OpenLI: History, Software and Practical Implementations

Dave Mill - SearchLight
Shane Alcock - WAND, University of Waikato

AusNOG 2022

Dave and Shane

- Dave
  - SearchLight - ISP and Enterprise Consultant
  - Has consulted on many OpenLI implementations in ISPs
  - “Industry advocate” or “token figurehead” of the OpenLI project
  - dmill@searchlight.nz - dave@mill.net.nz
- Shane
  - WAND - University of Waikato
  - 50% time working on OpenLI
  - openli-support@waikato.ac.nz – shane.alcock@waikato.ac.nz

Introductions

- Palmerston North, New Zealand: OpenLI Centre of Excellence

- Plan
  - Background behind OpenLI
  - OpenLI Software
  - ISP Implementations
  - Support options

Lawful Intercept - LI

- LI
- Lawful Intercept
- Intercept
- Telecommunications Interception
- Legal Intercept

Lawful intercept requirements in NZ

Telecommunications (Interception Capability and Security) Act 2013

Public Act 2013 No 91
Date of assent 11 November 2013

Lawful intercept requirements in NZ

Telecommunications (Interception Capability and Security) Useable Format Notice 2017

Pursuant to section 42 of the Telecommunications (Interception Capability and Security) Act 2013 ("Act") and having consulted in accordance with section 42(2) of the Act the Minister for Communications gives the following notice determining a useable format for the purposes of sections 10(5)(a) and 24(7)(a) of the Act.

Notice

1. Title—This notice is the Telecommunications (Interception Capability and Security) Useable Format Notice 2017.

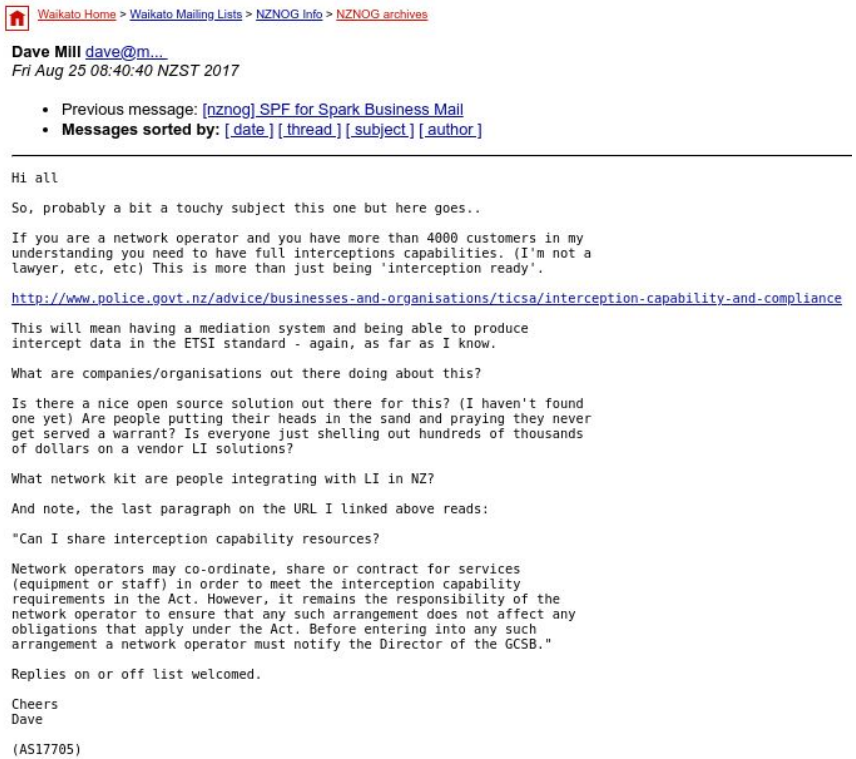
2. Commencement—This notice commences on 17 August 2017.

3. Purpose—This notice determines a useable format for the purposes of sections 10(5)(a) and 24(7)(a) of the Telecommunications (Interception Capability and Security) Act 2013.

4. Application—This notice applies to any person who is subject to section 9 (Network operators must ensure public telecommunications networks and telecommunications services have full interception capability) and section 24 (Duty to assist) of the Act.

5. Useable format—For the purposes of sections 10(5)(a) and 24(7)(a) of the Act, call associated data and the content of a telecommunication is in a useable format if it complies with each of the ETSI standards specified in the table in clause 8 of this notice to the extent those standards are applicable to the activities of the network operator or the service provider, as the case may be.

NZNOG List Post



Waikato Home > Waikato Mailing Lists > NZNOG Info > NZNOG archives

Dave Mill dave@m...
Fri Aug 25 08:40:40 NZST 2017

- Previous message: [nznog] SPF for Spark Business Mail
- **Messages sorted by:** [date] [thread] [subject] [author]

Hi all

So, probably a bit a touchy subject this one but here goes..

If you are a network operator and you have more than 4000 customers in my
understanding you need to have full interceptions capabilities. (I'm not a
lawyer, etc, etc) This is more than just being 'interception ready'.

http://www.police.govt.nz/advice/businesses-and-organisations/ticsa/interception-capability-and-compliance

This will mean having a mediation system and being able to produce
intercept data in the ETSI standard - again, as far as I know.

What are companies/organisations out there doing about this?

Is there a nice open source solution out there for this? (I haven't found
one yet) Are people putting their heads in the sand and praying they never
get served a warrant? Is everyone just shelling out hundreds of thousands
of dollars on a vendor LI solutions?

What network kit are people integrating with LI in NZ?

And note, the last paragraph on the URL I linked above reads:

"Can I share interception capability resources?

Network operators may co-ordinate, share or contract for services
(equipment or staff) in order to meet the interception capability
requirements in the Act. However, it remains the responsibility of the
network operator to ensure that any such arrangement does not affect any
obligations that apply under the Act. Before entering into any such
arrangement a network operator must notify the Director of the GCSB."

Replies on or off list welcomed.

Cheers
Dave

(AS17705)

NZNOG Mailing list

- Kicked off many private and a few public replies
- There was interest for collaborative investigation for ETSI solutions
- Also talked to Richard Nelson at the University of Waikato
  - Interested if existing WAND expertise and libtrace useful
  - It was useful…

$$$$$

- $50k
- Inspire and Lightwire
  - $$$
    $$
- NZNOG Talk in Queenstown
- WAND agreed to start the project

Original Sponsors

Original Website

The OpenLI Project.

OpenLI is being written by the WAND Network Research Group at the University of Waikato. The primary aim is to meet the requirements of New Zealand's TICSA legislation. The work is being funded by a group of NZ services providers who came together in response to an email by Dave Mill to the NZNOG mail list.

Delivery

04 Jan 2019

salcock

1.0.0

a6a27b2

Compare

OpenLI 1.0.0

The first official release of OpenLI!

See https://openli.nz for more details on what OpenLI is and an overview of how it works.

As this is an initial release, we expect that there may be a few issues / incompatibilities for new users, despite our best efforts to test the code as thoroughly as we could. Please be patient and report any problems to us (preferably via a Github issue) as soon as possible. With any luck, we should be able to get something pretty stable that works well for most people within a few months of this initial release.

