ASSURE911

Next Generation 9-1-1 Texting, Video Calling and Network Management

October 2012
IPSTA Conference

Welcome

Barbara Kemp, Assure911

IIT 911 Task Force Chairperson
IIT ICE5 Project Manager
CSI Consultant
bk@assure911.net

Brian Knueppel, Acme Packet Systems

NENA ICE5 Co-chair
bknueppel@acmepacket.com

David Staub, Assure911

IIT Lab Project Mentor
dbs@assure911.net

Topics

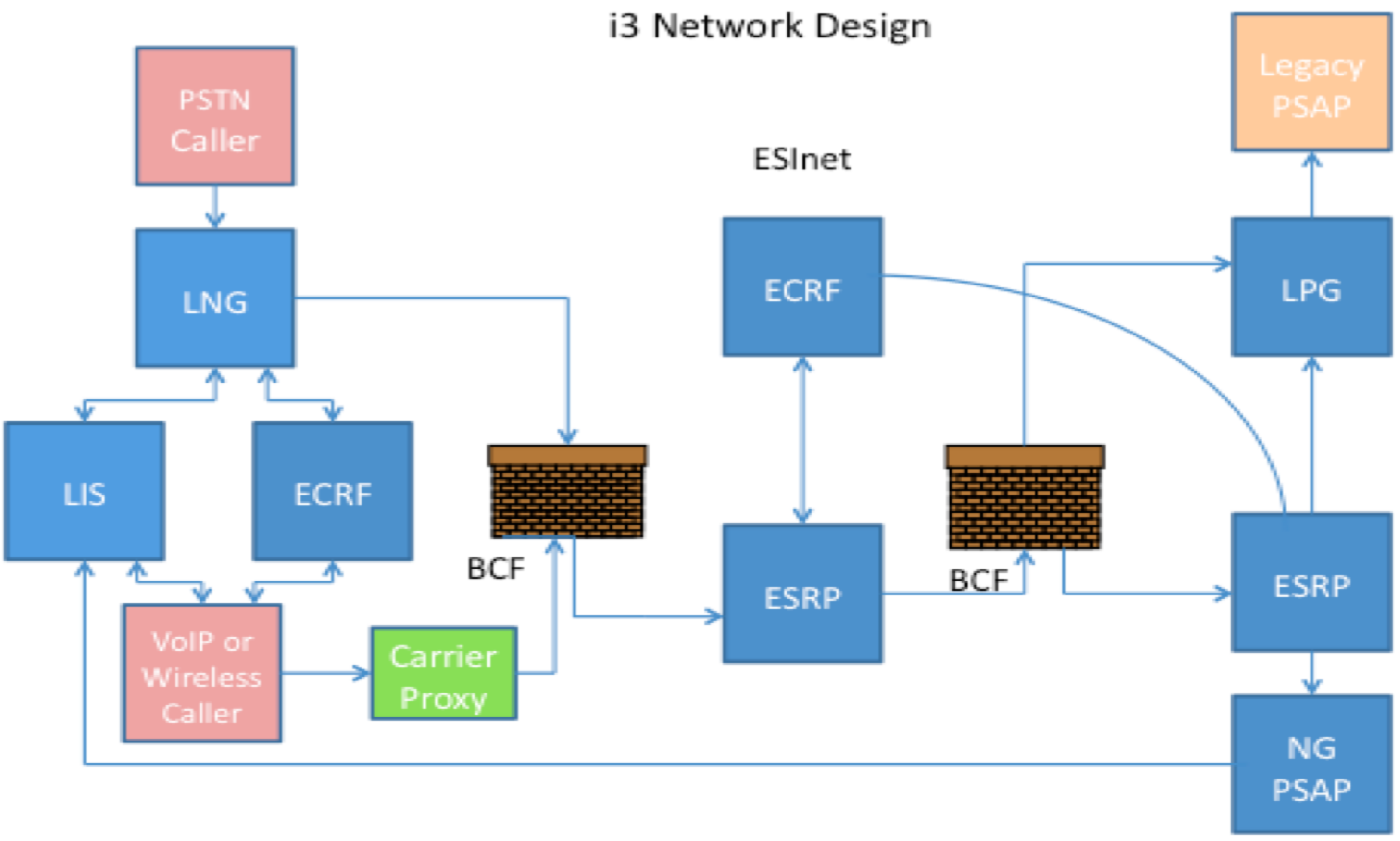
- Purpose
- NG 9-1-1 Call Flow
- NENA ICE5 at IIT RTCL
- ESInet Security
- NG 9-1-1 System Reliability
- Network Management
- Path Forward

Purpose

- Public Safety Migration to NG 9-1-1
  - Experience
  - Public Safety
    - Legal
    - Financial
    - Managerial
  - Challenges
    - Maintenance
      General Overload
    - Event Related Overload

NG 9-1-1 Call Flow

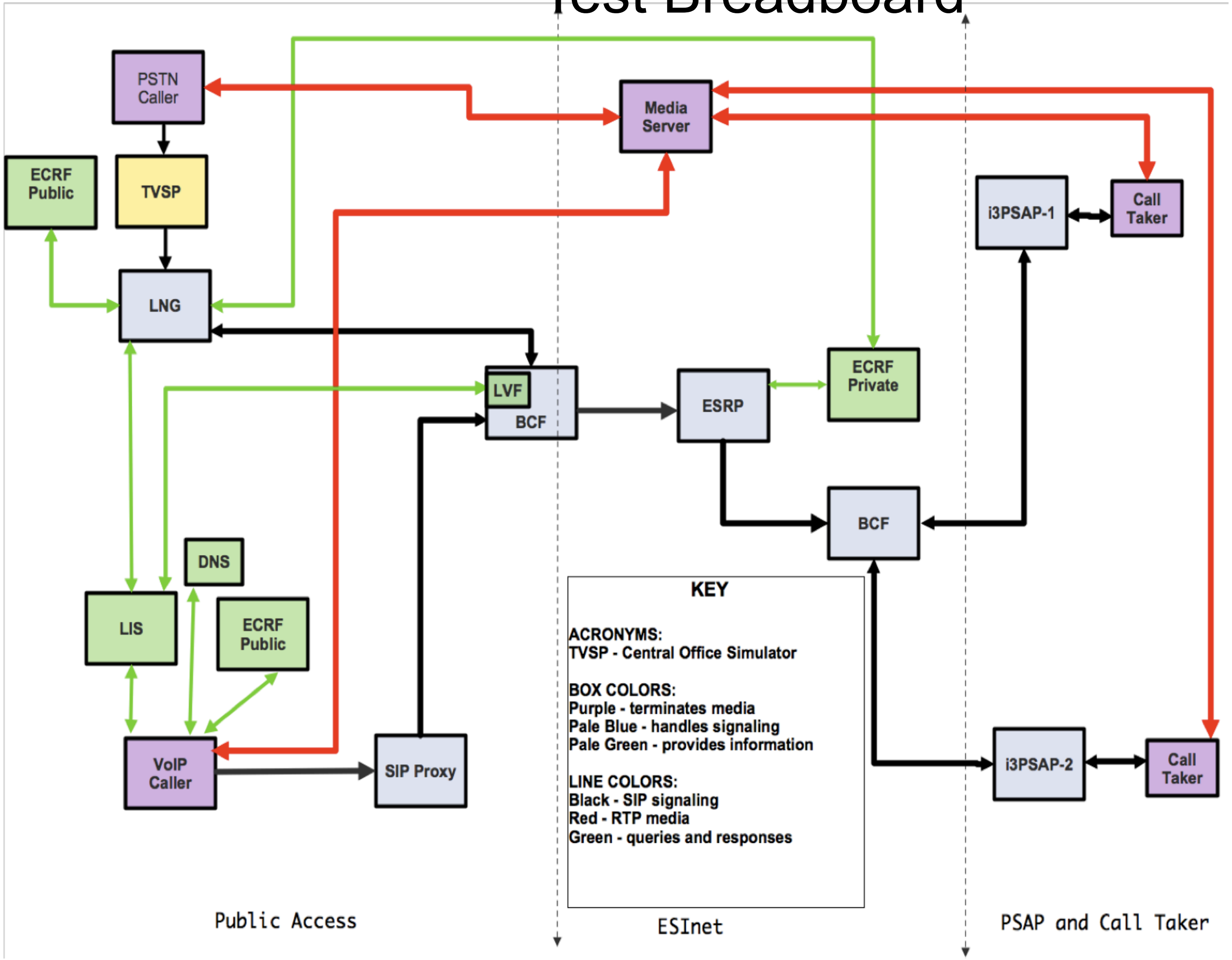
ASSURE911



Call Flow Drawing courtesy of Brian Rosen; IIT RTCL Conference and Expo Tutorial 2011

Full text on www.assure911.net

Test Breadboard



KEY

ACRONYMS:
TVSP - Central Office Simulator

BOX COLORS:
Purple - terminates media
Pale Blue - handles signaling
Pale Green - provides information

LINE COLORS:
Black - SIP signaling
Red - RTP media
Green - queries and responses

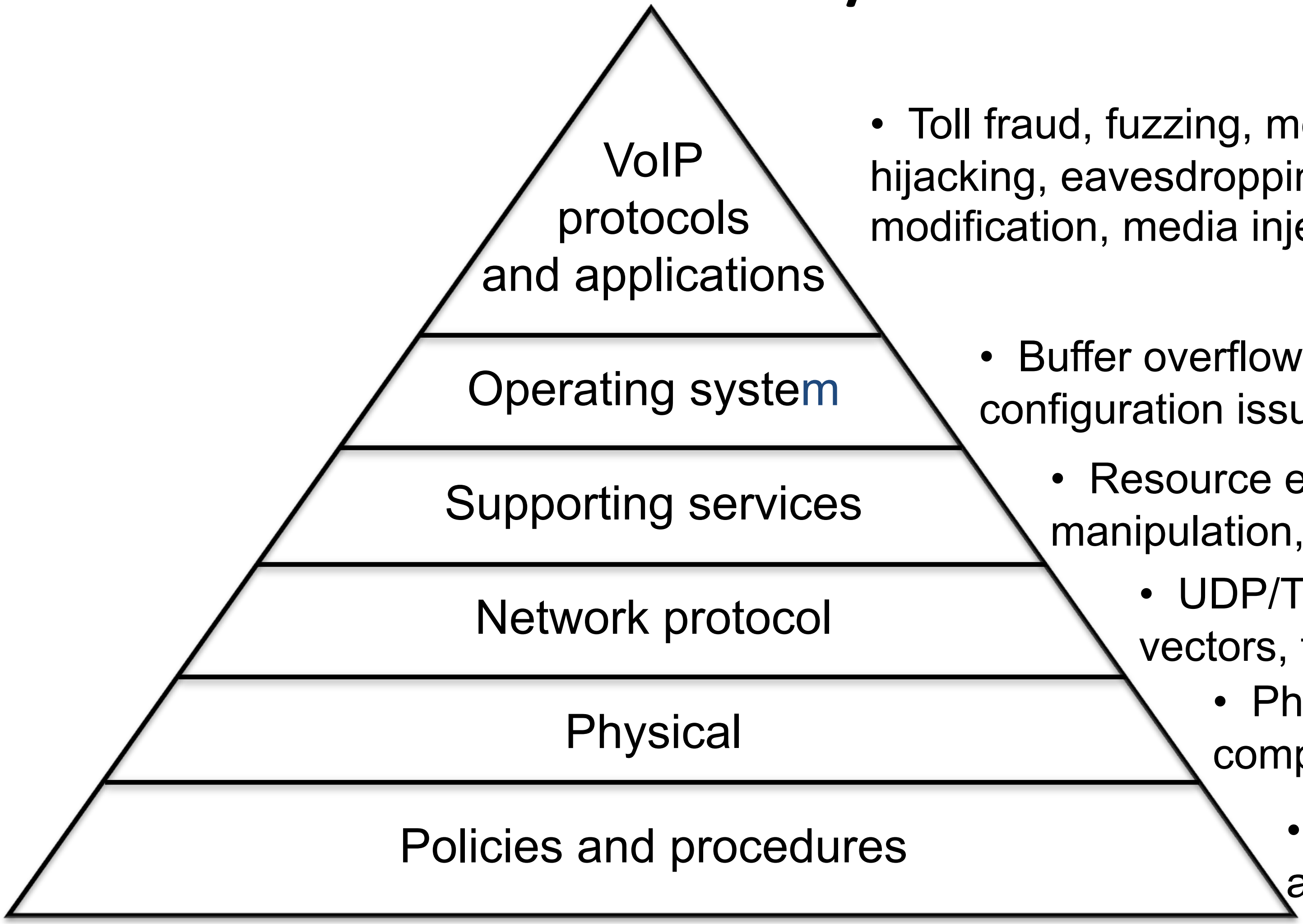
ICE 5 Event at IIT RTCL

Security

- Brian Knueppel – Acme Packet

  bknueppel@acmepacket.com
- Goal: Protect the Next Generation 9-1-1 Network against Denial of Service Attacks and Overloads
- NENA definition of a Border Control Function (BCF)
- Product: Session Border Controller (SBC) – more than a firewall

