

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

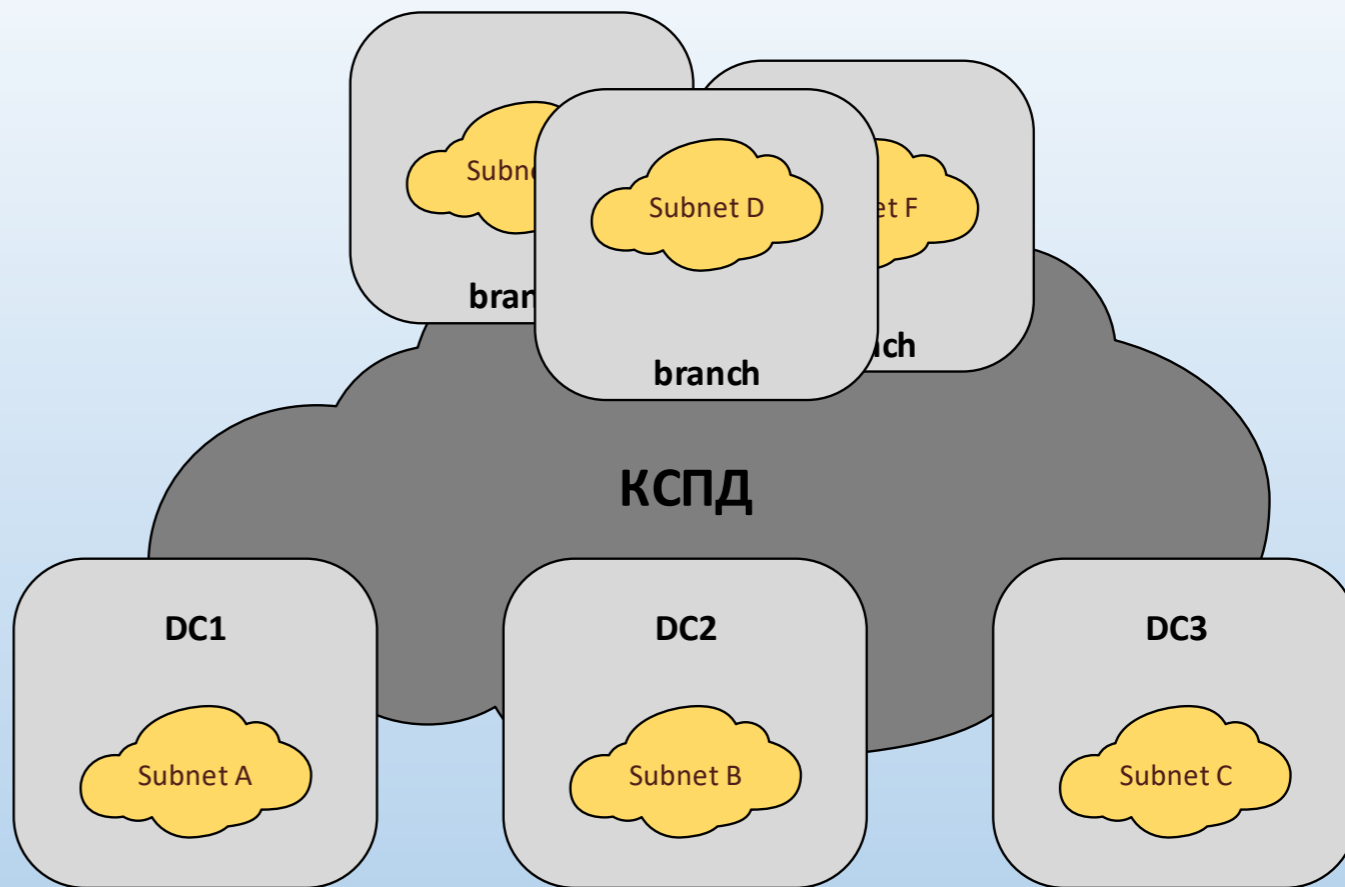
- Кого защищать? Если филиалов много
- Выбор в пользу L2 VPN
- Континент 3.9 – чем проще, тем лучше

