ProCurve Networking
HP Innovation

Multiple CAs per port

Paul Congdon
March 14, 2005

hp invent

Problem Space

ProCurve Networking
HP Innovation

Many requests for multiple 802.1X supplicants per physical 802.3 port

It is possible to authenticate multiple supplicants on shared media (e.g. 802.11)

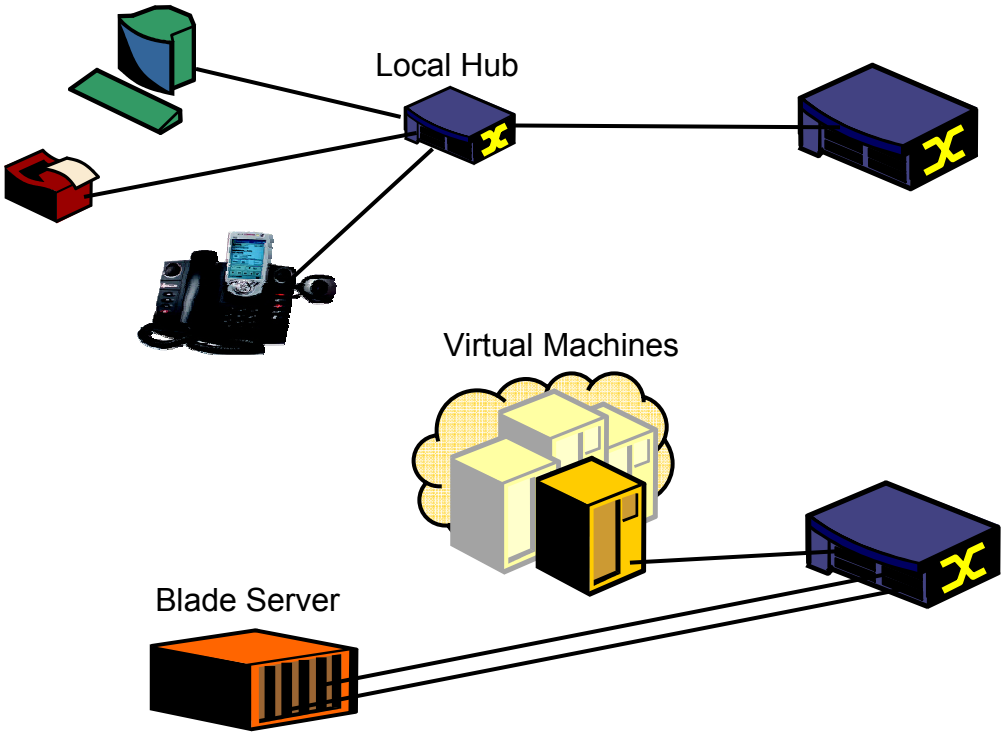
However, after authentication there is no security without encryption (enter MACSec)

Different devices on the shared segment may have different security requirements

Current .1AE draft only supports a single CA per physical port so all secured devices must be in the same group

