Network Engineer. Basic

Построение отказоустойчивой корпоративной сети.

Меня хорошо видно & слышно?

Защита проекта
Тема: Построение отказоустойчивой корпоративной сети.

Алексей К

План защиты

- Цель и задачи проекта
- Какие технологии использовались
- Что получилось
- Выводы
- Вопросы и рекомендации

Цель и задачи проекта

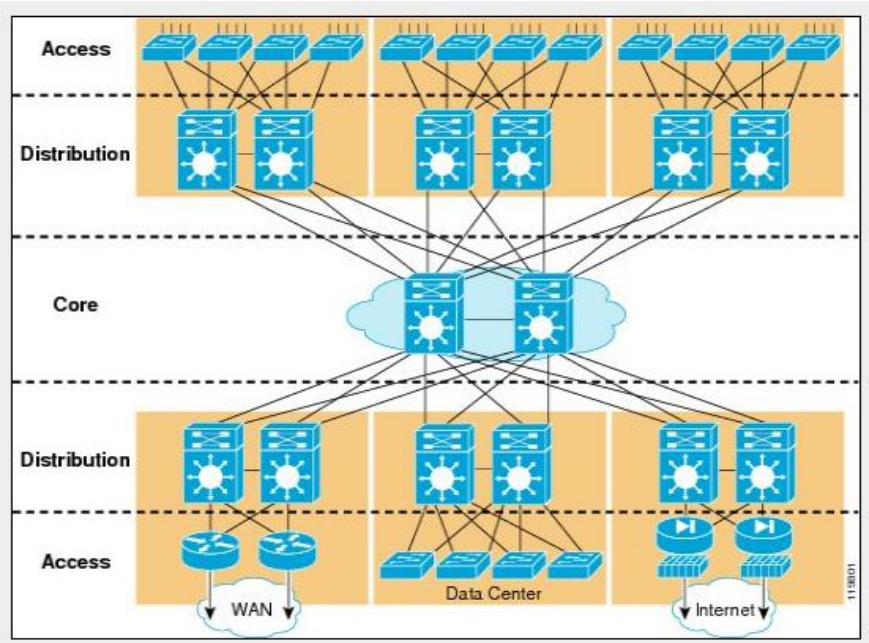
Обеспечение непрерывности работы сети, минимизация простоев и прерываний бизнес-процессов.

1.	Резервирование критических компонентов
2.	Реализация отказоустойчивых топологий
3.	Мониторинг и управление
4.	Безопасность инфраструктуры

Какие технологии использовались

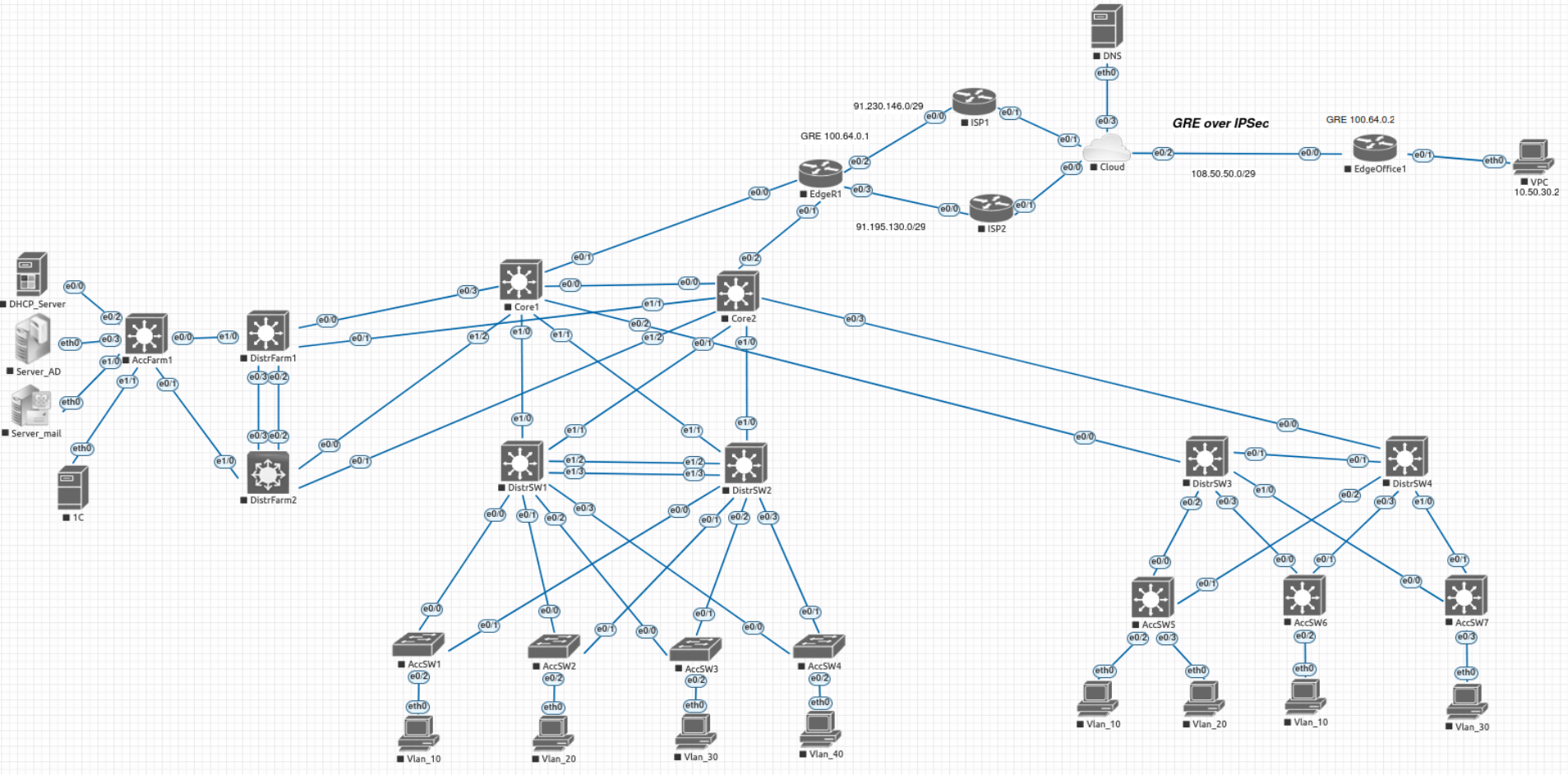
1	VLAN, STP, Trunk, EtherChannel, FHRP, DHCP
2	Inter VLAN routing; динамическая, статическая маршрутизация
3	PAT, ACL, ip sla, track, EEM (Cisco Embedded Event Manager)
4	GRE Over IPSec, port-security, DHCP snooping, bpdu guard, storm control,

