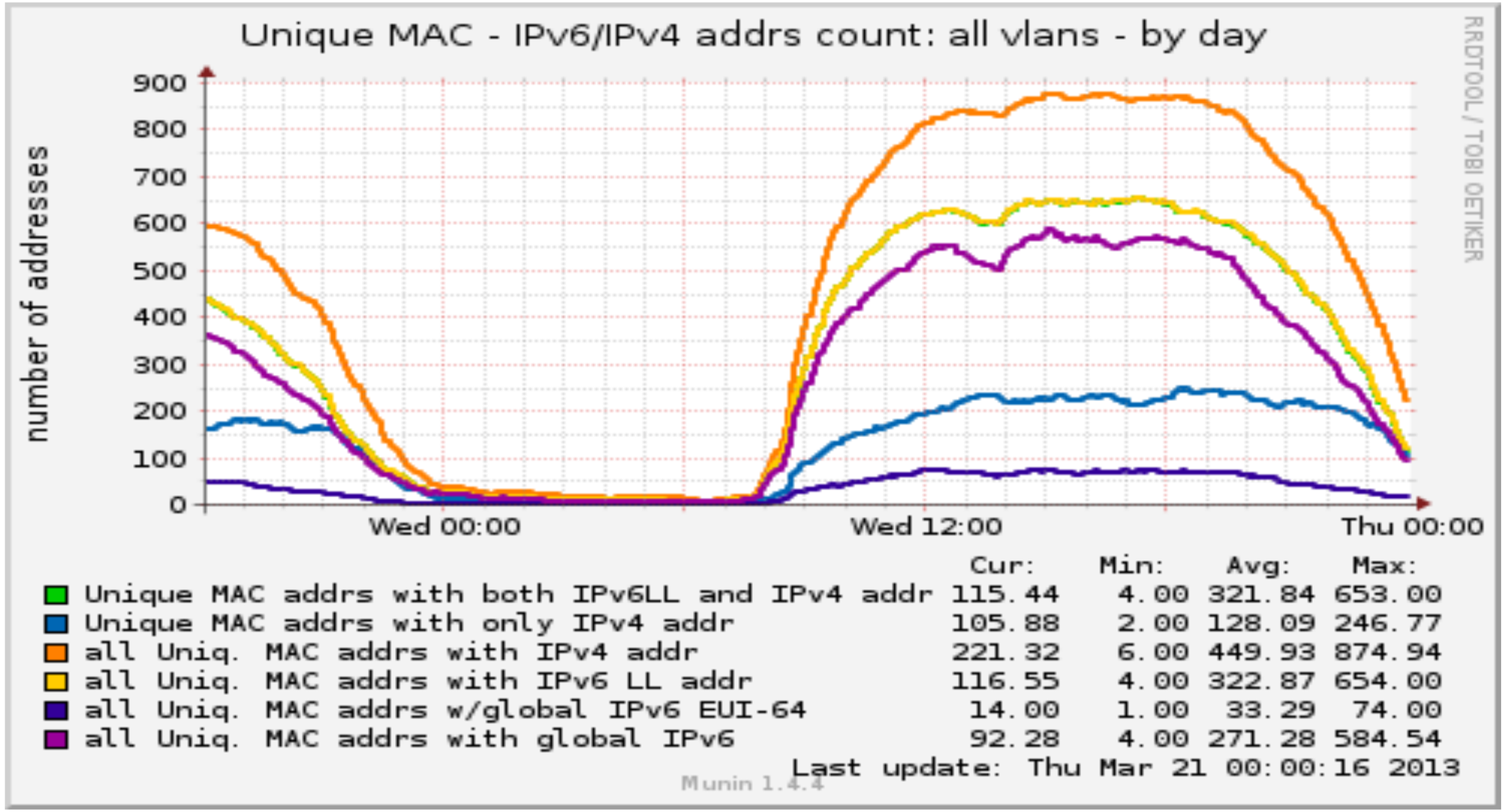
IPv6 WiFi: опыт внедрения

Andrew Yourtchenko - Cisco

Сегодня 60-70% WiFi устройств поддерживают IPv6



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

© 2012 Cisco and/or its affiliates. All rights reserved.