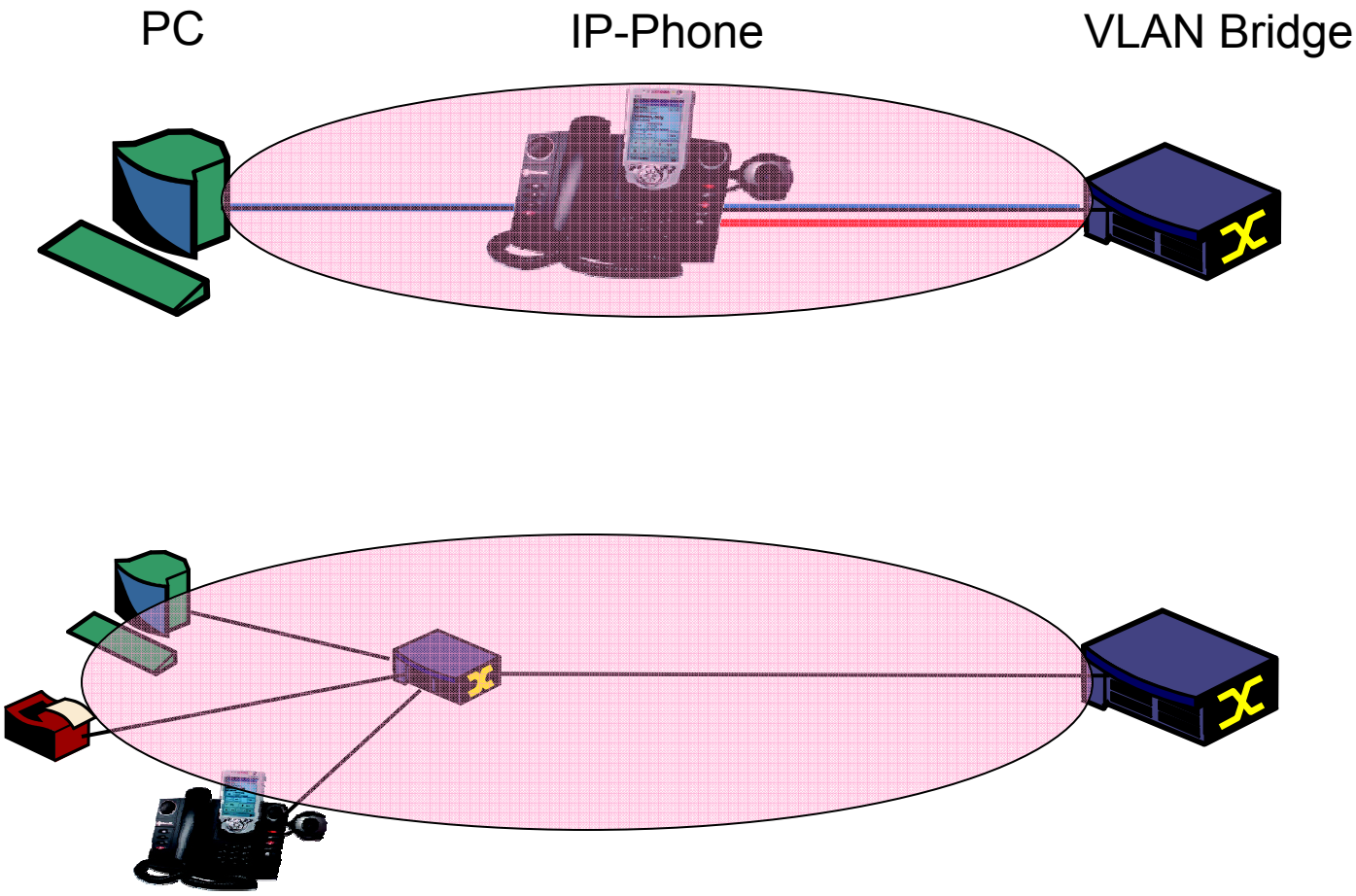
Some Simple Problem Scenarios

- Many IP Phones come with a 2-port 'bridge-like' device to avoid additional wire.
- These IP Phones typically do NOT act like authenticators to the downstream PC.