Трехуровневая модель организации сети



- Уровень ядра (Core) – отвечает за быстрый транспорт между уровнями распределения, большой трафик, мощное оборудование
- Уровень распределения (Distribution) – обеспечение маршрутизации, фильтрации, QOS, суммирование маршрутов, ACL, PBR. Аккумулирование каналов LAN, WAN.
- Уровень доступа (Access) – подключение к рабочим станциям и серверам, высокая доступность, безопасноть портов

Общая структура сети

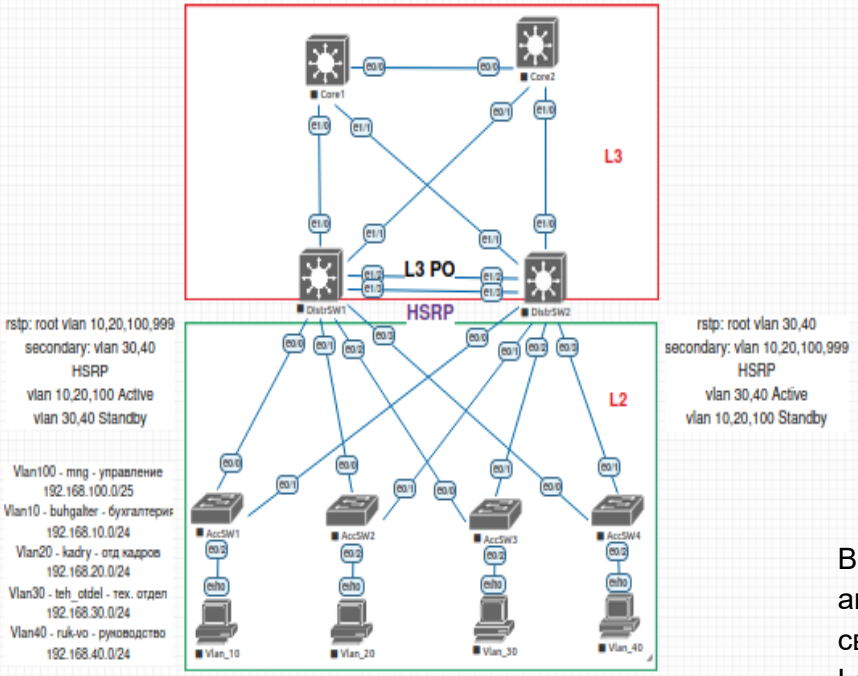


Краткий ip план

Префикс	VLAN №	VLAN name	Шлюз	Примечание
192.168.0.0/17 (Абонентская сеть 1)				
192.168.10.0/24	10	buhgaler	192.168.10.1 (HSRP)	Area 1
192.168.20.0/24	20	kadry	192.168.20.1 (HSRP)	
192.168.30.0/24	30	teh_otdel	192.168.30.1 (HSRP)	
192.168.40.0/24	40	Ruk-vo	192.168.40.1 (HSRP)	
192.168.100.0/24	100	management	192.168.100.1 (HSRP)	
	666	PL		
	999	Native		
192.168.128.0/19 (Абонентская сеть 2)				
192.168.128.0/24	10	ekonomist	192.168.128.1	Area 2
192.168.129.0/24	20	otd_prodaz	192.168.129.1	
192.168.130.0/24	10	it	192.168.130.1	
192.168.131.0/24	30	wi-fi_users_DHCP	192.168.131.1	
	666	PL		
172.16.1.0/24 (Серверная ферма)				
172.16.1.2/27	10	DHCP_Server	172.16.1.1	Area 3
172.16.1.34/29	11	AD_Server	172.16.1.33	
172.16.1.42/29	12	Mail_server	172.16.1.41	
172.16.1.50/29	13	1C	172.16.1.49	
10.0.0.0/24				p2p area 0
10.10.10.0/24				Loop area 0
10.0.1.0/24				p2p area 1
10.10.11.0/24				Loop area 1
10.0.2.0/24				p2p area 2
10.10.12.0/24				Loop area 2
10.0.3.0/24				p2p area 3
10.10.13.0/24				Loop area 3
10.64.100.0/24				GRE
91.230.146.0/29				ISP1
91.195.130.0/29				ISP1

Рассмотрим каждый из блоков по отдельности

Модель 1: Layer 2 – Loop-Free Topology (Distr L3, Acess L2)



- Сеть сегментирована на VLAN по отделам
- Один VLAN на один коммутатор доступа (отсутствие пересекающихся VLAN)
- Между distribution - канал L3 (EtherChannel) для избежания замкнутого контура L2
- RSTP root primary и secondary на distribution
- FHRP (HSRP,VRRP, GLBP) на distribution. В данном случае используется HSRP . Для VLAN 10,20,100,999 Active HSRP DistrSW1, для VLAN 30,40 Active HSRP DistrSW2 (небольшая балансировочка). Настройка приоритетного вытеснения, уменьшение таймеров.

В случае пересекающихся VLAN, при выходе из строя одного из аплинков в сторону distribution, может получиться, что одни из access свитчей станет транзитным.В таком случае возможно использовать Looped Topology. При этом, линк между distribution будет L2. Кроме того, увеличивается широковещательный домен. Ну и конечно же, работа STP здесь в полный рост.

Модель 1: настройка Trunk, RSTP, EtherChannel, HSRP.