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

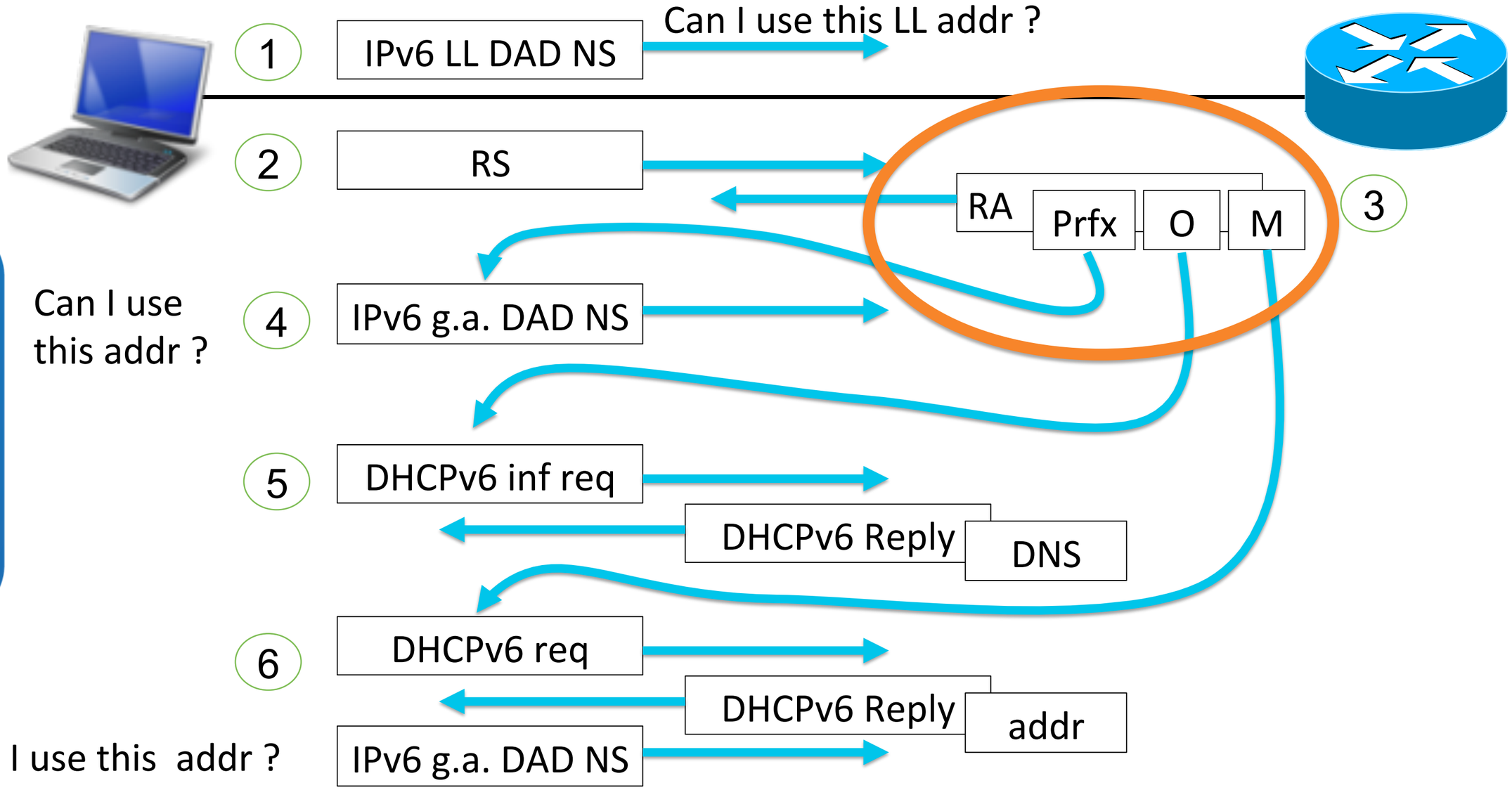
© 2012 Cisco and/or its affiliates. All rights reserved.

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

© 2012 Cisco and/or its affiliates. All rights reserved.

