Source Address Validation for Broadband Networks
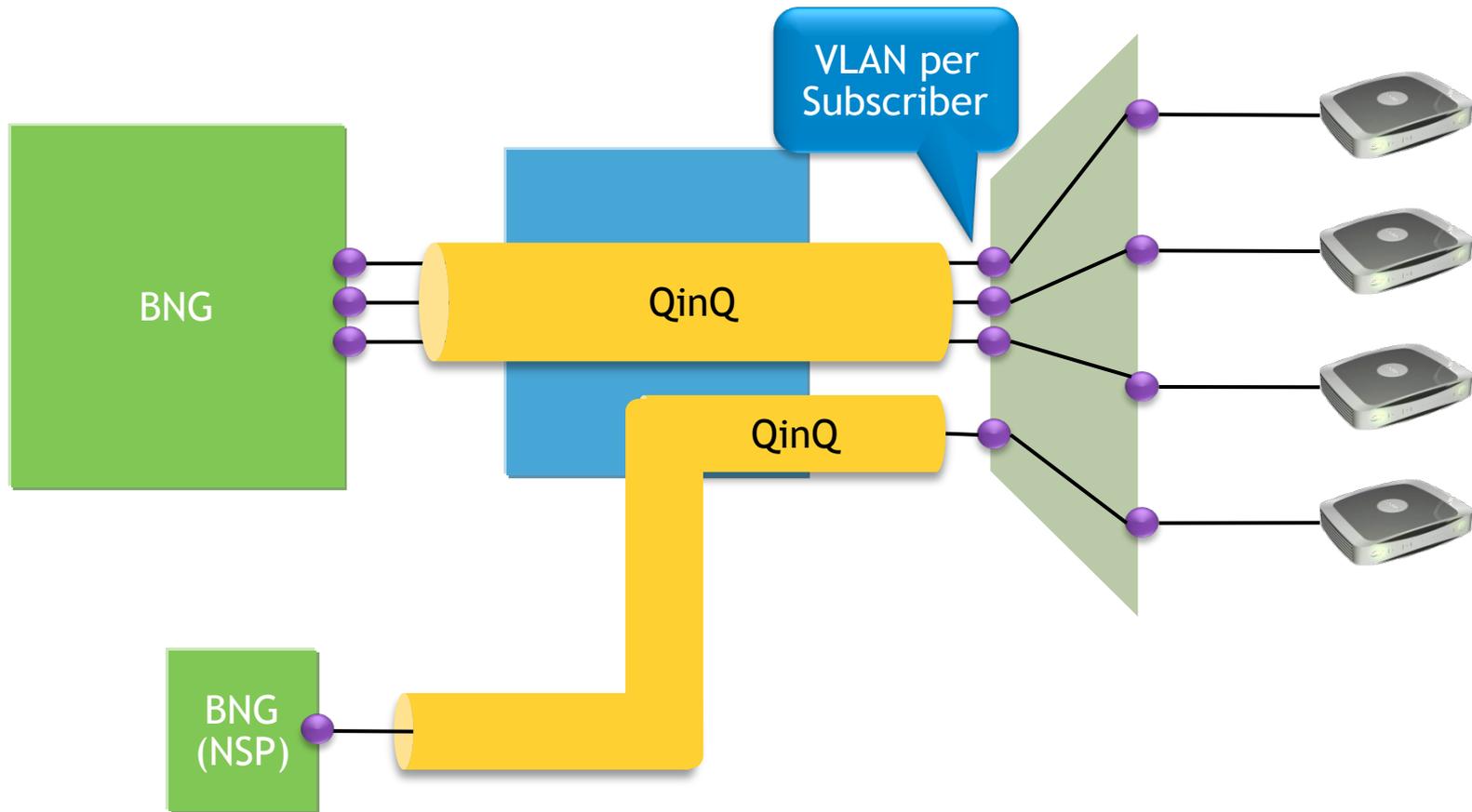