▾ Assets 2

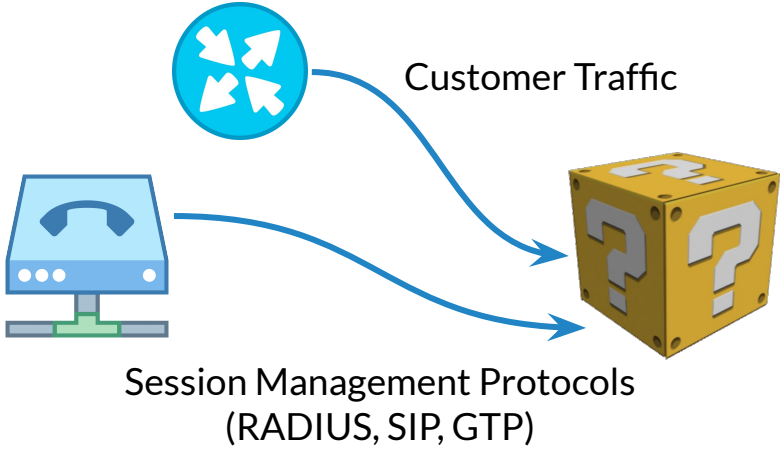
Source code (zip)	04 Jan 2019
Source code (tar.gz)	04 Jan 2019

Beginnings of OpenLI

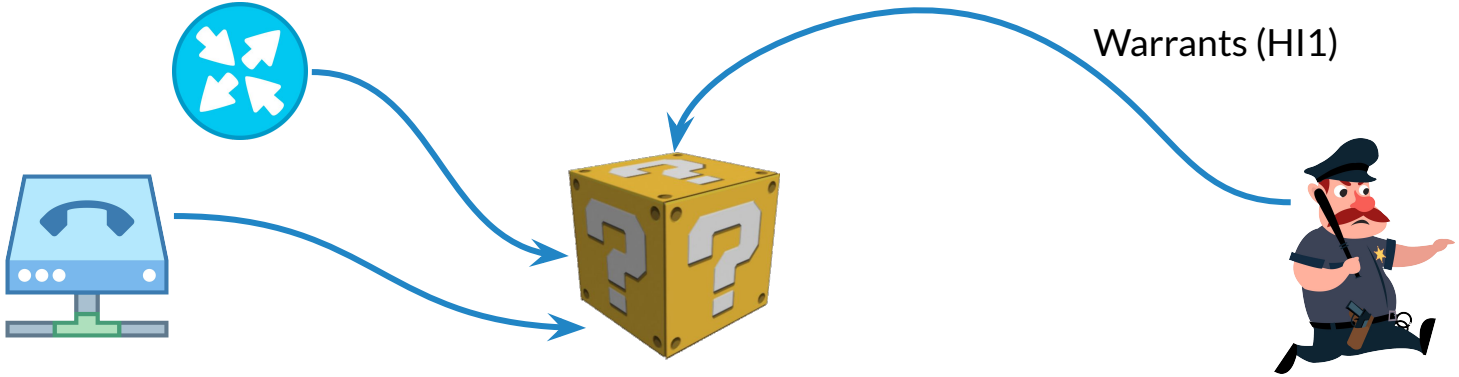
- Shane Alcock - WAND
- Principal coder for OpenLI - 95%?
- Over to Shane…

