THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

University of Waikato
Network Research Group

openLI

Integration with Vendor Mirroring

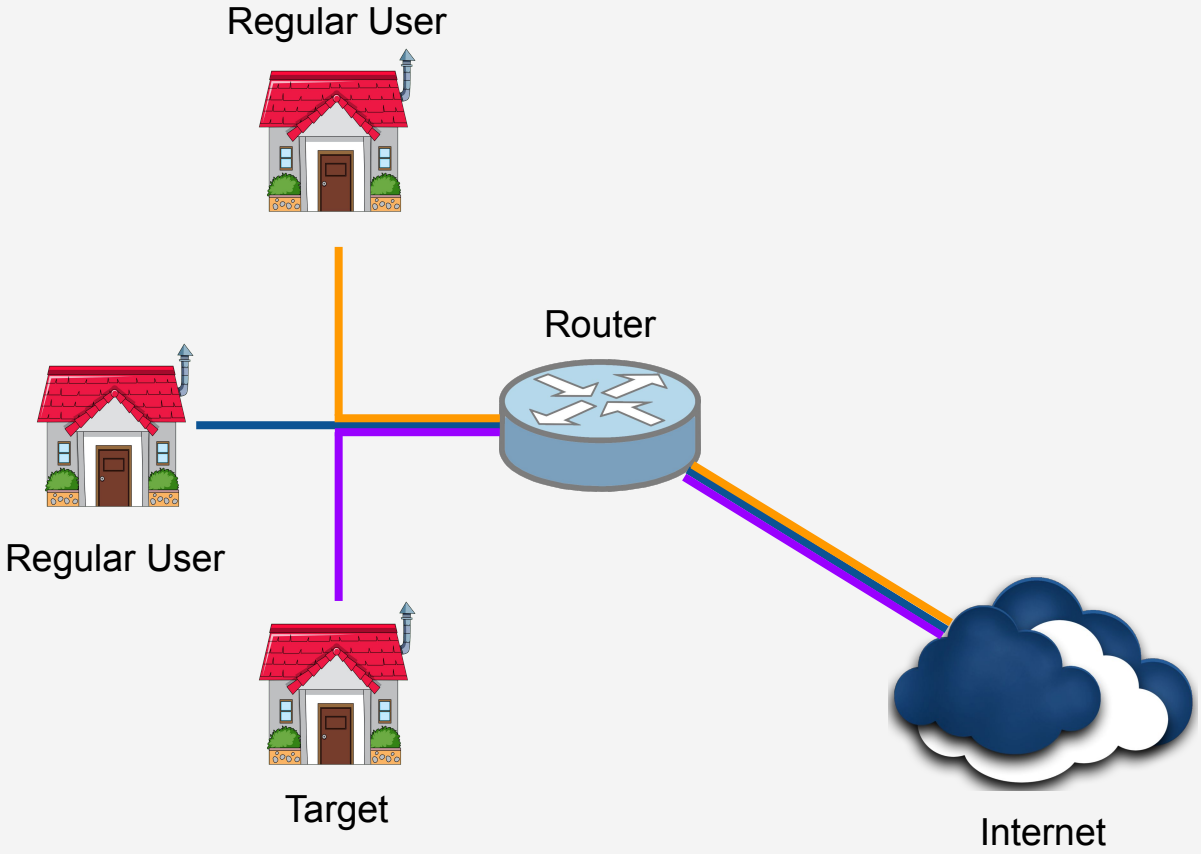
OpenLI Training: Chapter Seventeen

Shane Alcock