Where are Risks/Vulnerabilities



VoIP protocols and applications

Operating system

Supporting services

Network protocol

Physical

Policies and procedures

- Toll fraud, fuzzing, message floods, hijacking, eavesdropping, MITM call modification, media injection
- Buffer overflows, malware, DoS, configuration issues
- Resource exhaustion, account manipulation, covering tracks
- UDP/TCP floods, ICMP vectors, fuzzing, D/DoS
- Physical access compromise, reboot
- Weak passwords, abuse of services

Threat Landscape

Threat	Example	Result
Reconnaissance scan	Address or port scan used to footprint network topology	Targeted denial of service, fraud, theft of service
Man-in-the-middle	Attacker intercepts session to impersonate (spoof) caller	Targeted denial of service, breach of privacy, fraud, theft
Eavesdropping	Attacker sniffs session	Breach of privacy, fraud, theft
Session hijacking	Attacker compromises valuable information by re-routing call	Breach of privacy, fraud, theft
Session overloads	Excessive signaling or media (malicious, non-malicious)	Denial of service
Protocol fuzzing	Malformed packets, semantically or syntactically incorrect flows	Denial of service
Media injection	Attacker inserts unwanted or corrupt content into messages	Denial of service, fraud

Border Control Function (BCF)

- A BCF sits between external networks and the ESInet and between the ESInet and agency networks. All traffic from external networks transits a BCF.
- The BCF comprises several distinct elements pertaining to network edge control and SIP message handling.
- Border Firewall
  - Access control
  - Protect from malware attacks
- Session Border Control
  - Prevention
  - Detection
  - Reaction

Session Border Control (SBC)

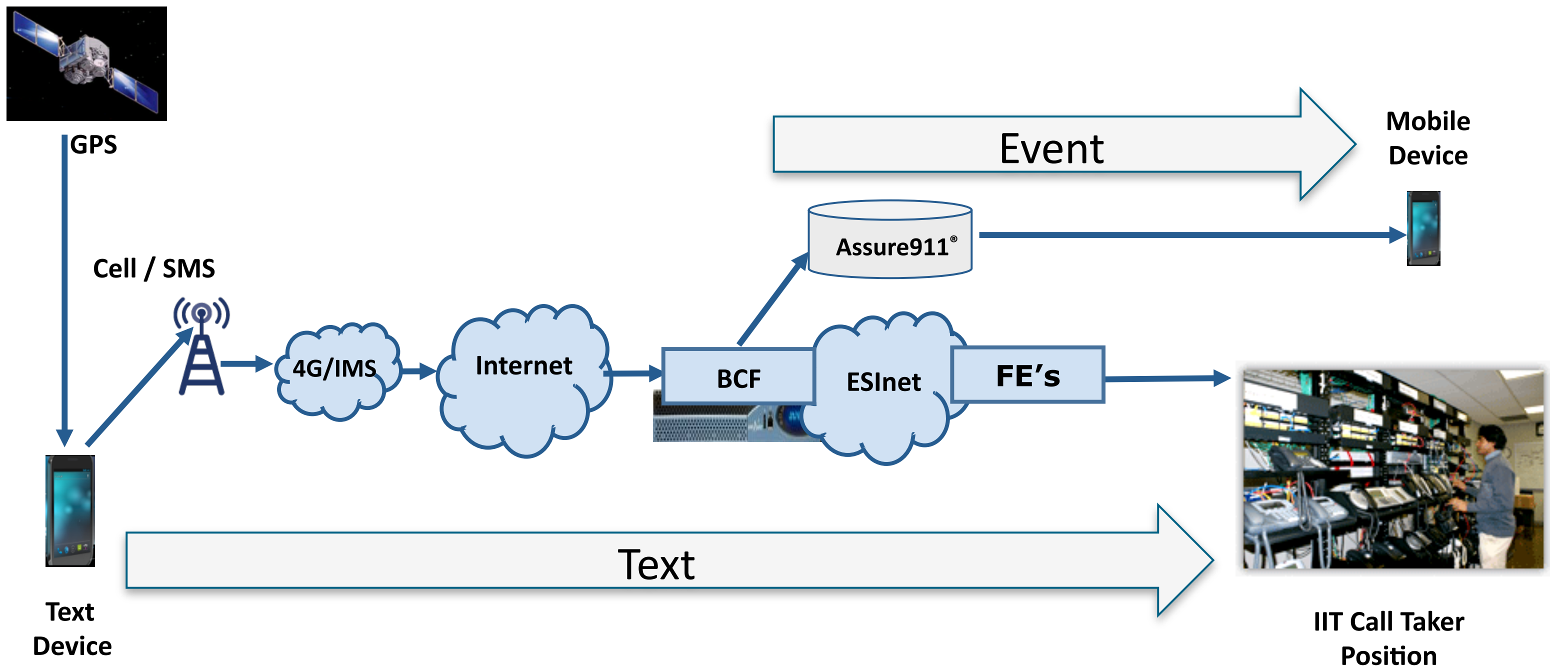
- Protecting live global IP communications networks
- Functional element within BCF
  - DOS/DDOS protection, overload, resource admission control
  - SIP normalization
  - Resolve NAT issues
  - Open/close pinholes
  - B2BUA
  - IPV4-IPV6 interworking
  - VPN bridging
  - Transport and encryption: signaling and/or media
  - QoS marking, priority, reporting
  - Call detail records
  - Transcoding

NENA Reference Documents

- Requirements, standards, procedures, practices
  - Reference NG-SEC 75-001
  - Auditing, and assessing levels of security and risk to NG9-1-1 entities, assets or elements, and exception approval / risk acceptance process in the case of non-compliance to these guidelines
- Network
  - Reference NID 08-506
  - Information that will assist in developing the requirements for and/or designing ESInets capable of meeting the requirements of an NG9-1-1 system
- Functional Elements
  - Reference NENA i3 08-003
  - Describes the detailed functional elements and interfaces to those functional elements

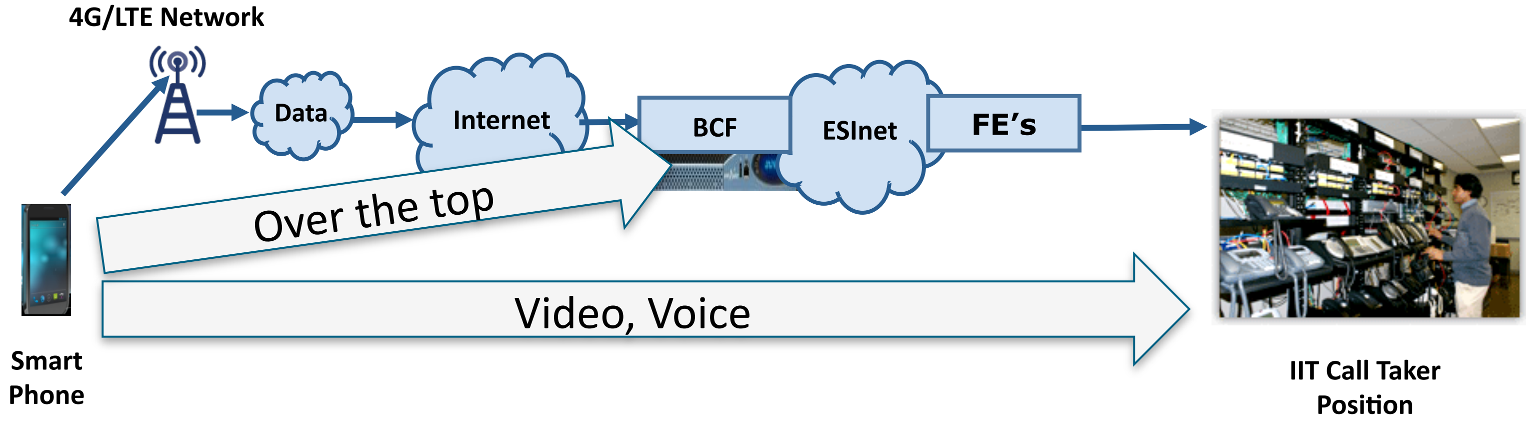
Secure Text Demo – with alert

- Cellular network origination (SMS)
- Using test number (not 911)
- 4G/IMS->i3 ESInet (secured)
- Event sent in parallel(keyword "bomb")



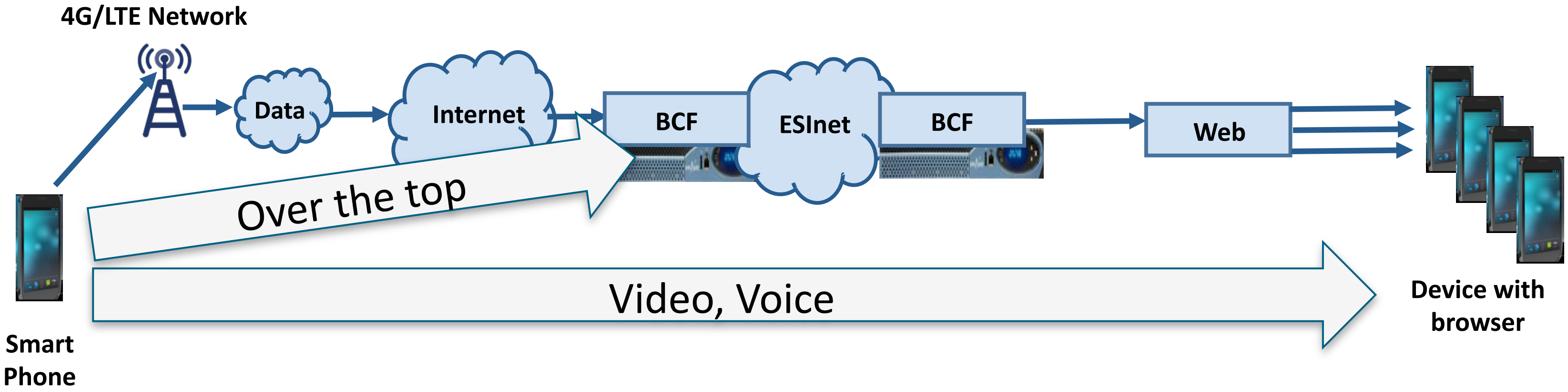
Secure Video Demo

- Android device
- Over the top 4G/LTE
- ESInet (secured)



