Gigamon®

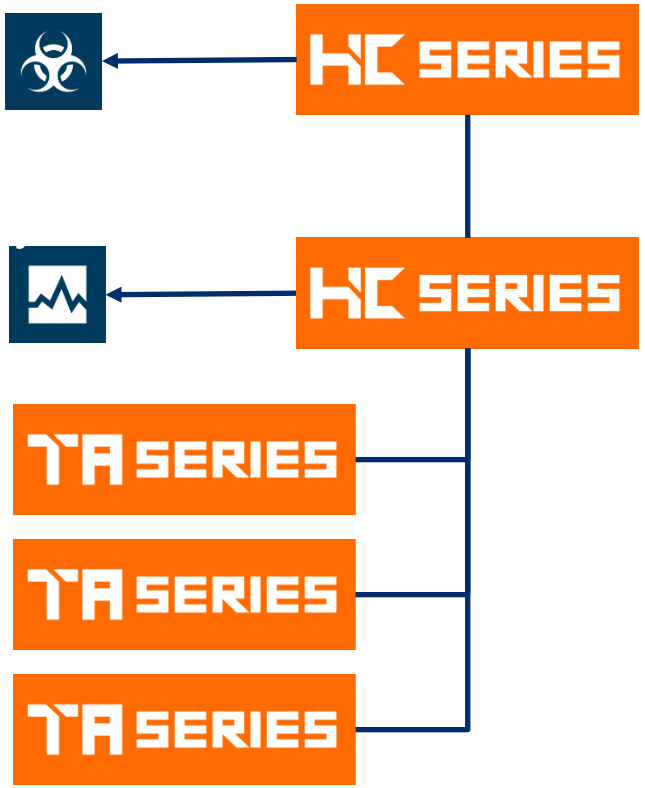
Gigamon. Копирование и фильтрация трафика. Часть 2

Александр Грачев

Менеджер по развитию бизнеса
Нетвелл

Традиционный кластер

ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ ДЛЯ ОБЪЕДИНЕНИЯ УСТРОЙСТВ



Преимущества:

- ✓ Устройства объединенные в кластер имеют единое управление и работают как единая платформа.
- ✓ Возможность использования функций GigaSMART для всех устройств в кластере, при наличии соответствующего модуля и лицензий хотя бы на одном устройстве.
- ✓ До 32 устройств в одном кластере.
- ✓ Наилучший способ обмена трафиком между устройствами Gigamon

Недостатки:

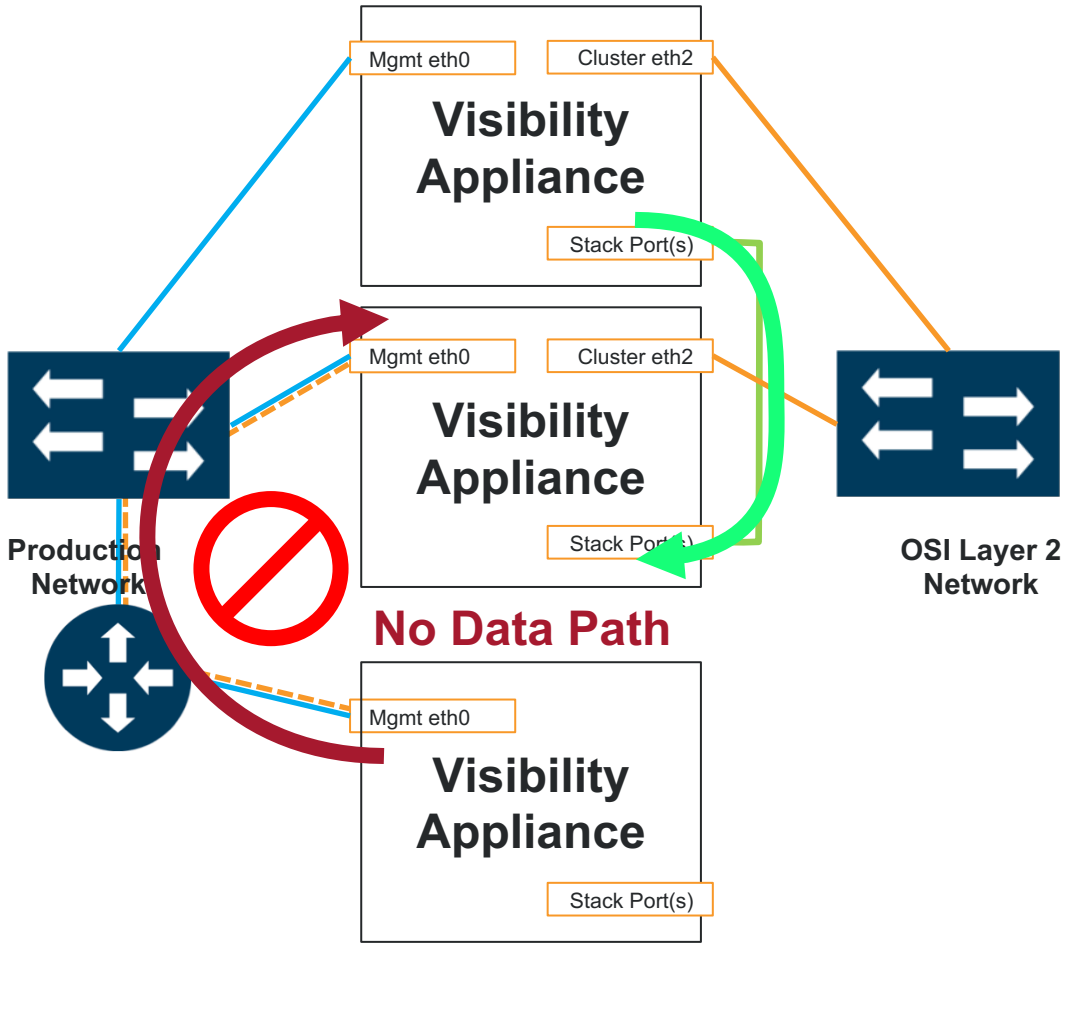
- – Отсутствие резервированной архитектуры.
- – Необходимо L1 соединение устройств, из-за использования расширений Ethernet