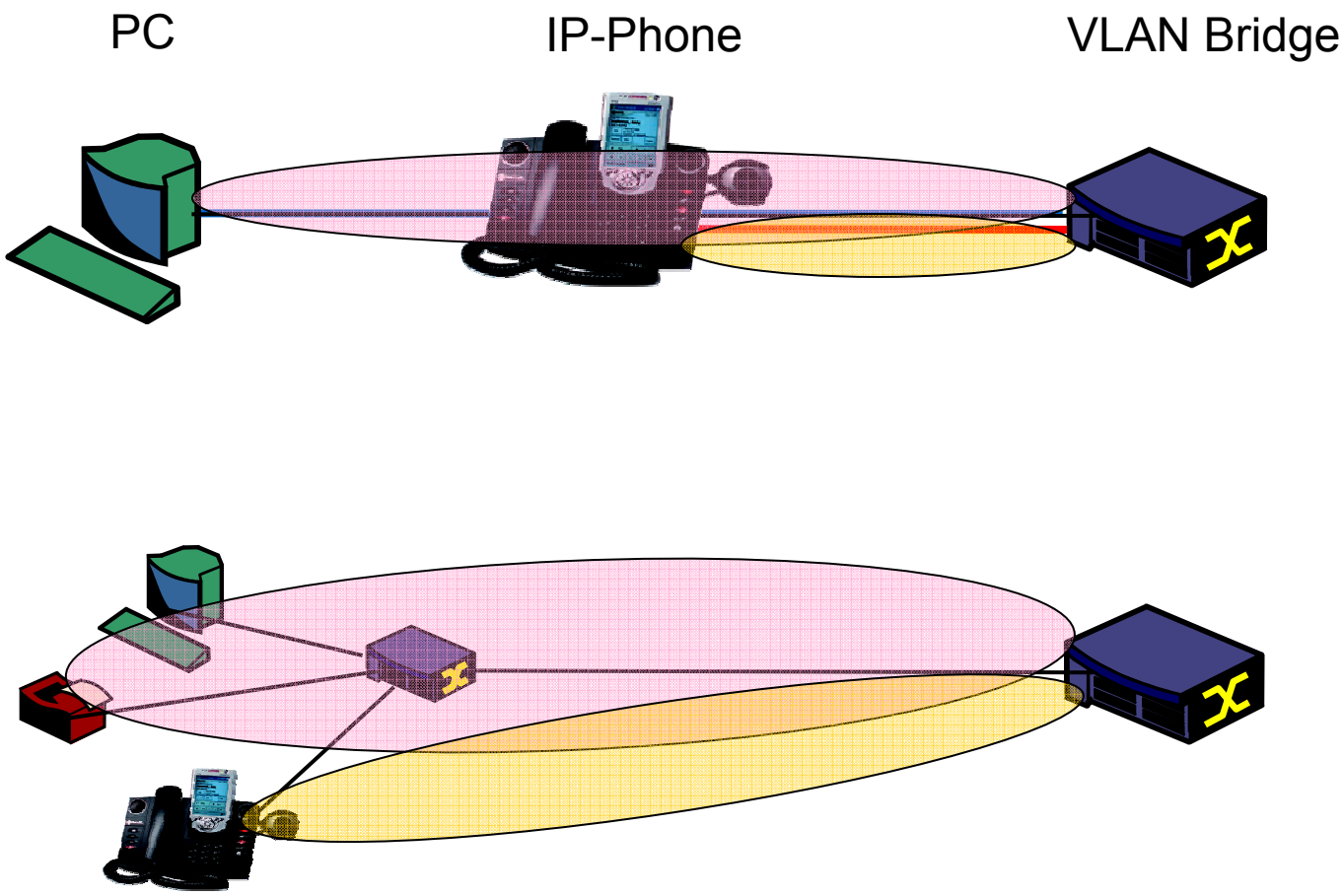
- Small local unmanaged hubs/switches used for port expansion in the work area.
- Virtual Machines share common hardware but appear as separate servers
- Blade servers aggregate multiple distinct servers with internal unmanaged switches

MACSec puts everyone in the same group



MACSec with Multiple CAs provides separation

ProCurve Networking
HP Innovation



Why not just use VLANs?

ProCurve Networking
HP Innovation

(+) Often very little desire to bridge between different secured devices

(+) VLAN forward is easy. Does not create virtual ports

(+) VLAN tag provides a nice 'handle' to identify CA

(-) VLAN aware end-points are not common
(…but neither is MACSec)

(-) Protocol VLANs (and other non-tagged VLAN types) don't work

(-) VLAN Tag is currently inside MSDU

(-) Some end-points might want to use VLANs

(-) Doesn't scale well in bridge-to-bridge case and we already have this for .1ad bridges

(-) Would require MACSec shim between ISS and EISS and lots of key management

(-) RADIUS likes to provision 'ports'

But what does multiple CAs do to bridges?

ProCurve Networking
HP Innovation

Fundamentally requires the creation of 'virtual ports' attached to 'emulated LANs'

Requires a method for identifying the virtual port traffic

- Not another 'tag' please
- Traditional 802.3 doesn't have an LLID

Forwarding to multiple 'virtual ports' on the same physical port might be hard to do:

- Flooding requires packet replication
  - This is true already for physical ports already
- No model for a shared broadcast channel port in 802.1 (yet)

How can this be made to work?

ProCurve Networking
HP Innovation

Define how multiple CAs are provisioned and maintained

- Largely an .1af issue (may need multiple .1af instances)

