Butch Evans Consulting
butche@butchevans.com

CALEA Workshop

Implications and procedures for Mikrotik WISPs

Butch Evans Consulting
butche@butchevans.com

About Me

- IANAL, nor do I play one on TV
- I have worked with Mikrotik RouterOS for 3-4 years
- I've been involved with the ISP business since 1993; Full time consulting since 2006
- I am a network engineering consultant and a certified Mikrotik Trainer
  - I do engineering work as well as troubleshooting
  - I have one fully developed course for Mikrotik in partnership with WISP-Router and another is under development (see Eje for some flyers about the courses)
- I am working with WISPA to help create an “industry standard” that will provide a safe harbor for WISPs using Mikrotik

Butch Evans Consulting
butche@butchevans.com

Some Background about CALEA

- What IS CALEA anyway?
  - Communications Assistance for Law Enforcement Act
- Ok...so WHAT IS CALEA?
  - CALEA is a statute that defines obligations of telecommunications carriers (including WISPs) to insure their ability, pursuant to lawful authorization, to isolate and enable government to intercept electronic communications of a subject, as well as the delivery of intercepted communications to Law Enforcement

Butch Evans Consulting
butche@butchevans.com

How does CALEA affect ME?

- Who does CALEA apply to?
  - In April 22, 2005 Wireless Broadband Task Force Report; GN Docket No. 04-163,
  - The Department of Justice filed comments with the FCC requesting that the Commission continue to preserve the vital national security and criminal law enforcement capabilities of CALEA as it develops a deregulatory framework for wireless broadband Internet access services.
- Doesn’t anybody care that I don’t have the money for this?
  - NO (kind of)
  - These statutes apply to WISPs – even if you (we) don't like it

Butch Evans Consulting
butche@butchevans.com

What are my capability requirements?

- What Do I Actually Have to Be Able to Do? Pursuant to a court order or other lawful authorization, WISPs must be able to:
  - Expeditiously isolate all wire and electronic communications of a target transmitted by the carrier within its service area;
  - Expeditiously isolate call-identifying information of a target;
  - Provide intercepted communications and call-identifying information to law enforcement; and

Butch Evans Consulting
butche@butchevans.com

Capability Requirements (cont.)

- Carry out intercepts unobtrusively, so targets are not made aware of the electronic surveillance, and in a manner that does not compromise the privacy of other network users
- Deliver the intercept traffic to the requesting LEA – you must be capable of starting this stream within 48 hours of receiving a subpoena/court order and it is required to be in a specific format (T1-IAS)

Butch Evans Consulting
butche@butchevans.com

About “Safe Harbor”

- What is Safe Harbor?
  - To be covered by a safe harbor means that your network meets standards that are adopted by industry or the FCC
  - T1-IAS is a “safe harbor” standard
  - WISPA (http://www.wispa.org/) is developing a standard that will provide safe harbor which Mikrotik will meet (that's MY goal anyway)

Butch Evans Consulting
butche@butchevans.com

More than one type of subpoena

- Some subpoenas will require different response times
- Some subpoenas will require different data captures
- There are cases where you will possibly be required to begin capturing data before a subpoena is delivered
  - These are extreme cases – life and death type deals
  - MOST of the time, you will have a court order that tells exact details of the request

Butch Evans Consulting
butche@butchevans.com

The letter vs spirit of the law

- Requirements are very stringent
  - Some requirements are intentionally vague
  - Lots of “wiggle room” in the law
- The law has a human side – well, enforcement is human anyway
- As long as you can provide the necessary information, you SHOULD be ok
- You should know your limitations

Butch Evans Consulting
butche@butchevans.com

SO..what do I do now?

- DON'T PANIC
  - CALEA is not to be ignored, but it isn't THAT big a deal
    - CALEA action is going to be VERY RARE
    - MANY vendors are incorporating CALEA compliance solutions, including Mikrotik – that's why we're here.

