TUTORIAL (1)

Why 802 needs an Emergency Services Project and what we think it should look like.

Geoff Thompson/InterDigital
Scott Henderson/RIM

802 ES-ECSG

Technical/Regulatory Problem Statement

911 call origination identification was originally based on the wireline legacy incumbent local exchange carriers' databases of their customers.

This system fell apart or was seriously weakened as:

- Local phone service ceased to be dominated by a wireline monopoly.
- Cellular phones became significant. (They had no built-in location mechanism. They also had a weakened sense of just where they wanted to call for 911.)
- VoIP phone services grew. They also had no inherent location or call target mechanism

Regulatory Technical Problem Statement

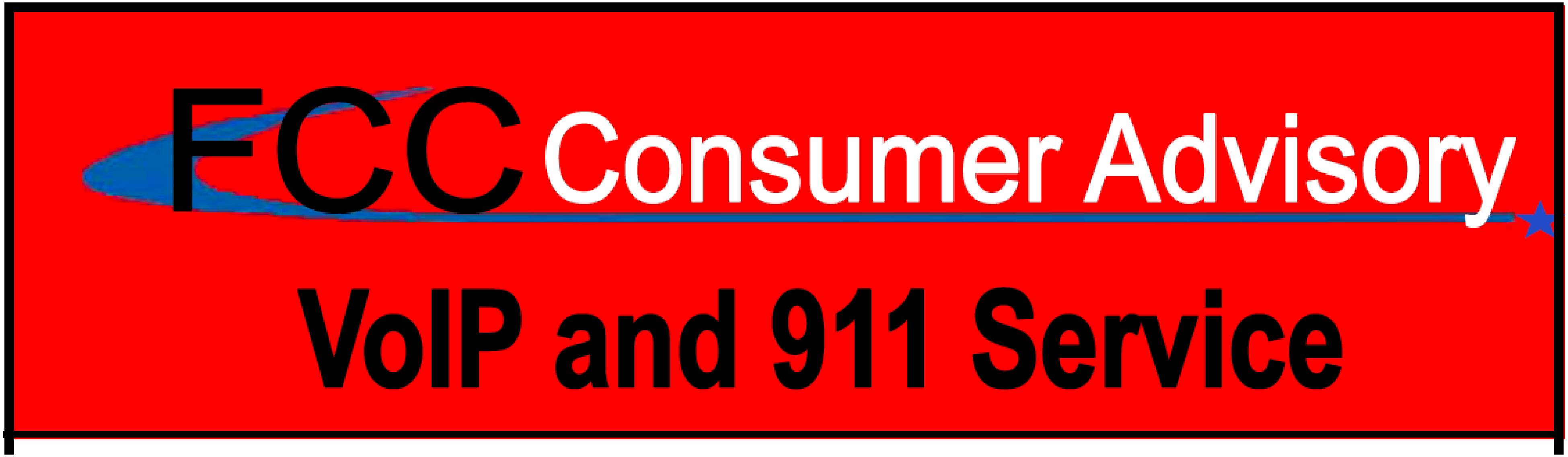
Emergency Services calls need:

- To be directed to the appropriate PSAP
- Carry originating location information
- Be handled on a high priority basis
- To provide sufficient information for call-back

Further:

- Systems are required to provide service to any user. (Authorized subscriber or not)

FCC Consumer Info Sheet



FCC Consumer Advisory

VoIP and 911 Service

http://www.fcc.gov/cgb/consumerfacts/voip911.pdf

(Example:) US Requirement

(adapted from: http://www.fcc.gov/cgb/consumerfacts/voip911.pdf)

The US FCC has imposed the following requirement:

- All interconnected VoIP providers must automatically provide 911 service to all their customers as a standard, mandatory feature without customers having to specifically request this service.
  VoIP providers **may not** allow their customers to “opt-out” of 911 service.

