IP-сеть – объект защиты и инструмент кибербезопасности

Дугин Андрей Олегович
Начальник отдела обеспечения информационной безопасности
МТС

http://aodugin.blogspot.com

Масштаб защищаемой сети

- 11 часовых поясов
- Сотни тысяч защищаемых ресурсов
- Корпоративный и коммерческий SOC 24x7

Наши эксперты делятся знаниями

- **Конференции**
  - PHDays
  - SOC Форум
  - Инфофорум
  - ZeroNights
  - Код ИБ
  - NZNOG (Новая Зеландия)
  - SGNOG (Сингапур)
- **Публикации**
  - Системный администратор
  - Защита информации. Инсайд
  - Information Security/ Информационная безопасность
  - IEEE Xplore

Модель OSI

Уровень	Протокол	Идентификатор
L7 Приложения	HTTP, SMTP, POP3, SSH	Приложение
L6 Представления	XDR, ICA	Формат
L5 Сессионный	SOCKS	Настройки
L4 Транспортный	TCP, UDP, SCTP	Протокол/порт, флаг
L3 Сетевой	IP(v4/v6), IPX, IPSEC, ARP	IP-адрес
L2 Канальный	Ethernet, PPP, Token Ring	MAC-адрес
L1 Физический	WiFi, RS-232, RJ-45, DWDM	Разъемы, lambda