Butch Evans Consulting
butche@butchevans.com

CALEA Compliance Options

- Compliance options
  - Do it yourself
    - Network design and documentation MUST begin NOW
  - TTP
    - They can assist with some of the technical requirements of compliance, but the responsibility of compliance still lies with you

Butch Evans Consulting
butche@butchevans.com

First and Foremost

- Some forms that should already be filed
  - Form 445 – This form basically updates the FCC on how you are planning to become compliant. It was due on Feb 12, 2007
  - Your SSI – System Security and Integrity manual – This is a plan that states how you will respond to a subpoena. Due on March 12, 2007
  - Final compliance date is (was) May 12, 2007

Butch Evans Consulting
butche@butchevans.com

Getting Legal Assistance

- These forms can be completed by you or your attorney
  - Kris Twomey can do this for you for $250 (maybe less)
  - kris@lokt.net (202)-250-3413 http://www.lokt.net/

Butch Evans Consulting
butche@butchevans.com

What if my equipment can't?

- Hotspots
  - If you have a hotel as an ISP customer and they run a hotspot (free or otherwise)
- If you have a NAT device that does not allow you to capture data
  - You may be required to capture all data to and from that device
- Live streaming requirement and your bandwidth availability

Butch Evans Consulting
butche@butchevans.com

Network Design and Documentation

- Your design choices will affect how and where a “tap” must be located
  - Bridged/Static Routed/Dynamic Routed
  - Firewall can affect this as well
  - Wireless - “default forwarding”
  - NAT
  - Static Addressing/DHCP
  - PPPoE/PPtP
- YOU MUST be able to determine the identity of every customer and you CANNOT wait until you get a subpoena

Butch Evans Consulting
butche@butchevans.com

Definitions

- Tap – hardware or software device that facilitates the intercept (capture) of the data traffic
  - Historically, a “tap” was a hardware device that provided a place in the network to facilitate recording of a phone call.
  - A hardware tap is a device that provides a “tee” that “mirrors” all data, allowing for that data to be intercepted
  - A software tap is the name given to a device that will see all data on a given segment, and has the ability to capture that data and send it to a storage server – Mikrotik's CALEA support provides a software tap

Butch Evans Consulting
butche@butchevans.com

More Definitions

- Intercept – the process of collecting (capturing) data for the LEA
- Tap point – the location in the network where the data is actually collected. Network design issues will affect where this point must be.
- Storage Server (CALEA server) – A device serves as a store and forward location. Collected data is sent here to be collected (at a later time) by the LEA

Butch Evans Consulting
butche@butchevans.com

Mikrotik CALEA Feature List

- Multiple subject/multiple destination packet interception
- Streaming support for the following formats:
  - PacketCable 2.0 Packet Cable Electronic Surveillance Delivery Function to Collection Function Interface Specification
  - IPCalblecom Electronic Surveillance Standard
    - Approved method for Communication Content delivery to LEA according to ATIS-1000013.2007 (Lawfully Authorized Electronic Surveillance For Internet Access and Services)
  - TZSP format - for reception with 'Ethereal', tcpdump, trafr (sniffer stream reader for linux)

Butch Evans Consulting
butche@butchevans.com

Mikrotik CALEA Support

- Two parts
  - CALEA-server package
    - Provides support for accepting multiple CCC streams
    - Stores streamed content for delivery to LEA
    - Uses libpcap format (industry standard)
    - Automatically creates new files based on
      - User specified file size
      - User specified packet count
      - User specified interval
    - Automatically creates a hash file (md5/sha1/sha256)

Butch Evans Consulting
butche@butchevans.com

Mikrotik CALEA Support (cont)

- Part two
  - Intercept portion (tap)
    - Manage multiple intercepts for a given target
    - Manage multiple intercepts for multiple targets
    - Implemented using firewall filters
      - Currently only CLI

Butch Evans Consulting
butche@butchevans.com

Sample Configuration for an Intercept

Intercept requirements:
Capture all data to and from a user with IP address of 10.10.10.10

Intercept router (tap) configuration:

```
/ip firewall filter
add action=sniff-pc chain=forward sniff-id=477 \
    sniff-target=192.168.5.140 sniff-target-port=1888 \
    src-address=10.10.10.10

add action=sniff-pc chain=forward dst-address=10.10.10.10 \
    sniff-id=477 sniff-target=192.168.5.140 \
    sniff-target-port=1888
```

Butch Evans Consulting
butche@butchevans.com

CALEA Server Side Configuration

CALEA-Server package is required.

