SAVI IP Source Guard

draft-baker-sava-implementation

Fred Baker

Cases covered in the draft

- Draft specifies IPv6, could include IPv4
- Network cases:
  - Switched LANs and access networks
    - Protect in switch
  - Non-switched LANs and access networks
    - Protect neighboring host and router from peers
  - Upstream router
    - Traditional ingress filtering

Premises:

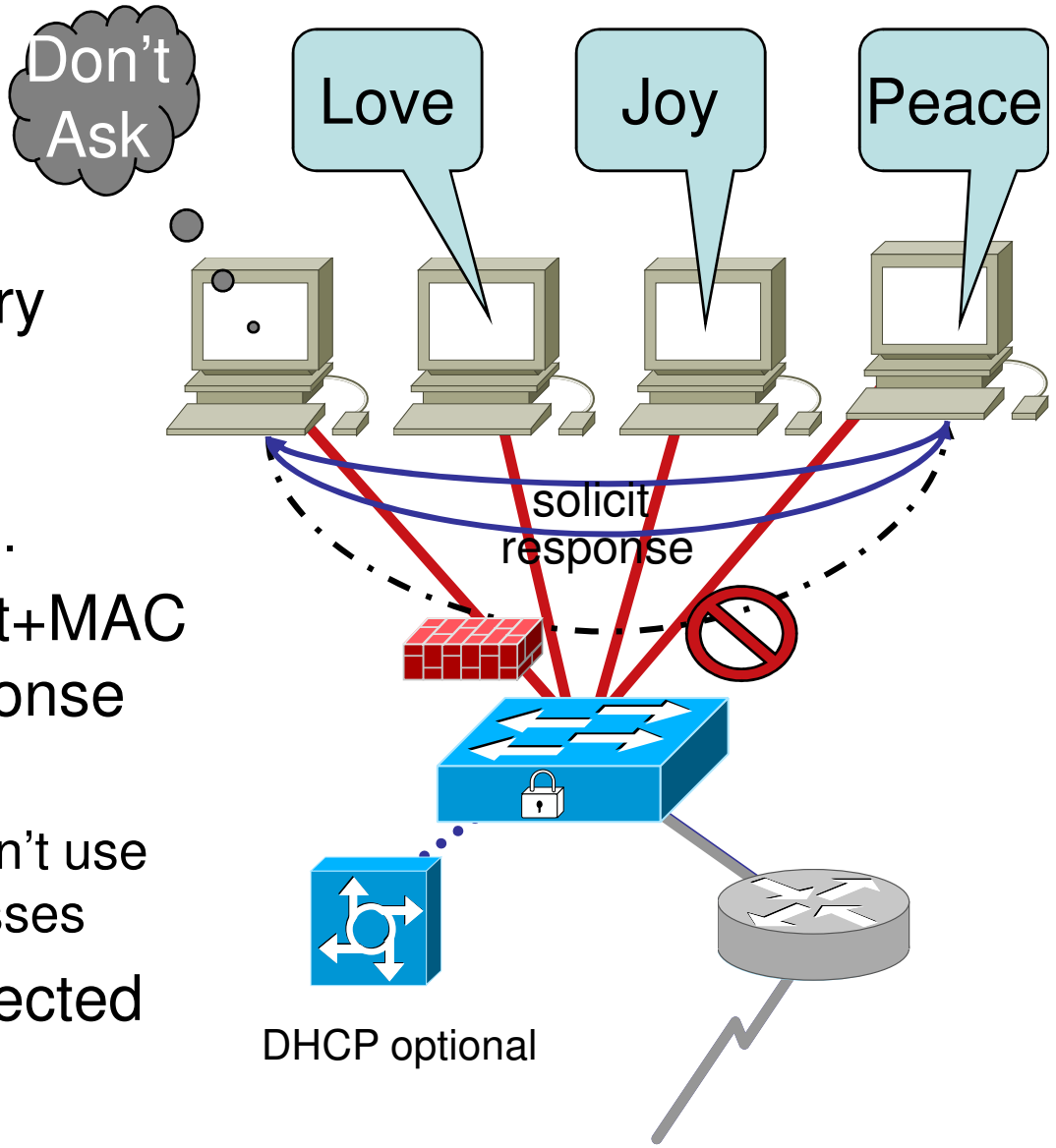
- Addresses assigned using DHCP or SAA
- Multiple addresses per interface
- On interfaces with sub-interfaces such as VLANs, the sub-interface is under discussion
- Host has one interface
  - That said, see draft-baker-6man-multiprefix-default-route
  - Proposes separate default routes/default gateways by source address
  - One could protect more cases with that model

