Simple Law Enforcement Monitoring

Fred Baker

draft-baker-slem-architecture-01.txt

ftp://ftpeng.cisco.com/fred/ietf/slem.ppt

ftp://ftpeng.cisco.com/fred/ietf/slem.pdf

The message I wish had been found in many Raven messages

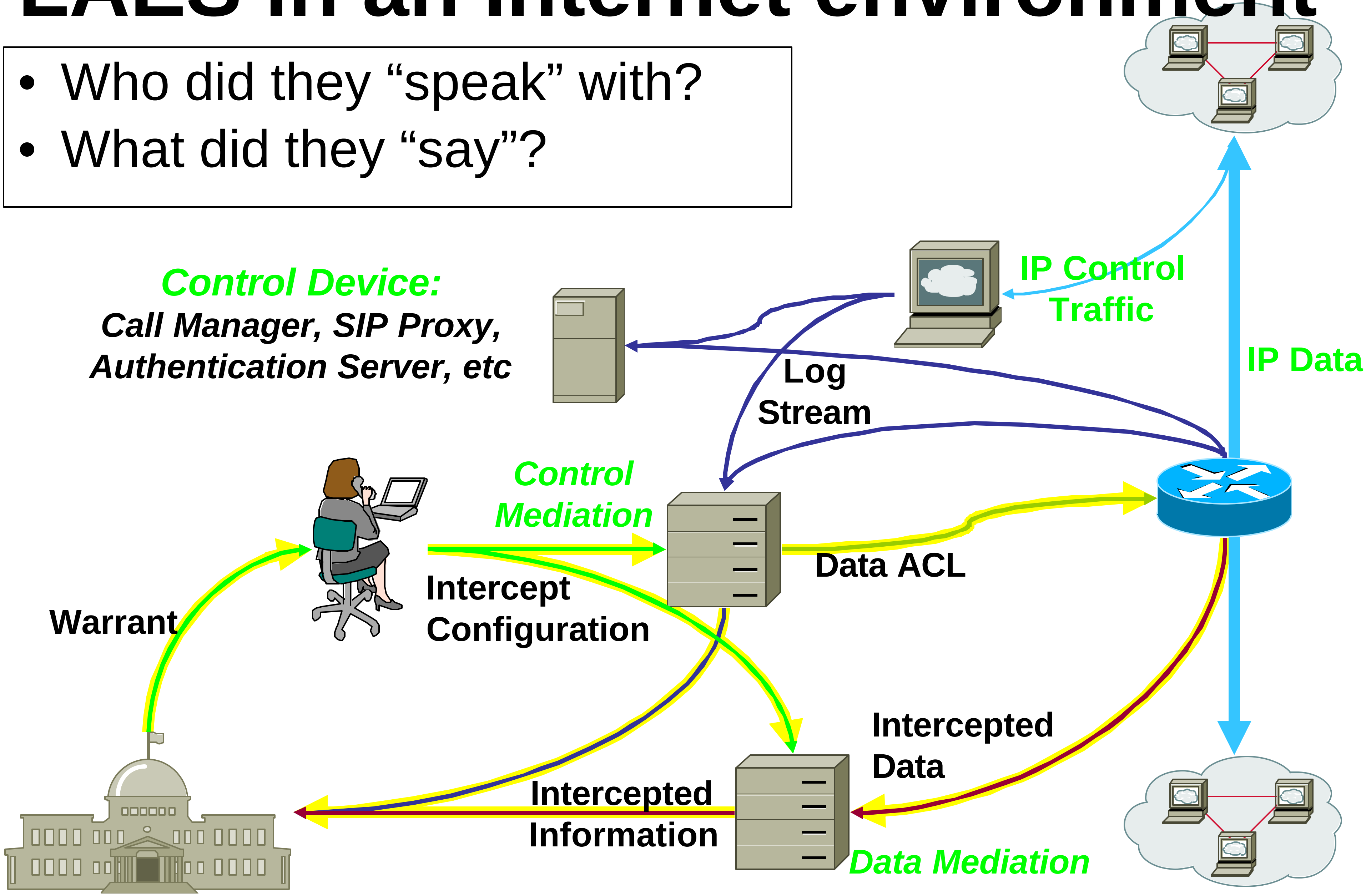
- I am not a lawyer
- I do not play one on TV

Lawfully Authorized Electronic Interception (LAES)

- Forensic investigation of specific persons or organizations
  - –Focuses on the crime/criminal being investigated
- Involves disclosure of a person's communications
  - –In most countries, the difference between voice and data communication is irrelevant

LAES in an Internet environment

- Who did they “speak” with?
- What did they “say”?



The legal mandate for Lawfully Authorized Electronic Interception

Current state of law

- **Laws being worked on in “western” countries**
  - –US CALEA and related laws
  - –European legislation resulting from legal normalization process
  - –Japan, Australia, and others
- **11 September attack used to push US legislation**
  - –Cryptography limitations and export controls discussed during debate

EU Efforts

- **Council of Europe-Convention on Cyber-crime**
  - **Left to each country to implement requirements.**
  - **Provides for mutual assistance among signing states**
  - **Applies to public and private ISPs**
  - **Requires ISPs to preserve communications data (e.g., origin, route, type of service) for up to 90 days and provide it to LEA.**
  - **ISP must also provide for real-time collection or recording of traffic data and content for LEA.**
  - **Open to EU members and drafters, including Canada and Japan**

Overview of Electronic Surveillance

- **Four fundamental types of requests:**
  - – **Past billing/statistical records of communications**
    - **In telephone system, billing records**
  - – **Contents of computer long term storage**
    - **Eg, search and seizure of computers and disk drives**
  - – **Current billing/statistical records of communications, desirable in real time**
    - **In telephone system, “pen register” or “trap and trace”**
  - – **Delivery of content**
    - **“Content Intercept”**

Cybercrime Treaty, Article 20
“Real-time collection of traffic data”