Обзор – новое подключение IPv6

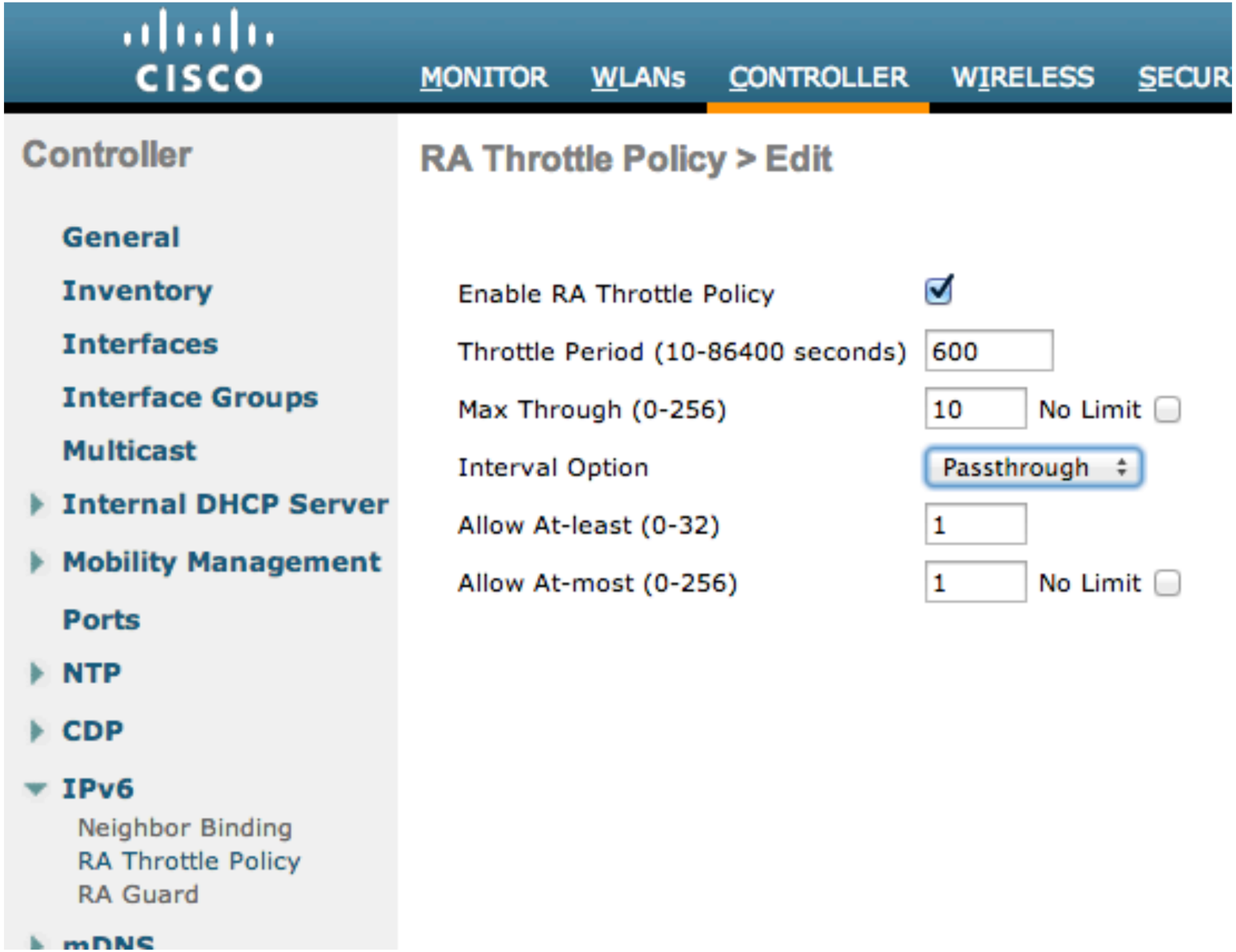


© 2012 Cisco and/or its affiliates. All rights reserved.

Multicast Router Advertisement в WiFi сети конференции

© 2012 Cisco and/or its affiliates. All rights reserved.

