Проектирование ЛВС предприятия с серверными мощностями распределенными между офисом и ЦОД

Network Engineer. Basic.

Меня хорошо видно & слышно?


Защита проекта
Тема: Проектирование ЛВС предприятия с серверными мощностями распределенными между офисом и ЦОД

Вельдин Алексей

Системный администратор
ООО «Спортивные Лотереи»

План защиты

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

Цель и задачи проекта

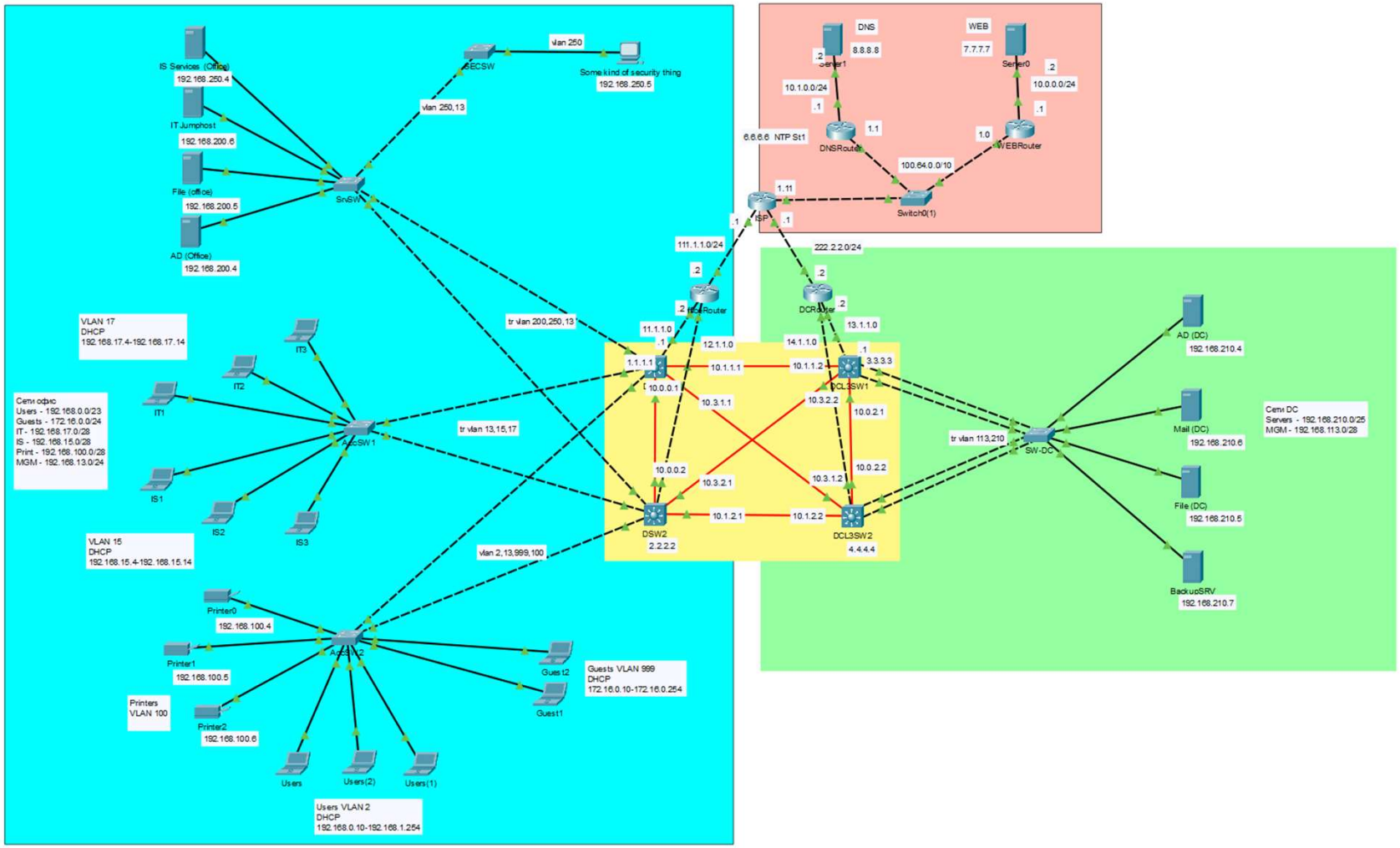
Цель проекта: спроектировать сеть компании с распределенными серверными мощностями

1. Определение задач: масштабируемость, отказоустойчивость, безопасность
2. Определение ресурсов
3. Выбор используемых технологий
4. Проектирование и моделирование схемы сети
5. Тесты и проверки

Используемые технологии:

1.	VLAN	Для разделения сетей
2.	HSRP/Etherchannel/STP	Для обеспечения отказоустойчивости
3.	OSPF	Динамическая маршрутизация
4.	DHCP/CDP/NTP	Вспомогательный функционал
5.	NAT	Для выхода во внешнюю сеть
5.	ACL	Для обеспечения безопасности
6.	SSH	Для удаленного управления сетевыми устройствами

Схема сети:


IS Services (Office)
192.168.250.4
IT Jumphost
192.168.200.6
File (office)
192.168.200.5
AD (Office)
192.168.200.4
SnSW
ECSW
vlan 250
Some kind of security thing
192.168.250.5
vlan 250,13
DNS
8.8.8.8
WEB
7.7.7.7
Server1
Server0
10.1.0.0/24
10.0.0.0/24
DNSRouter
WEBRouter
6.6.6.6 NTP St1
100.64.0.0/10
Switch0(1)
ISP
111.1.1.0/24
222.2.2.0/24
ISPRouter
DCRouter
tr vlan 200,250,13
11.1.1.0
12.1.1.0
14.1.1.0
13.1.1.0
1.1.1.1
10.0.0.1
10.1.1.1
10.1.1.2
1.3.3.3
DCL3SW1
10.3.1.1
10.3.2.2
10.0.2.1
VLAN 17
DHCP
192.168.17.4-192.168.17.14
Сети офис
Users - 192.168.0.0/23
Guests - 172.16.0.0/24
IT - 192.168.17.0/28
IS - 192.168.15.0/28
Print - 192.168.100.0/28
MGM - 192.168.13.0/24
IT1
IT2
IT3
IS1
IS2
IS3
AccSW1
tr vlan 13,15,17
10.0.0.2
10.3.2.1
10.3.1.2
10.0.2.2
DSW2
2.2.2.2
10.1.2.1
10.1.2.2
DCL3SW2
4.4.4.4
VLAN 15
DHCP
192.168.15.4-192.168.15.14
vlan 2,13,999,100
tr vlan 113,210
SW-DC
AD (DC)
192.168.210.4
Mail (DC)
192.168.210.6
File (DC)
192.168.210.5
BackupSRV
192.168.210.7
Сети DC
Servers - 192.168.210.0/25
MGM - 192.168.113.0/28
Printer0
192.168.100.4
Printer1
192.168.100.5
Printer2
192.168.100.6
Printers
VLAN 100
AccSW2
Guest2
Guest1
Guests VLAN 999
DHCP
172.16.0.10-172.16.0.254
Users
Users(2)
Users(1)
Users VLAN 2
DHCP
192.168.0.10-192.168.1.254

VLAN

Сеть поделена на 2 части: офис и ЦОД. 8 VLAN в офисе и 2 в ЦОД. Плюс VLAN 777 в качестве нативного и для неиспользуемых портов. VLAN терминируются на SVI на L3 коммутаторах.

VLAN	Network	Name	Description
2	192.168.0.0/23	Users	Основные пользователи
13	192.168.13.0/24	MGM	Подсеть менеджмента в офисе
15	192.168.15.0/28	Sec	Пользователи информационной безопасности
17	192.168.17.0/28	IT	Пользователи отдела IT
100	192.168.100.0/27	Print	Подсеть для принтеров и прочей переферии
113	192.168.113.0/28	DCMGM	Подсеть менеджмент в датацентре
200	192.168.200.0/25	OfficeSRV	Подсеть серверов в офисе
210	192.168.210.0/25	DCSRV	Подсеть серверов в Датацентре
250	192.168.250.0/27	ISS	Подсеть сервисов информационной безопасности
999	172.16.0.0/24	Guests	Подсеть для гостей
777		PARKINGLOT	

Адресация

Users			
Network	192.168.0.0	IP Range	192.168.0.1-192.168.1.254
Mask	255.255.254.0	VLAN	2
DHCP 192.168.0.10-192.168.1.254			
Address	Device	Name	Description
192.168.0.1	HSRP		GW
192.168.0.2	Switch	DSW1	
192.168.0.3	Switch	DSW2	
192.168.0.4	Switch	AccSW2	

OfficeSRV			
Network	192.168.200.0	IP Range	192.168.200.1-192.168.200.127
Mask	255.255.255.128	VLAN	200
Static			
Address	Device	Name	Description
192.168.200.1	HSRP		GW
192.168.200.2	Switch	DSW1	
192.168.200.3	Switch	DSW2	
192.168.200.4	Server	AD	
192.168.200.5	Server	File	
192.168.200.6	Server	IT Jump	

SEC			
Network	192.168.15.0	IP Range	192.168.15.1-192.168.15.14
Mask	255.255.255.240	VLAN	15
DHCP 192.168.15.5-192.168.15.14			
Address	Device	Name	Description
192.168.15.1	HSRP		GW
192.168.15.2	Switch	DSW1	
192.168.15.3	Switch	DSW2	
192.168.15.4	Switch	AccSW1	

MGM			
Network	192.168.13.0	IP Range	192.168.13.1-192.168.13.254
Mask	255.255.255.0	VLAN	13
Static			
Address	Device	Name	Description
192.168.13.1	HSRP		GW
192.168.13.2	Switch	DSW1	
192.168.13.3	Switch	DSW2	
192.168.13.4	Switch	SrvSW	
192.168.13.5	Switch	AccSW1	
192.168.13.6	Switch	AccSW2	
192.168.13.7	Switch	SecSW	
192.168.13.8	WR		Wi-Fi

ISS			
Network	192.168.250.0	IP Range	192.168.250.1-192.168.250.31
Mask	255.255.255.224	VLAN	250
Static			
Address	Device	Name	Description
192.168.250.1	HSRP		GW
192.168.250.2	Switch	DSW1	
192.168.250.3	Switch	DSW2	
192.168.250.4	Server	ISServices	