Use the SCI as a look-up for CA instance

- Make SCI use mandatory
- Require a unique Port Identifier component

Define how controlled and uncontrolled ports relate

- See following diagrams

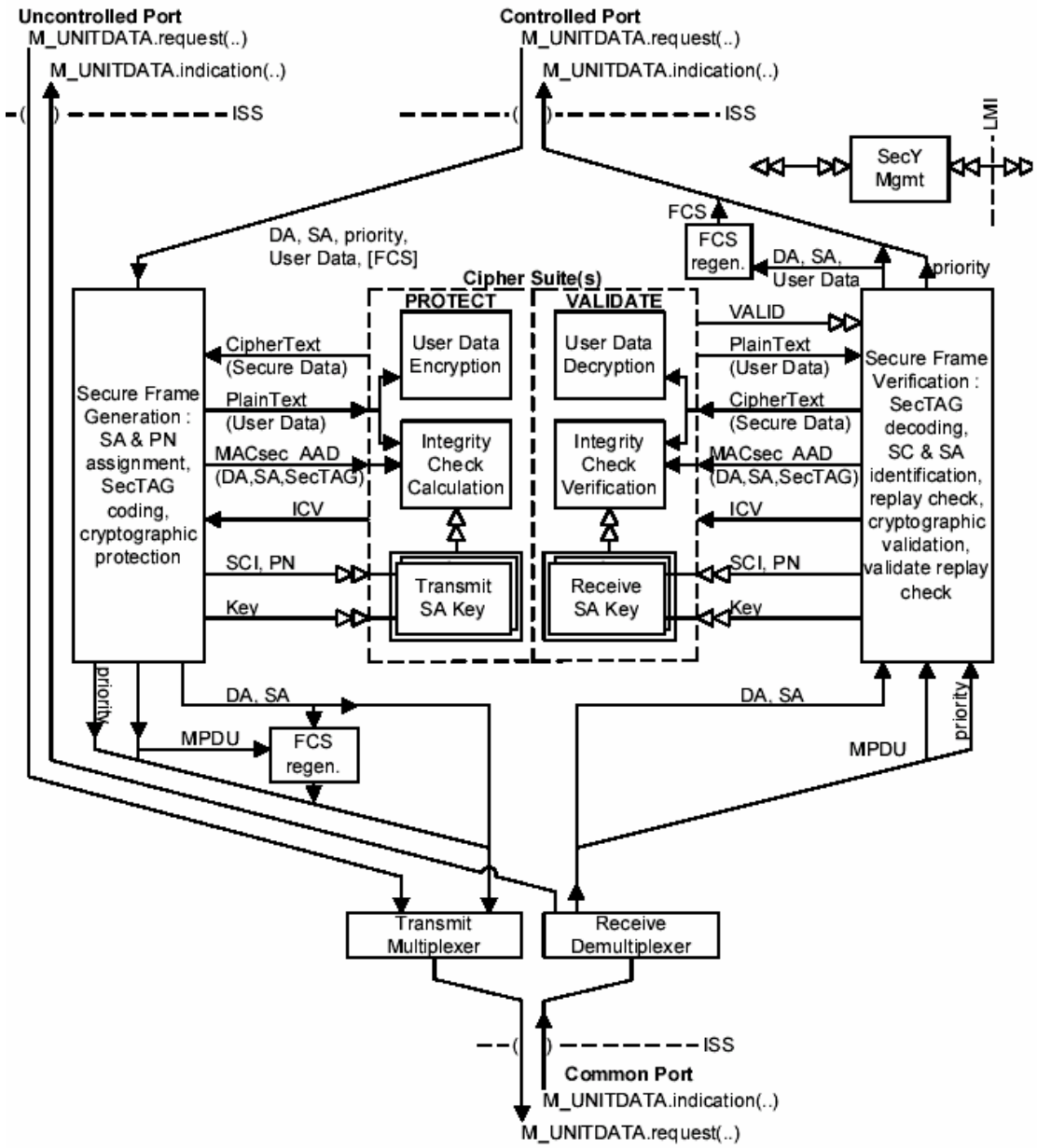
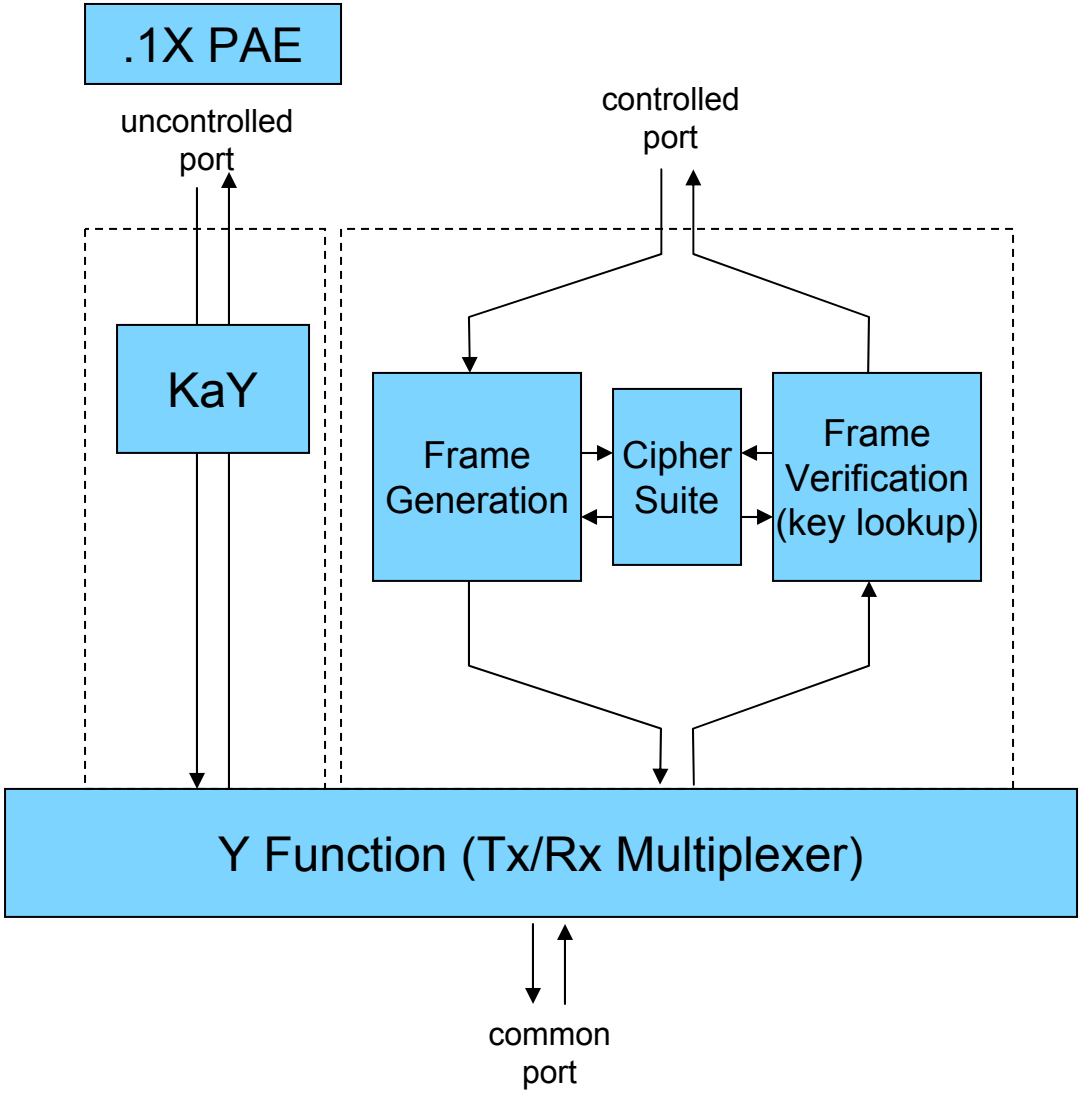


