Solutions for P802.1Qbz / P802.11ak: Architecture issue

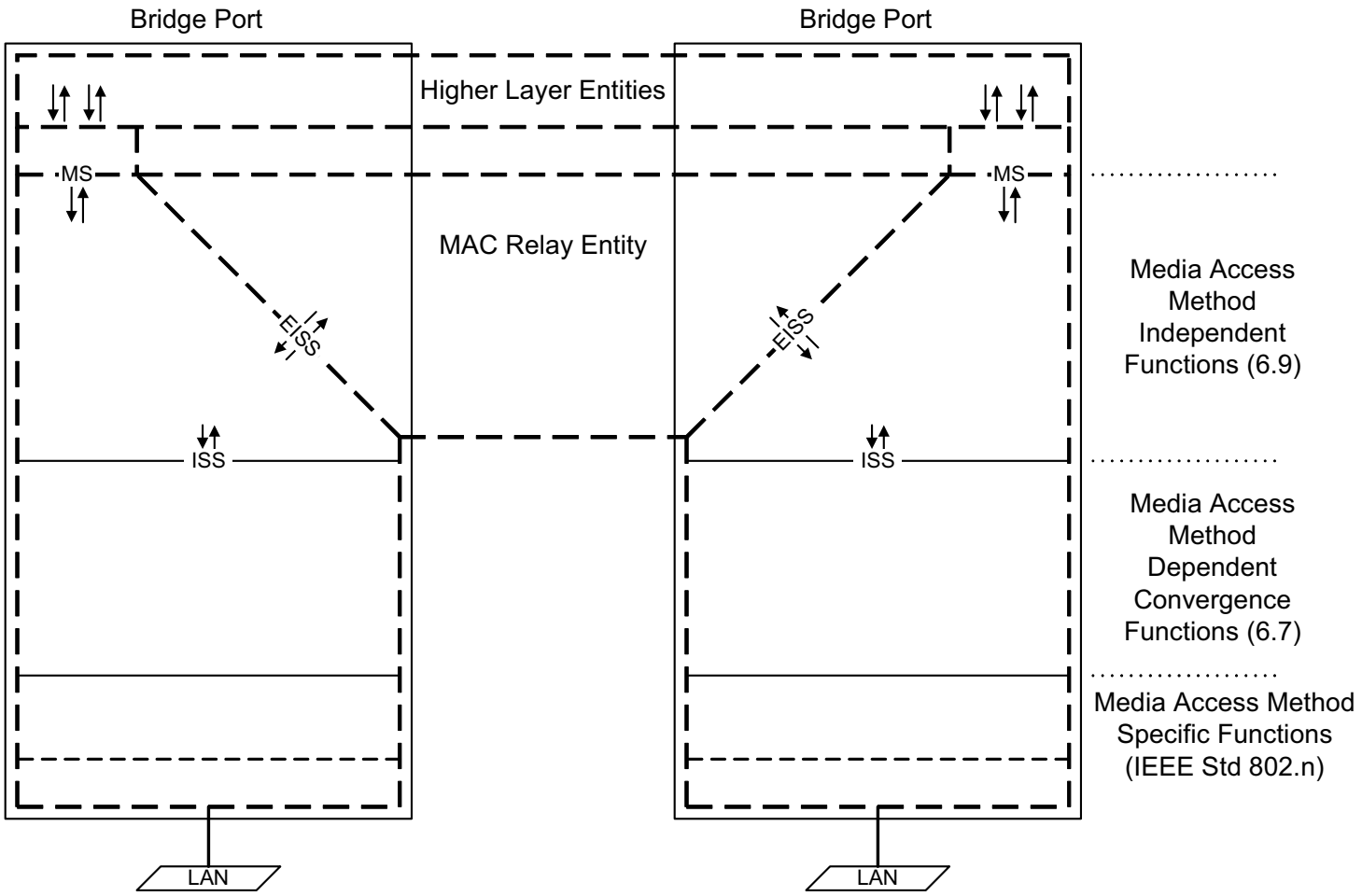
Norman Finn
January, 2013

Version 1

Introduction

- This presentation is available at: http://www.ieee802.org/1/files/public/docs2012/bz-nfinn-soln-architecture-0113-v01.pdf
- It attempts to answer one of the questions raised by: http://www.ieee802.org/1/files/public/docs2012/bz-nfinn-pt-to-pt-problem-list-1112-v02.pdf

IEEE Std 802.1Q-2011 Figure 8-2



NOTE—The notation "IEEE Std 802.n" in this figure indicates that the specifications for these functions can be found in the relevant standard for the media access method concerned; for example, n would be 3 (IEEE Std 802.3) in the case of Ethernet.