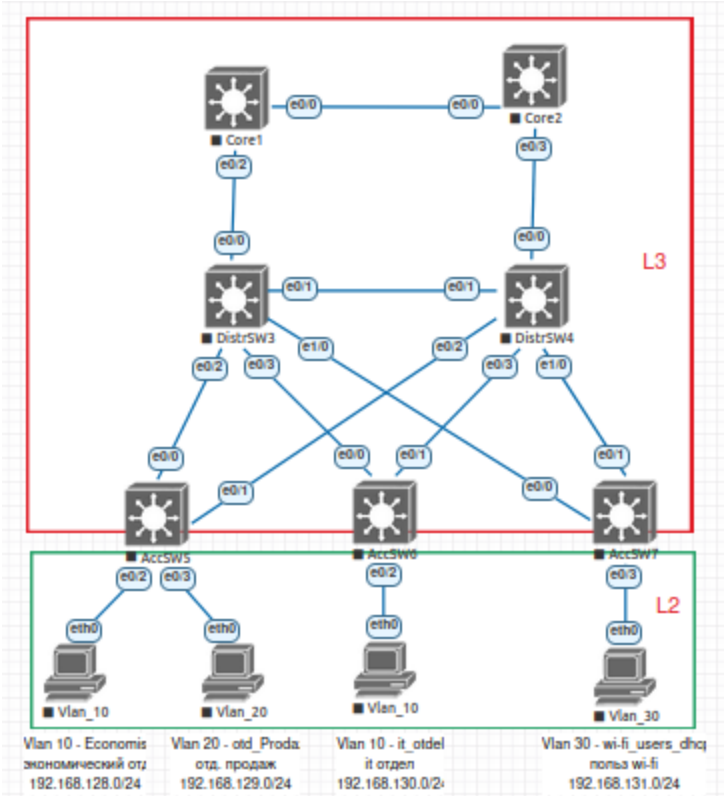
```
interface Loopback0
 ip address 10.10.10.1 255.255.255.255
 ip ospf 1 area 0
!
interface Port-channel1
 description LINK_PO1_DISTRSW2
 no switchport
 ip address 10.0.1.21 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 1 area 1
!
interface Ethernet0/0
 description LINK_ACCSW1
 switchport trunk allowed vlan 10,100,999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Ethernet0/1
 description LINK_ACCSW2
 switchport trunk allowed vlan 20,100,999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Ethernet0/2
 description LINK_ACCSW3
 switchport trunk allowed vlan 30,100,999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Ethernet0/3
 description LINK_ACCSW4
 switchport trunk allowed vlan 40,100,999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Ethernet1/0
 description LINK_CORE1
 no switchport
 ip address 10.0.0.1 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 1 area 0
!
interface Ethernet1/1
 description LINK_CORE2
 no switchport
 ip address 10.0.0.9 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 1 area 0
!
interface Ethernet1/2
 description LINK_PO1_DISTRSW2
 no switchport
 no ip address
 channel-group 1 mode active
!
interface Ethernet1/3
 description LINK_PO1_DISTRSW2
 no switchport
 no ip address
 channel-group 1 mode active
```

```
interface Vlan20
 description HSRP_VL20_KADRY
 ip address 192.168.20.253 255.255.255.0
 standby version 2
 standby 20 ip 192.168.20.1
 standby 20 timers msec 200 msec 750
 standby 20 priority 120
 standby 20 preempt delay minimum 90
 ip ospf hello-interval 3

DistrSW1#sh standb bri
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl10        10   120 P Active  local           192.168.10.254  192.168.10.1
Vl20        20   120 P Active  local           192.168.20.254  192.168.20.1
Vl30        30   100   Standby 192.168.30.254  local           192.168.30.1
Vl40        40   100   Standby 192.168.40.254  local           192.168.40.1
Vl100       100  120 P Active  local           192.168.100.126 192.168.100.1
DistrSW1#
```

```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 10,20,100,999 priority 24576
spanning-tree vlan 30,40 priority 28672
!
```

```
DistrSW1#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------
1    default                          active
10   buh                              active
20   kadry                            active
30   teh_otdel                        active
40   ruk-vo                           active
100  mng                              active
999  native                           active
1002 fddi-default                     act/unsup
```

Модель 2: Access L3



- Более приоритетное решение
- Сеть полностью маршрутизируемая
- Каждый коммутатор доступа настроен на уникальный VLAN
- Шлюз по умолчанию и корневой мост перемещается на уровень доступа
- Отсутствие FHRP, STP.
- Динамическая балансировка трафика
- Минимальное время конвергенции

- На схеме представлена сегментация сети, адресация конечных устройств статическая. Для VLAN 30 – пользователи WI-FI (DHCP, сервер DHCP в серверной ферме)

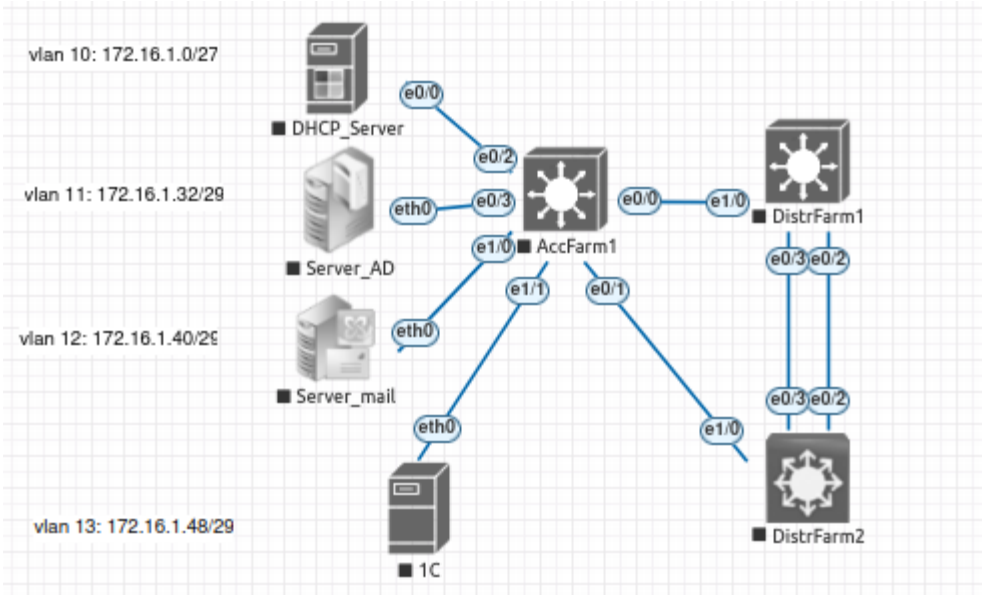
Модель 2: настройка Access L3.

```
interface Loopback0
 ip address 10.10.12.3 255.255.255.255
 ip ospf 2 area 2
!
interface Ethernet0/0
 description LINK_DISTRSW3
 no switchport
 ip address 10.0.2.14 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 2 area 2
!
interface Ethernet0/1
 description LINK_DISTRSW4
 no switchport
 ip address 10.0.2.18 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 2 area 2
!
interface Ethernet0/2
 switchport access vlan 666
 switchport mode access
 shutdown
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Ethernet0/3
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Vlan30
 description WI-FI_USERS_DHCP
 ip address 192.168.131.1 255.255.255.0
 ip helper-address 172.16.1.2
 ip ospf 2 area 2
!
router ospf 2
 router-id 10.10.12.3
 area 2 stub no-summary
 passive-interface default
 no passive-interface Ethernet0/0
 no passive-interface Ethernet0/1
!
```

```
AccSW7#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
30   WI-FI_USERS_DHCP                 active    Et0/3
666  PL                               active    Et0/2
```

```
VPCS> ip dhcp
DORA IP 192.168.131.2/24 GW 192.168.131.1

VPCS> sh ip

NAME        : VPCS[1]
IP/MASK     : 192.168.131.2/24
GATEWAY     : 192.168.131.1
DNS         : 8.8.8.8
DHCP SERVER : 172.16.1.2
DHCP LEASE  : 86379, 86400/43200/75600
MAC         : 00:50:79:66:68:17
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500

VPCS>
```

