Embedding VNTag functionality into the SecTAG

Paul Congdon

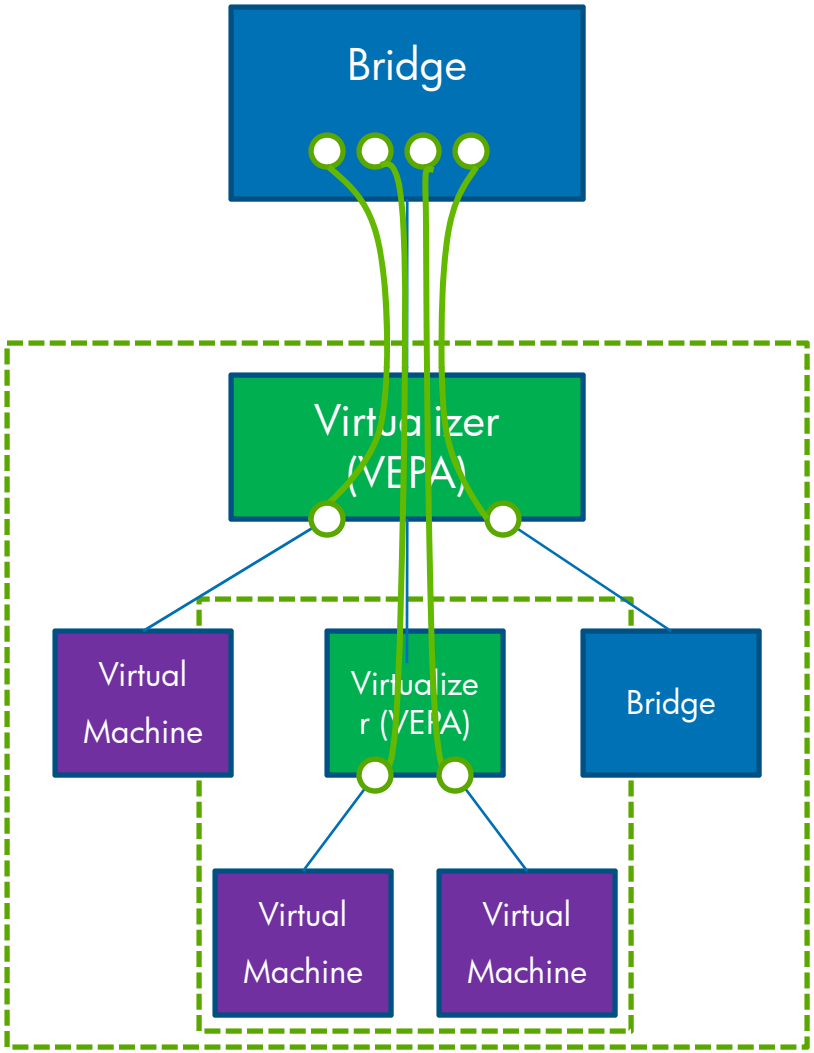
IEEE 802.1 Interim – New Orleans

1/15/09

Objectives

- Show how the capability proposed by the VNTag can be included in the MACSec SecTAG.
- Demonstrate the advantages of using the SecTAG over creating an entirely new tag
- Discuss compatibility of SecTAG changes with current MACSec specification

Background



Existing MACSec use model

- MACSec has a model for virtual ports today
- Could be used 'without' crypto for the same purpose