DCMGM			
Network	192.168.113.0	IP Range	192.168.113.1-192.168.113.254
Mask	255.255.255.0	VLAN	113
Static			
Address	Device	Name	Description
192.168.113.1	HSRP		GW
192.168.113.2	Switch	DCL3SW1	
192.168.113.3	Switch	DCL3SW2	
192.168.113.4	Switch	SW-DC	

IT			
Network	192.168.17.0	IP Range	192.168.17.1-192.168.17.14
Mask	255.255.255.240	VLAN	17
DHCP 192.168.17.5-192.168.17.14			
Address	Device	Name	Description
192.168.17.1	HSRP		GW
192.168.17.2	Switch	DSW1	
192.168.17.3	Switch	DSW2	
192.168.17.4	Switch	AccSW1	

Guests			
Network	172.16.0.0	IP Range	172.16.0.1-172.16.0.254
Mask	255.255.255.0	VLAN	999
DHCP 172.16.0.10-172.16.0.254			
Address	Device	Name	Description
172.16.0.1	HSRP		GW
172.16.0.2	Switch	DSW1	
172.16.0.3	Switch	DSW2	
172.16.0.4	Switch	AccSW2	

DCSRV			
Network	192.168.210.0	IP Range	192.168.210.1-192.168.210.127
Mask	255.255.255.128	VLAN	210
Static			
Address	Device	Name	Description
192.168.210.1	HSRP		GW
192.168.210.2	Switch	DCL3SW1	
192.168.210.3	Switch	DCL3SW2	
192.168.210.4	Server	AD	
192.168.210.5	Server	File	
192.168.210.6	Server	Mail	
192.168.210.7	Server	BackupSRV	

VLAN

```
DSW1#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    Users                            active
13   MGM                              active
15   IS                               active
17   IT                               active
100  Printers                         active
200  OfficeSRV                        active
250  ISSRV                            active
777  ParkingLot                       active    Gig1/0/4, Gig1/0/5, Gig1/0/6, Gig1/0/7
                                                Gig1/0/8, Gig1/0/9, Gig1/0/10, Gig1/0/11
                                                Gig1/0/12, Gig1/0/13, Gig1/0/14, Gig1/0/15
                                                Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19
                                                Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/23
                                                Gig1/1/4
999  Guests                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
DSW1#
```

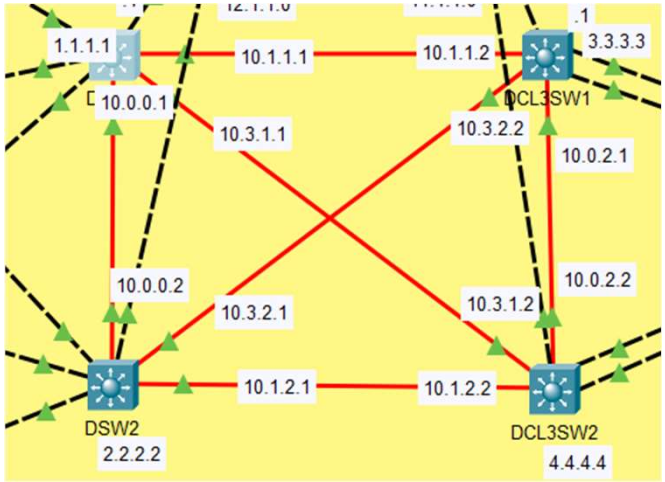
```
DCL3SW1#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
113  DCMGM                            active
210  DCSRV                            active
777  ParkingLot                       active    Gig1/0/2, Gig1/0/3, Gig1/0/4, Gig1/0/5
                                                Gig1/0/6, Gig1/0/7, Gig1/0/8, Gig1/0/9
                                                Gig1/0/10, Gig1/0/11, Gig1/0/12, Gig1/0/13
                                                Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17
                                                Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/21
                                                Gig1/0/22, Gig1/1/4
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

```
DSW1#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig1/0/1    on           802.1q         trunking      777
Gig1/0/2    on           802.1q         trunking      777
Gig1/0/3    on           802.1q         trunking      777

Port        Vlans allowed on trunk
Gig1/0/1    13,200,250
Gig1/0/2    13,15,17
Gig1/0/3    2,13,100,999

Port        Vlans allowed and active in management domain
Gig1/0/1    13,200,250
Gig1/0/2    13,15,17
Gig1/0/3    2,13,100,999

Port        Vlans in spanning tree forwarding state and not pruned
Gig1/0/1    200,250
Gig1/0/2    15,17
Gig1/0/3    2,13,100,999
```

```
DCL3SW1#sh int tr
Port        Mode         Encapsulation  Status        Native vlan
Po2         on           802.1q         trunking      777

Port        Vlans allowed on trunk
Po2         113,210

Port        Vlans allowed and active in management domain
Po2         113,210

Port        Vlans in spanning tree forwarding state and not pruned
Po2         113,210
```

HSRP

На каждой паре L3 коммутаторов в офисе и ЦОД настроен HSRP и настроена балансировка по принципу «четные VLAN в одну сторон, нечетные в другую»




