# CALEA Update

Paul Schopis
December 13, 2006

# Disclaimer

- The opinions expressed are my own
- I am not a lawyer

# CALEA Enquiring Minds Want to know

- What is?
- Does it affect me?
- What do I have to do?
- How much will it cost?

# Prime Directive

1. At the end of the day, you are responsible
2. We strongly suggest you engage your institution's legal counsel to find out what your obligations are
3. If the FBI etc decide you need to be compliant your legal counsel will need to be able to defend you

# In a Nutshell

In October 1994, Congress took action to protect public safety and ensure national security by enacting the Communications Assistance for Law Enforcement Act of 1994 (**CALEA**), Pub. L. No. 103-414, 108 Stat. 4279. The law further defines the existing statutory obligation of telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization. The objective of CALEA implementation is to preserve law enforcement's ability to conduct lawfully-authorized electronic surveillance while preserving public safety, the public's right to privacy, and the telecommunications industry's competitiveness.

# In a Nutshell

**May 3, 2006** Second Report, Memorandum Opinion, and Order -- The primary goal of the Order is to ensure that Law Enforcement Agencies have all of the resources that CALEA authorizes with regard to facilities-based broadband Internet access providers (ISP) and interconnected voice over Internet protocol (VOIP) providers.

# There are basically two parts

1. First, one must have an operational plan i.e. who does what etc
2. Secondly, one must have a technical compliance plan

# There are basically two parts

1. The operational plan must filed with the FCC sometime in February 2007. Exact date has not yet been specified
2. The technical compliance must be doable by May 14, 2007. This date has never moved and is not expected to.

# Who is affected?

- There are several sources of confusion
- Footnote 74 - First Report and Order FCC
- Footnote 100 - First Report and Order FCC

# Footnote 74

74 As we tentatively concluded in the *Notice*, we define "broadband" as those services having the capability to support upstream or downstream speeds in excess of 200 kilobits per second (kbps) in the last mile, *Notice*, 19 FCC Rcd at 15693, para. 36 n.77, but we also include as "broadband" – for purposes of CALEA only – those services such as satellite-based Internet access services that provide similar functionalities but at speeds less than 200 kbps. We explained in the *Notice* that "facilities-based" meant entities that "provide transmission or switching over their own facilities between the end user and the Internet Service Provider (ISP)." *Id*. at 15693, para. 37, n.79.

# Footnote 100

100 *See* 47 U.S.C. § 1002(b)(2)(B); *see also House Report*, 1994 U.S.C.C.A.N. at 3498; *Second Report and Order*, 15 FCC Rcd at 7112, para. 12; Notice, 19 FCC Rcd at 15679, para. 8. **Relatedly, some commenters describe their provision of broadband Internet access to specific members or constituents of their respective organizations to provide access to private education, library and research networks, such as Internet2's Abilene Network, NyserNet,and the Pacific Northwest gigaPoP. See, e.g., EDUCAUSE Comments at 22-25. To the extent that EDUCAUSE**
members (or similar organizations) are engaged in the provision of facilities-based private broadband networks or intranets that enable members to communicate with one another and/or retrieve information from shared data libraries not available to the general public, these networks appear to be private networks for purposes of CALEA. Indeed, DOJ states that the three networks specifically discussed by EDUCAUSE qualify as private networks under CALEA's section 103(b)(2)(B). DOJ Reply at 19. We therefore make clear that providers of these networks are not included as "telecommunications carriers" under the SRP with respect to these networks. **To the extent, however, that these private networks are interconnected with a public network, either the PSTN or the Internet, providers of the facilities that support the connection of the private network to a public network are subject to CALEA under the SRP.**

# If you are required to comply

- Upon receipt of warrant or court order, engage legal counsel to determine validity and extent of warrant's requirements
- Engage POC and only staff required to meet warrant's requirements
- Remember; you are required to protect others privacy

# Section 103 (4)(A)&(B)

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects--

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and
(B) information regarding the government's interception of communications and access to call-identifying information

# More Confusion

- Many believe that we are required to provide captured packets i.e. for example a TCPdump or ethereal to a disk.
- But.....

# What do they want?

CALEA Pub. L. No. 103-414, 108 Stat. 4279
Section 103 (3)
(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier;

Section VI. Appendix A: Final Rules § 22.1102, §§ 22.902, and 64.2202.
"Capability that permits an LEA to associate call-identifying information with the content of a call. A call-identifying message must be sent from the carrier's IAP to the LEA's Collection Function within eight seconds of receipt of that message by the IAP at least 95% of the time, and with the call event timestamped to an accuracy of at least 200 milliseconds."

# What do they want?

- Previous slide is ugliest scenario
- They can just ask for “dialing or signaling information” if that is the case netflow may potentially be enough*

# What do they want?

## From Title 18 United States Code

Pen Register
“a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.....

# What do they want?

## From Title 18 United States Code

Trap and Trace
"a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication".

