Application Note

Subscriber-Aware Visibility

Rethinking Operator Infrastructure Monitoring

Challenge

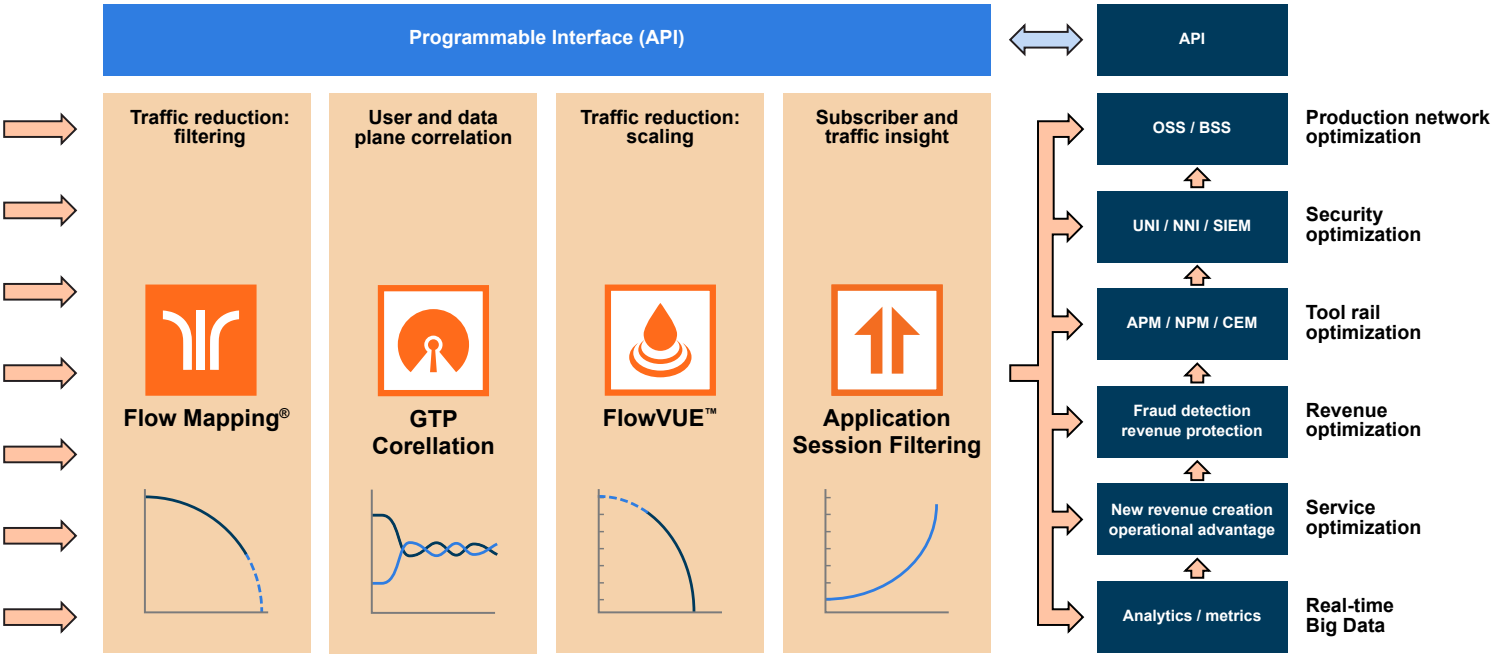
Mobile carriers are facing a deluge of traffic in their pipes from an increasingly mobile workforce and the proliferation of smart devices and applications. It started with the introduction of 4G/LTE networks and will accelerate with new 5G networks as well as IoT, virtual and augmented reality, and connected cars. At home, work, and all points in between, mobile subscribers are leading "always connected" digital lifestyles, and the growth of traffic levels is exploding. Managing and monitoring this influx of data on large bandwidth, high-speed networks is a real issue for service providers. In particular deploying and scaling the tools that are needed to process all the traffic on their networks. With ARPU (Average Revenue Per User) going down, and the need to drive down the subscriber cost proportionately, the traditional approach of scaling tools at the same rate as traffic grows does not work and does not meet the demands of network performance and customer experience.

The Gigamon Solution: Subscriber-Aware Visibility

At Gigamon® we understand the Service Provider challenge of meeting the demands of network performance and customer experience while dealing with exploding traffic levels. Gigamon's Visibility Fabric provides pervasive and continuous visibility across all network traffic enabling the rollout of new technologies, including IP Voice (VoLTE/VoWiFi), network virtualization and 100Gb transport links.

GigaSMART® technology extends the intelligence and value of the Gigamon Visibility Fabric.

For example, GTP correlation, a GigaSMART application, enables user and data plane correlation. After correlation, both the user and data plane traffic can be directly sent to the tools when the primary objective is offloading tools from the overhead of GTP correlation.
But Gigamon's solution goes much further than just tool optimization: it is one of the core building blocks for operators looking to build a best-in-class, modern, subscriber-aware visibility platform as shown in the figure below.



Gigamon's solution for a best-in-class, modern, subscriber-aware visibility platform

By combining GTP correlation with other traffic intelligence capabilities (like Flow Mapping®, FlowVUE® and Application Session Filtering) in the Unified Visibility Fabric, operators can gain deep insights into their networks and both:

- optimize their per-subscriber monitoring cost
- and offer new services that increase the Average Revenue Per User (ARPU).

This is done with tiered monitoring strategies that separate higher-ARPU subscribers from lower-ARPU subscribers.

Such an architecture enables operators to scale their traffic to meet their tools processing throughput. Whitelisting allows all traffic from specific IMSIs to be sent to the tools whereas sampling selects a configurable set of user sessions for analysis. Both whitelisting and sampling are part of the FlowVUE application in the GigaSMART suite of traffic intelligence applications offered by Gigamon for mobile operators. These capabilities can be used by operators in a variety of ways to implement highly scalable and efficient monitoring methodologies. Some examples are:

- Filter or eliminate entire application sessions corresponding to voluminous Over-The-Top (OTT) traffic such as YouTube, NetFlix and other video sites from reaching the tools, eliminating expensive unnecessary upgrades to the tooling infrastructure
- Decrypt SSL traffic destined to servers hosted by the operator and feed them to a security tool for malware inspection
- Send only a sample of non-premium sessions to the monitoring tools for analysis
- Sample a set of sessions to analyze the quality of service at a particular cell site
- Support the use of the APN attribute as a criteria for FlowVUE and GTP Whitelist features allowing traffic to be routed to different tools or discarded based on the type of network connection the device has requested.

Useful (and often critical) Subscriber-Aware Visibility use cases include:

1. Enabling Stateful GTP Correlation
2. Identifying High-Value and/or Roaming Subscribers Based on IMSIs
3. IMSI-based Load Balancing Across a Group of Monitoring Tools
4. Identifying Traffic from GTP Versions
5. Identifying Traffic from GTP Logical Interfaces
6. Implementing GTP Correlated FlowVUE Subscriber Sampling Traffic to Tools
7. Implementing GTP Correlated IMSI Whitelist along with GTP Correlated FlowVUE Subscriber Sampling Traffic to Tools
8. Implementing GTP Correlated IMSI Whitelist and GTP Correlated FlowVUE Subscriber Sampling Traffic to Tools along with APN Whitelist and APN Scaling
9. Implementing GTP Correlated IMSI Whitelist and GTP Correlated FlowVUE Subscriber Traffic Scaling to Tools using QCI
10. Implementing GTP Correlated FlowVUE Subscriber Sampling IMS Traffic to Tools with dedicated pools for each Tool
11. GTP Tunnel ID-Based Filtering
12. Distributing Traffic Based on Inner IP Addresses and Inner TCP Port Values

Use Case One: Enabling Stateful GTP Correlation

GPRS Tunneling Protocol (GTP) is commonly used to carry mobile data across service provider networks and includes control plane (GTP-c) and user-data plane (GTP-u) traffic. Therefore, visibility into a subscriber's activity requires the ability to understand the stateful nature of GTP (v1 and/or v2) and to correlate subscriber-specific control and data sessions to gain an accurate view of the subscriber's session. Using Gigamon's GTP correlation application carriers can gain access to the subscriber's data in these GTP tunnels by reliably correlating and passing all of the identified subscriber's control and data sessions to the analytics/monitoring probes and billing subsystems to ensure an accurate view of the monitored session. To help achieve this goal, Gigamon® Visibility Fabric™ nodes correlate the subscriber-IDs exchanged as part of the control sessions to the corresponding tunnel endpoint identifiers (TEID) that are part of the user-data plane traffic (see Figure 1).