Multicast Router Advertisements: RA throttling

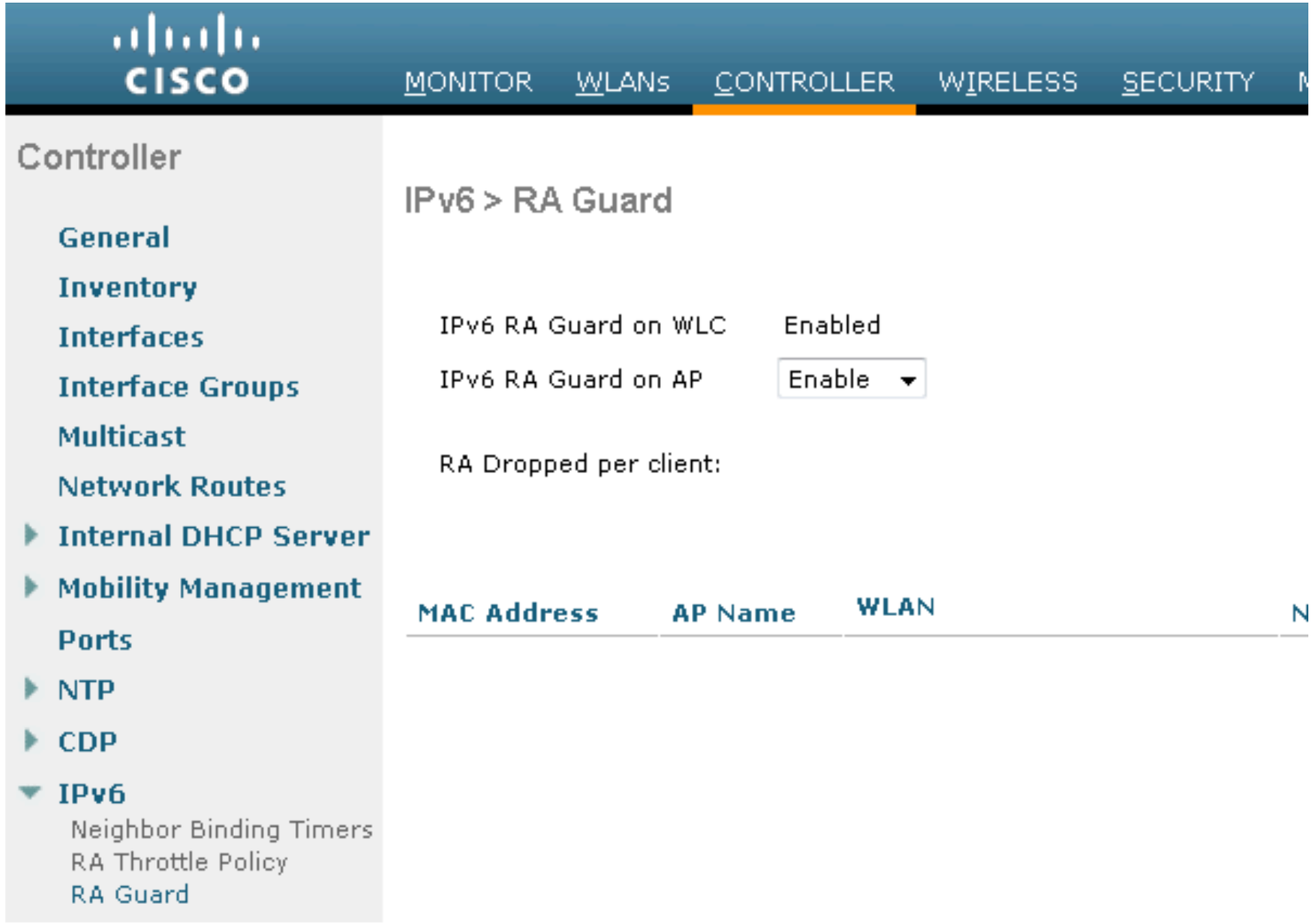


© 2012 Cisco and/or its affiliates. All rights reserved.

Безопасность Neighbor Discovery

Демо: Windows 7 & “Rogue” RA

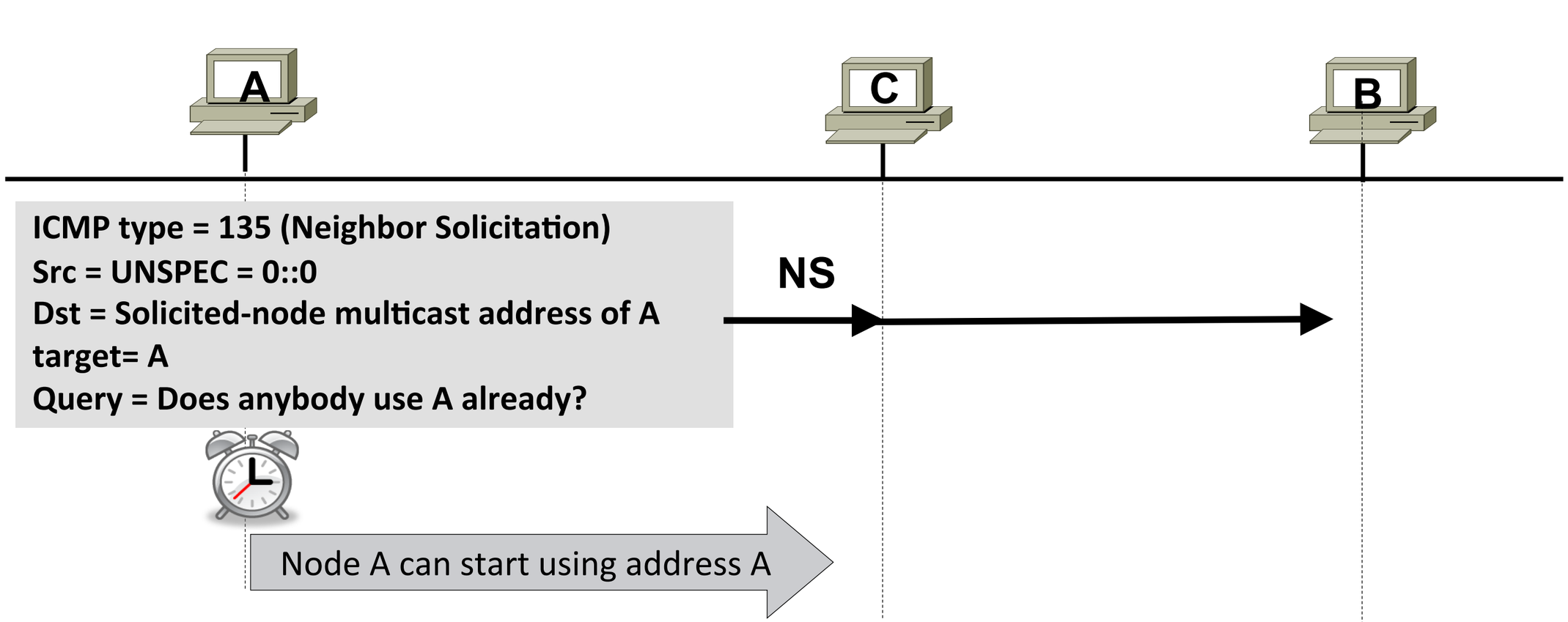
WLC RA guard: запрет несанкционированных RA



© 2012 Cisco and/or its affiliates. All rights reserved.