# What do they want?

- The widely held belief that campuses are immune is predicated on the assumption that the campuses meet the requirements of a private network
- However two scenarios can trump this

1. Public access to facilities
2. The upstream cannot meet the request for valid technical reasons

# What do they want?

- In the first case, if a campus has a library that allows public access to terminals that can get internet access then the campus may fail the private network test

# What to they want?

- In the second case, if an LEA comes to OARnet with a user id, name, jack plate id, or mac address OARnet does not have access to that information
- Reasonably speaking, we may need to engage the campus
- Additionally, CALEA specifically empowers an LEA to serve a warrant to a down stream

# What do they want?

**SEC. 108. ENFORCEMENT ORDERS.**

**(a) GROUNDS FOR ISSUANCE- A court shall issue an order enforcing this title under section 2522 of title 18, United States Code, only if the court finds that--**

**(1) alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement for implementing the interception of communications or access to call-identifying information; and**

**(2) compliance with the requirements of this title is reasonably achievable through the application of available technology to the equipment, facility, or service at issue or would have been reasonably achievable if timely action had been taken.**

# What do they want?

- An other issue is the precedence of local loop
- In conversations with FBI engineers, the FBI took the position that local loop traditionally (Telecom) is the line connecting the end point (Handset) to the network*
- Translated, they "get" that the best place to capture a call is closest to the end point

*Source: Steve Wallace @ I2MM 12/05/06 CALEA Quilt Session

# What they cannot do

## Cannot mandate a particular solution as long as it meets the articulated requirement

CALEA Section 103 (b)
(1) DESIGN OF FEATURES AND SYSTEMS CONFIGURATIONS- This title does not authorize any law enforcement agency or officer--
(A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or
(B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

# What they cannot do

## Cannot require you to decrypt messages you did not encrypt

CALEA Section 103 (b)(3)
(3) ENCRYPTION- A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.

# Covering Your Assets

## Safe Harbor provision

FCC 98-223, cc Docket No 97-213 Memorandum
Opinion and Order, released 9/11/98.

“Although CALEA does not specify technologies or standards that carriers must use to meet the assistance capability requirements, it does contain a ‘safe harbor’ provision.

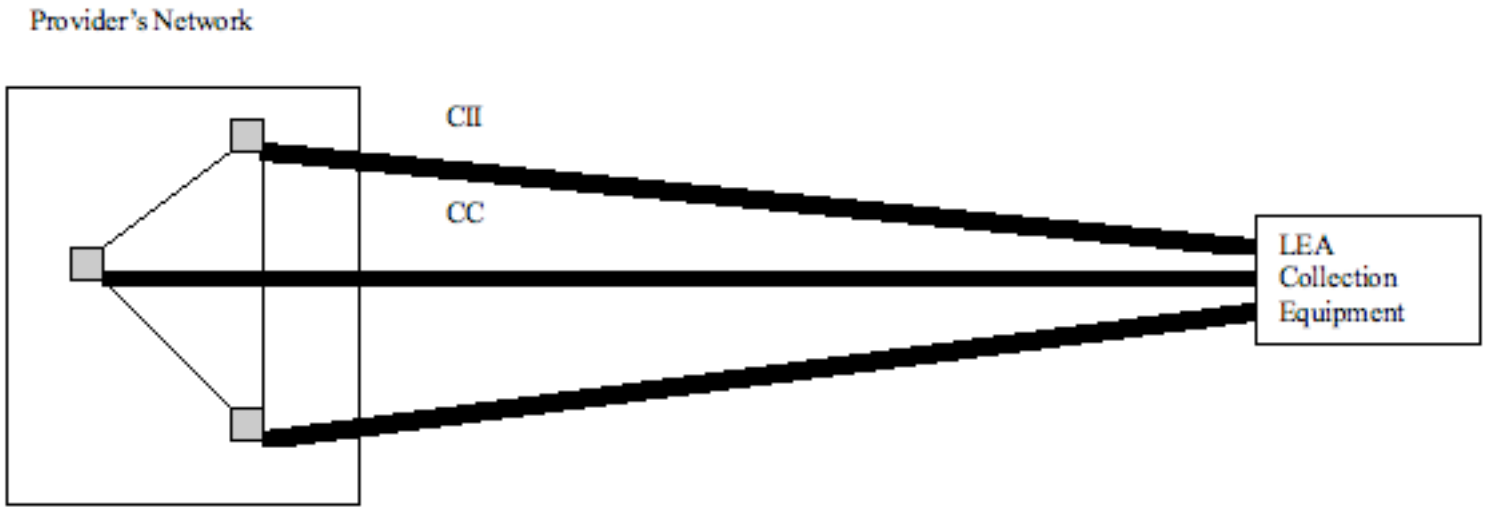
CALEA Section 107 (A) (2)

(2) COMPLIANCE UNDER ACCEPTED STANDARDS- A telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103.