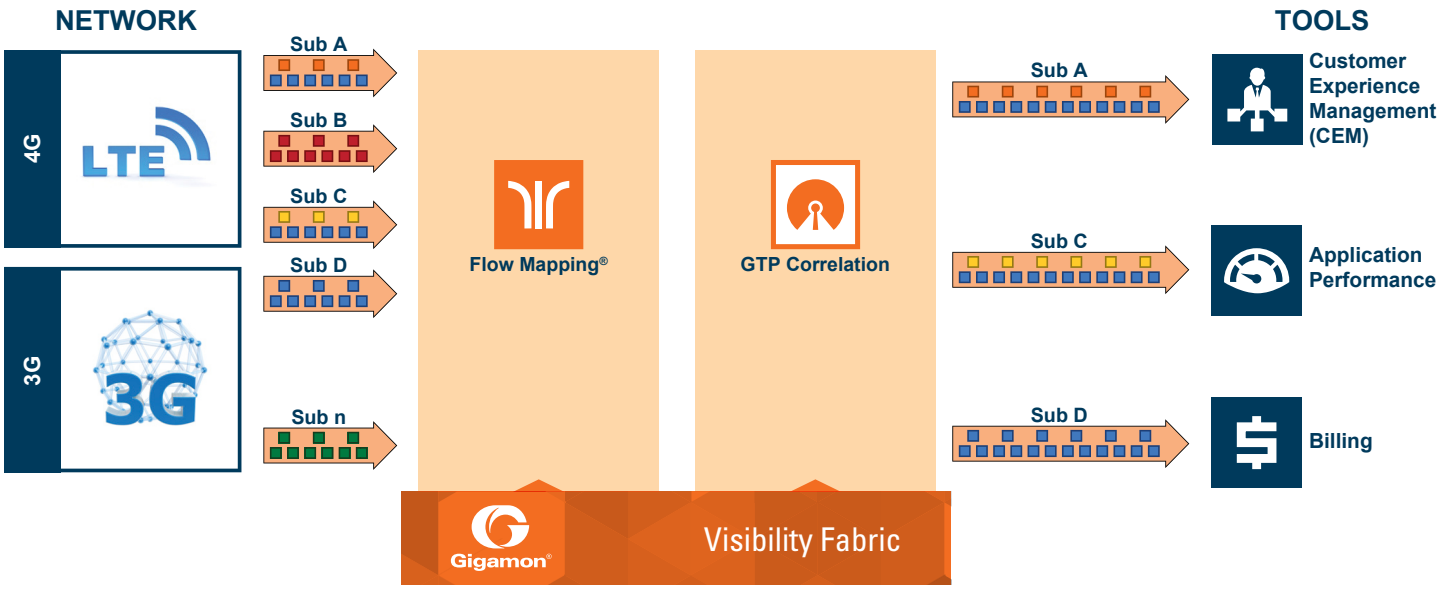


Figure 1: GTP correlation in a 3G/LTE network

With GTP correlation enabled, operators have multiple options to act on the subscriber generated GTP sessions including the flexibility to (among other things):

- Identify high-value subscribers based on an International Mobile Subscriber Identity (IMSI) or a group of IMSIs and forward the applicable traffic to the operator's monitoring/analytics/customer experience management tools, thus limiting the amount of traffic to those tools
- Classify traffic from roaming subscribers based on the IMSI prefix and forward to billing subsystems and/or monitoring tools to apply specific QoE/QoS policies
- Implement an infrastructure for load-balancing across a group of monitoring tools leveraging statically configured IMSI-based rules
- Classify GTPv1 from GTPv2 traffic and redirect the respective traffic streams to the appropriate analytics and/or monitoring tools
- Combine the processing capability of multiple GTP correlation engines to meet the scale needs in a large mobile operator. This capability allows the operator to use a scale-out architecture without being constrained by the capacity of a single GTP correlation engine
- Enable 100% of GTP-c traffic to be sent to the tools while sending only a configurable sample of the more voluminous GTP-u traffic to the tools
- Route traffic to tools based on requested network connection (APN), e.g. IMS for VoLTE

Use Case Two: Identifying High-Value and/or Roaming Subscribers Based on IMSIs

GTP correlation can be used for identifying a subscriber or a group of subscribers based on their IMSI. The IMSI is used to identify the user of a cellular network, is a unique identification associated with all cellular networks, and is typically exchanged as part of the GTP control sessions. GTP correlation keeps track of the IMSIs that a carrier is interested in monitoring and correlates these to the corresponding data/user-plane sessions for the subscriber and/or group of subscribers. Figure 2 shows an example of how filter rules are configured to select all the traffic related to subscribers identified by a particular IMSI prefix and forward it to a monitoring tool.

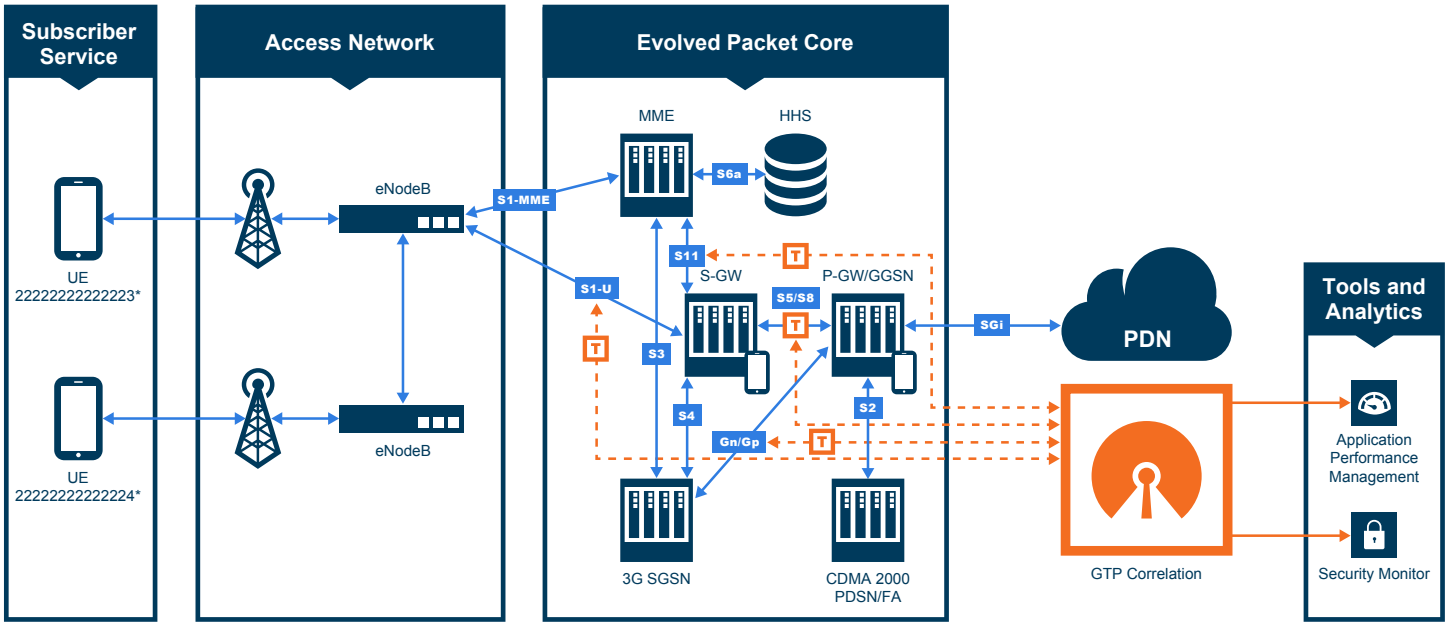


Figure 2: An example of how filter rules are configured to select all the traffic related to subscribers identified by a particular IMSI prefix and forward it to a monitoring tool

- Forward all traffic specific to the filtered IMSIs 22222222222223* including GTP-c and GTP-u to the tool

```
# Configure ports
port 1/1/x3 type network
port 1/1/x4 type tool

# configure gsgroups gsops to enable GTP correlation
gsgroup alias gsg1 port-list 1/1/e1
gsop alias gtp_sf flow-ops flow-filtering gtp port-list gsg1

## Configure vport on same gsgroup
vport alias vp1 gsgroup gsg1

### Filter out GTP packets to vport using the map below:
map alias to_vp
  to vp1
  from 1/1/x3
  rule add pass portsrc 2123
  rule add pass portsrc 2152
  exit

## Add IMSIs that you want to forward to tool:
map alias IMSI-list1
  use gsop gtp_sf
  to 1/1/x4
  from vp1
  flowrule add pass gtp imsi 22222222222223*
  exit
```

Use Case Three: IMSI-based Load Balancing Across a Group of Monitoring Tools

If a single instance of the monitoring tool cannot keep up with the traffic volumes it receives using IMSI-based rules, these incoming traffic streams can instead be distributed across a group of tools while ensuring that a particular subscriber's traffic always ends up on the same tool thus maintaining the integrity of the flows.

Figure 3 illustrates this traffic being distributed across two monitoring tools. In fact, traffic can be distributed to up to 16 tools. Operators also have the option to forward any traffic that does not match the configured filter rules to a tool port—otherwise called the collector.