Duplicate Address Detection: проверка уникальности

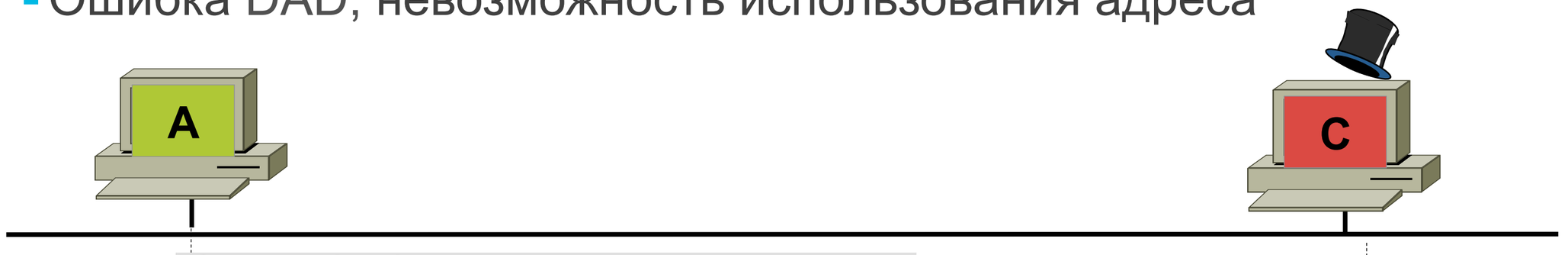
- Проверка уникальности адреса перед его активизацией
- Требуема (MUST) при SLACC, рекомендована (SHOULD) by DHCP
- Запрос ND на случай если кто-то уже использует этот адрес



© 2012 Cisco and/or its affiliates. All rights reserved.

Уязвимость в протоколе – блокировка работы

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



From RFC 4862 5.4:
« *If a duplicate @ is discovered… the address cannot be assigned to the interface*»
What If: Use MAC@ of the Node You Want to DoS and Claim Its IPv6 @

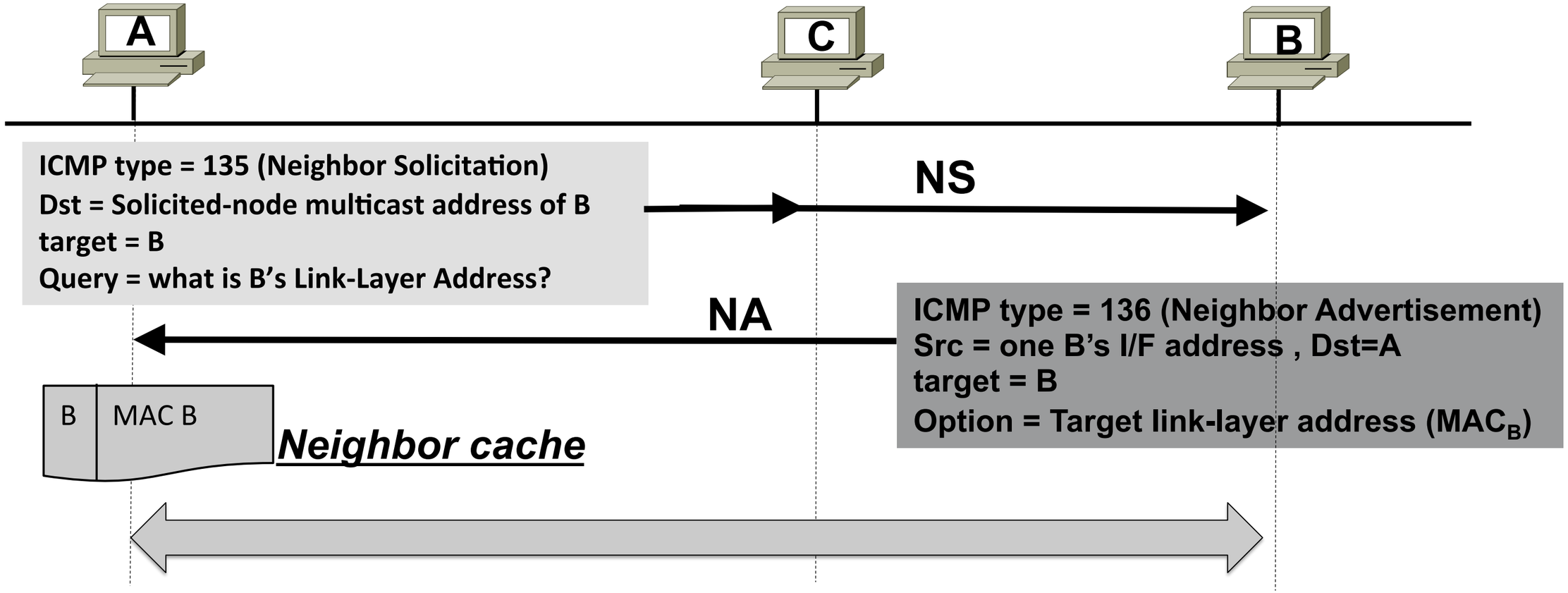
Attack Tool:
Dos-new-IPv6

Mitigation in IOS:
Configuring the IPv6 address as anycast disables DAD on the interface

© 2012 Cisco and/or its affiliates. All rights reserved.