The LI Mystery Box

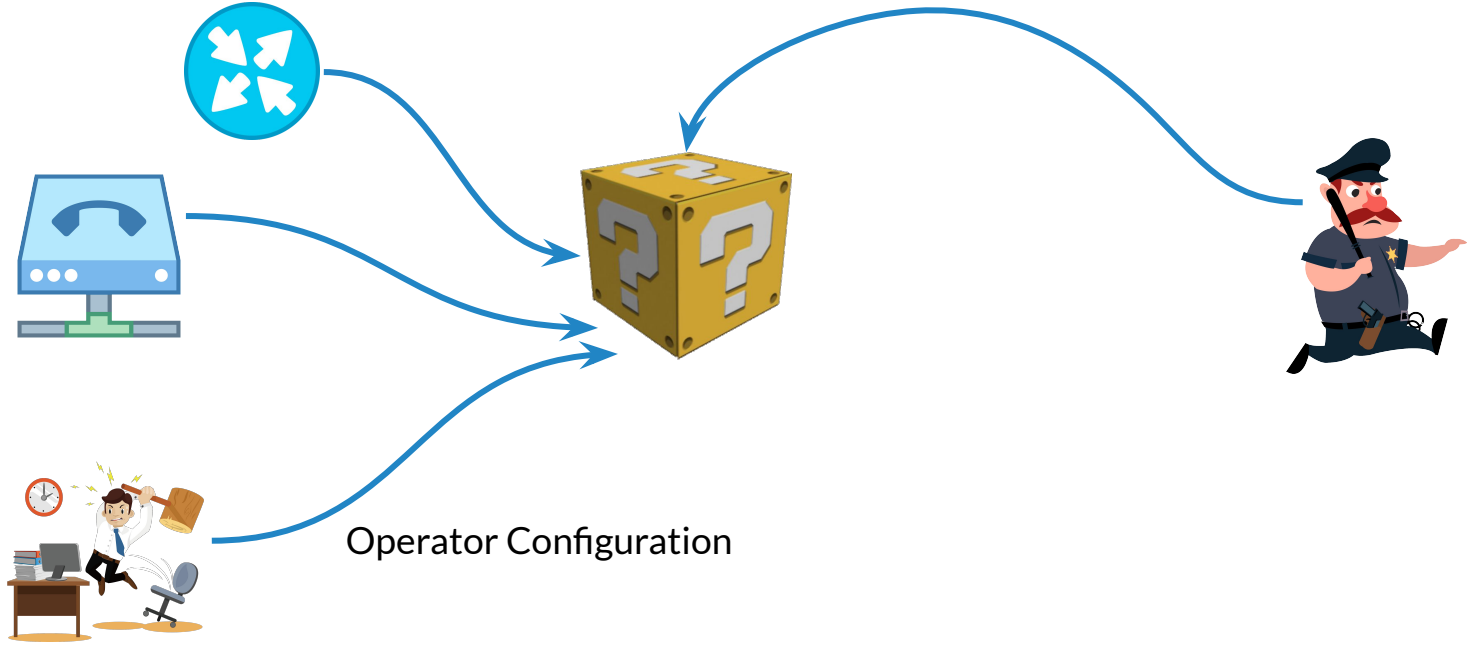
The LI Mystery Box



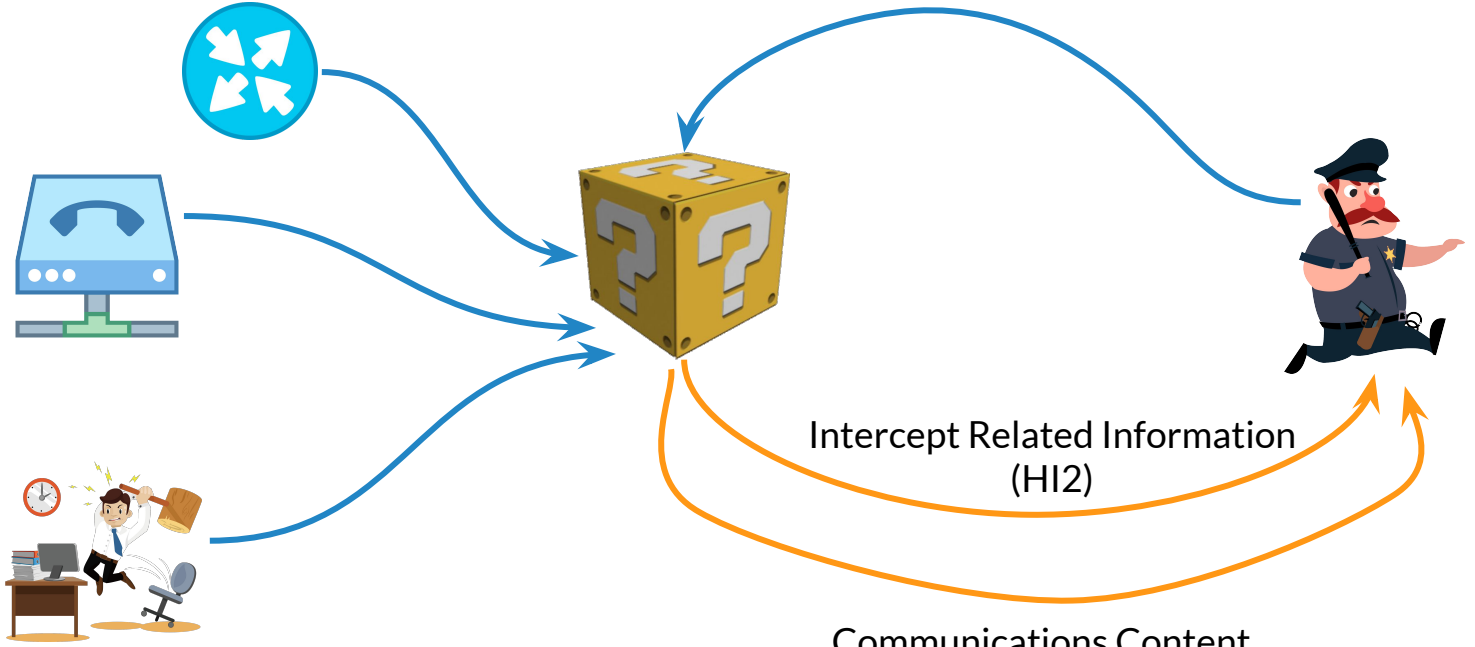
The LI Mystery Box



The LI Mystery Box



The LI Mystery Box



OpenLI

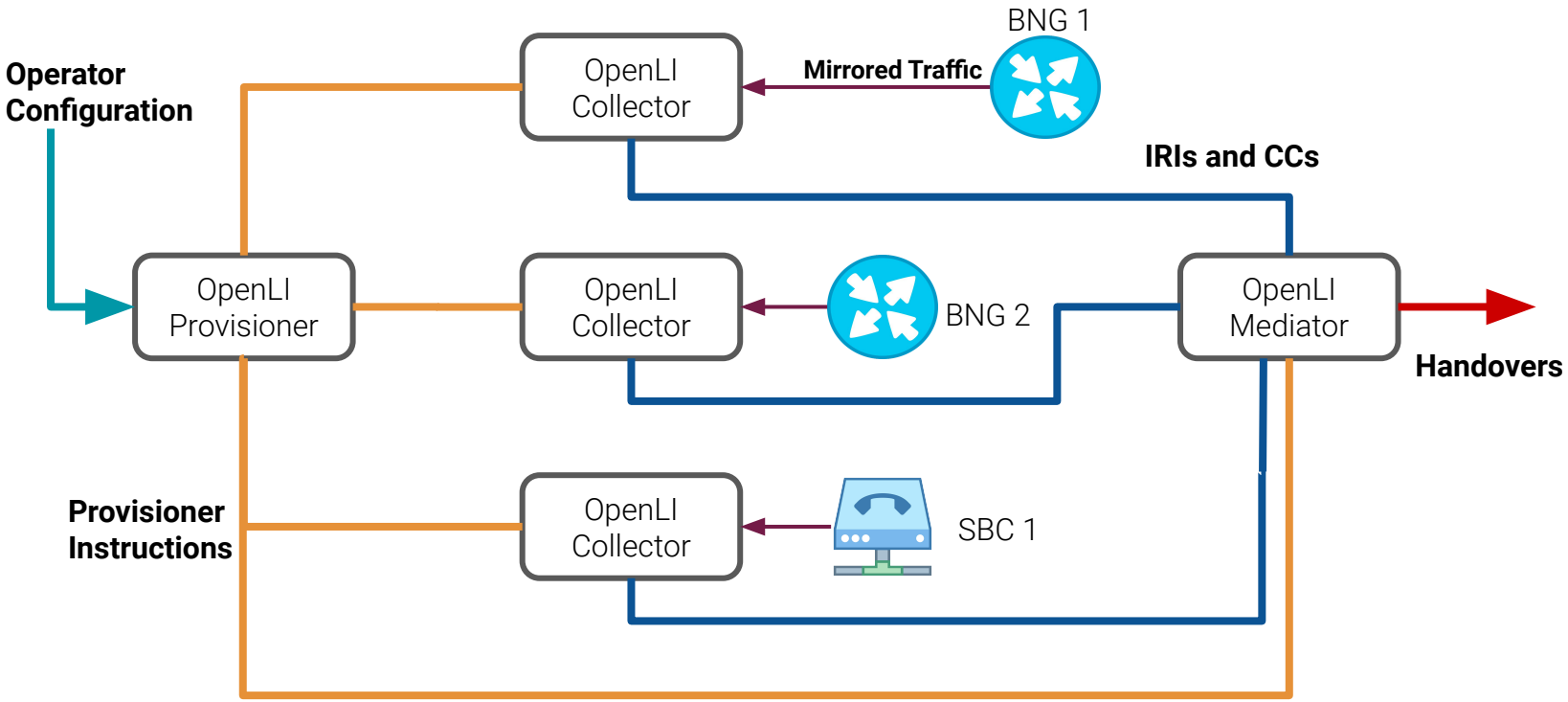
- Commercial LI solutions are super expensive …
  - But ETSI standards are public and used in many countries

- So why not write our own version and release it open source?
  - Give smaller operators an affordable option
  - Keep it simple, but be flexible where we can

OpenLI Components

- Provisioner – Centralised Manager
- Collector(s) – Distributed Workers
- Mediator – Output to LEAs

High Level Deployment Example



Compliance

- Compliant with ETSI standards for …
  - IP traffic intercepts
  - VoIP call intercepts
  - Mobile data intercepts (3G and 4G)

- Email interception is under development now

- Already deployed by a number of NZ ISPs
  - We know our software interoperates with our authorities

Cost

- Low cost
  - Software itself is free
  - Runs on commodity hardware under Linux
  - Software support at $10K USD per annum (max)

Trust

- Code is open source and auditable
  - No black boxes or hidden backdoors

Integration

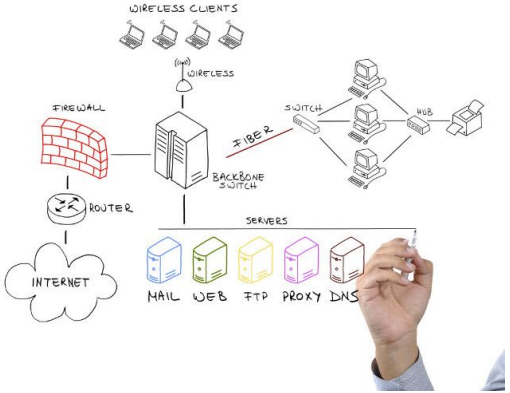
- OpenLI interoperates with (some) vendor LI mirroring features
  - Use your existing equipment to mirror customer traffic to OpenLI
    - Juniper JMirror
    - Nokia
    - TZSP (RouterOS)
    - Cisco might be coming soon…

Performance

- Multi-gigabit sustained interception per collector node
- Can use modern high-performance packet capture methods
  - DPDK, XDP

Flexibility

- Flexible deployment options
  - Separate software components for different roles
    - Provisioner, collectors, mediator
  - Configure intercepts via simple REST API
  - Distribute collector nodes throughout your network
  - Software can run inside VMs or containers



DIY Deployment

- Software is packaged for major Linux flavours
  - Debian, Ubuntu, Rocky, Alma, Fedora
- We provide documentation and a tutorial
  - Containerised training lab with practical exercises
- You figure out how to integrate into your network
  - User community is pretty friendly
  - Or hire someone like Dave

Back to Dave

OpenLI – ISP Implementations

Dave Mill - SearchLight Ltd

OpenLI - Legislation

- No defined technical standards for implementation in AU

- ETSI LI:
  - Nice to work with
  - Easy to test with
  - Agencies prefer it
  - Somewhat stateful/robust

- OpenLI: Supports both ETSI, and/or (rolling) PCAPs
- PCAPs coupled with an SFTP server could be an option

OpenLI - Modular

- Every ISP is different
- No standard deployment
- Can deploy the components, especially the OpenLI Collector(s), where it suits your network architecture