IP-сеть. Компоненты


Firewall/VPN


Router


Switch


Admin


User PC


RADIUS

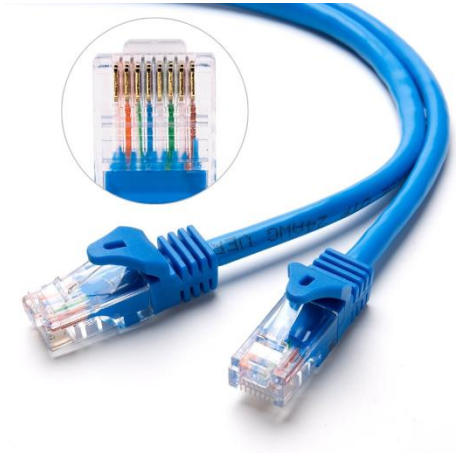

TACACS+

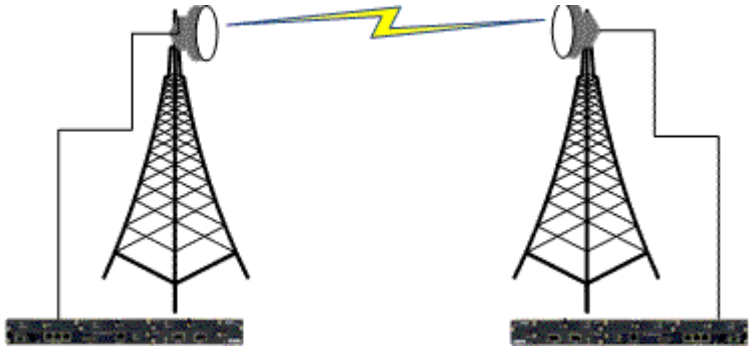

Fault Management
Performance Management

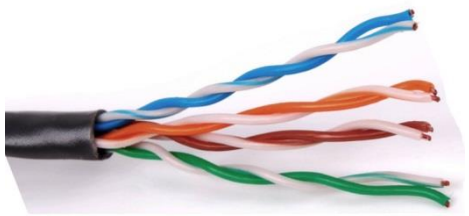

Security Management

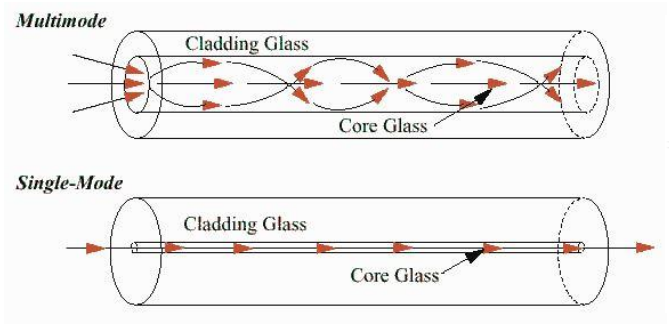

Configuration Management

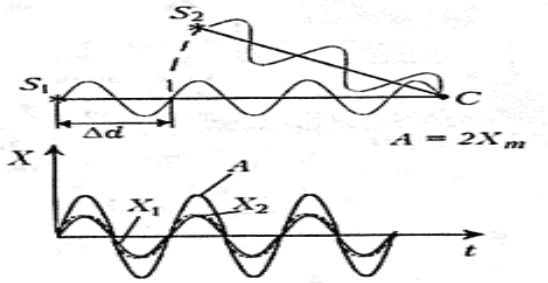
Layer 1 – Физический











Layer 1 – Физический

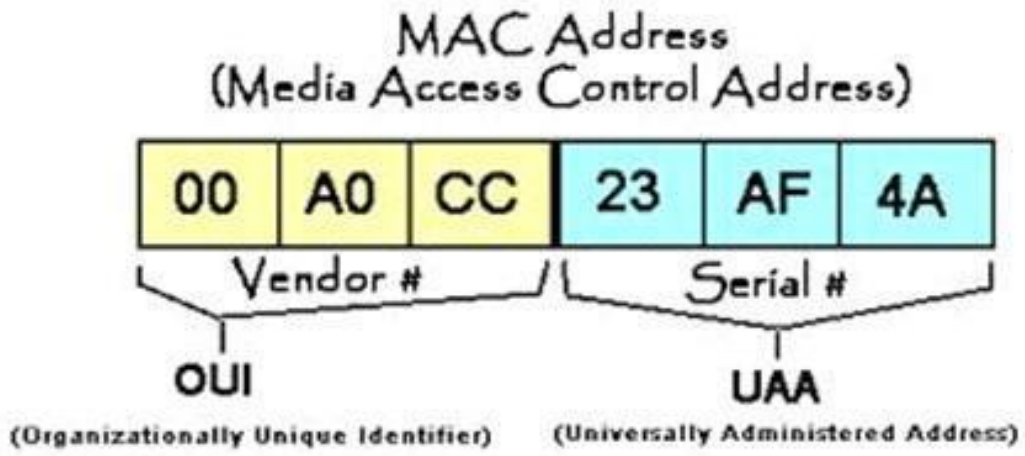
Виды атак

- Хищение оборудования
- Обрыв кабеля (помехи)
- Ответвление трафика
- Прослушивание эфира
- Нелегитимные точки доступа, модемы

Защита от атак

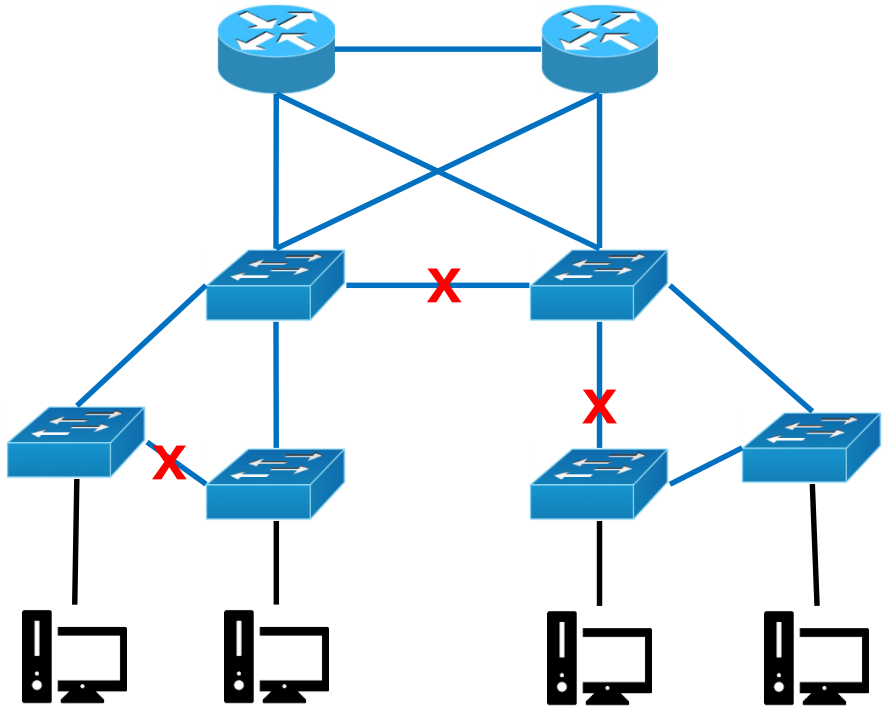
- Охрана объектов
- Кабельная канализация, короб
- Экранированное помещение
- Шифрование
- Мониторинг целостности канала и уровня сигнала