Критерии выбора

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

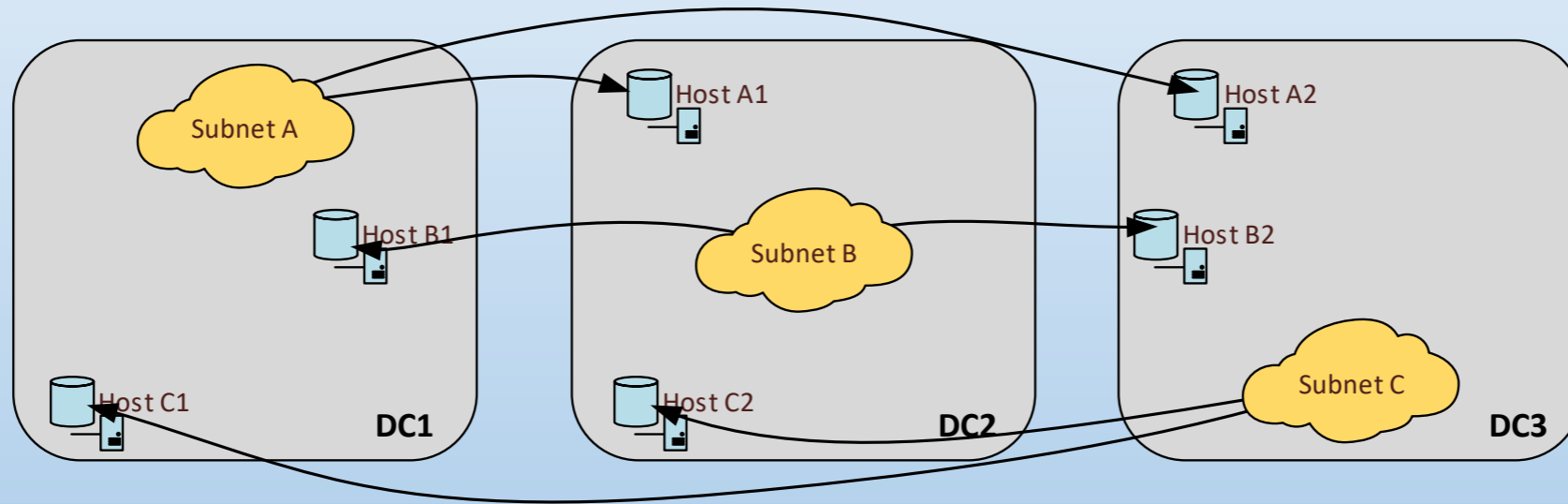
Структура филиалов

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



Миграция VM между ЦОД

