CALEA Compliance on a Budget

WISPA CALEA Standard for IP Network Access

WISPA CS IPNA v.1
WISPA CA IPNA v.2

INTRODUCTION(S)

- Who is WISPA?
  - Trade Organization for WISPs
  - Lobby (voice) in DC
- What was done?
  - WISPA created a committee of several members, along with some outside assistance to create an industry standard

So What is CALEA?

The Communications Assistance for Law Enforcement Act (CALEA) is a United States wiretapping law passed in 1994 (Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010). In its own words, the purpose of CALEA is:

To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes.

The CALEA Committee Process

What did we do?

Process started around April of 2007 with a trip to Quantico to interview the FBI CALEA Implementation Unit.

Much work was done on a mailing list with the aid of a Wiki.

We created a standard that will facilitate an the implementation of an OpenSource CALEA solution.

Goals of the Process

Open source solution to the CALEA standards effort for IP network.
Status: In development (code is being written).

A standard which would pass review of the FBI
Status: Accomplished.

A standard which vendors could implement.
Status: Accomplished.

Obtain ***temporary*** safe harbor for WISPs who can not meet the isolation requirement today.
Status: Accomplished.

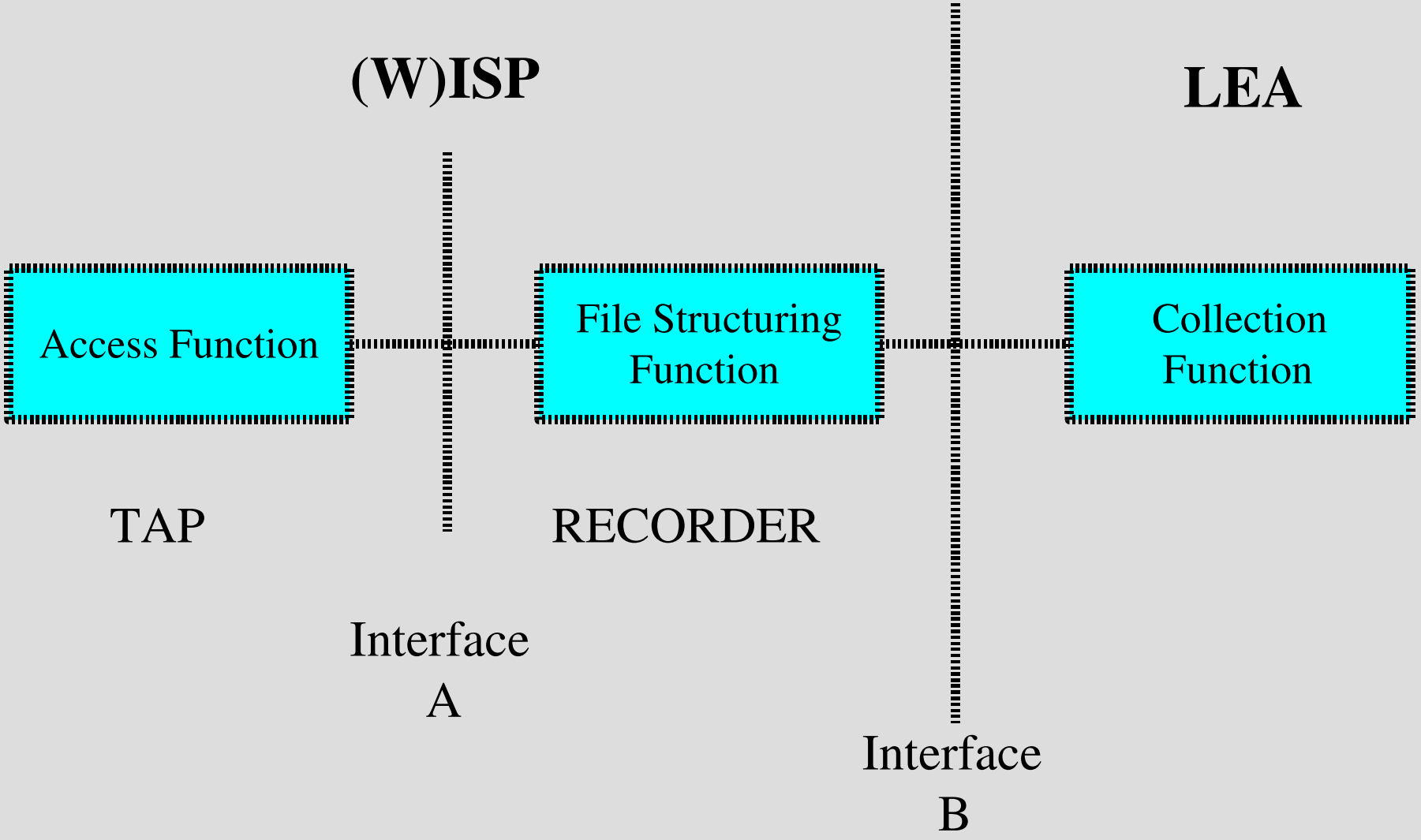
Safe Harbor

What is safe harbor? ***Safe Harbor is immunity from prosecution for failing to be able to satisfy a CALEA action.***

Some network architectures do not lend themselves to CALEA compliance and need to be “grandfathered” under a standard which allows operators to become compliant over time.

