Коммутатор SNR-S4550-24XQ в качестве фильтра и агрегатора трафика для СОРМ

Проблемы с зеркалированием клиентского трафика на съемник СОРМ, возникают перед каждым оператором, с ростом объемов трафика.

Мы узнали, что один их наших клиентов использует для зеркалирования коммутатор SNR-S4550-24XQ, и попросили поделиться информацией об используемой схеме. Думаем этот опыт будет интересен нашим читателям.

Описание решения, присланное нашим клиентом:

С планомерным увеличением объемов клиентского трафика остро встал вопрос об уходе от схемы сбора трафика для СОРМ с использованием активного оборудования ядра сети в сторону использования пассивных оптических съемников.

Предыдущая схема была достаточно типовая - оборудование СОРМ подключалось непосредственно к Cisco 6500 двумя 10G интерфейсами. На Cisco настраивалось необходимое число RSPAN сессий с целью загнать весь трафик в определенный RSPAN VLAN. На этом же узле к данному RSPAN Vlan применялась VLAN Access map с целью отфильтровать интересующий трафик. В завершении, с помощью еще одной RSPAN сессии, трафик из RSPAN VLAN отправлялся в SPAN порты (2x10G) - непосредственно в СОРМ.

Очевидные минусы схемы - нагрузка на Cisco "лишним" SPAN трафиком, необходимостью его фильтрации.

При переходе к схеме с использованием оптических съемников возникает необходимость в агрегации большого числа 10G линков с последующей фильтрацией интересующего трафика на OSI L3-L4, так как текущая конфигурация СОРМ включает лишь два 10G интерфейса. Исходя из этих выводов, мы сформировали требования к коммутатору:

- хорошая 10G port density;
- L3-L4 ACL для switched трафика;
- наличие "базового" набора фич, таких как no mac address learning per port, QinQ Tunnel, Traffic Segmentation/Protected Port/Private VLAN;
- бюджетная цена ввиду нулевой доходности "проекта".

Таким образом, с помощью SNR-S4550 решаются следующие задачи:

- агрегация трафик с оптических съемников (6x10G портов на RX);
- фильтрация трафика, поступающего со съемников, перед отправкой в СОРМ.