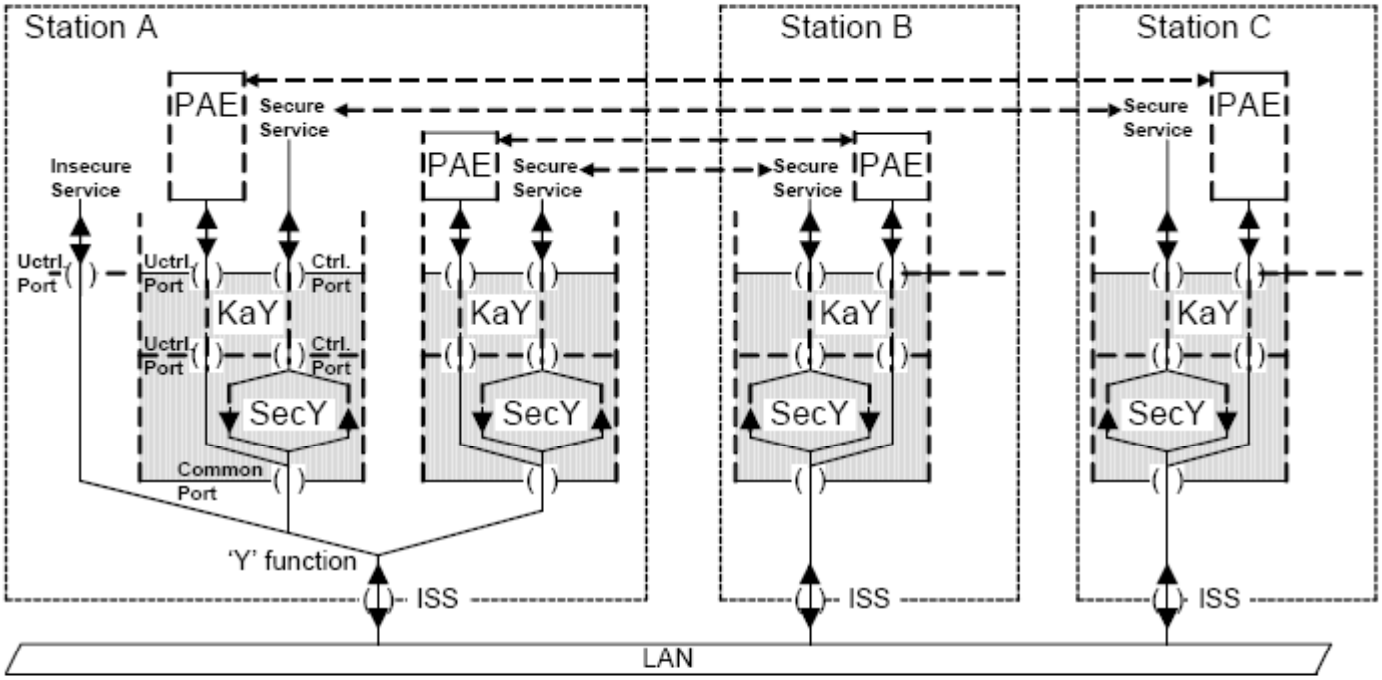