Secure Video Demo – with broadcast

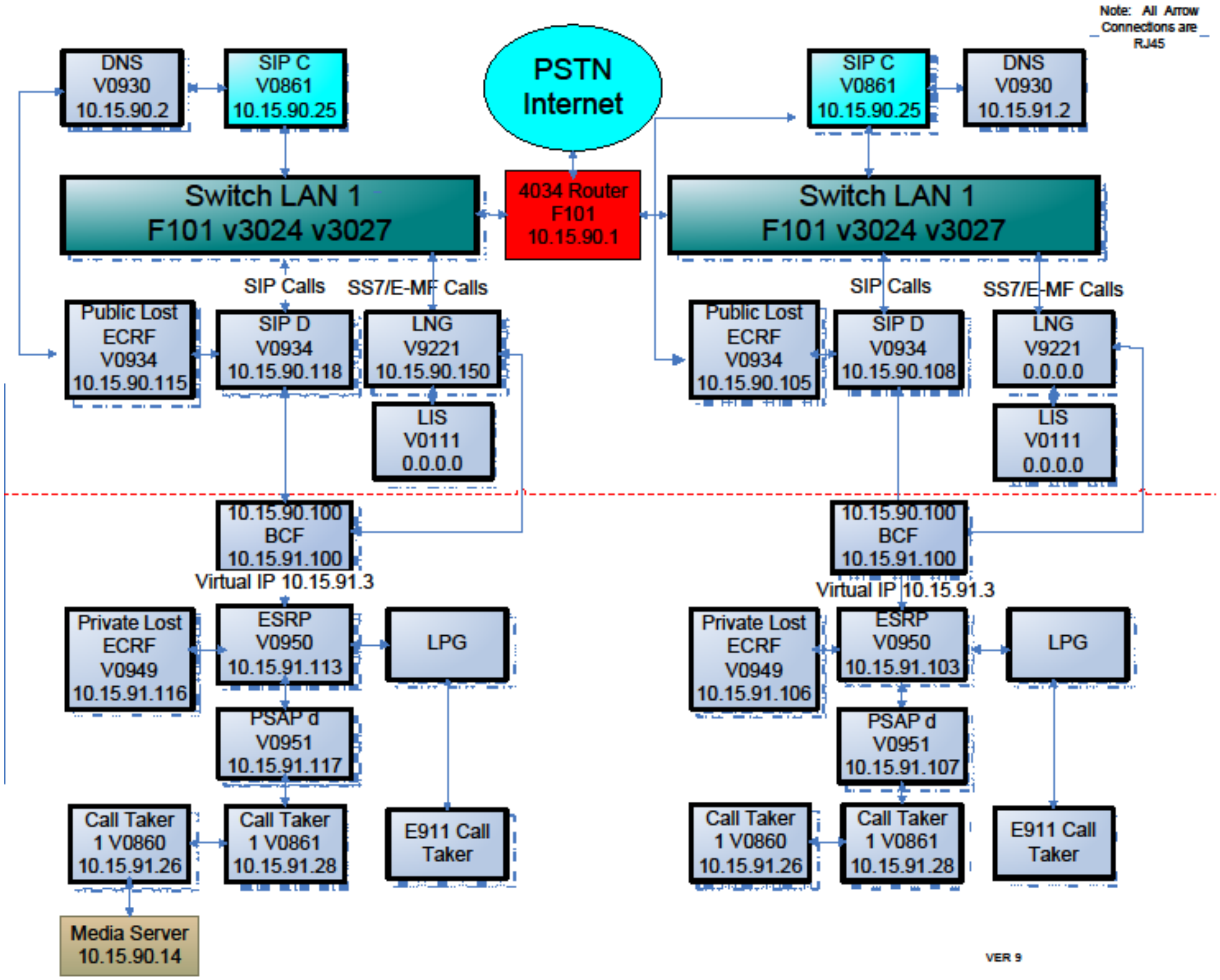
- Android device
- Over the top 4G/LTE
- ESInet (secured)



NG 9-1-1 System Reliability

- Testing at IIT funded by Assure911
  - Performed by Joe Cusimano and Kbrom Tewoldu
  - Dual Data Center Configuration
    - Duplex ESInets: Primary/Master- Standby/Slave
  - Resiliency to PSAP and ESRP Failures
    - Including use of IIT UCARP program for IP address resiliency
  - Security: Access Control
  - Performance Under Load