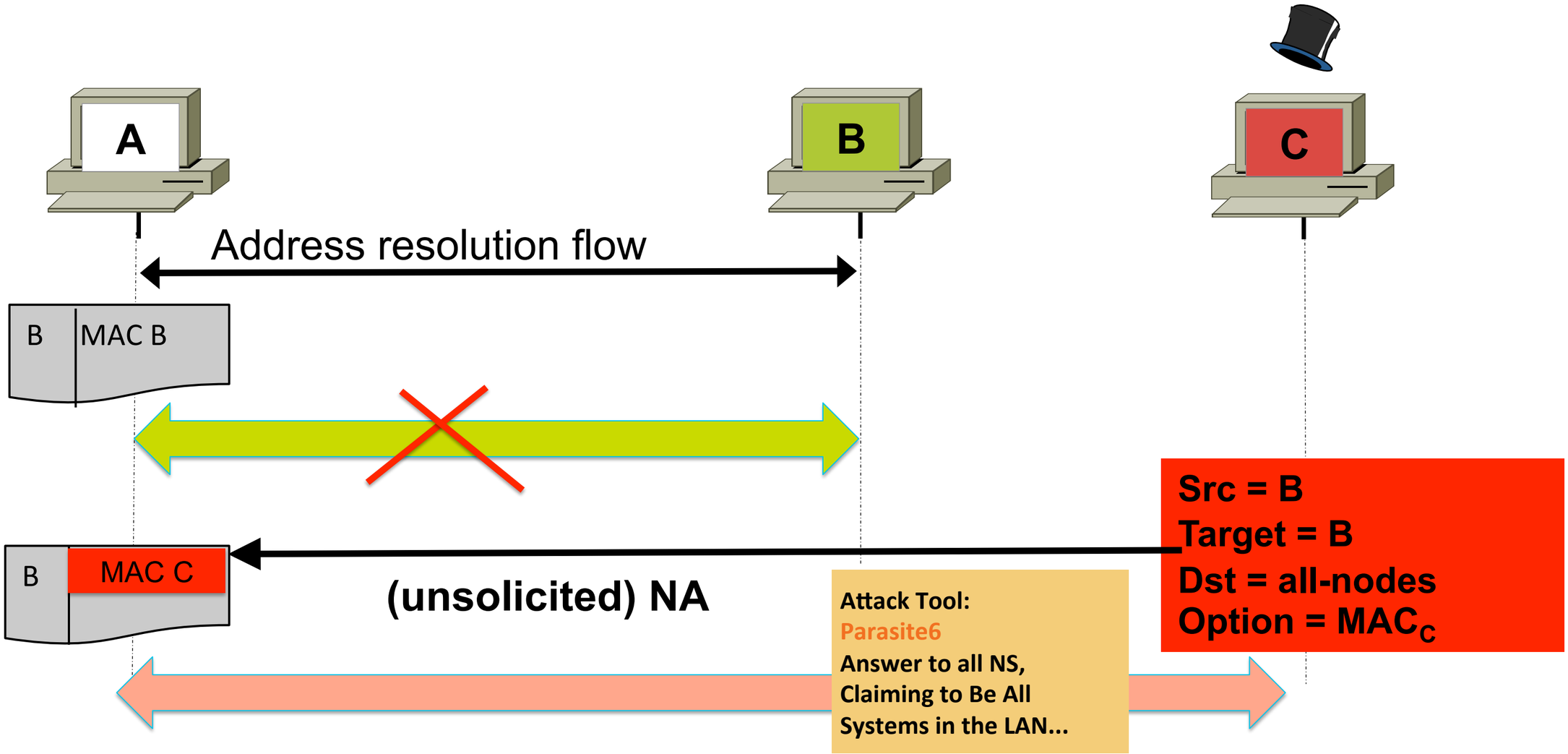
IPv6 Neighbor Discovery: поиск Ethernet-адреса

- 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)”