This is the stream receiver for the preceeding slide:

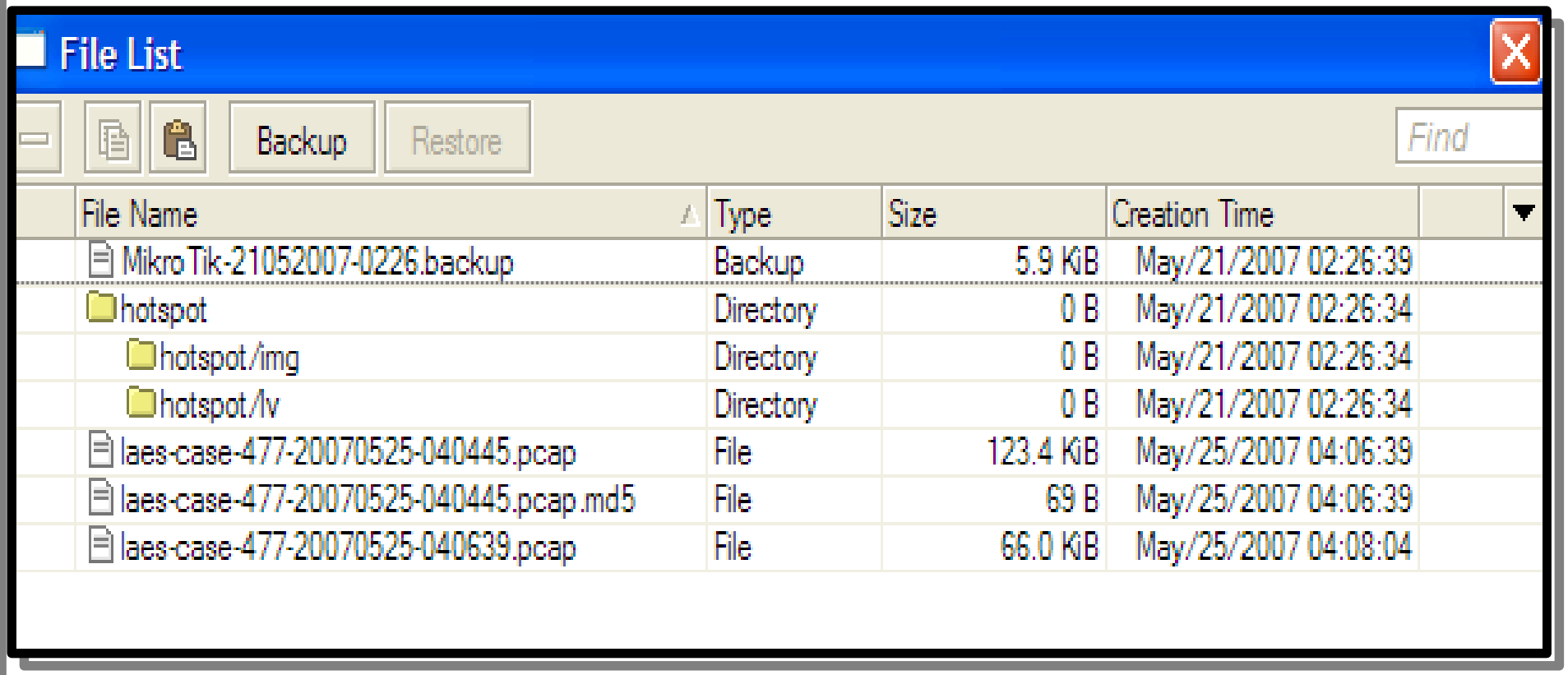
```
/tool calea add action=pcap intercept-port=1888 \
   case-id=477 intercept-ip=192.168.5.140
```