Layer 2 – Канальный



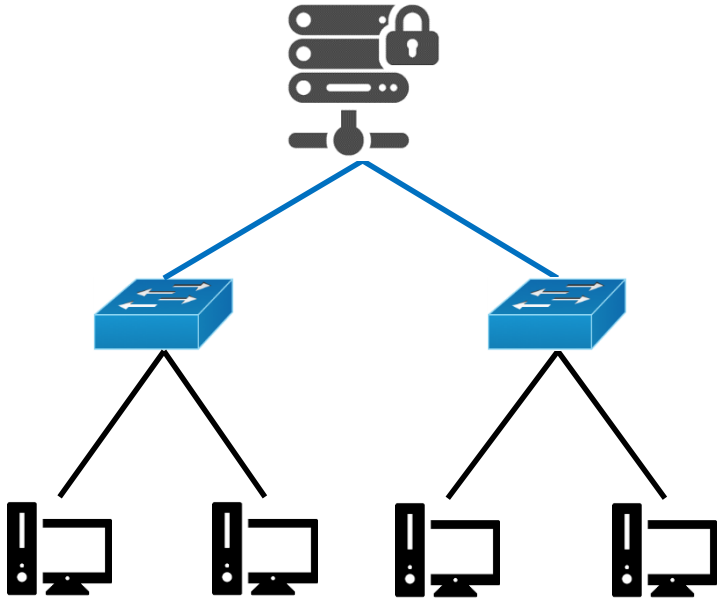

```
switch1#show mac address-table
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0009.5b44.9d2c    DYNAMIC     Fa0/1
   1    000f.66e3.352b    DYNAMIC     Fa0/1
   1    0012.8015.c940    DYNAMIC     Fa0/24
   1    0012.8015.c941    DYNAMIC     Fa0/24
```

Layer 2 – Канальный. Spanning Tree



- STP root
- STP instances

Layer 2 – Канальный. 802.1x



- RADIUS
- Network Access Server
- Supplicant

Layer 2 – Канальный

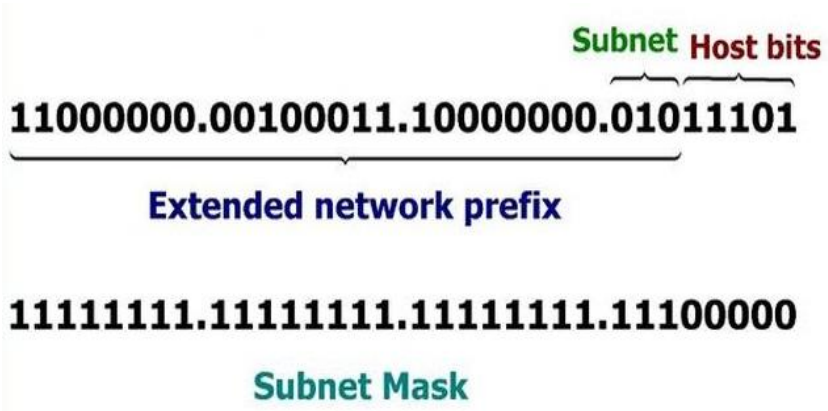
Виды атак

- Переполнение таблицы коммутации
- Подмена MAC-адреса
- Broadcast storm

Защита от атак

- 802.1x
- Port security
- Spanning Tree
  - BPDUguard
  - Rootguard
  - Loopguard

Layer 3 – Сетевой



Address	Age(min)	Hardware Adddr	Type	Interface
192.168.20.5	9	0000.0c07.f892	ARPA	FastEthernet0/0
192.168.60.5	8	0000.0c07.ac00	ARPA	FastEthernet0/1
192.168.20.1	-	0000.0c63.ae45	ARPA	FastEthernet0/0
192.168.40.5	9	0000.0c07.4320	ARPA	FastEthernet0/2
192.168.60.1	-	0000.0c63.1300	ARPA	FastEthernet0/1
192.168.40.1	-	0000.0c36.6965	ARPA	FastEthernet0/2

