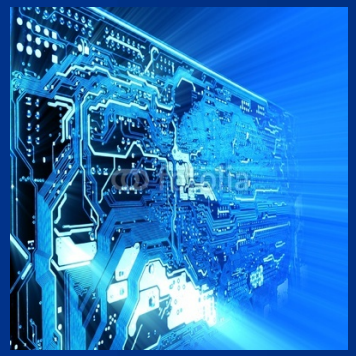
APCO International
Leaders in Public Safety Communications™

APCO International™ Emerging Technology Forum

Planning for NG9-1-1: Cybersecurity Considerations & Integration with FirstNet

Jay English
Director
Comm. Center & 9-1-1 Services
APCO International



Topics to Cover

- NG9-1-1 – the new frontier
- Securing NextGen systems
- Integration with FirstNet
- Issues that need to be on the radar

"NG9-1-1"

- Next Generation systems will be a "network of networks" providing connectivity between PSAPs on a network within a specified geographic area to other networks both regionally and nationally
- With advancement of technology comes an increased opportunity for sharing of data, and potential threats of infiltration and exploitation of the system
- Reliant on data rather than traditional voice with tremendous potential for achieving a new level of interoperability.

Stand up Secure Broadband Networks

INTERCONNECT PSAPS AND OTHER AGENCIES

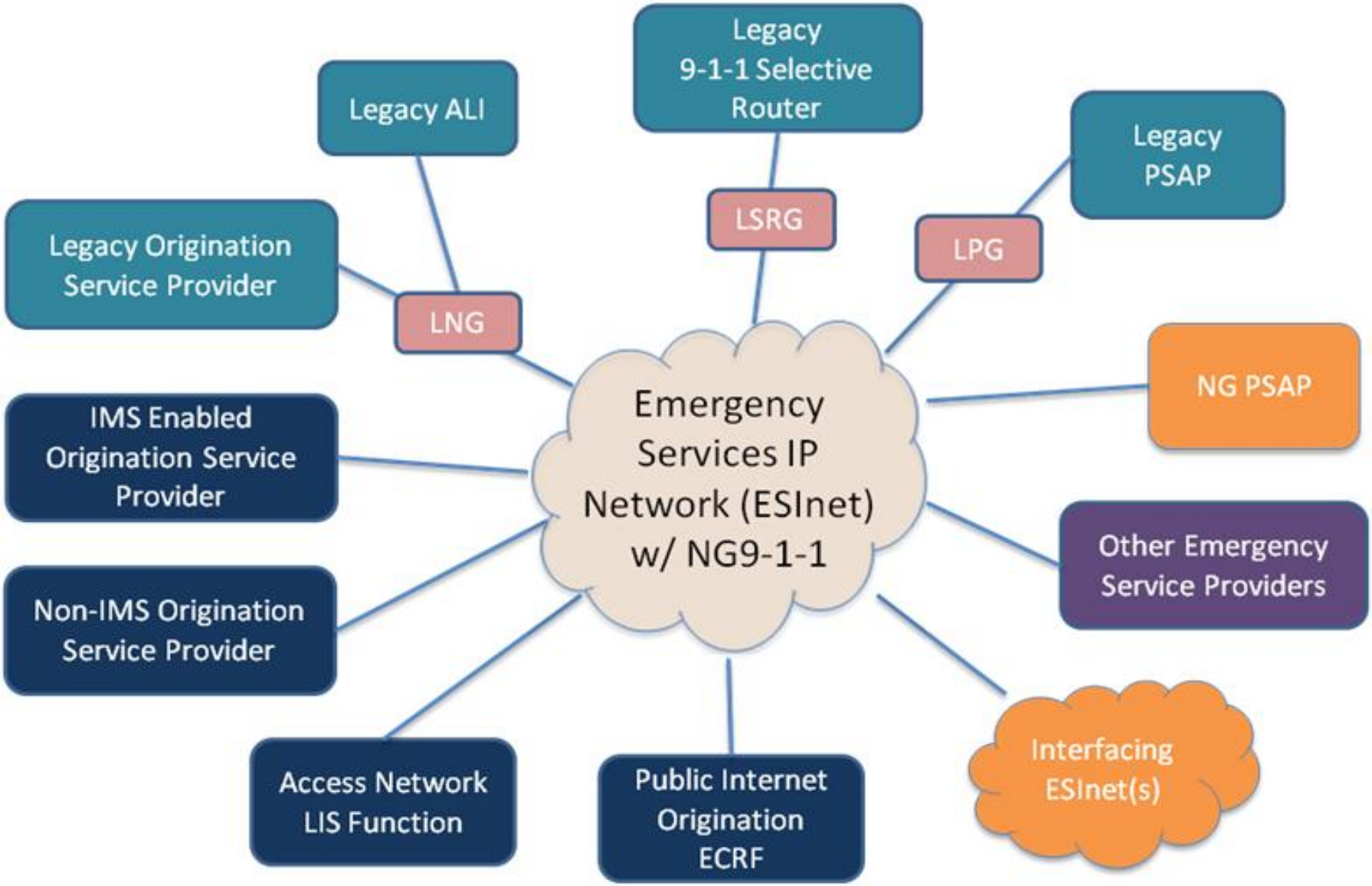
Agencies share resources such as CAD, RMS, email & Internet applications