Кластер Out-of-Band

Out-of-Band Cluster

Out-of-band

- Предпочтительный ТИП кластера
- Control plane и Data Plane проходят по разным интерфейсам
- Только Master и Standby должны иметь адреса управления из одной подсети, остальные члены кластера могут быть из других подсетей.
- Наиболее стабильный тип кластера
- Поддерживаемые топологии – цепь, звезда, смешанная цепь+звезда



Кластер Inband

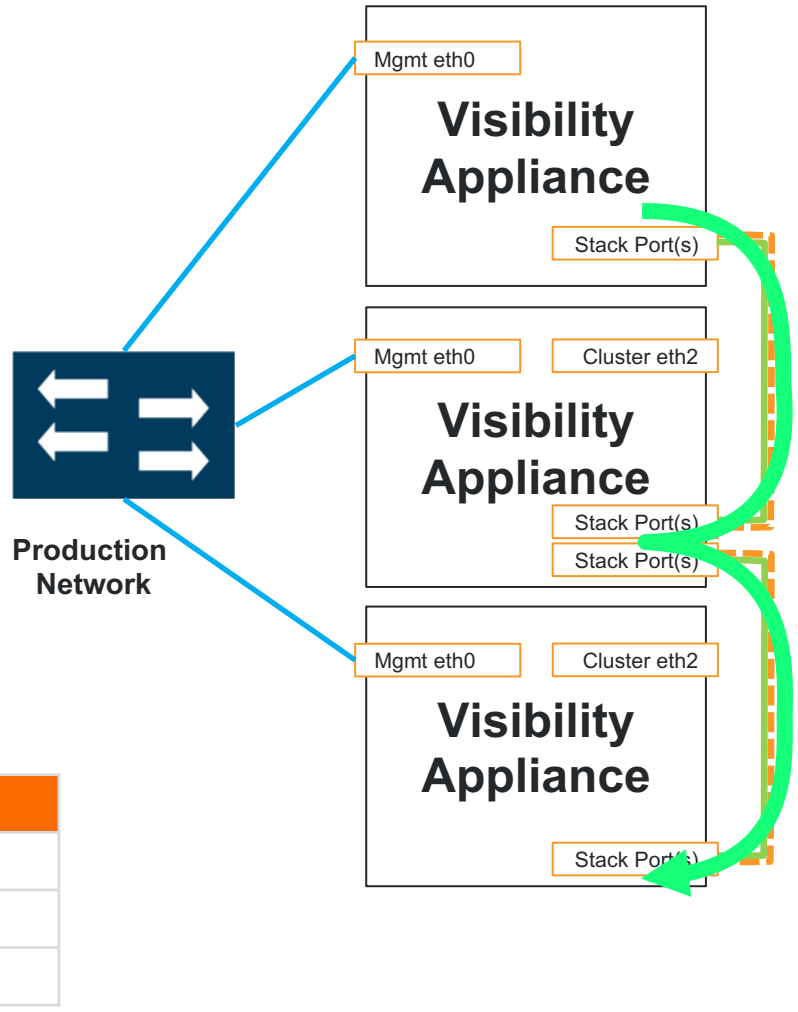
Inband Cluster

Choose a cluster architecture

There are three general cluster architectures to select from.

1. Out-of-band
   - Preferred
   - Single path between appliances
   - Supports remote nodes

2. Inband
   - Control plane и Data Plane проходят по разным интерфейсам
   - Поддерживаемые топологии – цепь, звезда, смешанная цепь+звезда

