L2 VPN
для защиты филиальной сети

Всеволод Стамм

- Построение защищенного взаимодействия филиалов с ЦОД и почему выбрали L2 VPN
- Организация резервирования
- Возникшие проблемы, диагностика, опыт общения с поддержкой при критичном инциденте

Кого, как и чем защищаем

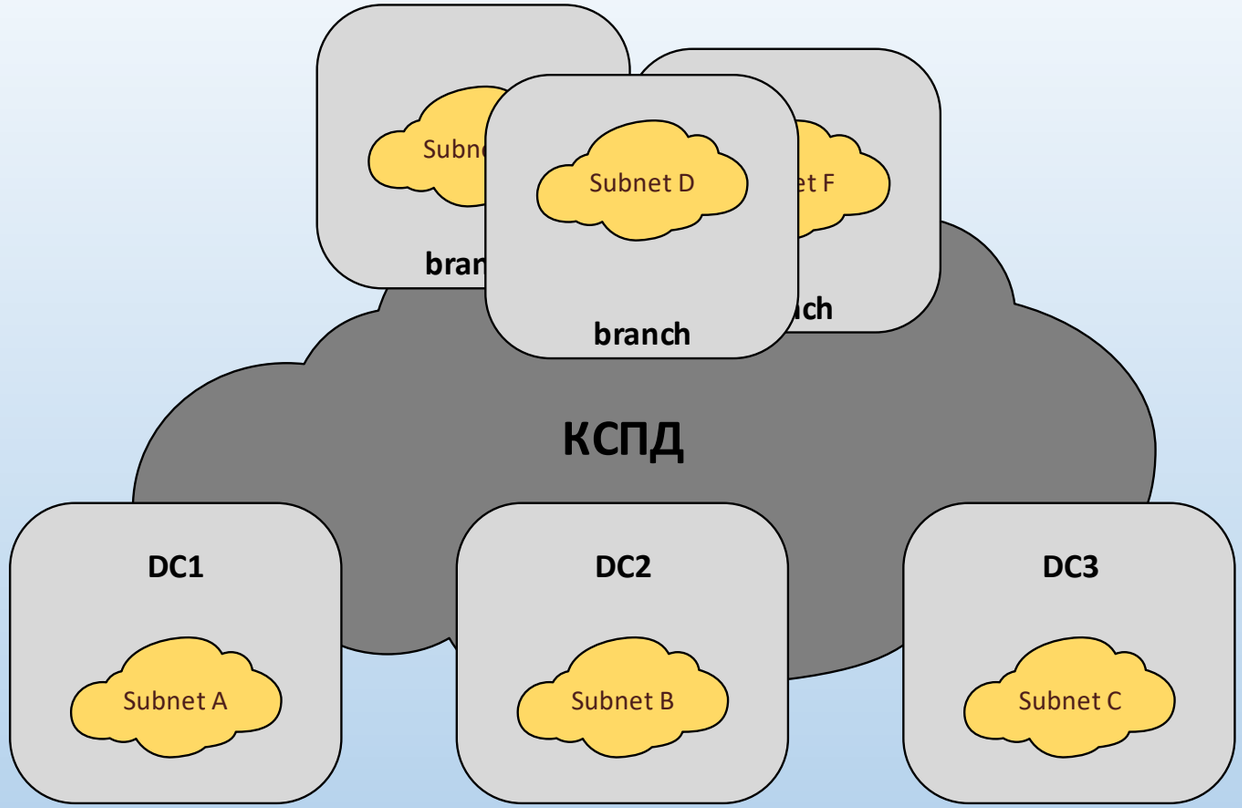
- Кого защищать? Если филиалов много
- Выбор в пользу L2 VPN
- Континент 3.9 – чем проще, тем лучше

Критерии выбора

- Наибольшее количество сотрудников (пользователей сервисов в ЦОД)
- Централизованные сервисы (взаимодействуют с сервисами в ЦОД)