SAVI Working Group
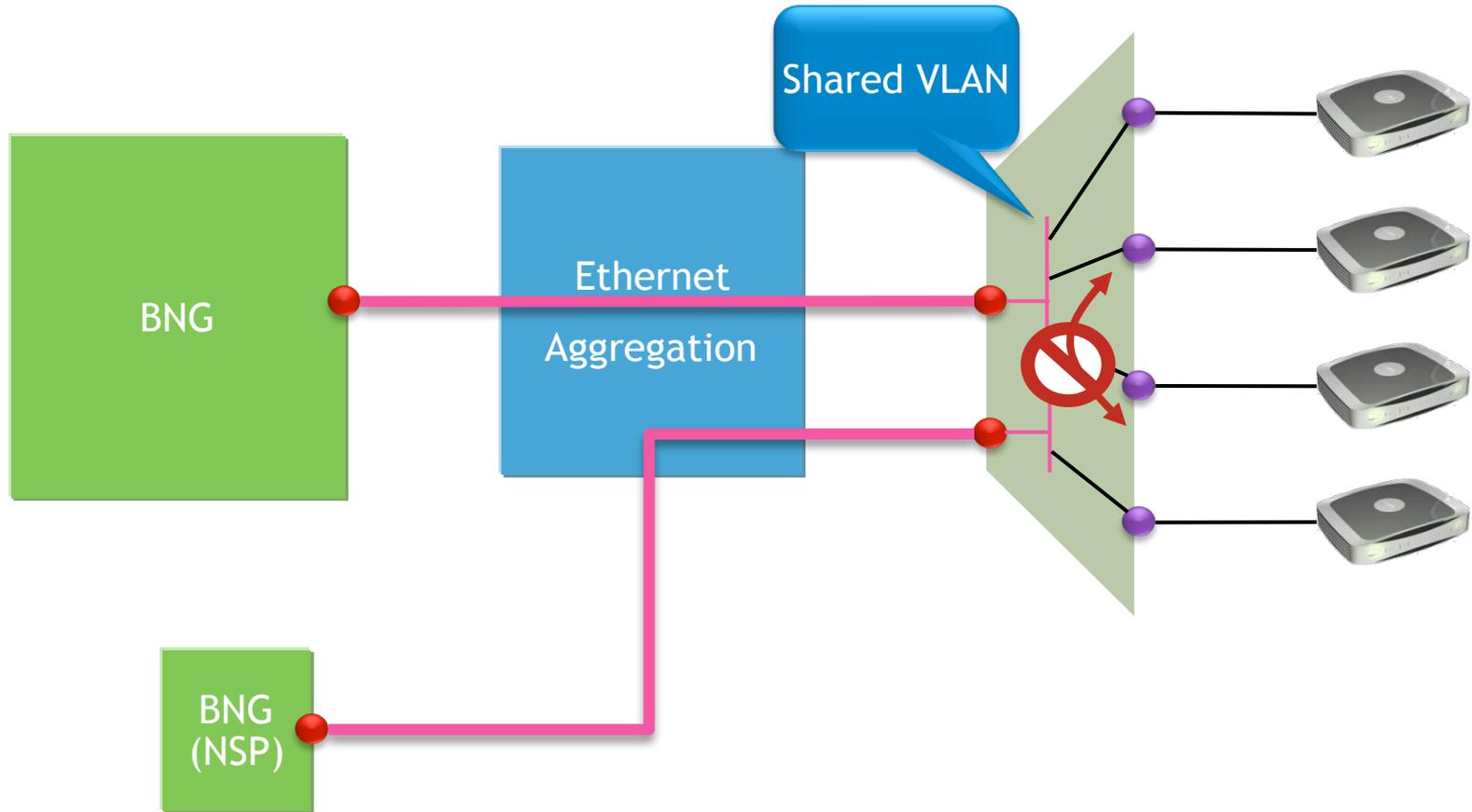