Блок: Серверная ферма



- Коммутатор AccFarm1 L3 соединен избыточными связями с DistrFarm1 и DistrFarm2 L3.
- Между DistrFarm1 и DistrFarm2 L3 EtherChannel (PAgP)
- Сервера DHCP, AD, mail, 1C и другие

```
AccFarm1#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   DHCP_Server                      active
11   SERVER_AD                        active    Et0/3
12   SERVER_MAIL                      active    Et1/0
13   1C                               active    Et1/1
666  PL                               active    Et1/2, Et1/3
```

```
interface Loopback0
 ip address 10.10.10.7 255.255.255.255
 ip ospf 3 area 0
!
interface Port-channel1
 description LINK_PO1_DISTRFARM2
 no switchport
 ip address 10.0.3.1 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 3 area 3
!
interface Ethernet0/0
 description LINK_CORE1
 no switchport
 ip address 10.0.0.46 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 3 area 0
!
interface Ethernet0/1
 description LINK_CORE2
 no switchport
 ip address 10.0.0.54 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 3 area 0
!
interface Ethernet0/2
 description LINK_PO1_DISTRFARM2
 no switchport
 no ip address
 channel-group 1 mode active
!
interface Ethernet0/3
 description LINK_PO1_DISTRFARM2
 no switchport
 no ip address
 channel-group 1 mode active
!
interface Ethernet1/0
 description LINK_ACCFARM1
 no switchport
 ip address 10.0.3.5 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 3 area 3
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
router ospf 3
 router-id 10.10.10.7
 area 3 stub no-summary
 area 3 range 10.0.3.0 255.255.255.0
 area 3 range 172.16.1.0 255.255.255.0
 passive-interface default
 no passive-interface Ethernet0/0
 no passive-interface Ethernet0/1
 no passive-interface Ethernet1/0
 no passive-interface Port-channel1
```