Requirements: Other countries

- Many other countries have similar requirements.
- There are national differences, especially with respect to:
  - Emergency numbers other than “911”.
  - Some countries have several numbers
  - Some countries prohibit location info.
  - Other details

Defined Problem lies in Multiple Domains

- IP, routing and higher layer portions of the problem belong to the IETF.
- These problems are being addressed primarily by IETF ECRIT.
- The below Layer 3 portion of the problem is for 802 to address.
- 802.11 and 802.16 have already done some explicit work in this area.
- Needs to be handled uniformly across 802.

802 Problem

- IEEE 802 needs a single standard so that IP applications “should” not need to know which 802 MAC is currently being used.
- This is envisioned as a “shim layer” that goes between an 802 end station MAC and its upper layer client.
- There will be similar pieces required for 802.1 relays to add per-hop location information (required for location back-up information when no end-location information is provided).

TUTORIAL (2)

SUPPORT OF EMERGENCY SERVICES and THEIR (present and future) REGULATORY REQUIREMENTS FOR PACKET NETWORKS IS A HUGE, COMPLEX PROBLEM FOR WHICH THE PROBLEM ITSELF IS NOT YET FULLY DEFINED.

TUTORIAL (3)

There are pieces of the ES problem that:

- Are well defined today
- Have existing regulatory requirements
- Are not addressed across 802.

TUTORIAL (4)

The biggest piece:

- 802 originated (and VoIP originated) “calls” to the PSTN don't carry the information required for emergency calls (e.g. 911 calls)
(There are proprietary exceptions)
- There are existing regulatory requirements for these calls that are not being met.

TUTORIAL (5)

Regulatory Requirements:

- Call request directed to the correct PSAP
- Provide calling party location
- Non-subscriber access to network
- PSAP can call back
- Very high priority
- Call integrity (no drop, spoof-proof)

TUTORIAL (6)

Why VoIP doesn't work today:

- The Internet was designed to be “location neutral”.
- Traditional “911” was designed around and serviced by a localized static wired infrastructure (end office circuit switched systems)
- VoIP services are highly decentralized and often cross national boundaries (regulatory problem)

TUTORIAL (7)

Why VoIP doesn't work today (cont'd):

- Today, the VoIP service provider has no knowledge of the callers location within the Internet (almost true)
- A PSAP has no prior knowledge that a caller is within their service area.
- Therefore associating caller and proper PSAP is a big problem
- VoIP service providers are not yet fully regulated; there are significant technical, geopolitical and legal jurisdiction problems involved.

TUTORIAL (8)

The IETF – ECRIT group has taken on the task of solving this problem for the upper layers.

See:

http://www.ietf.org/dyn/wg/charter/ecrit-charter.html

- 7 Internet drafts, 7 RFCs
- Includes “Framework” and “Best Current Practices”
- Add in or refer to Richard Barnes preso at KL

TUTORIAL (n)

The IETF – ECRIT group has taken on the task of solving this problem for the upper layers.

802 needs to work with ECRIT to provide a complete solution.

The solution should look the same to ECRIT without regard to which 802 technology is in use.

TUTORIAL (n)

What does ECRIT need from 802 to meet these requirements?

- Provide better location than just the router
- Emergency calls should be given priority in the 802 network
- Callback is currently a problem
- Spoofing and security are issues
- Prefer LOCAL connection (e.g. bypass various tunneling schemes)
- Provide service to unauthenticated user

TUTORIAL (n)

What we believe 802 needs to finish the task:

- Specific interface specs from ECRIT
- Harmonized and reconciled to our requirements
- Agreement within various 802 W.G.s to tweak their pieces.
- An ES WG to generate a single standard to reconcile the upper layer interface.