Wojciech Dec   wdec@cisco.com
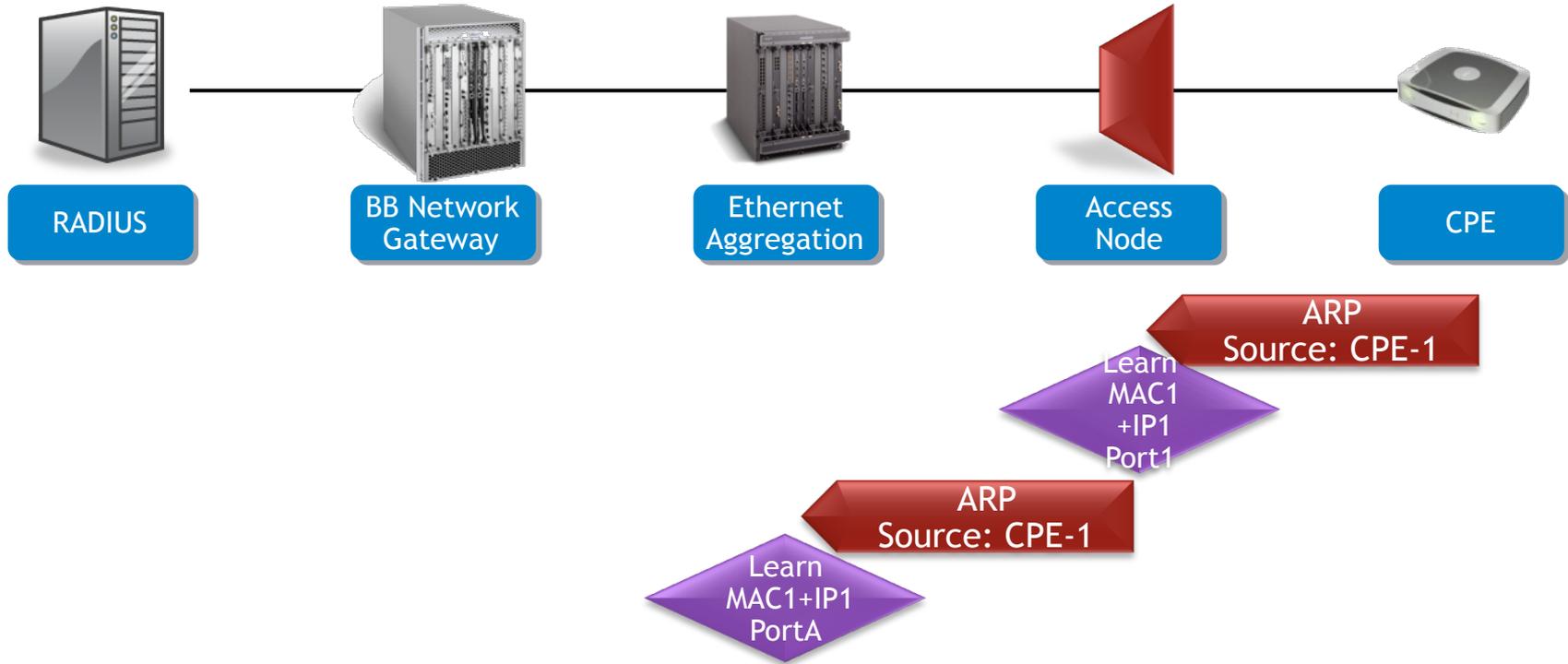**IETF75**