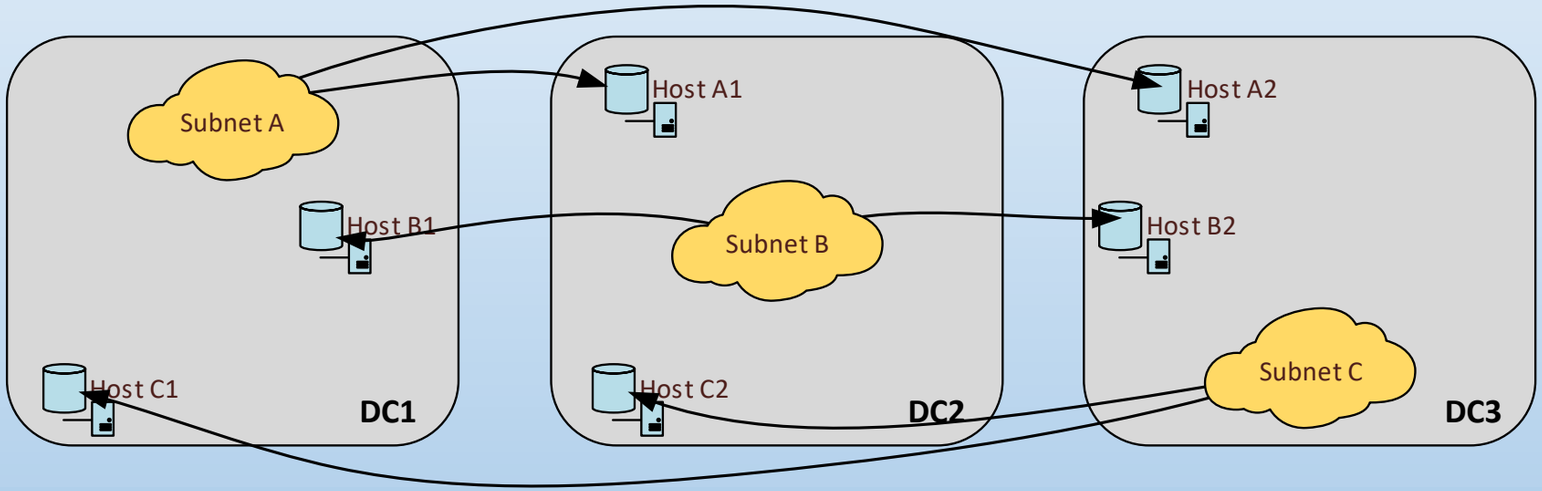
Структура филиалов

- Большое количество региональных филиалов и структурных подразделений филиалов
- Три ЦОД с централизованными сервисами



Миграция ВМ между ЦОД

- Домашний ЦОД – место где была создана виртуальная машина
- Гостевой ЦОД – место куда мигрирована виртуальная машина