Implement IP Selective Routing

- IPSR replaces the functions of legacy selective routers by routing 9-1-1 calls via IP to a PSAP. It routes calls using existing mechanisms (e.g. ANI, p-ANI, ESRK) and converts incoming calls to SIP signaling.

Session Initiation Protocol

The IPSR interface to the PSAP is defined by the ATIS/ESIF Request For Assistance Interface standard (RFAI)


Legacy
9-1-1 Selective
Router
Legacy ALI
Legacy
PSAP
LSRG
LPG
Legacy Origination
Service Provider
LNG
NG PSAP
Emergency
Services IP
Network (ESInet)
w/ NG9-1-1
IMS Enabled
Origination Service
Provider
Other Emergency
Service Providers
Non-IMS Origination
Service Provider
Interfacing
ESInet(s)
Access Network
LIS Function
Public Internet
Origination
ECRF

APCO International
Leaders in Public Safety Communications™

Cyber Security and Next Gen Systems

Jay English
Director
Comm. Center & 9-1-1 Services
APCO International

NG9-1-1

- Legacy 9-1-1 systems are relatively secure, and while threats exist they are somewhat limited
  - TDoS
  - Carrier outages
  - Capacity issues
- While secure, the system is extremely dated and limited.
  - Location limitations
  - Media capabilities
  - CAMA trunks / Circuit switched technology

NG9-1-1

- With advancement of technology comes an increased threat of infiltration and exploitation of the system
- NG9-1-1 systems and ESINets will be vulnerable to the same threats as existing IP networks and systems
- Training and awareness are important considerations
- Our people, not just the equipment, are key
- There are resources “out there”
  - TFOPA work underway
  - NIST, US-CERT, DHS all have products available