> “ **Each Party shall…**
>
> **–… compel a service provider, within its existing technical capability, to:**
>
> **– i. collect or record …**
>
> **–traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.** ”

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Cybercrime treaty, Article 21
“Interception of content data”

“

- **Each Party shall …**
- **a. collect or record …**
- **b. compel a service provider…**
  - **i. collect or record …**
  - **ii. co-operate … in the collection or recording of,**
- **content data, in real-time, of specified communications in its territory transmitted by means of a computer system.**

”

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

CALEA wrinkles

- Communications Assistance for Law Enforcement Act
- Voice intercept mandated
  - –Features installed only for CALEA compliance subject to FBI funding
  - –Lack of capability cause for $10K/day fines
- Data intercept allowed for, especially Title III and FISA
  - –If an ISP has the capability, its use can be subpoenaed
  - –If it does not, an ISP must provide “reasonable assistance” to law enforcement (i.e., do what it can, or provide access to install LEA-owned equipment) to permit LAES

IETF Comments on the thrust of law

IETF Issues in Internet Privacy and Security

- IETF primary concern:
  - –Security of the infrastructure
- Two statements:
  - –RFC 2804 - “IETF Policy on Wiretapping”
  - –RFC 1984 - “IAB and IESG Statement on Cryptographic Technology and the Internet”

RFC 2804 on LAES

“

- Wiretapping ... releases information that the information sender did not expect to be released.
  - –The system is less secure than it could be had this function not been present.
  - –The system is more complex than it could be had this function not been present.
  - –Being more complex, the risk of unintended security flaws in the system is larger.
- Wiretapping, even when it is not being exercised, therefore lowers the security of the system.

”

RFC 2804

RFC 2804 major findings

- Six major considerations:
  - IETF is wrong forum
    - National definitions call for national standards
  - IETF wants to maximize security
  - LAES can already be accomplished
  - Adding LAES to protocols adds complexity that reduces security
  - Encryption is your friend
  - LAES technology should be openly described

RFC 2804 “will not” statements

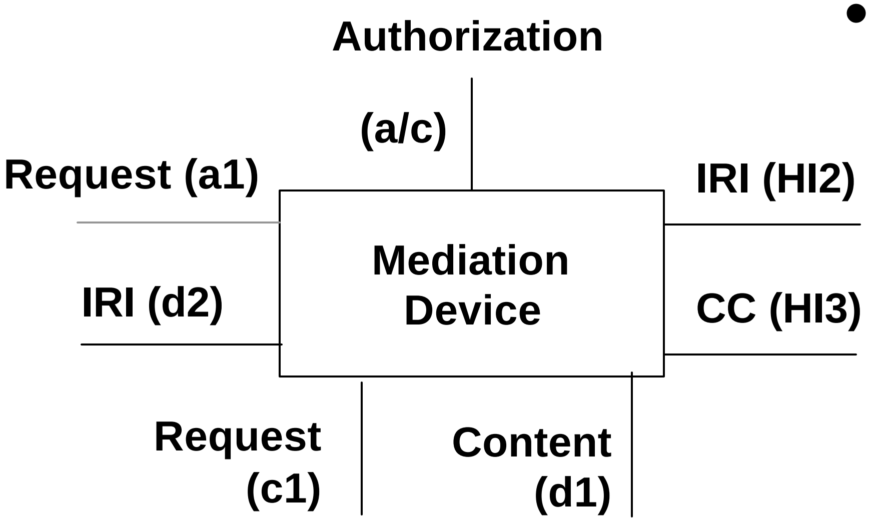
- **IETF will not**
  - **Take a moral position on LAES**
    - **No consensus**
  - **“The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards.”**
  - **Implications**
    - **At minimum, the question that triggered Raven, “IETF will not add LAES capabilities to unrelated protocols”**
      - **Complexity and security issues**
    - **Perhaps, “IETF will not standardize LAES technology”**

Approaches to LAES

Fundamental Requirements

- **Need to identify traffic related to a surveillance subject and (somehow) report it**
- **Need to maintain secrecy of the intercept from subject and uncleared staff**
- **Need to audit the use of intercept technology**

Mediation Device/Delivery Function



- Authorization
- Mediation Device:
  - Formats to country-specific handover interface
  - Delivers to LEA(s)
  - Replicates for multiple taps on same target
  - Filtering of CC and IRI, and
  - may do Request for IRI & CC