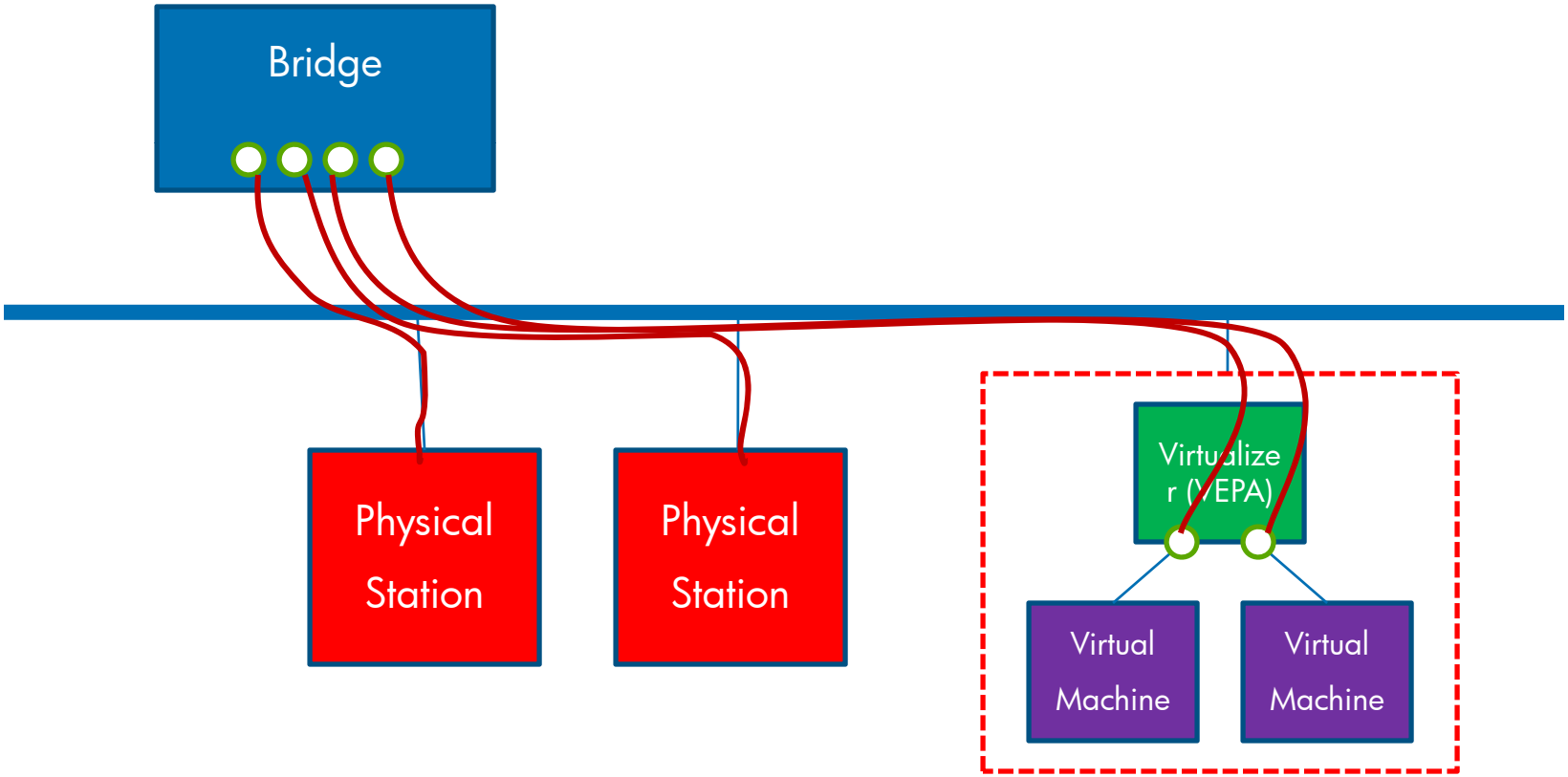