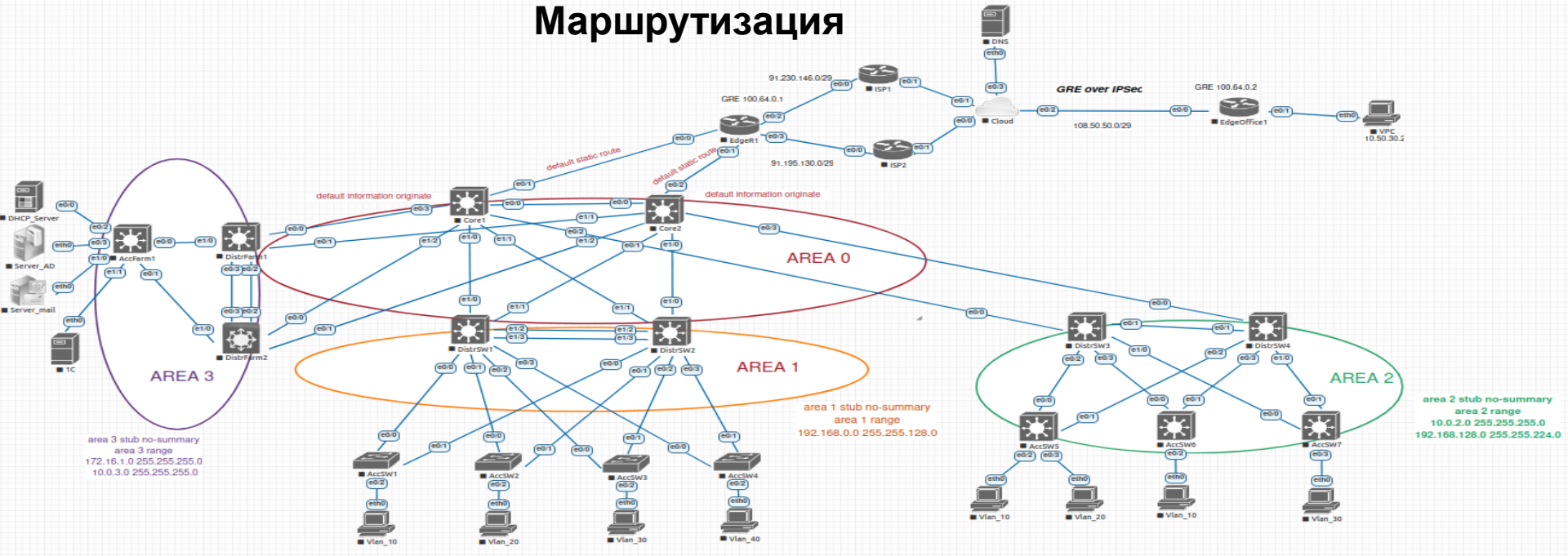
Рекомендации для L2 Access

- Сегментация сети на VLAN
- Отключение неиспользуемых портов и перевод их в неиспользуемый VLAN
- Не используйте VLAN 1. Добавление Native VLAN.
- Порты в строго в режиме: mode access или mode trunk
- Явно указывать, какие VLAN разрешены в trunk
- Защита от широковещательных штормов storm control
- Включение portfast, bpdu guard на портах пользователей
- Использование port security на пользовательских портах
- Использование DHCP Snooping для защиты DHCP сервиса
- Использование RSTP, коммутатор распределения/ядра должен быть корневым для необходимых VLAN

```
!
ip dhcp snooping vlan 10
ip dhcp snooping
!
errdisable recovery cause storm-control
errdisable recovery interval 180
!
interface Ethernet0/0
 description LINK_DISTRSW1
 switchport trunk allowed vlan 10,100,999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Ethernet0/1
 description LINK_DISTRSW2
 switchport trunk allowed vlan 10,100,999
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 999
 switchport mode trunk
!
interface Ethernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security violation protect
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.6806
 switchport port-security
 spanning-tree bpduguard enable
!
interface Ethernet0/3
 switchport access vlan 666
 switchport mode access
 shutdown
!
interface Vlan100
 ip address 192.168.100.10 255.255.255.128
 no ip route-cache
```

```
AccSW1(config)#do sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   buh                              active    Et0/2
100  mng                              active
666  PL                               active    Et0/3
999  native                           active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Маршрутизация



- Многозонный OSPF
- Магистрали point-to-point /30
- Area 1, Area 2, Area 3 – tottaly stub (AccSW5, AccSW6, AccSW7, AccFarm1 – получают только маршрут 0.0.0.0 от своих ABR)
- На ABR суммирование маршрутов в Core
- Для уменьшения времени реагирования на изменение сети, уменьшен Hello и Dead Interval 3/12
- Core1, Core2 инжектируют маршрут по умочанию в сеть 0.0.0.0 в сторону Edge Router (default information originate).
- Все интерфейсы в passive interface, кроме up link.

Пример настройки OSPF на DistrSW3.

```
interface Loopback0
 ip address 10.10.10.5 255.255.255.255
 ip ospf 1 area 0
!
interface Ethernet0/0
 description LINK_CORE1
 no switchport
 ip address 10.0.0.37 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 1 area 0
!
interface Ethernet0/1
 description LINK_DISTRSW4
 no switchport
 ip address 10.0.2.1 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 1 area 2
!
interface Ethernet0/2
 description LINK_ACCSW5
 no switchport
 ip address 10.0.2.5 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 1 area 2
!
interface Ethernet0/3
 description LINK_ACCSW6
 no switchport
 ip address 10.0.2.9 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 1 area 2
!
interface Ethernet1/0
 description LINK_ACCSW7
 no switchport
 ip address 10.0.2.13 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 1 area 2
!
interface Ethernet1/1
 shutdown
!
interface Ethernet1/2
 shutdown
!
interface Ethernet1/3
 shutdown
!
router ospf 1
 router-id 10.10.10.5
 area 2 stub no-summary
 area 2 range 10.0.2.0 255.255.255.0
 area 2 range 192.168.128.0 255.255.224.0
 passive-interface default
 no passive-interface Ethernet0/0
 no passive-interface Ethernet0/1
 no passive-interface Ethernet0/2
 no passive-interface Ethernet0/3
 no passive-interface Ethernet1/0
!
```

```
Gateway of last resort is 10.0.0.38 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 10.0.0.38, 00:06:52, Ethernet0/0
      10.0.0.0/8 is variably subnetted, 38 subnets, 3 masks
O        10.0.0.0/30 [110/20] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.0.0.4/30 [110/30] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.0.0.8/30 [110/30] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.0.0.12/30 [110/20] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.0.0.16/30 [110/20] via 10.0.0.38, 00:06:52, Ethernet0/0
C        10.0.0.36/30 is directly connected, Ethernet0/0
L        10.0.0.37/32 is directly connected, Ethernet0/0
O        10.0.0.40/30 [110/30] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.0.0.44/30 [110/20] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.0.0.48/30 [110/20] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.0.0.52/30 [110/30] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.0.0.56/30 [110/30] via 10.0.0.38, 00:06:52, Ethernet0/0
O IA     10.0.1.20/30 [110/25] via 10.0.0.38, 00:06:42, Ethernet0/0
O        10.0.2.0/24 is a summary, 00:07:02, Null0
C        10.0.2.0/30 is directly connected, Ethernet0/1
L        10.0.2.1/32 is directly connected, Ethernet0/1
C        10.0.2.4/30 is directly connected, Ethernet0/2
L        10.0.2.5/32 is directly connected, Ethernet0/2
C        10.0.2.8/30 is directly connected, Ethernet0/3
L        10.0.2.9/32 is directly connected, Ethernet0/3
C        10.0.2.12/30 is directly connected, Ethernet1/0
L        10.0.2.13/32 is directly connected, Ethernet1/0
O        10.0.2.16/30 [110/20] via 10.0.2.14, 00:06:22, Ethernet1/0
                      [110/20] via 10.0.2.2, 00:06:12, Ethernet0/1
O        10.0.2.20/30 [110/20] via 10.0.2.10, 00:06:22, Ethernet0/3
                      [110/20] via 10.0.2.2, 00:06:12, Ethernet0/1
O        10.0.2.24/30 [110/20] via 10.0.2.6, 00:06:32, Ethernet0/2
                      [110/20] via 10.0.2.2, 00:06:12, Ethernet0/1
O IA     10.0.3.0/24 [110/25] via 10.0.0.38, 00:06:32, Ethernet0/0
O        10.10.10.1/32 [110/21] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.10.10.2/32 [110/21] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.10.10.3/32 [110/11] via 10.0.0.38, 00:06:52, Ethernet0/0
O        10.10.10.4/32 [110/21] via 10.0.0.38, 00:06:52, Ethernet0/0
C        10.10.10.5/32 is directly connected, Loopback0
O        10.10.10.6/32 [110/31] via 10.0.0.38, 00:06:12, Ethernet0/0
O        10.10.10.7/32 [110/21] via 10.0.0.38, 00:06:42, Ethernet0/0
O        10.10.10.8/32 [110/21] via 10.0.0.38, 00:06:42, Ethernet0/0
O        10.10.12.1/32 [110/11] via 10.0.2.6, 00:06:32, Ethernet0/2
O        10.10.12.2/32 [110/11] via 10.0.2.10, 00:06:22, Ethernet0/3
O        10.10.12.3/32 [110/11] via 10.0.2.14, 00:06:22, Ethernet1/0
O IA     10.10.13.1/32 [110/31] via 10.0.0.38, 00:06:32, Ethernet0/0
     172.16.0.0/24 is subnetted, 1 subnets
O IA     172.16.1.0 [110/31] via 10.0.0.38, 00:06:01, Ethernet0/0
O IA  192.168.0.0/17 [110/21] via 10.0.0.38, 00:06:42, Ethernet0/0
O     192.168.128.0/19 is a summary, 00:06:22, Null0
O     192.168.128.0/24 [110/11] via 10.0.2.6, 00:06:01, Ethernet0/2
O     192.168.129.0/24 [110/11] via 10.0.2.6, 00:06:01, Ethernet0/2
O     192.168.130.0/24 [110/11] via 10.0.2.10, 00:06:01, Ethernet0/3
O     192.168.131.0/24 [110/11] via 10.0.2.14, 00:06:22, Ethernet1/0
DistrSW3#
```