TR-101 1:1 Model

TR-101 N:1 Model

3

MAC+IP Anti-Spoofing

RADIUS

BB Network Gateway

Ethernet Aggregation

Access Node

CPE

ARP
Source: CPE-1

Learn
MAC1
+IP1
Port1

ARP
Source: CPE-1

Learn
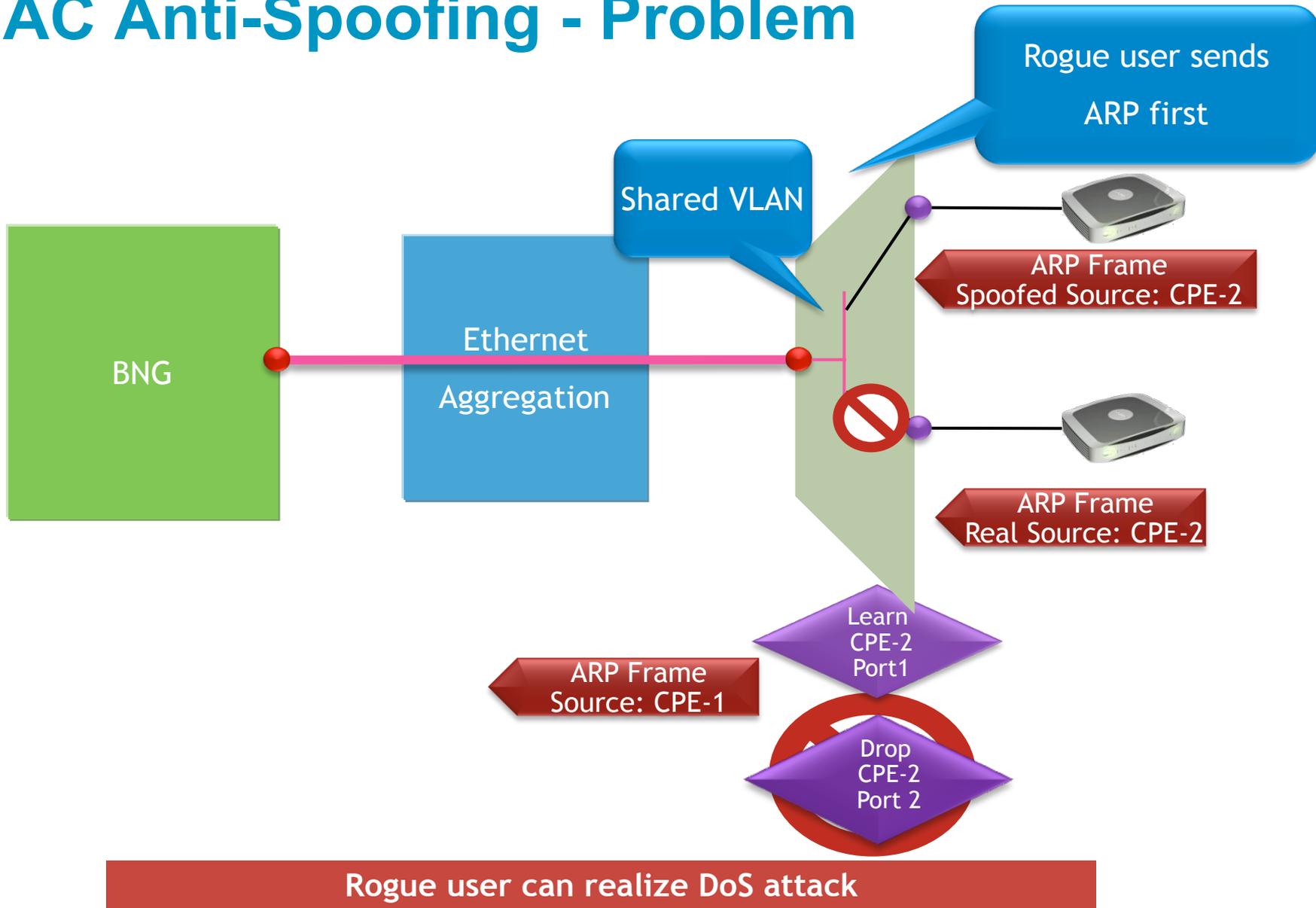MAC1+IP1
PortA

Once learnt, only the designated ports will forward Ethernet frames with the learnt source MAC+IP address

4 | Presentation Title | Month 2007

MAC Anti-Spoofing - Problem

Rogue user sends ARP first

Shared VLAN

BNG

Ethernet Aggregation

ARP Frame
Spoofed Source: CPE-2

ARP Frame
Real Source: CPE-2

Learn
CPE-2
Port1

ARP Frame
Source: CPE-1

Drop
CPE-2
Port 2

Rogue user can realize DoS attack

DHCP(v4) Anti-Spoofing (Access Node)

RADIUS   **BB Network Gateway**   **Ethernet Aggregation**   **Access Node**   **CPE**