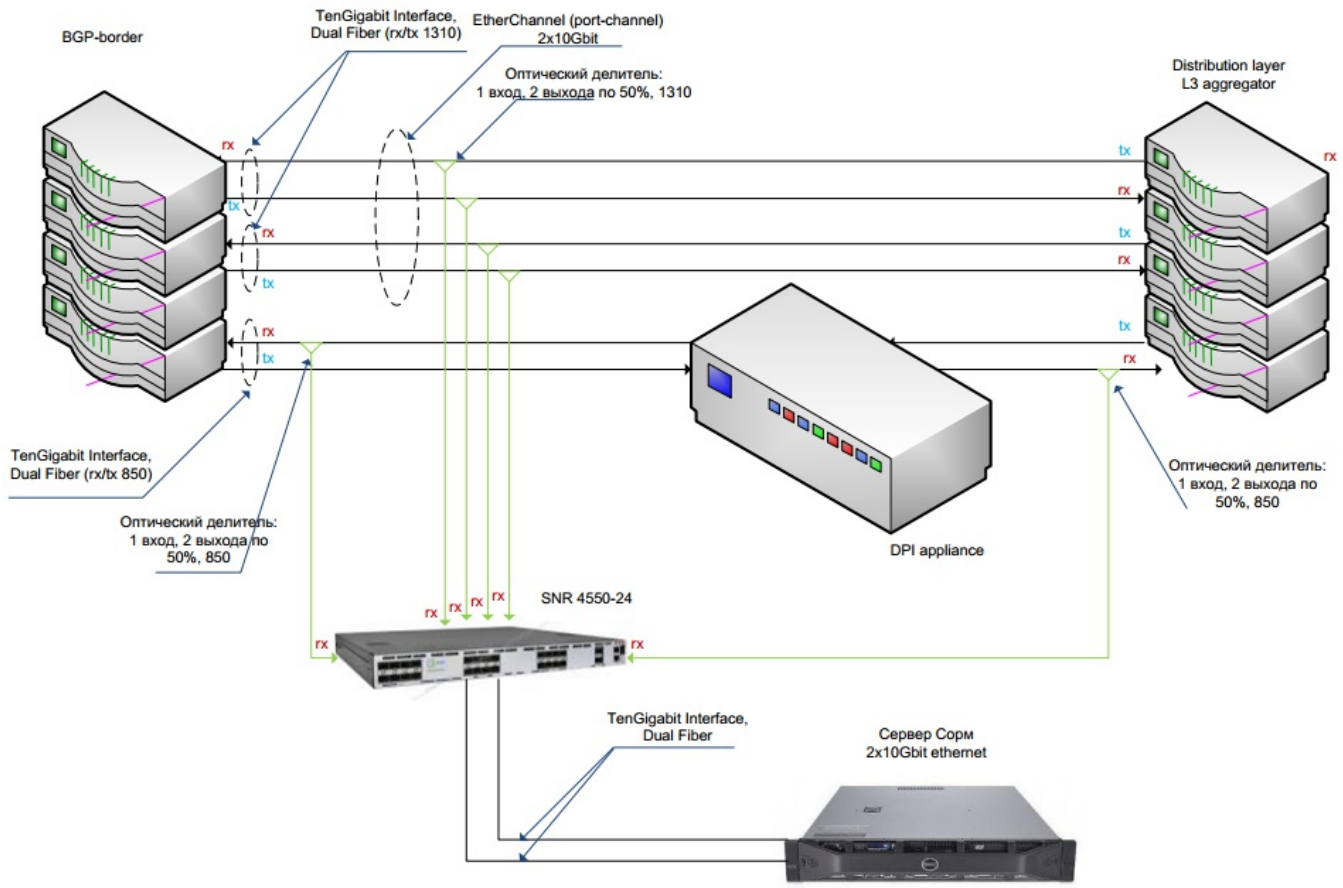


Схема подключения SNR-S4550-24XQ

Основные моменты конфигурации коммутатора SNR-S4550-24XQ:

1. Используем "mac-address-learning disable interface Ethernet " на всех RX портах, чтобы коммутатор не запоминал мак адреса в кадрах и производил широковещательную рассылку поступающих кадров.
2. Используем два VLAN (по числу TX портов) для группировки RX и TX портов в две группы (3 RX + 1 TX per group), чтобы широковещательная рассылка не дублировалась в оба TX порта.
3. Используем две "isolate-port group" с целью изолировать RX порты в каждом из VLAN друг от друга.
4. Используем ACL для фильтрации поступающего трафика.
5. Используем QinQ Tunnel что бы сохранить оригинальный VLAN id кадров, так же пропадает необходимость настраивать коммутатор под все возможные варианты VLANов в RX трафике.

Сам конфиг:

```
vlan 1000

name SormGroup1

!

vlan 2000

name SormGroup2

!

firewall enable

!

ip access-list extended Sorm

!
```