```
DistrSW3#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.3        0   FULL/  -        00:00:10    10.0.0.38       Ethernet0/0
10.10.12.3        0   FULL/  -        00:00:09    10.0.2.14       Ethernet1/0
10.10.12.2        0   FULL/  -        00:00:09    10.0.2.10       Ethernet0/3
10.10.12.1        0   FULL/  -        00:00:11    10.0.2.6        Ethernet0/2
10.10.10.6        0   FULL/  -        00:00:09    10.0.2.2        Ethernet0/1
DistrSW3#
```

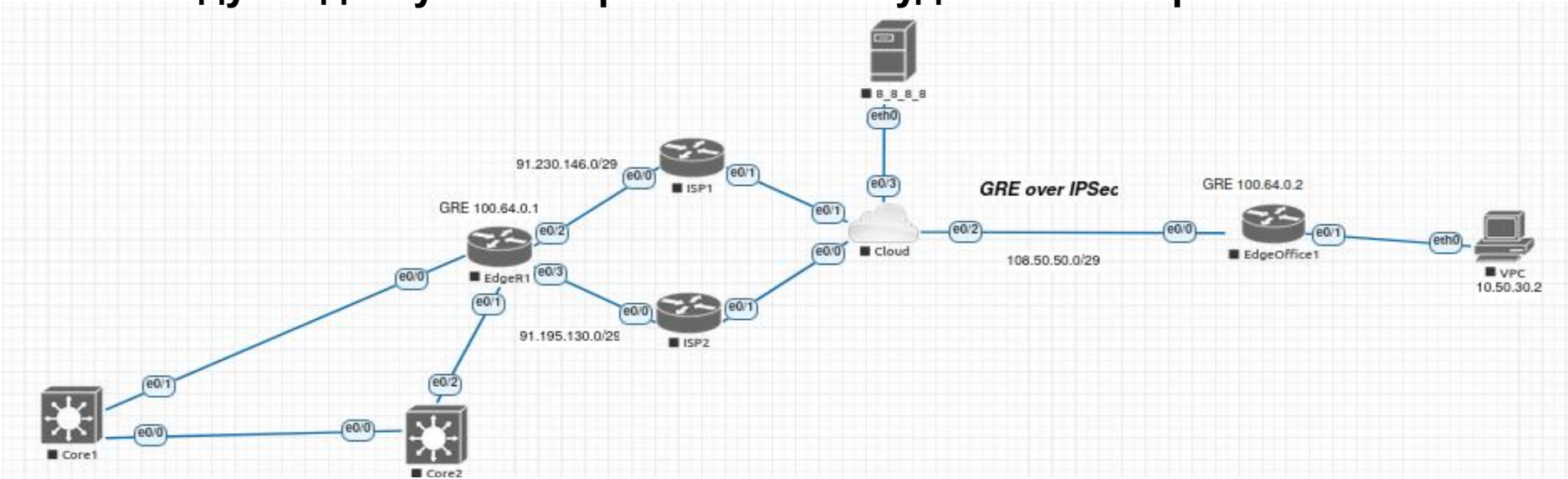
Пример настройки OSPF на AccSW5.

```
interface Loopback0
 ip address 10.10.12.3 255.255.255.255
 ip ospf 2 area 2
!
interface Ethernet0/0
 description LINK_DISTRSW3
 no switchport
 ip address 10.0.2.14 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 2 area 2
!
interface Ethernet0/1
 description LINK_DISTRSW4
 no switchport
 ip address 10.0.2.18 255.255.255.252
 ip ospf network point-to-point
 ip ospf hello-interval 3
 ip ospf 2 area 2
!
interface Ethernet0/2
 switchport access vlan 666
 switchport mode access
 shutdown
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Ethernet0/3
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Vlan30
 description WI-FI_USERS_DHCP
 ip address 192.168.131.1 255.255.255.0
 ip helper-address 172.16.1.2
 ip ospf 2 area 2
!
router ospf 2
 router-id 10.10.12.3
 area 2 stub no-summary
 passive-interface default
 no passive-interface Ethernet0/0
 no passive-interface Ethernet0/1
!
```