TUTORIAL (n)

What 802 needs to provide to finish the task:

A standard that includes means to:

- Provide end & per hop location in 802 networks.
- Give emergency calls priority in 802 networks
- Provide information to enable Callback
- Provide a LOCAL connection mechanism (e.g. bypass various tunneling schemes)
- Provide service to unauthenticated users

Spoofing and security are issues

TUTORIAL (n)

IN SHORT:

ES-ECSG intends to provide what ECRIT needs.

TUTORIAL (n)

Possible technical concepts:

- Provide end location in 802 networks.
  - 802 ES to provide/harmonize end station location MIB to ECRIT format requirements.
- Provide per-hop location in 802 networks.
  - Adapt/use existing mechanism from 802.1ag and equivalents from 802.11.

TUTORIAL (n)

Possible technical concepts:

- Give emergency calls priority in 802 networks.
  - Use existing priority mechanisms in 802.1Q

TUTORIAL (n)

Possible technical concepts:

- Provide information to enable Callback.
  - Provide both originating terminal location MIB information and per-hop network information as part of session initiation information to the network attachment router.
  - This would provide “hints” that the 802 network could use if call is disconnected and straightforward callback turns out to be a problem.

TUTORIAL (n)

Possible technical concepts:

- Provide a LOCAL connection mechanism (e.g. bypass various tunneling schemes).
    - Provide a VLAN (or equivalent) across all 802 networks that is dedicated exclusively to Emergency Services. It would have a single destination, i.e. the network attachment router.
    - We anticipate that packets will be steered to this new dedicated VLAN by the use of a new EtherType.

TUTORIAL (n)

Possible technical concepts:

- Provide service to unauthenticated users.
  - This could be difficult, but is a firm regulatory requirement.
  - We believe a dedicated VLAN will make it easier than it would be to do otherwise.
  - No authentication is needed to use the dedicated VLAN, but it can only be used to get to the PSAP.

TUTORIAL (n)

Spoofing:

- End and per-hop location information as provided will be available as a tool for use in dealing with this classical problem.

TUTORIAL (n)

Security:

- A dedicated VLAN sidesteps some of the issues associated with security.
- Providing location information is forbidden in some countries, mandatory in others.
- Information integrity across the call is a security issue.
- Provided location information is considered to be sensitive information.
- Information needed for call back is considered to be sensitive.
- The actual content of the call may be considered to be sensitive.

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)