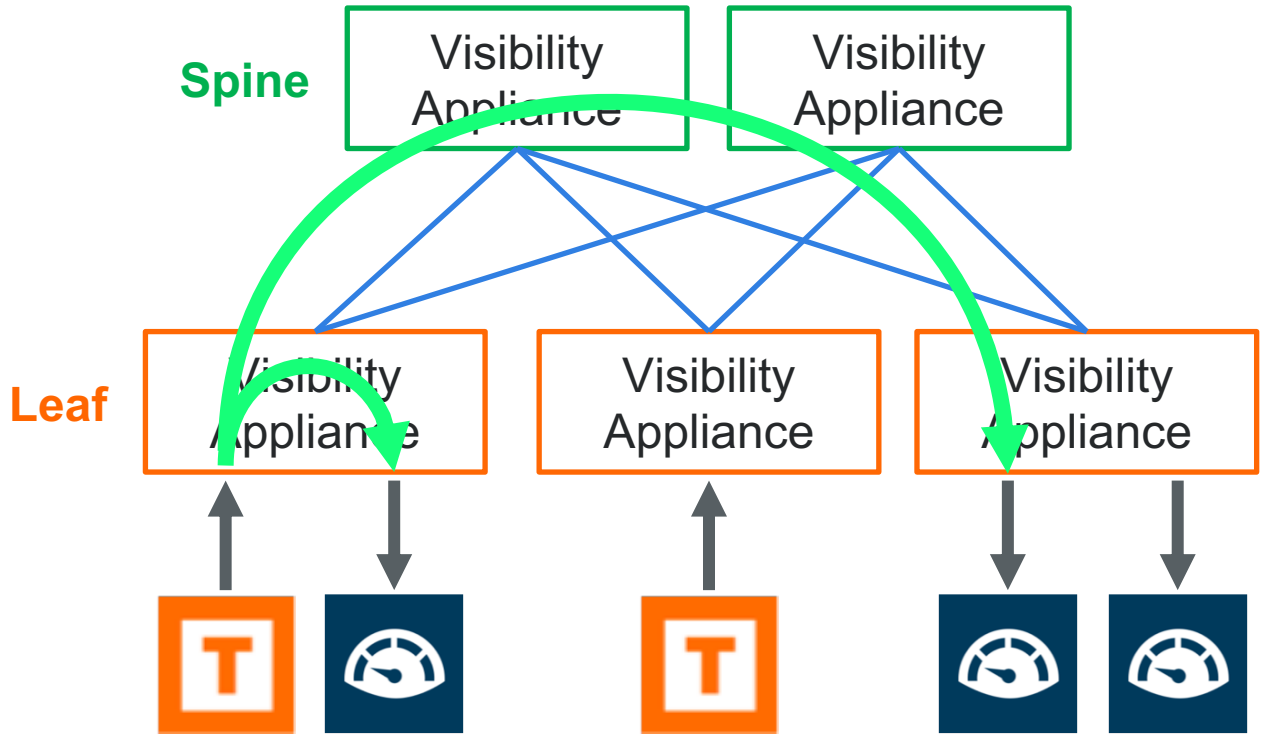


Кластер Spine Leaf

Choose a cluster architecture

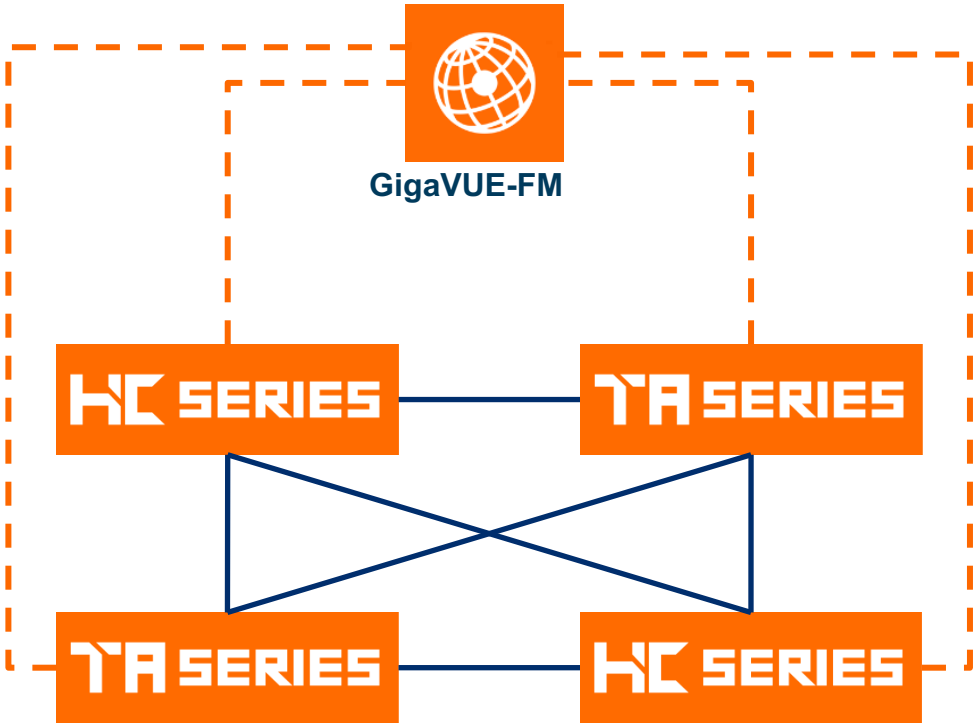
There are three general cluster architectures to select from.

1. Out-of-band
   - Preferred
   - Single path between appliances
   - Supports remote nodes
2. Inband
   - Supports only local nodes
   - Single path between appliances
3. **Leaf and Spine**
   - Развитие кластера Out-Of-Band с резервированной архитектурой