IIT RTCL ESInet Test Architecture



Note: All Arrow Connections are RJ45

DNS V0930 10.15.90.2

SIP C V0861 10.15.90.25

PSTN Internet

SIP C V0861 10.15.90.25

DNS V0930 10.15.91.2

Switch LAN 1 F101 v3024 v3027

4034 Router F101 10.15.90.1

Switch LAN 1 F101 v3024 v3027

SIP Calls

SS7/E-MF Calls

SIP Calls

SS7/E-MF Calls

Public Lost ECRF V0934 10.15.90.115

SIP D V0934 10.15.90.118

LNG V9221 10.15.90.150

Public Lost ECRF V0934 10.15.90.105

SIP D V0934 10.15.90.108

LNG V9221 0.0.0.0

LIS V0111 0.0.0.0

LIS V0111 0.0.0.0

10.15.90.100 BCF 10.15.91.100

Virtual IP 10.15.91.3

10.15.90.100 BCF 10.15.91.100

Virtual IP 10.15.91.3

Private Lost ECRF V0949 10.15.91.116

ESRP V0950 10.15.91.113

LPG

Private Lost ECRF V0949 10.15.91.106

ESRP V0950 10.15.91.103

LPG

PSAP d V0951 10.15.91.117

PSAP d V0951 10.15.91.107

Call Taker 1 V0860 10.15.91.26

Call Taker 1 V0861 10.15.91.28

E911 Call Taker

Call Taker 1 V0860 10.15.91.26

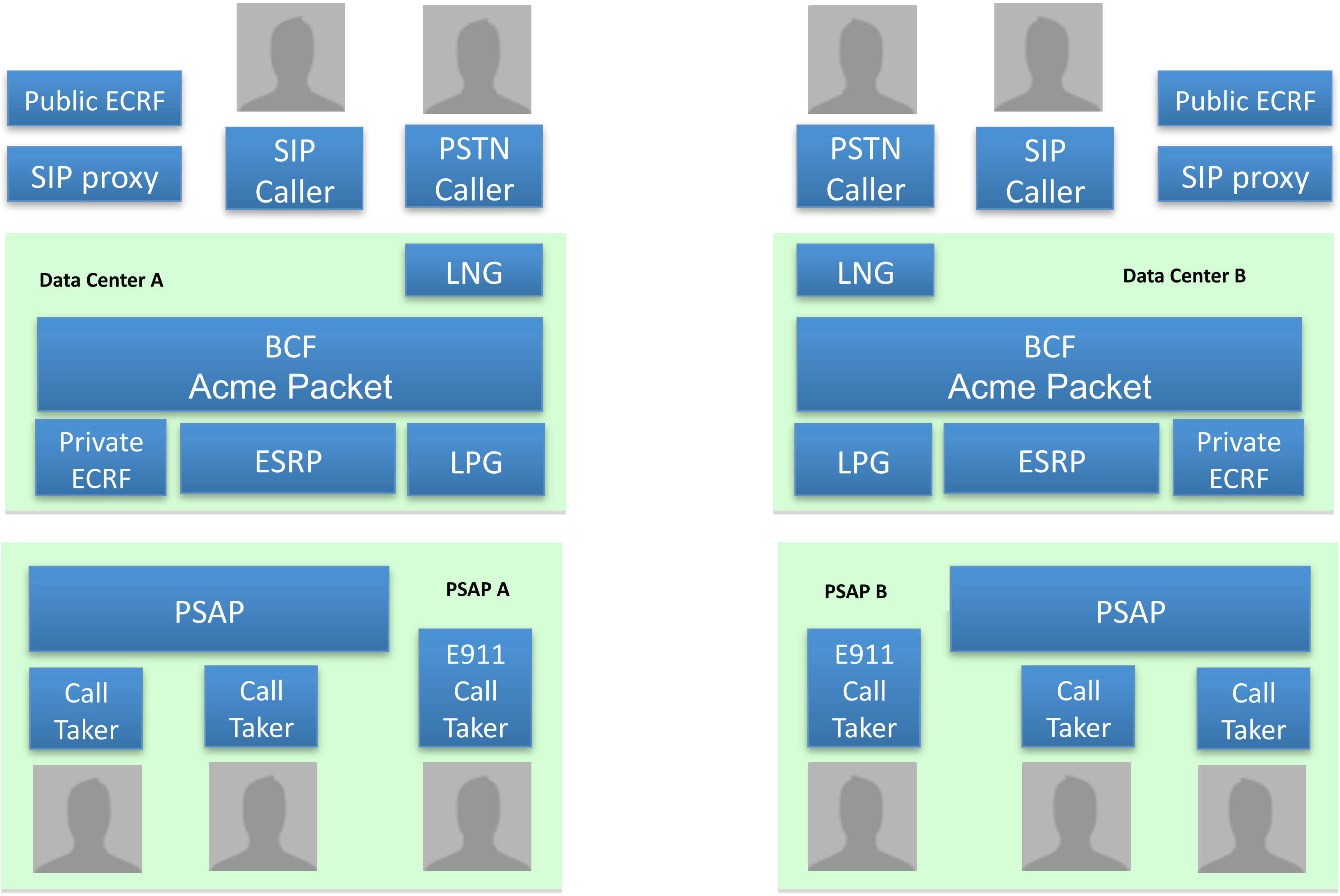
Call Taker 1 V0861 10.15.91.28

E911 Call Taker

Media Server 10.15.90.14

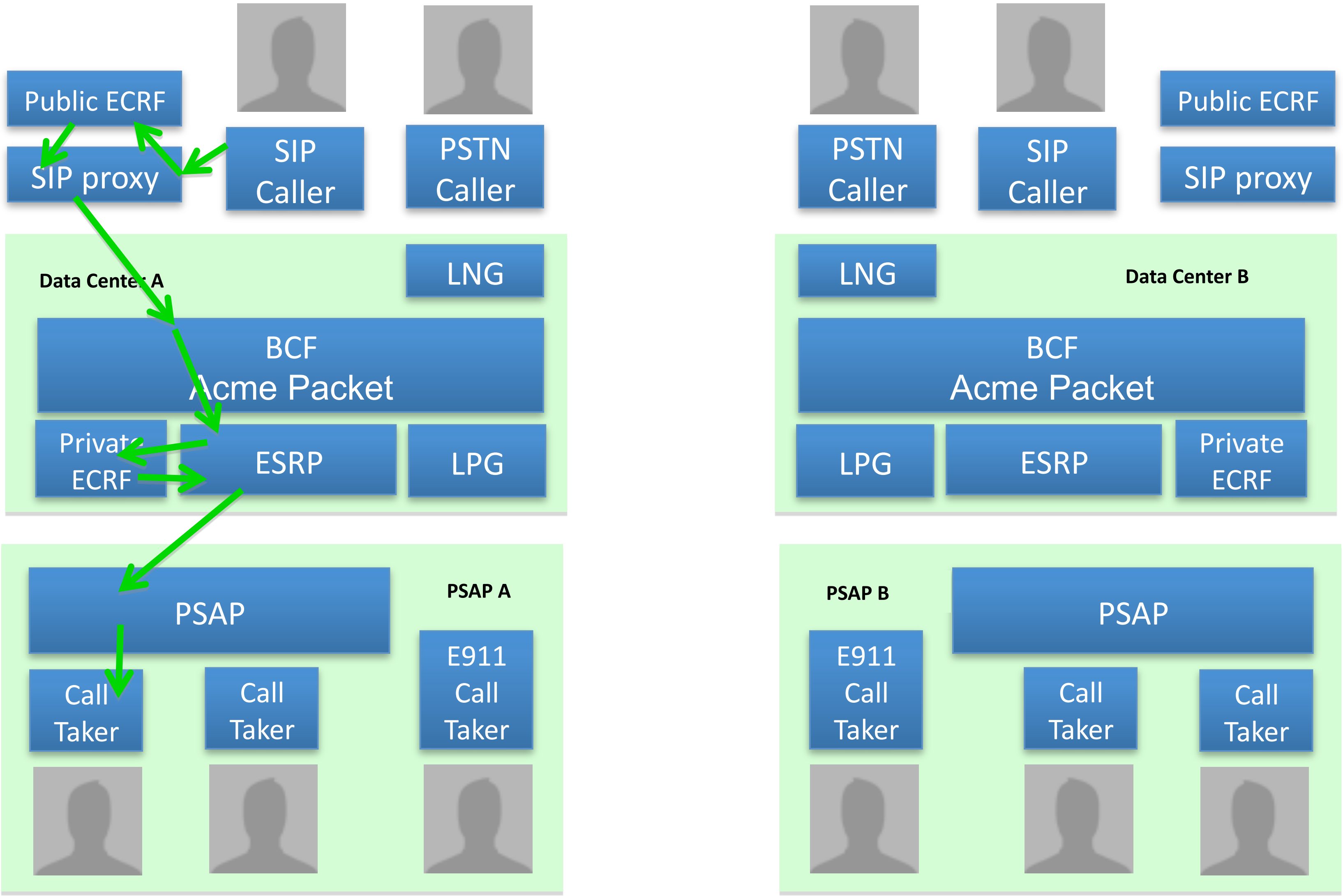
VER 9

IIT RTCL ESInet Test Architecture

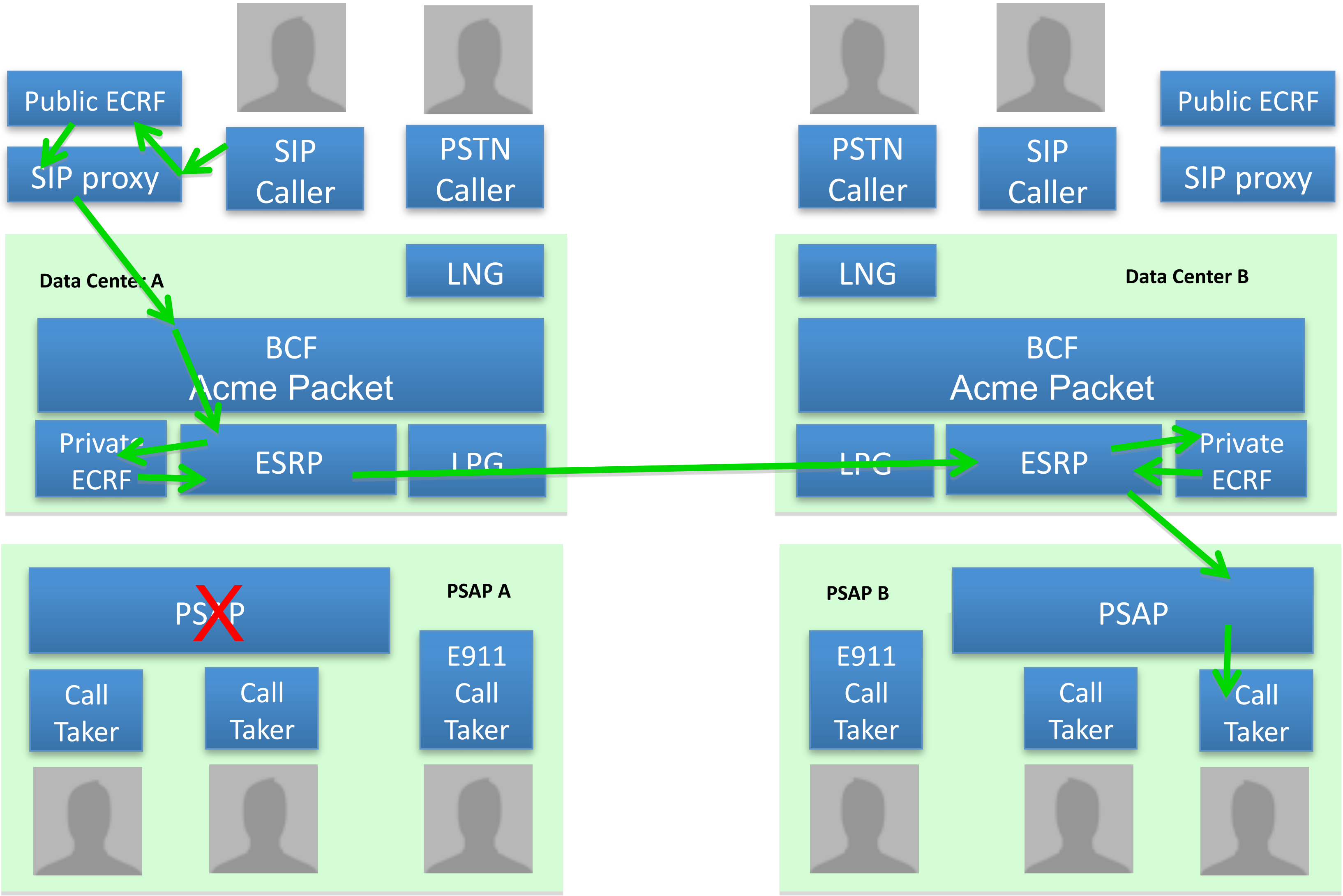


IIT Lab Testing - Typical SIP Call

ASSURE911

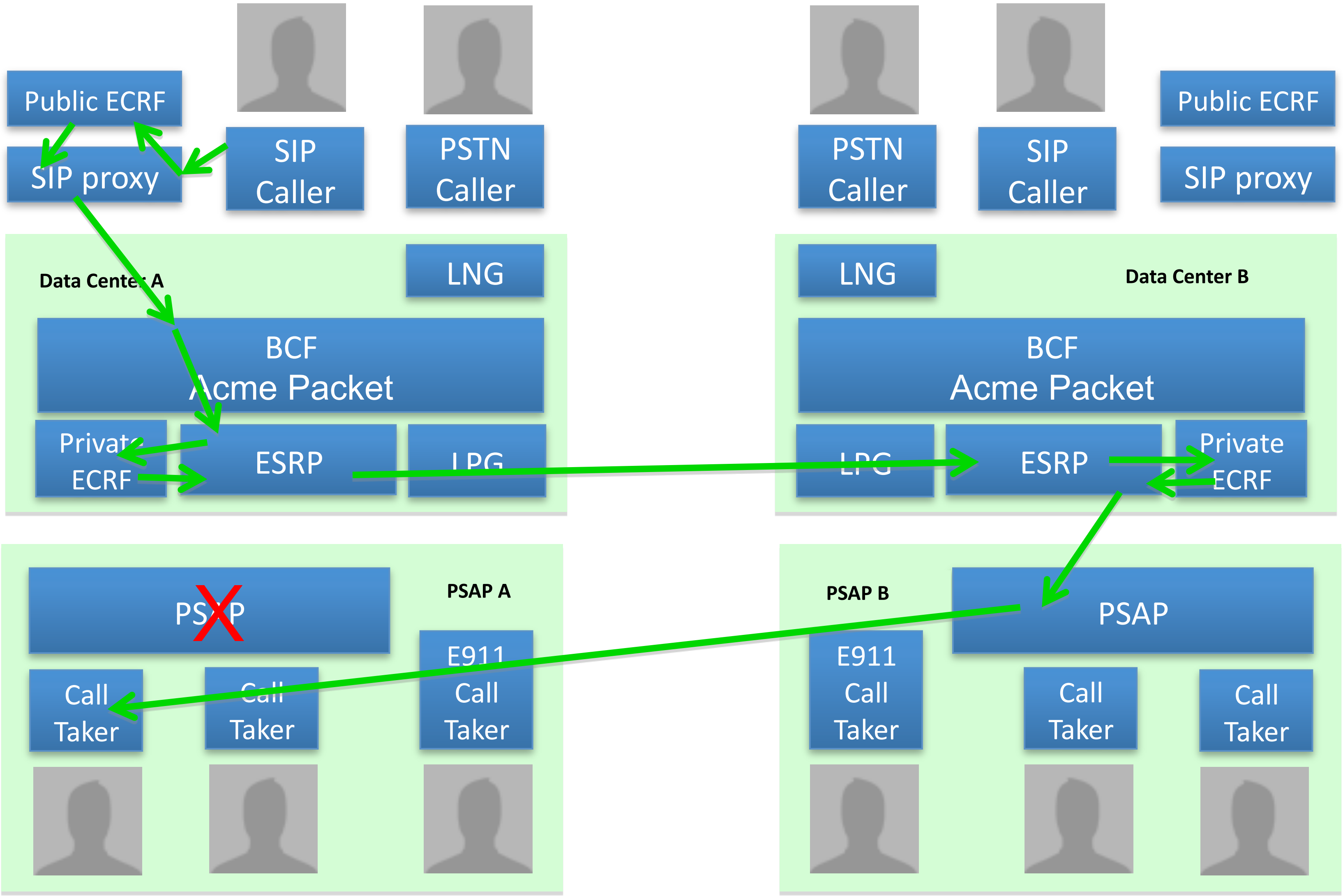


PSAP Failure



Partial PSAP Failure (Call Takers can register to PSAP B)

ASSURE911

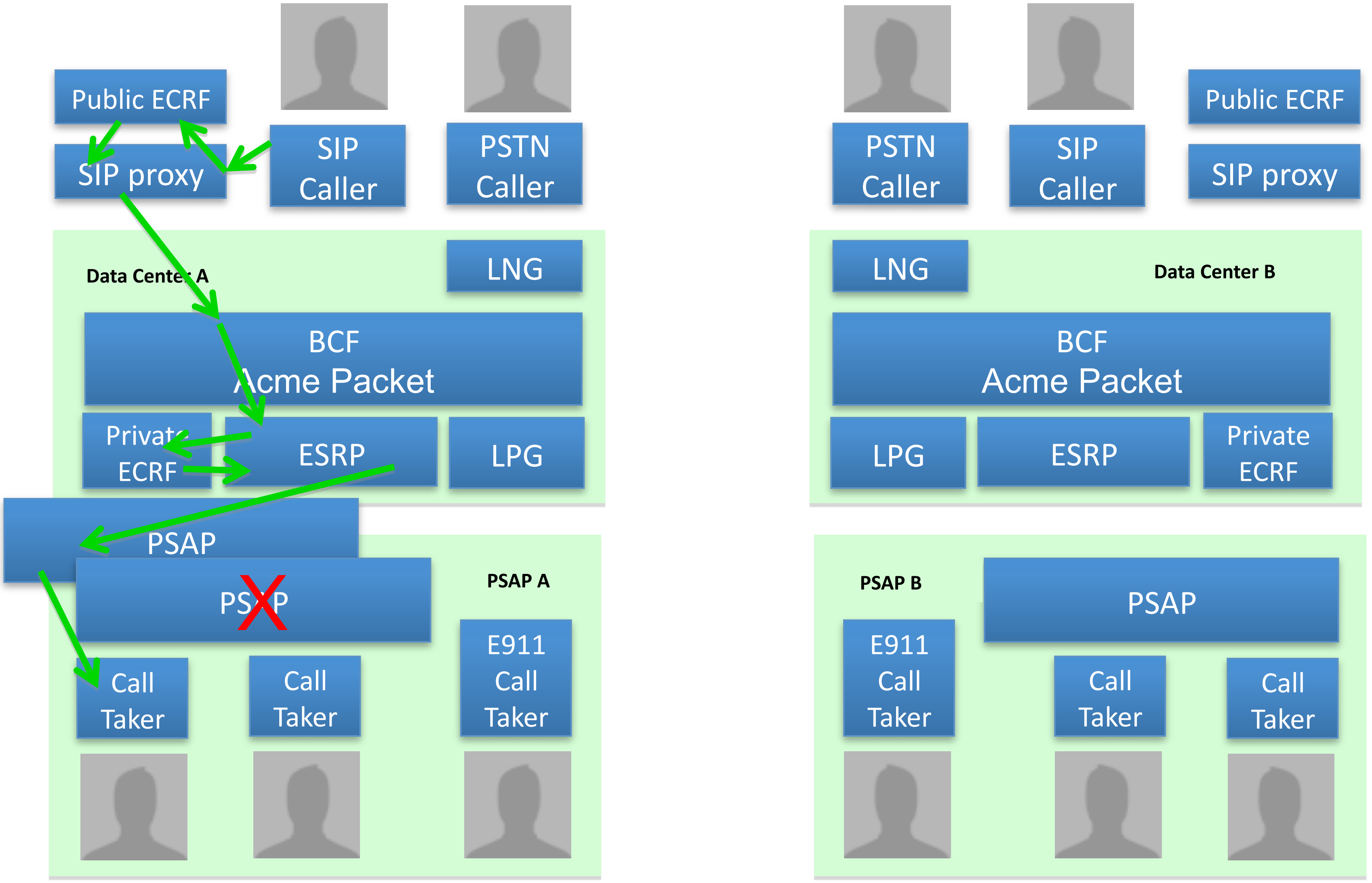


PSAP Resiliency

- Layer 1 and Layer 2
- UCARP Program running in Background for PSAP Test
- Remove RJ45 from ESInet Primary PSAP 10.15.91.117.
- System Switches from Primary Master to Backup PSAP IP Address 10.15.91.107
- Re-Register PSAP
- Initiate Test Call and Observe Invite Message in the Wire Shark Trace for conformance

