MACsec over an EVC

Brian Weis

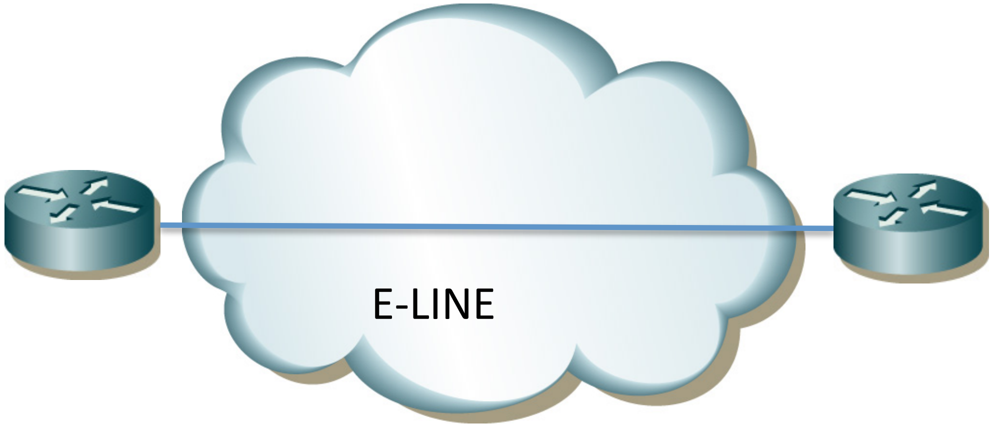
July 15, 2014

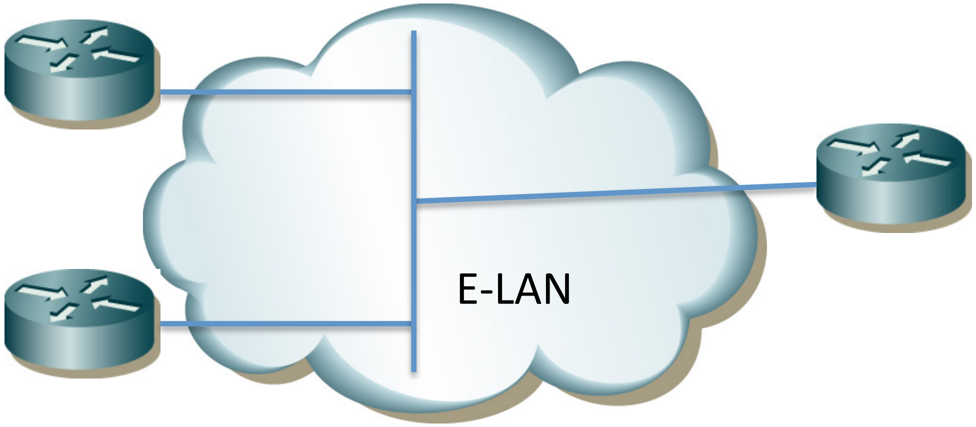
Ethernet Virtual Circuit (EVC)

- Defined by the Metro Ethernet Forum to define Carrier Ethernet
  - http://metroethernetforum.org
- Customers attach Customer Edge (CE) network equipment that are in the same broadcast domain
  - The actual topology of the SP network is hidden from the customer, the attached CE devices appear directly connected

E-LINE and E-LAN

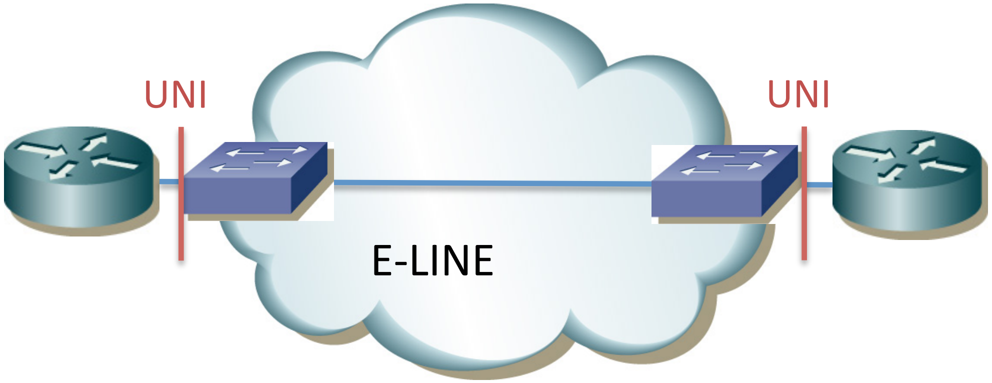
- E-LINE
  - Point to Point Connection
  - Emulates a private circuit
- E-LAN
  - Multipoint to Multipoint Connection
  - Emulates a LAN





Attachment to the SP Network

- The attachment between a CE and Provider Edge (PE) is called a User Network Interface (UNI)
- MEF describes that some Ethertypes and Protocols will be Peered, Discarded, or Tunneled by the PE (See MEF 6.1.1)
  - There are several types, but for our purposes they all Peer or Discard many Ethertypes and Protocols!