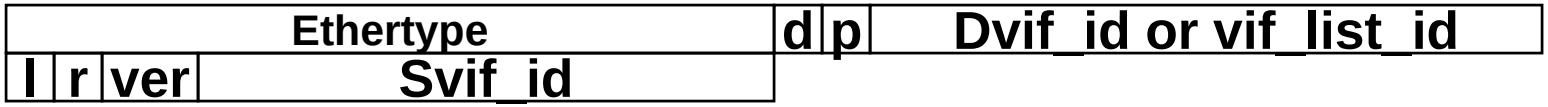
Figure 11-15—An example multi-access LAN

Current Use Model

Bridge Virtual Ports



VNTag Proposal

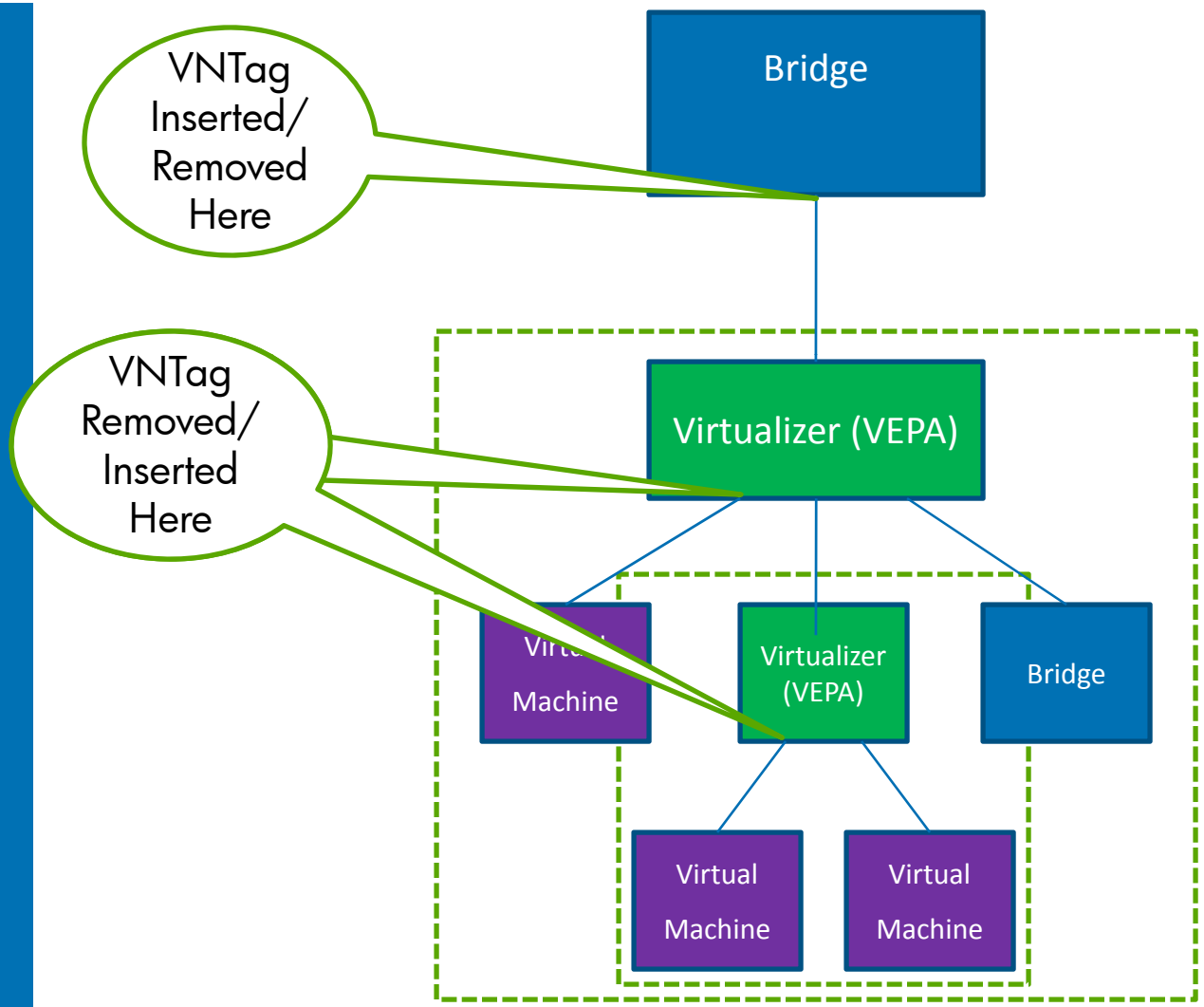


Ethertype:	**TBD, identifies the VNTag**
d:	**Direction, 0 indicates that the frame is traveling from the IV to the bridge. 1 indicates the frame is traveling from the bridge to the IV**