PSAP Server Failure - IP address taken over by backup

ASSURE911



ESRP Resiliency

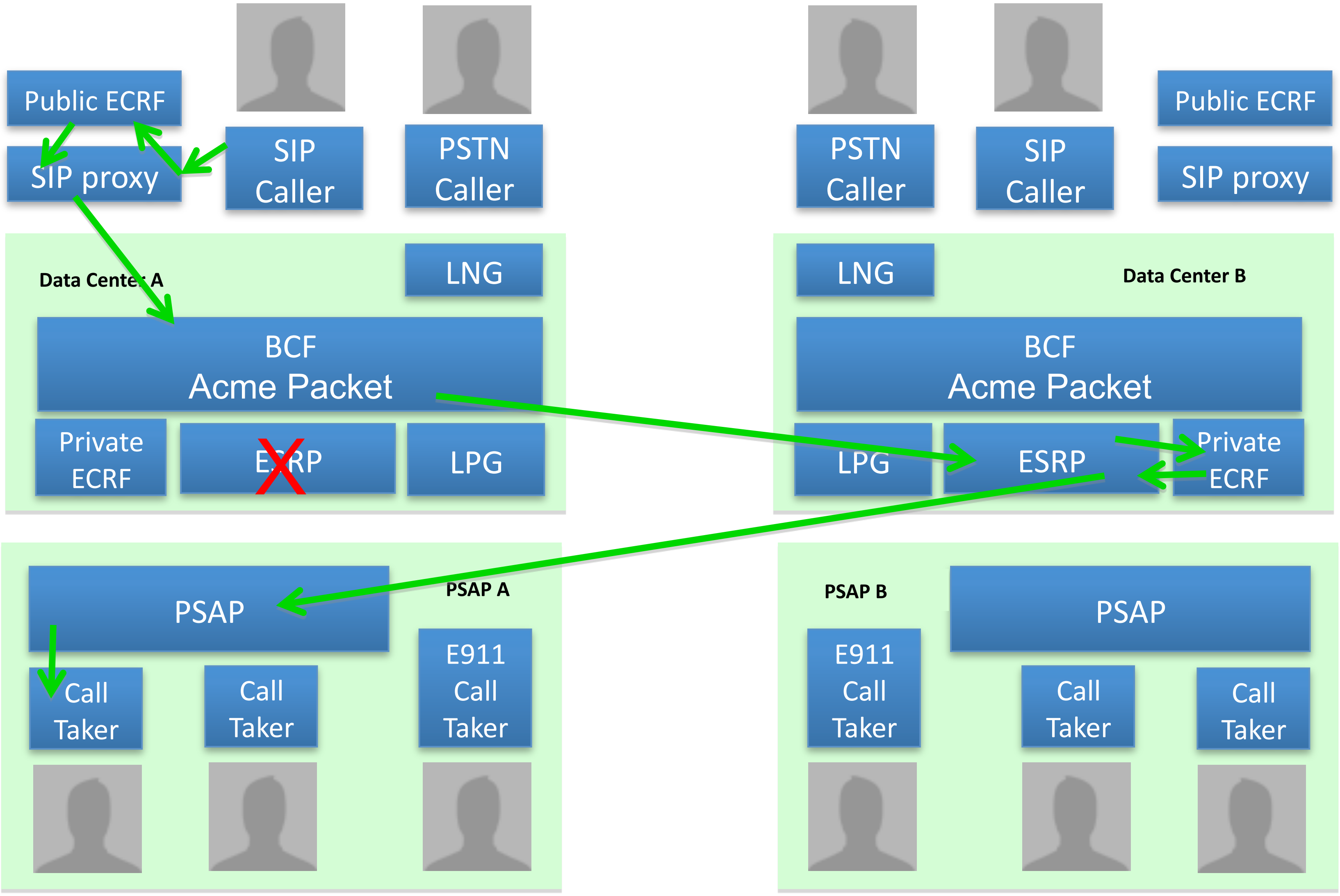
- Layer 5 SIP Message Routing Geographic Redundancy
- Acme Packet Session Border Controller (SBC) Configured to hunt to Alternate ESInet ESRP on failure

- Remove RJ45 from Primary ESRP
- Initiate test call and observe Wire Shark Trace
- Invite message indicates routing to alternate ESRP

- The SBC can be configured to also route invite messages alternately between both ESRPs (Round Robin)

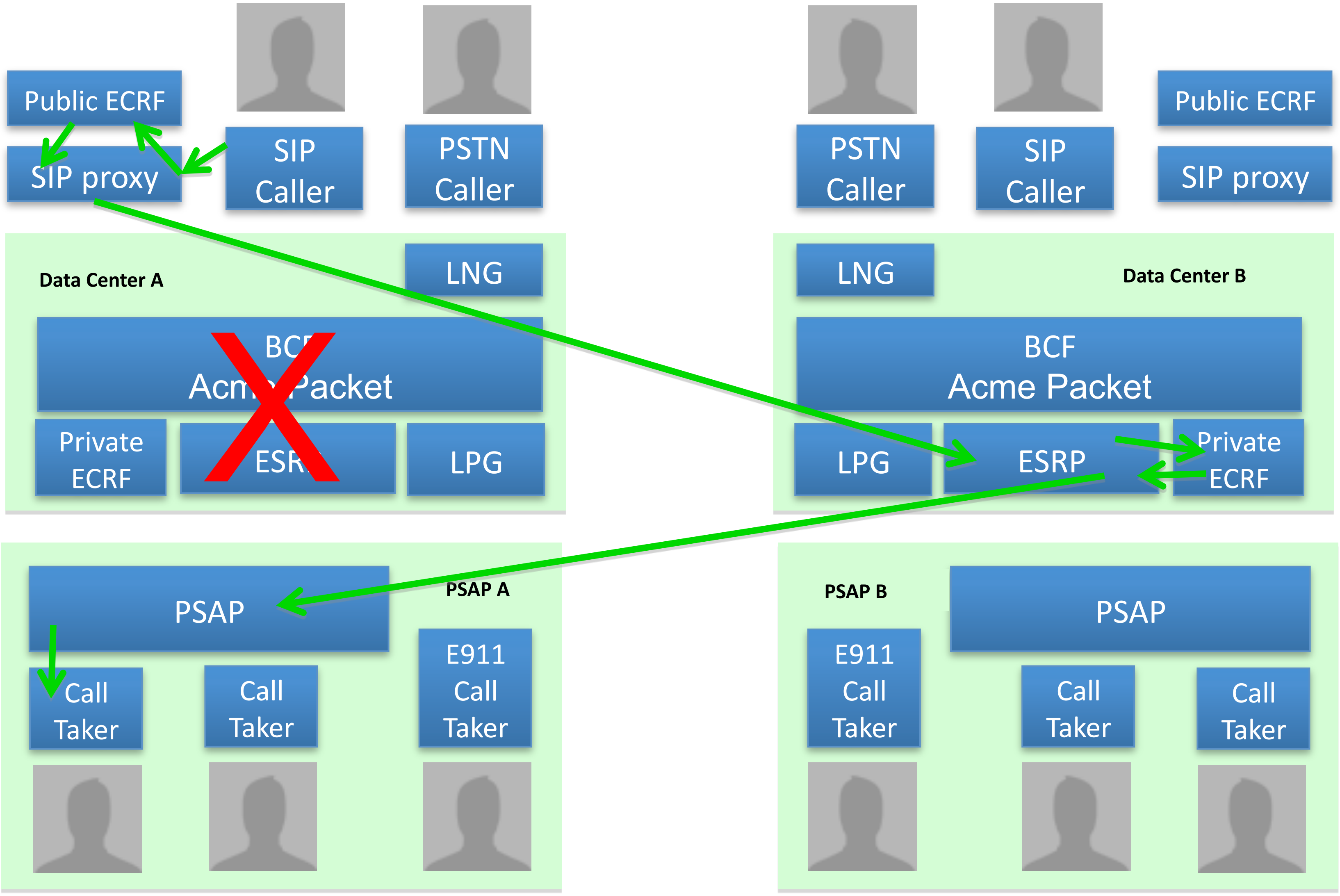
ESRP Failure

ASSURE911



Data Center Failure

ASSURE911



Security: System Access List

- Once configured with an IP address only addresses on the list are allowed access
- Configure System Access List Using IP Addresses 75.25.58.213 and Laptop LAN Address 10.10.10.20 Netmask 255.255.255.0
- Access Session Border Controller Management Port 10.10.10.17
- Remove 10.10.10.20
- Access SBC a 2nd time connection is refused

Performance

- Using the MU-8000 to initiate multiple invites to the ESInet – simulate DDoS
- Session Border Controller System Control List configured to restrict allowable session invites
- Access System Control List and set MU-8000 peer IP address 10.15.91.200 Thresholds set for 5
- Observe Wire Shark Traces to view allowed invite messages