- Forward all GTP-c and GTP-u traffic using IMSI-based hashing to tools T1 and T2
- Send the rest of the traffic to a shared collector

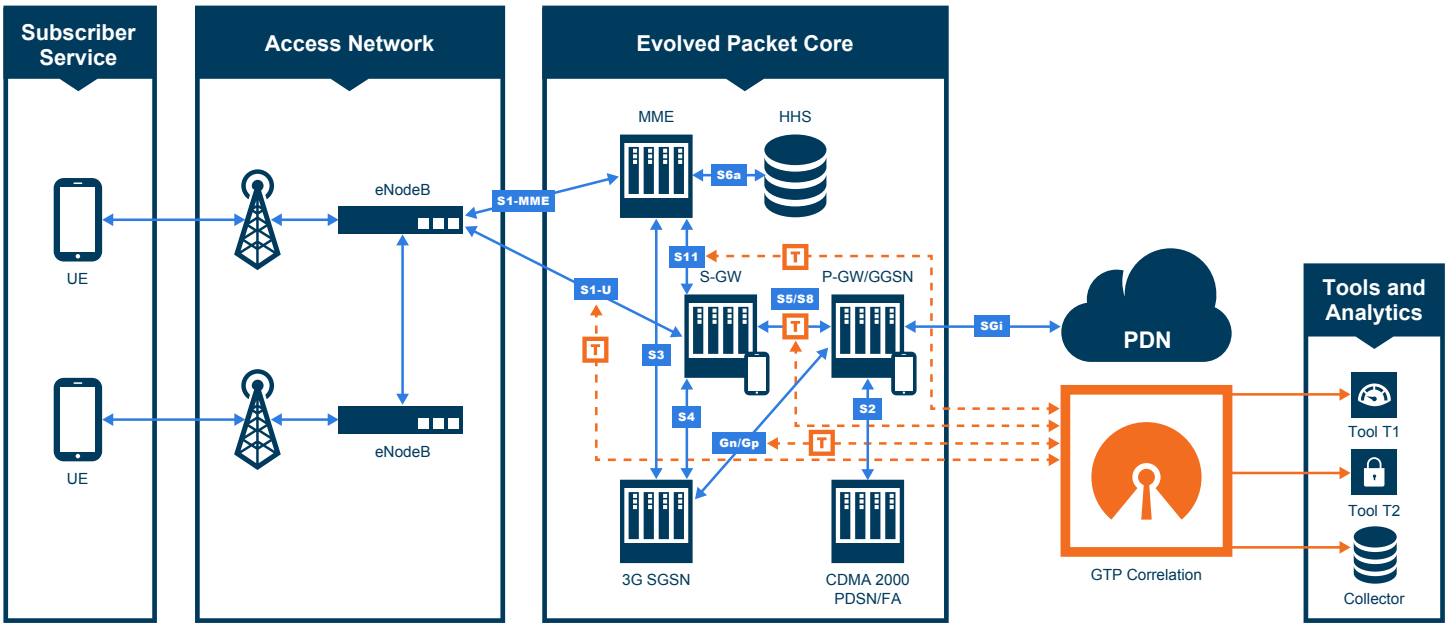


Figure 3: Illustration of traffic being distributed across two monitoring tools – forwarding GTP-c and GTP-u traffic using IMSI-based hashing to tools T1 and T2

```
# Configure ports
port 1/1/x3 type network
port 1/1/x4 type tool
port 1/1/x1 type tool
port 1/1/x2 type tool

port-group alias PG_IMSI_LB
  port-list 1/1/x1..x2
  smart-lb enable
  exit

# configure gsgroups, gsops to enable GTP correlation
gsgroup alias gsg1 port-list 1/1/e1
gsop alias gtp_sf flow-ops flow-filtering gtp lb app gtp metric hashing key imsi port-list gsg1

## Configure vport on same gsgroup
vport alias vp1 gsgroup gsg1
```

```
### Filter out GTP packets to vport using the map below:
map alias to_vp
  to vp1
  from 1/1/x3
  rule add pass portsrc 2123
  rule add pass portsrc 2152
  exit
map alias IMSI-LB
  use gsop gtp_sf
  to PG_IMSI_LB
  from vp1
  flowrule add pass gtp imsi *
  exit
map-scollector alias scoll
  from vp1
  collector 1/1/x2
exit
```

Use Case Four: Identifying Traffic from GTP Versions

As part of GTP correlation, Gigamon Visibility Fabric nodes also provide the flexibility to identify GTPv1 and GTPv2 messages. In an LTE network, LTE sessions on the S1U/S11, S2, S3/S4 and S5/S8 interfaces are maintained using GTPv2 Control plane signaling while legacy 3G sessions on the Gn/Gp interfaces are maintained using GTPv1 Control plane signaling. Utilizing the GTP Version filter allows traffic from 3G networks to be forwarded to 3G focused tools while directing LTE traffic to LTE specific tools. By correlating the control and user-plane sessions, Visibility Fabric nodes can identify, filter, and forward all sessions specific to a GTPv1 or GTPv2 to one or more monitoring/analytic tools. Figure 4 that follows shows the distribution of traffic based on GTP versions.

Distributing traffic based on GTP versions

- Filter and forward GTPv1 to tool T1
- Filter and forward GTPv2 to tool T2

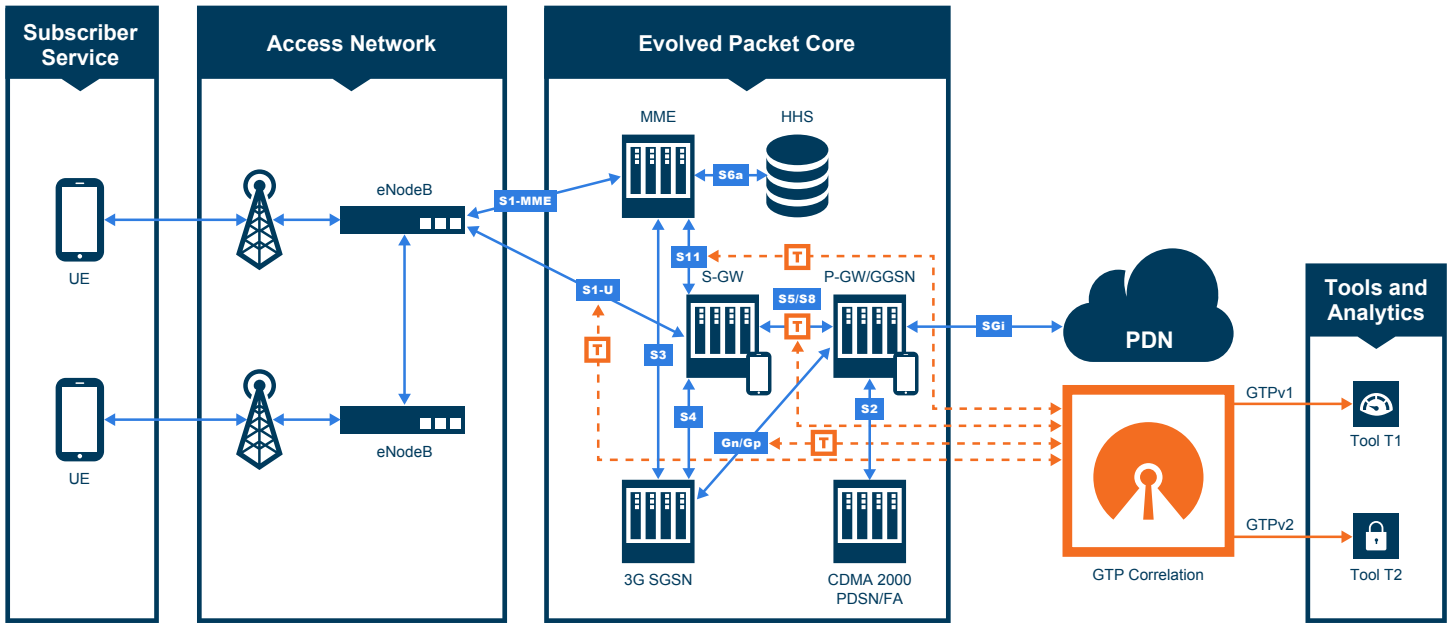


Figure 4: Distribution of traffic based on GTP versions

```
# Configure ports
port 1/1/x3 type network
port 1/1/x4 type tool
port 1/1/x1 type tool

# configure gsgroups, gsops to enable GTP correlation
gsgroup alias gsg1 port-list 1/1/e1
gsop alias gtp_sf flow-ops flow-filtering gtp port-list gsg1

## Configure vport on same gsgroup
vport alias vp1 gsgroup gsg1

### Filter out GTP packets to vport using the map below:
map alias to_vp
  to vp1
  from 1/1/x3
  rule add pass portsrc 2123
  rule add pass portsrc 2152
  exit

## Add GTPv1 Map to select sessions that are 3G Gn/Gp to send to tool on x4:
map alias GTPv1
  use gsop gtp_sf
  to 1/1/x4
  from vp1
  flowrule add pass gtp ver 1
  exit

## Add GTPv2 Map to select sessions that are LTE (S1U/S11, S5/S8) to send to tool on x1:
map alias GTPv2
  use gsop gtp_sf
  to 1/1/x1
  from vp1
  flowrule add pass gtp ver 2
  exit
```

Use Case Five: Identifying Traffic from GTP Logical Interfaces

Some network monitoring tools are required to see traffic from varying LTE/3G logical interfaces (S1U/S11, S5/S8, orGn/Gp) on dedicated tool ports, but do not have the ability to process traffic based on these varying logical interfaces. As part of GTP correlation, Gigamon Visibility Fabric nodes also provide the flexibility to identify traffic by LTE/3G logical interfaces. Utilizing LTE/3G Logical interface filtering, traffic flows from varying interfaces can be directed to associated tool ports. Figure 5 shows the distribution of traffic based on LTE/3G Logical Interface.