```
DSW1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl2         2    200 P Active   local           192.168.0.3     192.168.0.1
Vl113       13   100   Standby  192.168.13.3    local           192.168.13.1
Vl115       15   100   Standby  192.168.15.3    local           192.168.15.1
Vl117       17   100   Standby  192.168.17.3    local           192.168.17.1
Vl100       100  200 P Active   local           192.168.100.3   192.168.100.1
Vl200       200  200 P Active   local           192.168.200.3   192.168.200.1
Vl250       250  200 P Active   local           192.168.250.3   192.168.250.1
Vl999       999  100   Standby  172.16.0.3      local           172.16.0.1
```

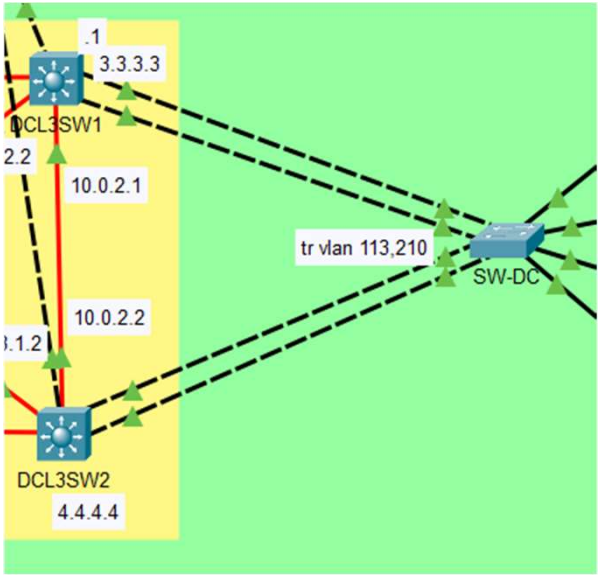
```
DCL3SW1#sh stand brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl113       113  100   Standby  192.168.113.3   local           192.168.113.1
Vl210       210  200 P Active   local           192.168.210.3   192.168.210.1
```

```
DSW2#
DSW2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl2         2    100   Standby  192.168.0.2     local           192.168.0.1
Vl113       13   200 P Active   local           192.168.13.2    192.168.13.1
Vl115       15   200 P Active   local           192.168.15.2    192.168.15.1
Vl117       17   200 P Active   local           192.168.17.2    192.168.17.1
Vl100       100  100   Standby  192.168.100.2   local           192.168.100.1
Vl200       200  100   Standby  192.168.200.2   local           192.168.200.1
Vl250       250  100   Standby  192.168.250.2   local           192.168.250.1
Vl999       999  200 P Active   local           172.16.0.2      172.16.0.1
```

```
DCL3SW2#sh stand brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl113       113  200 P Active   local           192.168.113.2   192.168.113.1
Vl210       210  100   Standby  192.168.210.2   local           192.168.210.1
```

Etherchannel

В ЦОД настроен LACP Active-Active



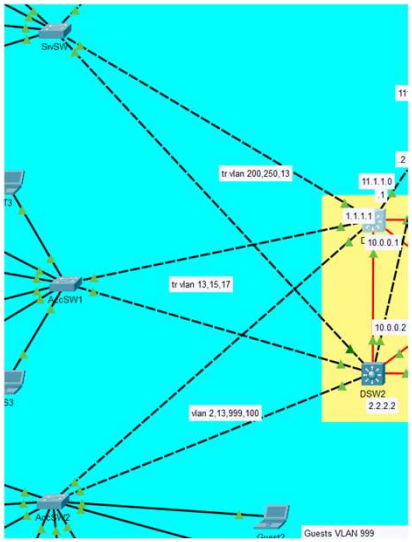

```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

2      Po2(SU)           LACP   Gig1/0/23(P) Gig1/0/24(P)
DCL3SW1#
```

```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           LACP   Gig1/0/23(P) Gig1/0/24(P)
DCL3SW2#
```

```
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           LACP   Gig0/1(P) Gig0/2(P)
2      Po2(SU)           LACP   Fa0/23(P) Fa0/24(P)
SWDC#
```

STP

На коммутаторах настроен Rapid PVST. По умолчанию включен BPDU Guard и access порты переведены в режим Portfast.

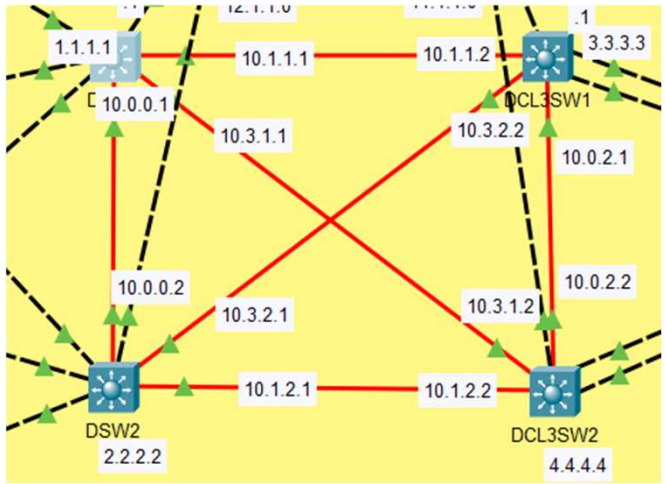



```
DSW2#sh spanning-tree sum
Switch is in rapid-pvst mode
Root bridge for: MGM IS IT Guests
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0002                      6         0        0          1          7
VLAN0013                      4         0        0          3          7
VLAN0015                      6         0        0          1          7
VLAN0017                      6         0        0          1          7
VLAN0100                      6         0        0          1          7
VLAN0200                      6         0        0          1          7
VLAN0250                      6         0        0          1          7
VLAN0777                      4         0        0          3          7
VLAN0999                      6         0        0          1          7

---------------------- -------- --------- -------- ---------- ----------
10 vlans                     50         0        0         13         63
```

```
AccSW1#sh run | begin bpdu
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 17
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 17
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 spanning-tree portfast
!
```

OSPF

Между офисом и ЦОД поднят процесс OSPF. Каждый коммутатор строит соседство со всеми участниками с целью обеспечения отказоустойчивости.