What makes up an intercept for an ISP

- CCs - Communication Contents
  IP Data / RTP

- IRIs - Intercept Related Information
  RADIUS / SIP

- Transporting the data to the LEA (Law Enforcement Agency)
  - Ideally ETSI over an internet-based VPN or private WAN
  - Previously pcaps on a firewalled ftp server, but phasing out

Required infrastructure

- Provisioner
  - Virtual
- Mediator
  - Virtual
  - Public IP for VPN … **OR**
  - Seperate Firewall … **OR**
  - Private WAN link
- Collector(s)
  - Likely one physical with DPDK friendly NIC
  - Virtual options / hybrid ideas on coming slides

Deploy a Provisioner

- Just need one
- Basic install as per wiki
- Generate TLS certs as per wiki
- Basic configuration
  - Enable TLS
  - Localhost LEA
  - PCAP LEA
- Start / Restart

Deploy a Mediator

- Might just need one. However, Australia is a bit larger than NZ…
- Basic install as per wiki
- Generate/distribute TLS certs as per wiki
- Basic configuration
  - Enable TLS
  - Pcap folder - useful for testing
- Start / Restart
- Install libtrace tools

Deploying a collector

- Do you need a physical collector with a 10G DPDK NIC?
  - How fast is your NBN typically?
  - Probably?
- Install DPDK as per wiki (optional)
- Install OpenLI-Collector as per wiki

- OpenLI : Modular and supports many collectors
- Many VM based solutions coming up

But, how do we make this work..?

- Know how to install Provisioner, Mediator and a Collector
- Can make them communicate via VRF/VLAN
- But how do I perform my intercept duties?

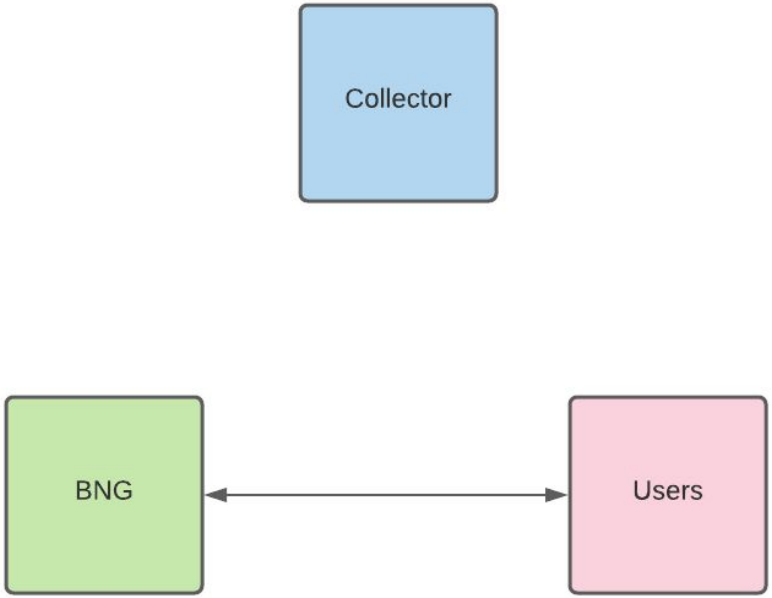
OpenLI – ISP deployment concepts

What makes up a data LI for an ISP

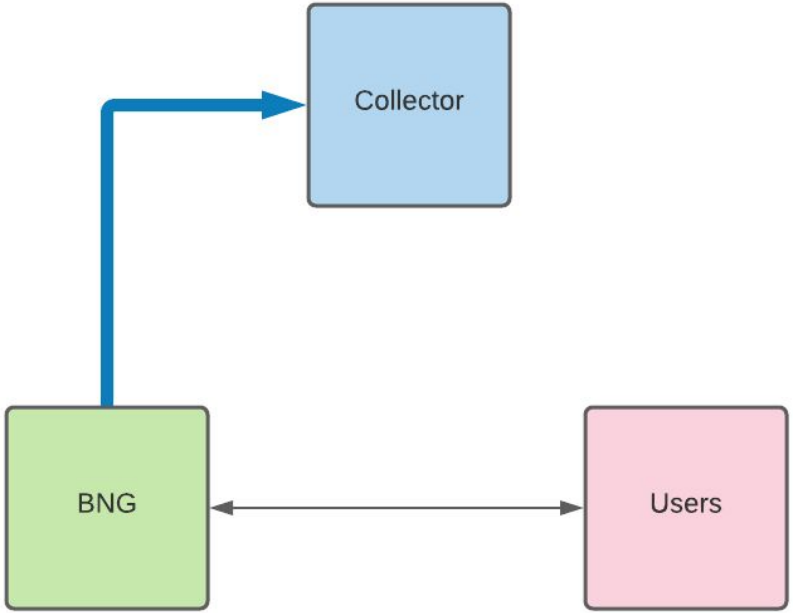
- CCs - Communication Contents
  IP Data

- IRIs - Intercept Related Information
  RADIUS

CCs - (simple) ISP with BNG



CCs - (simple) ISP with BNG



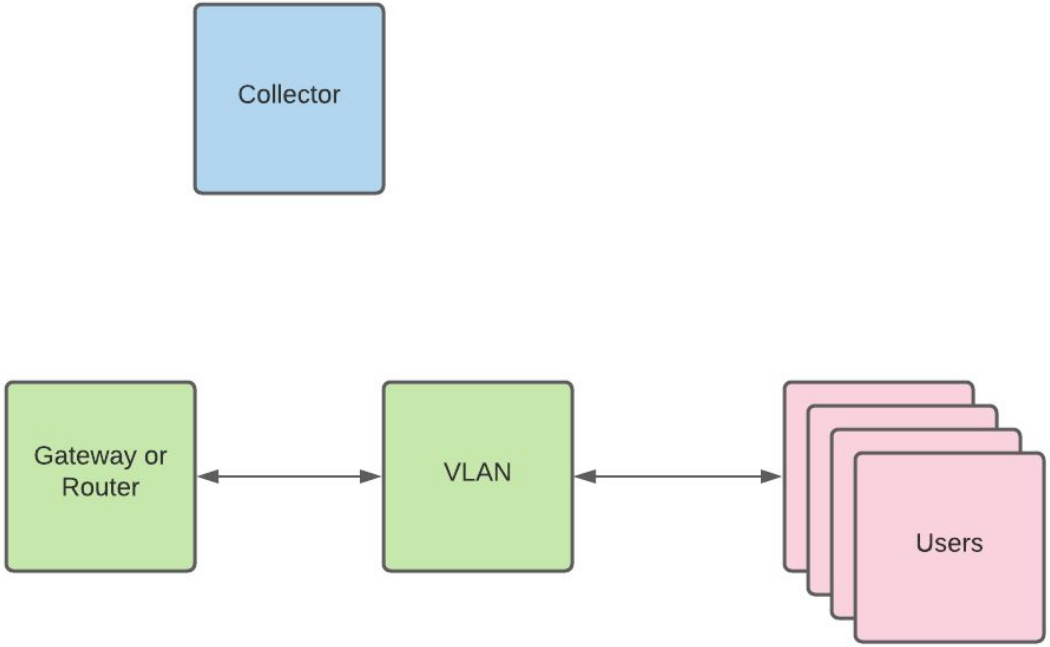
CCs - ISP with BNG

- Tap on BNG
  - Juniper: FlowtapLite feature and SSP License
    - Activated using RADIUS and uses CoAs for seamless on/off
  - Nokia: Config based - both written and not written
  - Cisco: CoA RADIUS or SNMP