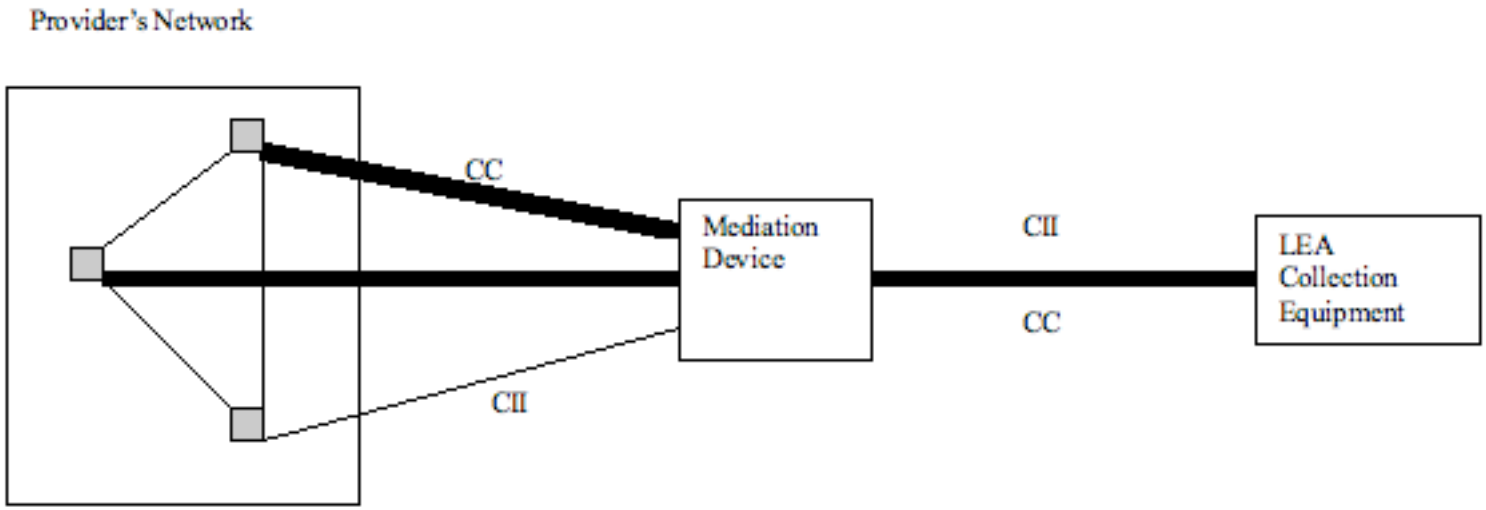
# Technology

- OK enough legalese what to we need to do technically
- The next couple of slides come from the FCC 04-187 Docket 04-295 RM-10865