To see the configured intercepts:

```
/tool calea print
Flags: X - disabled
 0   case-id=477 intercept-ip=192.168.5.140 intercept-port=1888
     action=pcap pcap-file-stop-interval=15m pcap-file-stop-size=1024
     pcap-file-hash-method=md5
```

Butch Evans Consulting
butche@butchevans.com

File System



File Name	Type	Size	Creation Time
MikroTik-21052007-0226.backup	Backup	5.9 KiB	May/21/2007 02:26:39
hotspot	Directory	0 B	May/21/2007 02:26:34
hotspot/img	Directory	0 B	May/21/2007 02:26:34
hotspot/lv	Directory	0 B	May/21/2007 02:26:34
laes-case-477-20070525-040445.pcap	File	123.4 KiB	May/25/2007 04:06:39
laes-case-477-20070525-040445.pcap.md5	File	69 B	May/25/2007 04:06:39
laes-case-477-20070525-040639.pcap	File	66.0 KiB	May/25/2007 04:08:04

Butch Evans Consulting
butche@butchevans.com

Intercept Options

The IP Firewall filters now have two additional actions:

sniff - generates a tzsp stream that can be directed to any Wireshark (Ethereal) server
sniff-pc - generates a Packet Cable stream that can be directed to a MikroTik RouterOS system with the calea package installed

By selecting either action, the following options will be available:

sniff-id (*Packet Cable protocol only*) - packet stream case ID
sniff-target - IP address of the data retention server
sniff-target-port - UDP port that the data retention server is listening on

Butch Evans Consulting
butche@butchevans.com

Data Retention (CALEA) Server

- Install the CALEA-server package for your RouterOS version in the normal fashion
- You will have an additional “tool menu” option
  - **/tool calea**
- Allows you to save incoming intercept data streams
- The server will create separate files for each stream
  - One data file and one hash file (if configured)
  - File Size determined by configuration options detailed in the next slide

Butch Evans Consulting
butche@butchevans.com

Data Retention Server Configuration

case-id - case ID set by the intercepting router (***sniff-id*** property)

intercept-ip - IP address of the intercepting router (IP address to receive the stream from)

intercept-port – UDP port to listen on;Set by the intercepting router (***sniff-target-port*** property)

action - storage format (only pcap for now)

pcap-file-stop-interval – This sets the maximum TIME between filesets. A new fileset will be created when this time is reached, unless the ***pcap-file-stop-size*** value is reached first.

pcap-file-stop-size - maximal file size, in KiB

pcap-file-hash-method - hashing algorithm (md5 or sha1) for the data file (saved once the data file is completed and closed); no file is created if set to none

Butch Evans Consulting
butche@butchevans.com

A Short Firewall Primer

- A firewall entry has two parts
  - The MATCH portion
  - The ACTION portion
- If the MATCH portion of the rule matches the packet being processed **100%,** then the ACTION will be taken for that packet

Butch Evans Consulting
butche@butchevans.com

Matching Packets

- The built-in chains
  - INPUT – Packets destined for the router
  - OUTPUT – Packets coming from the router
  - FORWARD – Packets going THROUGH the router
- Custom chains
  - You can create “custom chains” and then use a rule with action of “jump” to process these chains

Butch Evans Consulting
butche@butchevans.com

More On Matching

- The Mikrotik firewall has no sense of direction, that is “added” by your rule
  - src-address, dst-address, dst-port, in-interface, etc.
  - INPUT,OUTPUT and FORWARD are NOT related to packet direction
  - CALEA rules can be added for INPUT and FORWARD, though (generally), you will be using FORWARD chain
- Any field that is not specified in the rule is NOT TESTED to see if it matches

Butch Evans Consulting
butche@butchevans.com

Actions

- The defined action will be taken ONLY if the MATCH portion matches the packet **100%**
- Some actions will “enable” other parameters
  - **sniff-pc,** for example, enables sniff-id and the other CALEA related parameters
- Some actions will prevent later rules from being processed
  - Rules are processed in order
  - Be careful of how your rules are sorted in Winbox