We were given one year. IPNA v.1 sunsets one year from now and version two has no NAT exclusion.

CALEA Collection Model



CALEA Requirements

There are 13 legal *principles* which *must be met* to satisfy an action under the CALEA statute.

These principles exist to protect the privacy of all parties and to ensure that LEAs receive properly handled evidence.

CALEA Requirements

Transparency.

Your collection must be transparent to the target of the collection.

R-10 ... the subject can not detect ...

R-20 ... intercept shall be transparent ... to all other non-authorized persons...

CALEA Requirements

Confidentiality and Access Control

Your collection must be conducted in confidentially and no unauthorized persons may be aware of the intercepts.

R-30 ... only authorized persons shall have knowledge ... or access ...

CALEA Requirements

Authentication and Isolation (1)

You must be able to prove the data you collect was in fact from the target of the investigation.

R-40 ... to the extent used in ... business ... ensure ... communication originates from or is directed to ... subject AND ... shall not deliver communications which do not originate from or are not directed to... subject

CALEA Requirements

Authentication and Isolation (2)

R-50 Isolation ... is required ... isolate the target stream regardless of ... NAT ...

V.1 Safe Harbor – sunsets in one year

CALEA Requirements

Authentication and Isolation (3)

The NAT exemption (R-50)

R-50 (cont) ... required to attempt full compliance ...
If no reasonable alternative exists, you may be exempted ... If you meet all other requirements of CALEA. Very strict exemption.
Expires in one year.

CALEA Requirements

Validation

You must be able to prove that the data you collected is the data the target processed.

R-60 ... ensure that the intercepted communications ... are associated with the subject ...

CALEA Requirements

Nonrepudiation (1)

The LEA must be able to prove that the data you reported is the data they took to court.

R-70 ... keep and secure ... accurate records ... of intercepts and hashes ...

R-80 ... keep and secure ... sufficient records to prove, after the intercept ... the communications were associated with the subject ...

CALEA Requirements

Nonrepudiation (2)

The LEA must be able to prove the data you reported is the data they took to court

R-90 ... SHA256 ... shall be used ... for data integrity...

R-100 Copies of the hash ... shall be delivered to the LEA ...

AND those shall be maintained ... as a business record ...

CALEA Requirements

Correlation (1)

The data you collect must be correctly time stamped so that it can be correlated by traffic flow and by packet.

R-110 ... ensure ... OOB events and packet captures ... or summary reports ... are accurately correlated ... (by timestamp)

R-120 ... shall ensure ... intercept categories are correctly correlated ... (by timestamp)

CALEA Requirements

Correlation (2)

The data you collect must be correctly time stamped so that it can be correlated by traffic flow and by packet.

R-130 ... all systems ... have coordinated system times ... accurate to 200ms ...

R-140 ... shall use IAP and FSF time stamps as the basis for OOB message correlation ...

CALEA Requirements

Proportionality

The LEA is not allowed to accept unauthorized data and we are not allowed to collect it.

R-150 WISP shall ensure that only authorized communications categories ... are delivered ...

CALEA Requirements

Completeness

The WISP must collect all communications cited in the action

R-150 ... shall ensure ... complete communications ... shall be intercepted ...

CALEA Requirements

Compression

If compression is used to deliver data to the FSF the compression used must be lossless. Compression may not be between FSF and LEA

R-160 If ... compression is employed ... across the “a” interface ... (it) shall not allow loss of data ... WISP shall not use compression ... transmitting, buffering, storing, or delivering ... to the LEA

CALEA Requirements

Encryption

The WISP must provide either decrypted data or the keys when he provides the encryption service.

C-10 ... deliver ... intercepted data ... in unencrypted form or ... provide algorithms used ... and keys

CALEA Requirements

Performance

Must be able to collect multiple intercepts on multiple subjects at the same time

R-180 ... capable of ... multiple simultaneous intercepts per subject.

R-190 ... capable of ... multiple simultaneous intercepts ... multiple subjects.