Three fundamental approaches

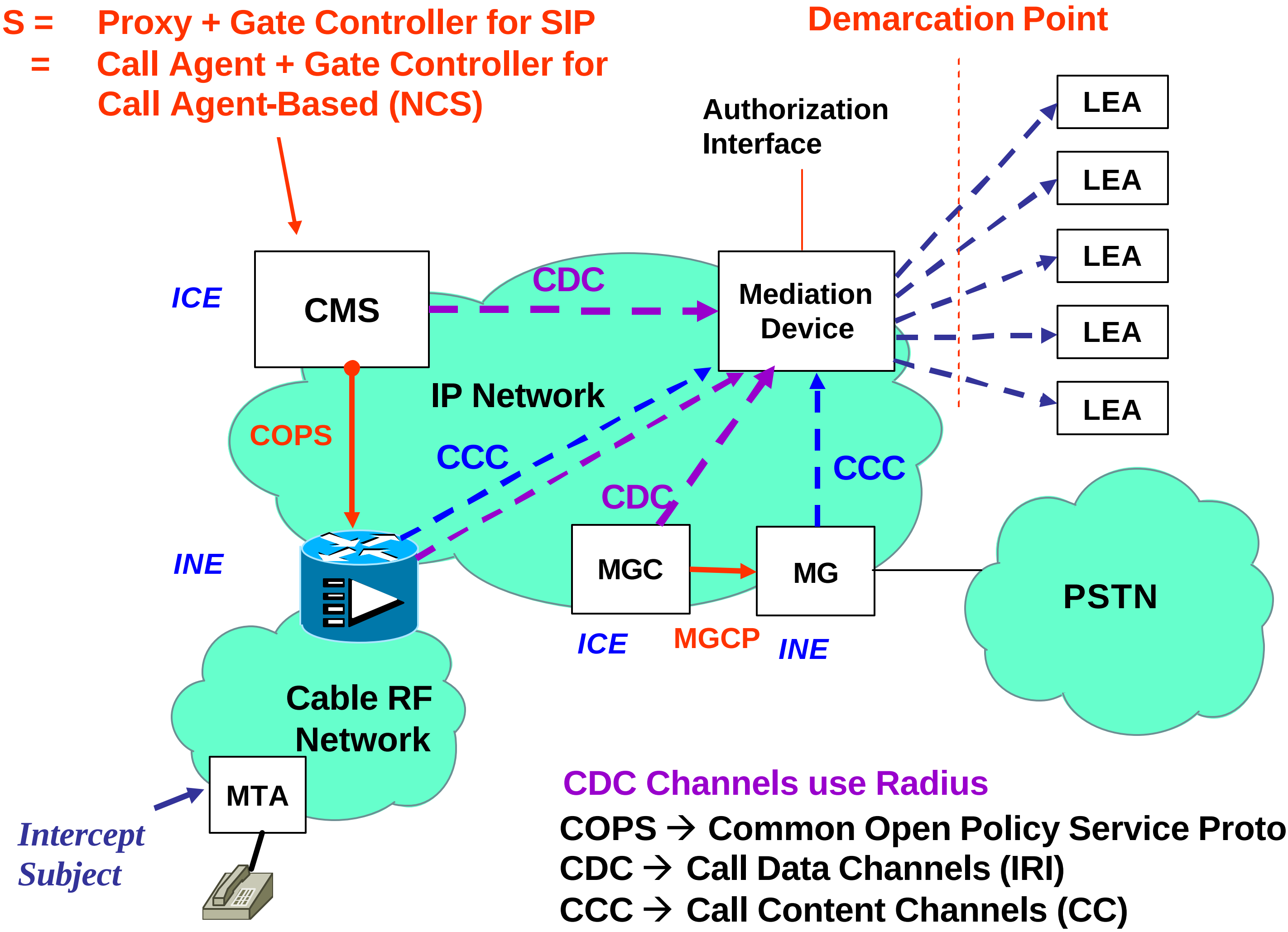
- **Fiber splitting**
  - **All traffic sent to a service center for reporting**
- **Port Mirroring**
  - **All identified traffic sent to a mediation device for reporting without protection**
- **Router/Switch data intercept**
  - **All identified traffic sent to a mediation device for reporting with protection**

Trade-offs in approaches

- Cost/Scalability of solution
- Integrity of data intercepted
- Security perimeter
- Ability to handle special cases
  - Hairpin calls, Dial access, tunnels
- Definition of “Call Identifying Information” (IRI)
  - IPFix records? Every IP header? IP+TCP?

PacketCable™ Architecture

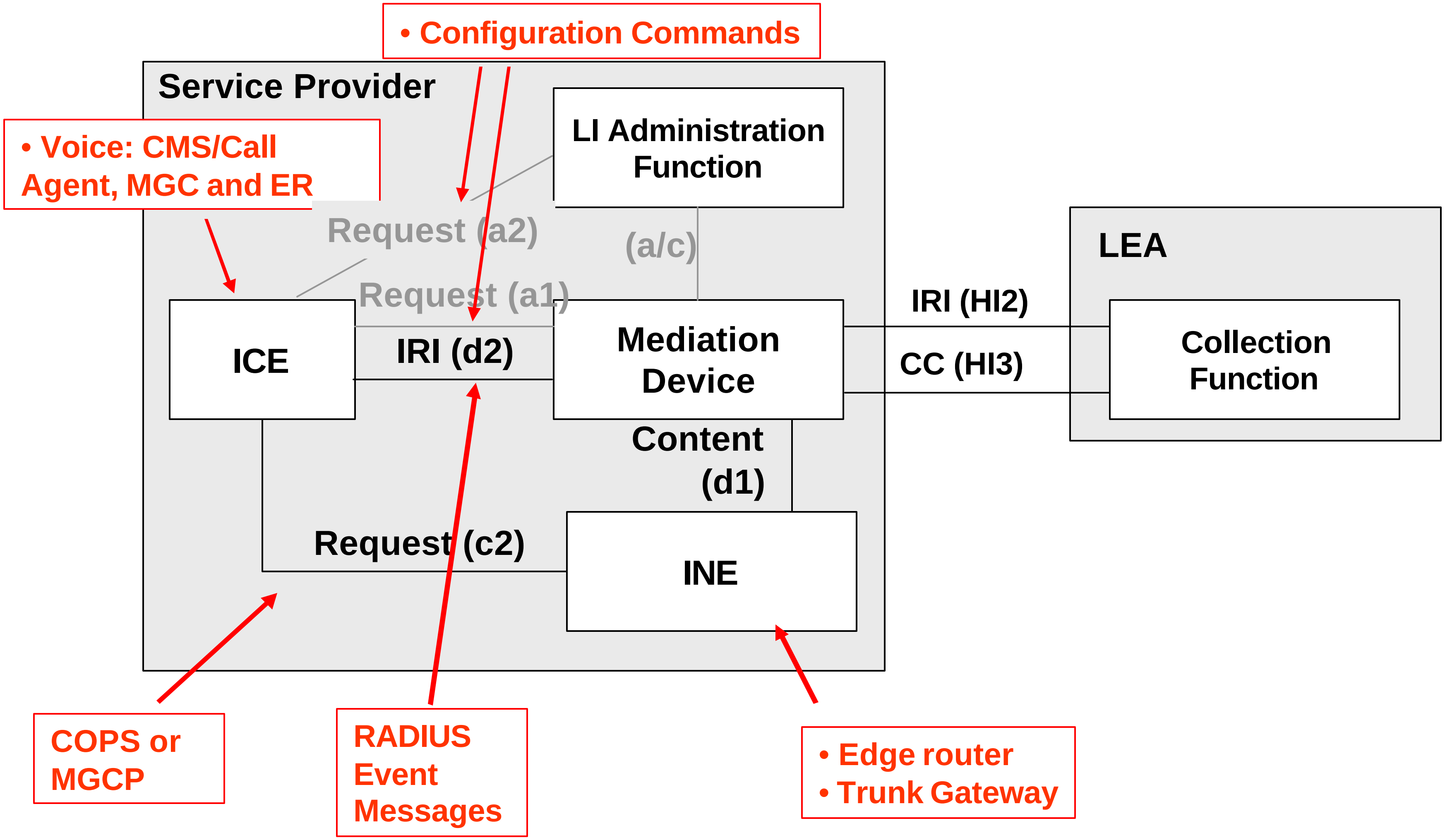
CMS = Proxy + Gate Controller for SIP
= Call Agent + Gate Controller for Call Agent-Based (NCS)



