SAVI: Validación de direcciones

Marcelo Bagnulo
Foro de seguridad de RedIRIS
Abril 2013
Universidad Carlos III de Madrid

Motivación

- Las motivaciones de quienes generan paquetes con direcciones falsas son, en su mayoría, no muy puras.
  - Ocultar la procedencia de los ataques
  - Obtener acceso restringido a ciertas direcciones
  - Hacerse pasar por otro dispositivo
- Es deseable evitar la falsificación de direcciones

Técnicas usadas

- Filtros de ingreso (BCP38)
  - Granularidad a nivel de prefijo
  - Puede utilizar información de ruteo
  - Limitación: granularidad a nivel de prefijo

Objetivos de SAVI

- Objetivo: validar direcciones con una granularidad de direcciones individuales
  - Aquellos paquetes con direcciones falsas de descartan
  - Configuración automática de los filtros/configuración manual mínima
- Sólo el dispositivo que es dueño de la dirección puede enviar paquetes con esta
  - Pero, ¿cómo sabemos quién es dueño de qué dirección?
    - Depende fuertemente del mecanismo de asignación de direcciones usado

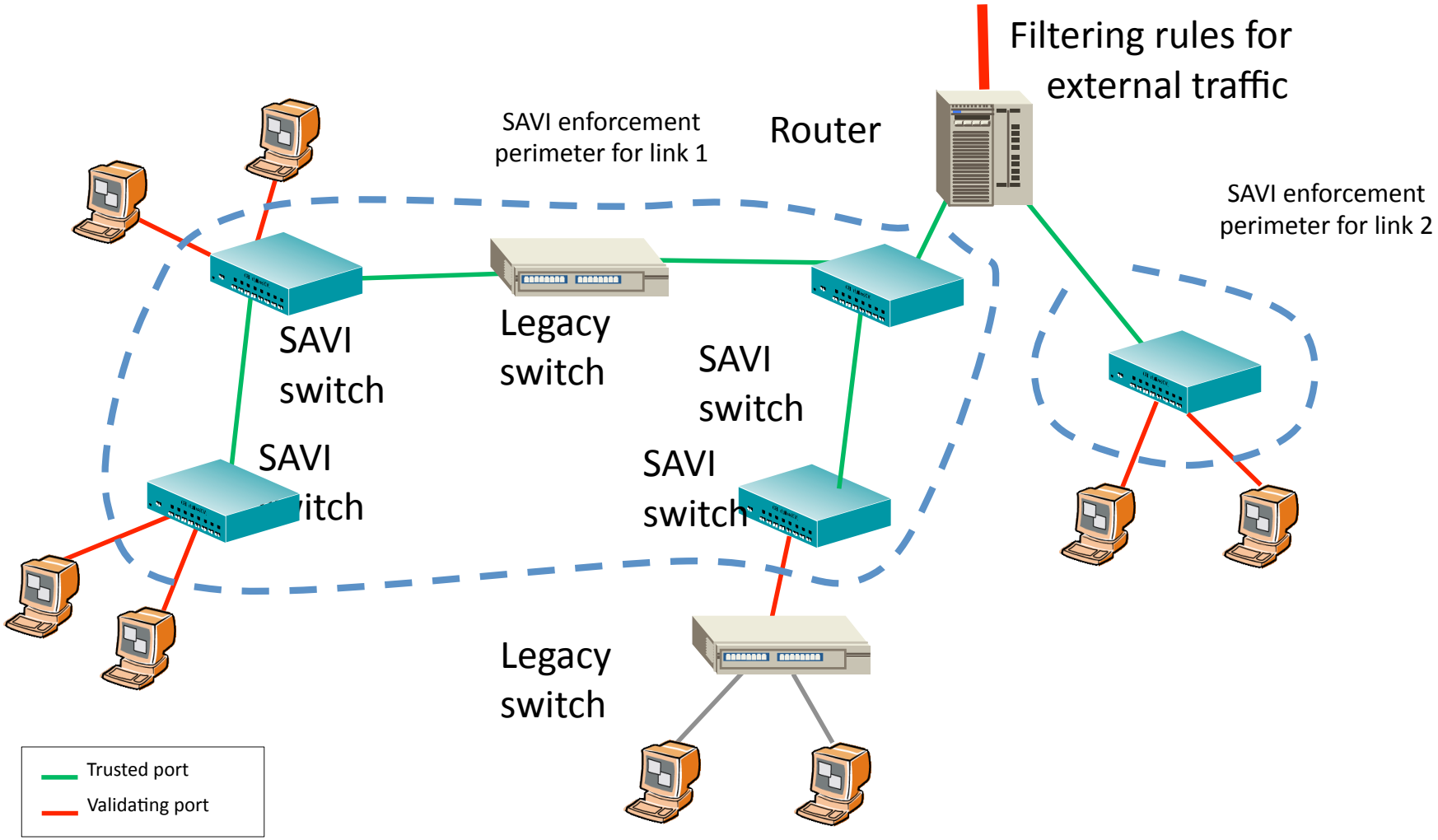
Elementos de SAVI

- Filtrado
- Creación de bindings

Filtrado SAVI

- Idea básica: los paquetes que tienen direcciones falsas son filtrados
- ¿Cómo sabemos que una dirección es falsa?
- Tabla de bindings: asociaciones entre direcciones y binding anchors
  - Binding anchor: propiedad verificable en el paquete difícil de falsificar, e.g. Puerto del switch
- Topología SAVI: Más cerca esté el dispositivo SAVI del nodo final, mayor protección.
  - Caso ideal: SAVI en los switches