CALEA Requirements

Transparent across Law Enforcement Agencies

No agency may know what other agencies are doing and personel investigating one case ID may not know about other case Ids.

R-200 Multiple LEA intercepts for the same ... or different subjects ... transparent to the respective LEAs ... or performed for the same LEA under different case IDs.

CALEA Requirements

Availability and Reliability

You must ensure the collection system does not loose or corrupt intercepted data.

R-210 ... use appropriate performance and reliability mechanisms ... that eliminate(s) ... likelyhood that ... intercept will be corrupted ... may require a reliable transport protocol ...

Current Status of MikroTik's Implementation

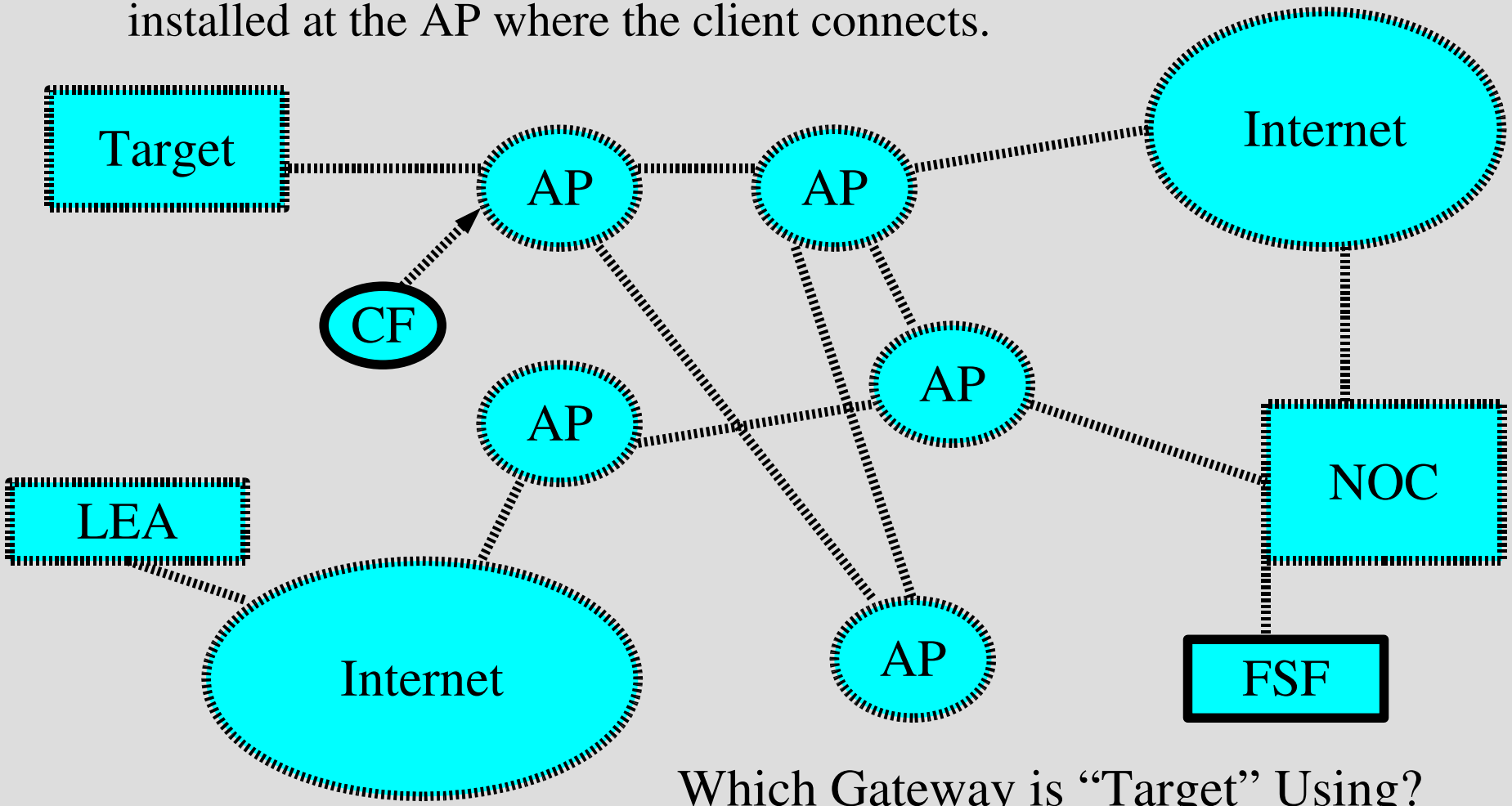
- Still in development
- Client/Server parts are done
  - Intercept portion (client side) is CLI access only
    - You need to be familiar with command line firewall rules to build an intercept
  - Server side will accept a stream from the client
- Much of the work has already been done
  - Intercept capability is there
  - Directory structure is there
  - Transparency between logins is done
- Completion is just weeks away – This will support the WISPA CALEA Standard