```
Gateway of last resort is 10.0.2.25 to network 0.0.0.0

O*IA  0.0.0.0/0 [110/11] via 10.0.2.25, 00:32:15, Ethernet0/1
                [110/11] via 10.0.2.5, 00:17:25, Ethernet0/0
      10.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
O        10.0.2.0/30 [110/20] via 10.0.2.25, 00:32:15, Ethernet0/1
                     [110/20] via 10.0.2.5, 00:17:25, Ethernet0/0
C        10.0.2.4/30 is directly connected, Ethernet0/0
L        10.0.2.6/32 is directly connected, Ethernet0/0
O        10.0.2.8/30 [110/20] via 10.0.2.5, 00:17:25, Ethernet0/0
O        10.0.2.12/30 [110/20] via 10.0.2.5, 00:17:25, Ethernet0/0
O        10.0.2.16/30 [110/20] via 10.0.2.25, 00:32:15, Ethernet0/1
O        10.0.2.20/30 [110/20] via 10.0.2.25, 00:32:15, Ethernet0/1
C        10.0.2.24/30 is directly connected, Ethernet0/1
L        10.0.2.26/32 is directly connected, Ethernet0/1
C        10.10.12.1/32 is directly connected, Loopback0
O        10.10.12.2/32 [110/21] via 10.0.2.25, 00:32:05, Ethernet0/1
                       [110/21] via 10.0.2.5, 00:17:25, Ethernet0/0
O        10.10.12.3/32 [110/21] via 10.0.2.25, 00:32:05, Ethernet0/1
                       [110/21] via 10.0.2.5, 00:17:10, Ethernet0/0
      192.168.128.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.128.0/24 is directly connected, Vlan10
L        192.168.128.1/32 is directly connected, Vlan10
      192.168.129.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.129.0/24 is directly connected, Vlan20
L        192.168.129.1/32 is directly connected, Vlan20
O     192.168.130.0/24 [110/21] via 10.0.2.25, 00:31:53, Ethernet0/1
                       [110/21] via 10.0.2.5, 00:17:25, Ethernet0/0
O     192.168.131.0/24 [110/21] via 10.0.2.25, 00:32:05, Ethernet0/1
                       [110/21] via 10.0.2.5, 00:17:10, Ethernet0/0
AccSW5#
```

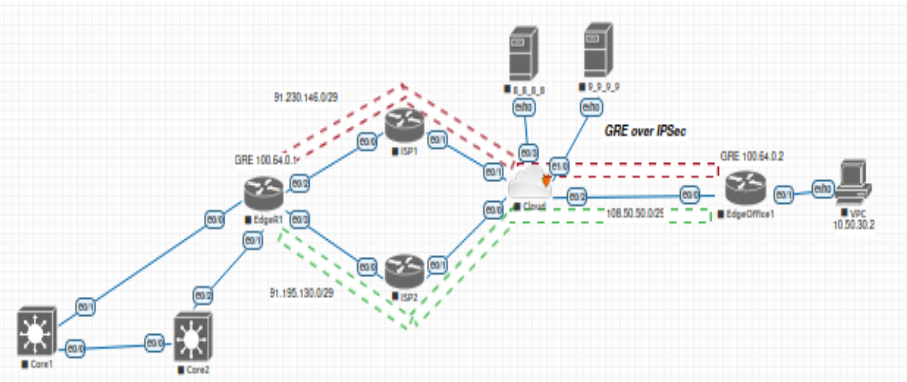
```
AccSW5#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.6        0   FULL/  -        00:00:11    10.0.2.25       Ethernet0/1
10.10.10.5        0   FULL/  -        00:00:09    10.0.2.5        Ethernet0/0
```

Модуль: доступ в интернет и связь с удаленным офисом



- В головном офисе имеем два провайдера, которые выделяют адреса: ISP1 91.230.146.0/29 и ISP2 91.195.130.0/29. Кроме того, имеется удаленный офис с выходом в интернет: ISP выделяет 108.50.50.0/29.
- ISP 1 используется для объединения двух офисов через пуличную сеть. Поднят туннель GRE over IPSec.
- ISP 2 используется для выхода пользователей в интернет
- В случае неисправностей на стороне ISP 2, выход в интернет осуществляется через ISP 1. После восстановления ISP 2, выход в интернет возвращается обратно через ISP 2 (для отслеживания используется механизм ip sla с track).
- В случае неисправностей на стороне ISP 1, с удаленным офисом поднимается резервный GRE Over IPSec через провайдера ISP 2 (подмена Source), используется инструмент Cisco EEM.
- Трансляция адресов PAT

Настройка GRE over IPSec



- EdgeR1-ISP1-EdgeOffice1 – основной туннель (красный)
- EdgeR1-ISP2-EdgeOffice2 – резервный туннель (зеленый)
- Статикой добавлен маршрут до 9.9.9.9 через ISP1
- Статикой добавлен маршрут в сеть удаленного офиса 10.50.3.0 через next-hop tunnel 100.64.0.2
- Настроен IPSec
- Ip sla 20 отслеживает доступность 9.9.9.9
- Track 20 привязан к ip sla 20
- Событие 1: Ресурс 9.9.9.9 – недоступен, срабатывает applet EEM ISP1-DOWN, происходит подмена Source на ISP2 (со стороны удаленного офиса – подмена destination)
- Событие 2: Ресурс 9.9.9.9 – доступен, срабатывает applet EEM ISP1-UP, возвращаем source ISP1

```
interface Tunnel0
 ip address 100.64.0.1 255.255.255.0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source 91.230.146.1
 tunnel destination 108.50.50.1
 tunnel protection ipsec profile protect-gre
!
```

```
track 20 ip sla 20
```

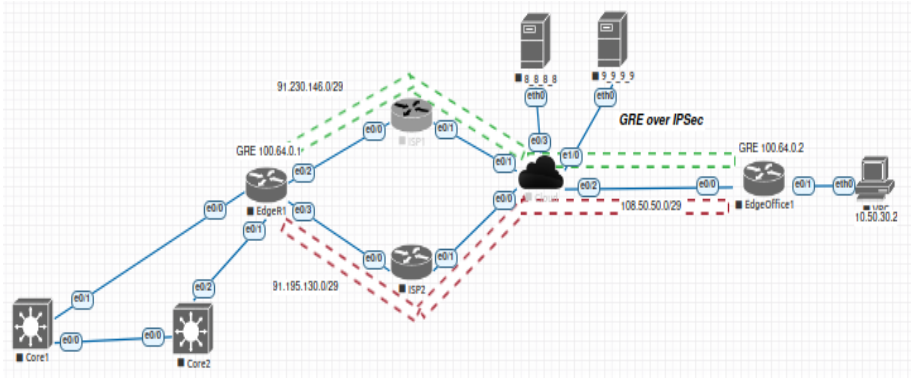
```
ip sla 20
 icmp-echo 9.9.9.9 source-interface Ethernet0/2
 threshold 1000
 timeout 1500
 frequency 3
ip sla schedule 20 life forever start-time now
```

```
ip route 9.9.9.9 255.255.255.255 91.230.146.6
ip route 10.50.30.0 255.255.255.0 100.64.0.2
```

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key mykey address 108.50.50.1
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
 mode transport
!
!
crypto ipsec profile protect-gre
 set security-association lifetime seconds 86400
 set transform-set TS
```

```
event manager applet ISP1-DOWN
 event track 20 state down
 action 10 cli command "enable"
 action 20 cli command "conf t"
 action 30 cli command "int tunnel 0"
 action 40 cli command "tunnel source 91.195.130.1"
 action 50 cli command "end"
 action 60 cli command "exit"
event manager applet ISP1-UP
 event track 20 state up
 action 10 cli command "enable"
 action 20 cli command "conf t"
 action 30 cli command "int tunnel 0"
 action 40 cli command "tunnel source 91.230.146.1"
 action 50 cli command "end"
 action 60 cli command "exit"
```