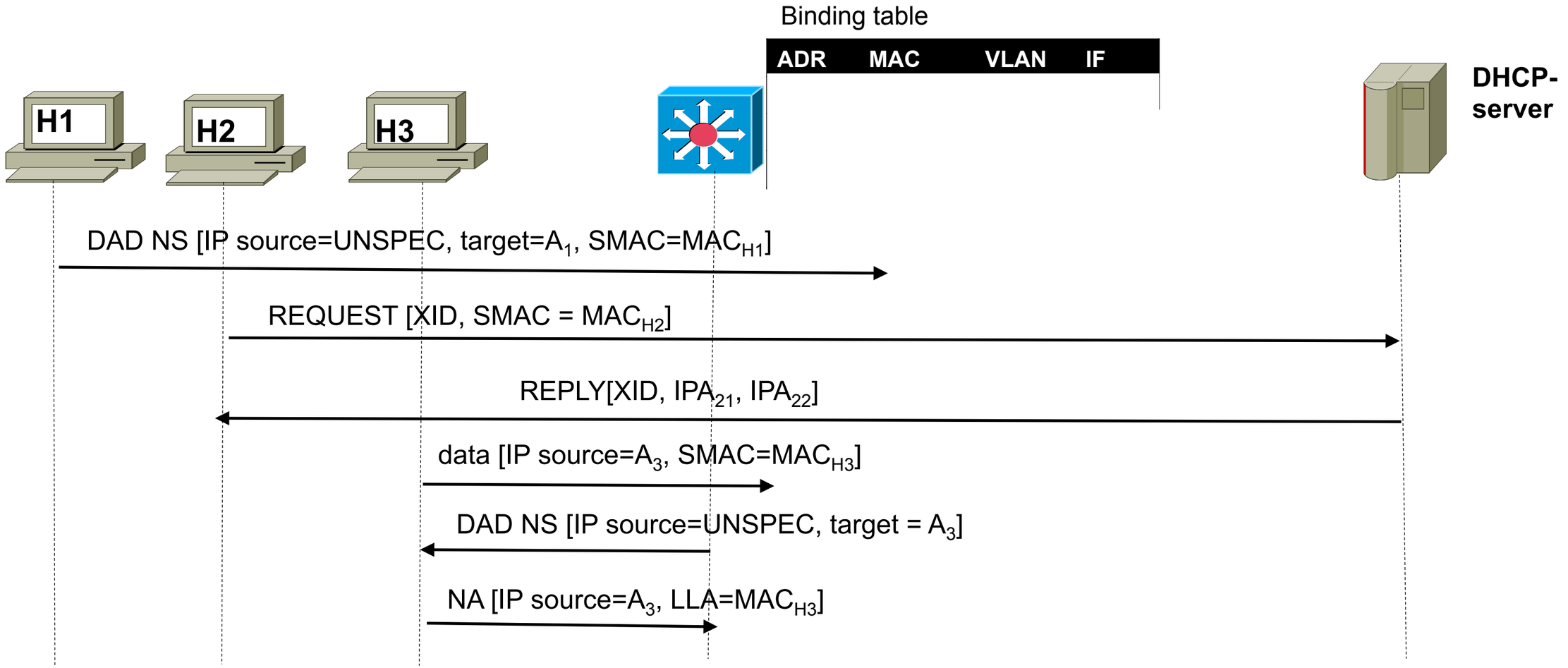
© 2012 Cisco and/or its affiliates. All rights reserved.

Уязвимость в протоколе – кража адреса



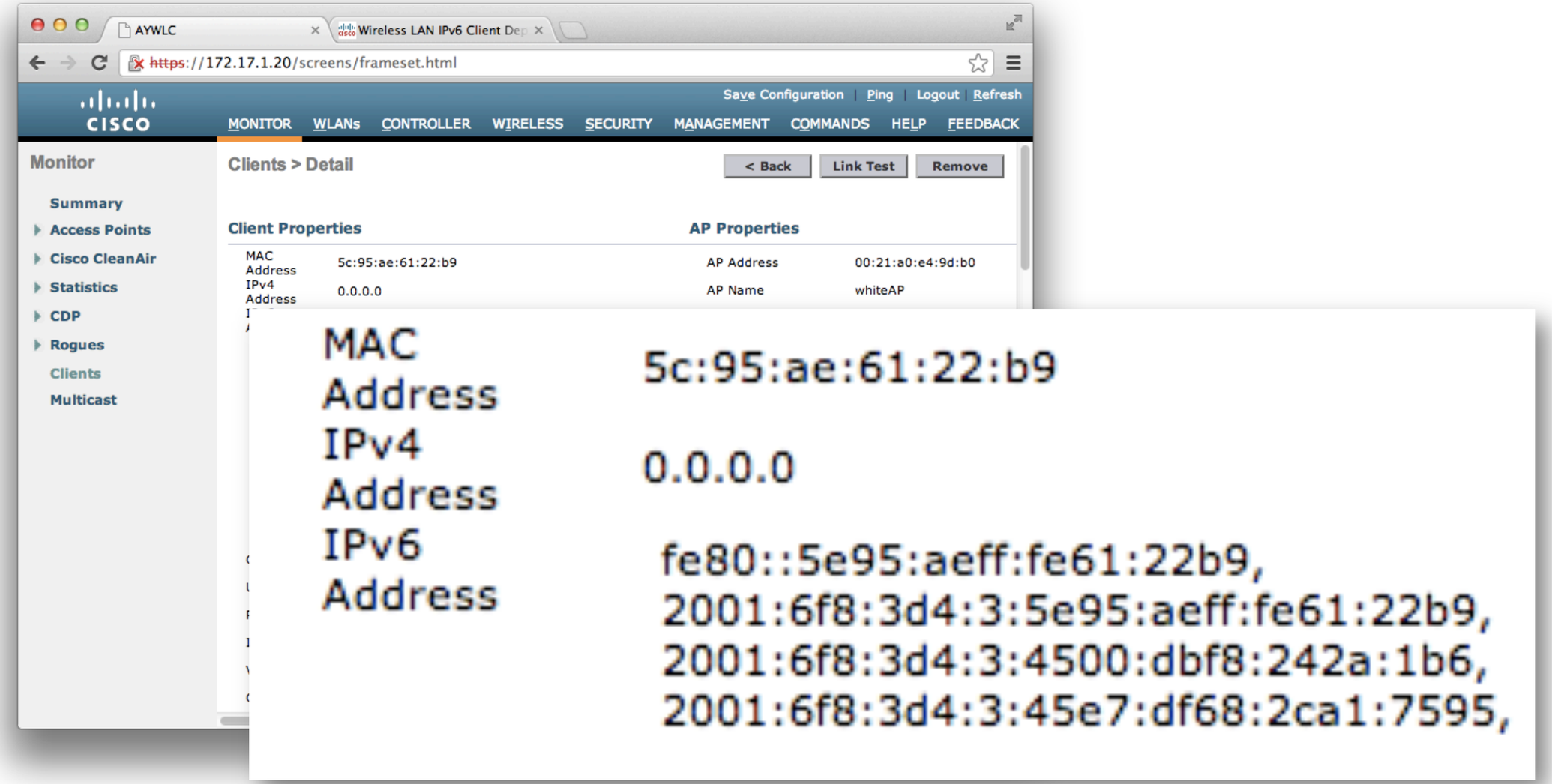
© 2012 Cisco and/or its affiliates. All rights reserved.