Fabric Maps

ПОСТРОЕНИЕ РАСПРЕДЕЛЕННЫХ ПОЛИТИК КОПИРОВАНИЯ ТРАФИКА БЕЗ КЛАСТЕРИЗАЦИИ



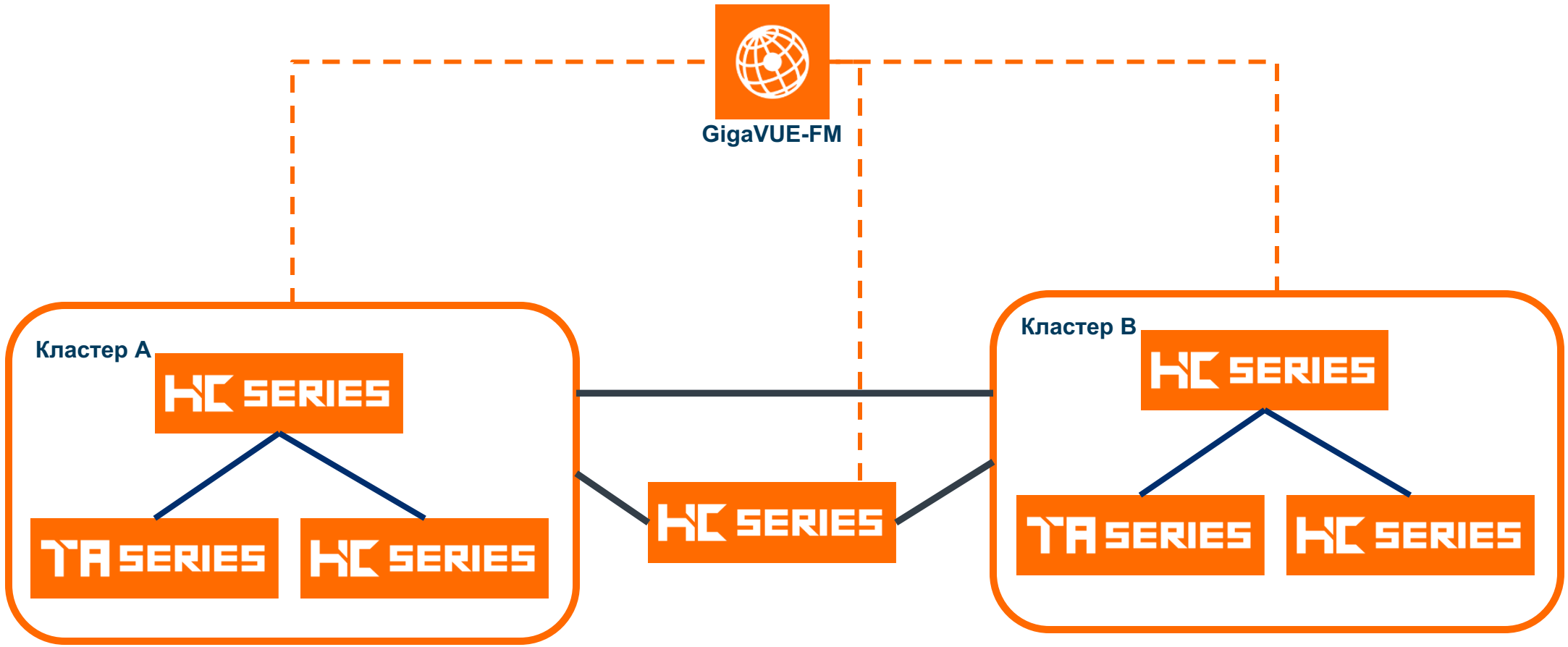
Преимущества:

- ✓ Все устройства работают в stand along режиме.
- ✓ GigaVUE-FM создает политики копирования и фильтрации на каждом устройстве.
- ✓ Вместо кластерных интерфейсов используются Circuit интерфейсы, которые работают поверх коммутируемых сетей.
- ✓ Возможность использования функций GigaSMART для всех устройств, при наличии соответствующего модуля и лицензий хотя бы на одном устройстве.
- ✓ До 200 устройств может работать совместно.
- ✓ Еще один «Наилучший способ обмена трафиком между устройствами Gigamon»
- ✓ Поддержка любой топологии соединения устройств
- ✓ В случае потери связи с между FM и пакетным брокером, политики пропускания трафика не изменяются.

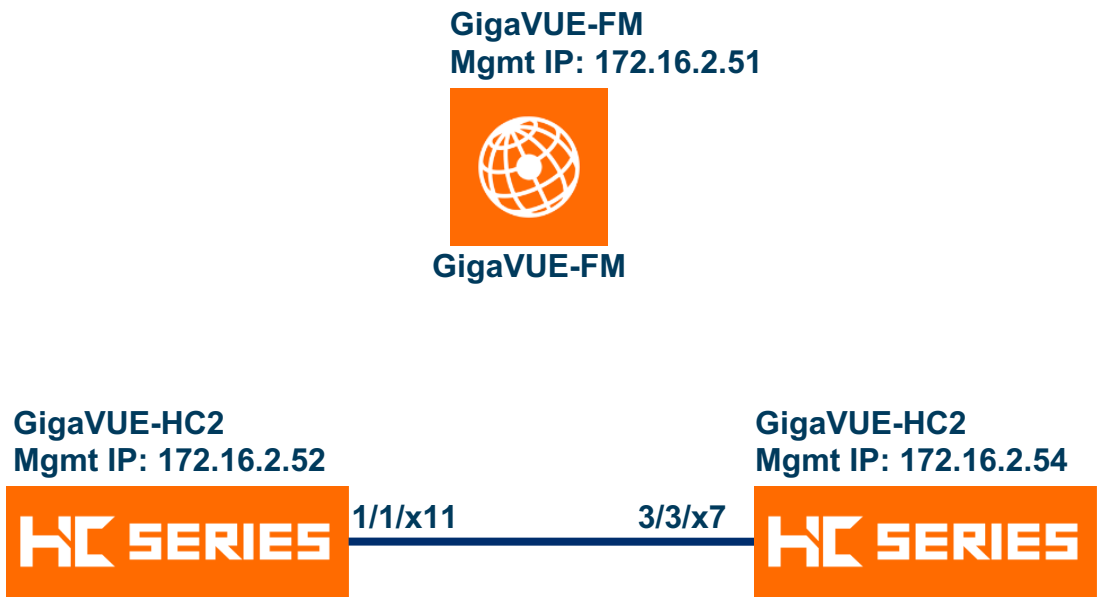
Недостатки:

- − Требуется GigaVUE-FM. Но разве это недостаток?