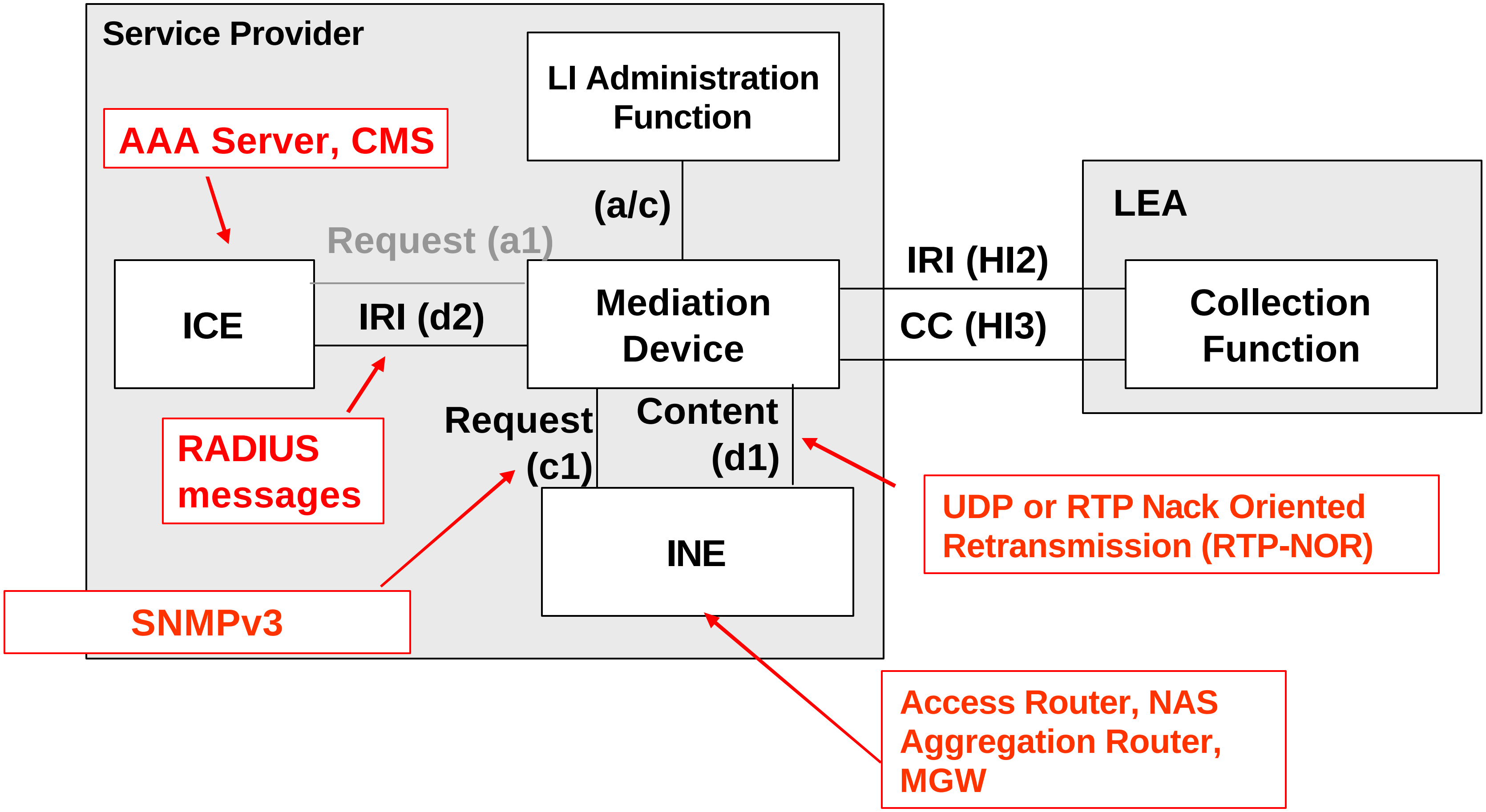
CDC Channels use Radius

COPS → Common Open Policy Service Protocol (RFC 2748)
CDC → Call Data Channels (IRI)
CCC → Call Content Channels (CC)