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

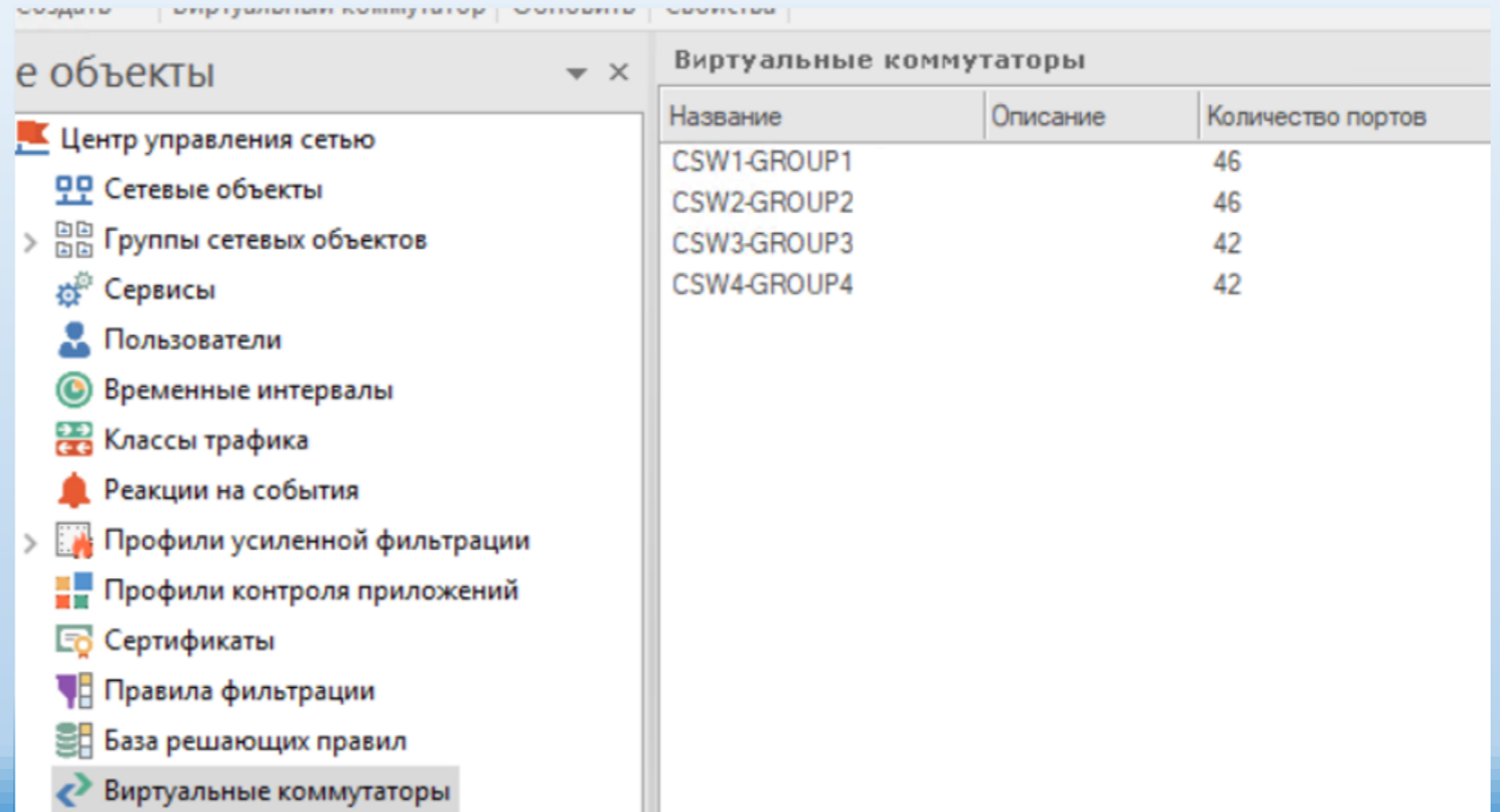


Плюсы Континет

- Визуальное создание топологии виртуального коммутатора
- Централизованная конфигурация криптокоммутаторов
- Простая инициализация криптокоммутатора

