Emergency Services Requirements

Presentation to IEEE 802.1

Internetworking

January 22, 2010

Geoff Thompson

Chair 802 Emergency Services ECSG
also Scott Henderson/RIM

(significant mat'l “borrowed” from Richard Barnes presentation to ESW6)

http: //geopriv.dreamhosters.com/esw6/PEACE-Vortrag_v5.ppt

Emergency Services Requirements

- Some regulatory requirements for VoIP (and messaging systems) trickle down to 802.
- There are more or less parallel requirements from various agencies around the world.
- FCC for the US (with the help of NENA) and ETSI for the EU are 2 of the more significant examples.

EU as leading example

- ETSI TS 102 424
  Specifically: ETSI TS 102 424 V1.1.1 (2005-09)
- Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements of the NGN network to support Emergency Communication from Citizen to Authority
- (FCC equivalents can be provided but are less concise.)

Contents

- References provided to governing EC documents
- Definitions & Abbreviations
- Cl. 4 Emergency Sessions Requirements

Requirements

- 4.1.1 Be able to identify local Emergency Services Number (e.g. should I call 211 or 911?)
- 4.1.2 Location information derived from the known information in the network
  - Can refine/add to information later in call
  - Location information is “private”
- 4.1.3 Priority call
- 4.2 Interconnected VoIP must support ES.
- 4.3 Further requirements for IP systems without PSTN in the middle.

Additional Requirement (from FCC)

- Interconnected VoIP providers must transmit all 911 calls, as well as a callback number and the caller’s registered physical location, to the appropriate emergency services call center or local emergency authority.
  (Ref: http://www.fcc.gov/cgb/consumerfacts/voip911.pdf)

“Requirements” from IETF

- Richard Barnes (GeoPriv Chair, ECRIT editor) memo
- ECRIT Architecture Slide (from Barnes IETF presentation to ESW6)

IETF WG Charters

- The GEOPRIV working group is chartered to continue to develop and refine representations of location in Internet protocols, and to analyze the authorization, integrity, and privacy requirements that must be met when these representations of location are created, stored, and used.
- ECRIT will describe when Internet technologies available to describe location and manage call routing may be appropriate and how they may be used.

Barnes memo

From: Richard L. Barnes [mailto:rbarnes@bbn.com]
Sent: Friday, January 15, 2010 8:44 AM
To: Tschofenig, Hannes (NSN – FI/Espoo)
Cc: Stephen McCann; Scott Henderson
Subject: Re: ECRIT Architecture

Hi Stephen, Scott,

The slides I used are here:
<http://geopriv.dreamhosters.com/esw6/PEACE-Vortrag_v5.ppt>

(Scott: Sorry for not getting back to you sooner with this.)

I don't have any objections to Scott/RIM briefing IEEE folks on ECRIT. If I might suggest a few things to keep in mind / emphasize:

-- ECRIT is designed to be application-agnostic, in the sense that it allows multiple application-layer communications systems to be used to contact PSAPs. This approach is the reason that the architecture is so cleanly layered, with the access network (layer 1/2) providing location, and everything else (LoST and the call itself) handled at the application layer. If requirements emerge for lower-layer networks to participate in application-layer exchanges, then it will significantly reduce the flexibility (and thus utility) of the architecture.

-- There are two obvious ways that layer 2 can contribute: location and access-control.

-- W.r.t. location: It would be very helpful for building location services if IEEE networks had a standard way for a location server to find and interrogate a server (e.g., over SNMP) about the location of endpoints on the network, which implies that the layer-2 network will need a way to track endpoints.

-- W.r.t. access control / unauthenticated access: Obviously, unauthenticated users have to first get access to the layer-2 network before they can do IP emergency communications. I think we can agree that whatever the approach taken to managing these users after connection, it would be helpful to have a standard way of authenticating and tagging "emergency-only" connections. Personally, I like the EAP (i.e., 802.1X) approach outlined in draft-schulzrinne-ecrit-unauthenticated-access:

<http://tools.ietf.org/html/draft-schulzrinne-ecrit-unauthenticated-access>

Hope this helps,

--Richard

Barnes memo extract 1

-- There are two obvious ways that layer 2 can contribute: location and access-control.

-- W.r.t. location: It would be very helpful for building location services if IEEE networks had a standard way for a location server to find and interrogate a server (e.g., over SNMP) about the location of endpoints on the network, which implies that the layer-2 network will need a way to track endpoints.