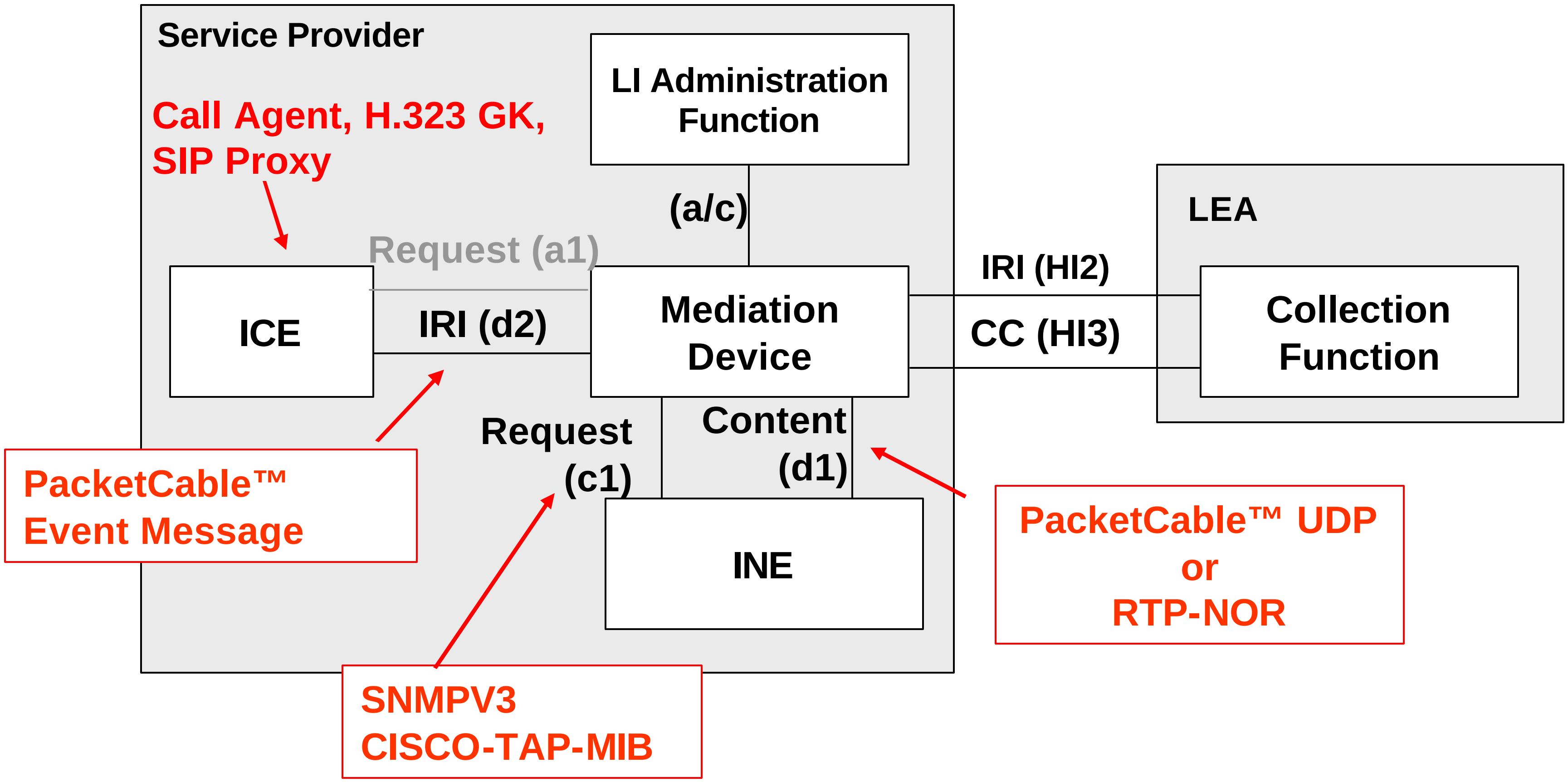
PacketCable™ Architecture



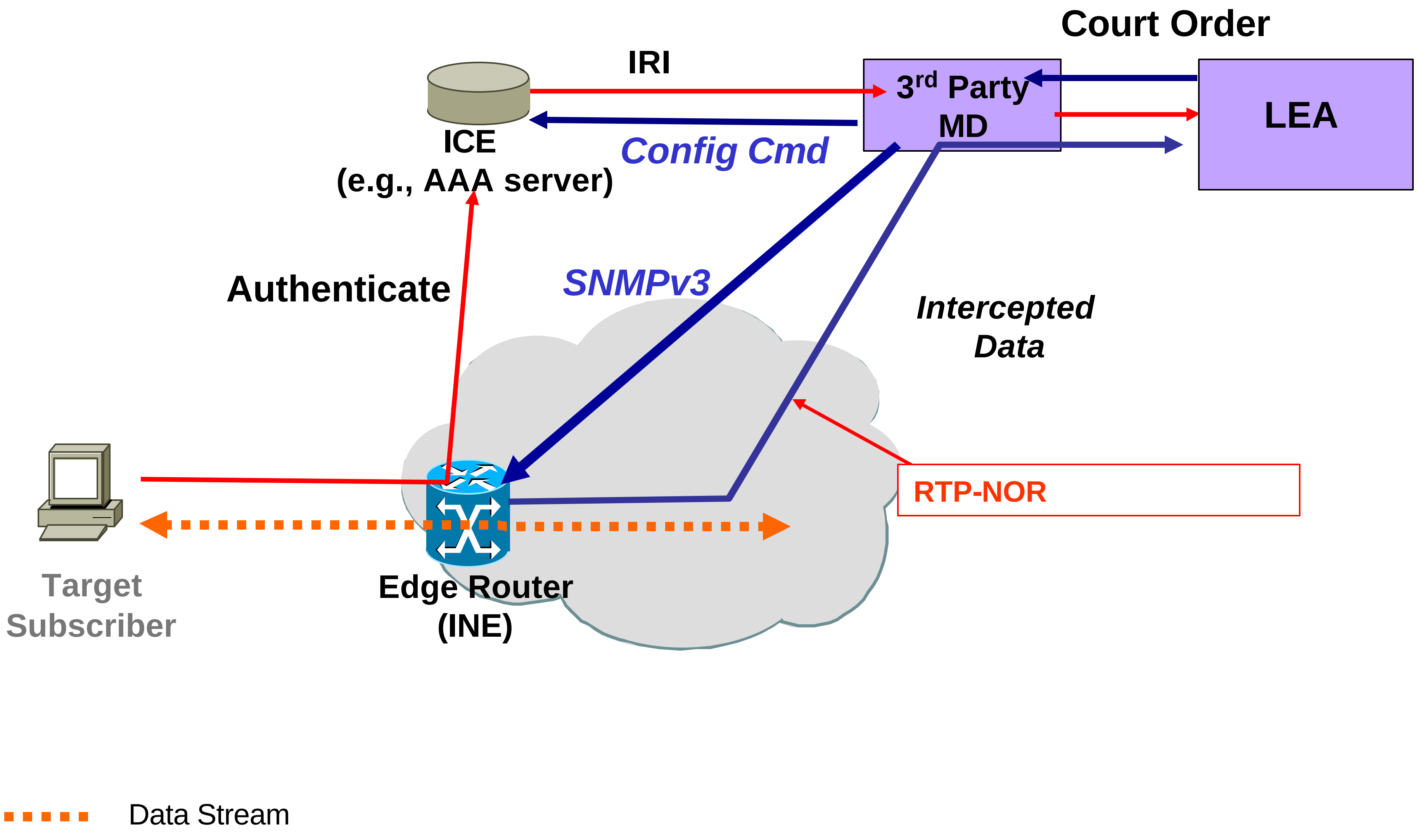
Cisco Service-Independent Intercept™ (SII) – Data Intercept