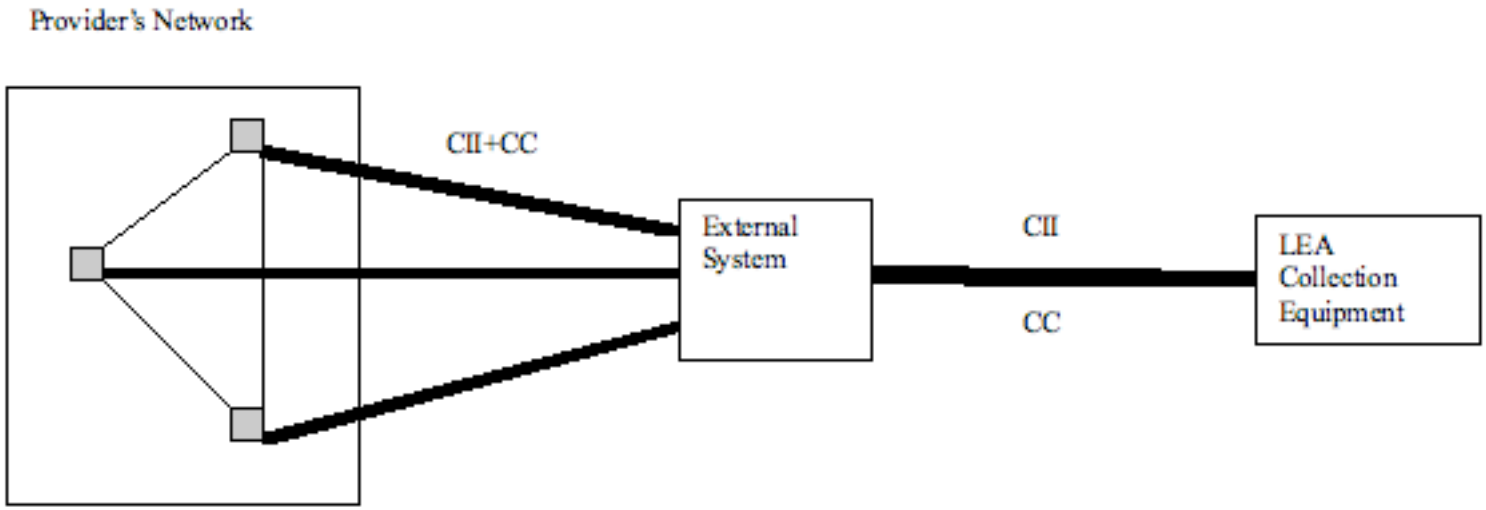
# Direct Model



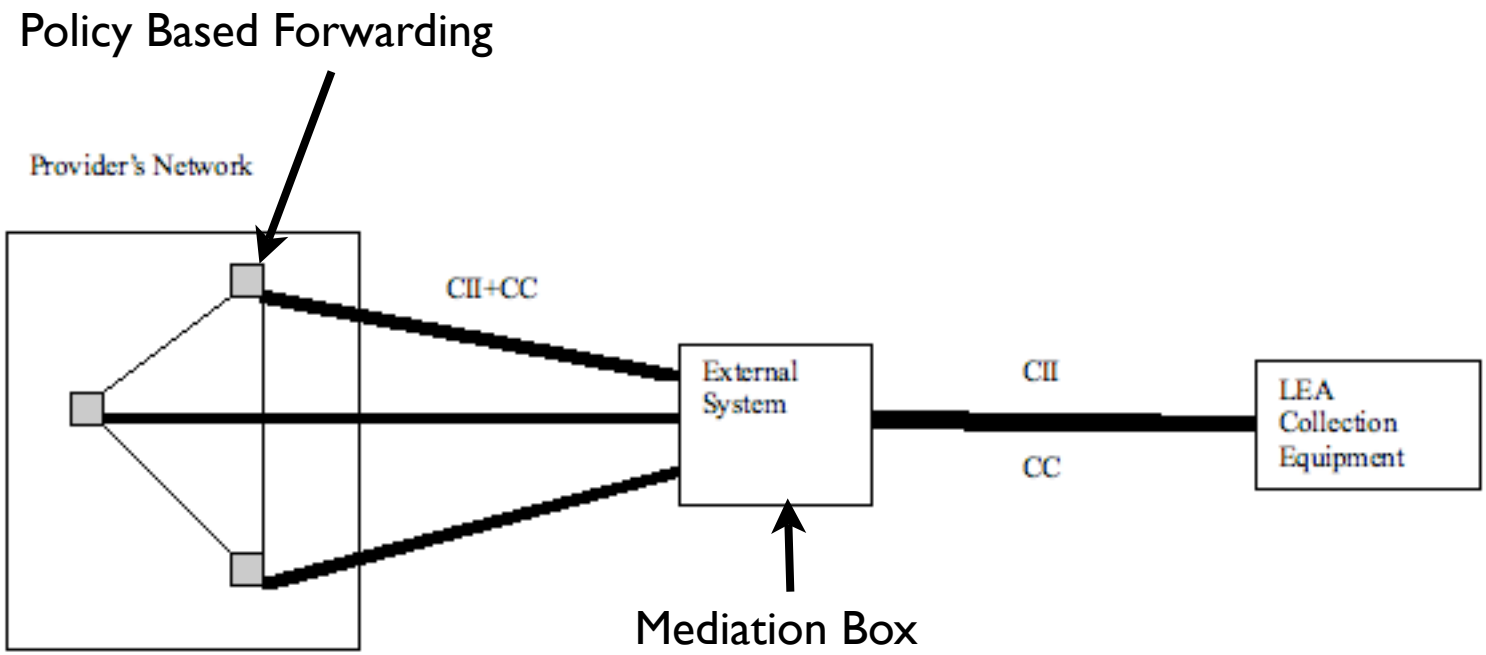
# Trusted Third Party CII & CC on Different Channels



# Trusted Third Party CII&CC on same channel (IP?)



# Paul's hack


Policy Based Forwarding
Provider's Network
CII+CC
External System
CII
CC
LEA Collection Equipment
Mediation Box

# Router Function

- Does forwarding based on source IP for outgoing packets and destination for inbound packets
- Sends to Mediation Box
- If campus switch could do forwarding based on source MAC or could tag for router to process when it hits the core
- Could forward with IP or send to MPLS tunnel to get Label