Figure 8-2—VLAN-aware Bridge architecture

IEEE Std 802.11-2011 Figure 5-1

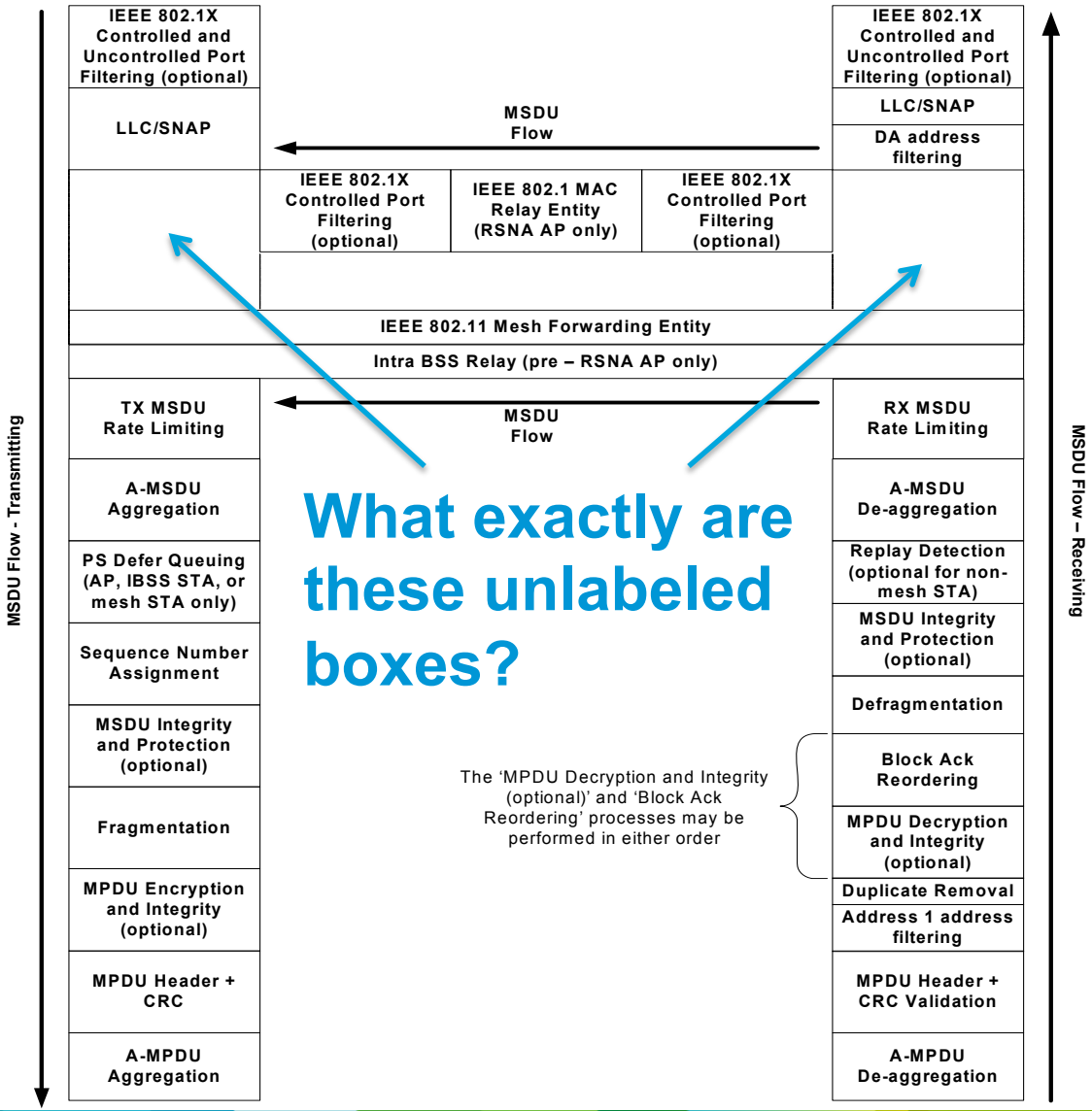
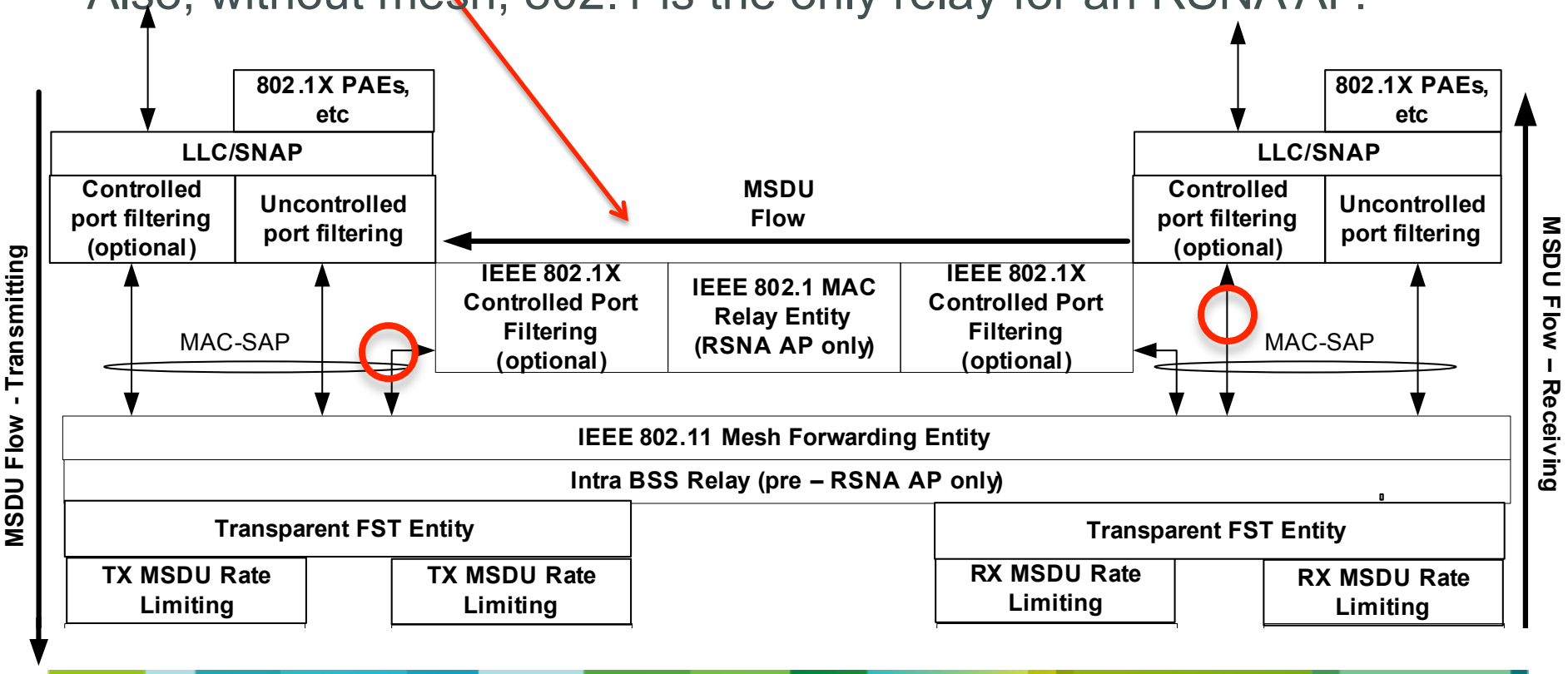