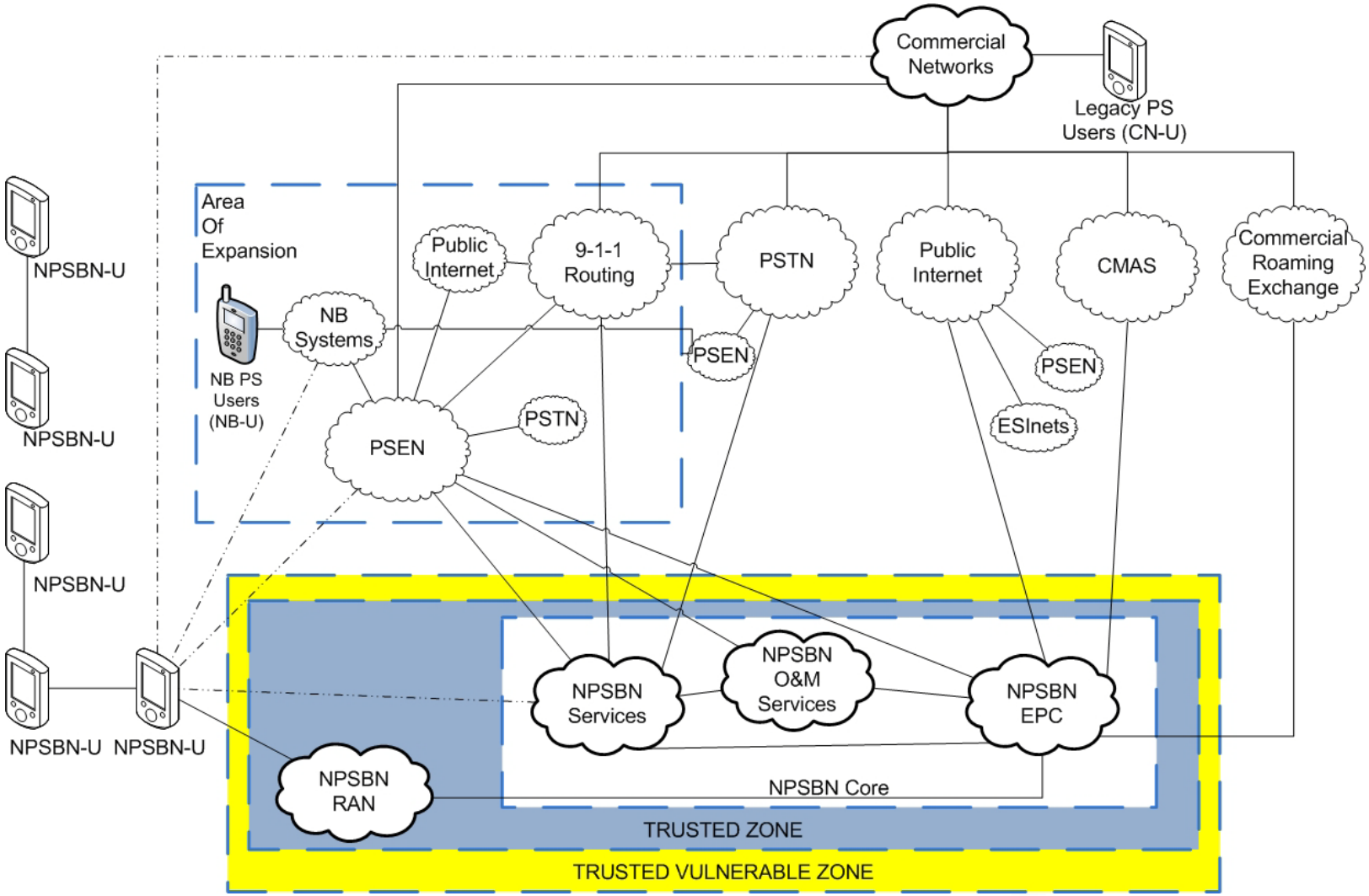
Types of Threats

- **Destruction:** Physical destruction of information or communications systems rendering them unusable
- **Corruption:** The changing of information such that it is no longer accurate or useful
- **Removal:** The removing of information so that it cannot be accessed, but is not destroyed
- **Disclosure:** Unauthorized release of confidential or sensitive information to the detriment of owner of said data
- **Interruption:** Interfering with communications such that legitimate users cannot send or receive messages

Planning

- Secure communications are a core requirement for PSAPs.
- Requirements to consider may include user credentialing, access control, authentication, auditing, confidentiality, data integrity, physical security, and applications.
- High level network requirements include services, device management and identity management.
- Services may be provided by a central authority and delivered through either centralized or distributed service mechanisms
- May want to consider the concept of a “trusted zone” and a “trusted vulnerable zone”.

Trusted Zones



Border Control Function - BCF

Planning

- Have a pre-plan. The TDoS attacks resulted in activation of a task force to provide best practices and much needed cooperation amongst multiple parties.
- Look into available security options for the networks all the way to the PSAP equipment level. Consider what your records systems will integrate with, your CAD and mobile requirements, recording and retention requirements, and integration of any outside network into your “closed” PSAP or jurisdictional systems.

APCO International

Leaders in Public Safety Communications™

FirstNet & Next Generation 9-1-1

Topics to Cover

- NG9-1-1 and FirstNet represent the “two halves” of public safety request and response. The PSAP represents the “nerve center” in the middle.
- i3, IMS, or a combination of the two, either way, it’s Next Generation “stuff”
- PSAPs will be more than simply 9-1-1 centers or dispatch centers.
- The use of a standards based, non-proprietary approach is critical to success.