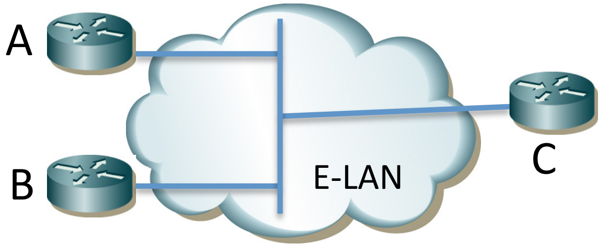


Issue 1: Ethertypes & Protocols

- According to MEF 6.1.1:
  - The UNI is supposed to either Peer or Discard the Ethertype 0x888E (EAPOL) rather than Tunnel it!
  - It's not clear yet how much a problem this is in practice, or what is the workaround
- Although not specified in MEF 6.1.1, many SP networks consume the Bridge group address and/or PAE group address!
  - Using the LAN broadcast address (FF-FF-FF-FF-FF-FF) is a feasible workaround, but is not specified in Table 11-1 of IEEE 802.1X-2010
  - This fate of new group addresses for EDE is unknown, but should be considered

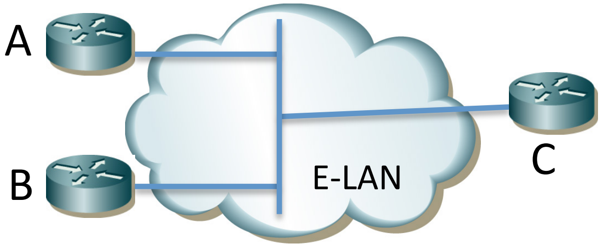
Issue 2: Live Peer Lists

- An EVC is more likely to have internal faults than a LAN
  - Partial failures are possible, such that the CE devices may not have the same sets of live peers
  - Each peer uses its own live list to install MACsec SAs. Can we guarantee that every peer installs the same MACsec SAs?
  - When XPN cipher suites are used, will the SSCIs be allocated identically on all CEs?



Issue 3: Incompatible Cipher Suites

- An EVC is more likely to have CEs with different sets of supported cipher suites
  - Assume A is the key server (KS), disributes a SAK, and chooses GCM–AES–XPN-128. Assume C does not support this cipher suite
  - A & B will install an Rx SA for C. C will not respond with a SAK Use indicating it has installed any Rx SAs, so after “MKA Life Time” has expired A will signal to use the SAK
  - But each will waste a precious Rx SA for C even though it will not be transmitting.



Issue 4: Deletion of a Dead Peer Rx SAs

- In an E-LAN peer becomes a dead peer, other participants will retain its Rx SA
  - There is no provision for selectively deleting Rx SAs
  - But there are some cases where deleting an SA because a peer has dropped off the live list is valuable. If it dies, do we trust it to continue to send MACsec frames, or might new frames come from an imposter that has extracted keys?
  - A local policy might be to distribute a new SAK when a peer leaves the live list. But this is not clear to someone doing a security analysis of MKA, and in a large group (where there is the most risk of key recovery) forcing a SAK rekey may not be operationally friendly. A risk analysis should be published.

Issue 5: Deletion of All MACsec SAs

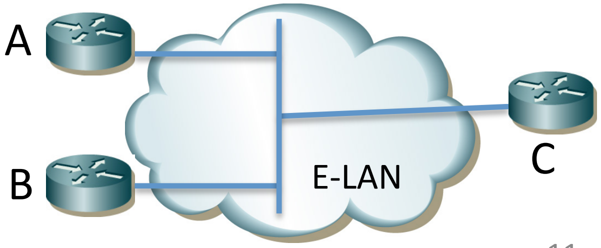
- IEEE P802.1Xbx specifies that Rx SAs of a suspended peer should not be deleted
  - "`An SAK that is already in use will continue to be used provided that each of these peers does not conclude that it is the CA's only active member, and provided that a fresh SAK is not distributed by a recognized Key Server.`"
- But RX SAs of a non-suspended peer that fails to respond within "MKA Life Time" are also not deleted
  - The only time SAs are deleted is in the CP state machine (Figure 12-2), using "deleteSAs()"
  - But "deleteSAs()" is not defined. Which SAs are deleted is not specified, but seems to mean those associated with the current KI value.

Issue 6: Deletion SAs after rekey

- When should old SAs be deleted after a rekey?
  - The answer is in Figure 12-2, when the "delete SAs()" function is called.
  - But it has been observed that deleting the SAs requires deleting each peer's SC/SA, and typical implementations do not maintain a peer list per SC. Such a requirement is not an obvious requirement
- The MACsec LMI may not be robust enough
  - It's not clear that there is an MACsec LMI that will allow MKA to delete SAs it doesn't know about
  - In particular, there does not seem to be an LMI for "delete all SAs associated with this AN", which would be useful when the peer list wasn't known.
  - This could be the result of an HA event where a backup processor takes over for a primary processor.

Issue 7: Link down event

- When MKA & MACsec are successful, the link is up. But if they fail, when does the link signaled to be down to higher level protocols?
- In an E-LAN, how is a partial failure reported to higher level protocols?
  - E.g., B becomes a dead peer. The links on A and C are still up, but how does higher level protocols determine that B is down? Will they just observe routing down, e.g.?



Issue 8: Churn of AN values

- Clause 9.8 says:
  - "A fresh SAK is not generated until the Key Server's Live Peer List contains at least one peer, and
    a) MKA Life Time (Table 9-3) has elapsed since the prior SAK was first distributed, or
    b) The Key Server's Potential Peer List is empty."
- The "or" in the list implies that an E-LAN with many (e.g., 10) peers coming online just at the wrong interval would cause a rapid succession of SAKs, possibly wrapping the AN values for the KS.
  - This seems non-deterministic, and prone to unreliability.

Issue 9: SecY SCI clarification

- IEEE 802.1AE-2006 Figure 10-6 shows SecY managed objects
  - The root SecY box shows an SCI.
  - It is never stated as being the same as the SC Tx SCI, but presumably this is the intent?