Wednesday's slides

TUTORIAL (n)

Security (2):

- The security considerations for ECRIT are put forth in IETF RFC-5069
- There are a few problems which seem to be intractable in a wireless environment with unauthenticated users.
- Originating call location information from unauthenticated users will be visible ("Hollywood Paparazzi Problem") unless we encrypt (at least) the over-the-air portion of those calls.
  - We believe that the current population of public access points has no way to provide encryption for unauthenticated users.
  - We believe that the current population of 802.11 access points has no way to preserve security while switching SSIDs (for further investigation).

TUTORIAL (n)

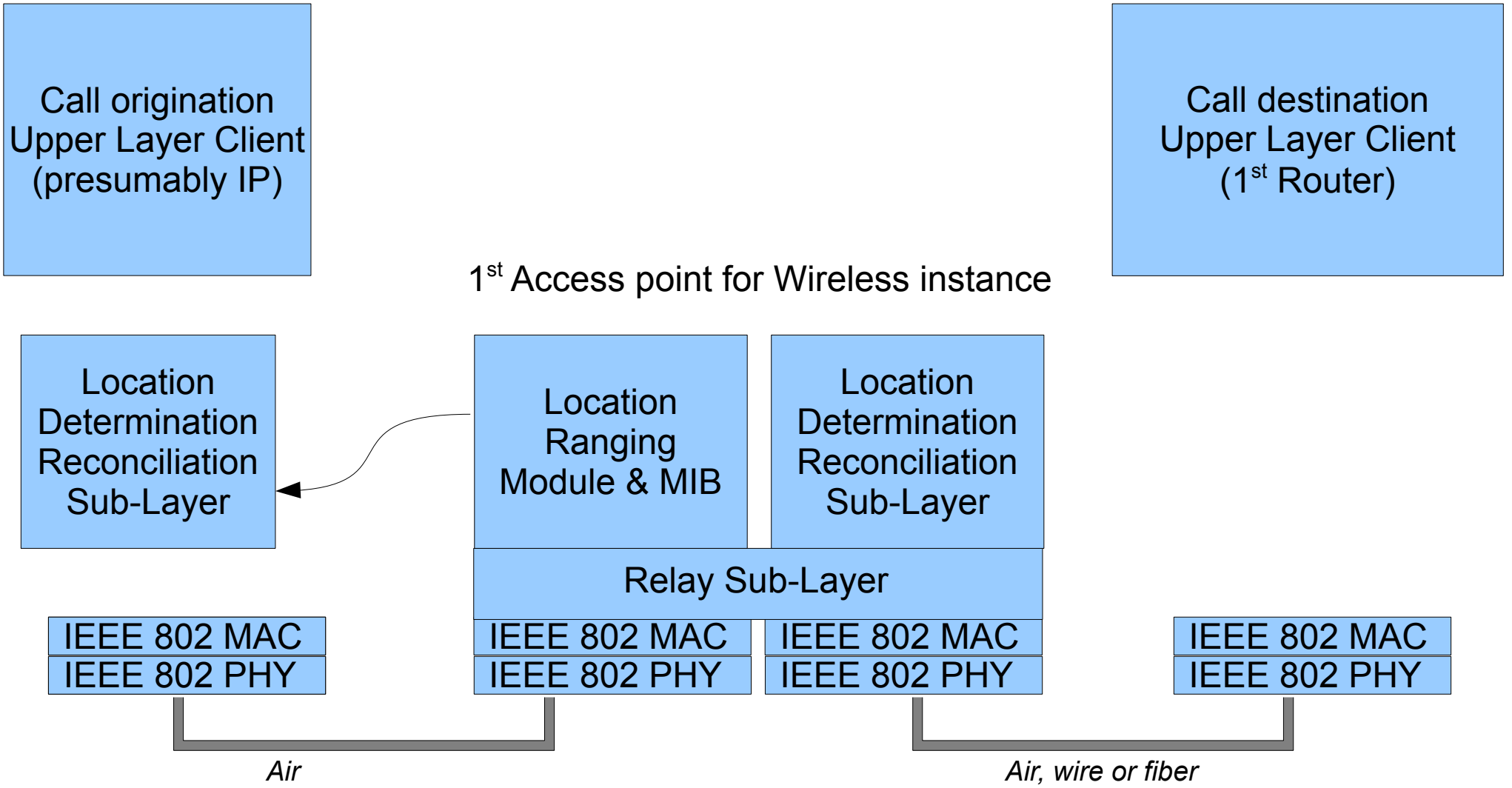
Security (3):

- First hop encryption is a significant challenge.
- First hop encryption will possibly require changes from the wireless MAC groups.
- First hop encryption should not be allowed to delay work on the primary functionality of “getting the call through”.