Cisco SII - Voice Intercept

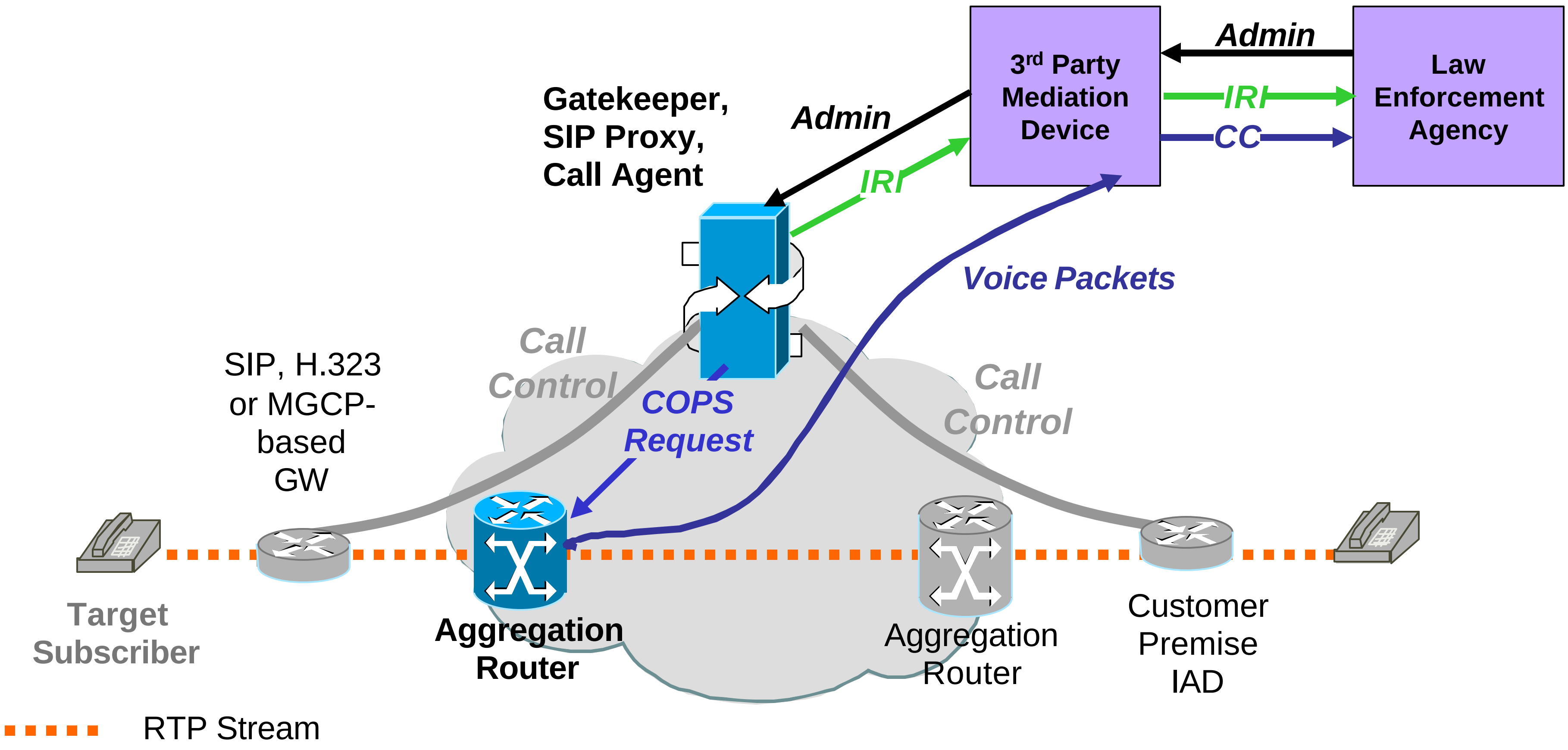


Cisco SII™ - Data Intercept



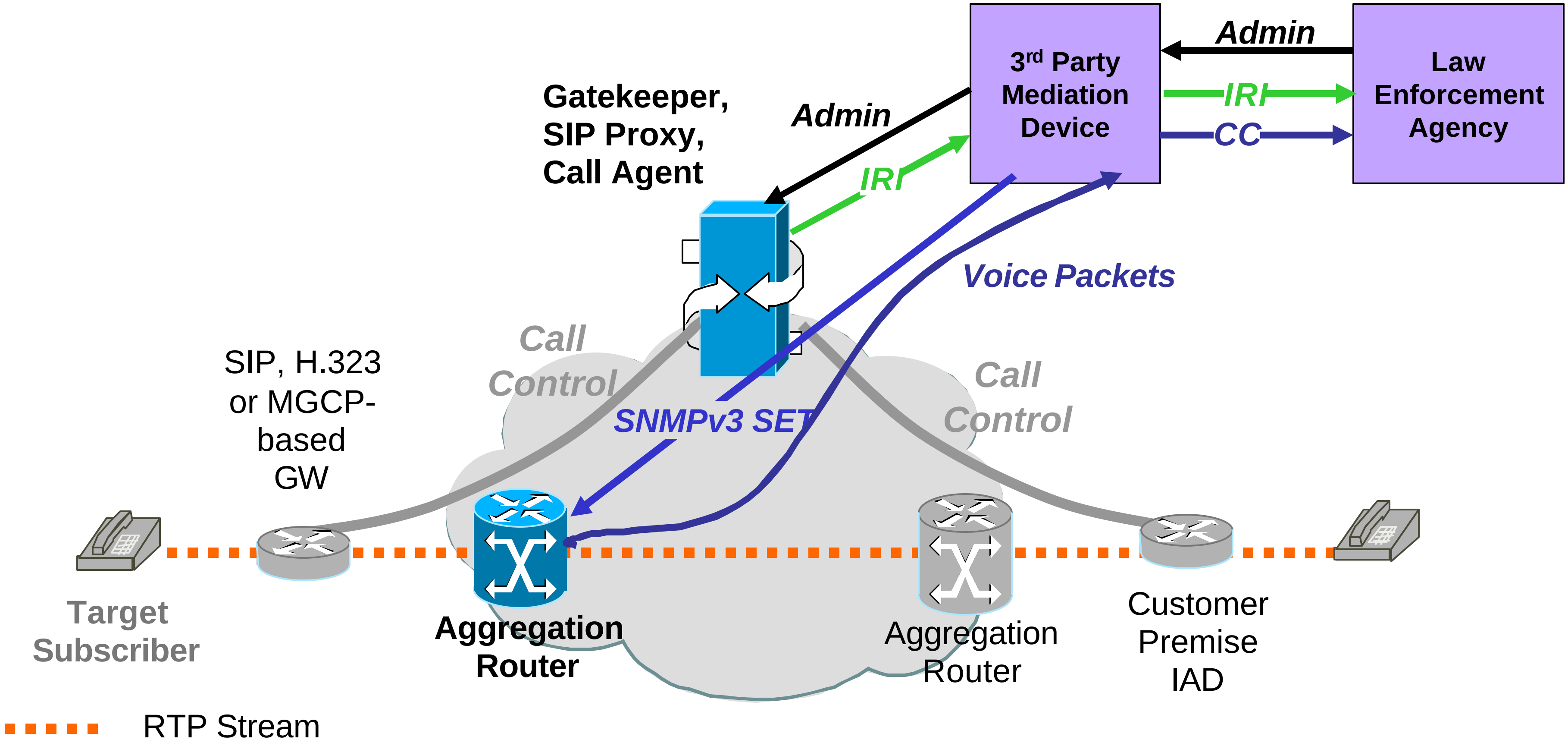
PC Voice Intercept –

Edge/Aggregation Router

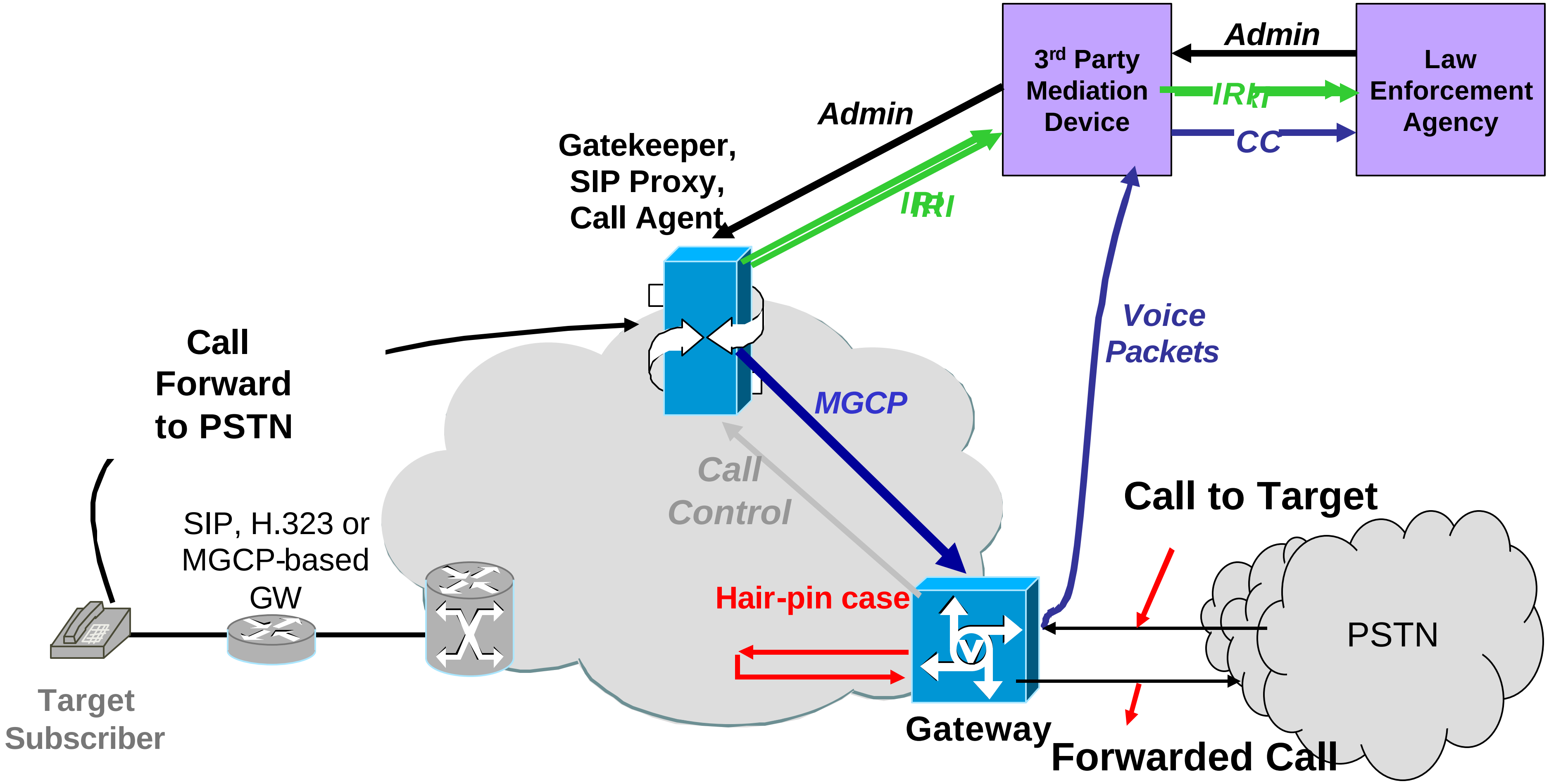


SII™ Voice Intercept –

Edge/Aggregation Router