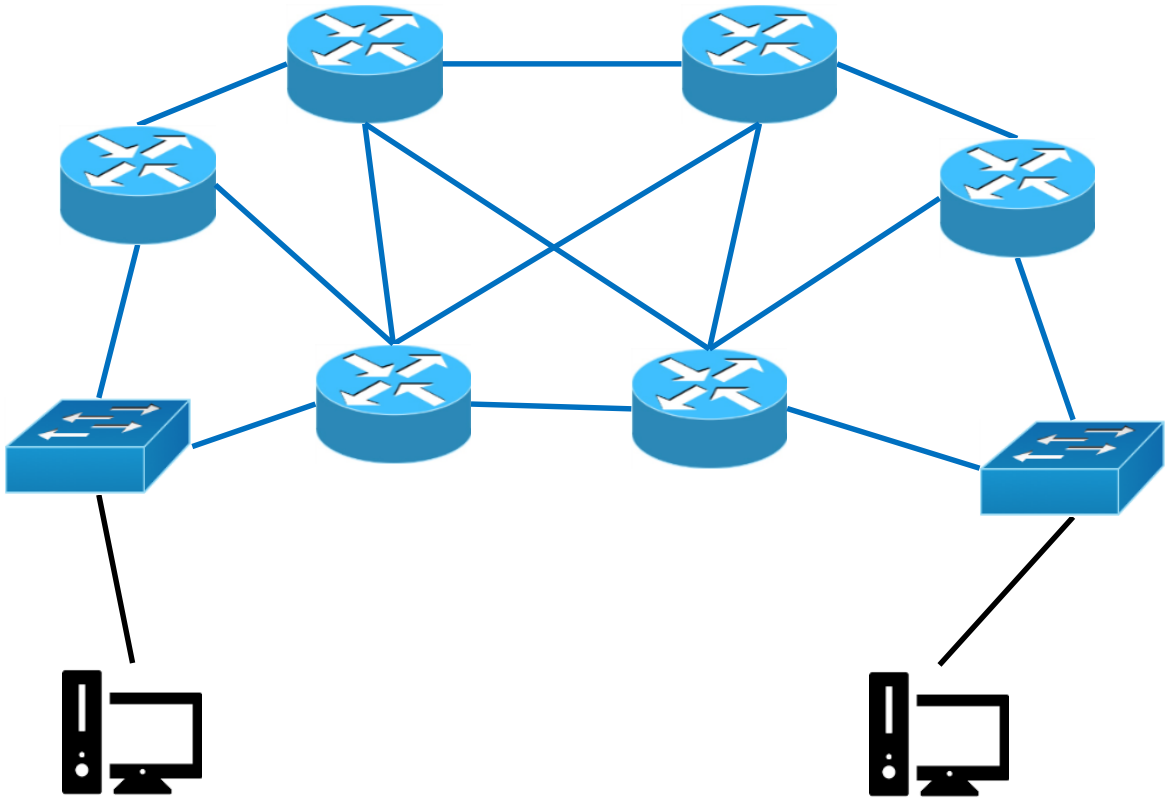
2345:6789:abcd:ef01:2345:6789:abcd:ef01

2345:6789:abcd:ef00::/63

0x|=| 000|

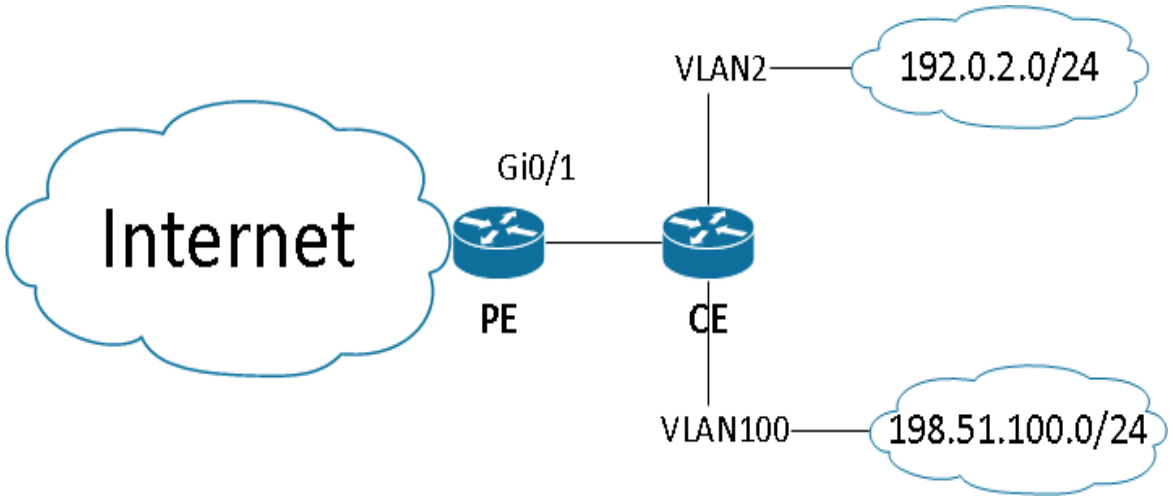
```
Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 46 subnets, 6 masks
C       10.1.193.2/32 is directly connected, Serial0/0/1
C       10.1.193.0/30 is directly connected, Serial0/0/1
D       10.1.193.6/32 [90/20517120] via 10.1.192.9, 2d01h, FastEthernet0/1
                      [90/20517120] via 10.1.192.1, 2d01h, FastEthernet0/0
D       10.1.193.4/30 [90/20517120] via 10.1.192.9, 2d01h, FastEthernet0/1
                      [90/20517120] via 10.1.192.1, 2d01h, FastEthernet0/0
D       10.1.193.5/32 [90/41024000] via 10.1.194.6, 2d01h, Serial0/0/0.122
```