```
DSW2#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           1   FULL/DR         00:00:31    10.1.2.2        GigabitEthernet1/1/1
1.1.1.1           1   FULL/BDR        00:00:37    10.0.0.1        GigabitEthernet1/1/2
3.3.3.3           1   FULL/DR         00:00:36    10.3.2.2        GigabitEthernet1/1/3
```

```
DSW2#sh ip route ospf
     10.0.0.0/30 is subnetted, 6 subnets
O       10.0.2.0 [110/2] via 10.1.2.2, 04:33:47, GigabitEthernet1/1/1
                 [110/2] via 10.3.2.2, 04:33:47, GigabitEthernet1/1/3
O       10.1.1.0 [110/2] via 10.3.2.2, 04:33:47, GigabitEthernet1/1/3
                 [110/2] via 10.0.0.1, 04:33:47, GigabitEthernet1/1/2
O       10.3.1.0 [110/2] via 10.1.2.2, 04:33:47, GigabitEthernet1/1/1
                 [110/2] via 10.0.0.1, 04:33:47, GigabitEthernet1/1/2
O    192.168.113.0 [110/2] via 10.1.2.2, 04:33:47, GigabitEthernet1/1/1
                   [110/2] via 10.3.2.2, 04:33:47, GigabitEthernet1/1/3
     192.168.210.0/25 is subnetted, 1 subnets
O       192.168.210.0 [110/2] via 10.1.2.2, 04:33:47, GigabitEthernet1/1/1
                      [110/2] via 10.3.2.2, 04:33:47, GigabitEthernet1/1/3
```

```
DCL3SW1#sh ip route ospf
     10.0.0.0/30 is subnetted, 6 subnets
O       10.0.0.0 [110/2] via 10.3.2.1, 01:20:22, GigabitEthernet1/1/3
                 [110/2] via 10.1.1.1, 01:20:22, GigabitEthernet1/1/1
O       10.1.2.0 [110/2] via 10.3.2.1, 01:20:22, GigabitEthernet1/1/3
                 [110/2] via 10.0.2.2, 01:20:22, GigabitEthernet1/1/2
O       10.3.1.0 [110/2] via 10.1.1.1, 01:20:22, GigabitEthernet1/1/1
                 [110/2] via 10.0.2.2, 01:20:22, GigabitEthernet1/1/2
O    192.168.0.0 [110/2] via 10.3.2.1, 01:20:22, GigabitEthernet1/1/3
                 [110/2] via 10.1.1.1, 01:20:22, GigabitEthernet1/1/1
O    192.168.13.0 [110/2] via 10.3.2.1, 01:20:22, GigabitEthernet1/1/3
                  [110/2] via 10.1.1.1, 01:20:22, GigabitEthernet1/1/1
     192.168.15.0/28 is subnetted, 1 subnets
O       192.168.15.0 [110/2] via 10.3.2.1, 01:20:22, GigabitEthernet1/1/3
                     [110/2] via 10.1.1.1, 01:20:22, GigabitEthernet1/1/1
     192.168.17.0/28 is subnetted, 1 subnets
O       192.168.17.0 [110/2] via 10.3.2.1, 01:20:22, GigabitEthernet1/1/3
                     [110/2] via 10.1.1.1, 01:20:22, GigabitEthernet1/1/1
     192.168.200.0/25 is subnetted, 1 subnets
O       192.168.200.0 [110/2] via 10.3.2.1, 01:20:22, GigabitEthernet1/1/3
                      [110/2] via 10.1.1.1, 01:20:22, GigabitEthernet1/1/1
```

DHCP

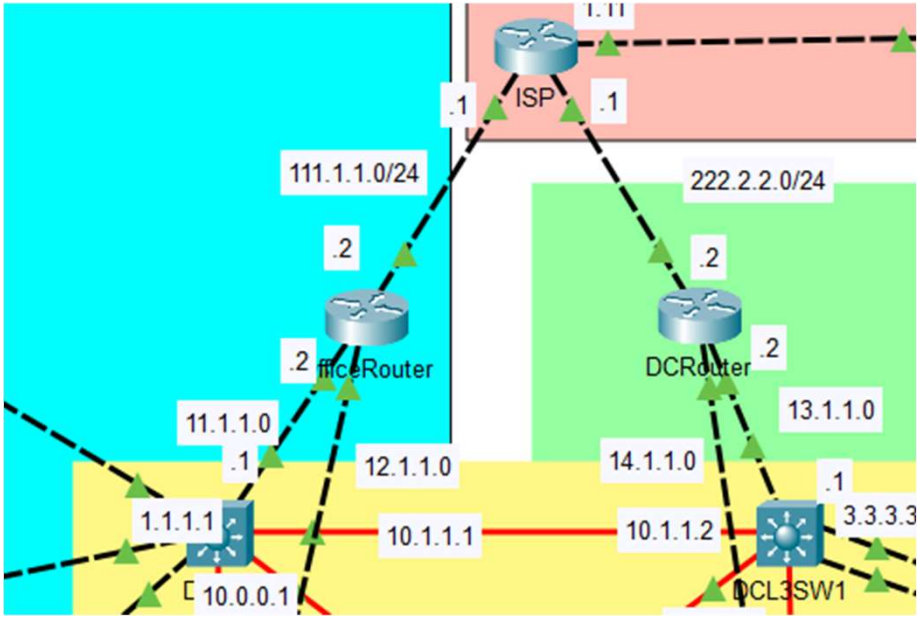
На Access свитчах подняты DHCP серверы для конечных пользователей.