Distributing traffic based on GTP versions

- Filter and forward S1U/S11 Sessions to tool T1
- Filter and forward S5/S8 Sessions to tool T2
- Filter and forward Gn/Gp Sessions to tool T3

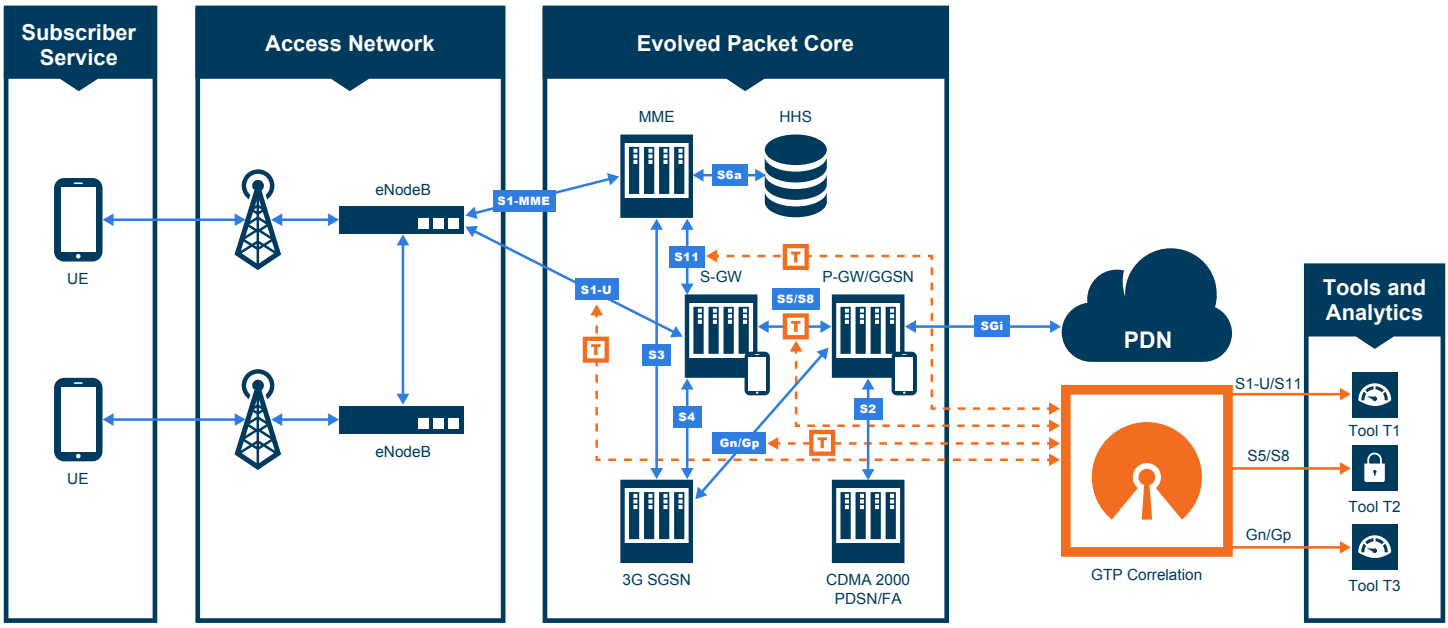


Figure 5: Distribution of traffic based on LTE/3G Logical Interface

```
# Configure ports
port 1/1/x1 type network
port 1/1/x2 type tool
port 1/1/x3 type tool
port 1/1/x4 type tool

# configure gsgroups, gsops to enable GTP correlation
gsgroup alias gsg1 port-list 1/1/e1
gsop alias gtp_sf flow-ops flow-filtering gtp port-list gsg1

## Configure vport on same gsgroup
vport alias vp1 gsgroup gsg1

### Filter out GTP packets to vport using the map below:
map alias to_vp
  to vp1
  from 1/1/x1
  rule add pass portsrc 2123
  rule add pass portsrc 2152
  exit

## Send traffic from S1U/S11 to Tool port 1/1/x2:
  map alias GTP-INTF_S1U_S11
  use gsop gtp_sf
  to 1/1/x2
  from vp1
  flowrule add pass gtp imsi * interface S11
  exit
```

```
## Send traffic from S5/S8 to Tool port 1/1/x3:
  map alias GTP-INTF_S5_S8
  use gsop gtp_sf
  to 1/1/x3
  from vp1
  flowrule add pass gtp imsi * interface S5
  exit

## Send traffic from Gn/Gp to Tool port 1/1/x4:
  map alias GTP-INTF_GnGp
  use gsop gtp_sf
  to 1/1/x4
  from vp1
  flowrule add pass gtp imsi * interface Gn
  exit
```

Use Case Six: Implementing GTP Correlated FlowVUE Subscriber Sampling Traffic to Tools

As traffic levels increase in LTE Mobile Core networks, tool capacity may not be able to scale to support resulting traffic volumes. As part of GTP correlation, Gigamon Visibility Fabric nodes also provide the flexibility to sample a subset of subscribers in the network and to forward all of the traffic for that sample subset to network monitoring tools. Figure 6 shows a use case of sampling 70% of subscribers.

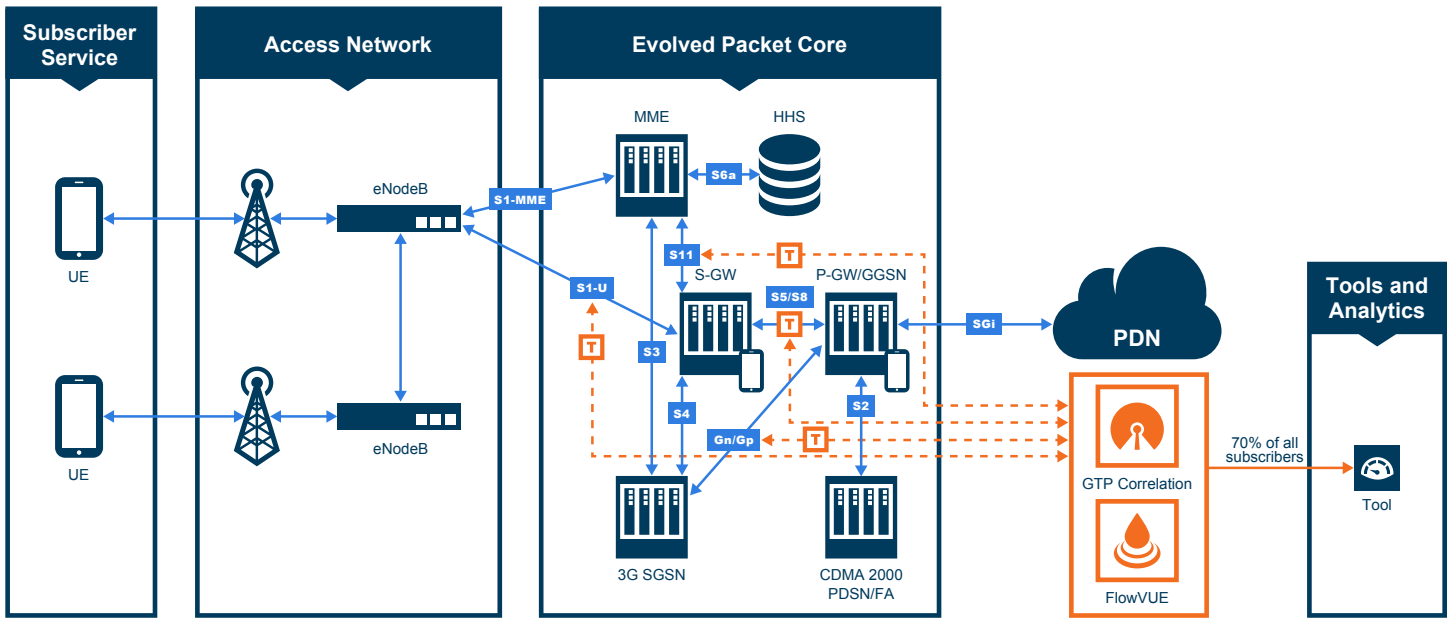


Figure 6: Use case sampling 70% of subscribers

```
# Configure ports
port 1/1/x1 type network
port 1/1/x2 type tool

# configure gsgroups, gsops to enable GTP correlation
gsgroup alias gsg1 port-list 1/1/e1
gsop alias gtp_sf flow-ops gtp-flowsample port-list gsg1

## Configure vport on same gsgroup
vport alias vp1 gsgroup gsg1
```

```
### Filter out GTP packets to vport using the map below:
map alias to_vp
  to vp1
  from 1/1/x1
  rule add pass portsrc 2123
  rule add pass portsrc 2152
  exit

## Send traffic for 70% of subscribers to tool port 1/1/x2:
  map alias GTP-SAMPLE
  use gsop gtp_sf
  to 1/1/x2
  from vp1
  flowsample add gtp imsi * percentage 70
  exit
```

Use Case Seven: Implementing GTP Correlated IMSI Whitelist along with GTP Correlated FlowVUE Subscriber Sampling Traffic to Tools

When GTP Correlated Subscriber Sampling is implemented, the network operator can determine how much subscriber traffic will be monitored. In order for the operator to make sure that their high-value subscribers, or their subscribers who need extra monitoring will be included, inclusion in a whitelist—which ensures their traffic is monitored regardless of the subscriber sampling percentage or random selection. As part of GTP correlation, Gigamon Visibility Fabric nodes provide the flexibility to identify up to 500,000 subscribers by IMSI in a named whitelist to ensure that these subscribers are monitored with a higher priority and outside of sampling. Figure 7 shows an example use case of 70% subscriber sampling with a named set of IMSI's in the whitelist.