Комбинирование Fabric Maps и кластера



Лабораторная инталяция




```
! Custer config data
cluster ID Netwell-test
cluster name Netwell-test
Cluster master ip address 172.16.2.53 /24
```

Пример конфигурирования кластера Out-of-Band через CLI (1)

! на мастере делаем

cluster id Netwell-test

cluster name Netwell-test

cluster interface eth0

cluster master interface eth0

cluster master address vip 172.16.2.53 /24

cluster enable

!! дальнейшие конфигурации выполняем через 172.16.2.53

!! мастер переходит в кластер с активным box-ID, chassis и card

Пример конфигурирования кластера Out-of-Band через CLI (2)

! добавление нового устройства в кластер

! Выполняем на новом устройстве, его адрес управления может быть из другой подсети

cluster ID Netwell-test

cluster name Netwell-test

cluster interface eth0

no cluster master auto-discovery

cluster master address primary ip 172.16.2.52

cluster enable

!! на VIP мастера далаем

show chassis

chassis box-id 3 serial-num C027C

card all

Пример конфигурирования кластера Out-of-Band через CLI (3)

! Порты соединяющие устройства переводим в тип STACK

!! на VIP мастера далаем

stack-link alias HC2-HC2 between ports 3/3/x7 and 1/1/x11

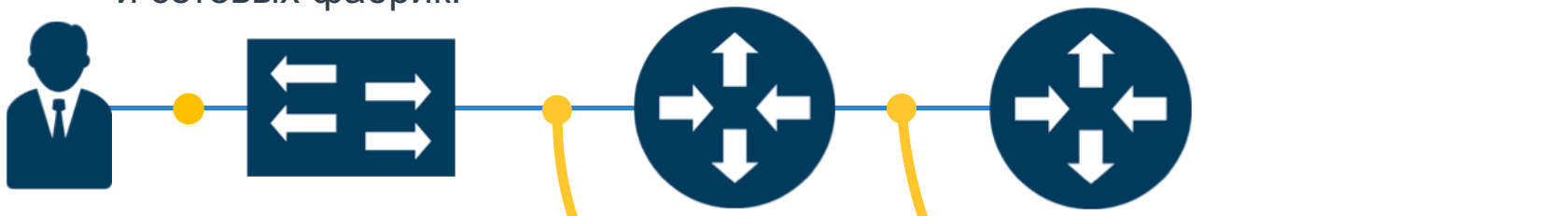
План подготовки к конфигурированию Fabric Maps.

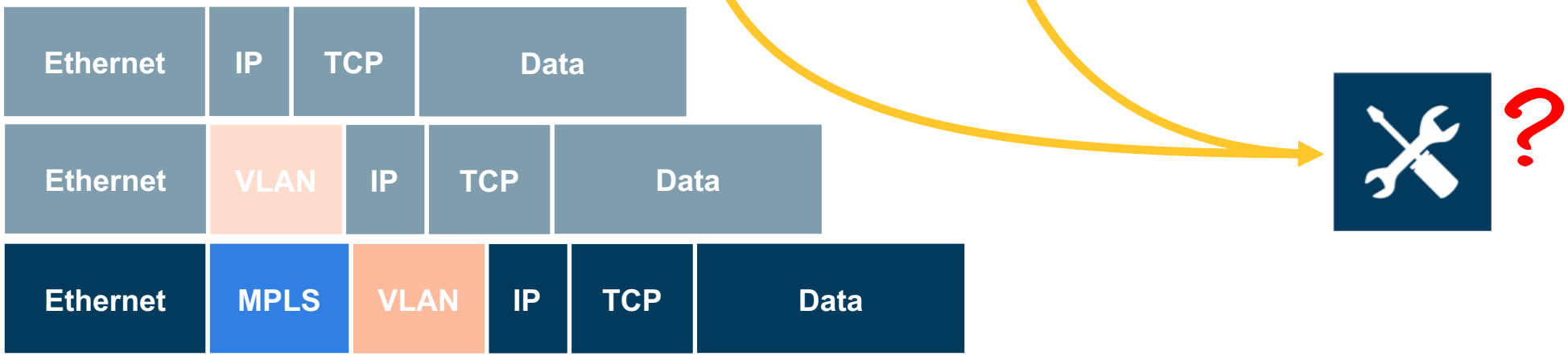
1) включаем GDP на портах между устройствами.
2) включаем GDP на шасси.
3) порты соединяющие устройства делаем TYPE=Circuit
4) создаем Gigastream из портов соединяющих устройства, даже если в каждом gigastream будет всего один порт.
5) делаем rediscovery устройств в FM.
6) теперь конфигурируем fabric maps.

Header Stripping

Удаляем заголовки из трафика

- Позволяет передавать получателям трафик без заголовков сетевых протоколов.
- Позволяет передавать трафик перехваченный из магистральных сетей и сетевых фабрик.