Perímetro de protección



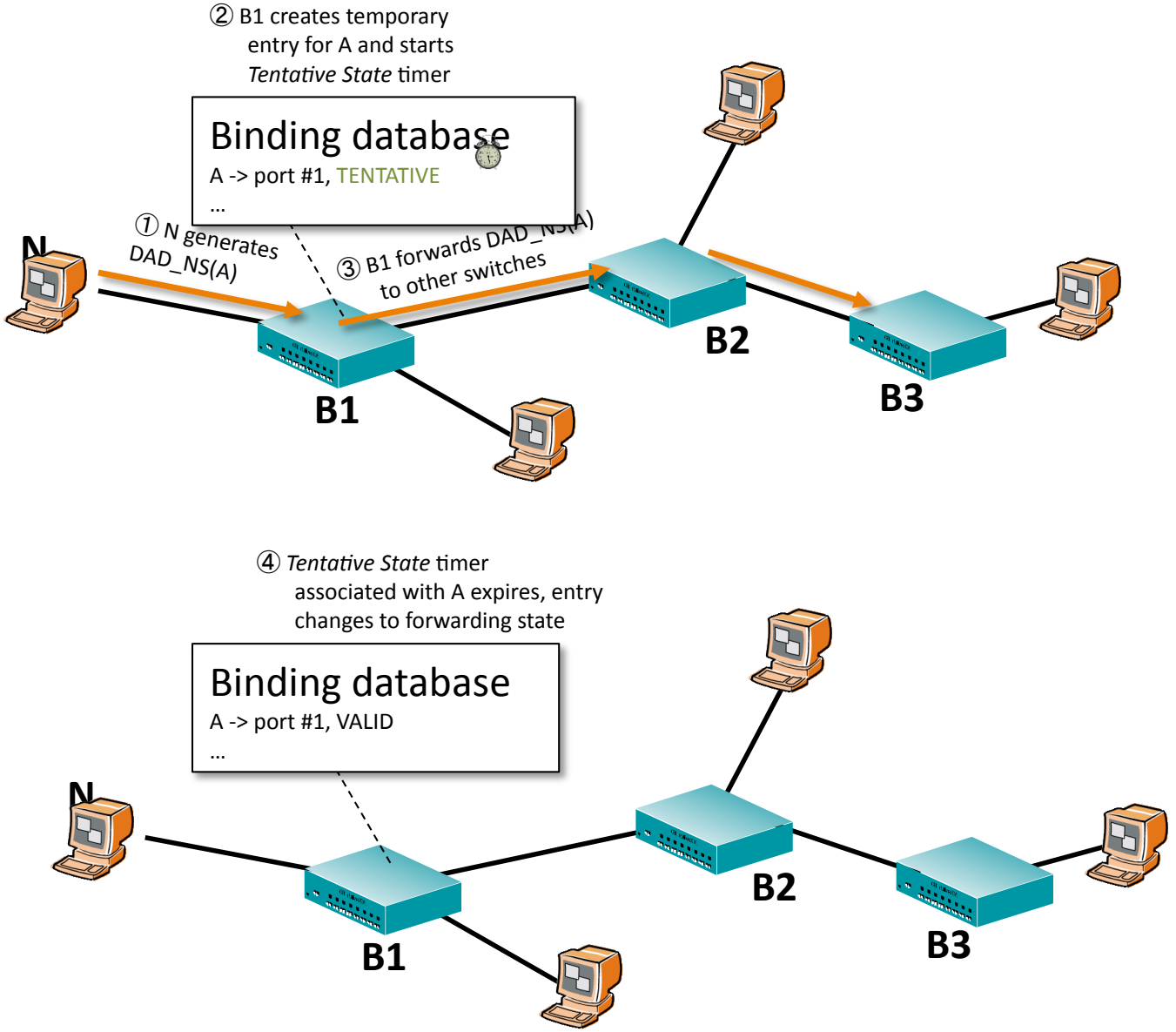
Creación de bindings

- El filtrado asume la existencia de una tabla de bindings, ¿cómo poblamos la tabla?
- Los bindings asocian una dirección a un binding anchor que pertenece al dueño de la dirección
- ¿Cómo saber quién es el dueño de la dirección?
  - En función de la configuración de la misma
- Sabores de SAVI:
  - SAVI FCFS
  - SAVI DHCP
  - SAVI SEND

SAVI FCFS

- Usado con direcciones IPv6 autoconfiguradas (SLAAC)
- El criterio para la propiedad es FCFS
- El dispositivo SAVI inspecciona los mensajes de ND para crear los bindings
  - DAD