p:	**Pointer: 1 indicates that a vif_list_id is included in the tag. 0 indicates that a Dvif_id is included in the frame**
vif_list_id:	**Pointer to a list of downlink ports to which this frame is to be forwarded (replicated)**
Dvif_id:	**Destination vif_id of the port to which this frame is to be forwarded. Two most significant bits are reserved.**

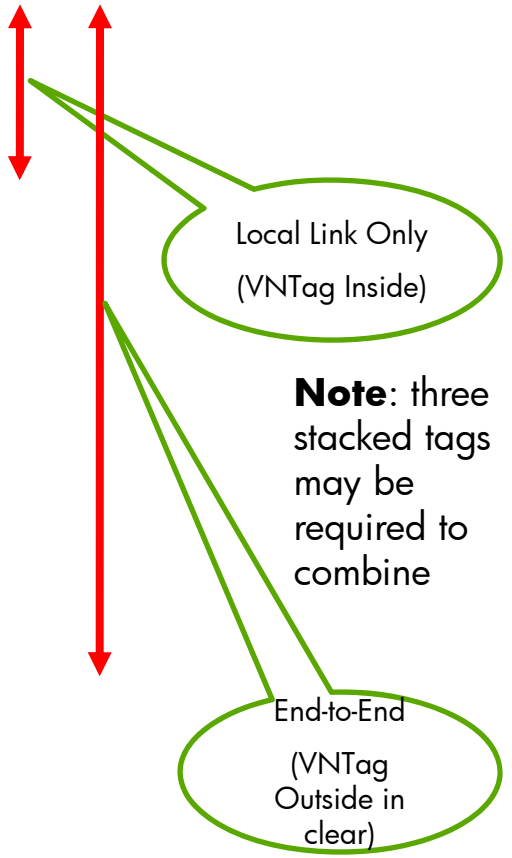
Note: the Dvif_id / vif_list_id field is reserved if d is 0.