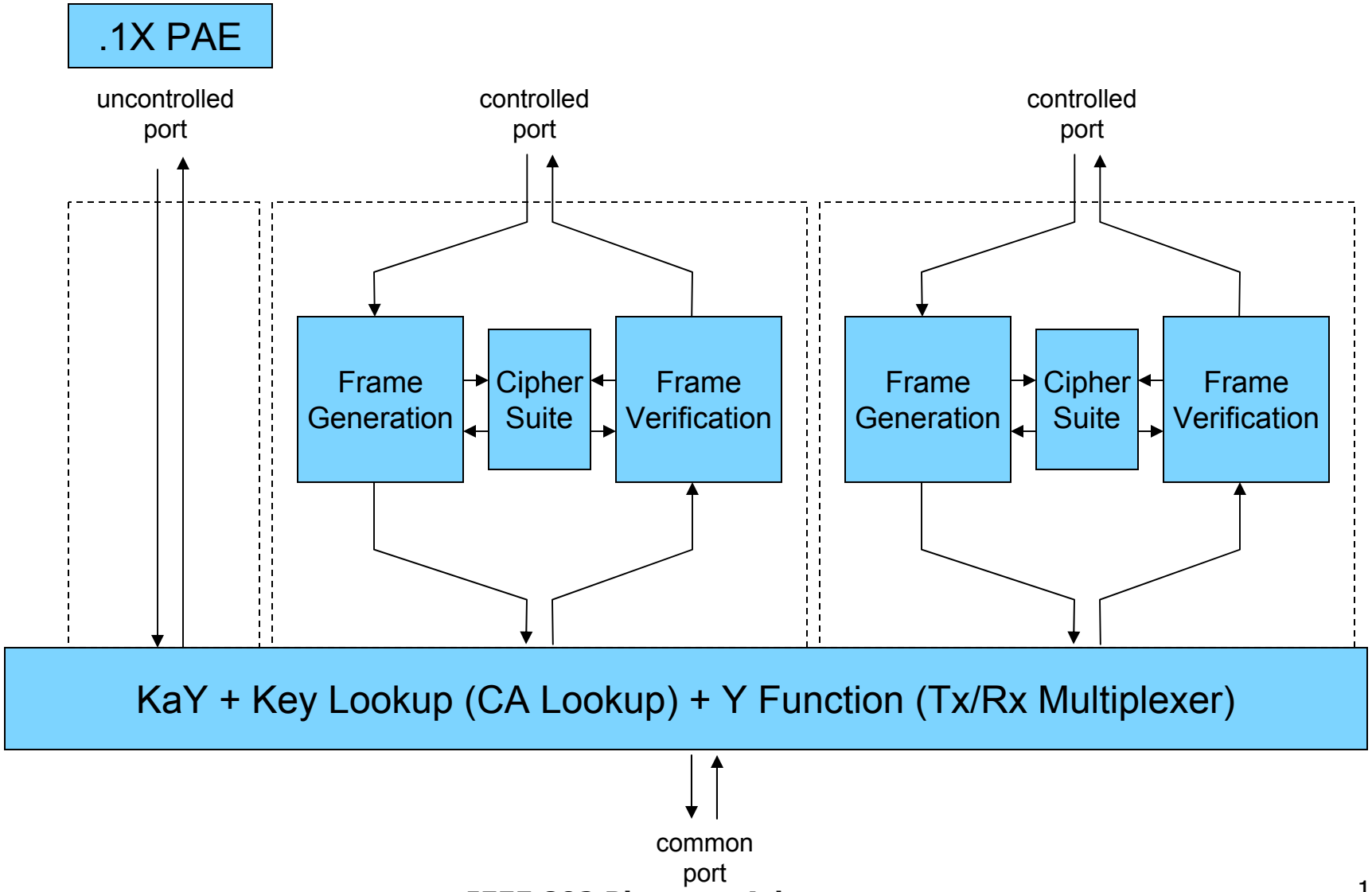
Figure 10-3—SecY architecture and operation