DHCP Discover

DHCP Offer

DHCP Request

DHCP Ack

Learn MAC + IP

Learn MAC + IP

DHCP Ack
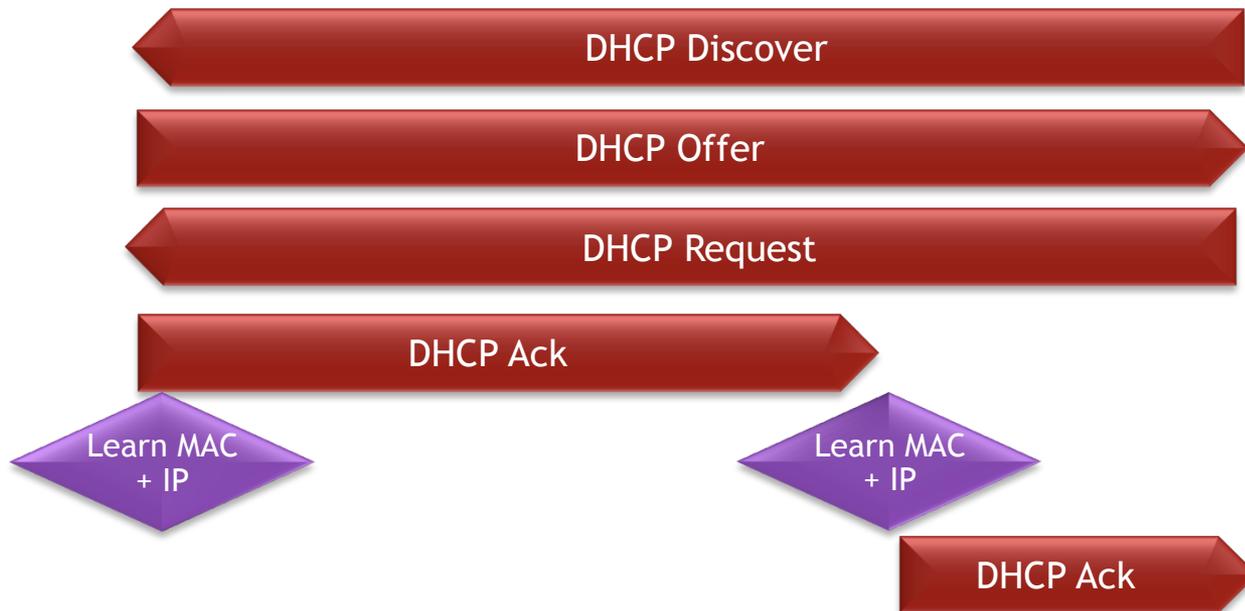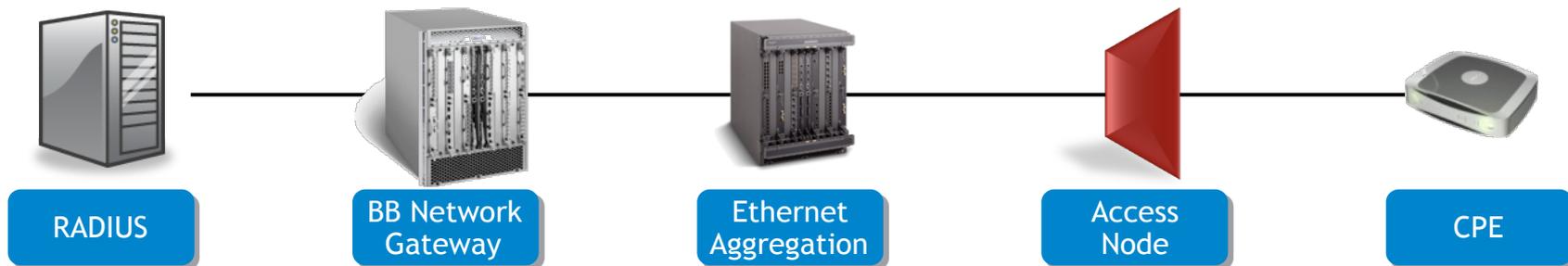
No broadcast traffic sent downstream by BNG (eg ARP)

High Level Requirements*

- Generally required (GR):
  - Allow only expected IP control protocol traffic on user port before user authorization
  - Allow use of dynamic address assignment procedures towards users
  - Per user/line IP address/prefix assignment
  - Prevent user spoofing BNG
  - Prevent user spoofing another user
  - Use standards based extensions to common protocol toolset (minimize introduction of new exotic protocols)
- Also Required (AR):
  - Protection against MAC spoofing (FCFS)
  - Detection/prevention of duplicate MAC address
  - Limit number of IP+MAC combinations on a port
  - Port locked to using authorized IP address(es) and MAC(s)
- Nice to have (NH):
  - The (AR) requirements set also for 1-1 VLAN
  - Throttle control protocol traffic
- IPv6 Specific**
  - Support for DHCPv6 based global address assignment to users
  - Support for SLAAC based global address assignment to users
  - Way of handling duplicate link locals; detection; prevention; resolution.
- *NOTE: There isn't an expectation for SAVI to resolve all of these
- **NOTE: Besides DHCP-PD, no firm consensus exists in the BBF on the adoption of these methods.