Time for a quick How-To

- Your network is running PPPoE
- Scenario 1
  - Collect ALL data for a customer who you know to be using userid of “joeblow”
- Scenario 2
  - Collect only emails sent and received by customer using IP address 10.10.10.2
    - We will demonstrate ONLY POP3 (TCP/110) and SMTP (TCP/25)

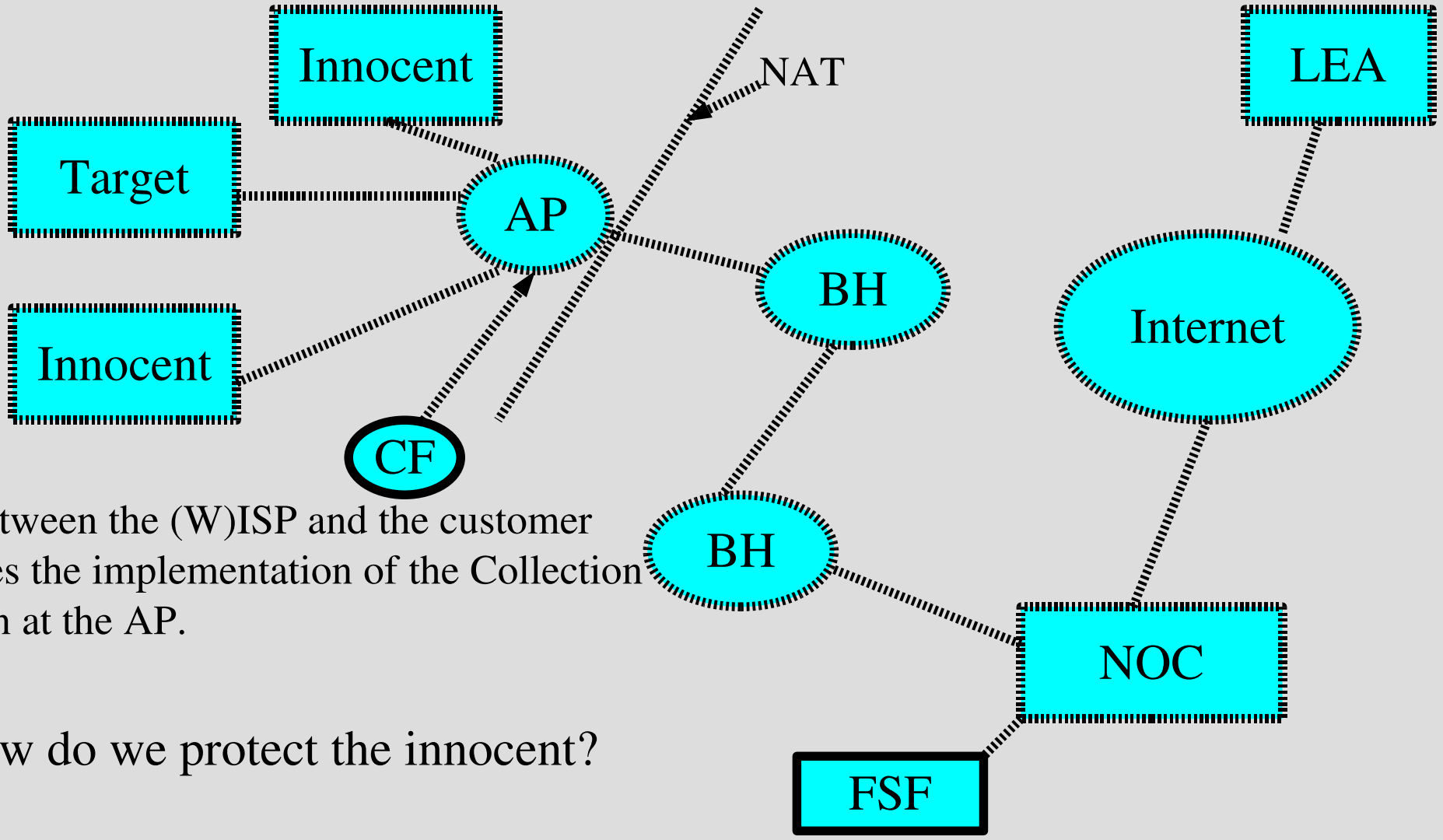
CALEA Considerations in Network Implementation

Mesh networks necessitate the collection function be installed at the AP where the client connects.