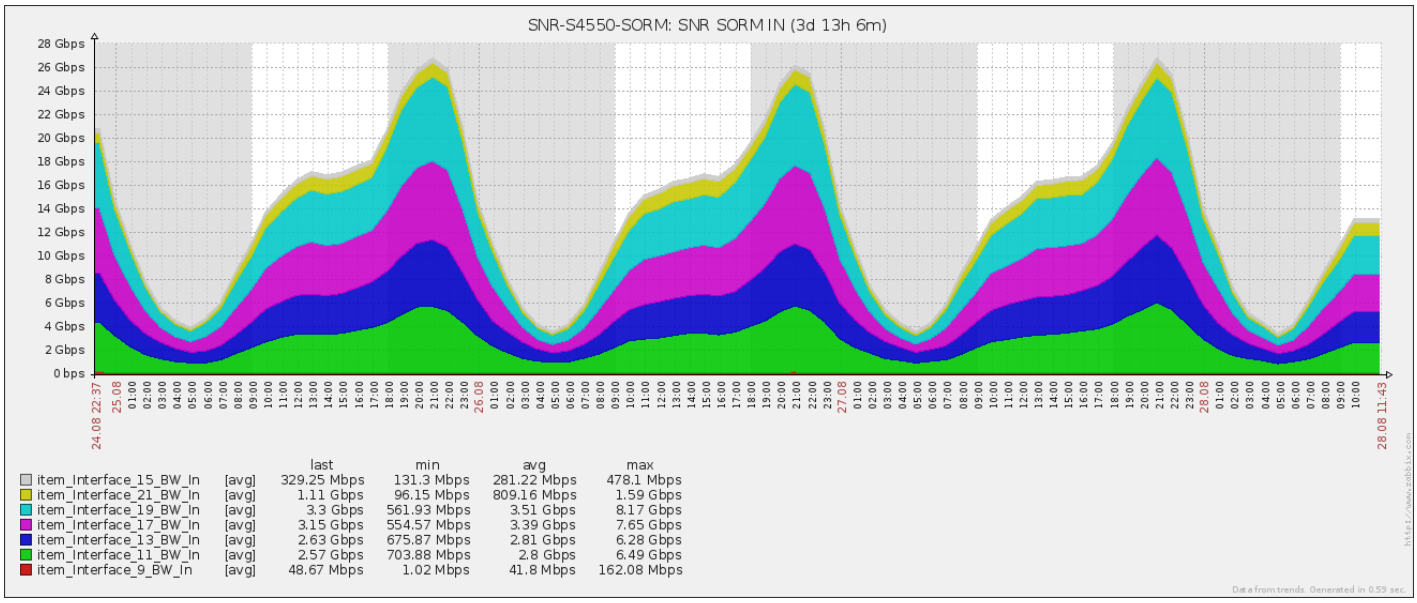
```
Interface Ethernet1/0/9
speed-duplex force1g-full
description SormInGroup1
dot1q-tunnel enable
switchport access vlan 1000
ip access-group Sorm in
!
Interface Ethernet1/0/10
description SormOutGroup1
dot1q-tunnel enable
switchport access vlan 1000
!
Interface Ethernet1/0/11
description SormInGroup1
dot1q-tunnel enable
switchport access vlan 1000
ip access-group Sorm in
!
Interface Ethernet1/0/13
description SormInGroup1
dot1q-tunnel enable
switchport access vlan 1000
ip access-group Sorm in
!
Interface Ethernet1/0/15
description SormInGroup1
transceiver-monitoring enable
dot1q-tunnel enable
switchport access vlan 1000
ip access-group Sorm in
!
Interface Ethernet1/0/17
description SormInGroup2
dot1q-tunnel enable
switchport access vlan 2000
ip access-group Sorm in
!
Interface Ethernet1/0/18
```

```
description SormOutGroup2
dot1q-tunnel enable
switchport access vlan 2000
!
Interface Ethernet1/0/19
description SormInGroup2
dot1q-tunnel enable
switchport access vlan 2000
ip access-group Sorm in
!
Interface Ethernet1/0/21
description SormInGroup2
transceiver-monitoring enable
dot1q-tunnel enable
switchport access vlan 2000
ip access-group Sorm in
!
mac-address-learning disable interface Ethernet1/0/9
mac-address-learning disable interface Ethernet1/0/10
mac-address-learning disable interface Ethernet1/0/11
mac-address-learning disable interface Ethernet1/0/13
mac-address-learning disable interface Ethernet1/0/15
mac-address-learning disable interface Ethernet1/0/17
mac-address-learning disable interface Ethernet1/0/18
mac-address-learning disable interface Ethernet1/0/19
mac-address-learning disable interface Ethernet1/0/21
!
isolate-port group SormGroup1 switchport interface Ethernet1/0/15
isolate-port group SormGroup1 switchport interface Ethernet1/0/13
isolate-port group SormGroup1 switchport interface Ethernet1/0/11
isolate-port group SormGroup1 switchport interface Ethernet1/0/9
isolate-port group SormGroup2 switchport interface Ethernet1/0/21
isolate-port group SormGroup2 switchport interface Ethernet1/0/19
isolate-port group SormGroup2 switchport interface Ethernet1/0/17
end
```