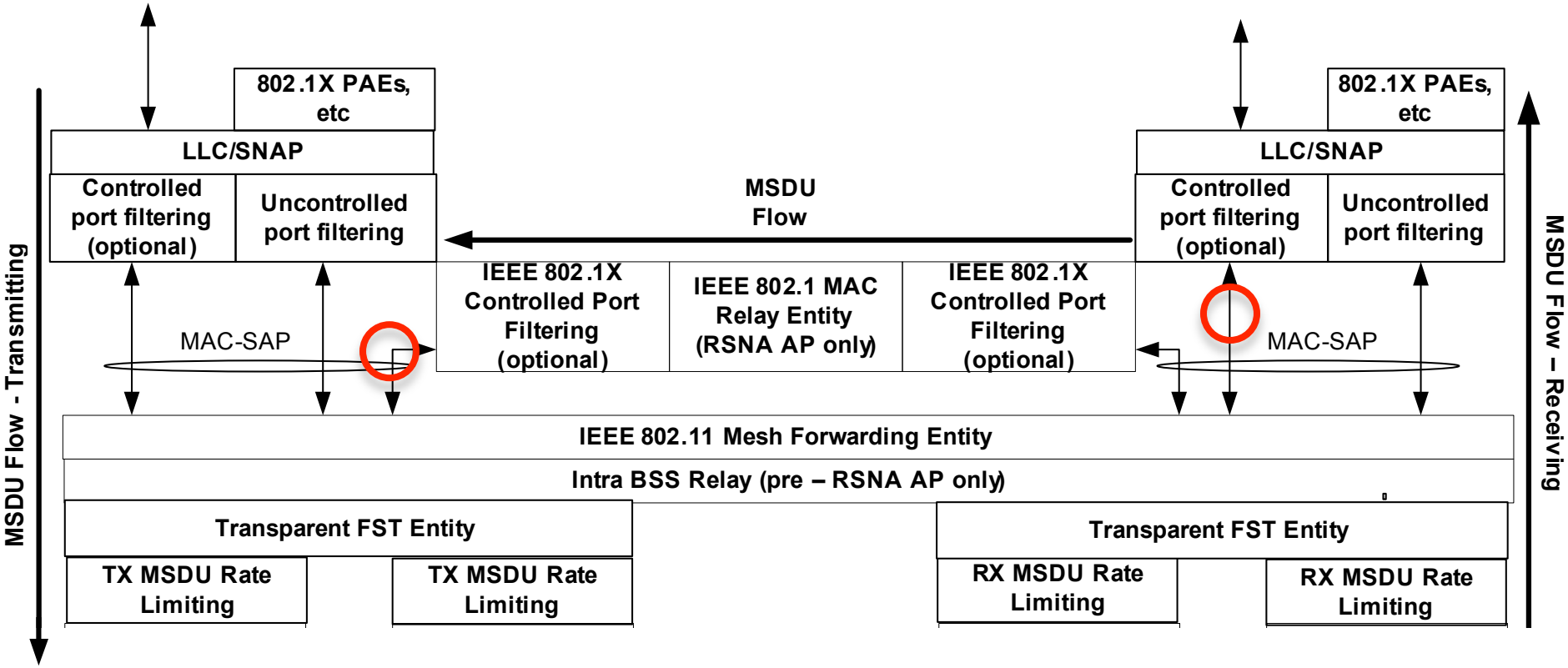
Figure 5-1—MAC data plane architecture

Is .11ad Fig 5-2 a “baggy pants”? Or not?

- This arrow shows a flow from AP through 802.1 relay back to AP. An 802.1 relay cannot do this unless it sees different stations as different ports. Arrow makes no sense if this is not baggy pants.
- Also, without mesh, 802.1 is the only relay for an RSNA AP.



IEEE Std 802.11ad-2012 Figure 5-2



- The FST (Fast Session Transfer) diagram clarifies this. The empty box in 5-1 is three entities all accessing the MAC-SAP.
- The double-ended arrows seem to be a little **confused**, given the one-way port representation, but the meaning seems clear.

MACsec layer difference resolution

- In **802.11** a good deal of 802.11-specific processing (queuing, fragmentation/defragmentation, etc.) is above the encryption/ decryption layers and the SecY (controlled/uncontrolled port split) in the stack. The SecY is several layers **below the MAC-SAP**.
- In **802.1Q**, encryption/decryption (MAC security) and the SecY are just **above the MAC-SAP**.
- Hence, between the empty box serving the LLC/SNAP port "baggy pants pocket" and the SecY, frames must be marked (using the equivalent of an extra ISS parameter) as belonging to the "controlled" or "uncontrolled" port.
- Putting the controlled/uncontrolled filtering as a Y at the top of the 802.11 stack (below the blank box) is equivalent to having the SecY at that location, and that architectural gap is bridged.

One Bridge Port per attached station

- The Bridge relay needs a separate instance of the MAC service for each connection to a station attached to this AP (whether AP or non-AP).
- Right now, AP offers one instance, the Portal.
- What can we do?
  - On ingress, the Transmitter Address can be used to drive a multiplexer that selects an ingress Bridge Port. Or, what should be the same thing, the security association ID can drive it.
  - On egress, the choice of output Bridge Port(s) drives the selection of Receiver Address, and thus the security association ID.
  - Of course, the real issue is, “What parameters go up and down the stack in the current AP specification.” If the answer is that the Destination Address feeds the egress stack, there could be a problem.
  - Of course, the bridge’s Filtering Database can be used to select the security association ID.

Emulation of Fat Yellow Coax?

- If the AP and its associated non-AP stations emulate a shared medium (fat yellow coax), the need for a separate MAC interface per associated non-AP station is not a problem.
- It would not be acceptable for the AP to broadcast every bridged frame to all bridges, whether the destination address was known to the AP, or not. So, presumably, **the AP has a MAC address table large enough to contain addresses for the whole network**, and can select the station / bridge to which a frame should be sent. But, that is all the point-to-point model asks for.
- In other words, unless the AP really is flooding every bridged frame everywhere, the data-plane requirements to be a “smart” implementation of a fat yellow coax are pretty much the same as that required to be a combined AP/bridge in the point-to-point model.