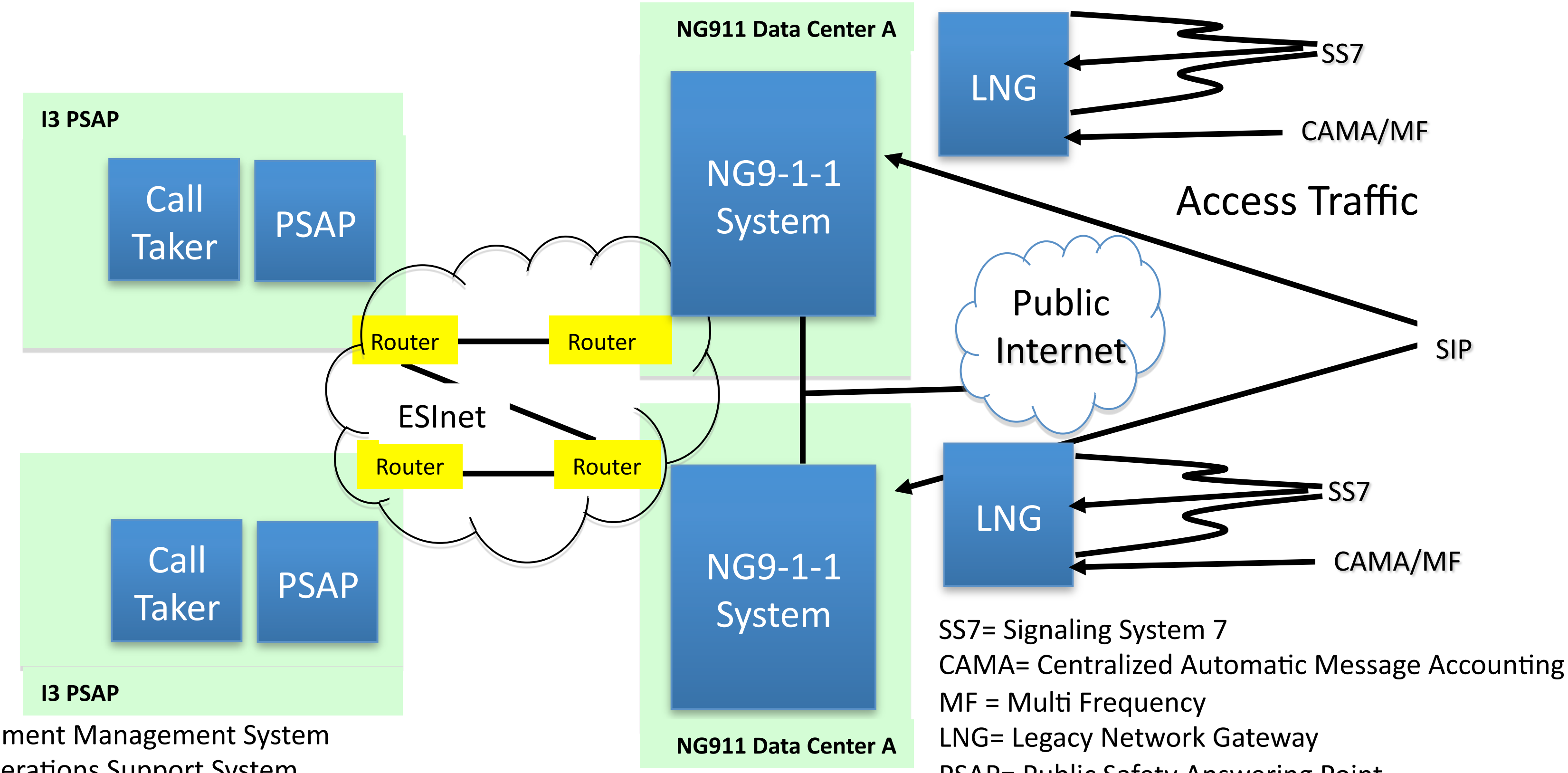
Network Management

End to End Network Management

Demonstration for Public Safety

NG 9-1-1 Systems are multi-provider

ASSURE911

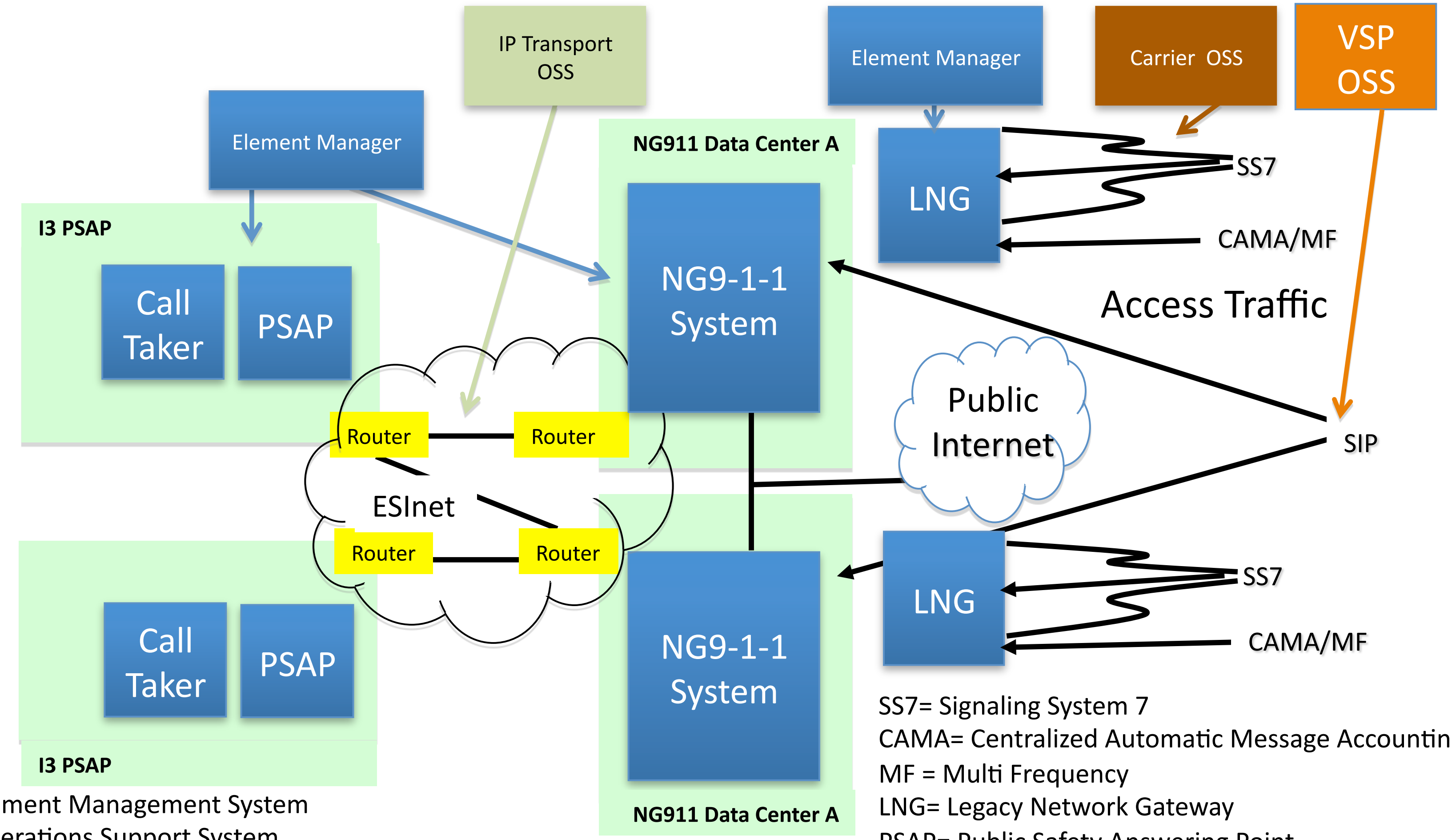


SS7= Signaling System 7
CAMA= Centralized Automatic Message Accounting
MF = Multi Frequency
LNG= Legacy Network Gateway
PSAP= Public Safety Answering Point
SIP = Session Initiation Protocol

EMS= Element Management System
OSS = Operations Support System
I3 = Current version of NENA NG 9-1-1 Specification

Each provider has their own solution for surveillance

ASSURE911

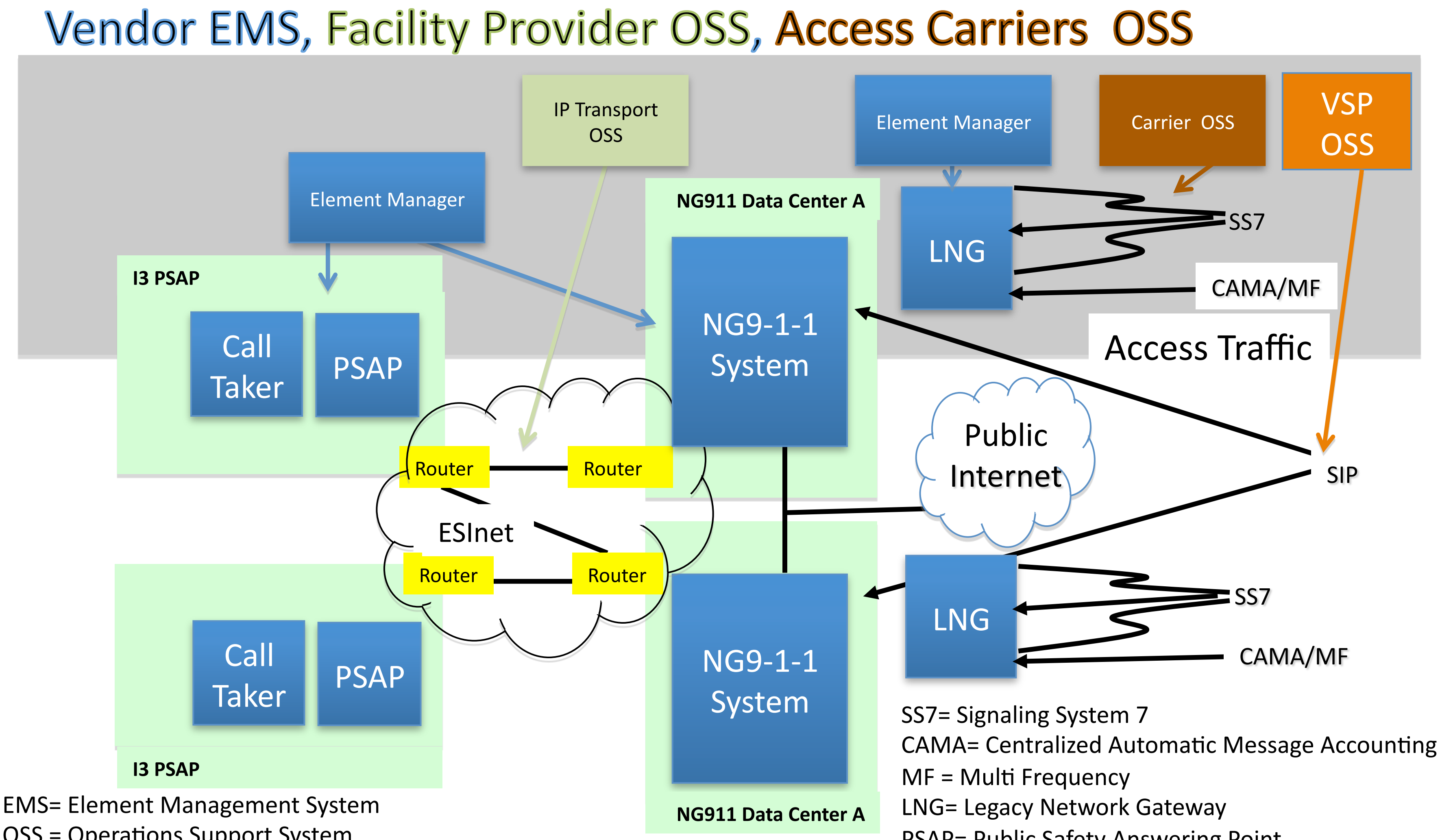


SS7= Signaling System 7
CAMA= Centralized Automatic Message Accounting
MF = Multi Frequency
LNG= Legacy Network Gateway
PSAP= Public Safety Answering Point
SIP = Session Initiation Protocol

EMS= Element Management System
OSS = Operations Support System
I3 = Current version of NENA NG 9-1-1 Specification

Highly reliable networks are proactively watched end-to-end

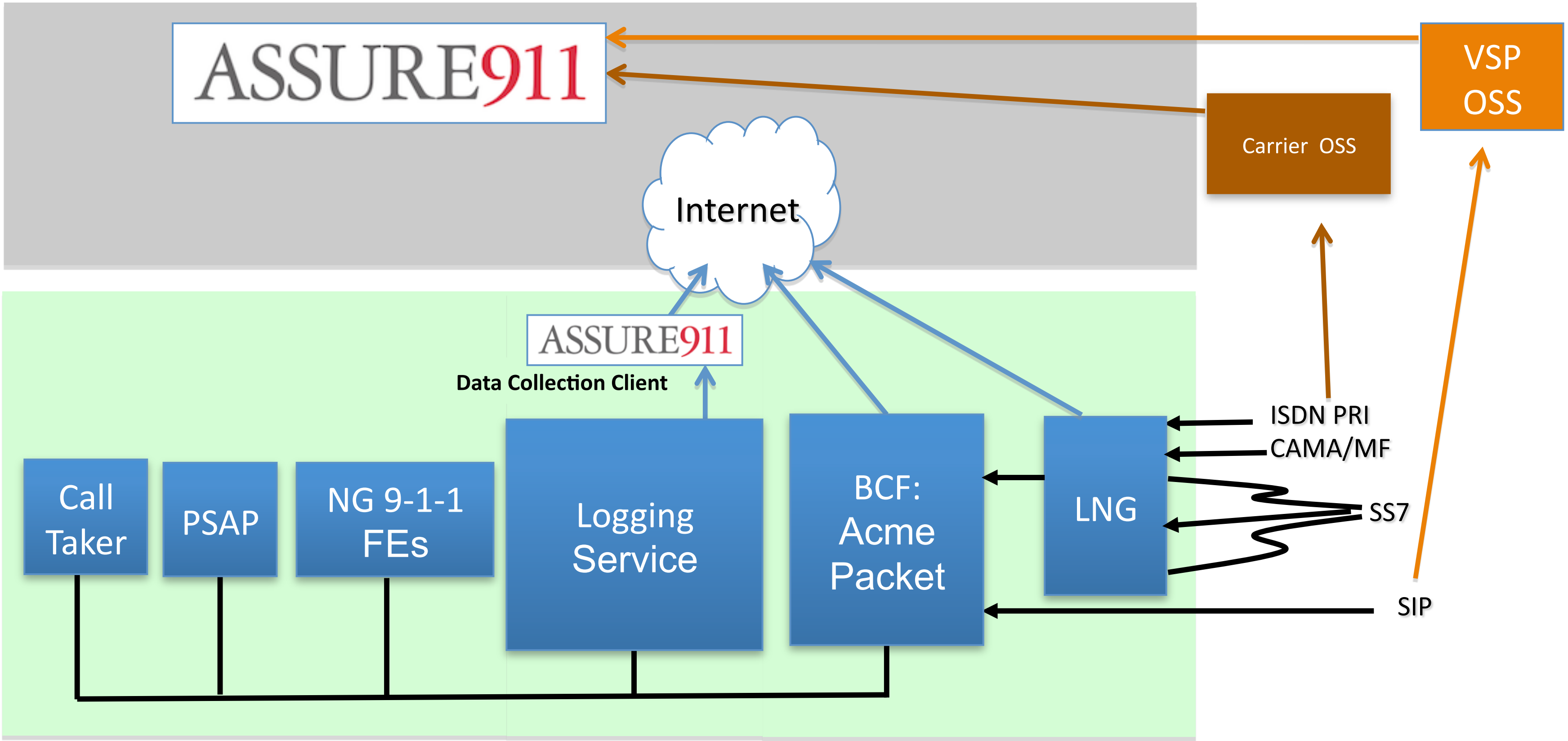
ASSURE911



SS7= Signaling System 7
CAMA= Centralized Automatic Message Accounting
MF = Multi Frequency
LNG= Legacy Network Gateway
PSAP= Public Safety Answering Point
SIP = Session Initiation Protocol

EMS= Element Management System
OSS = Operations Support System
I3 = Current version of NENA NG 9-1-1 Specification