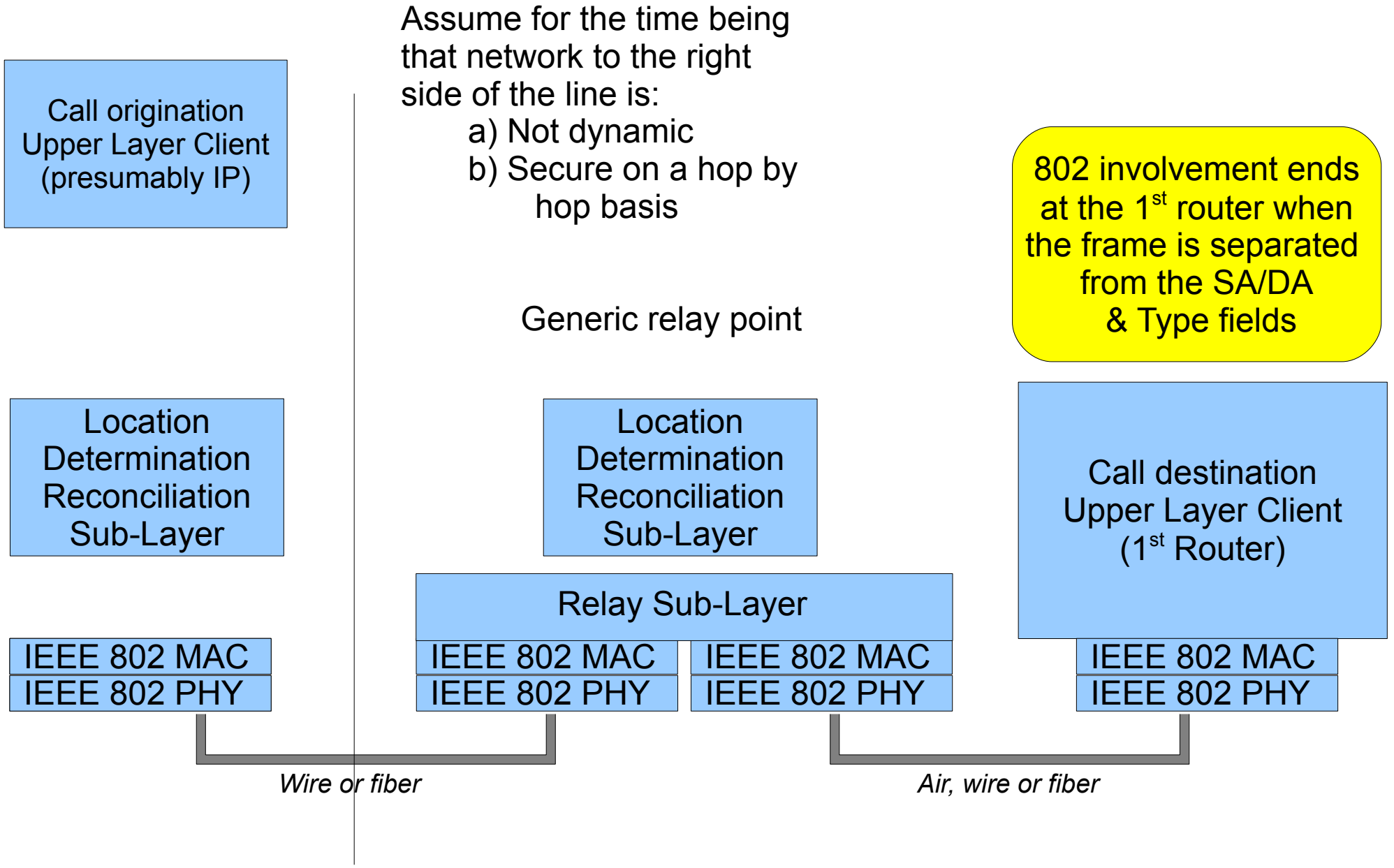
Diagrams

- Generate new topology and block functionality diagram which is like older 2 below but has at least 2 relay points.
- A diagram that actually describes a call sequence flow(?) chart:

IEEE 802 EMERGENCY SERVICES ARCHITECTURE
RE: Location Determination



IEEE 802 EMERGENCY SERVICES ARCHITECTURE
re: Location Determination



Call sequence via wireless end link

- AP->Sta Beacon of SSID for ES VLAN
- Sta picks a beacon
- Sta sends “Authenicate request”
- AP sends “Authenticate reply”
- Sta send “Associate request”
- AP sends “Authenticate reply”
- Sta sends DHCP request
- AP passes back DHCP response
  - DHCP response contains IP address for station, gateway IP address.
- Sta send ARP request with Gateway IP addr to get Gateway DA
- AP passes back ARP response from Gateway with its DA
- Sta can now communicate directly to Gateway via IP

Call sequence via wireless end link

- Sta sends ES SIP Request to Gateway
- (Is loc info sent at this point or in subsequent packets)?
- About now, 802 has pretty much set up its job except when the time comes for Call-Back.
  (Handover and roaming problems excluded)

Issues

- U.S. Government preference is for infrastructure based location over that from end station based location information.
  (GPS reliability in cities and inside buildings is a problem, as is spoofing.)
- 802.16 distance and angle measurement is not of sufficient accuracy to meet the requirements E911 & NG911.
- 802.11 service leaking into adjacent properties is a well known problem for which we have no solution.