SAVI thoughts

<No draft>

Erik Nordmark
erik.nordmark@sun.com
Complexity vs. Features

• Is it possible to handle hosts moving between switch ports?

• Is it possible to handle hosts that failover IP address between NICs?

• Note that DHCP-based approaches get no hint that a move or failover has occurred

• Perhaps there are simpler approaches that doesn't require hooking into DHCP
Straw-man

• To show that it should be possible to find solutions which have such properties
• To see how we can extend those towards more secure mechanisms e.g., when SeND is in use
First-come-first-serve SAVI

• Switch checks each packet against list of allowed IP addresses on the port
  – IP source address, but also
  – ARP source protocol address
  – Neighbor Discovery source/target
• If not in list for port, there are two cases
  – The IP address is in the list for some other port
  – The IP address is not in any list
    • Add to list for port (FCFS)
Conflict?

- Could be that the host moved to another port, or that the host failed over the IP address to another NIC/port
- Simply check if the IP address responds on the old port
  - Means sending one or a few ICMP echo packets.
  - If no response then we remove the IP address from the old port and add it to the new
Different failover schemes

- NIC bonding
  - One NIC at a time; IP address moves
- IP Multipathing
  - Both NICs active; IP address moves
- When both NICs are active a given source IP address could be used when sending packets out both NICs
  - That would be problematic with the strawman
  - And allowing that would be a security hole
  - Require configuration of the switch in that case??
Additional security with SeND

• Instead of ICMP echo send a unicast Neighbor Solicitation and wait for a Neighbor Advertisement
  – The signature would be verified as part of SeND
Additional security without SeND
Out-of-scope in current charter

• Purpose-built keys?
  – A key or tag (random number) associated with the IP address
  – Make ICMP echo reply include a key/tag

• Moves and failovers (including concurrent use of IP source address on multiple NICs) would be more secure
  – When conflict check that the same key is used in the ICMP echo reply on the new port
  – Also send ICMP echo on the old port to handle the concurrent use case
Next Steps?

- Should we make a internet-draft out of the straw man?