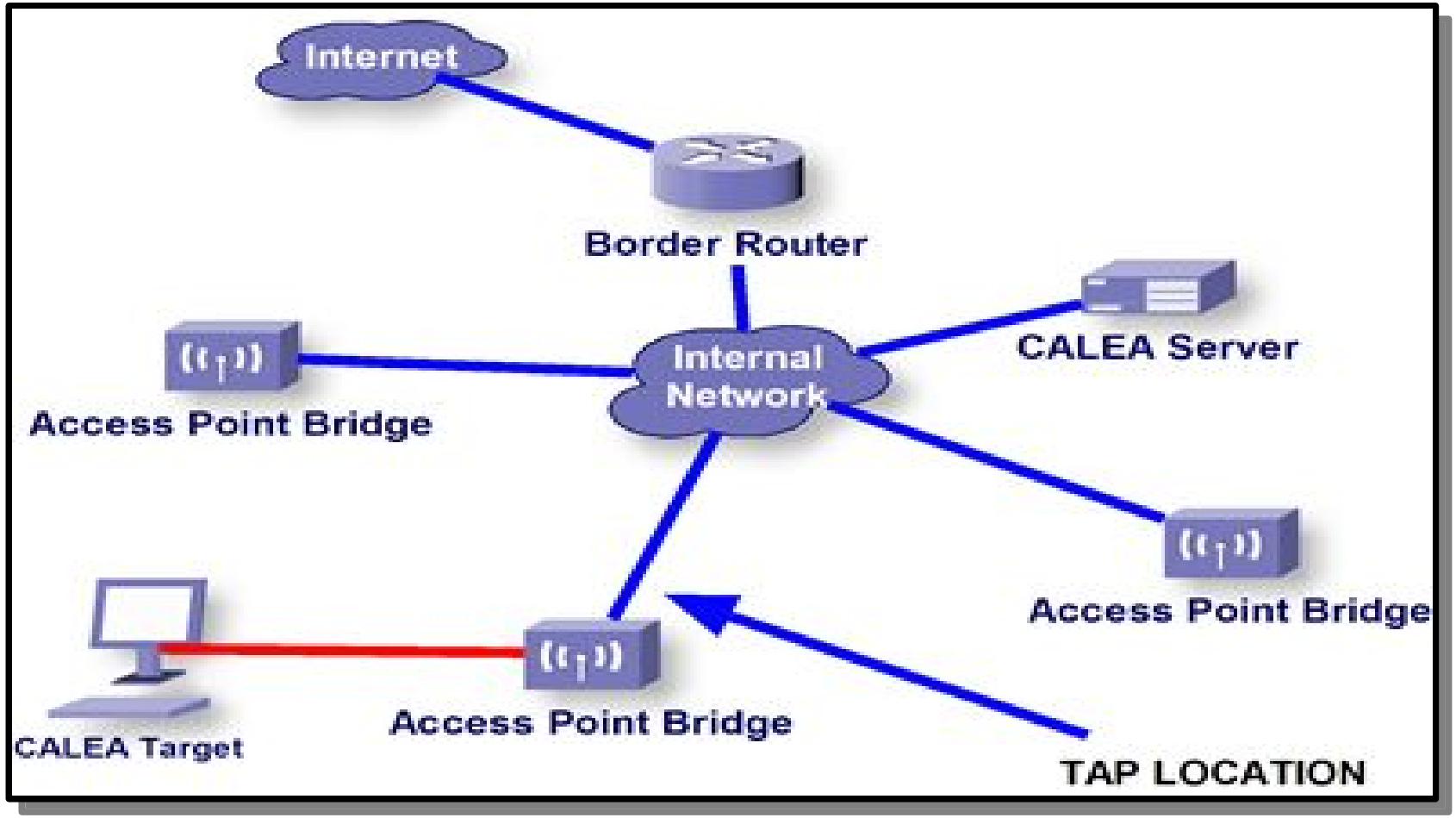
Butch Evans Consulting
butche@butchevans.com

CALEA and the Firewall

- Generally, you will use the FORWARD chain to intercept traffic
- The rules should be placed at the TOP of your FORWARD chain, but this should be discussed with the LEA
- The intercept rules (***sniff-pc*** and ***sniff*** actions) will allow the packet to be processed against the later rules
  - You could conceivably intercept traffic that will be dropped later in the firewall
- Insure that the firewall does NOT block your stream
  - UDP and a user-specified port