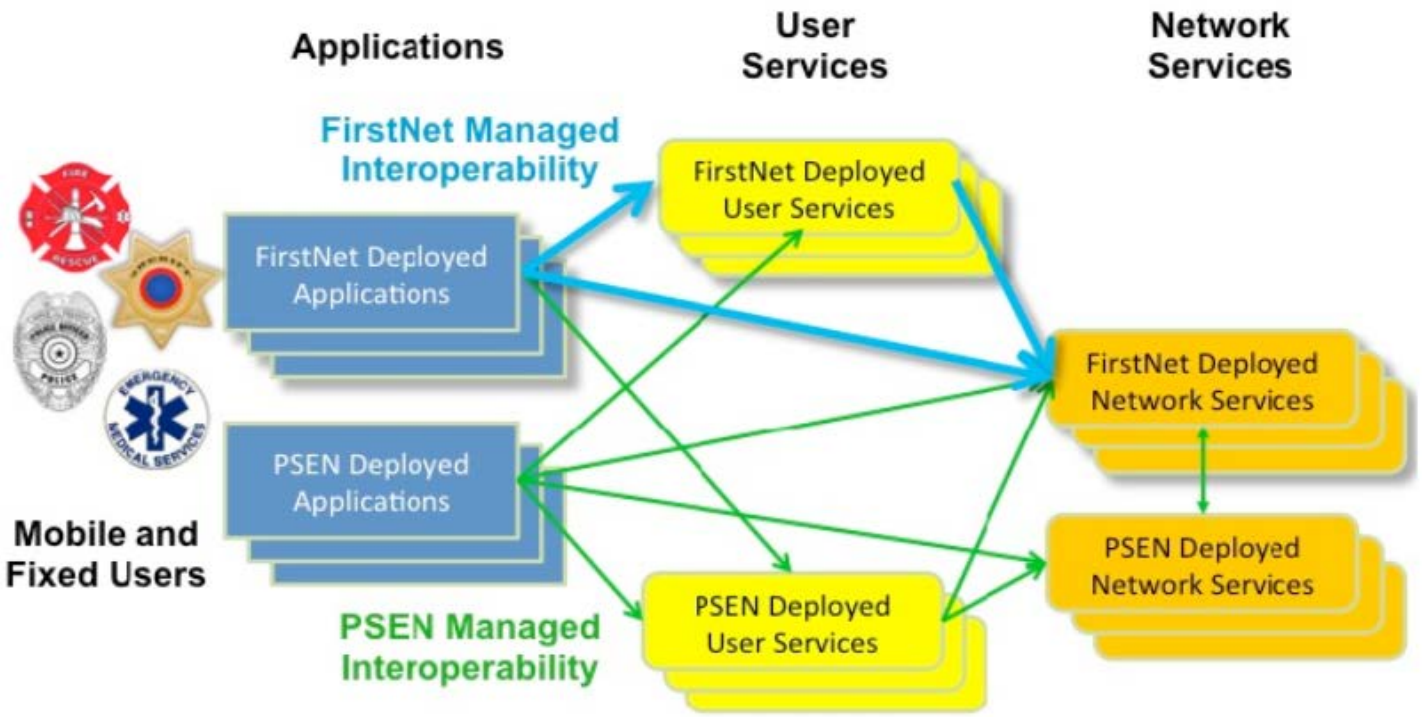
National Connectivity

Broadband

ESInets

Emergency Communications Stakeholders & Partners

FirstNet Apps



Examples			
	• Advanced multimedia telephone	• Cellular Telephony	• Location
	• Video	• Video	• Service Discovery
	• PTT Apps	• Direct-mode PTT (not for Launch)	• DNS
	• Fire situational awareness, etc.	• Messaging, etc.	• Identity
	• Computer-Aided Dispatch		• Dynamic QoS, etc.

What is the Common Denominator During an Emergency?

ALL Emergencies are LOCAL.