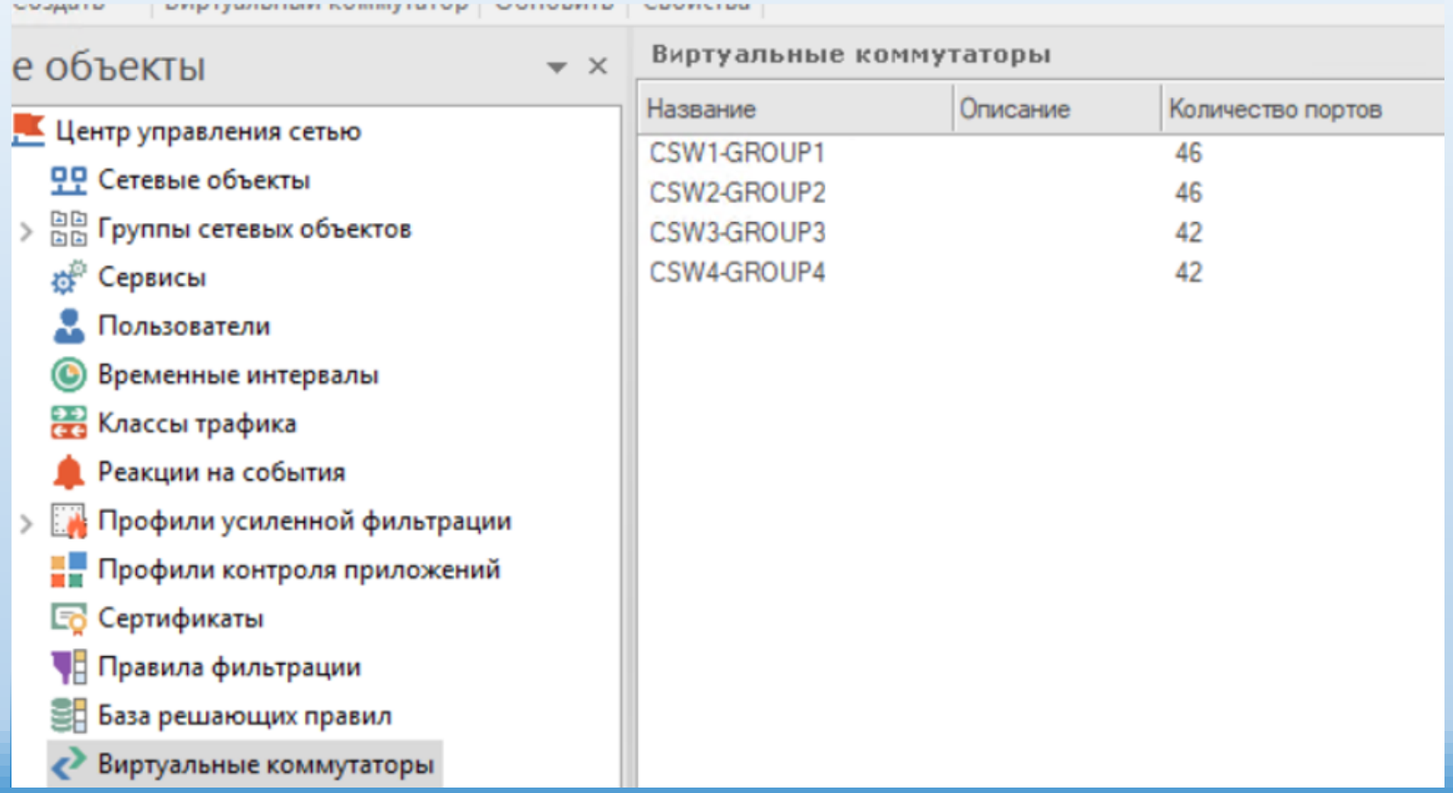


Плюсы Континет

- Визуальное создание топологи виртуального коммутатора
- Централизованная конфигурация криптокммутаторов
- Простая инициализация криптокоммутатора