University of Waikato
New Zealand
shane.alcock@waikato.ac.nz

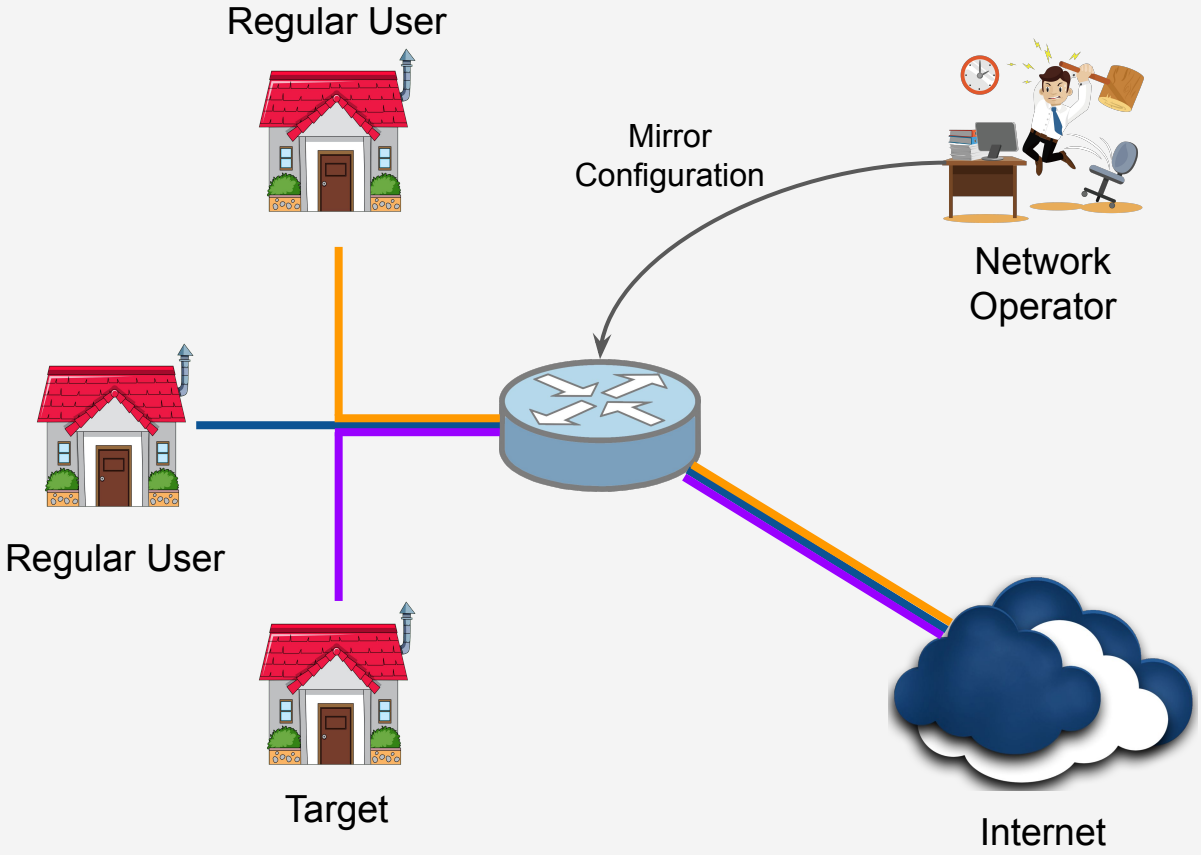
Vendor Mirroring

- Mirror individual subscriber traffic directly from routers
  - Often marketed as a “Lawful Intercept” feature