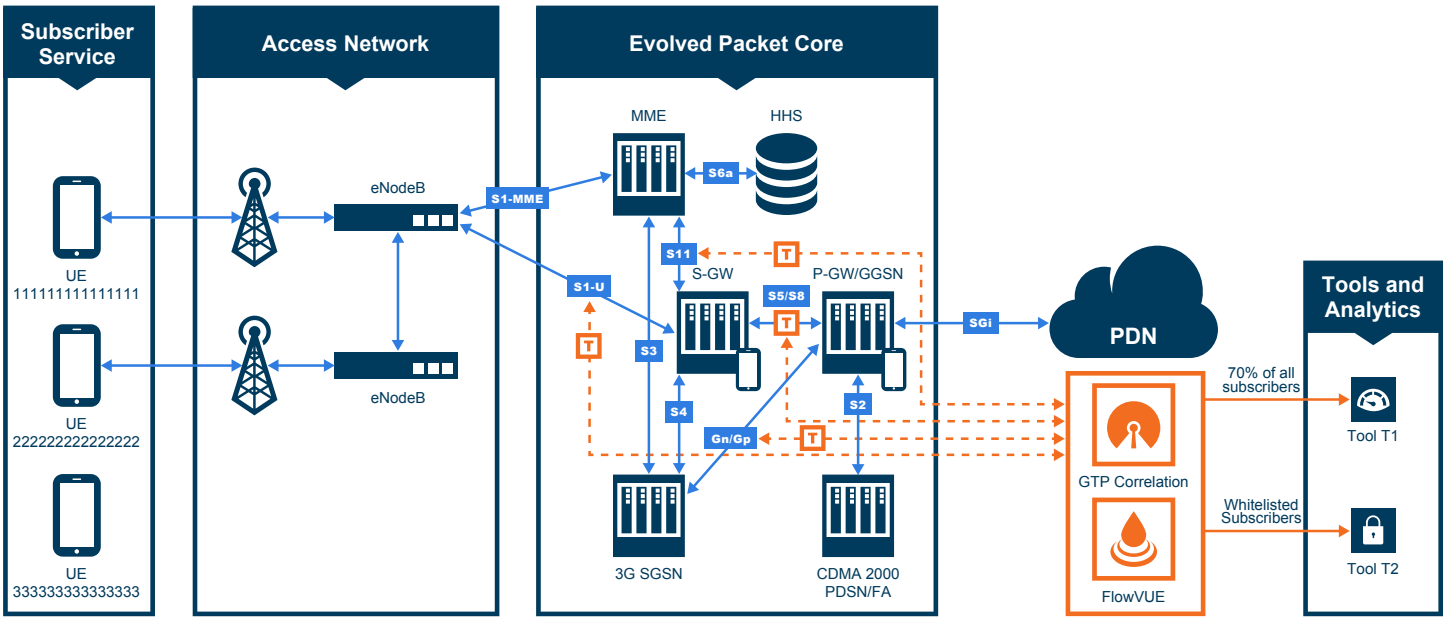


Figure 7: An example a use case of 70% subscriber sampling with a named set of IMSI's in the whitelist

```
# Configure ports
port 1/1/x1 type network
port 1/1/x2 type tool
port 1/1/x3 type tool

## Define a list of IMSIs to be included in a whitelist.
apps gtp-whitelist alias GSAPP_Whitelist create
apps gtp-whitelist alias GSAPP_Whitelist add imsi 111111111111111
apps gtp-whitelist alias GSAPP_Whitelist add imsi 222222222222222
apps gtp-whitelist alias GSAPP_Whitelist add imsi 333333333333333

# configure gsgroups, gsops to enable GTP correlation
gsgroup alias gsg1 port-list 1/1/e1
gsop alias gtp_sf flow-ops gtp-flowsample port-list gsg1
gsop alias gtp_wl flow-ops gtp-whitelist port-list gsg1


## Configure vport on same gsgroup
vport alias vp1 gsgroup gsg1

### Filter out GTP packets to vport using the map below:
map alias to_vp
  to vp1
  from 1/1/x1
  rule add pass portsrc 2123
  rule add pass portsrc 2152
  exit

## Send traffic for 70% of subscribers to tool port 1/1/x2:
  map alias GTP-SAMPLE
  use gsop gtp_sf
  to 1/1/x2
  from vp1
  flowsample add gtp imsi * percentage 70
  exit


## Send traffic for IMSIs in the GTP Whitelist to tool port 1/1/x3:
  map alias GTP-WHITELIST
  use gsop gtp_wl
  to 1/1/x3
  from vp1
  exit
```

Use Case Eight: Implementing GTP Correlated IMSI Whitelist and GTP Correlated FlowVUE Subscriber Sampling Traffic to Tools along with APN Whitelist and APN Scaling

When APN Whitelist and APN Scaling are combined with GTP Correlated Subscriber Sampling and GTP Correlated IMSI Whitelist, the network operator can determine how much subscriber traffic to a specific APN will be monitored. The APN attribute can also be used as a rule within an IMSI Whitelist map making sure that all high-value subscribers, or subscribers who need extra monitoring will be included when requesting a specific APN. This ensures their traffic is monitored regardless of the subscriber sampling percentage or random selection. As part of GTP correlation, Gigamon Visibility Fabric nodes provide the flexibility to identify up to 500,000 subscribers by IMSI in a named whitelist to ensure that these subscribers are monitored with a higher priority and outside of sampling. Figure 8 shows an example use case of 70% subscriber sampling with a named set of IMSI's in the whitelist for a specific APN of interest.

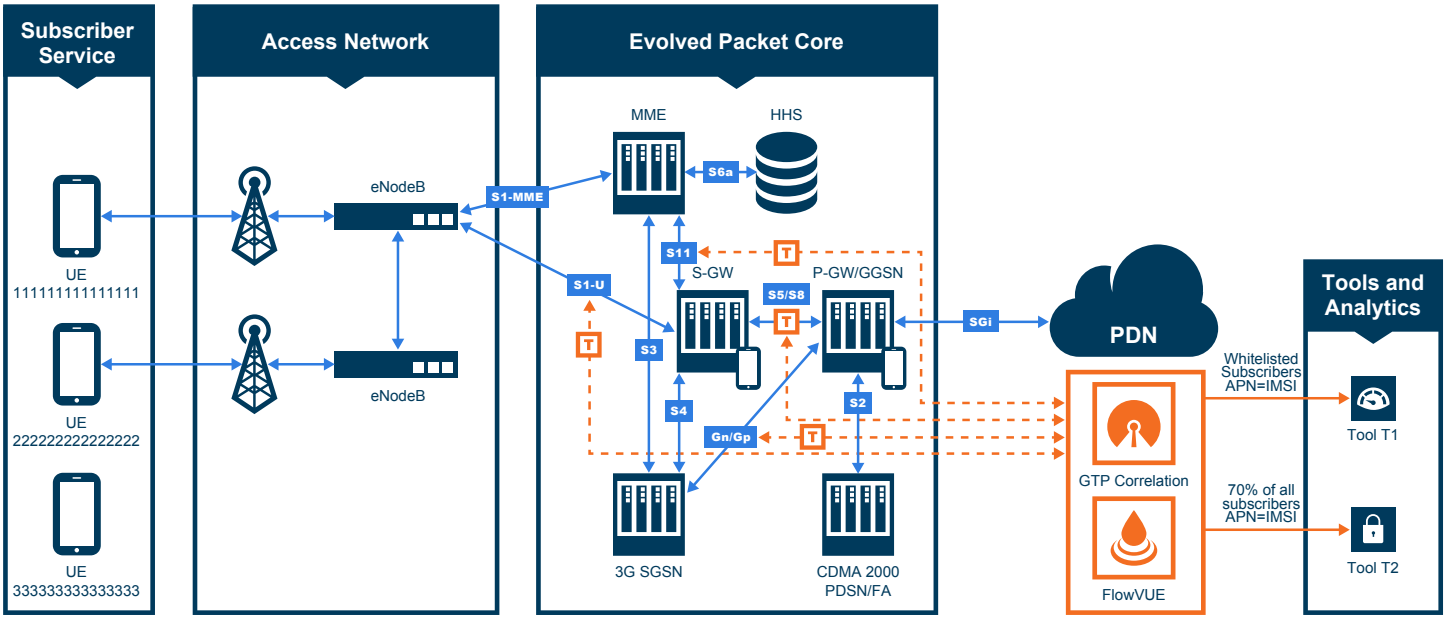


Figure 8: An example a use case for APN monitoring of 70% subscriber sampling with a named set of IMSI's in the whitelist

```
# Configure ports
port 1/1/x1 type network
port 1/1/x2 type tool
port 1/1/x3 type tool

## Define a list of IMSIs to be included in a whitelist.
apps gtp-whitelist alias GSAPP_Whitelist create
apps gtp-whitelist alias GSAPP_Whitelist add imsi 111111111111111
apps gtp-whitelist alias GSAPP_Whitelist add imsi 222222222222222
apps gtp-whitelist alias GSAPP_Whitelist add imsi 333333333333333

# configure gsgroups, gsops to enable GTP correlation
gsgroup alias gsg1 port-list 1/1/e1
gsparams gsgroup gsg1 gtp-whitelist add GSAPP_Whitelist
gsop alias gtp_sf flow-ops gtp-flowsample port-list gsg1
gsop alias gtp_wl flow-ops gtp-whitelist port-list gsg1


## Configure vport on same gsgroup
vport alias vp1 gsgroup gsg1
```

```
### Filter out GTP packets to vport using the map below:
map alias to_vp
  to vp1
  from 1/1/x1
  rule add pass portdst 2123  bidir
  rule add pass portdst 2152  bidir
  rule add pass ipfrag all-frag-no-first
    exit

## Send traffic for 70% of subscribers to tool port 1/1/x2:
  map alias GTP-SAMPLE
  type secondLevel flowSample
  use gsop gtp_sf
  to 1/1/x2
  from vp1
  flowsample add gtp apn ims* percentage 70
  exit


## Send traffic for IMSIs in the GTP Whitelist to tool port 1/1/x3:
  map alias GTP-WHITELIST
  type secondLevel flowWhitelist
  use gsop gtp_wl
  to 1/1/x3
  from vp1
  whitelist add gtp apn ims*
  exit
```