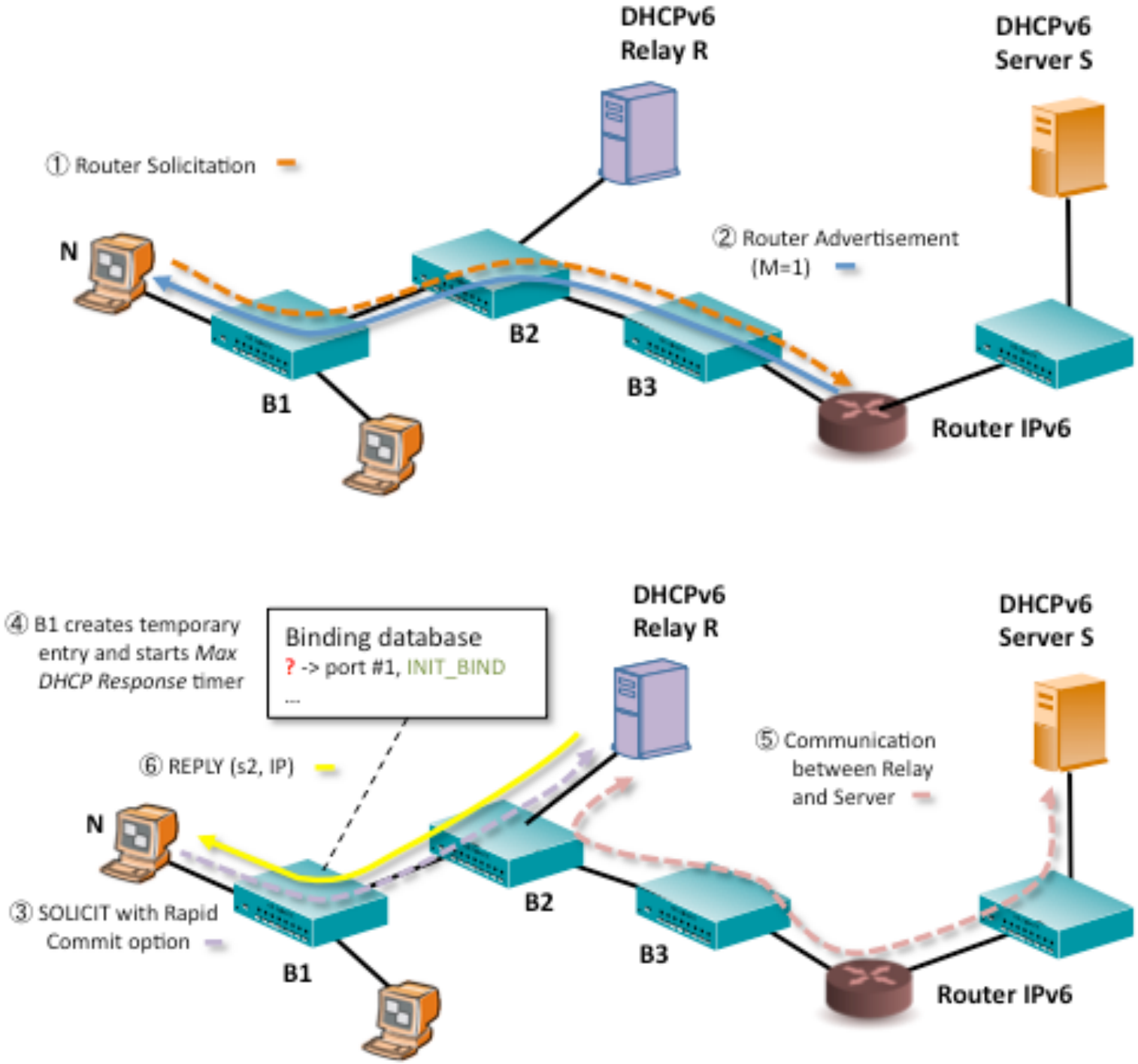
SAVI FCFS


② B1 creates temporary entry for A and starts *Tentative State* timer
Binding database
A -> port #1, TENTATIVE
...
① N generates DAD_NS(A)
③ B1 forwards DAD_NS(A) to other switches
N
B1
B2
B3
④ *Tentative State* timer associated with A expires, entry changes to forwarding state
Binding database
A -> port #1, VALID
...
N
B1
B2
B3

SAVI DHCP

- Se usa para direcciones IPv4 y IPv6 configuradas vía DHCP
- El criterio de propiedad es lo que digan los mensajes DHCP

SAVI DHCP


DHCPv6
Relay R
DHCPv6
Server S
① Router Solicitation
② Router Advertisement
(M=1)
N
B1
B2
B3
Router IPv6
④ B1 creates temporary
entry and starts *Max*
DHCP Response timer
Binding database
? -> port #1, INIT_BIND
...
⑤ Communication
between Relay
and Server
⑥ REPLY (s2, IP)
③ SOLICIT with Rapid
Commit option

SAVI SEND

- Es válido para direcciones CGAs
- La propiedad de las direcciones viene dada por la propiedad de la clave privada
- Utiliza el protocolo SEND para verificar la propiedad de la clave privada

Comentarios finales

- SAVI provee protección contra la falsificación de direcciones.
- 3 sabores de SAVI
  - SAVI FCFS
  - SAVI DHCP
  - SAVI SEND

Referencias

- E. Nordmark, M. Bagnulo, E. Levy-Abegnoli. “FCFS SAVI: First-Come First-Serve Source-Address Validation for Locally Assigned IPv6 Addresses”, IETF RFC 6620. May 2012.
- J. Bi, J. Wu, G. Yao, F. Baker. “SAVI Solution for DHCP”. draft-ietf-savi-dhcp-11.txt. December 2011.
- M. Bagnulo, A. Garcia-Martinez. SEND-based Source-Address Validation Implementation. draft-ietf-savi-send-07. March 2012.
- SAVI: The IETF Standard in Address Validation. Marcelo Bagnulo, Alberto García-Martínez. IEEE Communications Magazine, abril 2013.