PC Voice Intercept – Trunk Gateway
Hairpin Case



Admin

3rd Party Mediation Device

Law Enforcement Agency

IRI

CC

Admin

IRI

Gatekeeper, SIP Proxy, Call Agent

Voice Packets

Call Forward to PSTN

MGCP

Call Control

Call to Target

SIP, H.323 or MGCP-based GW

Hair-pin case

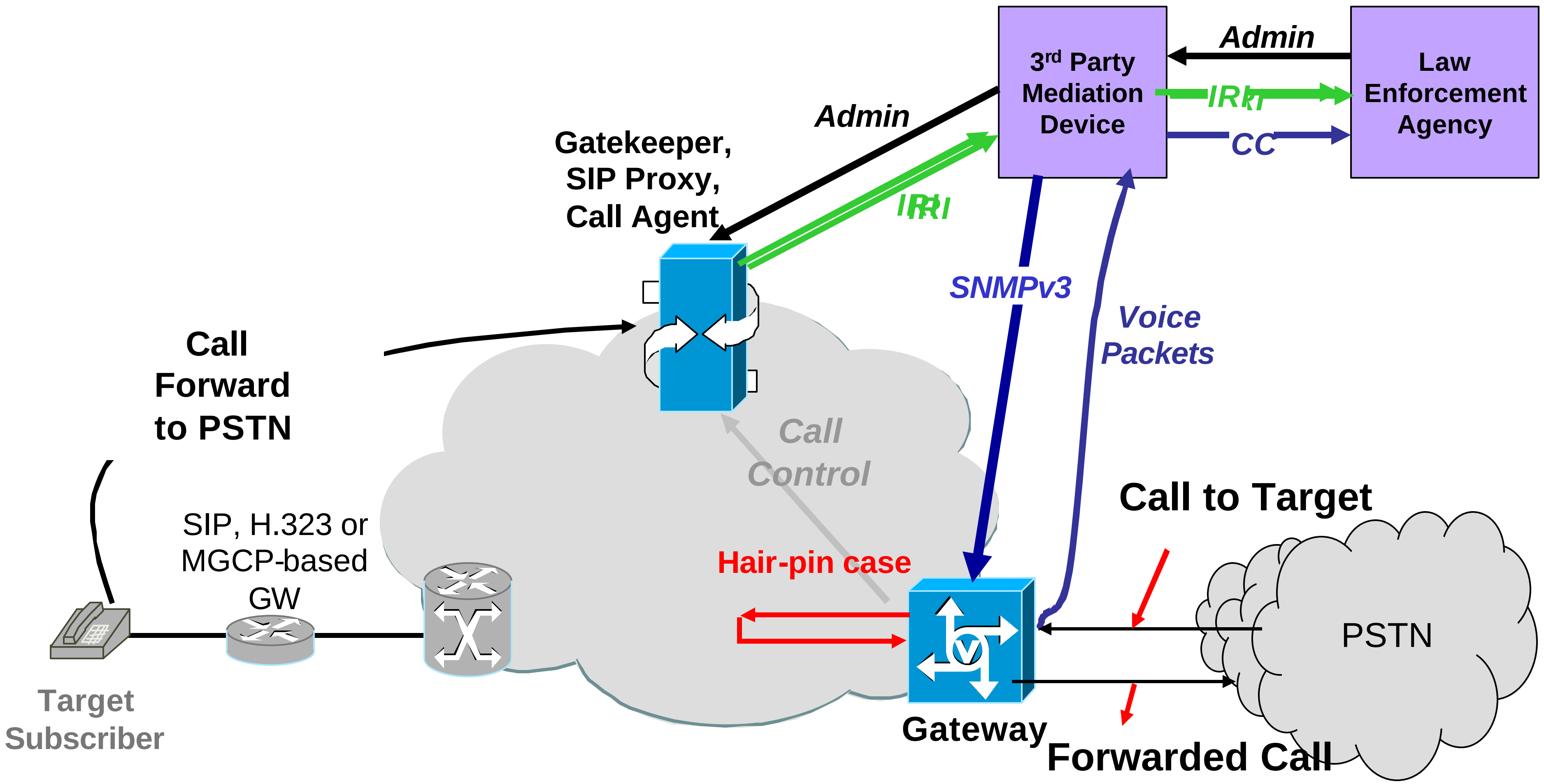
PSTN

Target Subscriber

Gateway

Forwarded Call

SII Voice Intercept – Trunk Gateway
Hairpin Case



Simple Law Enforcement Monitoring

Fred Baker

draft-baker-slem-architecture-01.txt

ftp://ftpeng.cisco.com/fred/ietf/slem.ppt

ftp://ftpeng.cisco.com/fred/ietf/slem.pdf