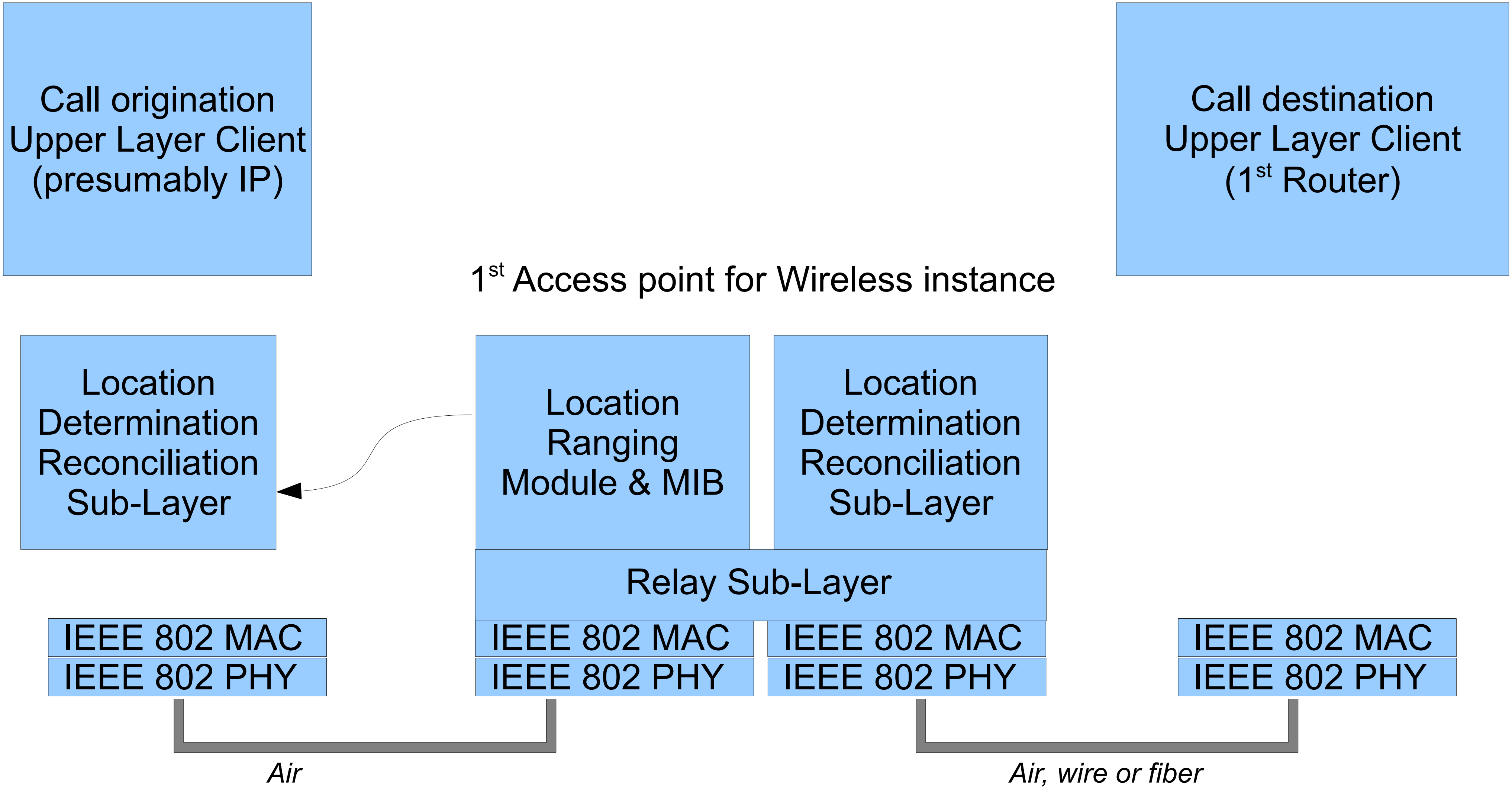
Security (3):