Удаление заголовков без GigaSMART. (VLAN, VXLAN и MPLS)

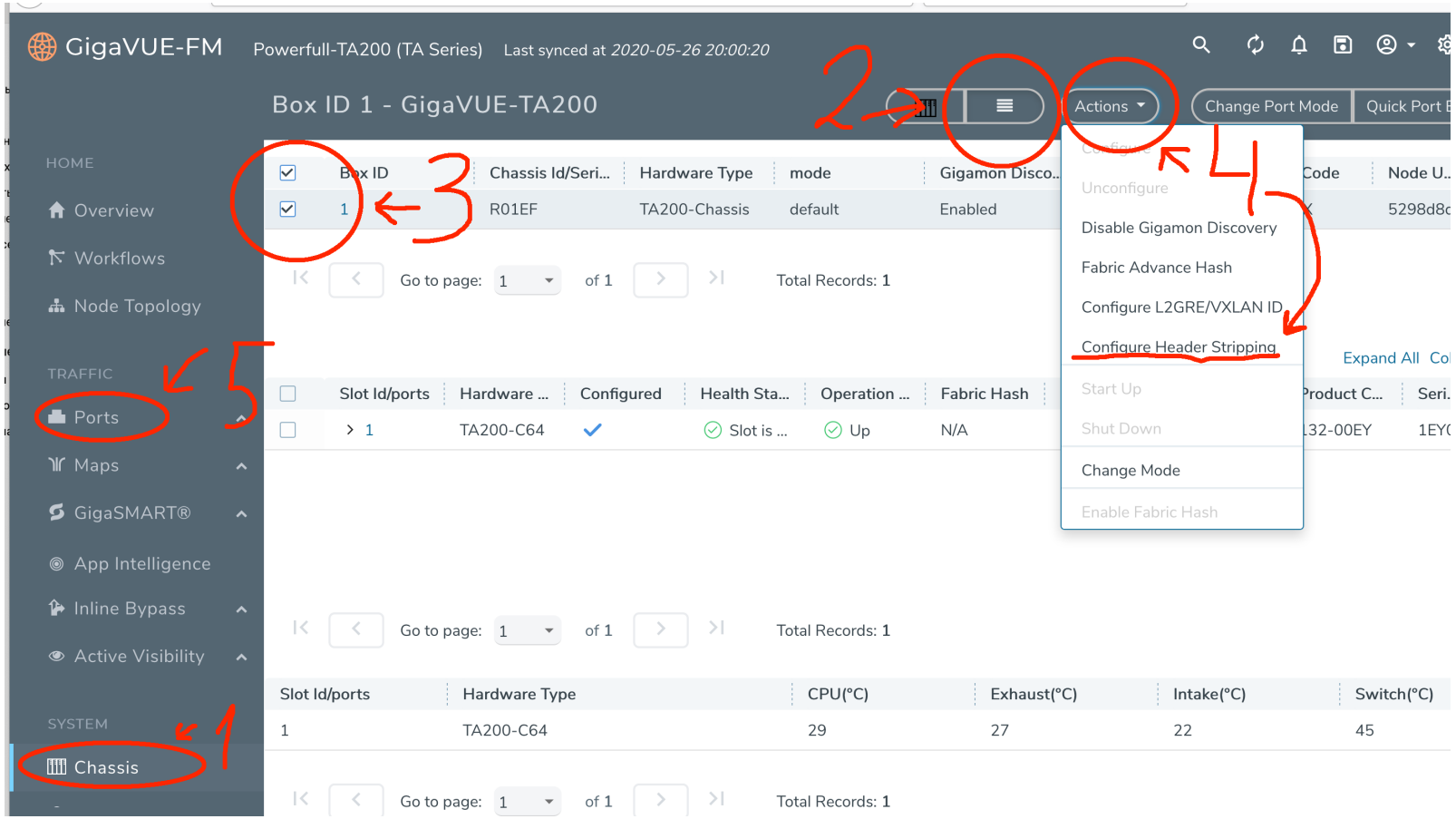
Некоторые правила и ограничения:

1) Поддерживаемые платформы - все из актуального портфолио, кроме TA10.
2) Удаляется Не более 2х меток MPLS в пакете.
3) Настраивается только для Network и Hybrid портов (VXLAN&MPLS stripping).
4) Только для L3 MPLS и L3 MPLS VPN.
5) Не работает с QnQ (VXLAN&MPLS stripping).
6) Порты с включенным VXLAN stripping не могут использоваться в одной map с включенным MPLS Stripping (проверить в MAP-Passall)
7) VXLAN stripping не работает с IPv6
8) VXLAN не будет работать если в MAP выполняется фильтрация по атрибутам относящимся к VXLAN (IP Source\Destination, MAC source)
9) Удаление VXLAN и MPLS меток настраивается только через GigaVUE-FM и CLI.

Удаление заголовков без GigaSMART. (VLAN, VXLAN и MPLS) config

Настройка в GUI (FM):

1) System =>Chassis, переходим в табличный вид и ставим галочку на около шасси
2) Нажимаем кнопку Actions и выбираем Configure Header Stripping.
3) Настраиваем нужные нам параметры Header Stripping.
4) Переходим в раздел Ports и конфигурируем порты.