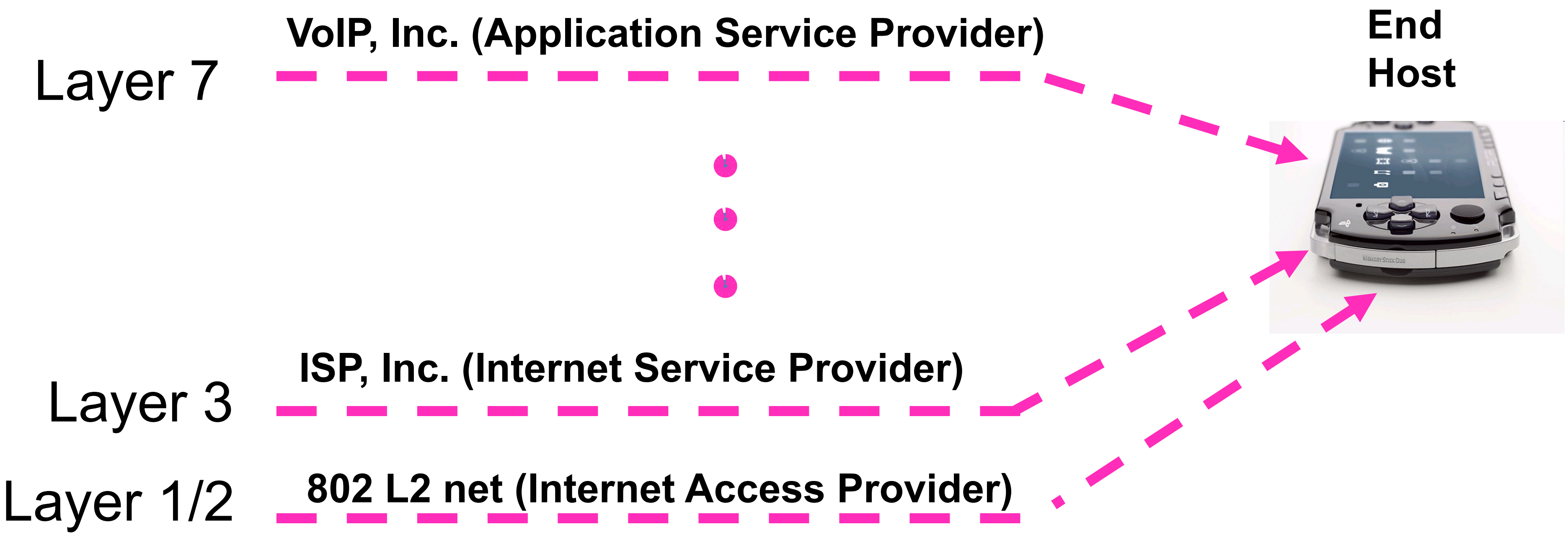
Barnes memo extract 2

-- W.r.t. access control / unauthenticated access:

Obviously, unauthenticated users have to first get access to the layer-2 network before they can do IP emergency communications. I think we can agree that whatever the approach taken to managing these users after connection, it would be helpful to have a standard way of authenticating and tagging "emergency-only" connections. Personally, I like the EAP (i.e., 802.1X) approach outlined in draft-schulzrinne-ecrit-unauthenticated-access:

<http://tools.ietf.org/html/draft-schulzrinne-ecrit-unauthenticated-access>

Architectural Considerations



Layer 7

VoIP, Inc. (Application Service Provider)