Use Case Nine: Implementing GTP Correlated IMSI Whitelist and GTP Correlated FlowVUE Subscriber Traffic Scaling to Tools using QCI

When QCI is used, Whitelist and Traffic Scaling are combined with GTP Correlated Subscriber Aware Traffic Scaling and IMSI Whitelisting. The network operator can direct GTP Bearer traffic of a given QCI to specific tools to enable operators to choose which QCI values, typically for a given APN, are sent to those tools for Subscribers in the Whitelist and those subset of subscribers whose traffic of QCI values will also be sent. In GTP Networks employing VoLTE, an APN such as ims.mobile-operator.com, may contain traffic of given QCI classes. QCI values 1 and 5 are typically used for specific traffic classes within the VoLTE APN traffic set. GTP-u bearer traffic marked with QCI value of 1 will identify traffic that is conversational voice, usually RTP. While GTP-u bearer traffic marked with QCI value of 5 represents the IMS Signaling, usually SIP. An operator may wish to ensure that a VoLTE monitoring tool will see all IMS traffic (Signaling and Voice) for those subscribers in the Whitelist. While ensuring that the same VoLTE monitoring tool will see IMS Signaling for all remaining subscribers and Conversational Voice traffic for 50% of the remaining subscribers. Knowing that the operator should have only QCI 1 and QCI 5 on their IMS network, the operator may wish to ensure that all traffic for all remaining subscribers which is not QCI 1 and not QCI 5 would be sent to the tool so that they can recognize the source of that traffic and correct the equipment that may be mislabeling the QCI values. As mentioned previously, Gigamon Visibility Fabric nodes provide the flexibility to identify up to 500,000 subscribers by IMSI in a named whitelist to ensure that these subscribers are monitored with a higher priority and outside of sampling. Figure 9 shows an example use case of 70% subscriber sampling with a named set of IMSI's in the whitelist for a specific APN of interest.

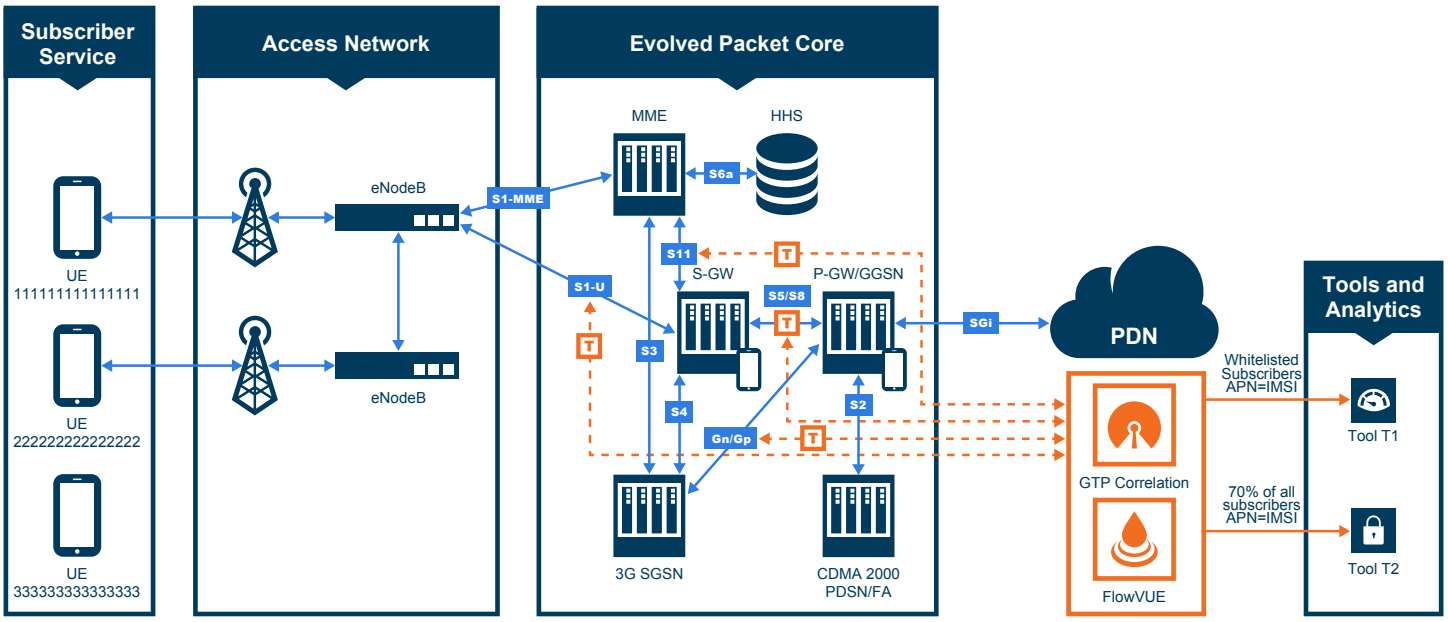


Figure 9: An example use case for APN/QCI monitoring of 50% Conversational Voice scaling with a named set of IMSI's in the whitelist T1 will get 50% of IMS traffic where QCI=1, 100% when QCI = 5 and 100% when QCI=Other T2 will get 100% of IMS traffic for whitelisted subscribers.

```
# Configure ports
port 1/1/x1 type network
port 1/1/x2 type tool
port 1/1/x3 type tool

## Define a list of IMSIs to be included in a whitelist.
apps gtp-whitelist alias GSAPP_Whitelist create
apps gtp-whitelist alias GSAPP_Whitelist add imsi 111111111111111
apps gtp-whitelist alias GSAPP_Whitelist add imsi 222222222222222
apps gtp-whitelist alias GSAPP_Whitelist add imsi 333333333333333

# configure gsgroups, gsops to enable GTP correlation
gsgroup alias gsg1 port-list 1/1/e1
gsparams gsgroup gsg1 gtp-whitelist add GSAPP_Whitelist
gsop alias gtp_sf flow-ops gtp-flowsample port-list gsg1
gsop alias gtp_wl flow-ops gtp-whitelist port-list gsg1


## Configure vport on same gsgroup
vport alias vp1 gsgroup gsg1

### Direct all GTP traffic to vport using the map below:
map alias to_vp
  to vp1
  from 1/1/x1
  rule add pass portdst 2123  bidir
  rule add pass portdst 2152  bidir
  rule add pass ipfrag all-frag-no-first
    exit
```

```
## Send traffic for 50% QCI=1 for subscribers where APN=ims* to tool port 1/1/x2:
## Send traffic for 100% QCI=5 for subscribers where APN=ims* to tool port 1/1/x2:
## Send traffic for 100% QCI=other for subscribers where APN=ims* to tool port 1/1/x2:
  map alias GTP-VOLTE-SCALE-WITH-QCI
  type secondLevel flowSample
  use gsop gtp_sf
  to 1/1/x2
  from vp1
  flowsample add gtp apn ims* qci 1 percentage 50
  flowsample add gtp apn ims* qci 5 percentage 100
  flowsample add gtp apn ims* qci * percentage 100
exit


## Send traffic for IMSIs in the GTP Whitelist where APN=ims* to tool port 1/1/x3:
  map alias GTP-WHITELIST
  type secondLevel flowWhitelist
  use gsop gtp_wl
  to 1/1/x3
  from vp1
  whitelist add gtp apn ims*
  exit
```

Use Case Ten: Implementing GTP Correlated FlowVUE Subscriber Sampling IMS Traffic to Tools with Dedicated Pools for Each Tool

Each of the prior use cases exemplifies multiple simple use cases that enable various GTP monitoring scenarios. Each of them represents a powerful set of functionality that can be used independently. However, as mobile traffic continues to grow while mobile revenue is either declining or flat, mobile operators are being challenged by the need to scale existing tool investments while making new investments only where new services are being deployed. Additionally, as the traffic complexity grows, so does the need for tool configurations, and this adds additional complexity. While each of the prior use cases defined in this Application Note can be used, combining them into a single policy that can support the needs of each tool owner in a large Mobile Operator environment becomes increasingly complex and simply does not serve the wider need. The Multiple Traffic Scaling configuration capability addresses this additional complexity and enables multiple tools to each have an independent configuration. The Gigamon Subscriber-Aware Visibility Fabric will manage this complexity internally for up to 5 independent tool sets. Consider the following scenario:

Network traffic load for a GTP network will peak at 60Gbps comprised of 20Gbps of 3G traffic and 40Gbps of LTE traffic (S1U/S11, S5/S8). Total VoLTE traffic is 5 Gbps.