```
AccSW2#sh ip dhcp bind
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.0.10     0030.A37A.9741           --                     Automatic
192.168.0.11     0030.F2A1.9095           --                     Automatic
192.168.0.12     0002.1636.1ADE           --                     Automatic
172.16.0.10      0001.63BB.CEA3           --                     Automatic
172.16.0.11      00D0.58AC.9766           --                     Automatic
AccSW2#sh ip dhcp pool

Pool VLAN2_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 510
 Leased addresses               : 3
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.0.1          192.168.0.1      - 192.168.1.254     3    / 2     / 510

Pool VLAN999_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 2
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 172.16.0.1           172.16.0.1       - 172.16.0.254      2    / 2     / 254
```

```
AccSW1#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.17.5     00D0.978E.C06B           --                     Automatic
192.168.17.7     0006.2A1A.A5E1           --                     Automatic
192.168.17.6     00E0.8F9B.A375           --                     Automatic
192.168.15.7     0001.C961.60C0           --                     Automatic
192.168.15.5     0001.C913.3091           --                     Automatic
192.168.15.6     0001.C79B.383E           --                     Automatic
AccSW1#sh ip dhcp po
AccSW1#sh ip dhcp pool

Pool VLAN17_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 14
 Leased addresses               : 3
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.17.1         192.168.17.1     - 192.168.17.14     3    / 2     / 14

Pool VLAN15_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 14
 Leased addresses               : 3
 Excluded addresses             : 2
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.15.1         192.168.15.1     - 192.168.15.14     3    / 2     / 14
```

CDP

CDP деактивирован на портах смотрящих во внешнюю сеть.



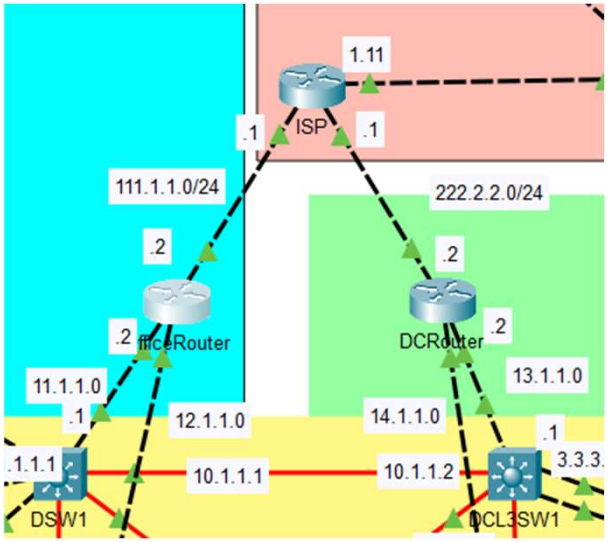

```
DCRouter#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce    Holdtme    Capability   Platform    Port ID
DCL3SW1        Gig 0/1           176                     3650        Gig 1/0/1
DCL3SW2        Gig 0/2           176                     3650        Gig 1/0/1
DCRouter#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     222.2.2.2       YES manual up                    up
GigabitEthernet0/1     13.1.1.2        YES manual up                    up
GigabitEthernet0/2     14.1.1.2        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
DCRouter#
```

```
OfficeRouter#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce    Holdtme    Capability   Platform    Port ID
DSW1           Gig 0/1           153                     3650        Gig 1/0/24
DSW2           Gig 0/2           153                     3650        Gig 1/0/24
OfficeRouter#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     111.1.1.2       YES manual up                    up
GigabitEthernet0/1     11.1.1.2        YES manual up                    up
GigabitEthernet0/2     12.1.1.2        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
OfficeRouter#
```

```
DSW1#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce    Holdtme    Capability   Platform    Port ID
SrvSW          Gig 1/0/1         130            S        2960        Gig 0/1
DCL3SW1        Gig 1/1/1         130                     3650        Gig 1/1/1
AccSW1         Gig 1/0/2         130            S        2960        Gig 0/1
AccSW2         Gig 1/0/3         130            S        2960        Gig 0/1
DSW2           Gig 1/1/2         130                     3650        Gig 1/1/2
DCL3SW2        Gig 1/1/3         130                     3650        Gig 1/1/3
Router         Gig 1/0/24        10             R        C2900       Gig 0/1
OfficeRouter
               Gig 1/0/24        130            R        C2900       Gig 0/1
DSW1#
```

NAT

С целью доступа в «интернет» в ЦОД был настроен NAT с перегрузкой, в офисе – динамический. Так же статический NAT представлен на схеме во «внешней сети»