Trust Anchors

- The key is to associate an IP address with a stable lower layer entity or set of entities:
  - Physical or logical port
  - 802.11 radio association
  - Ethernet MAC Address
  - Virtual circuit or other tunnel
- Every link layer has trust anchors that can be used for network layer address verification

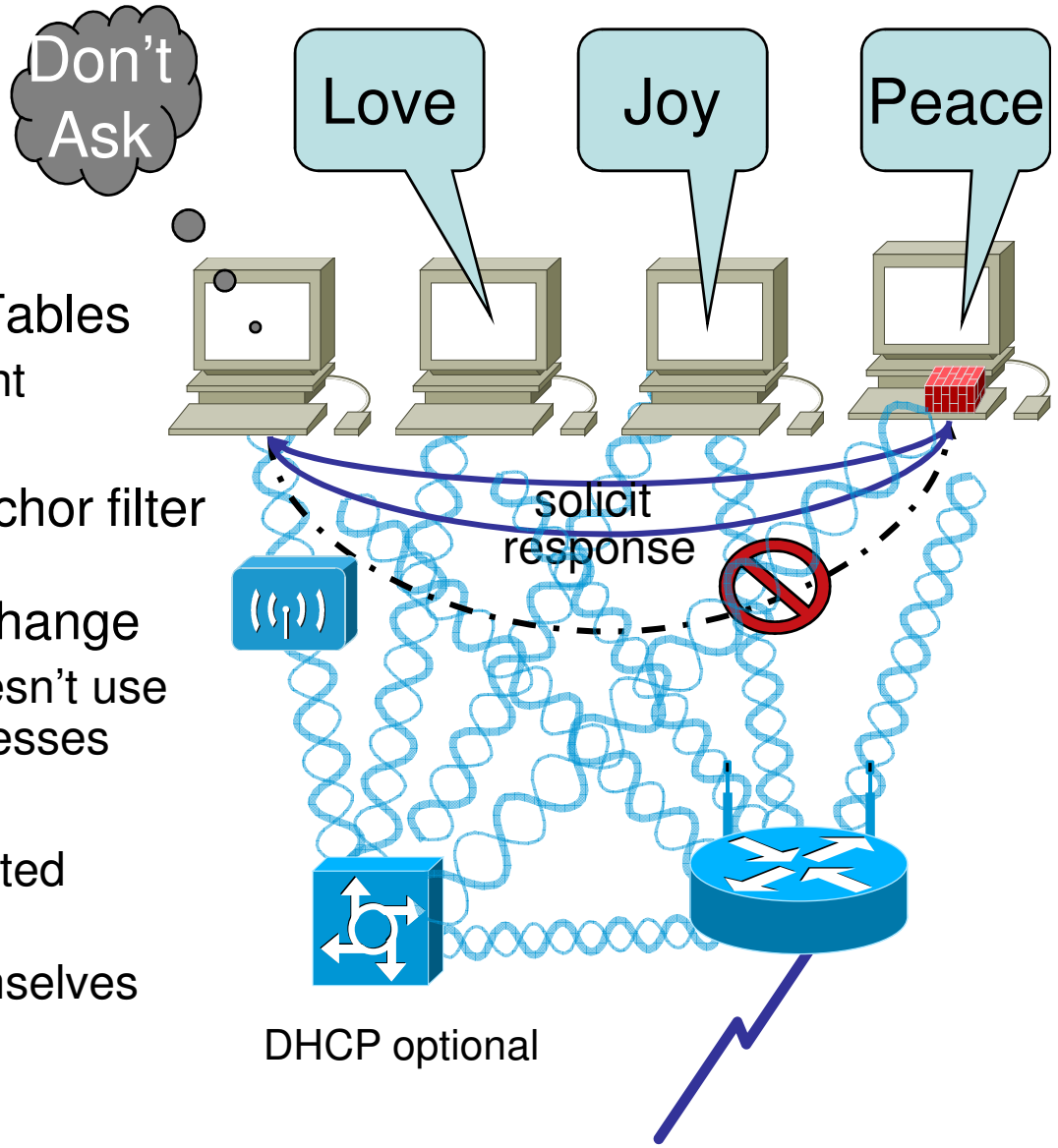
Algorithm for switched LANs

- Implement in the switch
- Snoop Neighbor Discovery
  - DHCP or SAA assignment
  - ND or SeND negotiation
  - Yes, that's a layer violation.
- Autoconfigure port or port+MAC filter on Solicitation/Response exchange
  - Discard IP traffic that doesn't use properly negotiated addresses
- Routers still can't be protected