Визуальное создание топологии ВК

- Количество созданных ВК
- Количество портов в каждом ВК

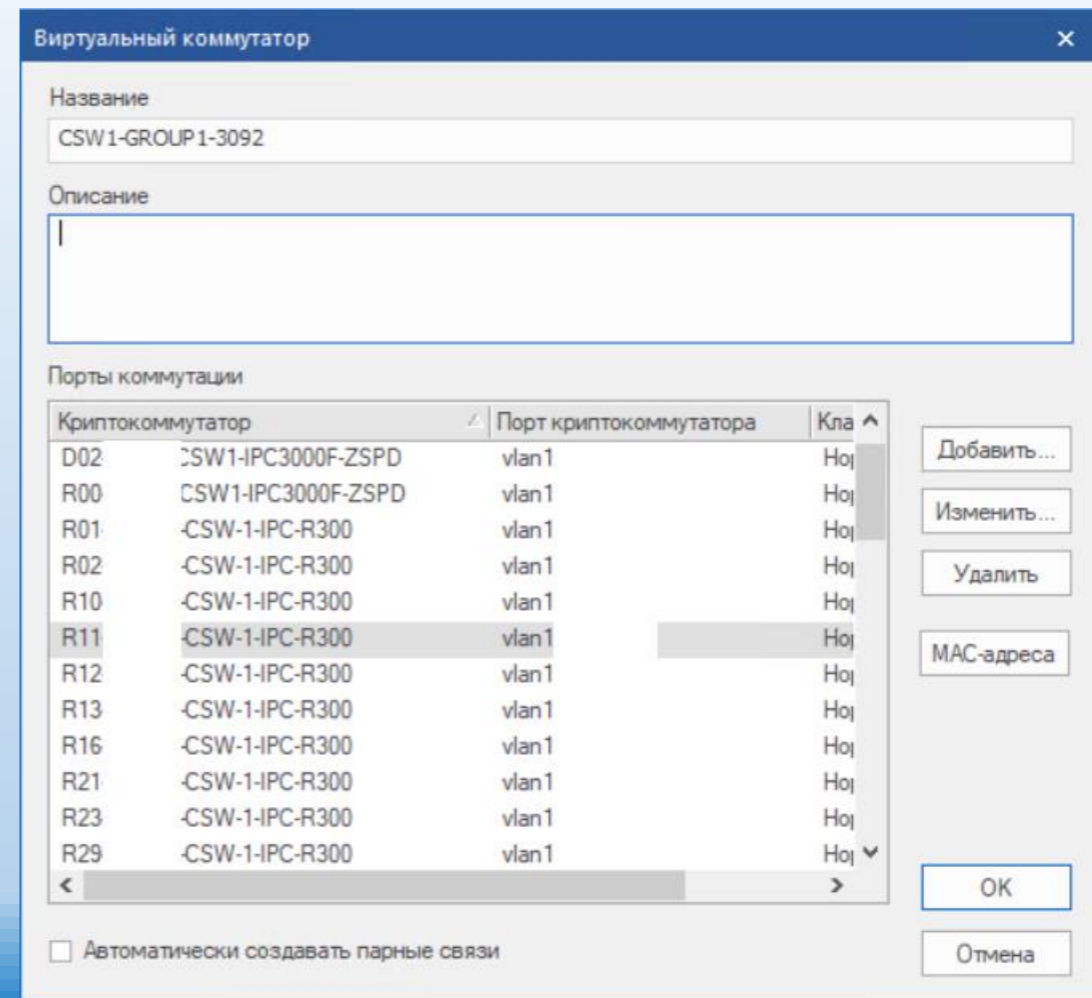


The screenshot shows a network management interface with a sidebar on the left and a main content area on the right. The sidebar is titled "е объекты" and contains a list of network management categories. The main content area is titled "Виртуальные коммутаторы" and displays a table with three columns: "Название", "Описание", and "Количество портов".

Название	Описание	Количество портов
CSW1-GROUP1		46
CSW2-GROUP2		46
CSW3-GROUP3		42
CSW4-GROUP4		42

Визуальное создание топологии ВК

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



Визуальное создание топологии ВК

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

Управление MAC-адресами

CSW1-GROUP1-3092

- ↔ R00- CSW1-IPC3000F
 - 🔗 vlan1
- ↔ D01- W1-IPC3000F-Z
 - 🔗 vlan1
- ↔ R69- CSW-1-IPC-600
 - 🔗 vlan1
- ↔ R71- CSW-1-IPC-R30
 - 🔗 vlan1
- ↔ R73- CSW-1-IPC-R30
 - 🔗 vlan1
- ↔ R76- CSW-1-IPC-R30
 - 🔗 vlan1
- ↔ R83- CSW-1-IPC-R30
 - 🔗 vlan1
- ↔ D02- -CSW1-IPC3000F
 - 🔗 vlan1
- ↔ R01- CSW-1-IPC-R30
 - 🔗 vlan1

