **Rogues**, **Clients**, and **Multicast**. The main content area is titled **Clients > Detail** and contains two tables: **Client Properties** and **AP Properties**.

Client Properties		AP Properties	
MAC Address	5c:95:ae:61:22:b9	AP Address	00:21:a0:e4:9d:b0
IPv4 Address	0.0.0.0	AP Name	whiteAP

```
MAC Address 5c:95:ae:61:22:b9
IPv4 Address 0.0.0.0
IPv6 Address fe80::5e95:aeff:fe61:22b9,
2001:6f8:3d4:3:5e95:aeff:fe61:22b9,
2001:6f8:3d4:3:4500:dbf8:242a:1b6,
2001:6f8:3d4:3:45e7:df68:2ca1:7595,
```



# Neighbor Binding table in 7.3: установки по умолчанию

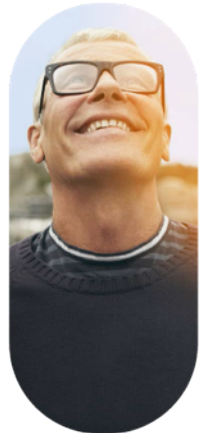


The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes the Cisco logo and tabs for MONITOR, WLANs, CONTROLLER (selected), WIRELESS, and SECURITY. The left sidebar lists various configuration categories under 'Controller', with 'Neighbor Binding' selected under the 'IPv6' section. The main content area displays the 'Neighbor Binding' configuration with four parameters: Down Lifetime (0-86400) set to 30, Reachable Lifetime (0-86400) set to 300, Stale Lifetime (0-86400) set to 86400, and Unknown Address Multicast NS Forwarding set to Disable.

Parameter	Value
Down Lifetime (0-86400)	30
Reachable Lifetime (0-86400)	300
Stale Lifetime (0-86400)	86400
Unknown Address Multicast NS Forwarding	Disable



# Демо: iPhone & Source Guard



## В заключение

- IPv6 на WiFi требует внимания к Multicast трафику
- RA Guard + Source Guard необходимы в любой IPv6 сети