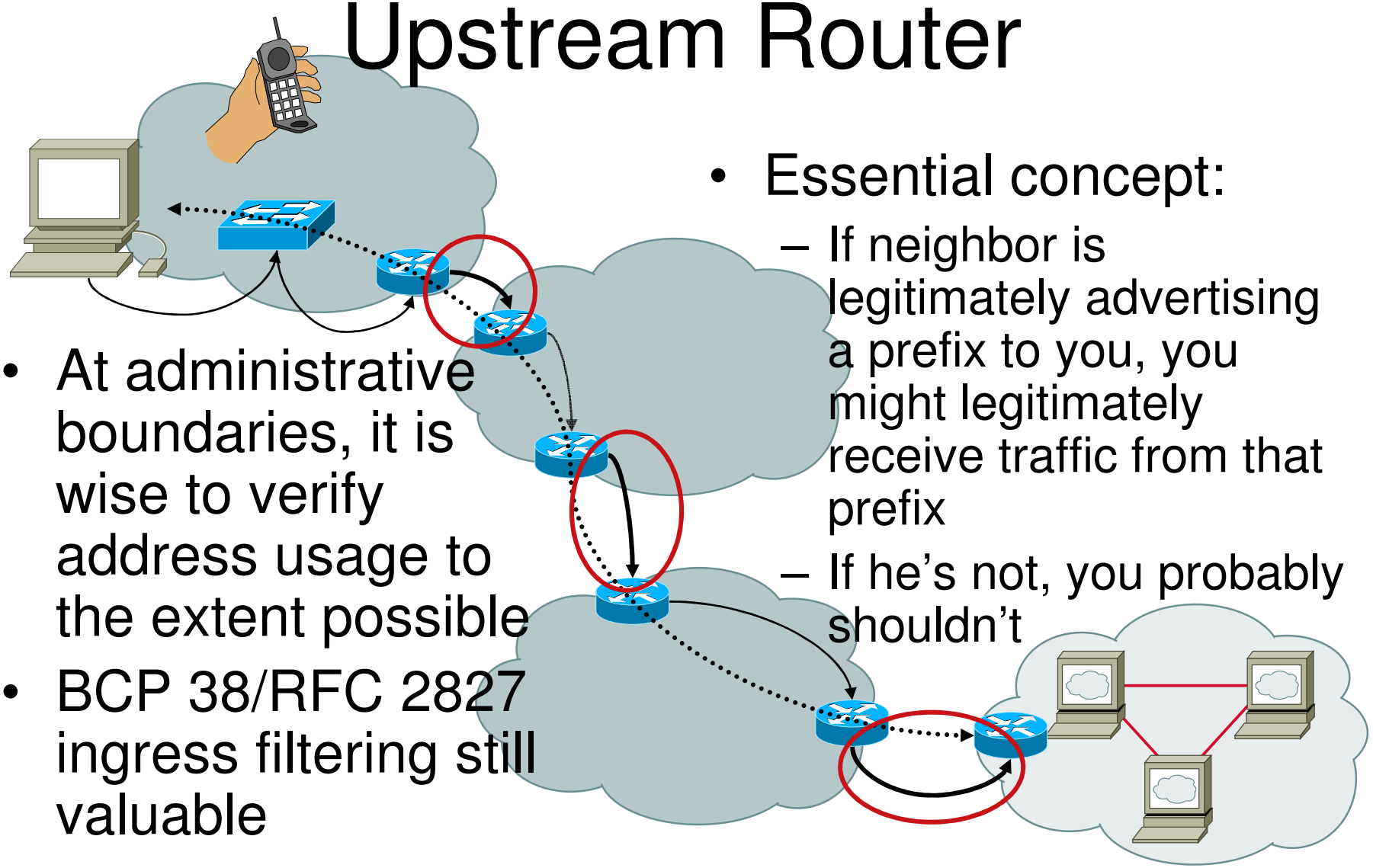


Algorithm for non-switched LANs

- Implement in host/router
- Use Neighbor Discovery Tables
  - DHCP or SAA assignment
  - ND or SeND negotiation
- Autoconfigure address:anchor filter in hosts/routers on Solicitation/Response exchange
  - Discard IP traffic that doesn't use properly negotiated addresses
- Routers:
  - Hosts still can't be protected against routers
  - Routers can protect themselves from rogue hosts