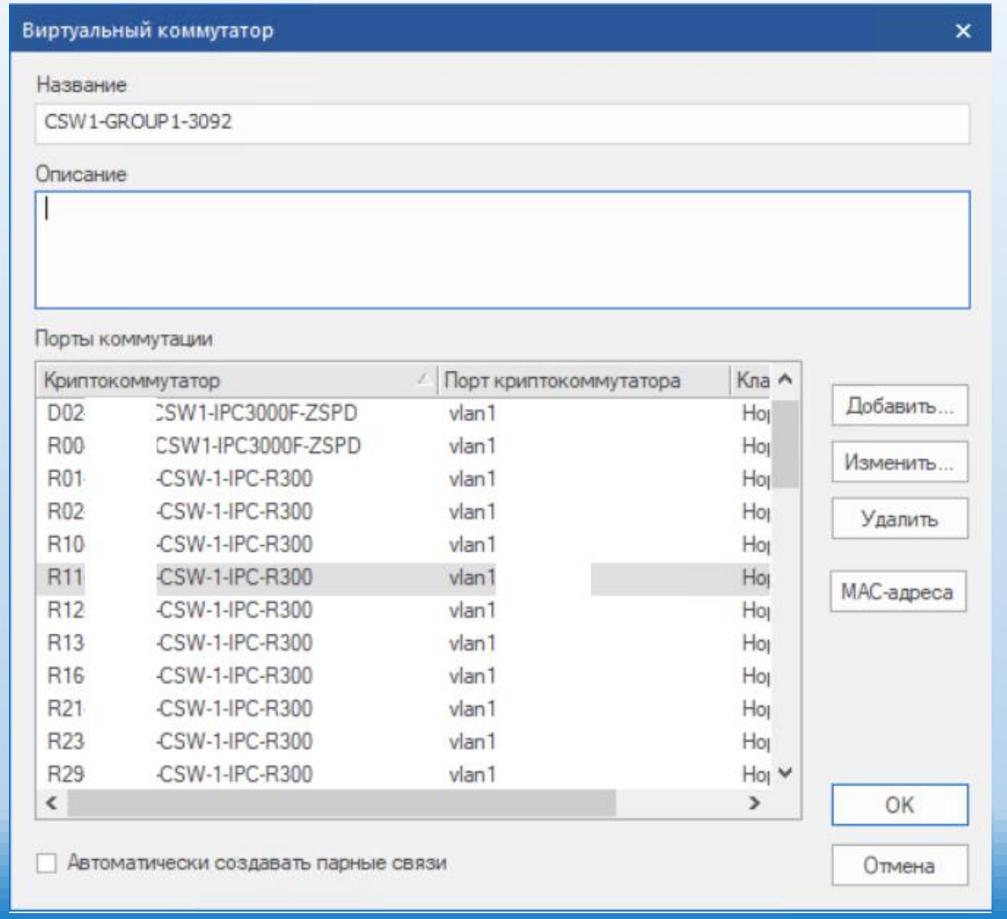
Визуальное создание топологи ВК

- Количество созданных ВК
- Количество портов в каждом ВК



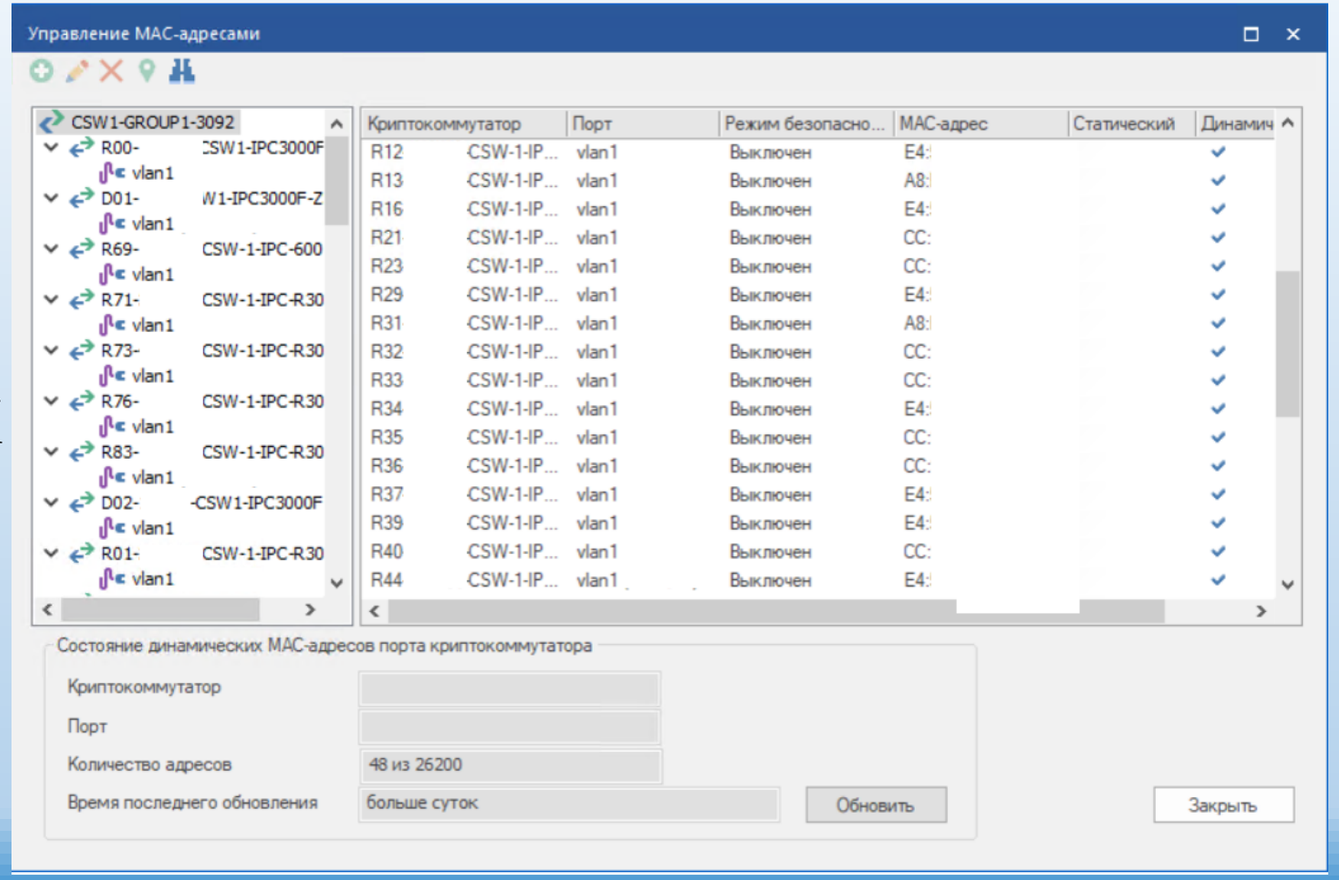
Визуальное создание топологи ВК

- Какие криптокоммутаторы добавлены в ВК
- Какие порты крипкокоммутаторов используются в ВК