Криптокоммутатор	Порт	Режим безопасно...	MAC-адрес	Статический	Динамич
R12	CSW-1-IP... vlan1	Выключен	E4:		✓
R13	CSW-1-IP... vlan1	Выключен	A8:		✓
R16	CSW-1-IP... vlan1	Выключен	E4:		✓
R21	CSW-1-IP... vlan1	Выключен	CC:		✓
R23	CSW-1-IP... vlan1	Выключен	CC:		✓
R29	CSW-1-IP... vlan1	Выключен	E4:		✓
R31	CSW-1-IP... vlan1	Выключен	A8:		✓
R32	CSW-1-IP... vlan1	Выключен	CC:		✓
R33	CSW-1-IP... vlan1	Выключен	CC:		✓
R34	CSW-1-IP... vlan1	Выключен	E4:		✓
R35	CSW-1-IP... vlan1	Выключен	CC:		✓
R36	CSW-1-IP... vlan1	Выключен	CC:		✓
R37	CSW-1-IP... vlan1	Выключен	E4:		✓
R39	CSW-1-IP... vlan1	Выключен	E4:		✓
R40	CSW-1-IP... vlan1	Выключен	CC:		✓
R44	CSW-1-IP... vlan1	Выключен	E4:		✓

Состояние динамических MAC-адресов порта криптокоммутатора

Криптокоммутатор:

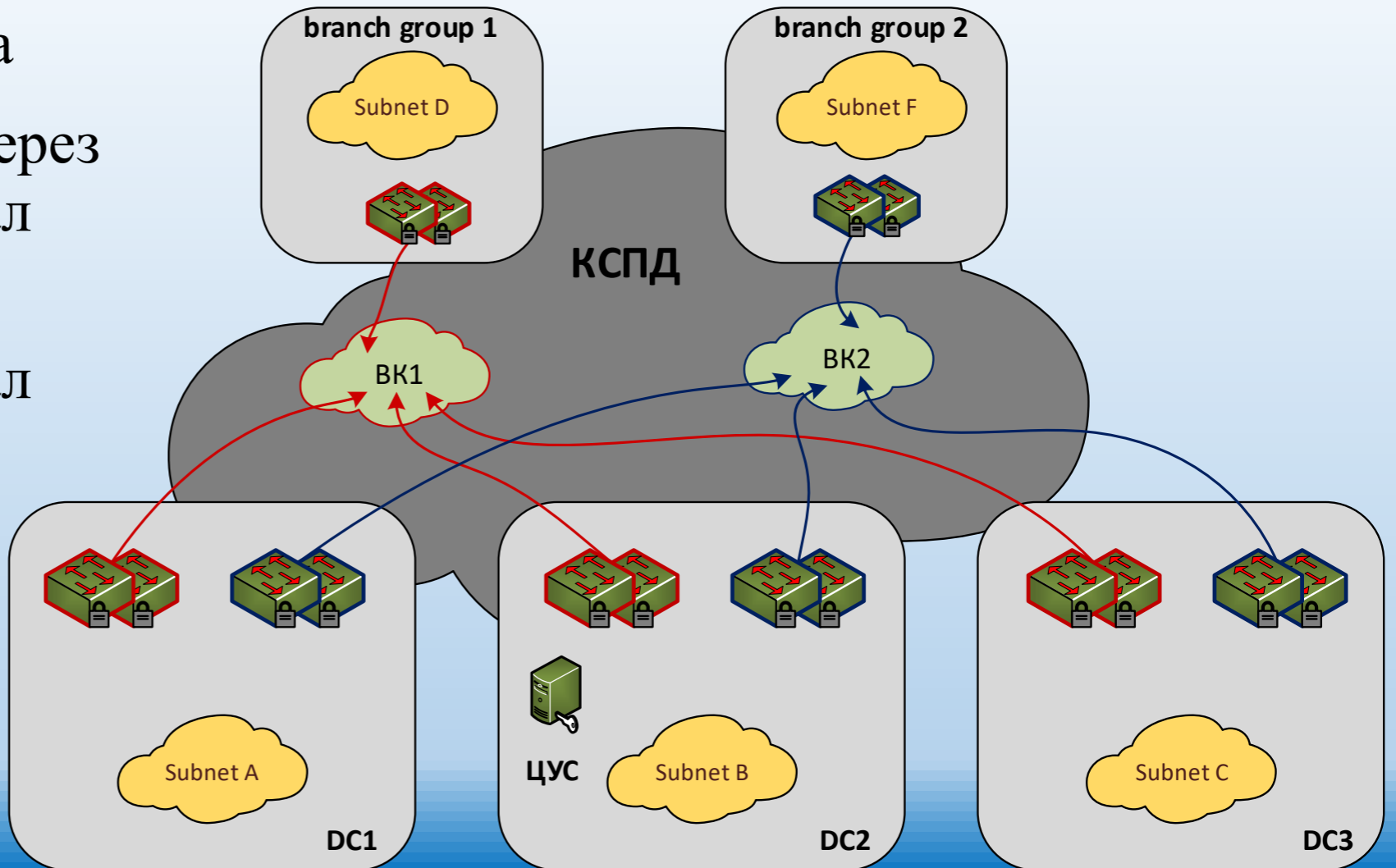
Порт:

Количество адресов: 48 из 26200

Время последнего обновления: больше суток

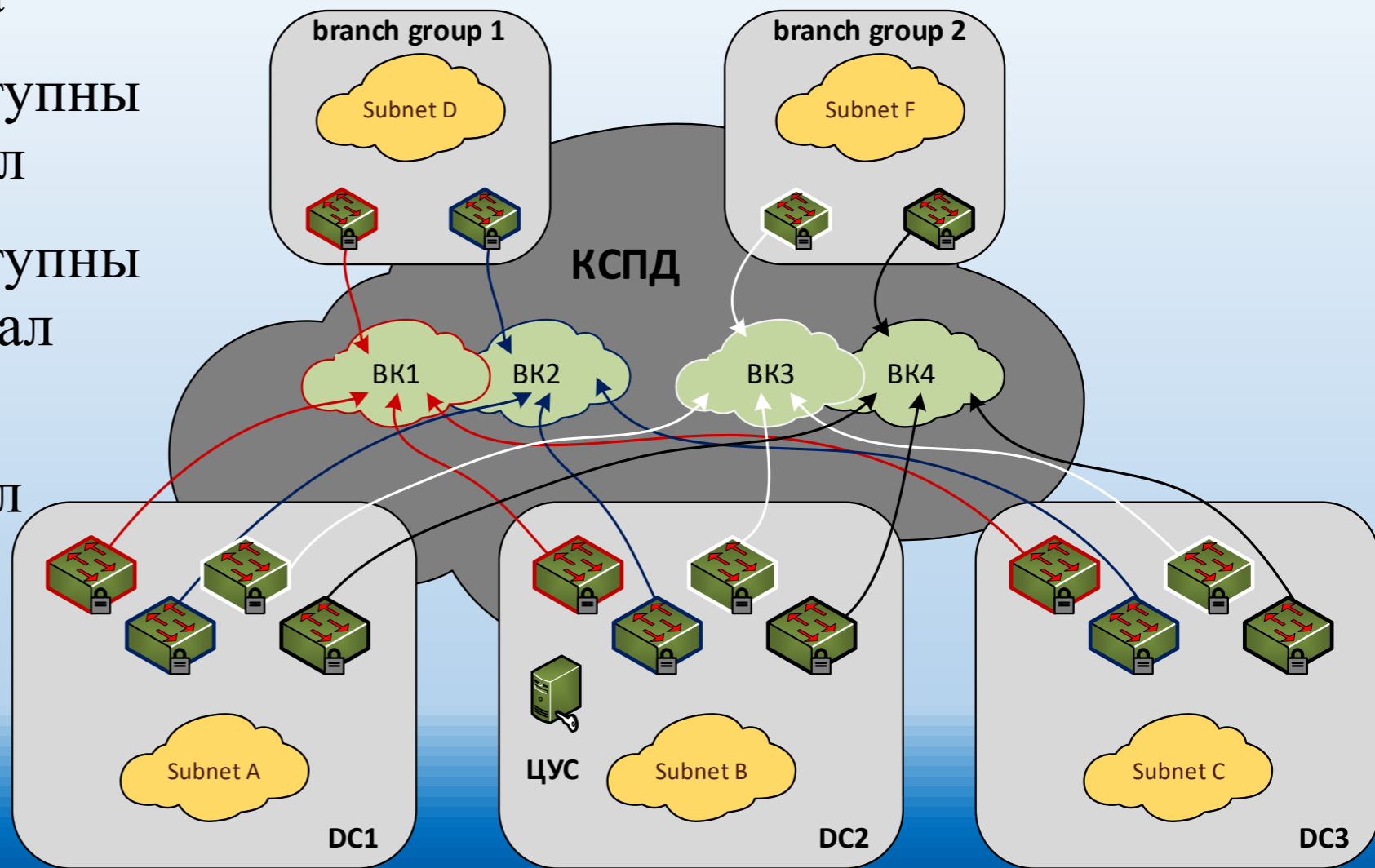
Начальная схема

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



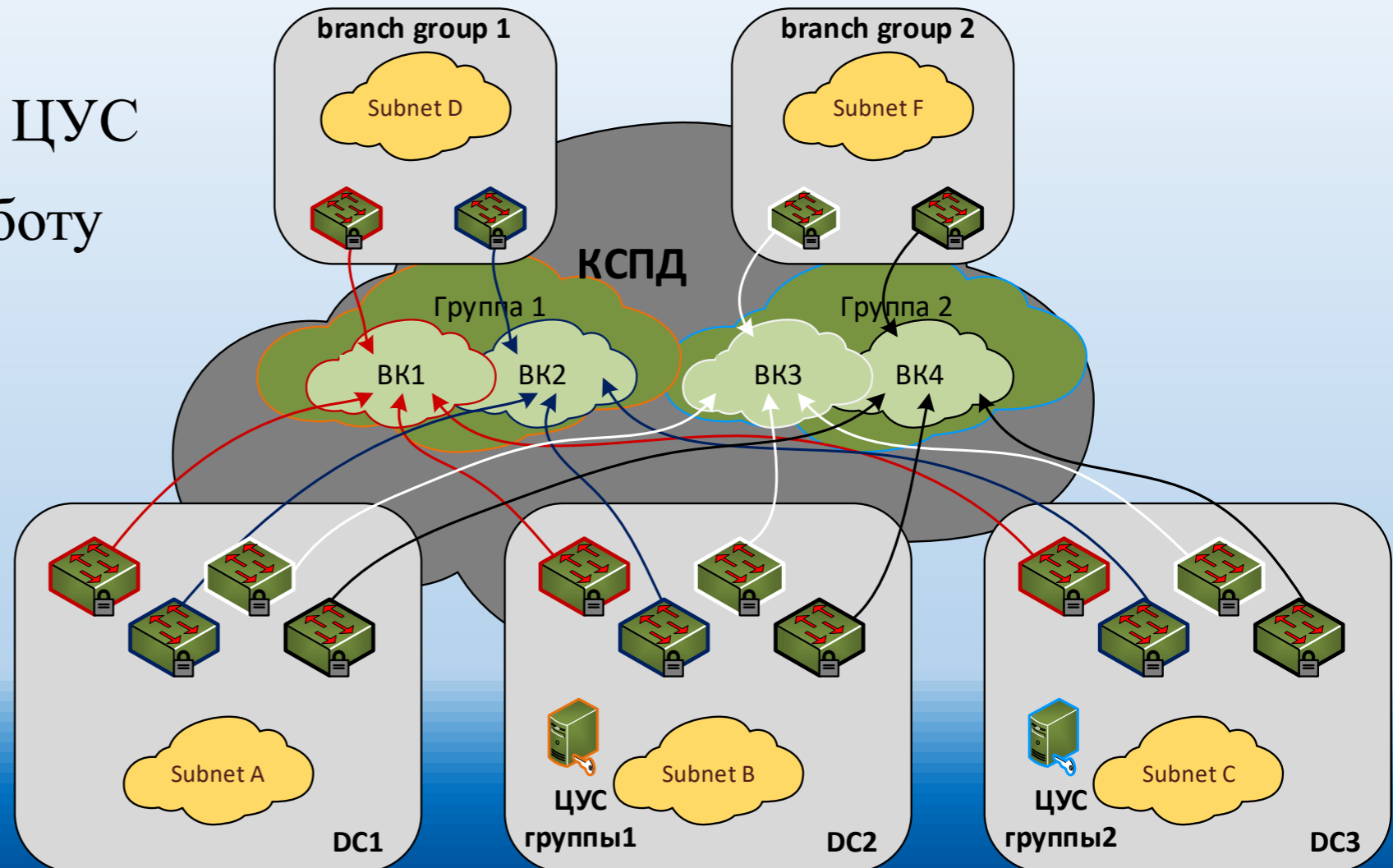
Итоговая схема

- 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

```
net.inet.ipcrypt.thread_stats:
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

```
bash-4.3# ps aux | grep ipcrypt
root      23 1103.2  0.0    0    192 -  DL  13:31  1324:43.17 [ipcrypt]
root      22    0.0  0.0    0    16 -  DL  13:31    0:00.01 [ipcrypt]