Layer 3 – Сетевой. Маршрутизация



- Статическая
- Динамическая

Layer 3 – Сетевой. RPF




```
PE(config)# interface Gi0/1
PE(config-if)# ip verify unicast source
reachable-via rx

CE(config)# interface vlan 2
CE(config-if)# ip verify unicast source
reachable-via rx

CE(config)# interface vlan 100
CE(config-if)# ip verify unicast source
reachable-via rx
```

Layer 3 – Сетевой

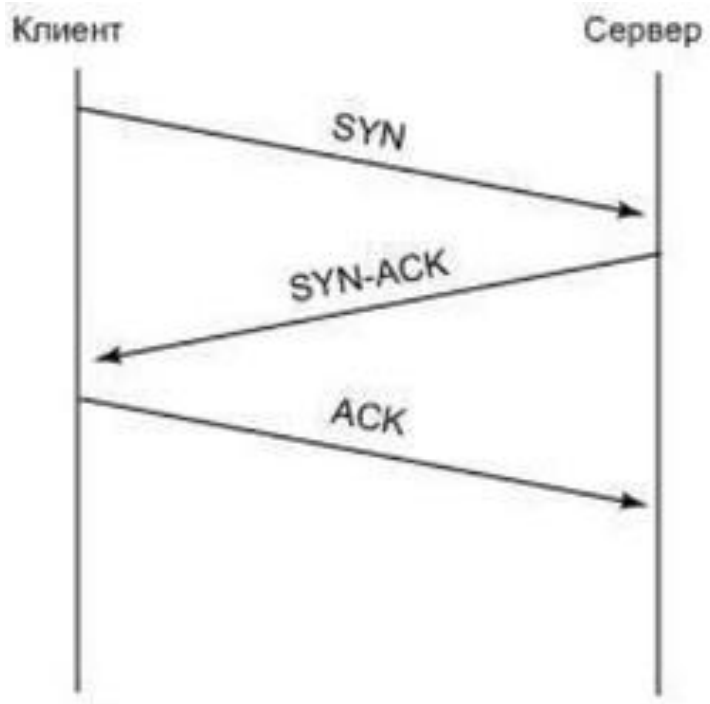
Виды атак

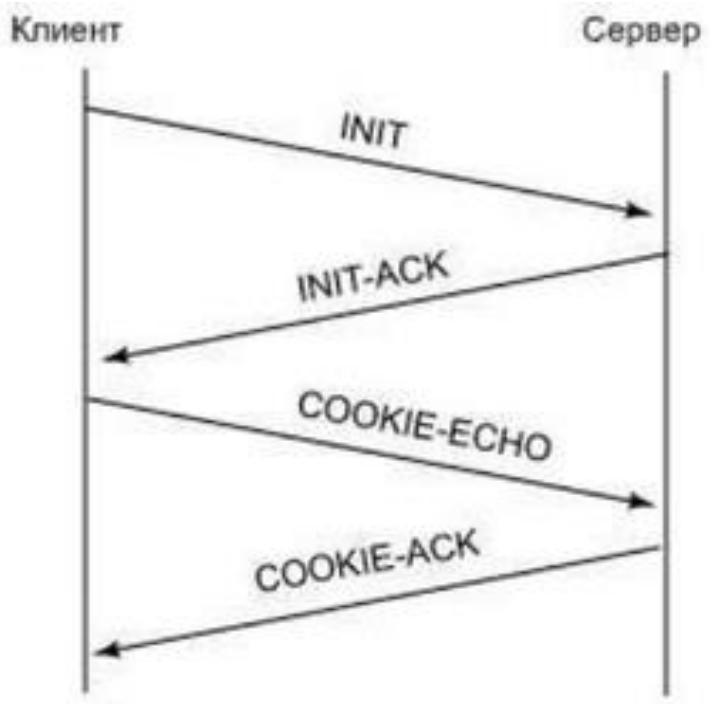
- Подмена IP-адреса
- Подмена ARP
- Подмена маршрута
- Переполнение таблицы маршрутизации
- Атаки на DHCP