End to End Monitoring

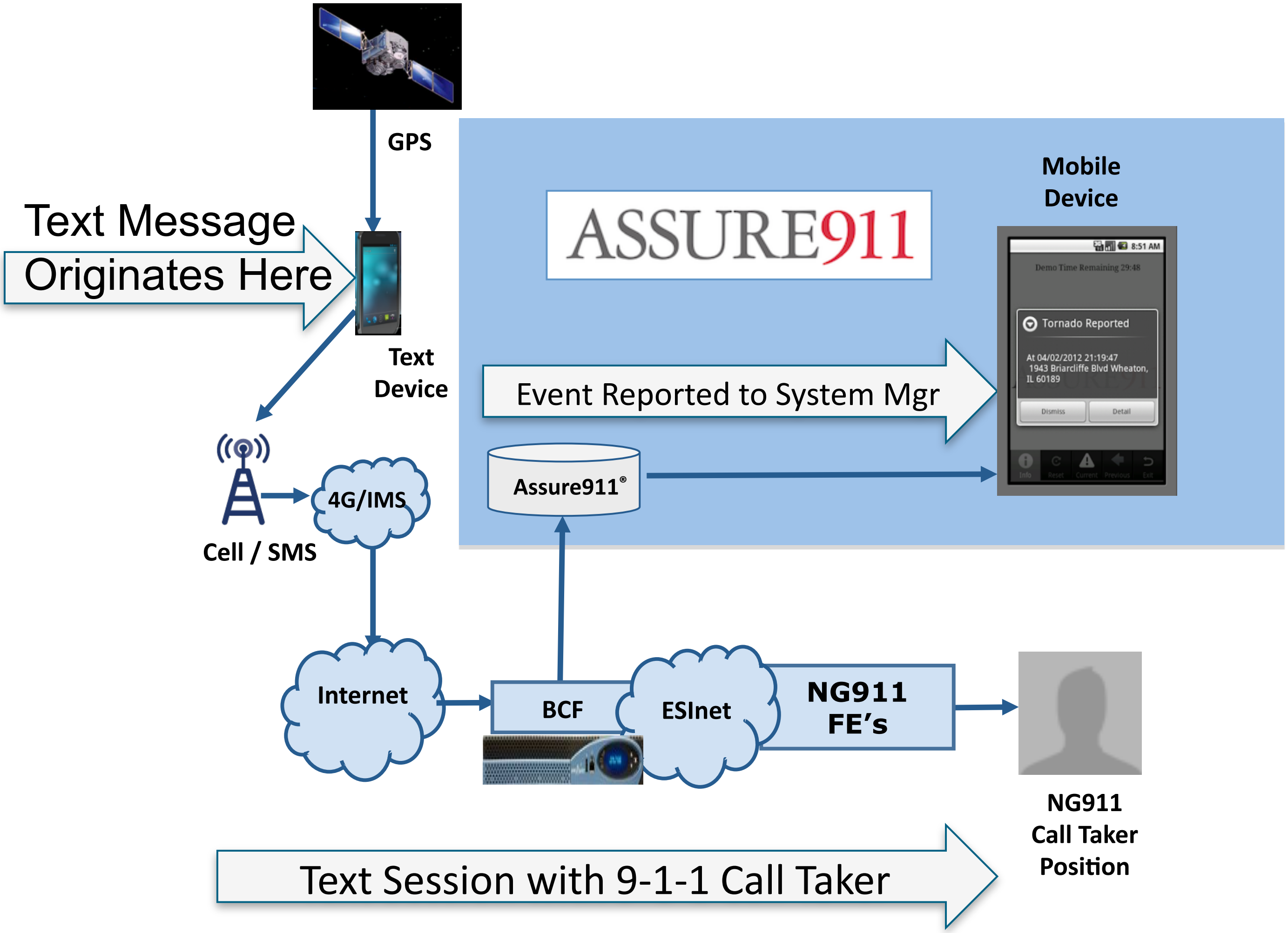


EMS= Element Management System
OSS = Operations Support System
I3 = Current version of NENA NG 9-1-1 Specification
SS7= Signaling System 7
CAMA= Centralized Automatic Message Accounting
MF = Multi Frequency

LNG= Legacy Network Gateway
PSAP= Public Safety Answering Point
SIP = Session Initiation Protocol
ISDN = Integrated Services Digital Network
PRI = Primary Rate Interface

Mobile Alerting: Border Control Function Event Reporting

(Demo App on Google Play®)



GPS

Text Message Originates Here

Text Device

Cell / SMS

4G/IMS

Internet

BCF

ESInet

NG911 FE's

NG911 Call Taker Position

ASSURE911

Event Reported to System Mgr

Assure911®

Mobile Device

8:51 AM

Demo Time Remaining 29:48

Tornado Reported

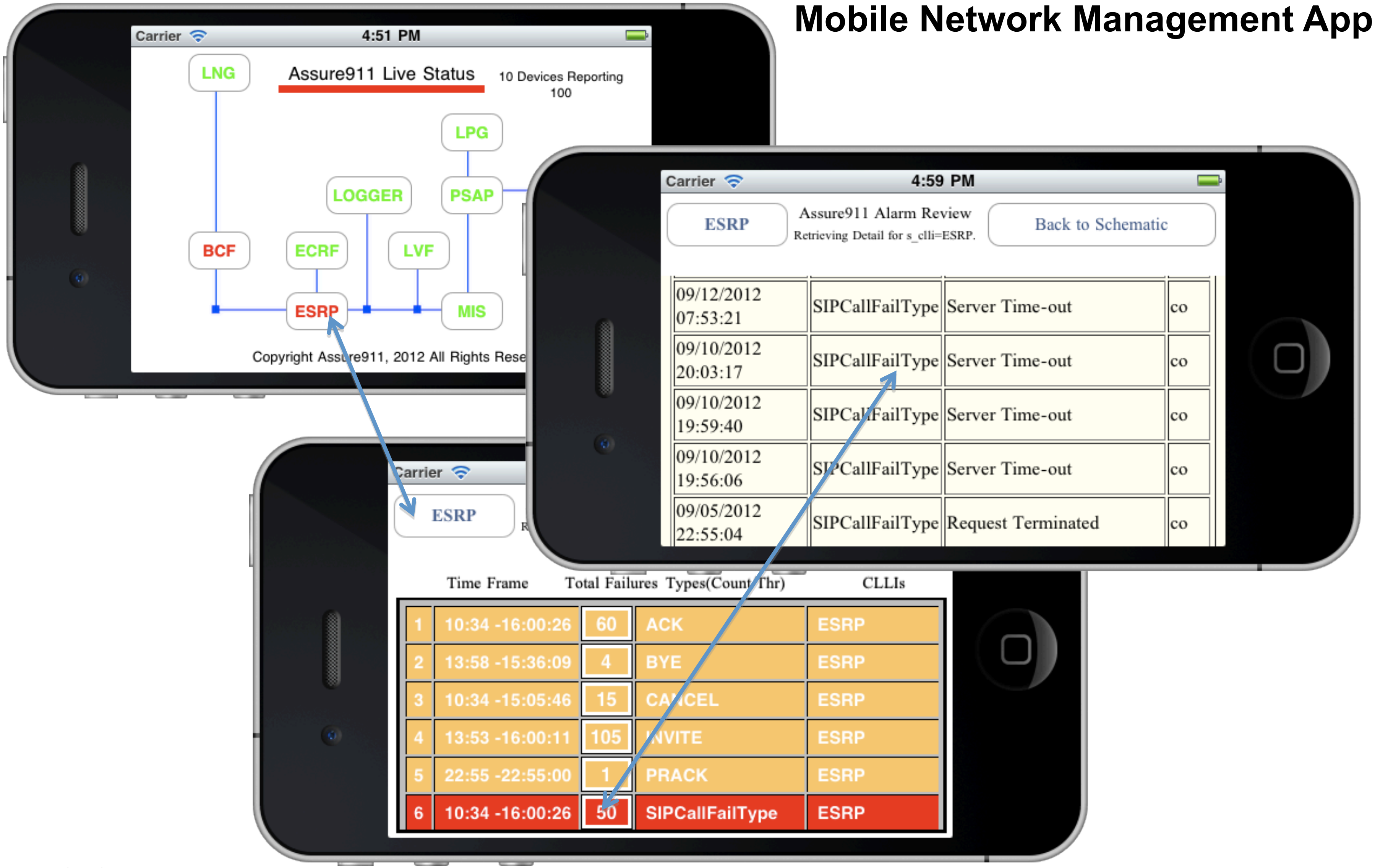
At 04/02/2012 21:19:47
1943 Briarcliffe Blvd Wheaton, IL 60189

Dismiss Detail

Info Reset Current Previous Exit

Text Session with 9-1-1 Call Taker

Mobile Network Management App



Carrier 4:51 PM

Assure911 Live Status

10 Devices Reporting
100

Copyright Assure911, 2012 All Rights Rese

Carrier 4:59 PM

Assure911 Alarm Review
Retrieving Detail for s_clli=ESRP.

09/12/2012 07:53:21	SIPCallFailType	Server Time-out	co
09/10/2012 20:03:17	SIPCallFailType	Server Time-out	co
09/10/2012 19:59:40	SIPCallFailType	Server Time-out	co
09/10/2012 19:56:06	SIPCallFailType	Server Time-out	co
09/05/2012 22:55:04	SIPCallFailType	Request Terminated	co

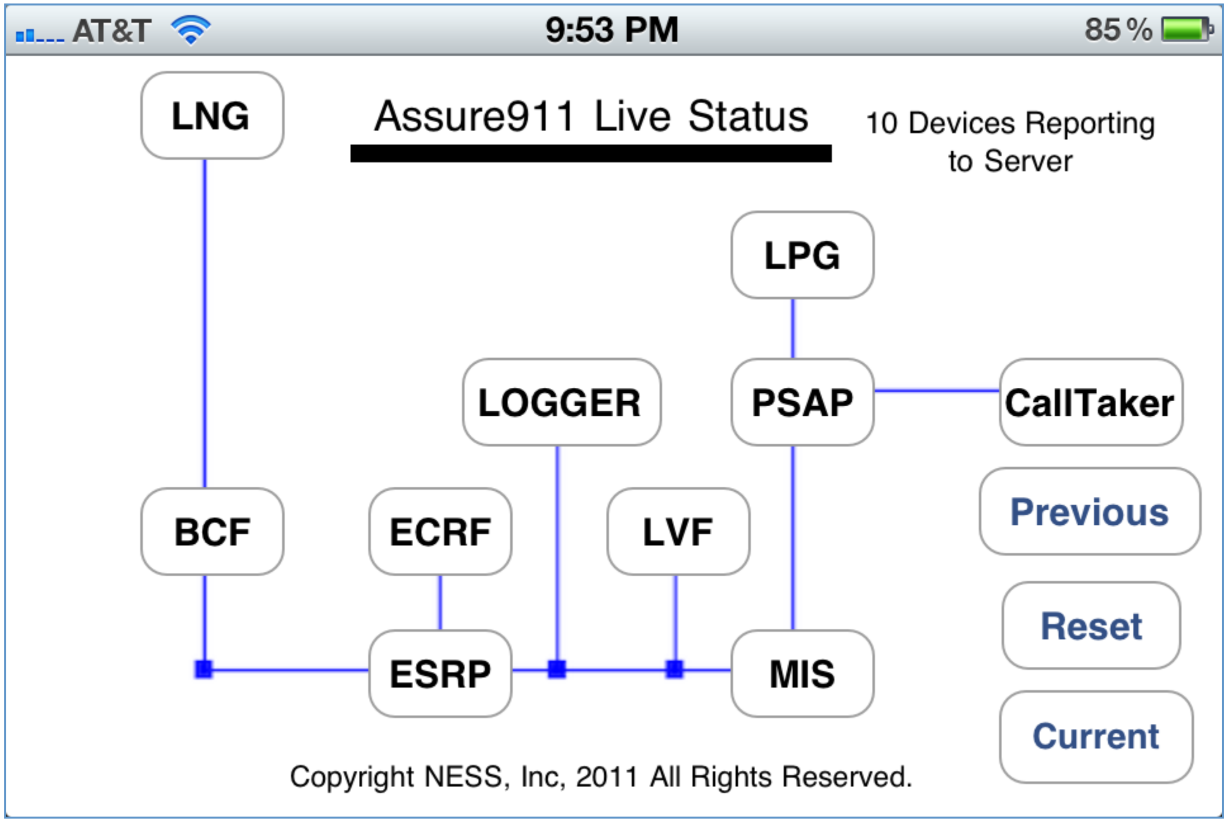
Carrier

	Time Frame	Total Failures	Types(Count Thr)	CLLIs
1	10:34 -16:00:26	60	ACK	ESRP
2	13:58 -15:36:09	4	BYE	ESRP
3	10:34 -15:05:46	15	CANCEL	ESRP
4	13:53 -16:00:11	105	INVITE	ESRP
5	22:55 -22:55:00	1	PRACK	ESRP
6	10:34 -16:00:26	50	SIPCallFailType	ESRP