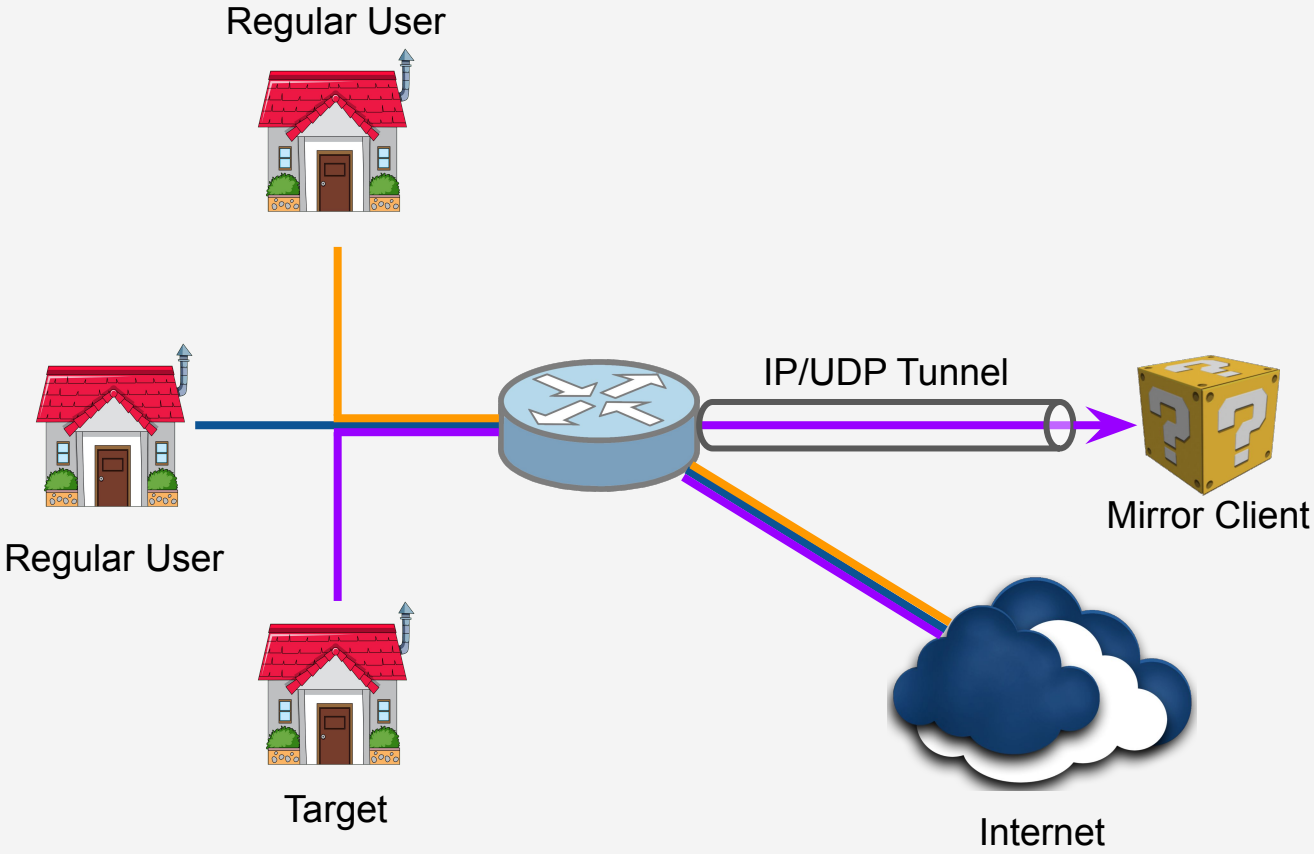
Vendor Mirroring



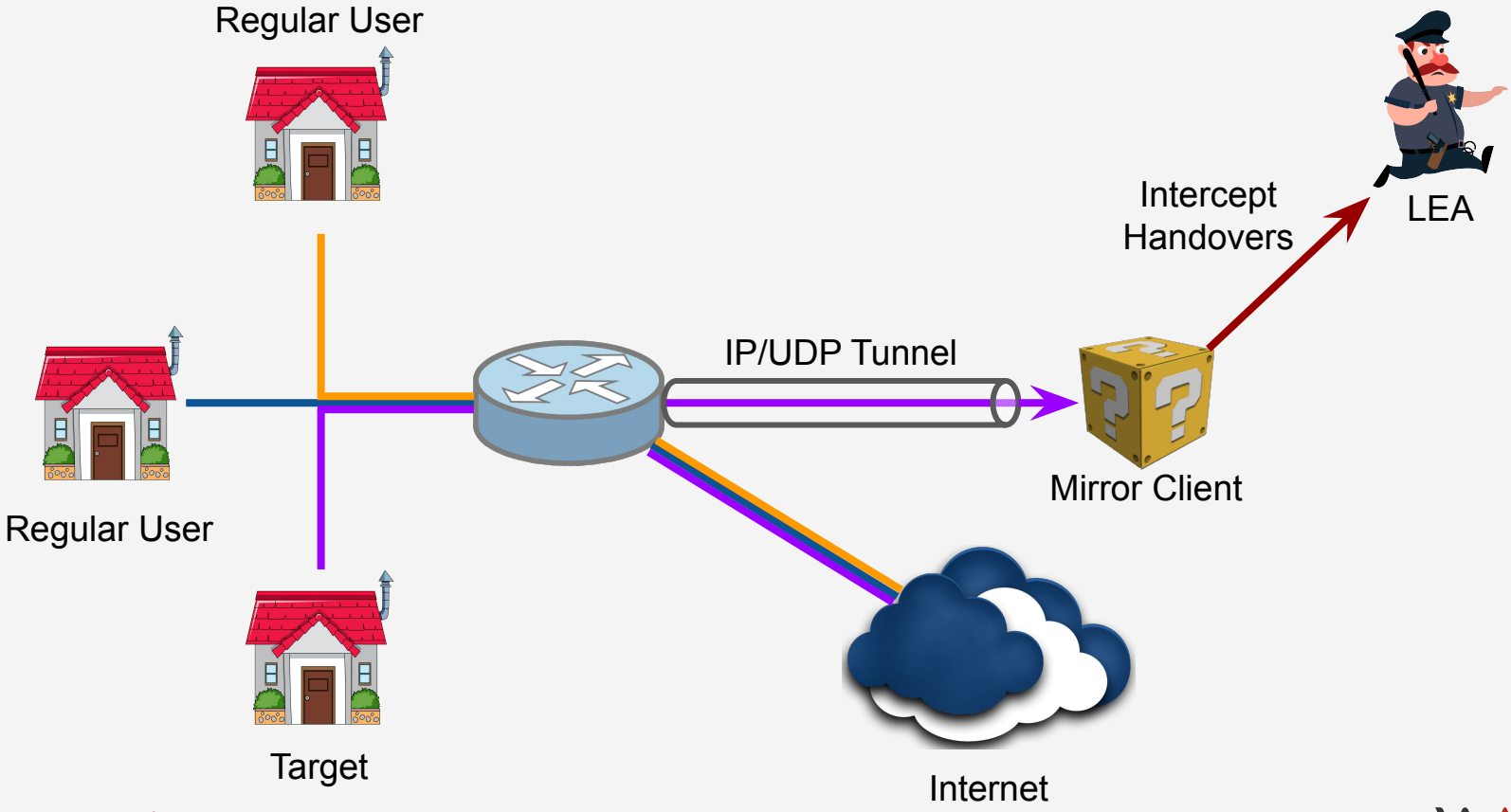
Vendor Mirroring



Vendor Mirroring



Vendor Mirroring



Vendor Mirroring

- The mirrored traffic is not ETSI-compliant!
  - Raw captured IP wrapped in a shim header
  - Missing key parameters
  - No IRIs
  - Will NOT satisfy LEAs who insist on ETSI standards
    - Need additional mediation device from the vendor