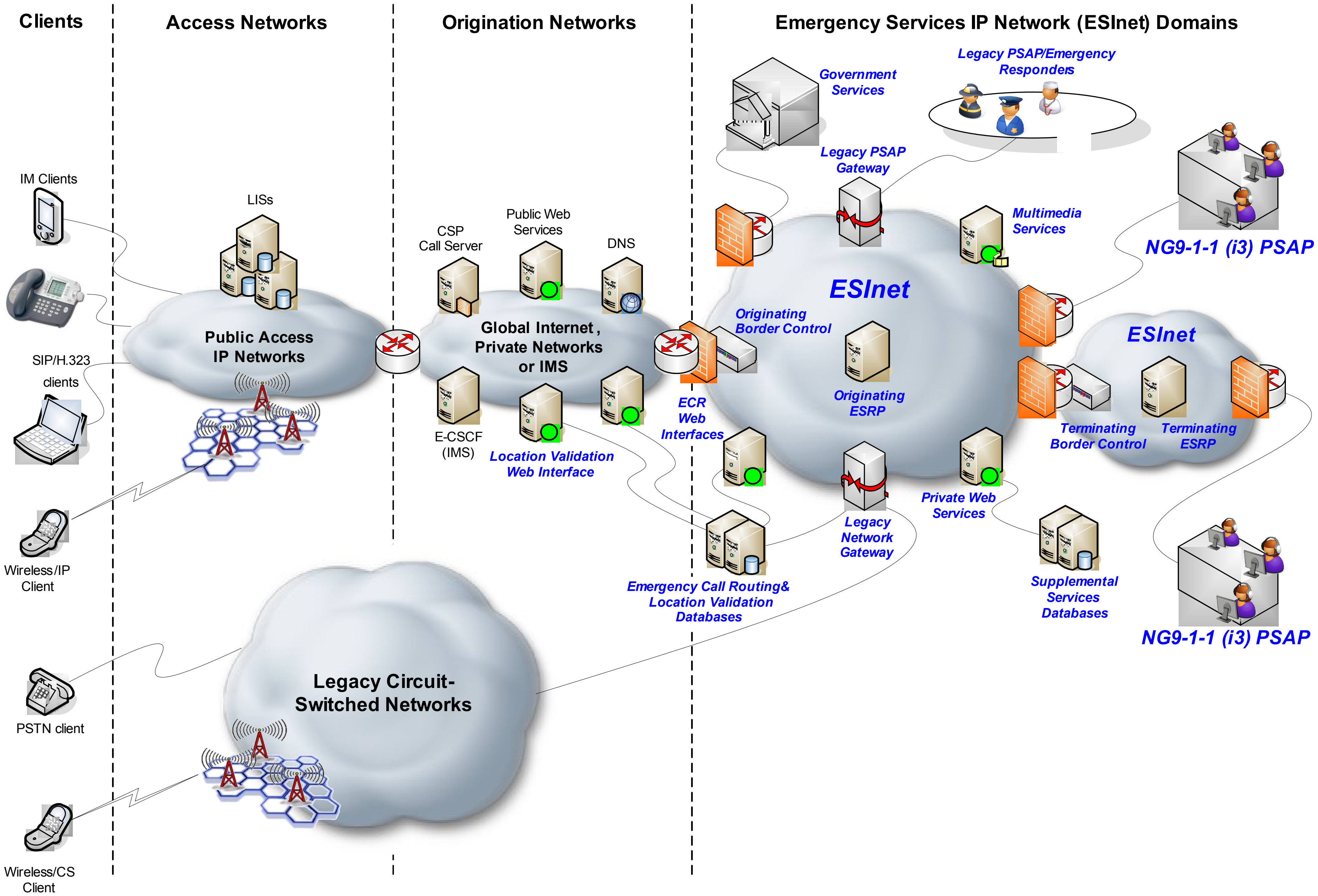
Layer 3

ISP, Inc. (Internet Service Provider)

Layer 1/2

802 L2 net (Internet Access Provider)

End Host


Clients
Access Networks
Origination Networks
Emergency Services IP Network (ESInet) Domains
IM Clients
SIP/H.323
clients
Wireless/IP
Client
PSTN client
Wireless/CS
Client
LISs
Public Access
IP Networks
Legacy Circuit-
Switched Networks
CSP
Call Server
Public Web
Services
DNS
Global Internet ,
Private Networks
or IMS
E-CSCF
(IMS)
Location Validation
Web Interface
Government
Services
Legacy PSAP/Emergency
Responders
Legacy PSAP
Gateway
Multimedia
Services
NG9-1-1 (i3) PSAP
ESInet
Originating
Border Control
Originating
ESRP
ECR
Web
Interfaces
Legacy
Network
Gateway
Private Web
Services
Emergency Call Routing&
Location Validation
Databases
Supplemental
Services
Databases
ESInet
Terminating
Border Control
Terminating
ESRP
NG9-1-1 (i3) PSAP

Other wants from IETF

- Unauthenticated Emergency Services
- Callback

Unauthenticated Emergency Services

- Reference: http://tools.ietf.org/id/draft-schulzrinne-ecrit-unauthenticated-access
- Cases:
  - The emergency caller does not have credentials for access to the network but still has credentials for his VoIP provider.
  - The emergency caller has credentials for network access but does not have credentials for a VoIP provider.
  - The emergency caller has valid credentials but is not authorized to make a call.
- Work assumes lower-layer procedures for omitting network access authentication.
- Technically complex and difficult to deploy. Introduces security vulnerabilities.

Callback

- Marking of Calls initiated by Public Safety Answering Points (PSAPs)
  - Touches the authority-to-citizen topic
  - Callback is an ordinary call, i.e. no preferential treatment. Call could get blocked, re-directed or ignored.
- Phone BCP describes a basic solution:
  - Store information about the participating communication parties of the emergency call for a limited period of time
  - When call callback arrives check against stored state.
  - Acts similar to stateful packet filtering firewalls.
- Problem statement, requirements and solution strawmans are provided in http://tools.ietf.org/id/draft-schulzrinne-ecrit-psap-callback