```
ip nat pool INET 123.123.123.1 123.123.123.254 netmask 255.255.255.0
ip nat inside source list 1 pool INET
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
ip route 192.168.0.0 255.255.0.0 11.1.1.1
ip route 172.16.0.0 255.255.0.0 11.1.1.1
ip route 192.168.0.0 255.255.0.0 12.1.1.1
ip route 172.16.0.0 255.255.0.0 12.1.1.1
!
ip flow-export version 9
!
!
ip access-list extended INET_ACL
access-list 1 permit host 11.1.1.1
access-list 1 permit host 12.1.1.1
access-list 1 permit 192.168.0.0 0.0.1.255
access-list 1 permit 192.168.15.0 0.0.0.15
access-list 1 permit 192.168.17.0 0.0.0.15
access-list 1 permit 172.16.0.0 0.0.0.255
access-list 1 permit 192.168.200.0 0.0.0.15
```

```
ip nat pool INET 124.124.124.124 124.124.124.124 netmask 255.255.255.0
ip nat inside source list 2 pool INET overload
ip classless
ip route 192.168.210.0 255.255.255.128 13.1.1.1
ip route 192.168.210.0 255.255.255.128 14.1.1.1
ip route 0.0.0.0 0.0.0.0 222.2.2.1
!
ip flow-export version 9
!
!
access-list 2 permit 192.168.210.0 0.0.0.127
access-list 2 permit host 13.1.1.1
access-list 2 permit host 14.1.1.1
```

ACL. Матрица доступа.

Vlan	Subnet	Wmask		Users	MGM	Sec	IT	Print	DCMGM	OfficeSRV	DCSRV	ISS	Guests	Inet
2	192.168.0.0	0.0.1.255	Users											
13	192.168.13.0	0.0.0.255	MGM							Jump				
15	192.168.15.0	0.0.0.15	Sec											
17	192.168.17.0	0.0.0.15	IT											
100	192.168.100.0	0.0.0.31	Print											
113	192.168.113.0	0.0.0.15	DCMGM							Jump				
200	192.168.200.0	0.0.0.127	OfficeSRV		Jump				Jump					Mail
210	192.168.210.0	0.0.0.127	DCSRV											Mail
250	192.168.250.0	0.0.0.31	ISS											
999	172.16.0.0	0.0.0.255	Guests											
	0.0.0.0	255.255.255.255	Internet							Mail	Mail			

ACL

Согласно матрице доступов написаны ACL и применены на входе интерфейсов SVI на L3 коммутаторах.

```
interface Vlan100
 mac-address 0090.2b54.2d05
 ip address 192.168.100.3 255.255.255.224
 ip access-group Print in
 standby version 2
 standby 100 ip 192.168.100.1
!
interface Vlan200
 mac-address 0090.2b54.2d06
 ip address 192.168.200.3 255.255.255.128
 ip access-group OfficeSRV in
 standby version 2
 standby 200 ip 192.168.200.1
!
interface Vlan250
 mac-address 0090.2b54.2d07
 ip address 192.168.250.3 255.255.255.224
 ip access-group ISS in
 standby version 2
 standby 250 ip 192.168.250.1
!
interface Vlan999
 mac-address 0090.2b54.2d08
 ip address 172.16.0.3 255.255.255.0
 ip access-group Guests in
 standby version 2
 standby 999 ip 172.16.0.1
 standby 999 priority 200
 standby 999 preempt
```

```
interface Vlan2
 mac-address 0090.2b54.2d01
 ip address 192.168.0.3 255.255.254.0
 ip access-group Users in
 standby version 2
 standby 2 ip 192.168.0.1
!
interface Vlan13
 mac-address 0090.2b54.2d02
 ip address 192.168.13.3 255.255.255.0
 ip access-group MGM in
 standby version 2
 standby 13 ip 192.168.13.1
 standby 13 priority 200
 standby 13 preempt
!
interface Vlan15
 mac-address 0090.2b54.2d03
 ip address 192.168.15.3 255.255.255.240
 ip access-group Sec in
 standby version 2
 standby 15 ip 192.168.15.1
 standby 15 priority 200
 standby 15 preempt
!
interface Vlan17
 mac-address 0090.2b54.2d04
 ip address 192.168.17.3 255.255.255.240
 ip access-group IT in
 standby version 2
 standby 17 ip 192.168.17.1
 standby 17 priority 200
 standby 17 preempt
```