- 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

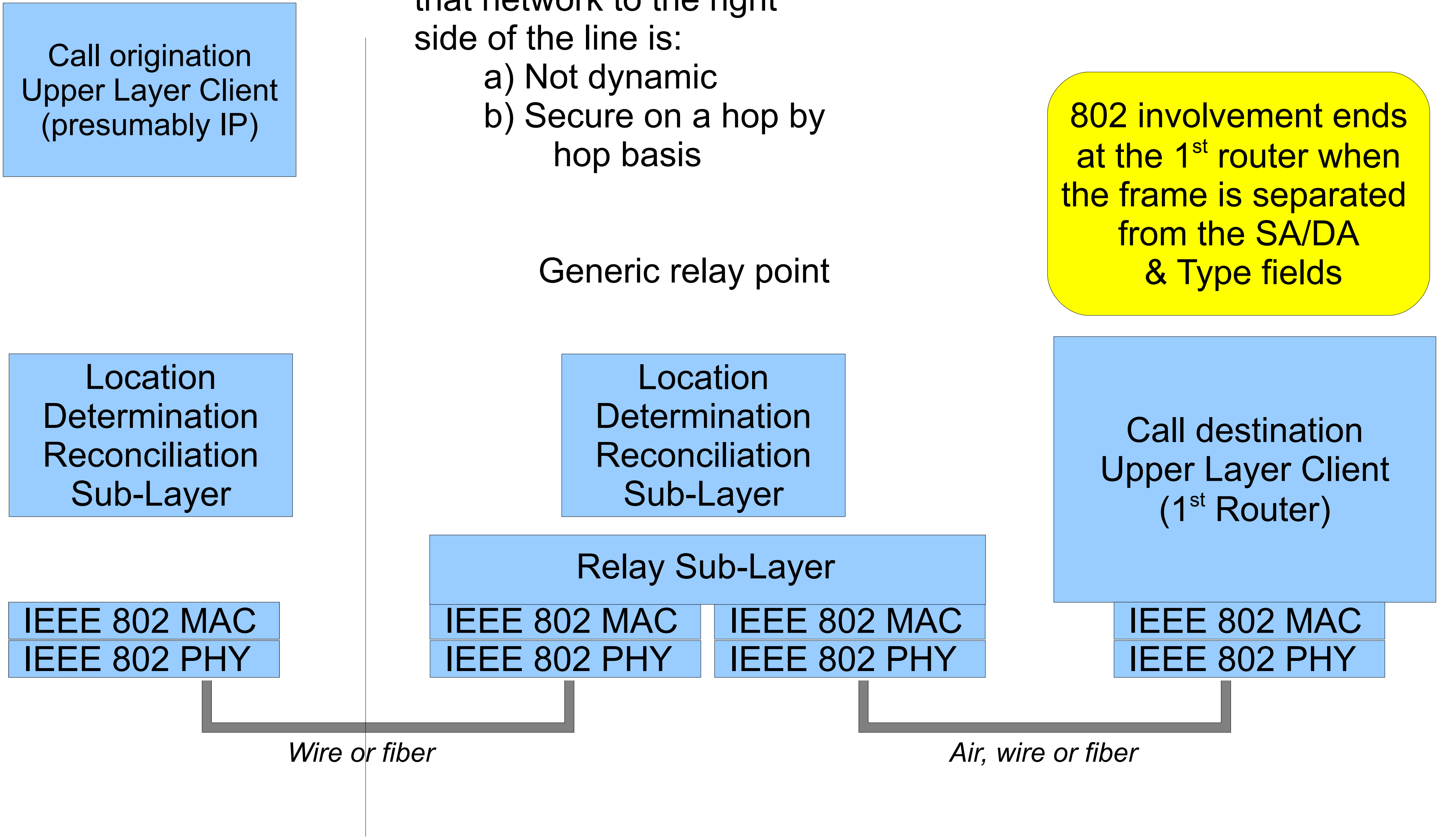

Call origination Upper Layer Client (presumably IP)
Call destination Upper Layer Client (1st Router)
1st Access point for Wireless instance
Location Determination Reconciliation Sub-Layer
Location Ranging Module & MIB
Location Determination Reconciliation Sub-Layer
Relay Sub-Layer
IEEE 802 MAC
IEEE 802 PHY
IEEE 802 MAC
IEEE 802 PHY
IEEE 802 MAC
IEEE 802 PHY
IEEE 802 MAC
IEEE 802 PHY
Air
Air, wire or fiber

IEEE 802 EMERGENCY SERVICES ARCHITECTURE re: Location Determination

Assume for the time being that network to the right side of the line is:

a) Not dynamic

b) Secure on a hop by hop basis



Call origination Upper Layer Client (presumably IP)

Location Determination Reconciliation Sub-Layer

IEEE 802 MAC

IEEE 802 PHY

Wire or fiber

Generic relay point

Location Determination Reconciliation Sub-Layer

Relay Sub-Layer

IEEE 802 MAC

IEEE 802 PHY

IEEE 802 MAC

IEEE 802 PHY

Air, wire or fiber

802 involvement ends at the 1st router when the frame is separated from the SA/DA & Type fields

Call destination Upper Layer Client (1st Router)

IEEE 802 MAC

IEEE 802 PHY

Call sequence via wireless end link

- AP->Sta Beacon of SSID for ES VLAN
- STA picks a beacon
- STA sends “Authenticate 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 location information 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. That is, being able to provide accurate street address information .