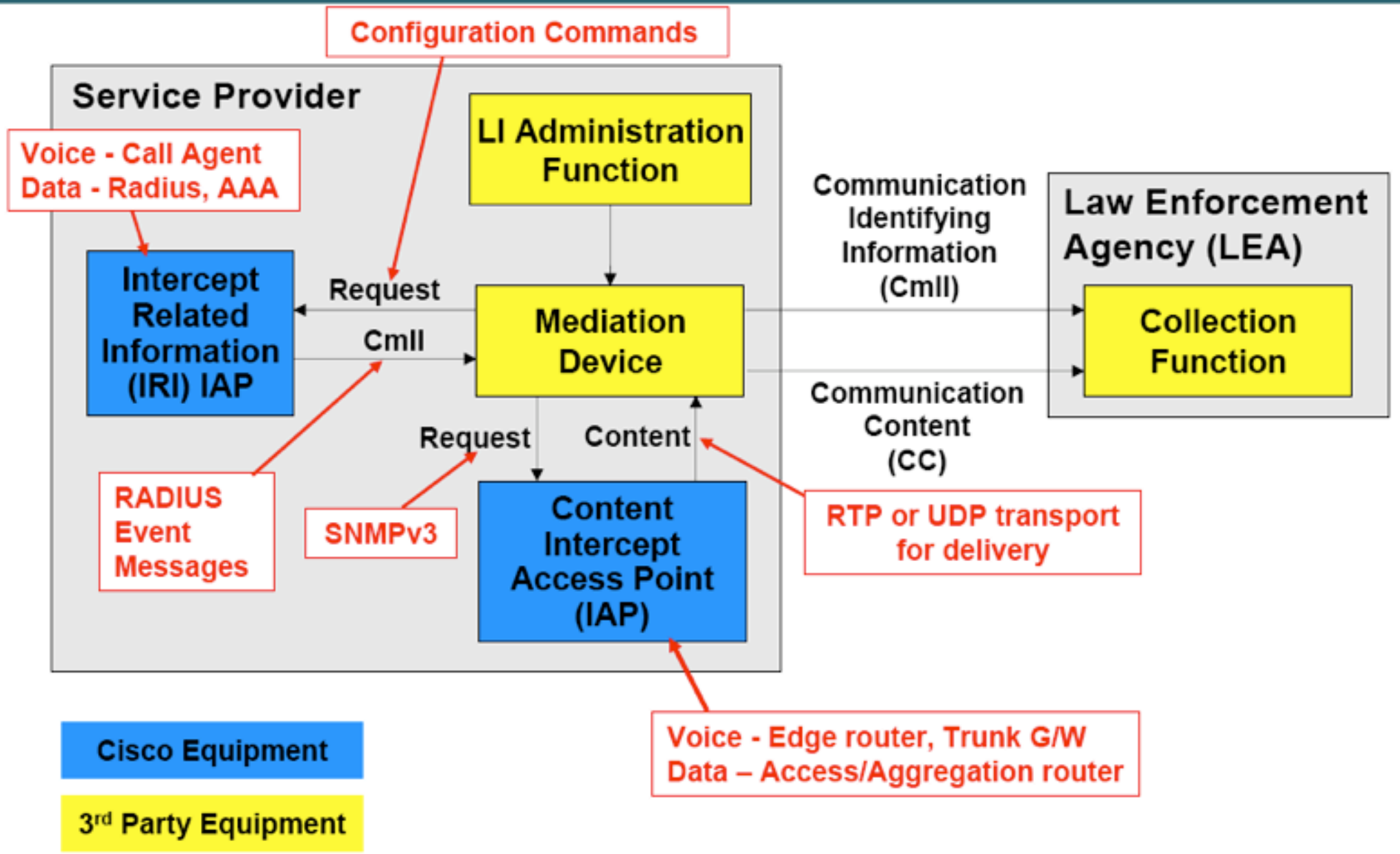
# Mediation Box Function

- Receive packet and duplicate
- Wrap original in new packet to forward to LEA
- Send copy to GW router
- For reverse path need to return to edge router in vlan, MPLS or some other tagging mechanism to prevent routing loop i.e. lets edge router "know" it has been read by mediation device