Which Gateway is “Target” Using?

CALEA Considerations in Network Implementation

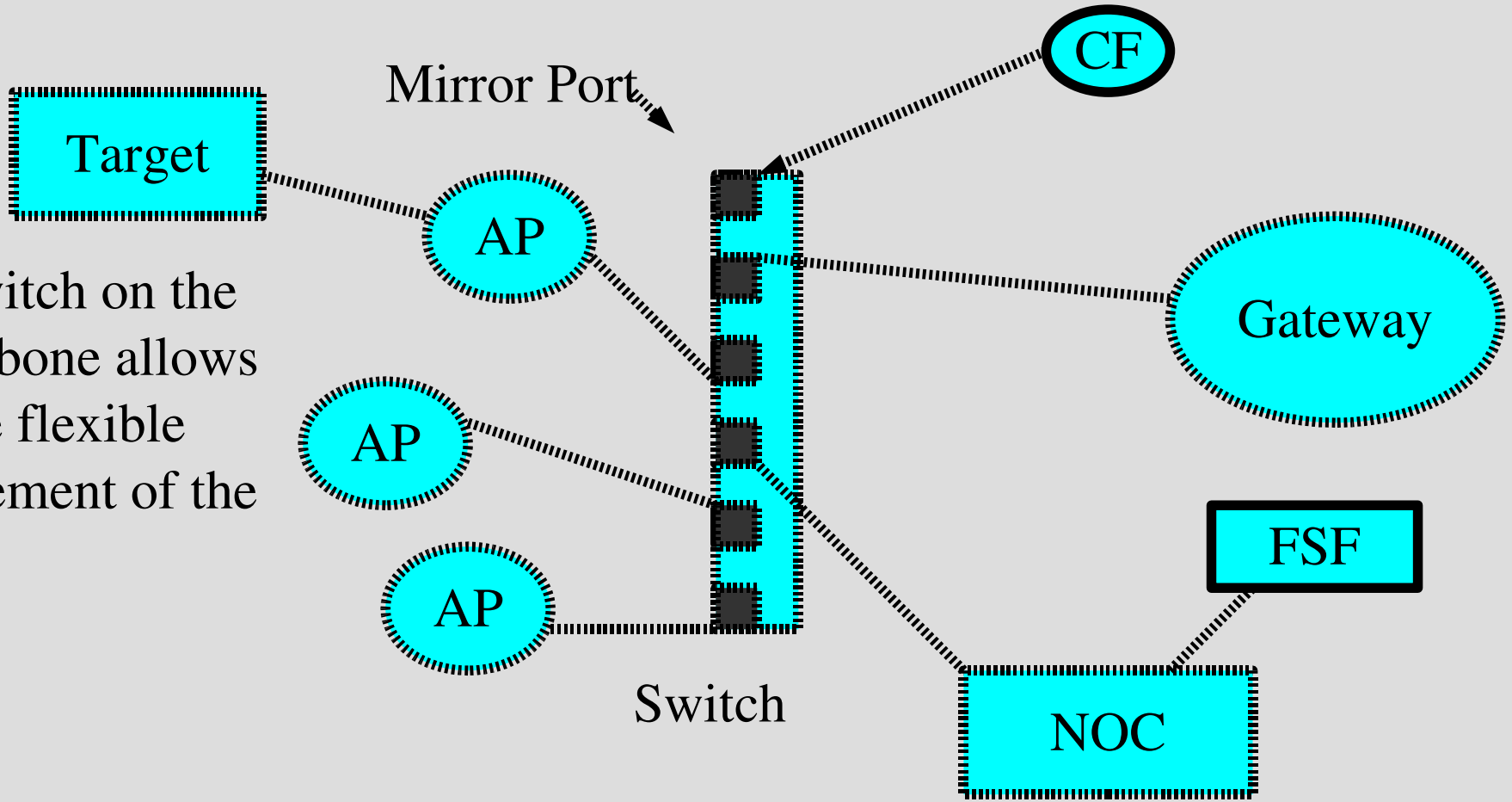


NAT between the (W)ISP and the customer mandates the implementation of the Collection Function at the AP.

How do we protect the innocent?

CALEA Considerations in Network Implementation

A switch on the backbone allows more flexible placement of the CF.



References and Further Information

- MikroTik's wiki
  - http://wiki.mikrotik.com/wiki/Calea
- WISPA Website
  - Main Page: http://www.wispa.org/
  - CALEA Standard page: http://www.wispa.org/calea/WCS/
- Butch Evans Consulting
  - http://www.butchevans.com/