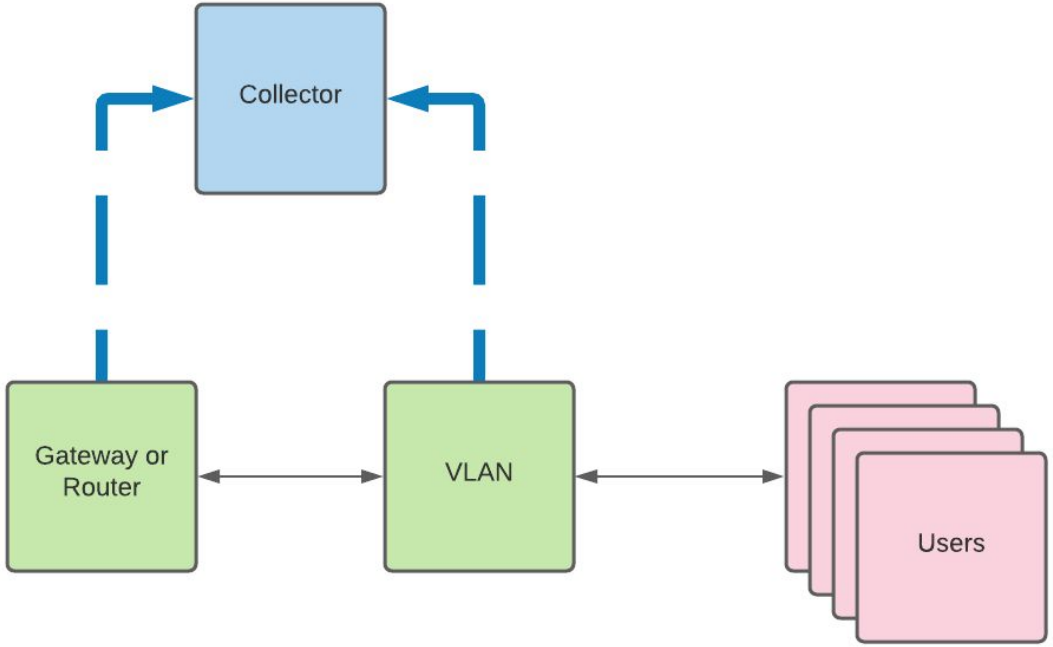
..AND..

- Provisioned on Provisioner. Either using intercept config, or REST API.

CCs - ISP with static IPs

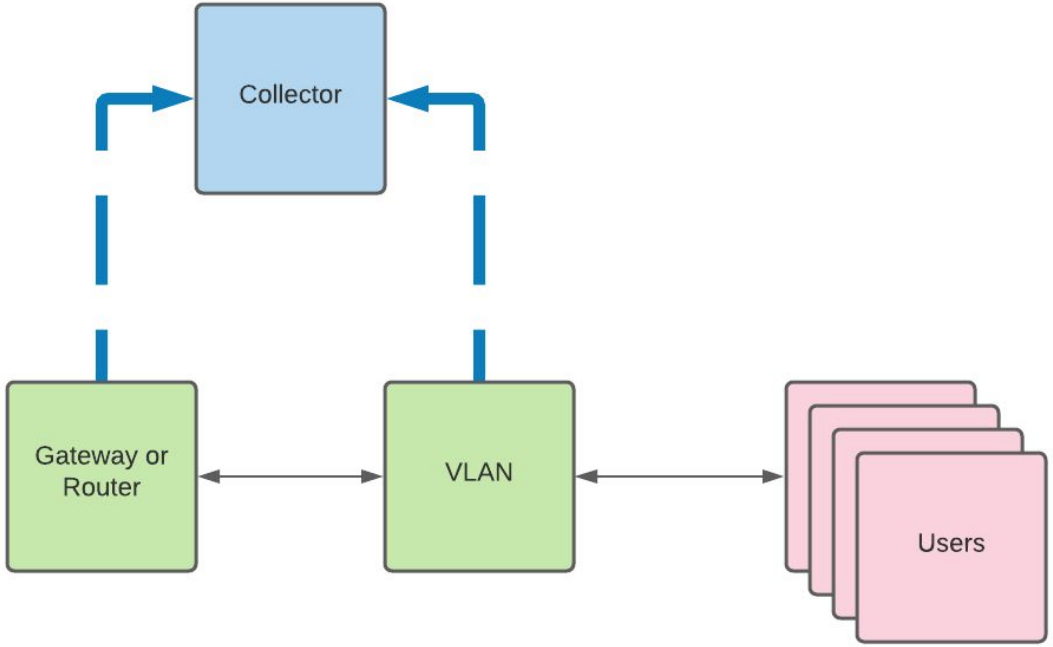


CCs - ISP with static IPs



CCs - ISP with static IPs

Mikrotik:
TZSP



CCs - ISP with Static IPs

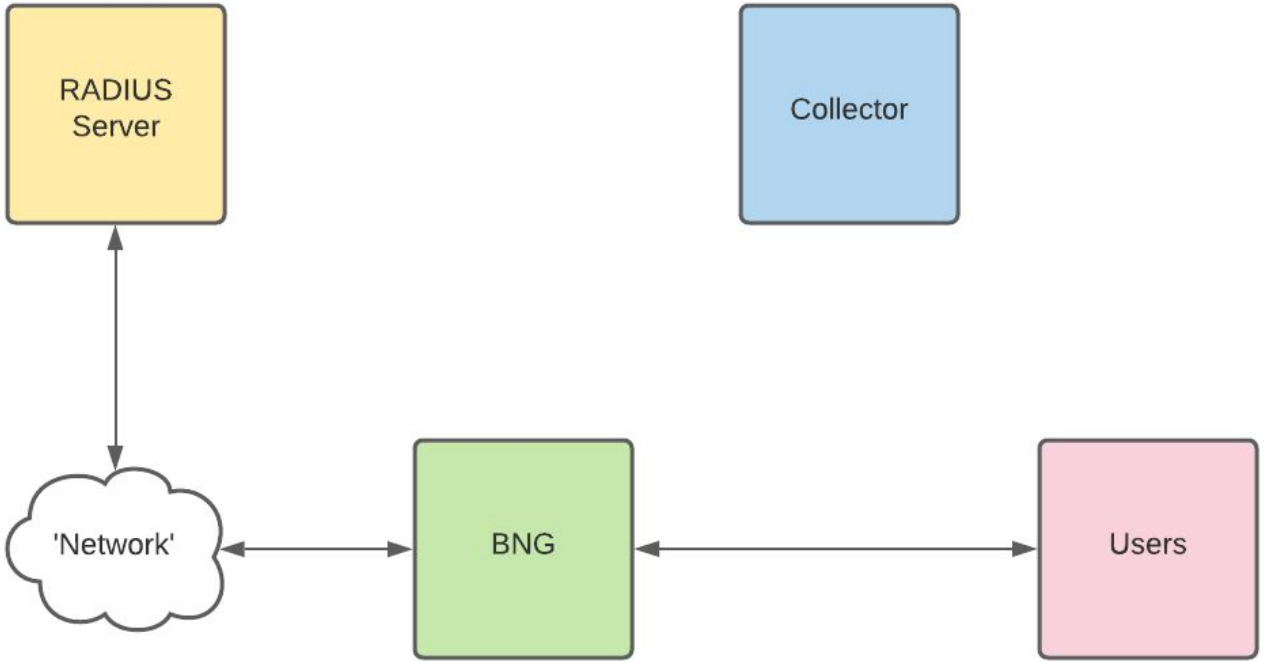
- Activated by:
  - Enabling tap on switch or router
  - Enabling intercept on Provisioner