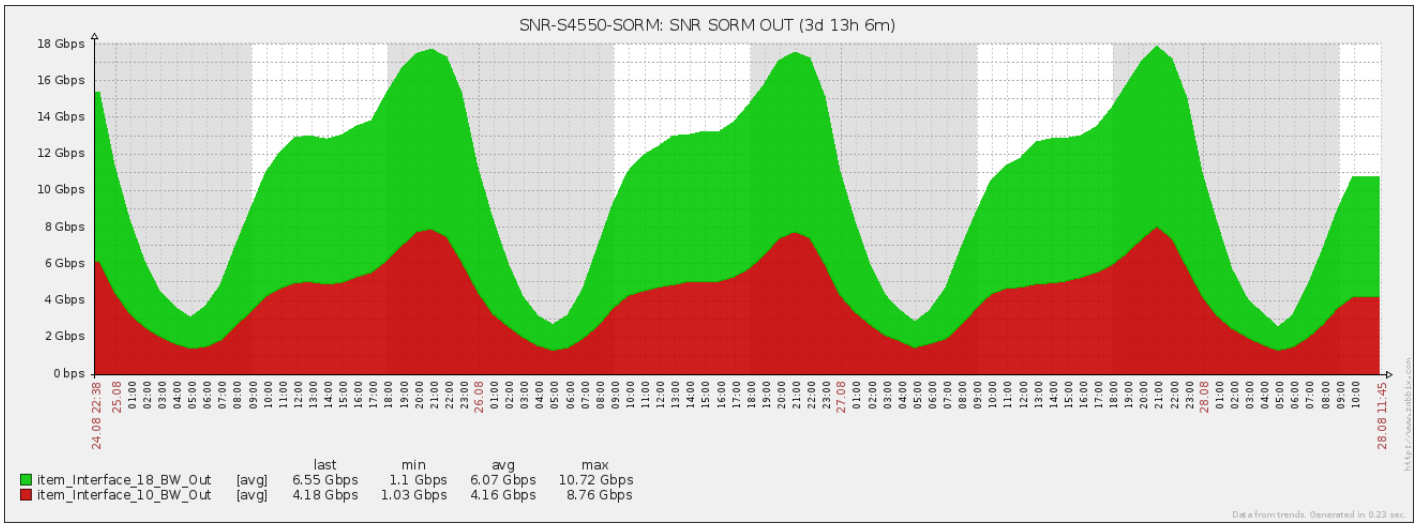
На вопрос "были ли какие-то сложности при внедрении решения?" получили ответ:

> Сложностей в настройке самого SNR не было, все предельно просто и понятно. С момента запуска проблем не возникало.

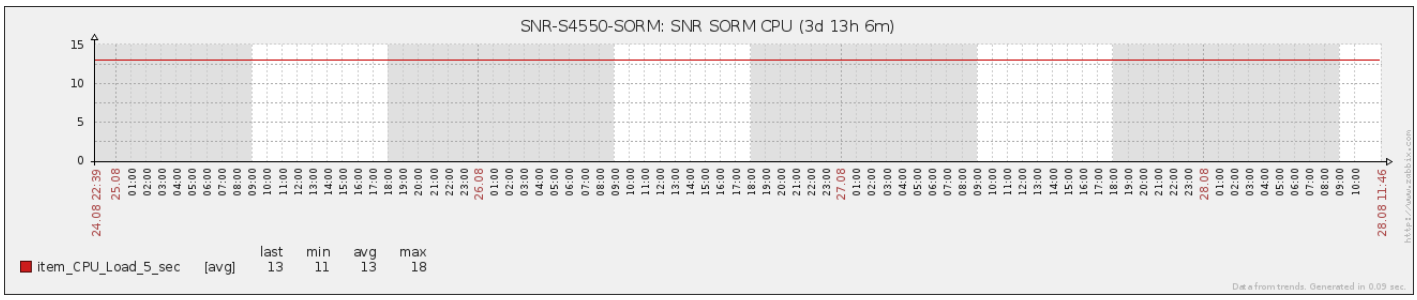
В дополнение графики загрузки портов и CPU SNR-S4550.



Порты со стороны оптических делителей



Порты со стороны СОРМ



Загрузка CPU