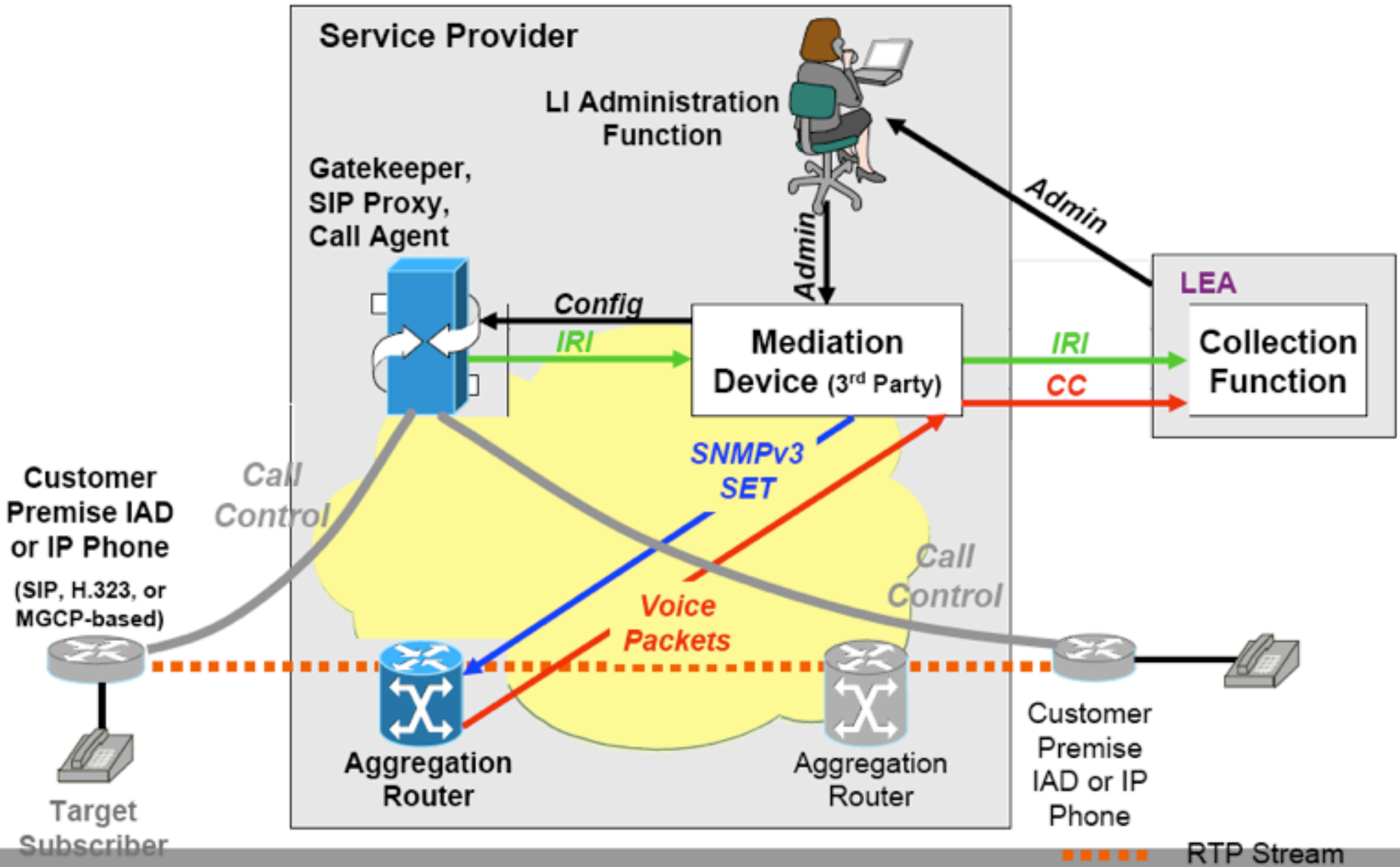
# So what are the vendors plans?

- Trusted third party service
- Can handle technical as well as legal

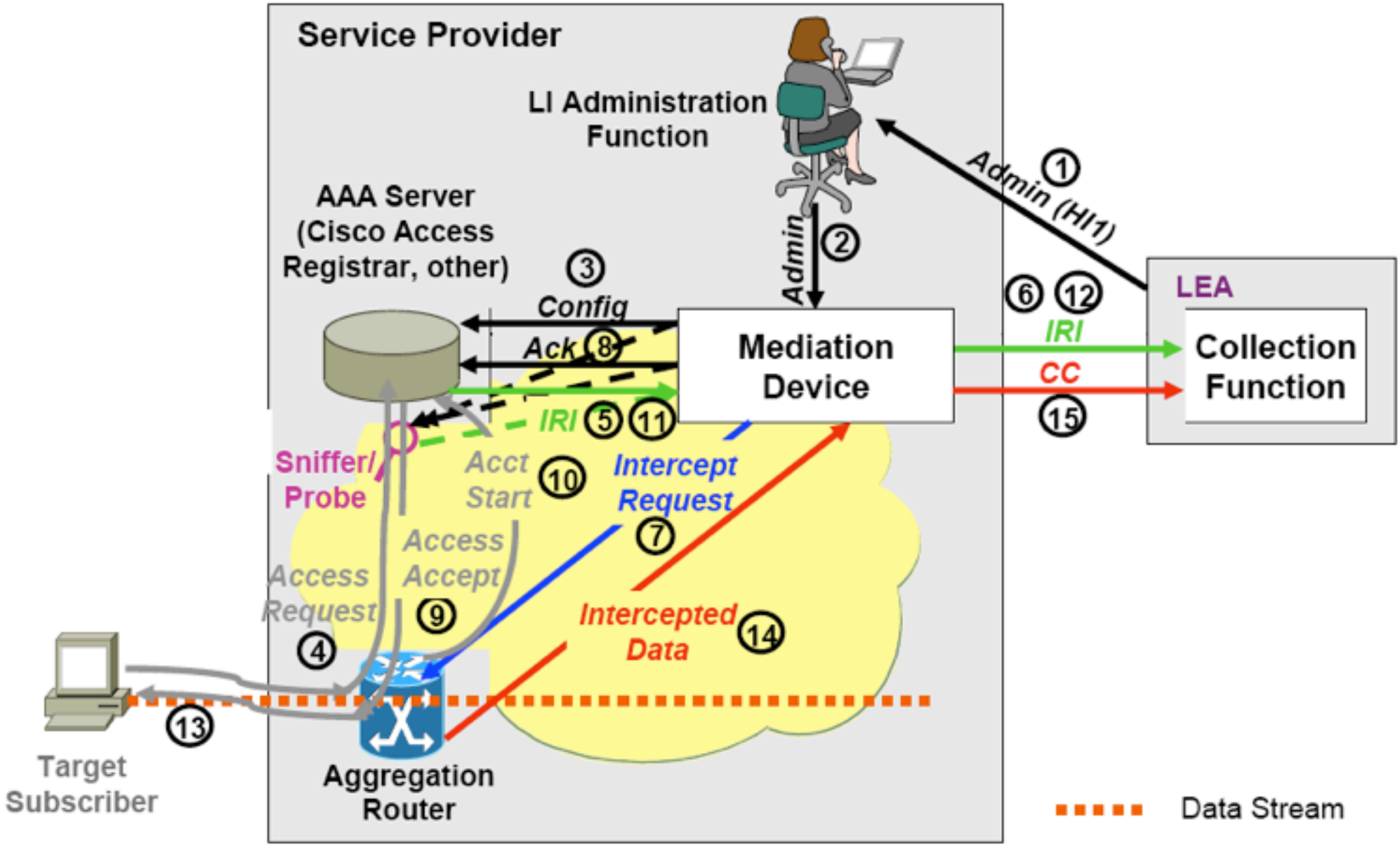
# Cisco Service Independent Intercept (SII)