Current Arch Redrawn



Instantiating Multiple SecYs

ProCurve Networking
HP Innovation



ISS/EISS Stack with MACSec

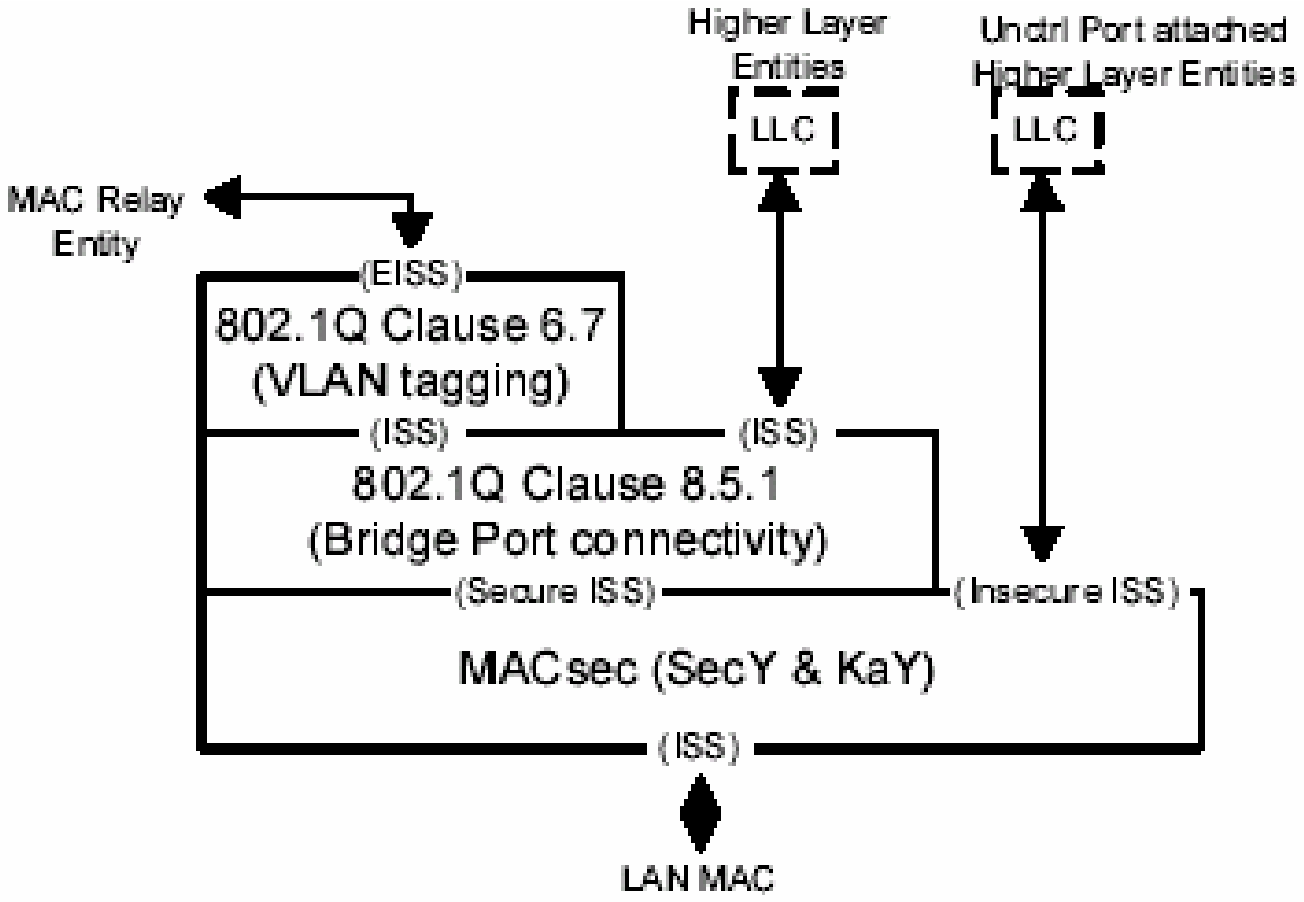
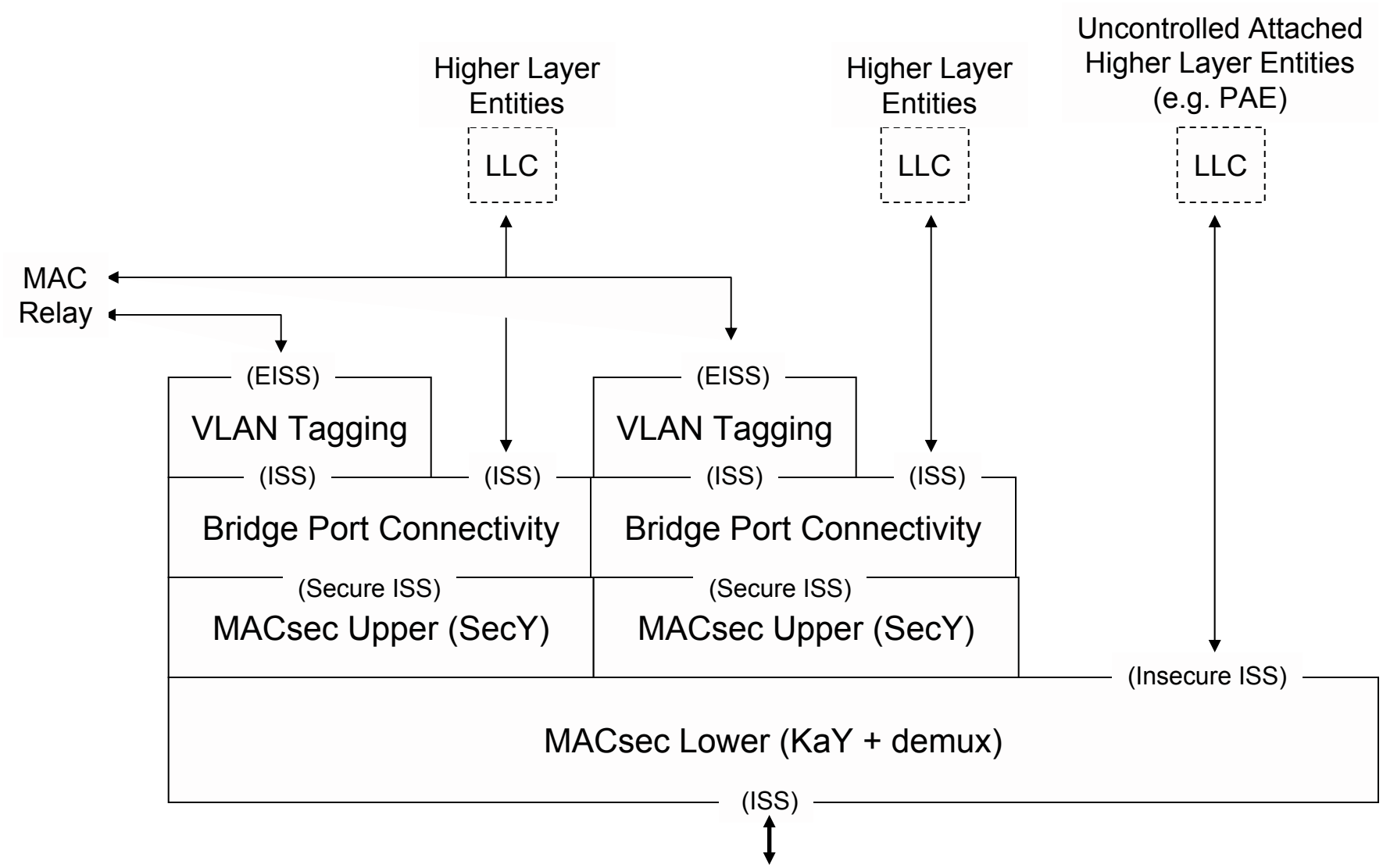