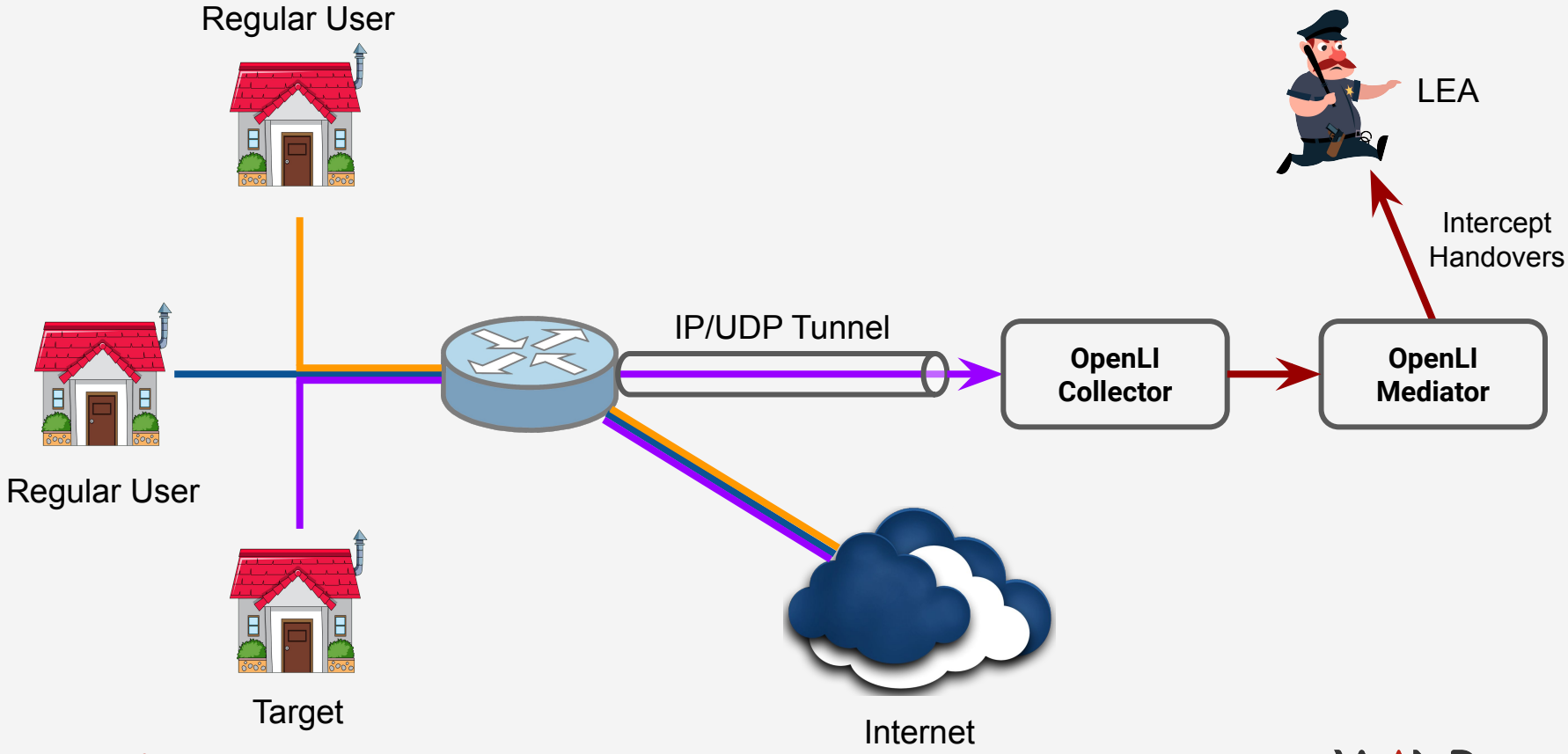
- But …
  - Ability to do per-subscriber mirroring in hardware is handy

Vendor Mirroring

- OpenLI collectors can parse some vendor mirror formats
  - Strip the shim headers, replace with valid ETSI headers
  - If corresponding AAA traffic is available, IRIs can be generated

- Currently support:
  - Juniper and Nokia mirroring
  - Other vendors could be added on request

Vendor Mirroring



Notifying Collectors

- Tell collectors which captured packets have been mirrored
  - Also need to know the vendor
    - Shims differ between vendors, of course
  - List vendor mirrors in collector's YAML configuration
    - Unfortunately, not supported by REST API (yet)

Notifying Collectors

- Configuring OpenLI to support a Juniper Packet Mirror
  - IP == destination IP from mirror configuration
  - Port == destination port from mirror configuration

```
# vim /etc/openli/collector-config.yaml
```

```
jmirrors:
    - "ip": "10.55.86.220"
      "port": "30742"
```