```
DSW1#sh access-lists
Extended IP access list Users
    10 permit udp any host 224.0.0.102 eq 1985 (2100 match(es))
    20 deny ip 192.168.0.0 0.0.1.255 192.168.13.0 0.0.0.255
    30 deny ip 192.168.0.0 0.0.1.255 192.168.113.0 0.0.0.15
    40 deny ip 192.168.0.0 0.0.1.255 192.168.250.0 0.0.0.31
    50 deny ip 192.168.0.0 0.0.1.255 172.16.0.0 0.0.0.255
    60 permit ip 192.168.0.0 0.0.1.255 any (2 match(es))
    70 deny ip any any
Extended IP access list MGM
    10 permit udp any host 224.0.0.102 eq 1985 (2102 match(es))
    20 permit ip 192.168.13.0 0.0.0.255 192.168.13.0 0.0.0.255 (1632 match(es))
    30 permit ip 192.168.13.0 0.0.0.255 192.168.113.0 0.0.0.15
    40 permit ip 192.168.13.0 0.0.0.255 host 192.168.200.6
    50 deny ip any any
Extended IP access list Sec
    10 permit udp any host 224.0.0.102 eq 1985 (2098 match(es))
    20 deny ip 192.168.15.0 0.0.0.15 192.168.13.0 0.0.0.255
    30 deny ip 192.168.15.0 0.0.0.15 192.168.17.0 0.0.0.15
    40 deny ip 192.168.15.0 0.0.0.15 192.168.113.0 0.0.0.15
    50 deny ip 192.168.15.0 0.0.0.15 172.16.0.0 0.0.0.255
    60 permit ip 192.168.15.0 0.0.0.15 any
    70 deny ip any any
Extended IP access list IT
    10 permit udp any host 224.0.0.102 eq 1985 (2094 match(es))
    20 deny ip 192.168.17.0 0.0.0.15 192.168.15.0 0.0.0.15
    30 deny ip 192.168.17.0 0.0.0.15 192.168.250.0 0.0.0.31
    40 deny ip 192.168.17.0 0.0.0.15 172.16.0.0 0.0.0.255
    50 permit ip 192.168.17.0 0.0.0.15 any
    60 deny ip any any
Extended IP access list Print
    10 permit udp any host 224.0.0.102 eq 1985 (2099 match(es))
    20 permit ip 192.168.100.0 0.0.0.31 192.168.0.0 0.0.1.255
    30 permit ip 192.168.100.0 0.0.0.31 192.168.15.0 0.0.0.15
    40 permit ip 192.168.100.0 0.0.0.31 192.168.17.0 0.0.0.15
    50 permit ip 192.168.100.0 0.0.0.31 192.168.100.0 0.0.0.31
    60 deny ip any any
Extended IP access list OfficeSRV
    10 permit udp any host 224.0.0.102 eq 1985 (2098 match(es))
    20 permit ip 192.168.200.0 0.0.0.127 192.168.0.0 0.0.1.255 (2 match(es))
    30 permit ip 192.168.200.0 0.0.0.127 192.168.15.0 0.0.0.15 (4 match(es))
    40 permit ip 192.168.200.0 0.0.0.127 192.168.17.0 0.0.0.15
    50 permit ip 192.168.200.0 0.0.0.127 192.168.200.0 0.0.0.127 (583 match(es))
    60 permit ip 192.168.200.0 0.0.0.127 192.168.210.0 0.0.0.127
    70 permit ip host 192.168.200.6 192.168.13.0 0.0.0.255 (23 match(es))
    80 permit ip host 192.168.200.6 192.168.113.0 0.0.0.15 (26 match(es))
    90 deny ip any any (3 match(es))
Extended IP access list ISS
    10 permit udp any host 224.0.0.102 eq 1985 (2095 match(es))
    20 permit ip 192.168.250.0 0.0.0.31 192.168.15.0 0.0.0.15
    30 permit ip 192.168.250.0 0.0.0.31 192.168.250.0 0.0.0.31
    40 deny ip any any
Extended IP access list Guests
    10 permit udp any host 224.0.0.102 eq 1985 (2099 match(es))
    20 deny ip 172.16.0.0 0.0.0.255 192.168.0.0 0.0.255.255
    30 deny ip 172.16.0.0 0.0.0.255 10.0.0.0 0.255.255.255
    40 permit ip 172.16.0.0 0.0.0.255 any
    50 deny ip any any
```

SSH

На сетевых устройствах настроен доступ по SSHv2.

```
ip ssh version 2
ip domain-name my-otus-project.org
!
username admin privilege 15 password 7 0822455D0A16
!
line vty 0 4
 exec-timeout 3 0
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 login
```

IT Jumphost

Physical | Config | Services | Desktop | Programming | Attributes

Command Prompt

```
Pinging 192.168.113.4 with 32 bytes of data:

Reply from 192.168.113.4: bytes=32 time<1ms TTL=253

Ping statistics for 192.168.113.4:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ssh -l admin 192.168.113.4

Password:

 Unauthorized access is strictly prohibited.

SWDC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWDC(config)#ex
SWDC#ex

[Connection to 192.168.113.4 closed by foreign host]
C:\>ssh -l admin 192.168.13.5

Password:

 Unauthorized access is strictly prohibited.

AccSW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccSW1(config)#ex
AccSW1#ex

[Connection to 192.168.13.5 closed by foreign host]
C:\>
```

Top

Выводы

- Была построена модель сети с распределенными ресурсами, отвечающая минимальным требованиям безопасности, масштабируемости и отказоустойчивости.
- Использован ряд технологий, изученных в ходе курса
- Был реализован ряд идей и многое, хоть и не всегда удачно, испробовано на практике

Планы по развитию сети

- Более точная настройка ACL
- DUAL ISP
- FireWall
- Безопасность
- VPN между офисом и ЦОД и для пользователей

Планы по развитию меня

- Увидимся на Prof курсе 30 сентября ☺

Вопросы и рекомендации

+ если есть вопросы

— если вопросов нет

Спасибо за внимание!