Удаление заголовков без GigaSMART. (VLAN, VXLAN и MPLS) config

MPLS & VXLAN stripping CLI config

```
header-strip box-id 1 mpls
  add 100..150
  exit
header-strip box-id 1 vxlan
  aging-interval 500
  exit

port 1/1/c8 header-strip mpls-l3
port 1/1/c9 header-strip vxlan
```

VLAN stripping CLI config

```
port 1/1/c12 type tool
port 1/1/c12 egress-vlan strip
```

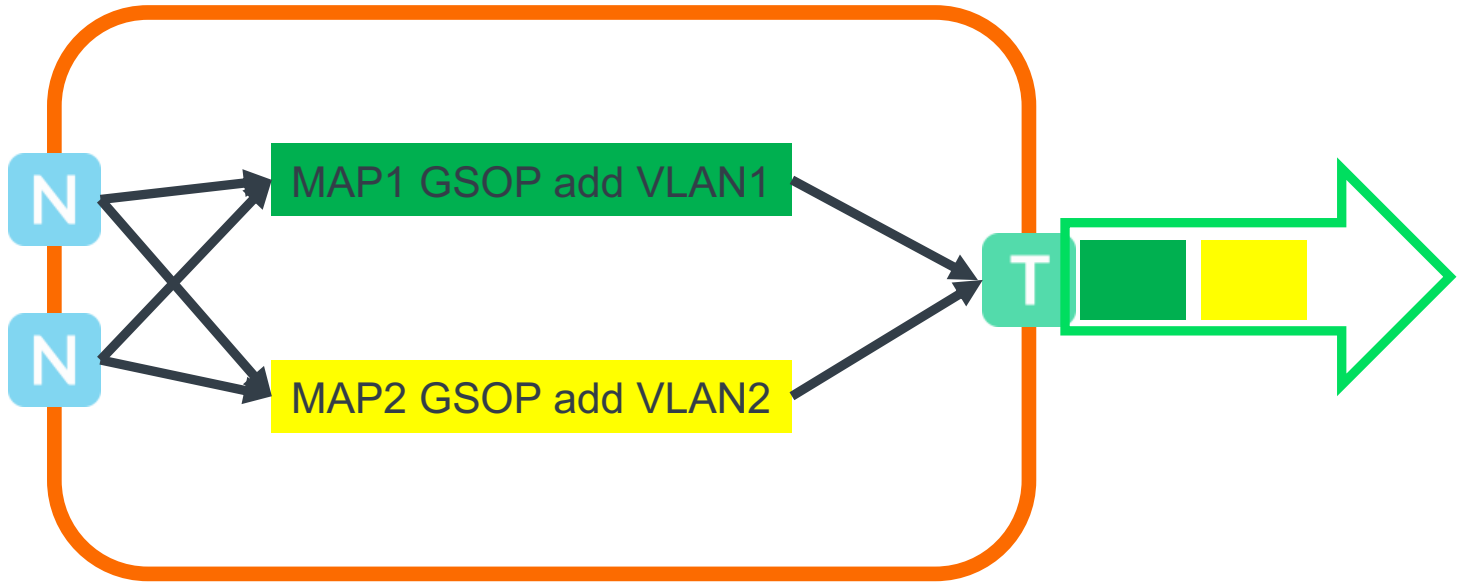
Удаление заголовков GigaSMART

Header stripping:

1) Позволяет удалять следующие заголовки: erspan, fabric-path, fm6000-ts, gre, gtp, isl, mpls (до 5ти меток), mpls+vlan, vlan, vntag, vxlan (до 2х VXLAN в пакете за один раз)
2) Так же позволяет самостоятельно настроить удаляемую часть заголовков в пакете, что дает возможность удалять инкапсуляции практических любых протоколов
3) Имеет простую настройку – настраивается только GigaSMART operation

Header addition:

1) Добавляет VLAN в пакет.
2) Имеет простую настройку – настраивается только GigaSMART operation
3) Может использоваться для того чтобы «покрасить» трафик каждого сервиса. Например WEB от Proxy 1 с VLAN1, WEB от Proxy 2 с VLAN 2

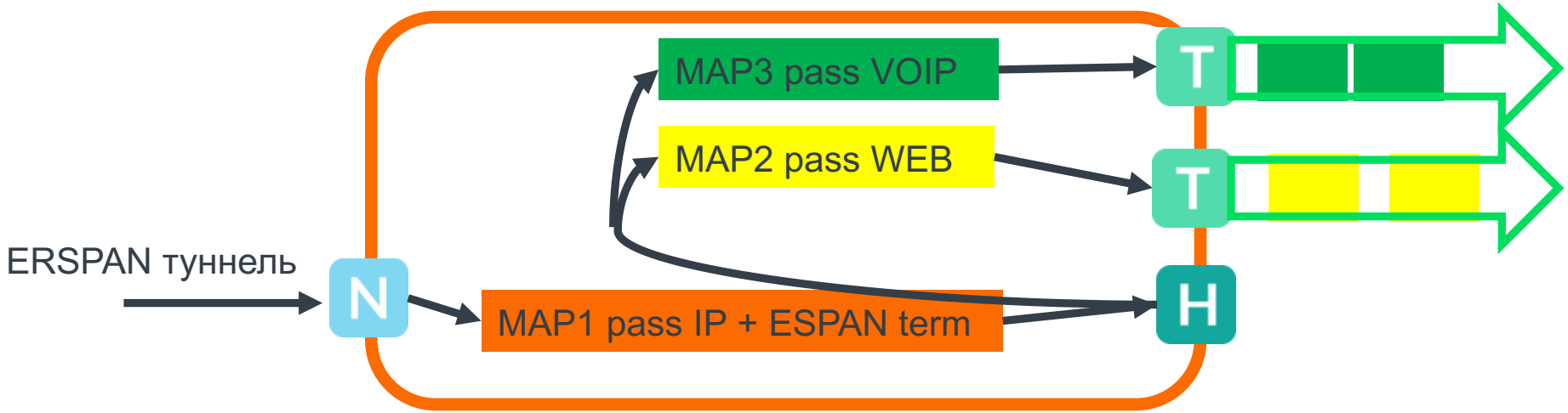


Tunneling

- Получение копии трафика от виртуальных решений Гигамон (GigaVUE-VM/V-Series nodes).
- Передача копий трафика между Гигамонами по IP сети.
- Получение копии трафика от сетевых устройств и виртуальных свичей через ERSPAN v2 и v3/VXLAN
- Поддержка IPv4 и IPv6

Tunneling. Конфигурирование.