What makes up an LI for an ISP

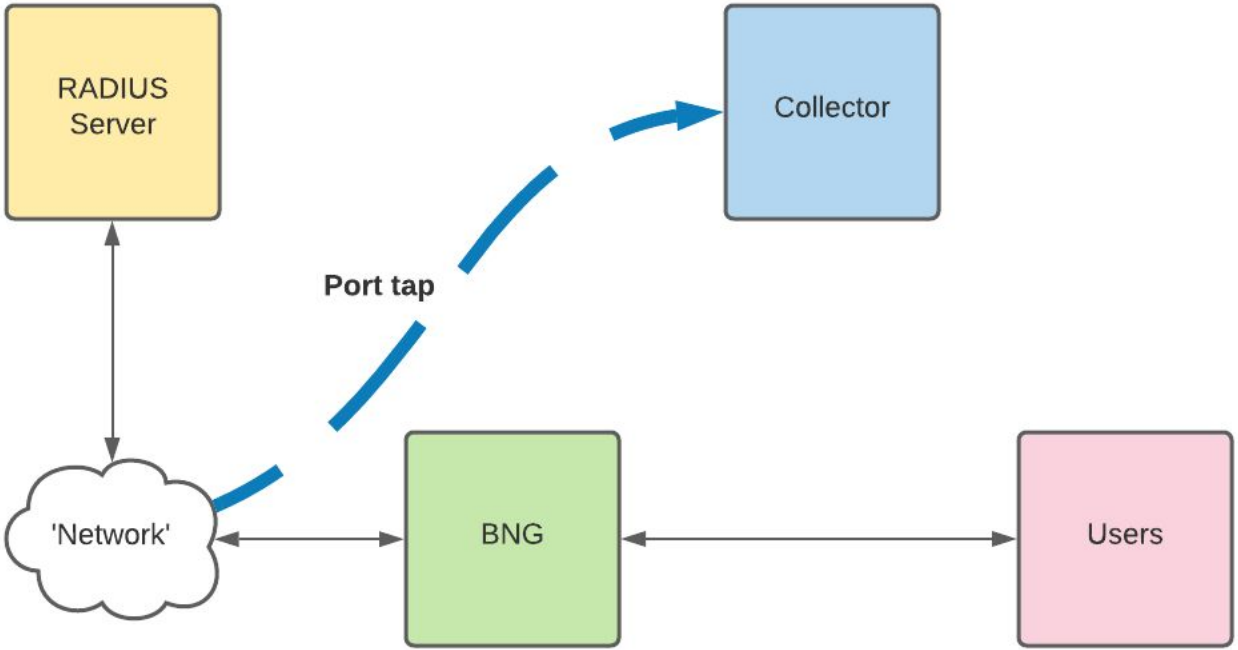
- CCs - Communication Contents
  IP Data