root    13123    0.0  0.0 14828 2520 0  S+  17:42    0:00.00 grep ipcrypt
bash-4.3# ps aux | grep ipcrypt
root      23 1103.6  0.0    0    192 -  DL  13:31  1378:39.41 [ipcrypt]
root      22    0.0  0.0    0    16 -  DL  13:31    0:00.01 [ipcrypt]
root    13332    0.0  0.0 14828 2520 0  S+  17:47    0:00.00 grep ipcrypt
bash-4.3# ps aux | grep ipcrypt
root      23 1103.4  0.0    0    192 -  DL  13:31  1380:50.44 [ipcrypt]
root      22    0.0  0.0    0    16 -  DL  13:31    0:00.01 [ipcrypt]
root    13342    0.0  0.0 14828 2520 0  S+  17:47    0:00.00 grep ipcrypt
bash-4.3# ps aux | grep ipcrypt
root      23 1096.7  0.0    0    192 -  DL  13:31  1393:33.13 [ipcrypt]
root      22    0.0  0.0    0    16 -  DL  13:31    0:00.01 [ipcrypt]
root    13392    0.0  0.0 14828 2520 0  S+  17:48    0:00.00 grep ipcrypt
bash-4.3# ps aux | grep ipcrypt
root      23 1100.0  0.0    0    192 -  DL  13:31  1437:11.28 [ipcrypt]
root      22    0.0  0.0    0    16 -  DL  13:31    0:00.01 [ipcrypt]
root    13562    0.0  0.0 14828 2520 0  S+  17:52    0:00.00 grep ipcrypt
bash-4.3#
```


Причина проблемы

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

Всем спасибо!