Figure 11-7— 802.1Q VLAN-aware Bridge Port with MACsec

Virtual Ports in a Bridge

ProCurve Networking
HP Innovation



Response to Note-1 of 7.2

ProCurve Networking
HP Innovation

turning security on or off radically changes the network connectivity... Staged deployment scenarios using integrity protection without validation become impossible.

- A SecY is only in a single CA, thus other CAs do not impact connectivity.

...if the keys for one CA ever coincide with or overlap the other, the CAs will merge for a period - and guarding against this problem simply exports a new and very unusual problem to key agreement.

- If this happens .1af is broken anyway

Third such a scheme requires explicit support from key agreement, which will have to carry an explicit multiplexing value to separate key agreement for the two separate instances.

- Yes, this is true

Fourth such a scheme requires explicit configuration of the ports attached to each "separate" CA if bridging is going to be provided between the instances.

- Yes, but no different than other dynamically created ports (e.g. LinkAgg)
- Can be part of the port authorization process

Fifth such a scheme will result in a high error rate, thus masking any other problems.

- No, multiplexing function delivers encrypted frames to the right instance of the cipher

We need to stick to one SecY being in one CA on one instance of an underlying service as far as possible.

- Proposal is consistent with a single SecY in one CA

Issues to address

ProCurve Networking
HP Innovation

How to multiplex instances of .1af

- Add a CA-ID to KSP?
- Does CA-ID need to be globally unique or just link unique?
- Use default value of CA-ID=0 for default case
- Use a simple incremental value for additional CAs?

How to provision end-points with identifier to reference CA

- http://www.ietf.org/internet-drafts/draft-adrangi-eap-network-discovery-10.txt describes how to select credentials for available named networks, but names are NAI Realms.
- 802.1X/EAP can be used to provision keys, could it also provision a CA-ID?
- Discovery phase of KSP could advertise number or names of instances
  - Like the SSID problem in 802.11?
- Manual configuration?

Wrap-up

ProCurve Networking
HP Innovation

A single CA per physical port limits MACSec applicability

- Strong desire to support the multiple 802.1X supplicant per port problem on traditional 802.3 media

Multiplexing CAs by VLAN is possible, and easier to implement, but restricts the usage model and doesn't match current architecture well.

Supporting multiple CAs is a manageable modification to 802.1AE

- SCI look-up is required on every packet anyway. Returning a CA instance that maps to a SecY is a small addition
- Bulk of the work may be required for 802.1af (which is not defined yet)
- Concept is fundamental to use model and should not be added later