- Tool A – Has peak capacity of 10Gbps across 4x10Gbps input ports using GTP IMSI Load Balancing and must see only 3G Traffic
- Tool B – Has peak capacity of 50Gbps across 16x10Gbps input ports using GigaStream® Load Balancing and can process all traffic
- Tool C – Has peak capacity of 2Gbps on 1x10Gbps input port and is used for analyzing all Whitelisted Subscribers
- Tool D – Has peak capacity of 10Gbps across 2x10Gbps input ports using GTP IMSI Load Balancing and is used for VoLTE monitoring for QCI=1 and QCI=5
- Tool E – Has peak capacity of 2Gbps on 1x10Gbps input port and needs to see all VoLTE traffic which is not QCI=1 and QCI=5

Any given subscriber session may meet the traffic scaling criteria for each of the 5 tools, other some subscriber sessions may meet the criteria for a subset of the tools and other subscriber sessions may not meet the criteria for any of the 5 tools. GTP Subscriber-Aware Visibility will identify each subscriber session and determine which of the 5 tools should see a copy of that session and it will mark the session to be delivered to those tools. Essentially, GTP Subscriber-Aware Visibility will enable 5 independent tool port traffic scaling configurations that can be managed independently. Figure 10 identifies that example.

What the example will do is as follows:

- Identify all Subscriber Sessions which are 3G and send 50% of them to Tool A using GTP IMSI Based Load Balancing
- Identify all Subscriber Sessions and send 80% of them to Tool B using GigaSTREAM Load Balancing
- Identify all Subscriber Sessions in the Whitelist and send all the traffic for these Subscribers to the single Tool Port for C
- Identify all IMS Subscriber Sessions and send the traffic for QCI=1 and QCI=5 to Tool D using GTP IMSI Based Load Balancing
- Identify all IMS Subscriber Sessions and send the traffic for all QCI values that are not QCI=1 and QCI=5 to single Tool Port E

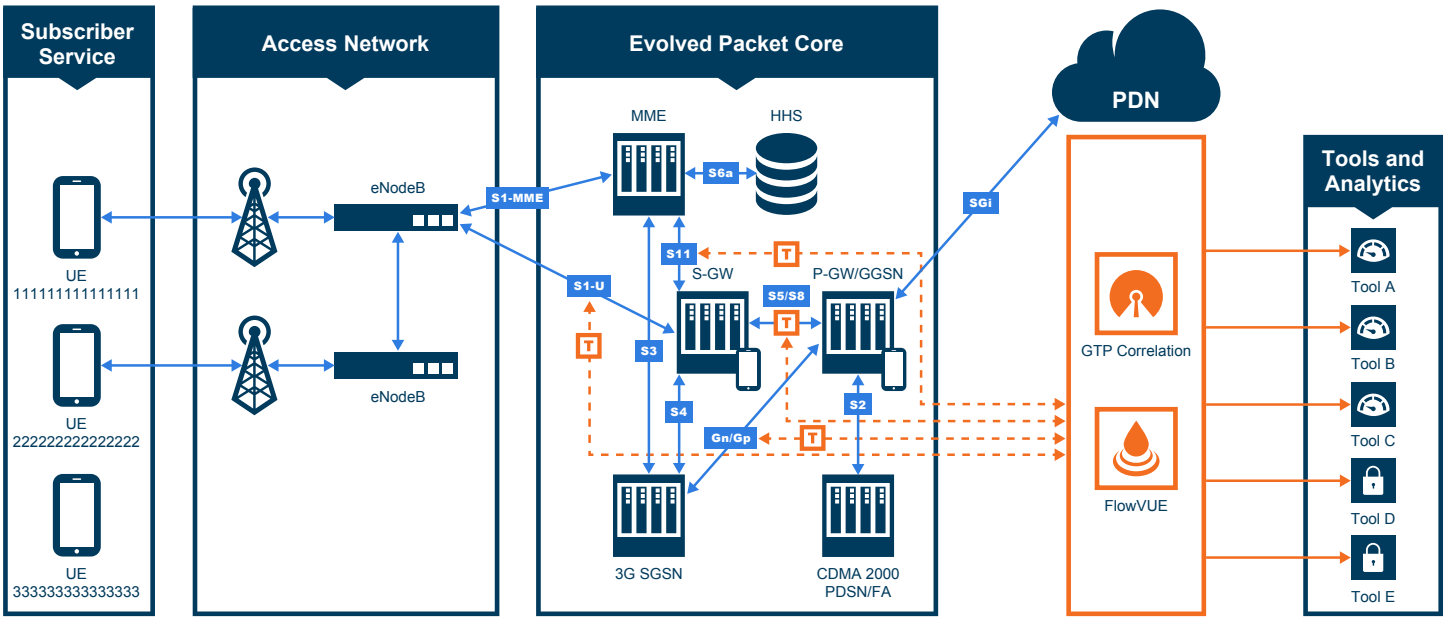


Figure 10: An example a use case for Multiple Traffic Scaling and Whitelisting configurations

```
# Configure ports
port 1/1/x17..x20 type tool  # Tool A
port 1/1/x1..x16 type tool  # Tool B
port 1/1/x21 type tool # Tool C
port 1/1/x23..x24 type tool # Tool D
port 1/1/x22 type tool # Tool E
port 1/2/q1..q4 type network  # GTP Traffic input on 4x40Gbps Network Ports

port-group alias pg_toolA
  port-list 1/1/x17..20
  smart-lb enable
  exit
port-group alias pg_toolD
  port-list 1/1/x23..x24
  smart-lb enable
  exit

gigastream alias ToolB_GS port-list 10/1/x1..x16 params hash advanced

## Define a list of IMSIs to be included in a whitelist.
apps gtp-whitelist alias Overlap2 create
apps gtp-whitelist alias Overlap2 fetch add http://10.0.0.10:/IMSI_WL.txt
```

```
# configure gsgroups, gsops to enable GTP correlation
gsgroup alias gsg1 port-list 1/3/e1..e2,1/4/e1..e2
gsparams gsgroup gsg1 gtp-whitelist add Overlap2
gsop alias gtp-whitelist-1 flow-ops gtp-whitelist lb app gtp metric hashing key imsi port-list
gsg1
gsop alias gtp-flowsample-1 flow-ops gtp-flowsample lb app gtp metric hashing key imsi port-list
gsg1

## Configure vport on same gsgroup
vport alias vport1 gsgroup gsg1 mode gtp-overlap

### Select GTP traffic from network and send to vport using the map below:
map alias GTP-Control
  param traffic control
  rule add pass portdst 2123 bidir
  to vport1
  from 1/2/q1..q4
  exit
map alias GTP-User
  rule add pass ipfrag all-frag-no-first
  rule add pass portsrc 2152 bidir
  to vport1
  from 1/2/q1..q4
  exit

#####
#####

map alias GTP-Whitelist-ToolC
  type secondLevel flowWhitelist-ol
  use gsop gtp-whitelist-1
  whitelist add gtp apn ims*
  to 1/1/x21
  from vport1
  exit

map alias GTP-FlowSample-ToolA
  type secondLevel flowSample-ol
  use gsop gtp-flowsample-1
  flowsample add gtp version 1 percentage 50
  to pg_ToolA
  from vport1
  exit
map alias GTP-FlowSample-ToolB
  type secondLevel flowSample-ol
  use gsop gtp-flowsample-1
  flowsample add gtp imsi * percentage 80
  to ToolB-GS
  from vport1
  exit
map alias GTP-FlowSample-ToolD
  type secondLevel flowSample-ol
  use gsop gtp-flowsample-1
  flowsample add gtp apn ims* qci 1 percentage 100
  flowsample add gtp apn ims* qci 5 percentage 100
  to pg_ToolD
  from vport1
  exit
```

```
map alias GTP-FlowSample-ToolE
  type secondLevel flowSample-ol
  use gsop gtp-flowsample-1
  flowsample add gtp apn ims* qci 1 percentage 0
  flowsample add gtp apn ims* qci 5 percentage 0
  flowsample add gtp apn ims* qci * percentage 100
  to 1/1/x22
  from vport1
  exit

map-group alias GTP-group-1 map-list GTP-Whitelist-ToolC,GTP-FlowSample-ToolA,GTP-Whitelist-
ToolB,GTP-FlowSample-ToolD,GTP-Whitelist-ToolE
```

Use Case Eleven: GTP Tunnel ID-Based Filtering

Figure 11 shows an example of filtering and forwarding traffic based on tunnel IDs that are included as part of the GTP user-plane messages. It also illustrates the concept of sending traffic that does not match any of the configured filters to a shared collector. Here GTP control sessions are being forwarded to all the monitoring tools leveraging the power of Flow Mapping® by filtering on Layer-4 UDP port 2123.