l:	**Looped: 1 indicates that this is a multicast frame that was forwarded out the bridge port on which it was received. In this case, the IV must check the Svif_id and filter the frame from the corresponding port**
r:	**reserved**
ver:	**Version of this tag, set to 0**
Svif_id	**The vif_id of the downlink port that received this frame from the VNIC (i.e. the port that added the VNTag). This field is reserved if d=1 and l=0.**

Proposed VNTag Scope



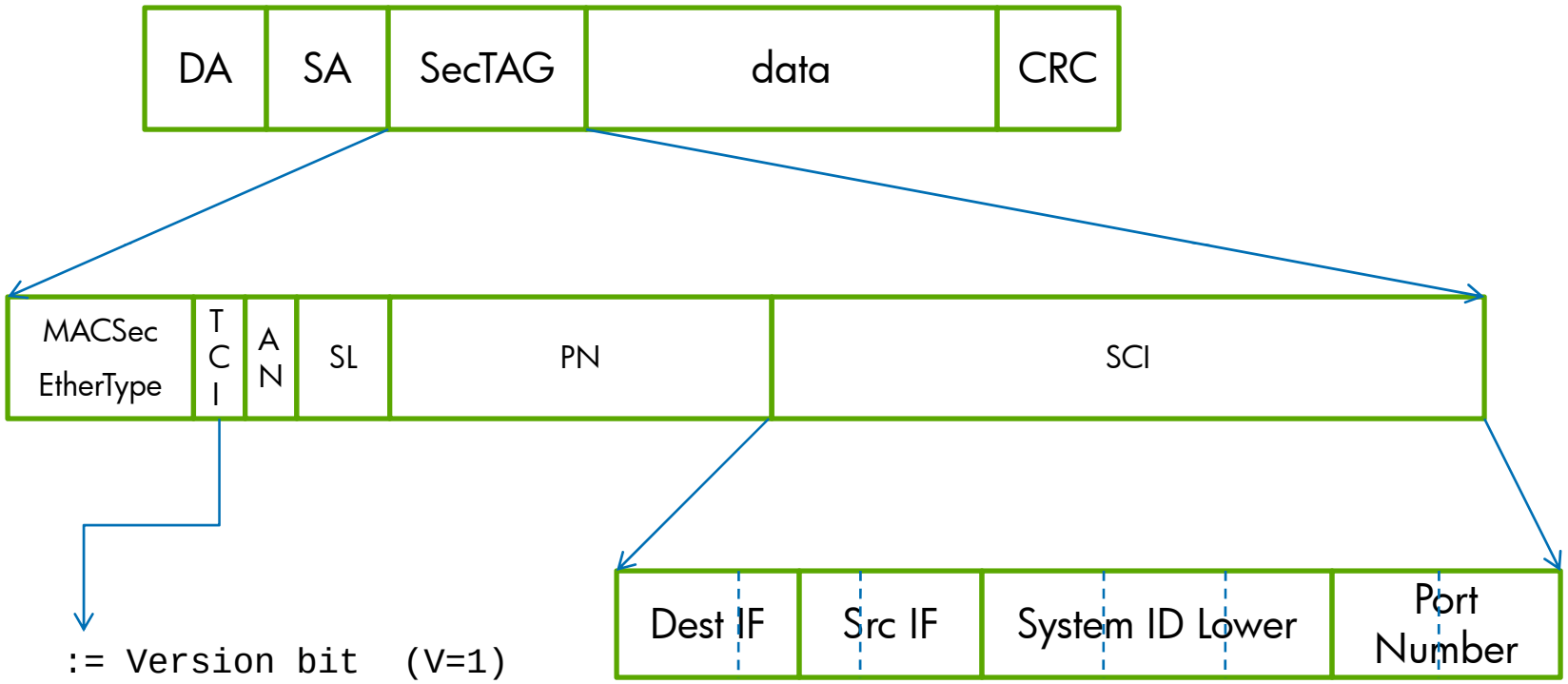
Security + VNTag



Note: three stacked tags may be required to combine

hp invent

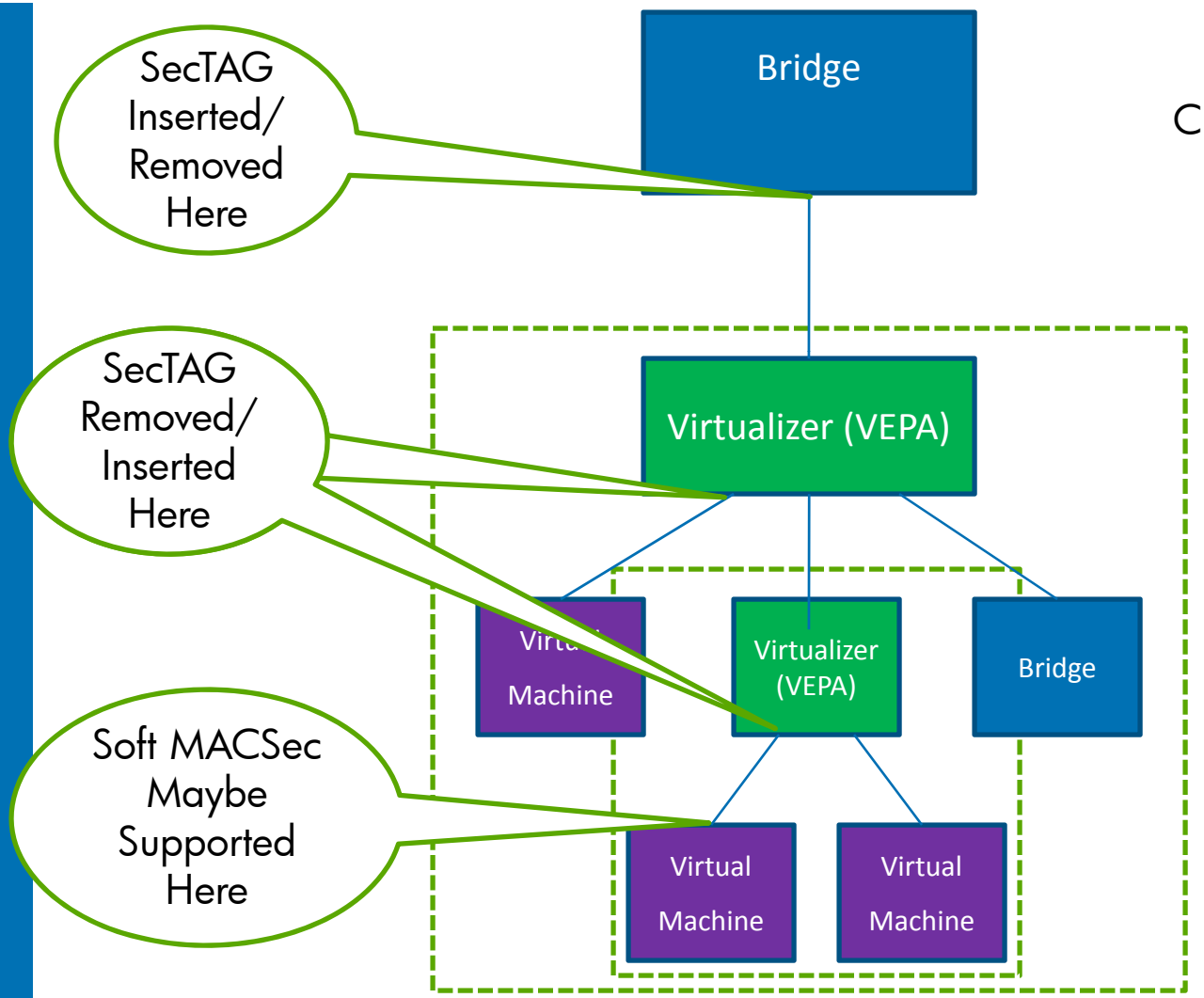
VNTag embedded in SECTag



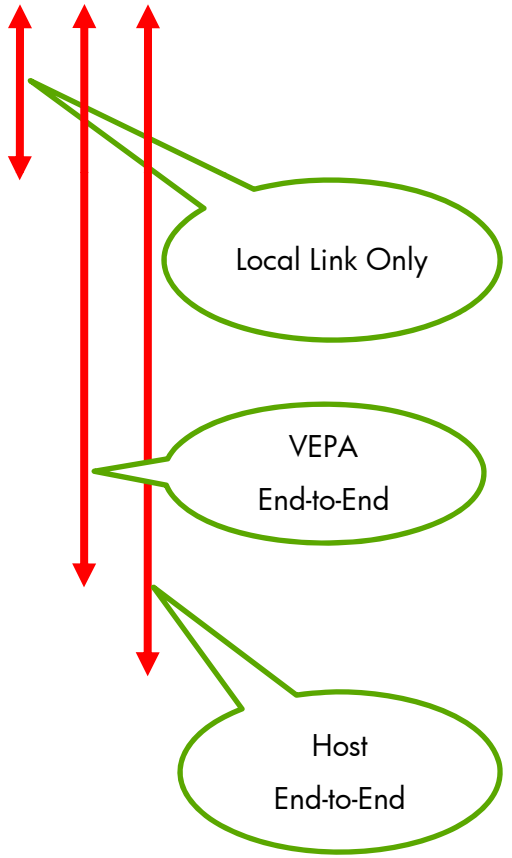

```
V   := Version bit  (V=1)
ES  := End-Station  (ES=1)
SC  := SCI included (SC=1)
SCB := Single copy broadcast (SCB=1)
E   := Encryption   (E=0)
C   := Changed Text (C=0)
AN  := Association Number (AN=00)
```

SecTAG Scope

Always just a single tag



Crypto Scope Options



Advantages of SECTag for virtualization

- Works exactly like VNTag when not using crypto
- Current use of MACSec supports tagless VEPA mode
- Bridge only needs one method of identifying virtual ports
- Supports ability to augment virtual port-ids with a 'secure' port-ids and use crypto to protect them
- Allows end-points to create multiple virtual ports within their domain (as done today)
- Only uses one tag header
- Does not leave parts of the frame unprotected and detects any modifications
- Enables convenient 'inline' implementations of MACSec crypto