In 9-1-1 Network Assurance …

… when you marry the network-wide view …

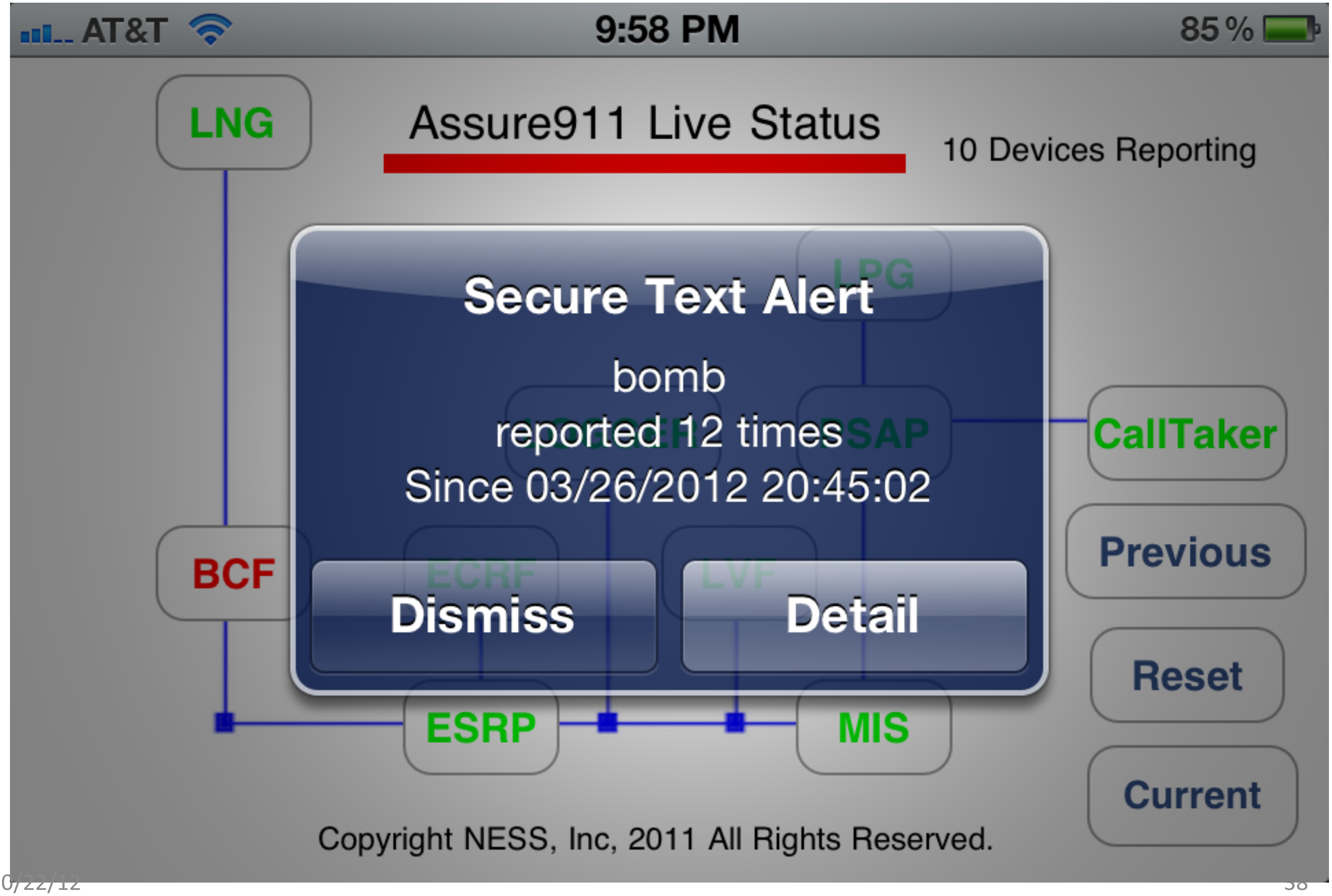
… with the ability of the BCF to monitor the content stream …



Assure911 Live Status

10 Devices Reporting to Server

Copyright NESS, Inc, 2011 All Rights Reserved.

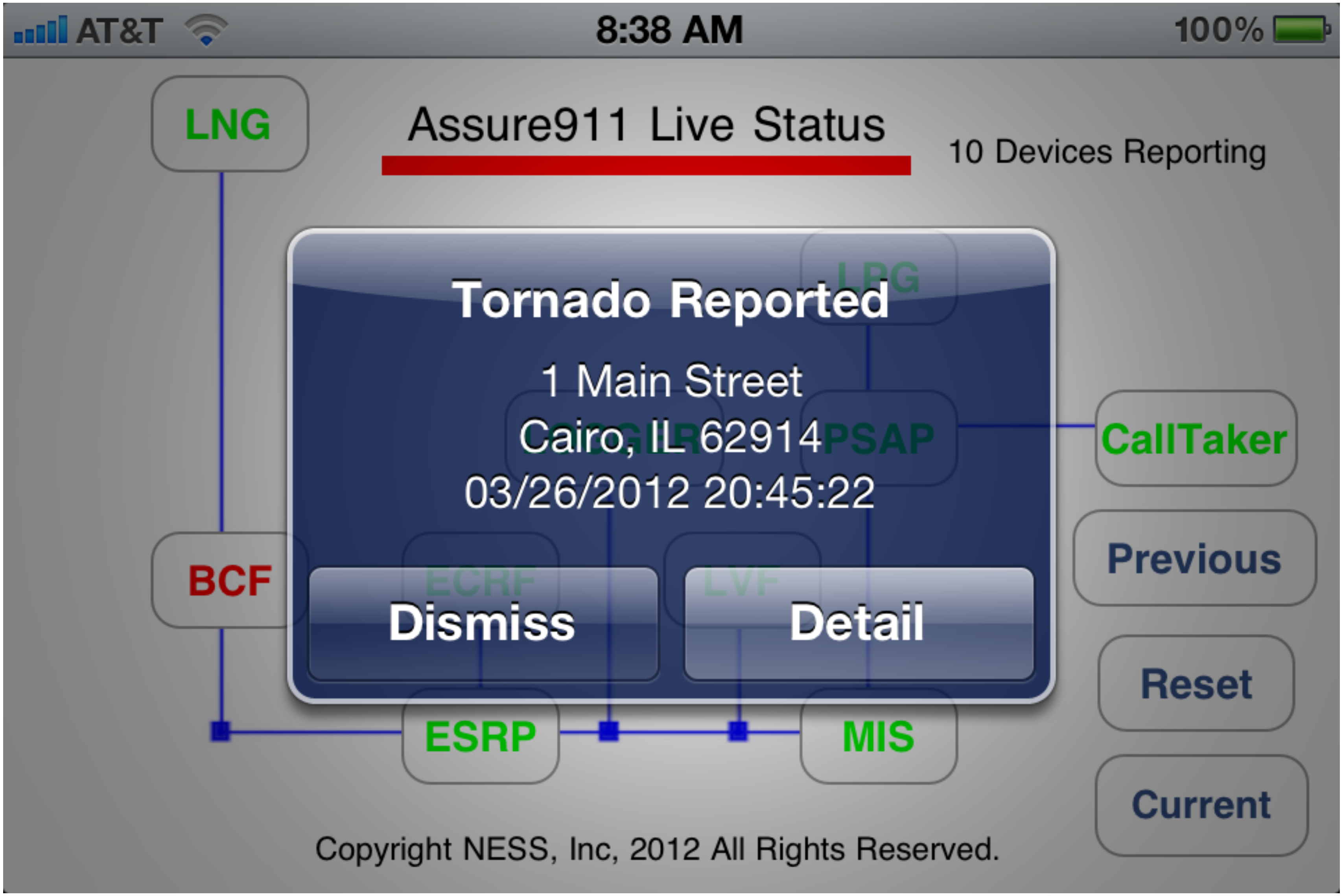


Assure911 Live Status

10 Devices Reporting

Secure Text Alert

bomb
reported 12 times
Since 03/26/2012 20:45:02



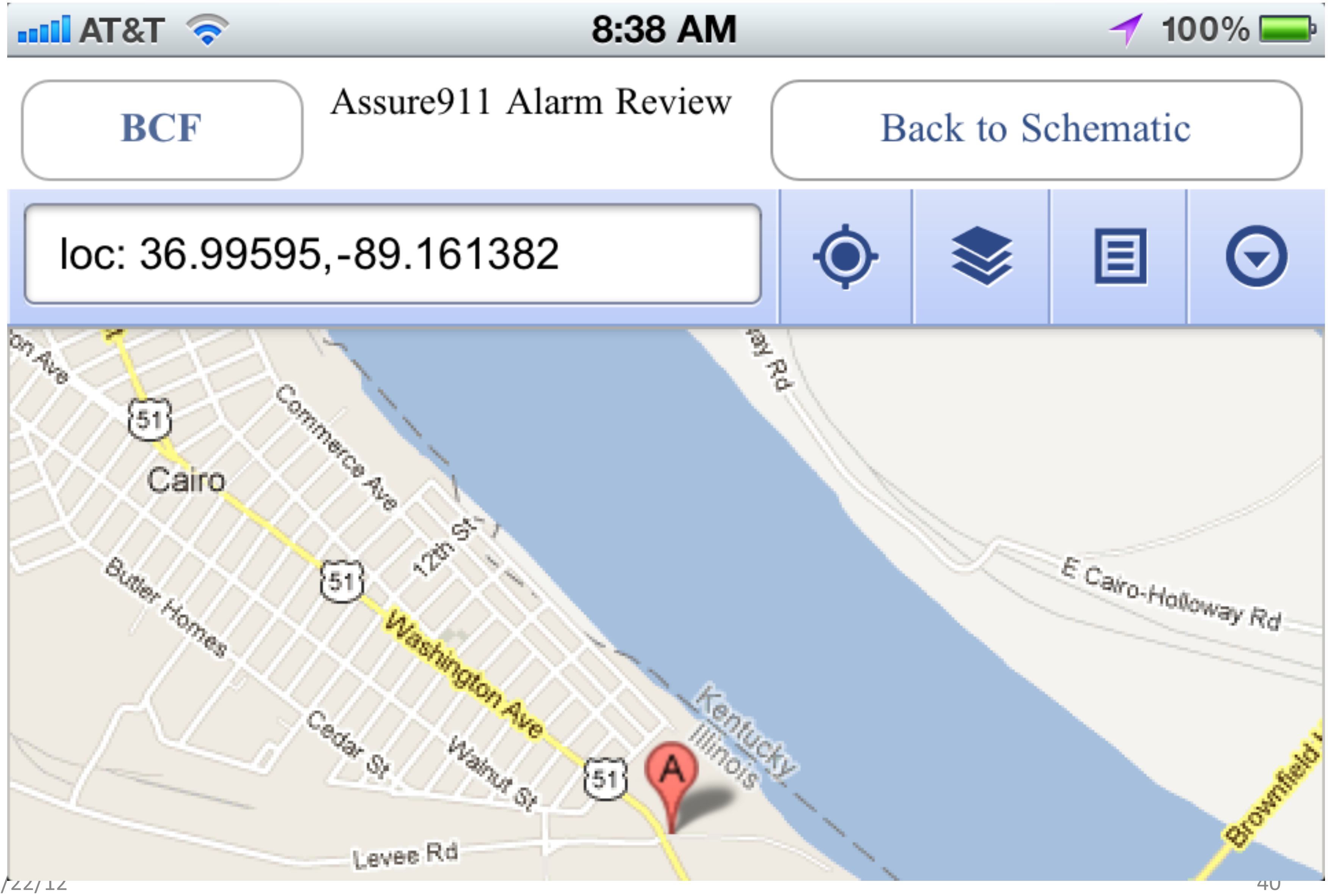
Assure911 Live Status

10 Devices Reporting

Tornado Reported

1 Main Street
Cairo, IL 62914
03/26/2012 20:45:22

Copyright NESS, Inc, 2012 All Rights Reserved.



loc: 36.99595,-89.161382

Thank You!

Assure911^{TM}

Patented, End-to-End NG 9-1-1 Status System

Assure911 is a registered trademark of Network Expert Software Systems, Inc. Used with permission.