- **IRIs - Intercept Related Information**
  RADIUS

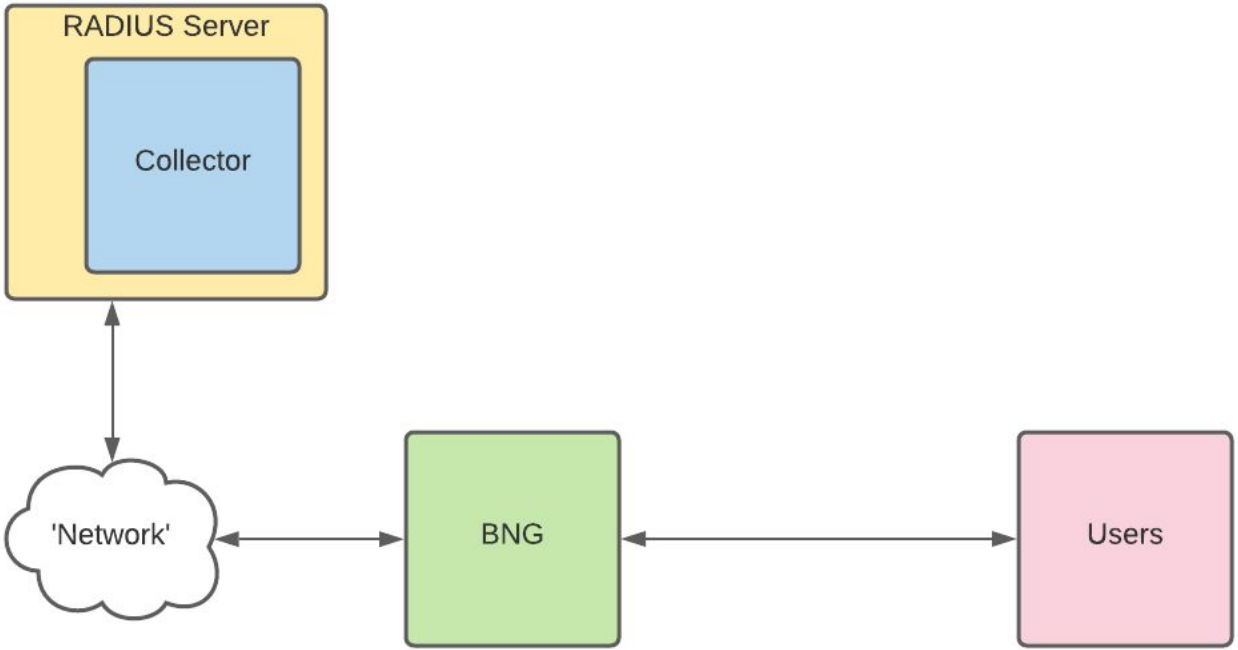
IRIs - ISP with BNG - RADIUS



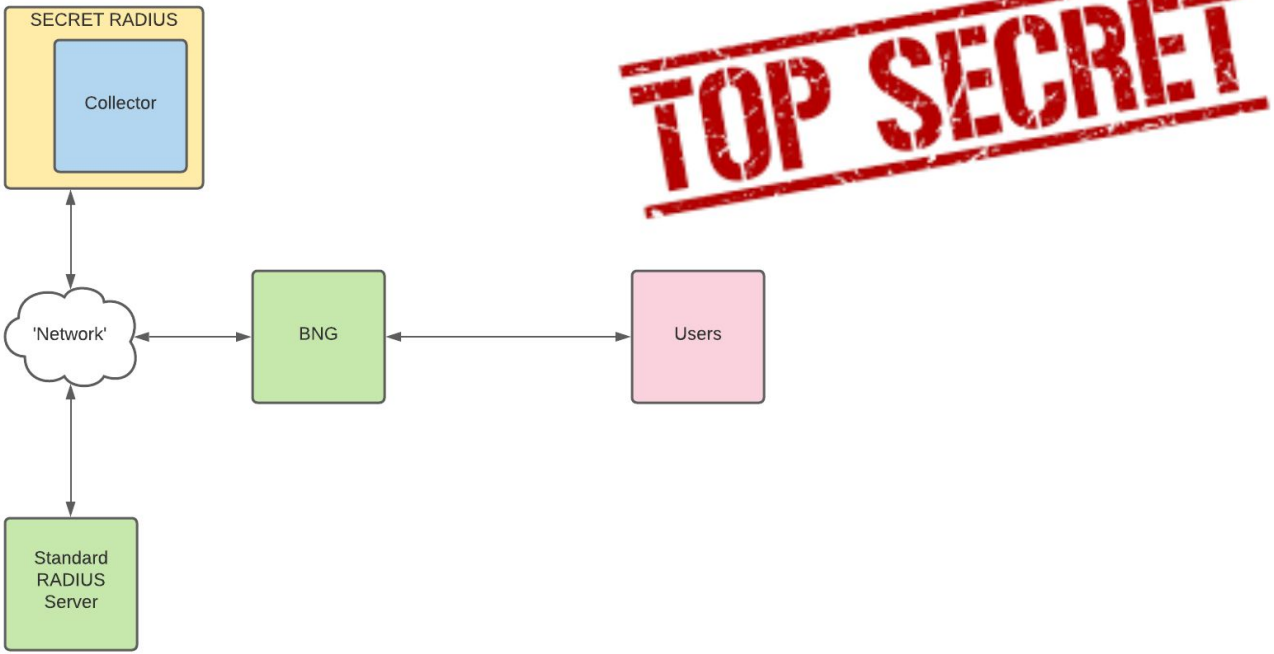
IRIs - ISP with BNG - RADIUS



IRIs - ISP with BNG - RADIUS



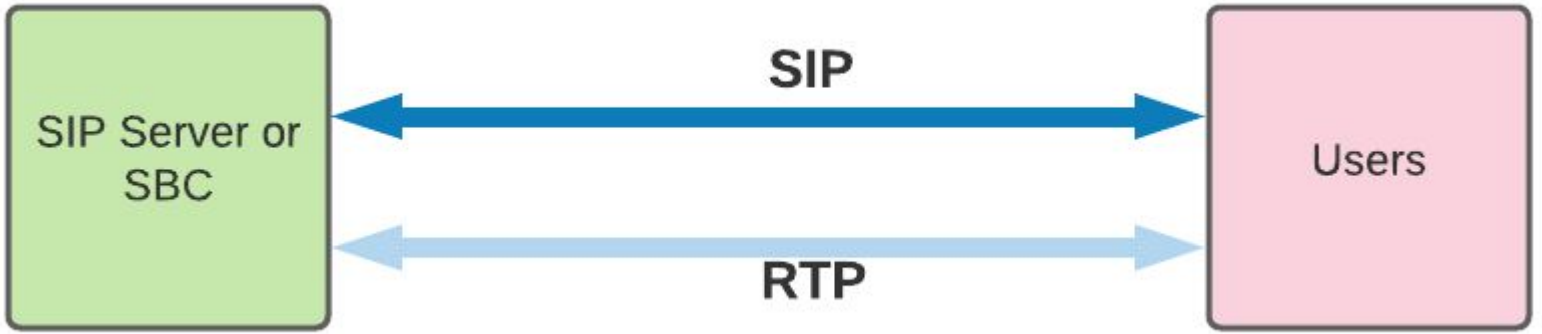
IRIs - ISP with BNG - RADIUS



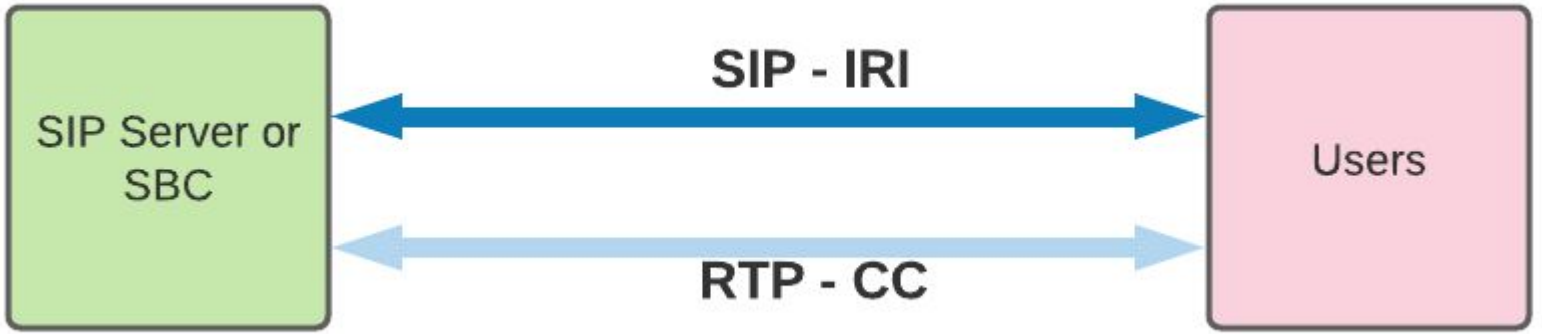
IRIs - ISP with BNG - RADIUS

- Many different ways to get RADIUS in to a collector
- Which way will depend on your current set-up and secrecy requirements
    - In Australia, what requirements are there to keep intercepts hidden?