Defense in Depth: Upstream Router

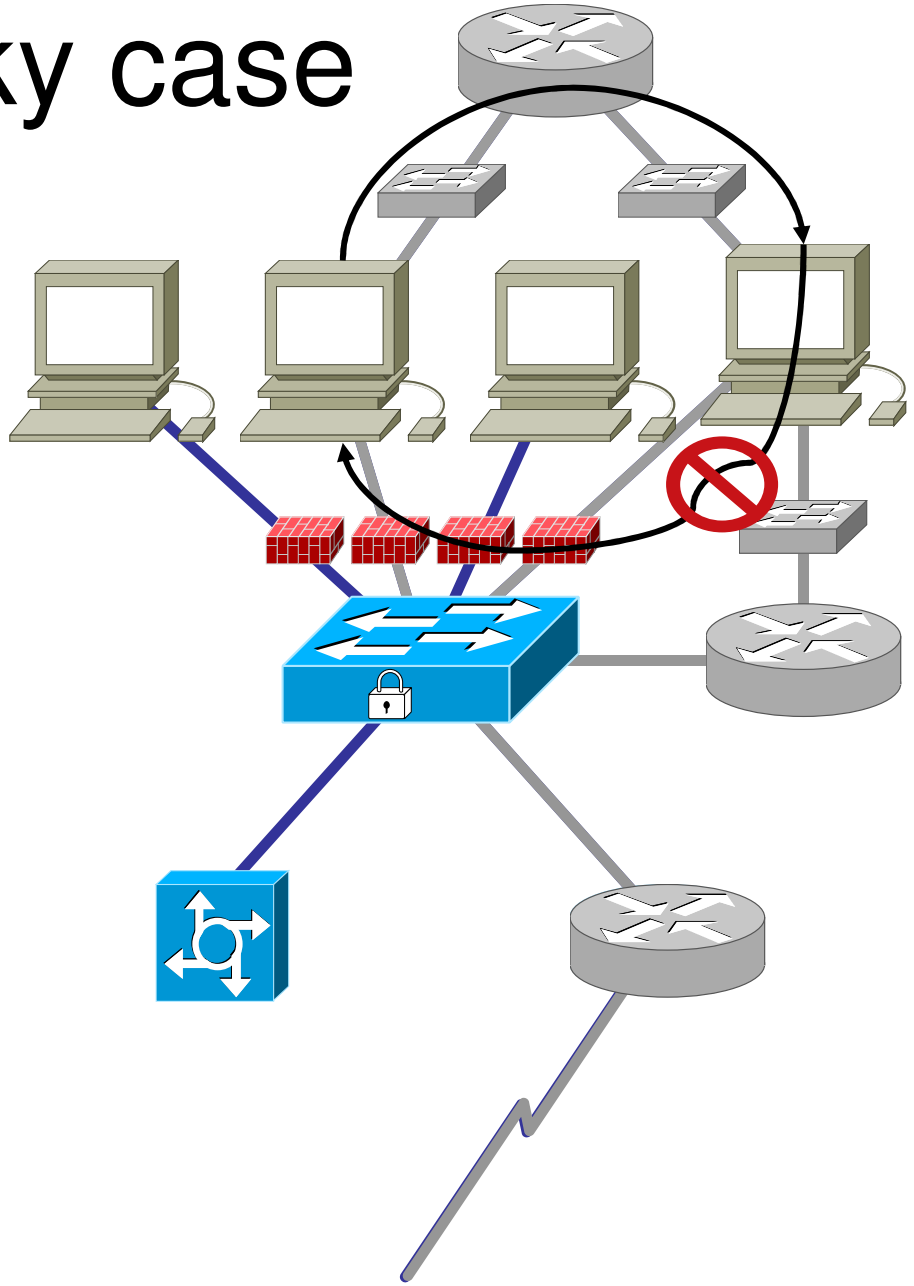


- At administrative boundaries, it is wise to verify address usage to the extent possible
- BCP 38/RFC 2827 ingress filtering still valuable

- Essential concept:
  - If neighbor is legitimately advertising a prefix to you, you might legitimately receive traffic from that prefix
  - If he's not, you probably shouldn't