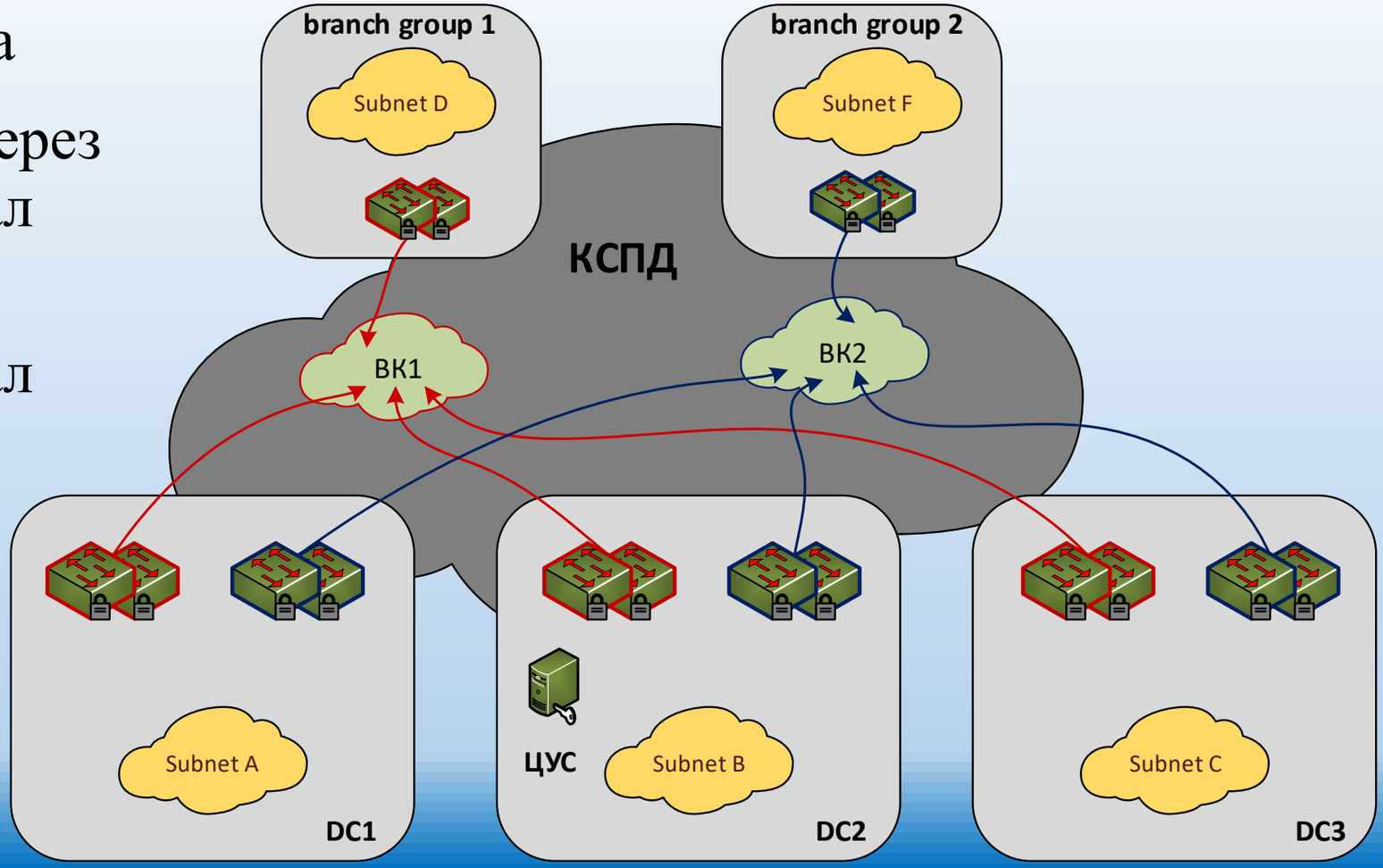
Визуальное создание топологи ВК

- Какое оборудование и его количество за каждым КК
- Общее количество адресов зарегистрированных на портах КК