Notifying Collectors

- Configuring OpenLI to support a Nokia / Alcatel-Lucent Mirror
  - IP == destination IP from mirror configuration
  - Port == destination port from mirror configuration

```
# vim /etc/openli/collector-config.yaml
```

```
alumirrors:
    - "ip": "10.15.0.243"
      "port": "8500"
```

Notifying Collectors

- Restart the collector to apply the configuration changes

```
# stop_collector.sh

# service openli-collector restart
```

Vendor Mirror Intercept Scenario

- Juniper Packet Mirror
  - Destination IP == 10.55.86.220
  - Destination port == UDP 30742

- Intercept warrant details
  - User name (anonymised) is `2On5uRWxvQDeBBepKBu`
  - User is a wireless customer
  - Requested LIID is “`NZP_20211010`”

Preparing for Interception

- Ensure OpenLI collector config contains JMirror details
  - Don’t forget to restart if you change the collector config

```
jmirrors:
    - “ip”: “10.55.86.220”
      “port”: “30742”
```

Preparing for Interception

- Configure single-subscriber mirror on Juniper device
  - Based on user identity: `2On5uRWxvQDeBBepKBu`
  - Mirror to 10.55.86.220, port 30742 UDP
  - Choose an intercept ID
    - Must be a number, so we can't use the assigned LIID
    - For this exercise, we've chosen `500`

REST API for Vendor Mirror Intercepts

- Exactly the same API as other IP intercepts
  - One new JSON property

http://<PROVIP>:<RESTAPIPORT>/ipintercept

REST API for Vendor Mirror Intercepts

- The JSON object for our Mirrored IP intercept

```
{
    “liid”: “NZP_20211010”,
    “authcc”: “NZ”,
    “delivcc”: “NZ”,
    “mediator”: 1,
    “agencyid”: “mocklea”,
    “starttime”: 0,
    “endtime”: 0,
    “user”: “2On5uRWxvQDeBBepKBu”,
    “accesstype”: “wireless”,
    “vendmirrorid”: 500
}
```

REST API for Vendor Mirror Intercepts

- The JSON object for our Mirrored IP intercept
  - “vendmirrorid” is used for all vendor mirror types

```
{
    “liid”: “NZP_20211010”,
    “authcc”: “NZ”,
    “delivcc”: “NZ”,
    “mediator”: 1,
    “agencyid”: “mocklea”,
    “starttime”: 0,
    “endtime”: 0,
    “user”: “2On5uRWxvQDeBBepKBu”,
    “accesstype”: “wireless”,
    “vendmirrorid”: 500
}
```

REST API for Vendor Mirror Intercepts

- Using curl to add the intercept on the provisioner

```
curl -X POST -H "Content-Type: application/json"
  -d '{
        "liid": "NZP_20211010",
       "authcc": "NZ",
        "delivcc": "NZ",
        "mediator": 1,
        "agencyid": "mocklea",
        "starttime": 0,
        "endtime": 0,
        "user": "2On5uRWxvQDeBBepKBu",
        "accesstype": "wireless",
        "vendmirrorid": 500
    }'
  http://172.19.0.3:8080/ipintercept
```

REST API for Vendor Mirror Intercepts

- Checking the collector logs…
  - There'll also be the usual messages on the other components

```
openlicollector[166]: OpenLI: received IP intercept from provisioner for
Vendor Mirrored ID 500 (LIID NZP_20211010, authCC NZ, start time 0, end time
0), target is 2On5uRWxvQDeBBepKBu
```

Running a Vendor Mirror Intercept

- Collector has a pcap called jmirror.pcap
  - Contains tunneled JMirror traffic with intercept ID 500
  - Contains corresponding RADIUS for the customer IP session
    - This will allow OpenLI to generate IRIs
    - RADIUS server is at 172.24.66.17:18133
    - Remember to add the server via the REST API!