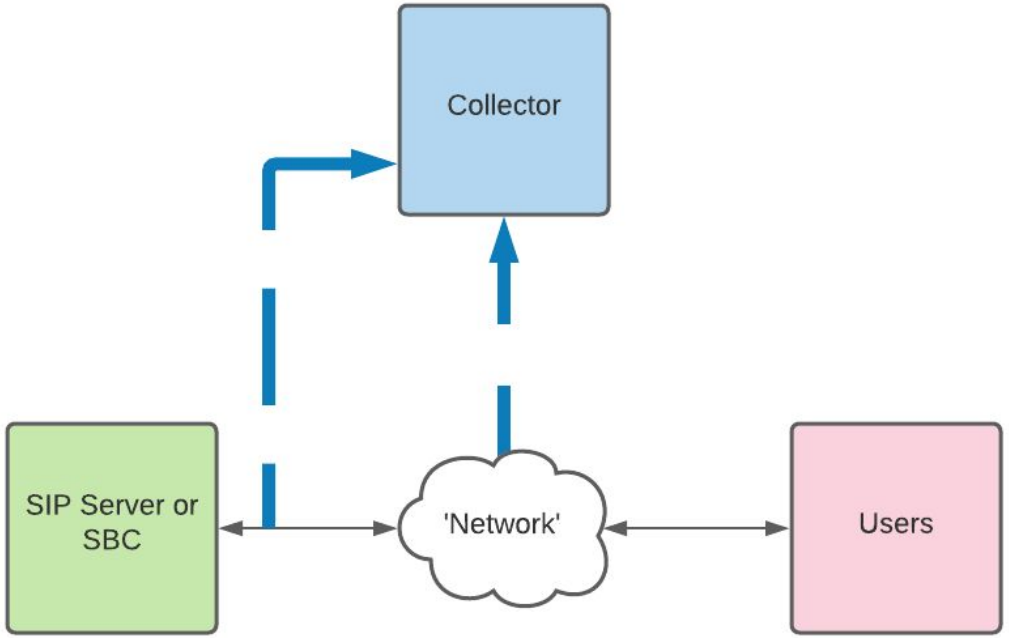
Voice



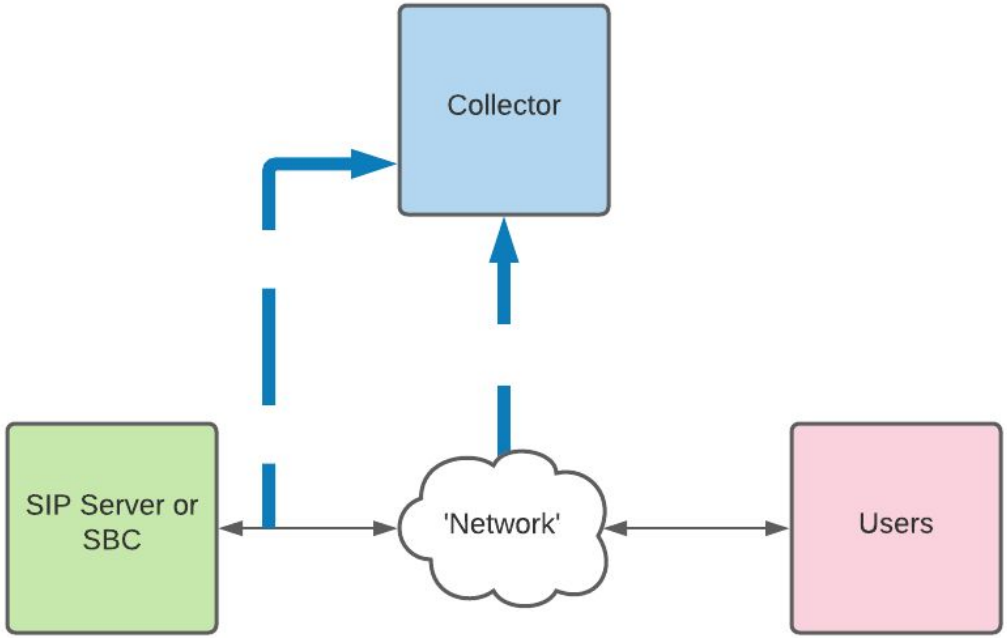
Voice



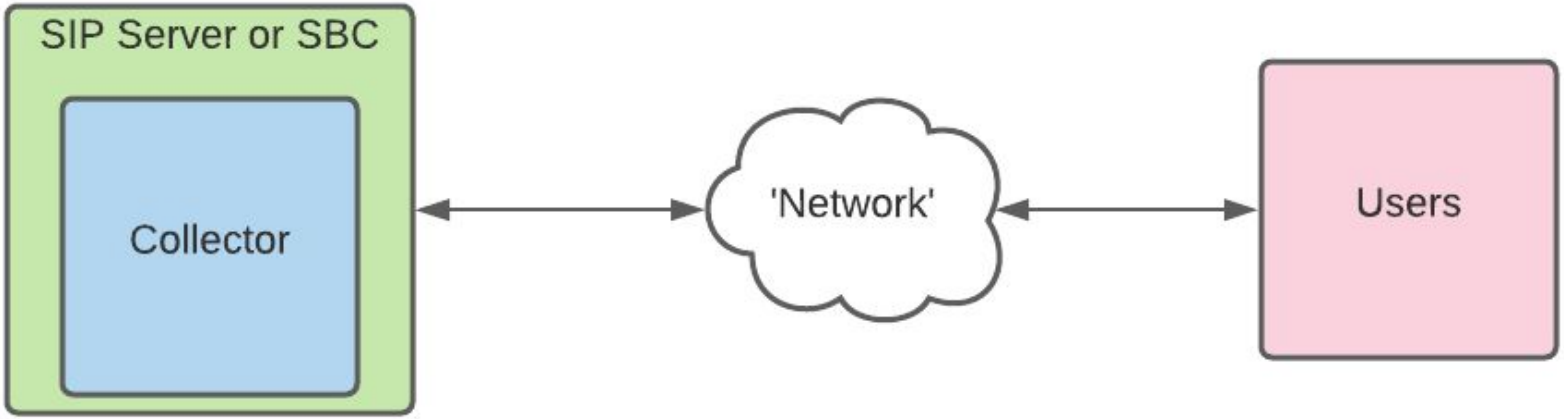
Voice



Voice - often Linux based SBCs…



Voice



Testing

- Very important!
- Don’t want to be served with an intercept you cannot execute

Inhouse testing

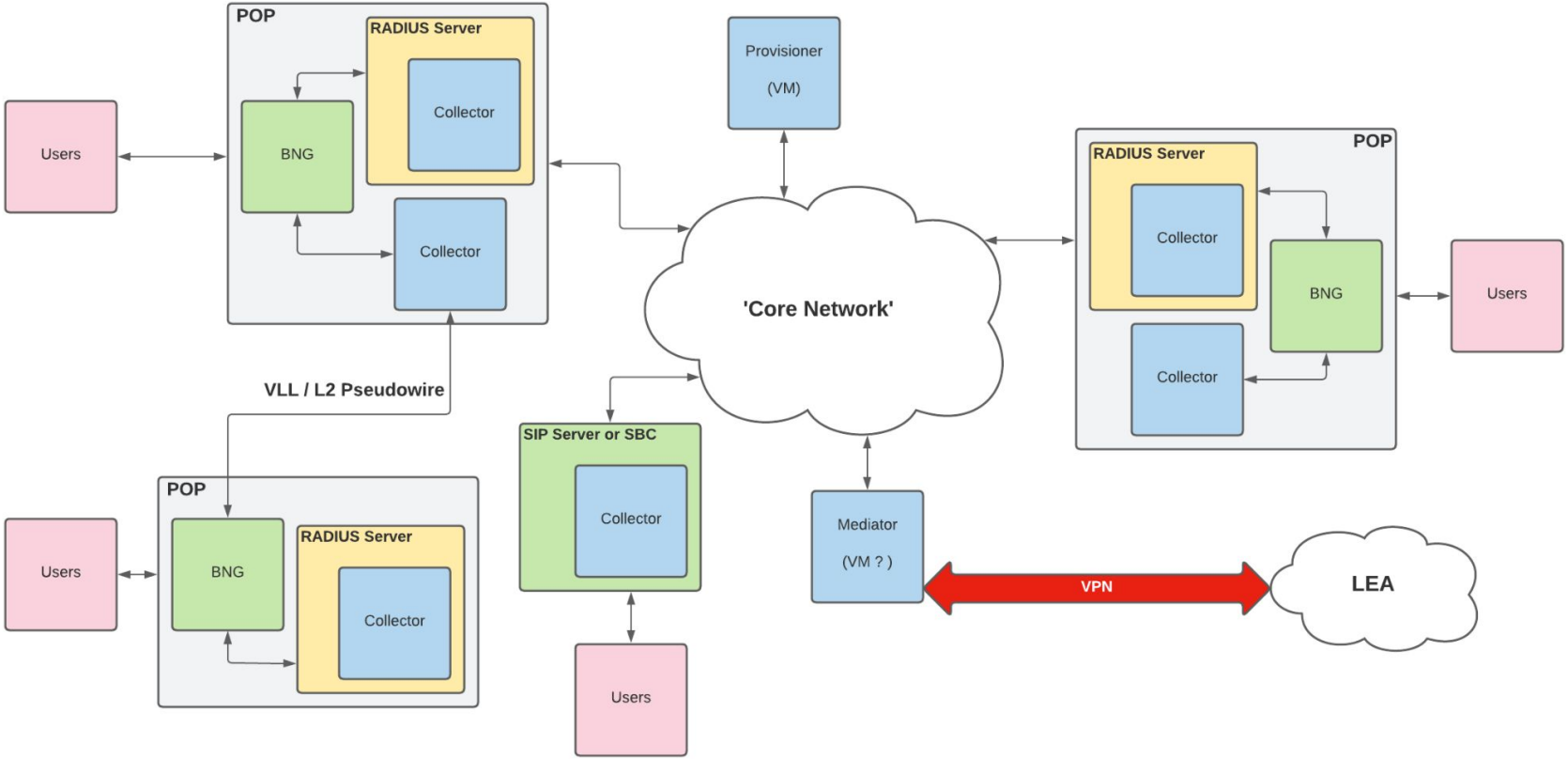
- Rolling pcaps on mediator

- Install libtrace tools on Mediator
- Set-up a test law-enforcement-agency on localhost/127.0.0.1
    - On Mediator:
    - tracepktdump etsilive:127.0.0.1:35530
    - tracepktdump etsilive:127.0.0.1:35531
      (or similar)

Law-Enforcement Agencies (LEAs)

- Australia:
  - ETSI LI over Private VPN
    - Adds complexities
    - Test to a remote host under your control first
  - PCAPs and SFTP server

- What agencies involved:
  - Federal Police
  - State Police?
  - Other agencies?



Back to Shane

The Future of OpenLI

- Sustainability is key
  - NZ University budgets are incredibly tight
  - Need to generate income to cover maintenance and support costs

Software Support Contracts

- Pay an annual fee to get priority assistance with bugs or requests
  - Not too onerous (ballpark is $10K US p/a, depending on network size)

- Combined, try to raise enough money to keep me around
  - On hand for immediate problems
  - Otherwise I use the time to improve and promote OpenLI further

Australia!

- We’re very keen to see if we can provide value to Australian ISPs
  - Especially the small-to-medium sized networks

- Very little public information about requirements for AU
  - We are building contacts and learning as we go

Final Word

- Talk to us!
  - We are willing and able to expand OpenLI to suit AU operator needs

- Talk to your colleagues!
  - Share knowledge, encourage transparency
  - Ask your NZ friends about OpenLI ;)

Question Time?

https://openli.nz

openli-support@waikato.ac.nz

salcock@waikato.ac.nz

dmill@searchlight.nz