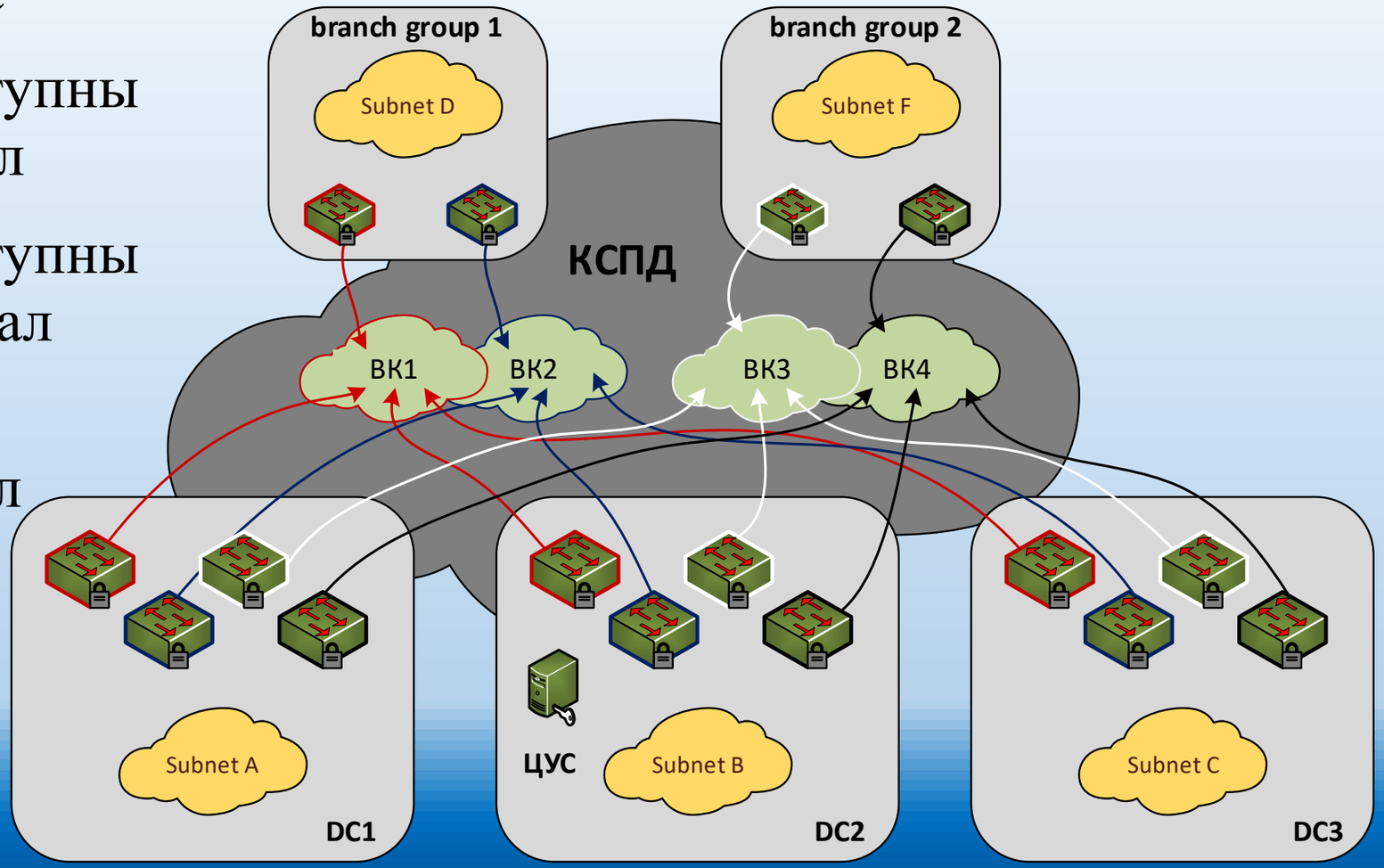
Начальная схема

- 2 виртуальных коммутатора
- ВК в филиалах доступны через основной и резервный канал
- ВК в ЦОД доступны через основной и резервный канал