Running a Vendor Mirror Intercept

- Again, we use tracereplay to push the traffic into the collector

```
tracereplay -X 10 /home/openli-coll/pcaps/jmirror.pcap ring:eth2
```

HI2 for a Vendor Mirror Intercept

- IRIs are much like what we saw with the RADIUS intercept
  - Note the assigned IP address for when we look at HI3

```
...
 ETSILI:       communicationIdentityNumber: 659579
...
 ETSILI:            targetUsername: 2On5uRWxvQDeBBepKBu
 ETSILI:            internetAccessType: wirelessLAN
 ETSILI:            iPVersion: IPv4
 ETSILI:            targetIPAddress:
 ETSILI:              iP-type: IPv4
 ETSILI:              iP-value:
 ETSILI:                iPBinaryAddress: 25.84.33.120
 ETSILI:              iP-assignment: Dynamic
 ETSILI:              iPv4SubnetMask: 255.255.255.255
...
```

HI2 for a Vendor Mirror Intercept

- IRIs are much like what we saw with the RADIUS intercept
  - Note the assigned IP address for when we look at HI3

```
...
 ETSILI:       communicationIdentityNumber: 659579
...
 ETSILI:            targetUsername: 2On5uRWxvQDeBBepKBu
 ETSILI:            internetAccessType: wirelessLAN
 ETSILI:            iPVersion: IPv4
 ETSILI:            targetIPAddress:
 ETSILI:              iP-type: IPv4
 ETSILI:              iP-value:
 ETSILI:                iPBinaryAddress: 25.84.33.120
 ETSILI:              iP-assignment: Dynamic
 ETSILI:              iPv4SubnetMask: 255.255.255.255
...
```

HI2 for a Vendor Mirror Intercept

- IRIs are much like what we saw with the RADIUS intercept
  - Also note the communication identity number

```
...
 ETSILI:       communicationIdentityNumber: 659579
...
 ETSILI:            targetUsername: 2On5uRWxvQDeBBepKBu
 ETSILI:            internetAccessType: wirelessLAN
 ETSILI:            iPVersion: IPv4
 ETSILI:            targetIPAddress:
 ETSILI:              iP-type: IPv4
 ETSILI:              iP-value:
 ETSILI:                iPBinaryAddress: 25.84.33.120
 ETSILI:              iP-assignment: Dynamic
 ETSILI:              iPv4SubnetMask: 255.255.255.255
...
```

HI3 for a Vendor Mirror Intercept

- You should have no trouble parsing the HI3 by now

```
Mon Oct 25 22:09:27 2021
 Capture: Packet Length: 152/152 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: NZP_20211010
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 659579
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 191
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1635199767
 ETSILI:       microSeconds: 693474
 ETSILI:     timeStampQualifier: timeOfInterception
```

HI3 for a Vendor Mirror Intercept

- You should have no trouble parsing the HI3 by now

```
Mon Oct 25 22:09:27 2021
 Capture: Packet Length: 152/152 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: NZP_20211010
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 659579
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 191
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1635199767
 ETSILI:       microSeconds: 693474
 ETSILI:     timeStampQualifier: timeOfInterception
```

HI3 for a Vendor Mirror Intercept

- You should have no trouble parsing the HI3 by now

```
ETSILI:   Payload:
ETSILI:     cCPayloadSequence:
ETSILI:       CCPayload:
ETSILI:         payloadDirection: indeterminate
ETSILI:         cCContents:
ETSILI:           iPCC:
ETSILI:             iPCCObjId: .5.3.10.2
ETSILI:             iPCCContents:
ETSILI:               iPPackets: ...
IP: Header Len 20 Ver 4 DSCP 00 ECN 0 Total Length 36
IP: Id 22356 Fragoff 0
IP: TTL 64 Proto 1 Checksum 48730
IP: Source 25.84.33.120 Destination 34.220.5.62
ICMP: Type: 0 (ICMP Echo Reply) Sequence: 13915
ICMP: Checksum: 22199
```

Summary

- OpenLI can translate some vendor-specific intercepts
  - Requires a little extra configuration
  - Direct the vendor intercept into the OpenLI collector

- Supported vendors
  - Juniper, Alcatel/Nokia
  - Others may be possible, please talk to us!

Next Time

- Encrypting internal OpenLI communications