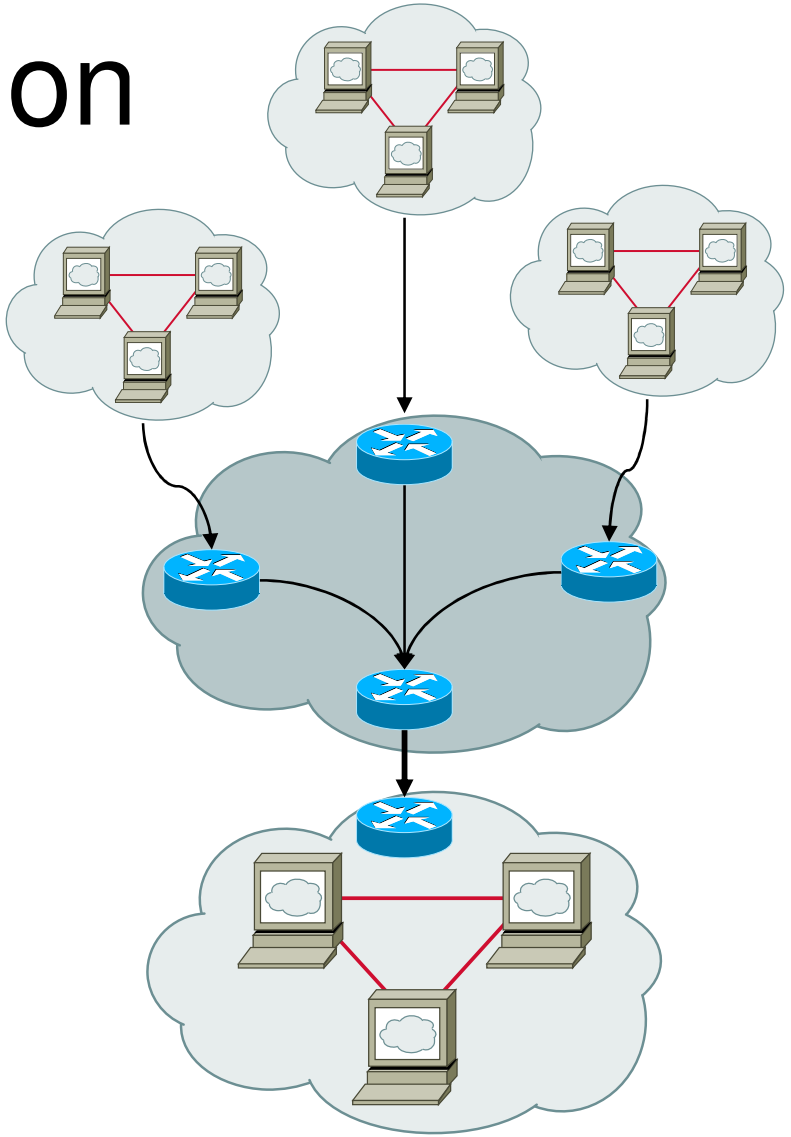
The snaky case

- Hosts may have multiple interfaces without routing between them.
  - Hosts send “from” the IP address of the interface they request on.
  - Hosts respond “from” the IP address the request was sent to
  - Host routing may not send data back the way it came
- Implication:
  - Hosts with multiple interfaces cannot be protected under these assumptions
  - But see draft-baker-6man-multiprefix-default-route



Value of source address verification

- Removes attacks that use spoofed addresses
- If I have eliminated spoofed addresses, I know that remaining attackers are using their real ones
- If I then eliminate traffic from/to bots, I free bandwidth for useful traffic
- My customers are happier.
  - –I may also gain customers if I build a reputation for having few successful attacks.



Security considerations: problem #1

- Spoofed addresses generally happen on first packet attacks
  - SYN attacks, DDOS, etc
- ND/SeND triggered by first packet - sending datagram to unknown destination
- New attacks:
  - First packet attacks on hosts still work in non-switched case
  - Host generating large number of addresses can fill neighboring host/router/switch tables

Security considerations: solution #1

- Any system MAY impose an upper bound on the number of addresses per neighbor it will store
  - If it does so, it SHOULD release old entries in a LRU fashion as is done with SYN attacks
- Any system receiving a datagram from a unknown neighbor SHOULD
  - Initiate ND/SeND to learn of the neighbor
  - Drop or queue the datagram pending ND/SeND resolution of the address
  - If queued, only then operate on it

Security considerations: Problem #2

- Stateless Address Autoconfiguration enables a “Front-running” attack:
  - Alice starts Duplicate Address Detection
  - Bob sees her probe and immediately starts using the address *without* DAD - for example, sends a LAN broadcast ping “from” that address
  - Alice is denied the use of the address

Security Considerations: Solution #2

- Don’t allow front-running attacks
- Presume:
  - Carol does not know of a system using address A
  - Alice initiates Duplicate Address Detection for the address
  - Carol receives the probe
  - Carol subsequently receives a datagram from Bob using the address
- Carol SHOULD drop Bob’s datagram with prejudice.