Настройка NAT с двумя ISP



- ISP2 – основной канал (красный)
- ISP1 – резервный канал (зеленыйй)
- Два статических маршрута 0.0.0.0 с разной метрикой
- Статикой добавлен маршрут до 8.8.8.8 через ISP2
- Используется PAT
- Ip sla 10 отслеживает доступность 8.8.8.8
- Track 10 привязан к ip sla 10
- Событие 1: Ресурс 8.8.8.8 – недоступен, переключаемся на ISP1 с очисткой NAT translation (applet EEM CLEAR_NAT_10)
- Событие 2: Ресурс 8.8.8.8 – доступен, возвращаемся на ISP2 с очисткой NAT

```
ip nat inside source route-map ISP1-NAT interface Ethernet0/2 overload
ip nat inside source route-map ISP2-NAT interface Ethernet0/3 overload
ip route 0.0.0.0 0.0.0.0 91.195.130.6 track 10
ip route 0.0.0.0 0.0.0.0 91.230.146.6 10
ip route 8.8.8.8 255.255.255.255 91.195.130.6
```

```
route-map ISP1-NAT permit 10
 match ip address LAN_TO_NAT_ISP
 match interface Ethernet0/2
!
route-map ISP2-NAT permit 10
 match ip address LAN_TO_NAT_ISP
```

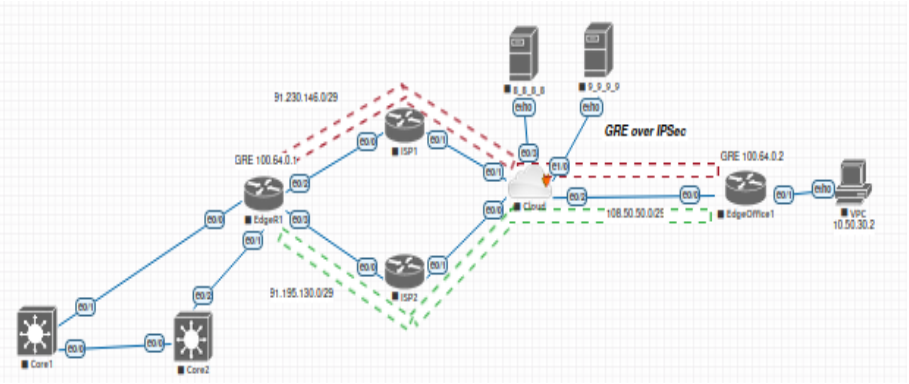
```
ip access-list extended LAN_TO_NAT_ISP
 permit tcp 192.168.0.0 0.0.255.255 any established
 permit udp 192.168.0.0 0.0.255.255 any
 permit ip 192.168.0.0 0.0.255.255 any
```

```
track 10 ip sla 10
```

```
ip sla 10
 icmp-echo 8.8.8.8 source-interface Ethernet0/3
 threshold 1000
 timeout 1500
 frequency 3
ip sla schedule 10 life forever start-time now
```

```
event manager applet CLEAR_NAT_10
 event track 10 state any
 action 10 cli command "enable"
 action 20 cli command "conf t"
 action 30 cli command "clear ip nat translation *"
 action 50 cli command "end"
 action 60 cli command "exit"
```

Удаленный офис



- Один ISP
- Статикой добавлены маршруты в сети головного офиса через next-hop tennel 100.64.0.1
- Статикой добавлен маршрут в сеть 0.0.0.0 (интернет)
- Ip sla 20 отслеживает доступность головного офиса через ISP1 (для построения основного туннеля)
- ip sla 20 привязан к track 20
- Событие 1: ISP1 головного офиса – недоступен, срабатывает applet EEM REMOTE-ISP1-DOWN, происходит подмена destination для построения туннеля с ISP2 головного офиса
- Событие 2: ISP1 головоного офиса – доступен, срабатывает applet EEM REMOTE-ISP1-UP, возвращаем destination ISP1

```
interface Tunnel0
 ip address 100.64.0.1 255.255.255.0
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source 91.230.146.1
 tunnel destination 108.50.50.1
 tunnel protection ipsec profile protect-gre
!
```

```
track 20 ip sla 20
```

```
ip sla 20
 icmp-echo 91.230.146.1 source-interface Ethernet0/0
 threshold 1000
 timeout 1500
 frequency 3
ip sla schedule 20 life forever start-time now
```

```
ip route 0.0.0.0 0.0.0.0 108.50.50.6
ip route 172.16.1.0 255.255.255.0 100.64.0.1
ip route 192.168.0.0 255.255.0.0 100.64.0.1
```

```
ip nat inside source list 1 interface Ethernet0/0 overload
```

```
access-list 1 permit 10.50.30.2
```

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key mykey address 91.230.146.1
crypto isakmp key mykey address 91.195.130.1
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
 mode transport
!
!
crypto ipsec profile protect-gre
 set security-association lifetime seconds 86400
 set transform-set TS
```

```
event manager applet REMOTE-ISP1-DOWN
 event track 20 state down
 action 10 cli command "enable"
 action 20 cli command "conf t"
 action 30 cli command "int tunnel 0"
 action 40 cli command "tunnel destin 91.195.130.1"
 action 50 cli command "end"
 action 60 cli command "exit"
event manager applet REMOTE-ISP1-UP
 event track 20 state up
 action 10 cli command "enable"
 action 20 cli command "conf t"
 action 30 cli command "int tunnel 0"
 action 40 cli command "tunnel dest 91.230.146.1"
 action 50 cli command "end"
 action 60 cli command "exit"
```

Выводы

- Данная схема была построена в eve-ng. В работе реализованы инструменты для построения отказоусточивой сети. Так же, проведены тесты с возможным выходом из строя оборудования, линков. Схема отрабатывает корректо.
- В дальнейшем предполагается развитие сети: разработка единой политики безопасности, установка МСЭ, создание DMZ, предоставление доступа для удаленных пользователей, организация системы мониторинга и управления. Так же, рассматривается расширение сети с подключением еще десятка удаленных офисов с применением технологии DMVPN/

Спасибо за внимание!