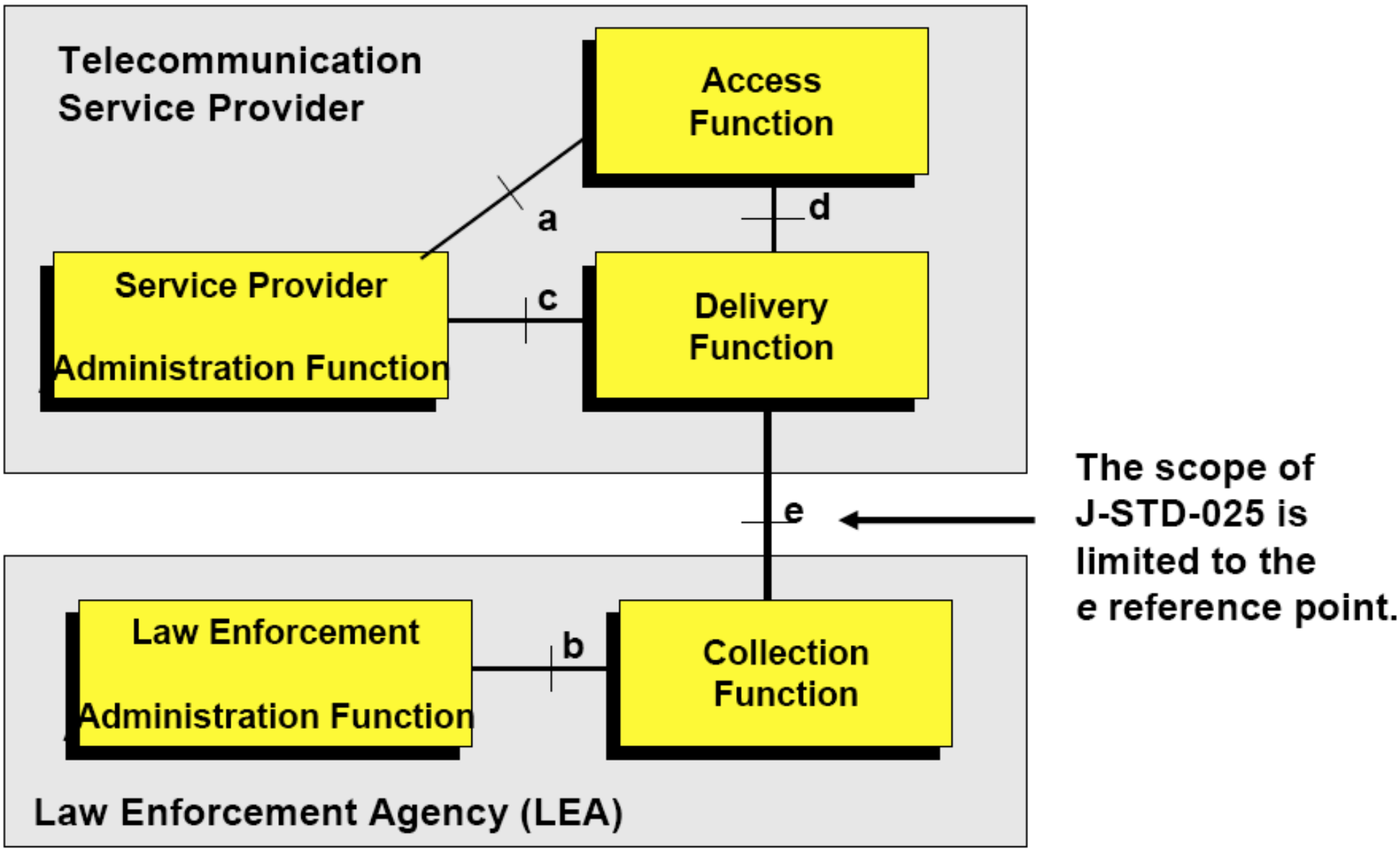


# LI Architecture – Voice Intercept

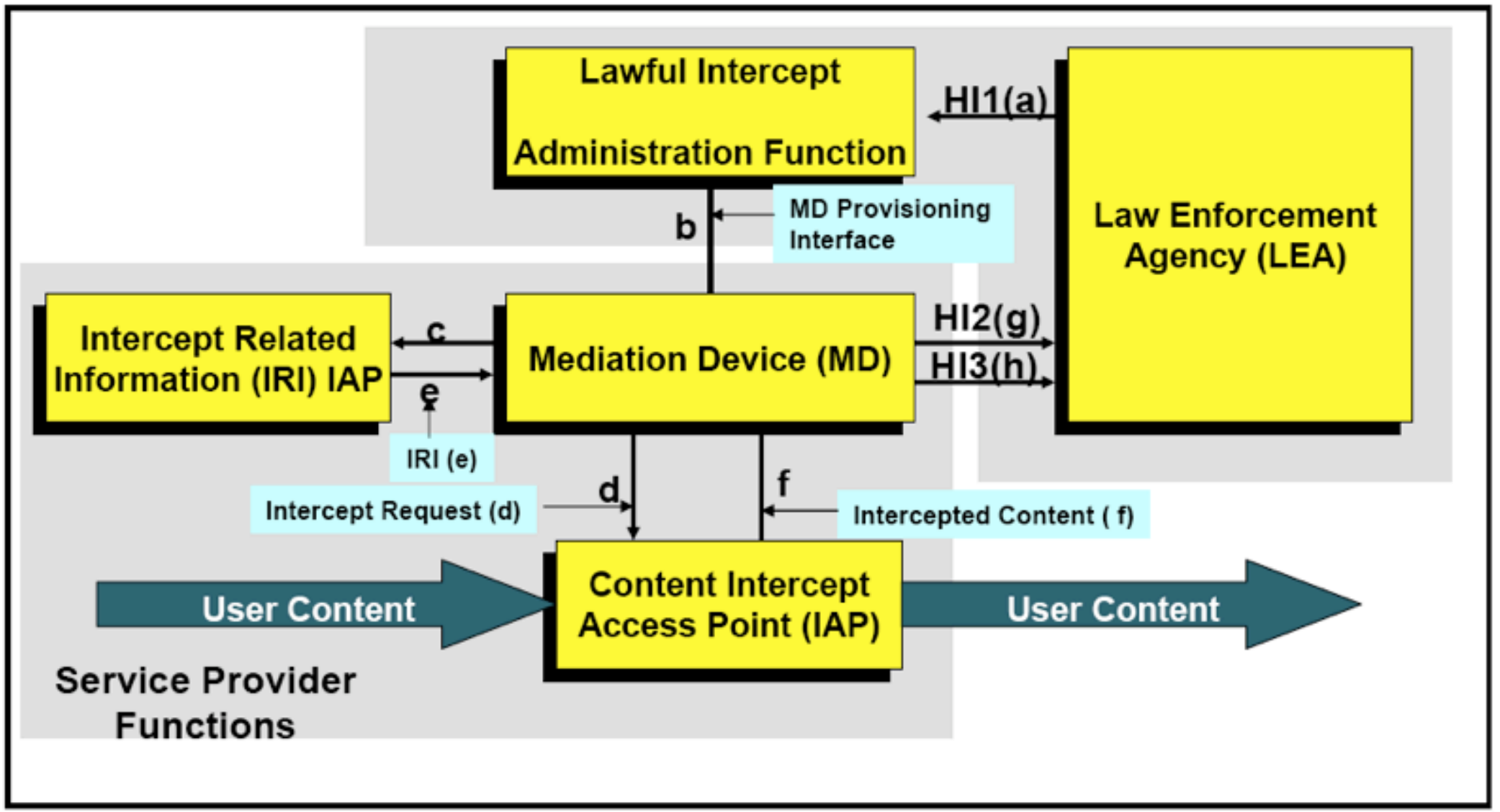


# LI Architecture – Data Intercept




Telecommunication
Service Provider
Access
Function
a
d
Service Provider
Administration Function
c
Delivery
Function
e
The scope of
J-STD-025 is
limited to the
e reference point.
Law Enforcement
Administration Function
b
Collection
Function
Law Enforcement Agency (LEA)

# IETF – RFC 3924




Lawful Intercept Architecture Reference Model

# Important Documents

- CALEA -. Pub L. No. 103-414, 108 Stat. 4279
- First Report and Order - FCC-05-153 Docket 04-295
- Rule Making and Declaritory Rule making FCC--4-187A1 Docket 04-295

# Important Websites

- www.askcalea.net
- www.fcc.gov
- www.atis.org
- www.educause.edu

# Questions?