- For GTP-u
  - Filter and forward teid ranges 0x001e8480..0x001e8489 to monitoring tool T1
  - Filter and forward teid ranges 0x001e8490..0x001e8499 to monitoring tool T2
  - Forward the rest of the traffic to a shared collector

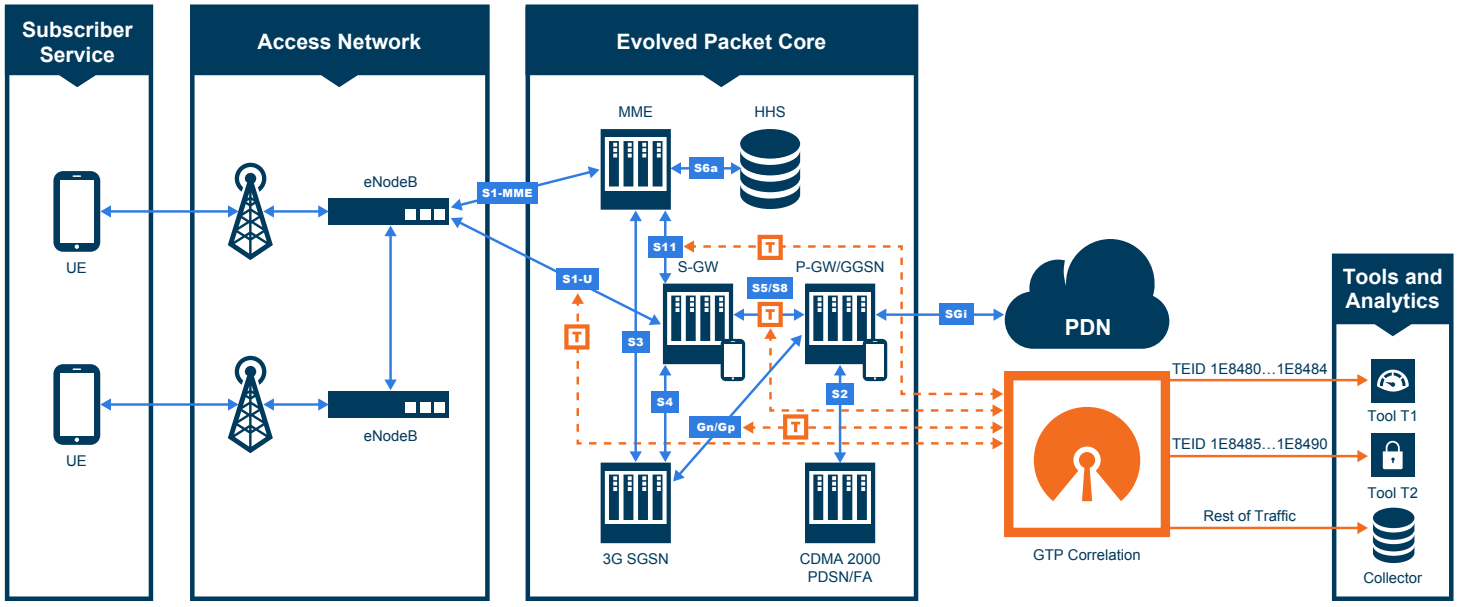


Figure 11: An example of filtering and forwarding traffic based on tunnel IDs that are included as part of the GTP user-plane messages

```
# Configure ports
port 1/3/x9 type network
port 1/3/x15 type tool
port 1/3/x13 type tool
port 1/3/x14 type tool

# configure gigasmart gsops
gsgroup alias gsg1 port-list 1/1/e1
gsop alias gsfil apf set port-list gsg1

# configure vport
vport alias vp1 gsgroup gsg1

# forward GTP-u traffic to second-level map
map alias to_vp
  to vp1
  from 1/3/x9
  rule add pass portsrc 2152
 exit
map alias ctrl_to_tool
  to 1/3/x13,1/3/x15
  from 1/3/x9
  rule add pass portsrc 2123
 exit

map alias m1
  use gsop gsfil
  to 1/3/x13
  from vp1
  gsrule add pass gtp gtpu-teid range 0x001e8480..0x001e8484 subset none
  exit

map alias m2
  use gsop gsfil
  to 1/3/x15
  from vp1
  gsrule add pass gtp gtpu-teid range 0x001e8485..0x001e8490 subset none
  exit

## Add collector for unmatched data
map-scollector alias scoll
from vp1
collector 1/3/x14
exit
```

Use Case Twelve: Distributing Traffic Based on Inner IP Addresses and Inner TCP Port Values

- Packets from VLAN 20 with GTP inner IP 65.128.7.21 and 98.43.132.70, inner TCP port 80 forward to tool T1
- Packets from VLAN 20 with GTP inner IP 65.128.7.21 and 98.43.132.70, inner TCP port 443 forward to tool T2
- All packets not matching above rules will go to tool T3

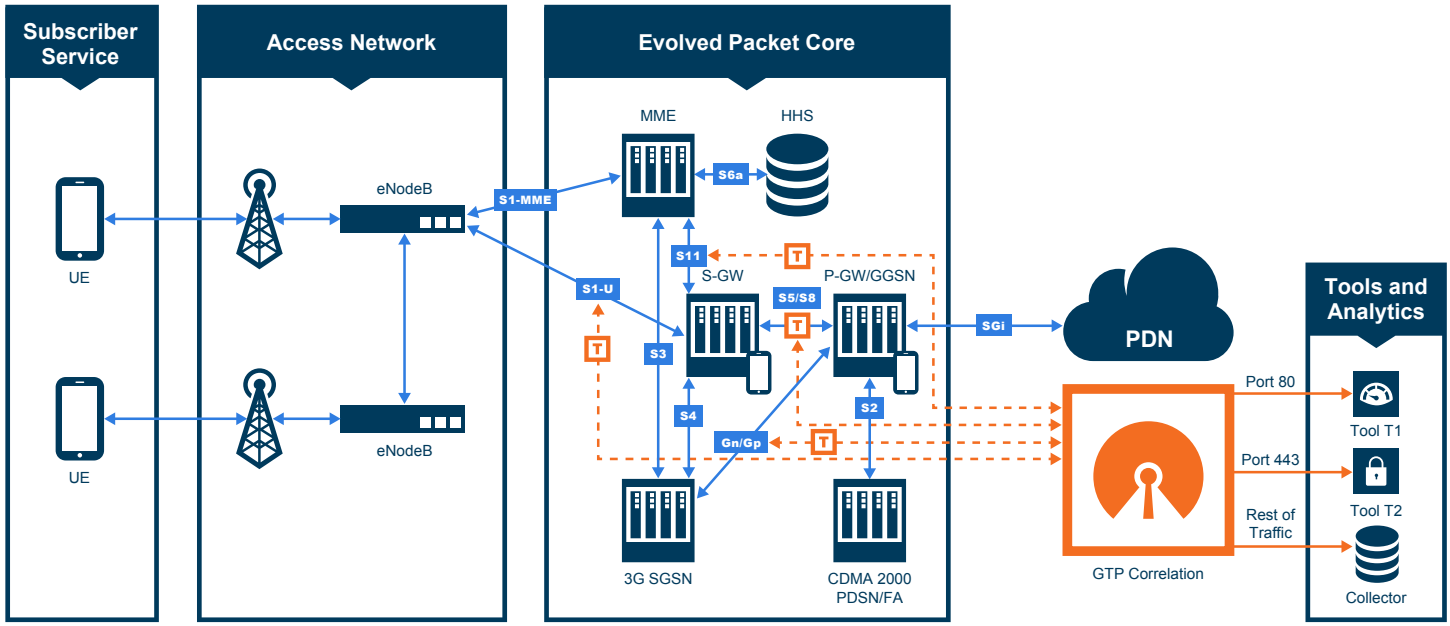


Figure 12: Distributing traffic based on inner IP addresses and inner TCP port values

```
vport alias gsTraffic gsgroup gsgrp1

map alias map1
from N1
to gsTraffic
rule add pass vlan 20 protocol udp portdst 2152

gsop alias <g1> apf port-list gsgrp1

map alias map2
from gsTraffic
to T1
use gsop g1
gsrule add pass ipv4 dst inner 65.128.7.21 /32 ipv4 proto inner tcpport dst inner 80
gsrule add pass ipv4 dst inner 98.43.132.70 /32 ipv4 proto inner tcpport dst inner 80

map alias map3
from gsTraffic
use gsop g1
gsrule add pass ipv4 dst inner 65.128.7.21 /32 ipv4 proto inner tcpport dst inner value 443
gsrule add pass ipv4 dst inner 98.43.132.70 /32 ipv4 proto inner tcpport dst inner 443

map-scollector alias mapC1
from gsTraffic
collector T3
```

About Gigamon

Gigamon provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Gigamon's Visibility Fabric™ and GigaSECURE®, the industry's first Security Delivery Platform, deliver advanced intelligence so that security, network, and application performance management solutions in enterprise, government, and service provider networks operate more efficiently. As data volumes and network speeds grow and threats become more sophisticated, tools are increasingly overburdened. One hundred percent visibility is imperative. Gigamon is installed in more than three-quarters of the Fortune 100, more than half of the Fortune 500, and seven of the 10 largest service providers.

For more information about the Gigamon Unified Visibility Fabric visit: **www.gigamon.com/solutions/service-providers**

4092-01 11/16

Gigamon®

3300 Olcott Street, Santa Clara, CA 95054 USA | +1 (408) 831-4000 | www.gigamon.com