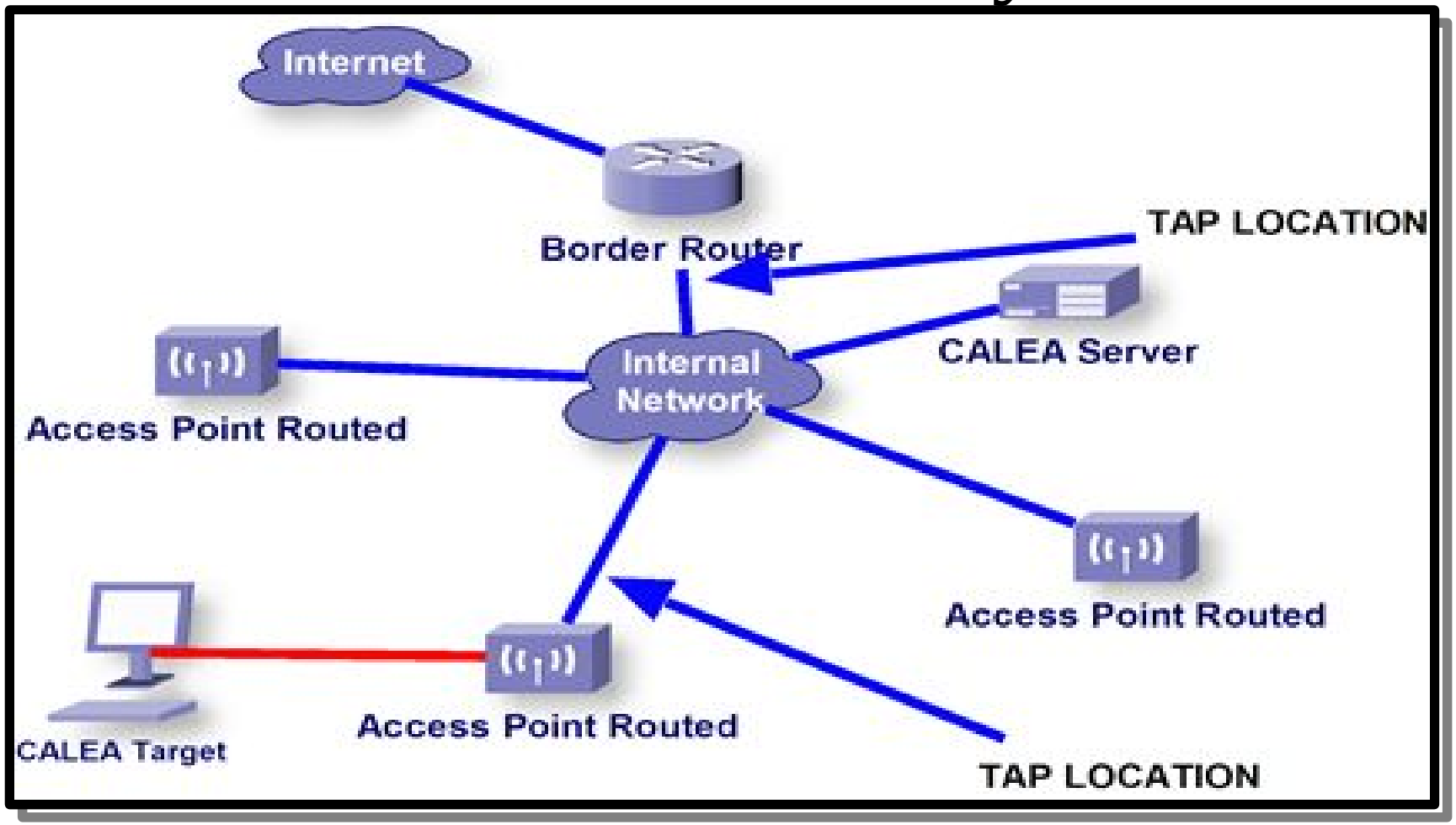
Butch Evans Consulting
butche@butchevans.com