Защита: отслеживание адресов на уровне L2



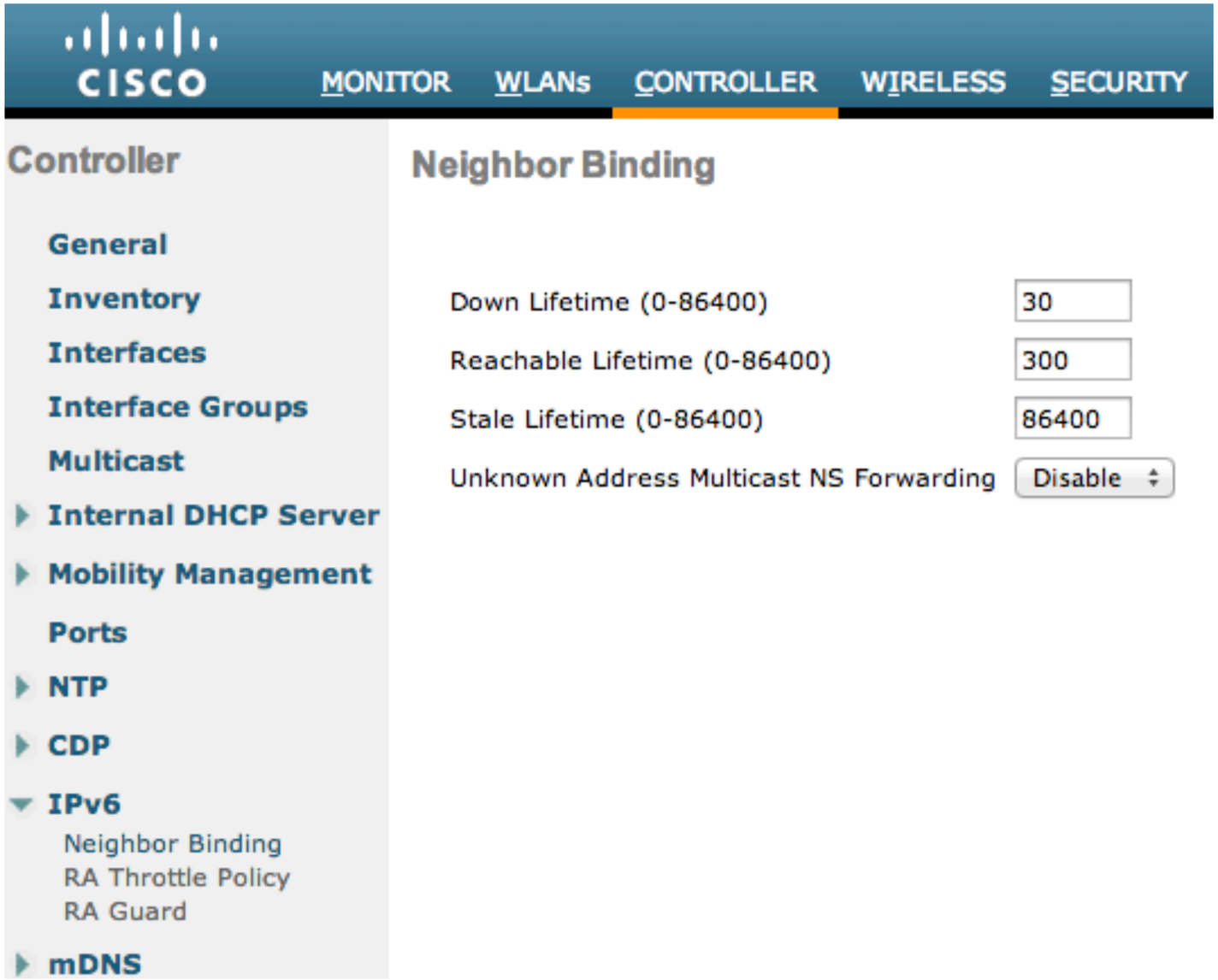
© 2012 Cisco and/or its affiliates. All rights reserved.

WLC 7.2 - FHS source-guard



© 2012 Cisco and/or its affiliates. All rights reserved.

Neighbor Binding table in 7.3: установки по умолчанию



© 2012 Cisco and/or its affiliates. All rights reserved.

Демо: iPhone & Source Guard

В заключение

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

© 2012 Cisco and/or its affiliates. All rights reserved.