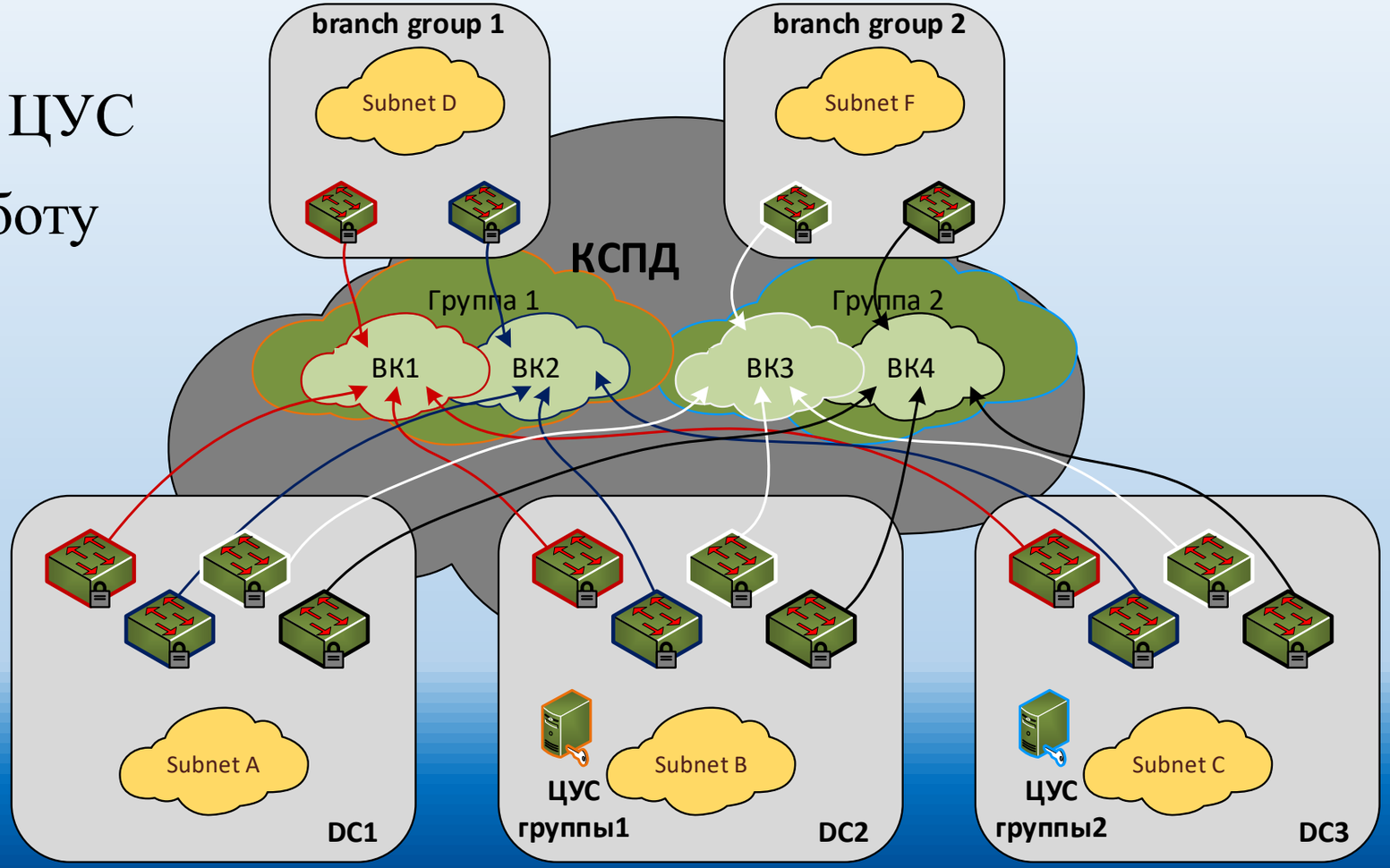
Итоговая схема

- 4 виртуальных коммутатора
- ВК1 и ВК3 в филиалах доступны только через основной канал
- ВК2 и ВК4 в филиалах доступны только через резервный канал
- ВК в ЦОД доступны через основной и резервный канал



Улучшение схемы

- 2 центра управления сетью
- Виртуальные коммутаторы поделены на группы между ЦУС
- Поломка ЦУС нарушает работу только одной из групп виртуальных коммутаторов



Обходим фрагментацию

- По КСПД не проходят фрагментированные ip-пакеты
- Увеличение MTU на внешних портах КК и на портах оборудования участвующего в пересылки шифрованного ip-пакета
- Настройка MSS для TCP трафика