Bridged Network Layout



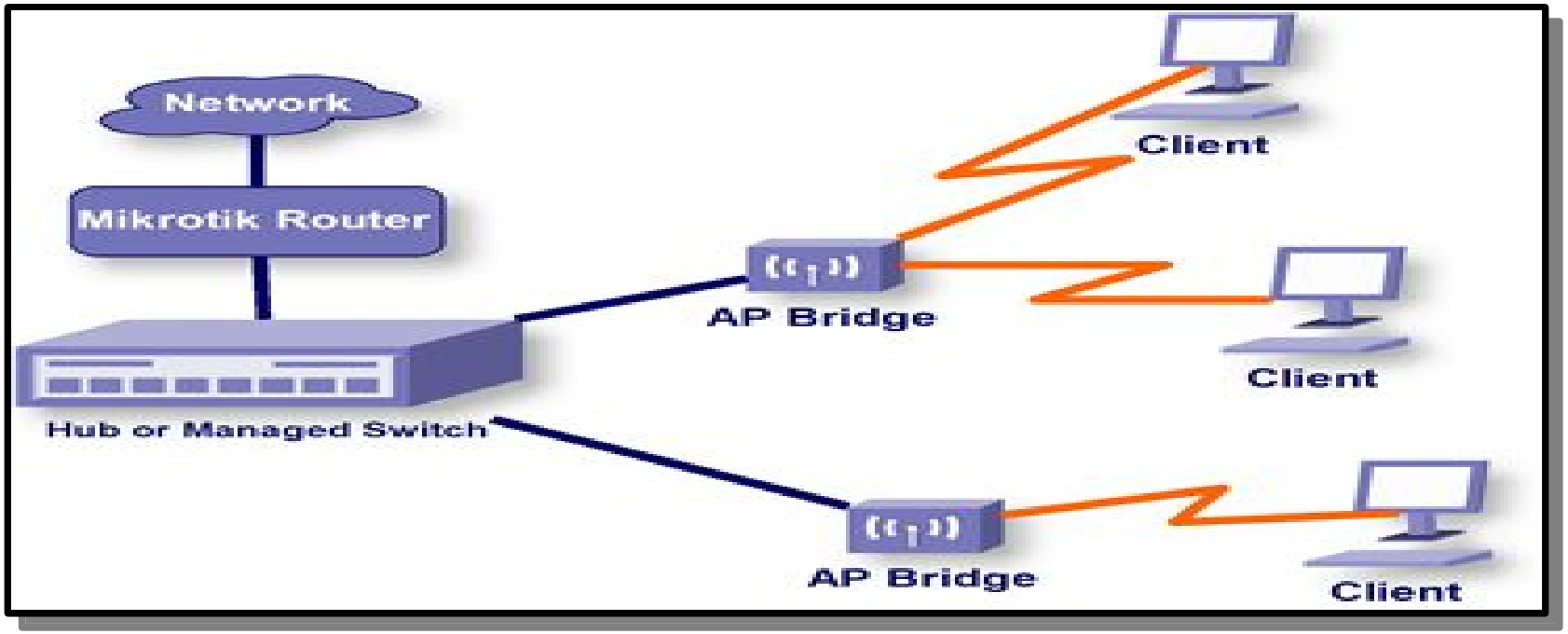
Butch Evans Consulting
butche@butchevans.com