1) Создаем IP Interface. Назначаем ему IP Адрес, шлюз по умолчанию, MTU и привязываем его к нужной Gigasmart group
2) Создаем GigaSMART операцию.
3) Создаем MAP-Byrule с GigaSMART операцией.
4) !!!!ВНИМАНИЕ!!!! Т.к. Сам заголовок тоннеля будет удален только на модуле GigaSMART, то если MAP, в которой будет применена GSOP – терминации тоннеля будет выполнять фильтрацию по заголовку этого тоннеля, а не по заголовку пакета находящегося внутри. Поэтому для фильтрации полученной копии трафика, нужно в MAP с «тоннельной» GSOP нужно указать порт-получатель Hybrid. А затем создавать карту в которой этот порт будет источником и выполнять фильтрацию.



NetFlow / IPFIX /CEF Generation

- Генерирует Netflow\IPFIX из копии трафика, которая есть на платформе.
- Если устройство в кластере отправляющий порт может располагаться на удаленном устройстве, не на том где есть модуль GigaSMART
- Поддерживаемые версии Netflow V5, Netflow V9, IPFIX+Метаданные
- Передача метаданных через CEF.
- Возможность генерирования NetFlow группой модулей GigaSMART, позволяет масштабировать производительность платформы.
- Генерация Netflow из IPv4 и IPv6 трафика, но передача коллектору только по IPv4
- Возможность передачи Netflow нескольким коллекторам-получателям

IPFIX расширенные метаданные

GigaSMART NetFlow Generation позволяет обогащать IPFIX информационными элементами верхних уровней. Их анализ позволяет контролировать работу сервисных платформ, а так же выявлять сложные высокоуровневые атаки и вредоносные активности в сети.

Доступные дополнительные информационные элементы:

Extension	Example Metadata
DNS	RDATA, Query Name, OPCODE, AXFR/IXFR (40+ информационных элементов)
HTTP	URLs, GET, POST, PUT, DELETE, and HEAD method types, ALL 2xx 3xx 4xx 5xx Коды ответов
SIP	INVITE, ACK, BYE, REGISTER, OPTIONS, and CANCEL типы запросов
Certificates	Cert Subject, SNI, Cert Issuer, Issue date (20+ информационных элементов)

NetFlow и IPFIX. Конфигурирование.

1 Exporter

- Получатель Netflow
- Конфигурируем в GigaSMART->Netflow

2 IP Interface

- Порт отправитель, должен быть Tool
- Конфигурируем в Ports-> IP Interfaces

3 Record

- Какую статистику собираем и версия Netflow
- Конфигурируем в GigaSMART->Netflow

4 Monitor

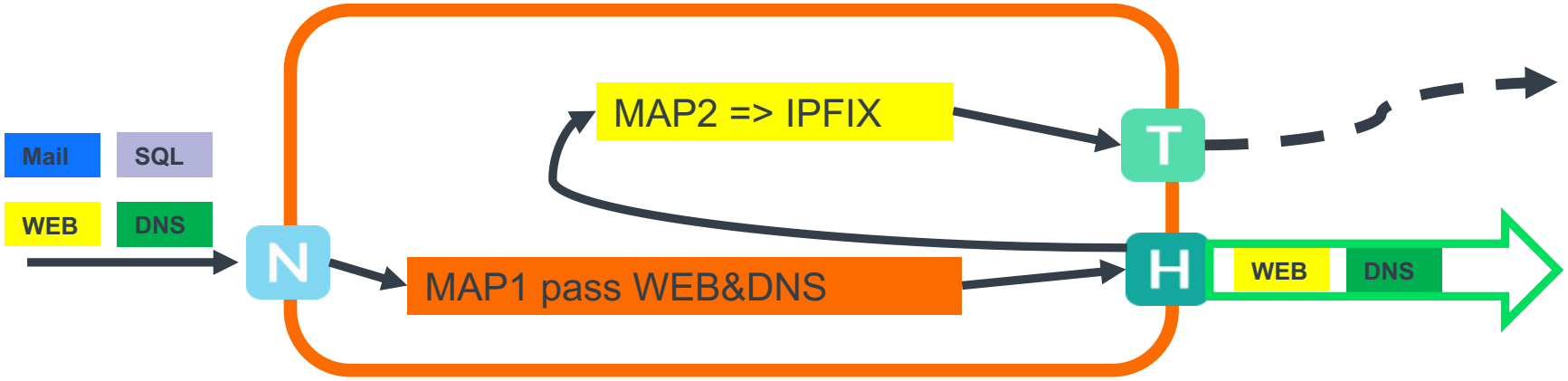
- Как формируем статистику
- Конфигурируем в GigaSMART->Netflow

5 Monitor-GSGROUP

- Привязываем Monitor к Gigasmart Group.
- Конфигурируем в GigaSMART->GigaSMART Groups

6-7 GSOP-MAP

- Создаем GigaSMART операцию
- Создаем MAP-ByRule с GigaSMART операцией



Внимание:

Часто бывает так что нам нужно отправлять трафик в «сыром» виде одним получателям и из него же сделать NetFlow другим. Одно из решений этой задачи приведено на рисунке слева

Gigamon®

Благодарю за внимание!