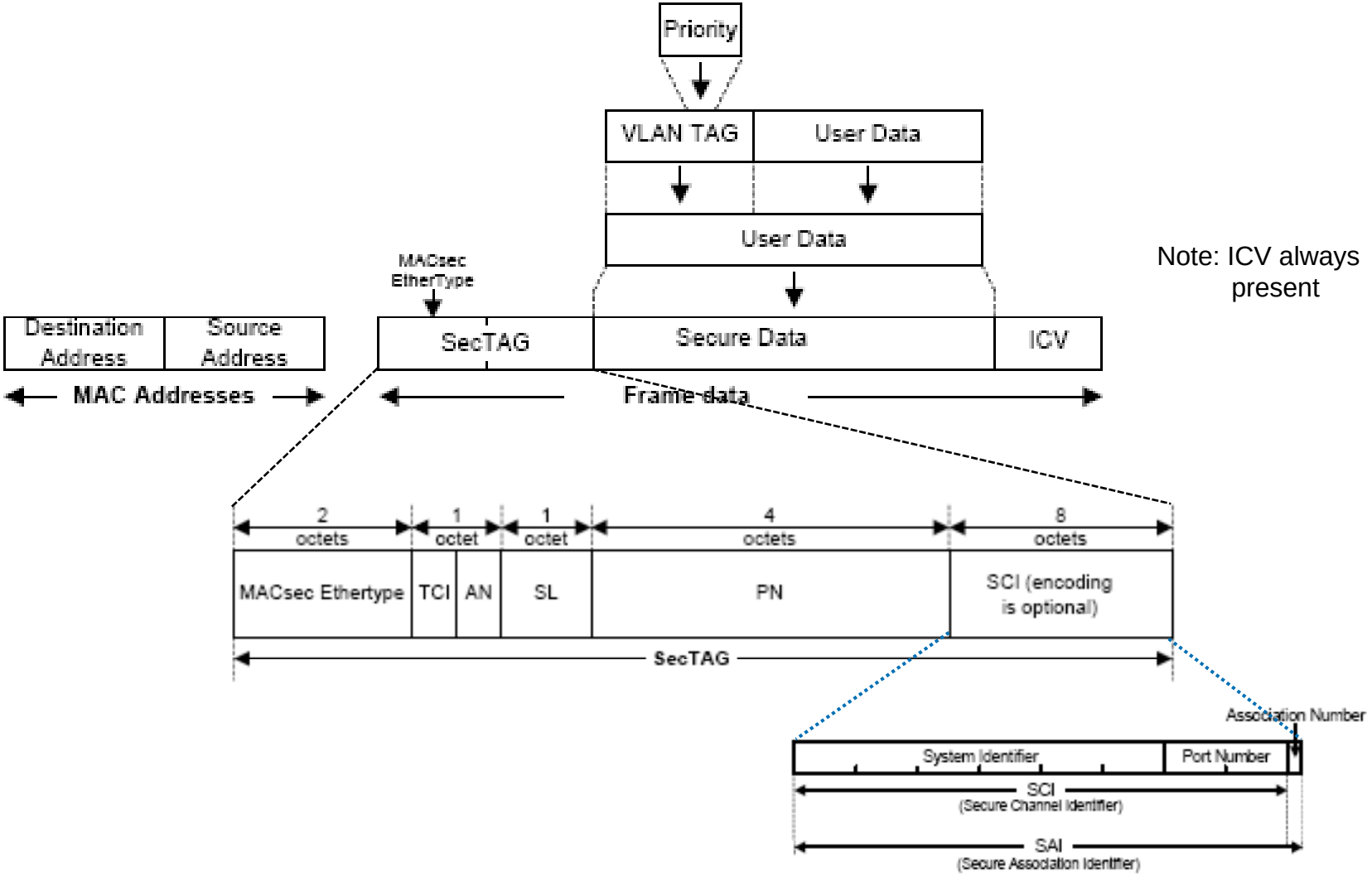
Compatibility with Existing MACSec

- Existing MACSec compatible with tagless VEPA
- Existing MACSec establishes bridge virtual ports
  - Identified by v=0
  - VEPA must map full SCI to virtual interface
- SecTAG for virtualization has structured SCI
  - Identified by v=1
  - Entity inserting SecTAG must be told what SCI to use
- SecTAG for virtualization can share inline crypto function
  - Identified by v=1
  - SecTAG is already inserted
- Current bump-in-the-wire MACSec may not expect SecTAG to already have been appended
  - May be identified by v=1

Conclusions

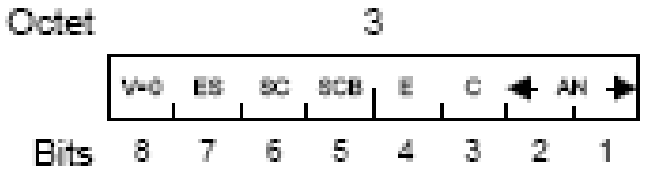
- A single method of identifying virtual ports is possible using just the SecTAG
- SecTAG without crypto is equivalent to VNTag with slightly more bits of overhead
- There are several flexible ways to 'turn-on' security in addition
- Compatible with existing MACSec implementations (v=0).
- Modest changes to 802.1AE required (see: new-congdon-vepa-1108-v01.pdf in Docs 2008)

MACSec Frames



Note: ICV always present

SecTAG Control Information




```
V   := Version bit (v=0)
ES  := End-Station
SC  := SCI included
SCB := Single copy broadcast (EPON)
E   := Encryption
C   := Changed Text
AN  := Association Number
```

- Version is 0, but if necessary could bump to 1 and define additional bits (not desired)
- End-Station bit needs to be 0 to allow SCI to be used to encode source virtual port number
- SCI must be included to allow 8 bytes of SCI to be included
- Single copy broadcast can only be used when SC is 0, but we need SC to encode port group
- Encryption may or may not be used as desired, but ICV is always included
- Changed Text is only set if the user data has been encrypted