Routed Network Layout



Butch Evans Consulting
butche@butchevans.com

Using external APs

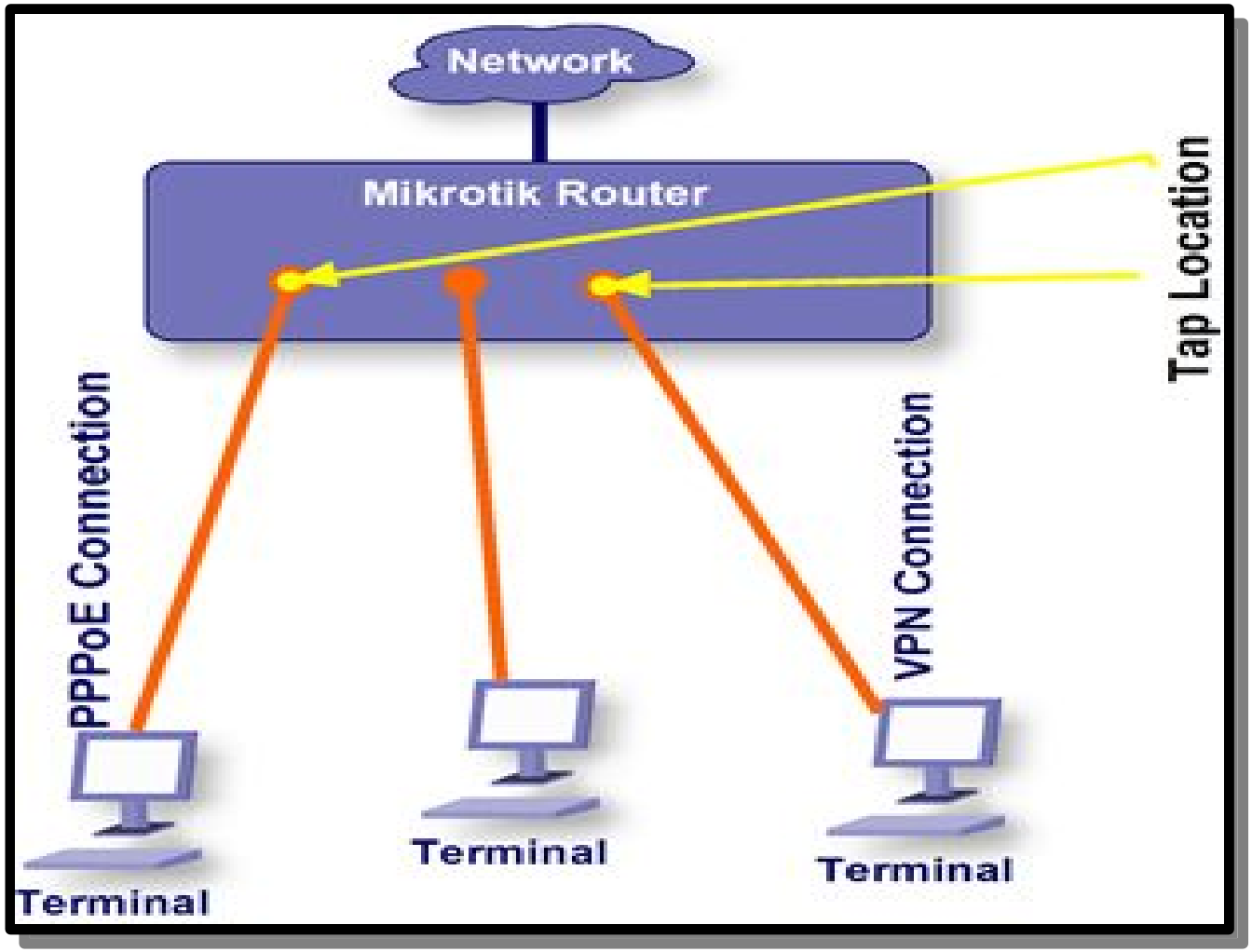


If using an external AP, you must insure that communications between customers of a single AP cannot communicate with one another

Mikrotik calls this “forwarding”. Other names for this feature include: InterBSS Relay and client to client communication

Butch Evans Consulting
butche@butchevans.com

VPN and PPPoE



Butch Evans Consulting
butche@butchevans.com

A Few Examples to Capture

- Capture all traffic to and from 10.10.10.10
- Capture all email (SMTP and POP3) traffic to and from 10.10.10.10
- Capture all traffic between 10.10.10.10 and 10.10.10.11
- Capture all HTTP traffic to and from 10.10.10.10

Contacting Butch Evans

Butch Evans Consulting
802 Stokelan Drive
Malden, MO 63863
573-276-2879

http://www.butchevans.com/
butche@butchevans.com