Возникшие проблемы

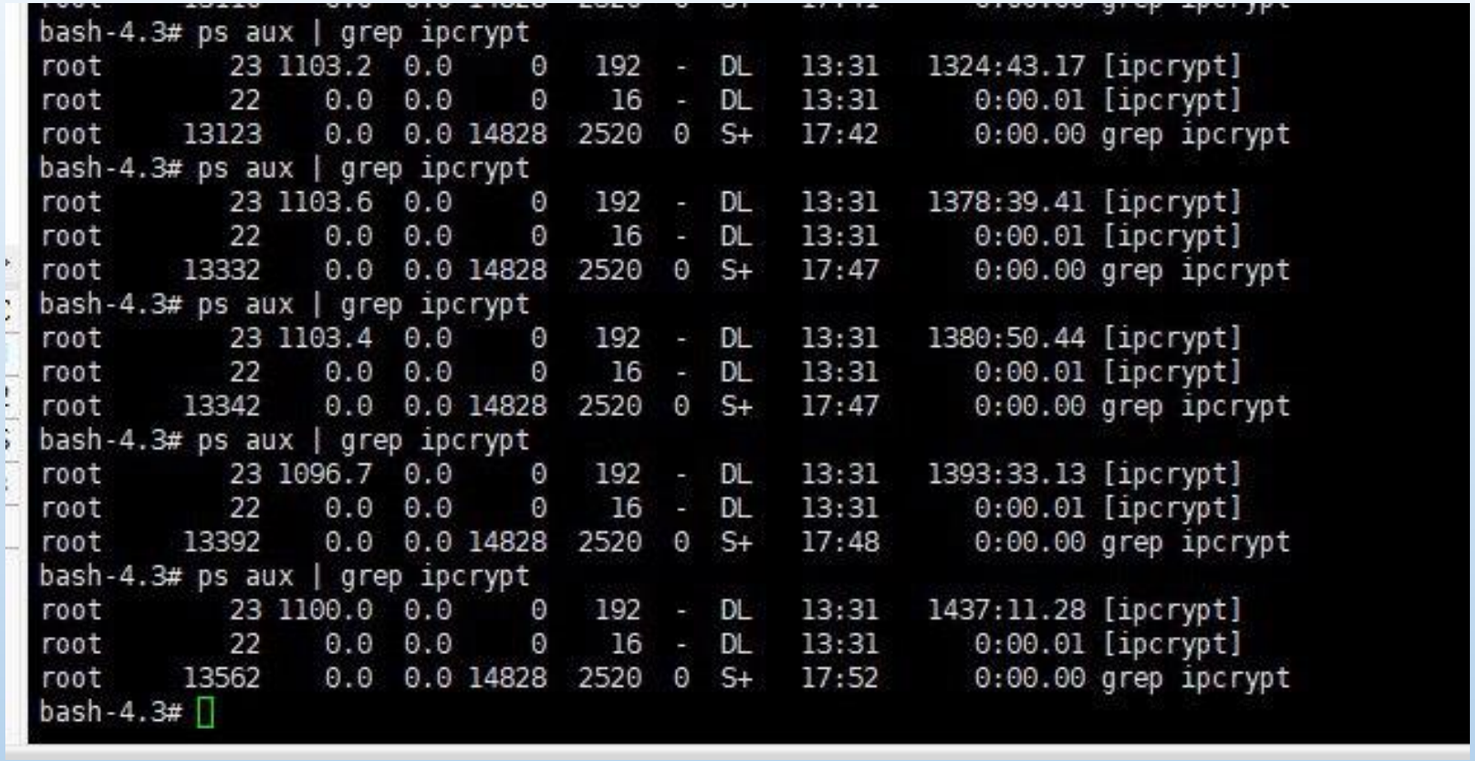
- Зависшие потоки шифрования
- В норме вместо 2048 должен быть 0

```
0 all/own/other 110126 17691 92435
bash-4.3# sysctl net.inet.ipcrypt | grep queue_s -A 15
net.inet.ipcrypt.queue_stats:
0 current/total/unorder 2048 28632956 6840413
1 current/total/unorder 2048 24354178 7493366
2 current/total/unorder 2048 12710407 625599
3 current/total/unorder 2048 1622019 42221
4 current/total/unorder 2048 8026763 300857
5 current/total/unorder 2048 12854659 443234
6 current/total/unorder 2048 34861136 1355297
7 current/total/unorder 2048 20697980 1215551
8 current/total/unorder 2048 13375587 439282
9 current/total/unorder 2048 2613315 108505
10 current/total/unorder 2048 2147407 119037
11 current/total/unorder 2048 7343041 948029

net.inet.ipcrypt.thread_stats:
0 all/own/other 1953141 360105 1593036
bash-4.3#
```

Возникшие проблемы

- Модуль шифрования работающий на пределе
- На цифре 1200 полный отказ в работе VPN



Причина проблемы

- Настройка MSS
- Флаг окончания списка опций (End Of Option List) в TCP
- RDP клиенты на iOS и macOS

Всем спасибо!