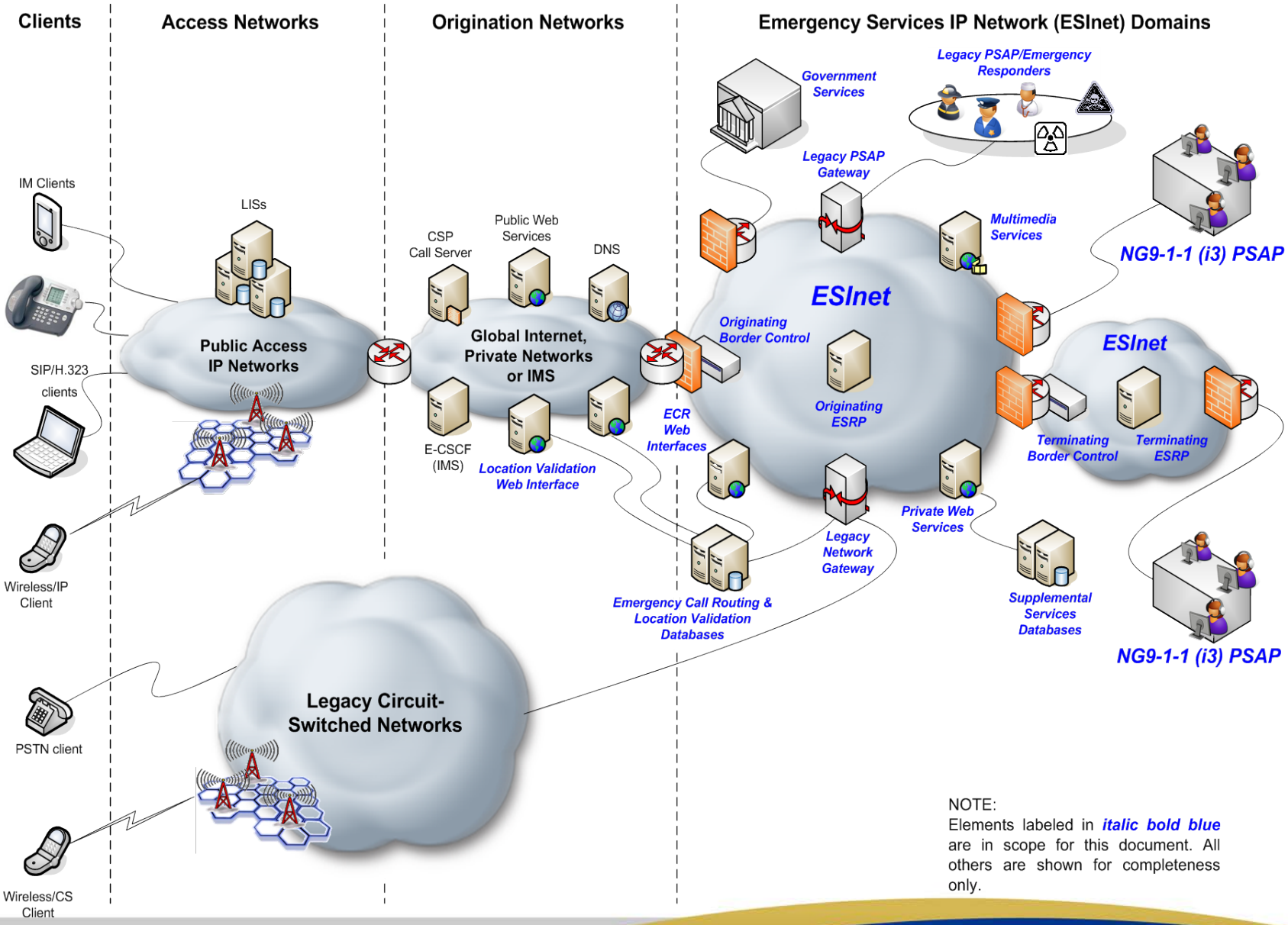
Interoperability of both voice and data services is critical as incidents unfold and expand.

Next Generation services can provide that interoperability

Can we truly achieve Interoperability?

- Multiple considerations
  - 9-1-1 interop between PSAP and jurisdictions
  - CAD to CAD
  - RMS data sharing
  - Intelligent databases
  - Mobile aspect
  - P25 and Mission Critical voice

Session Initiation Protocol



NOTE:
Elements labeled in ***italic bold blue*** are in scope for this document. All others are shown for completeness only.

NG9-1-1 Transition

Evolution not Revolution

APCO International™

Emerging Technology Forum

Q & A

APCO International

Leaders in Public Safety Communications™