Защита от атак

- Проверка обратного маршрута (uRPF-check)
- Dynamic ARP Inspection
- Аутентификация протоколов маршрутизации
- Prefix-list, maximum-prefix
- DHCP snooping (trust, untrust port, IP source guard)

Layer 4 – Транспортный





Layer 4 – Транспортный

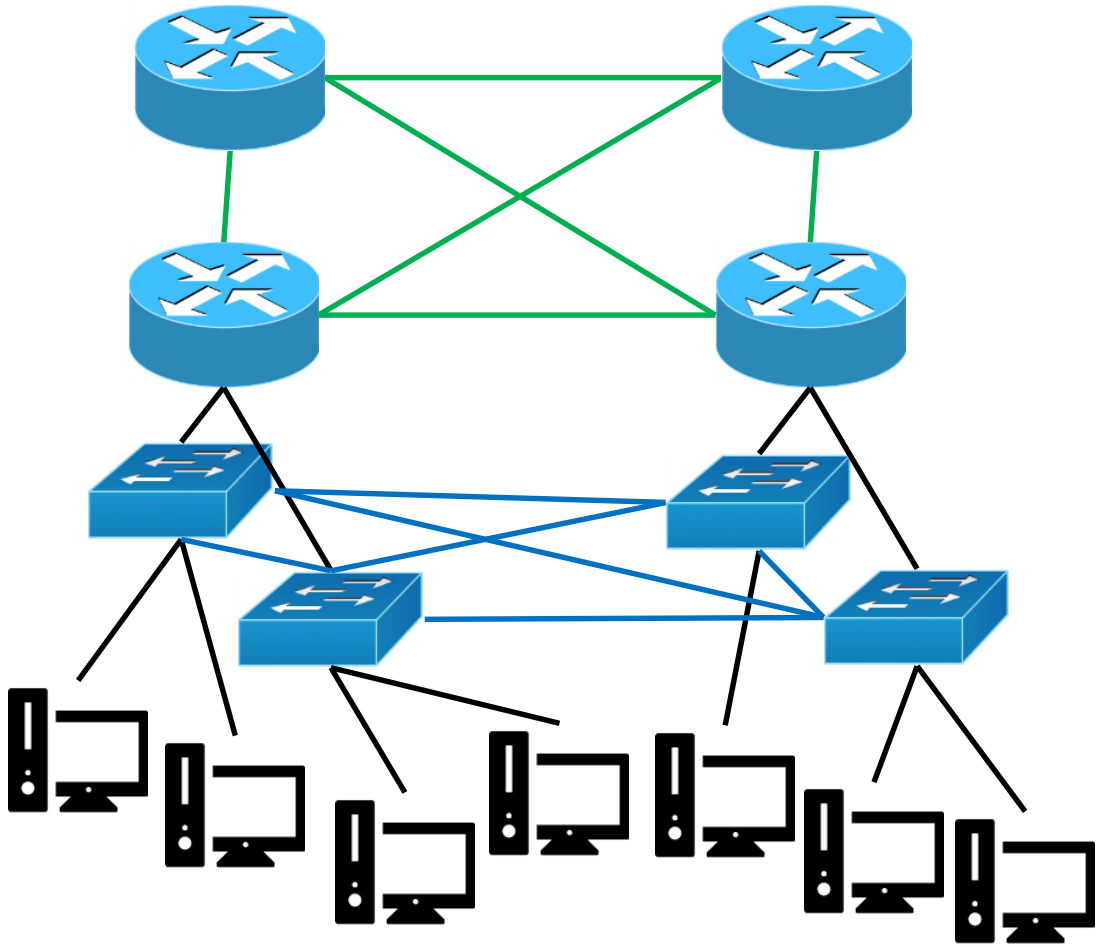
Виды атак

- Sniffing
- Spoofing
- TCP SYN-flood
- TCP hijacking
- UDP amplification DDoS

Защита от атак

- IPSEC
- RPF
- SYN-cookies
- SCTP

IP-сеть. Уровни

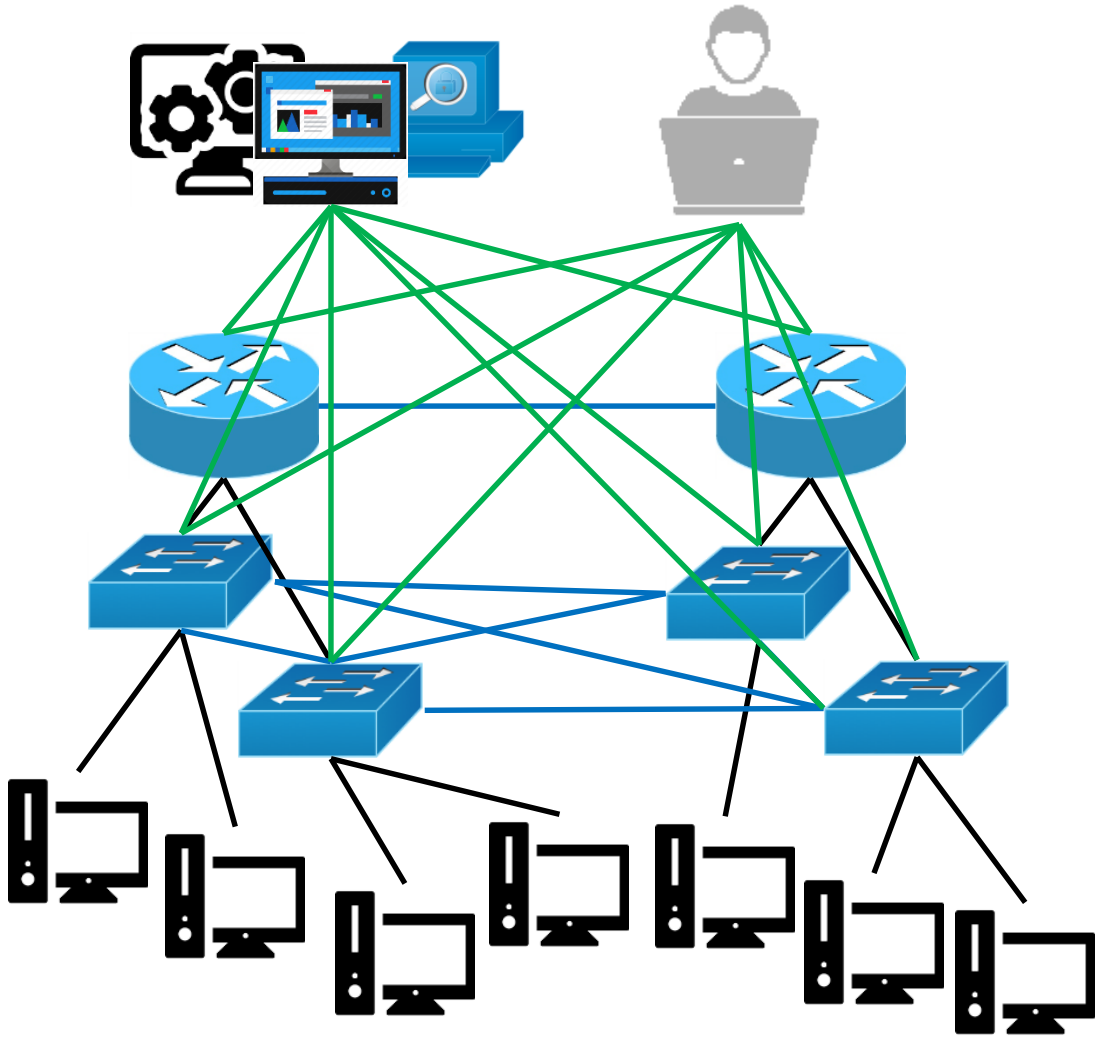


Core

Ditribution

Access

IP-сеть. Плоскости

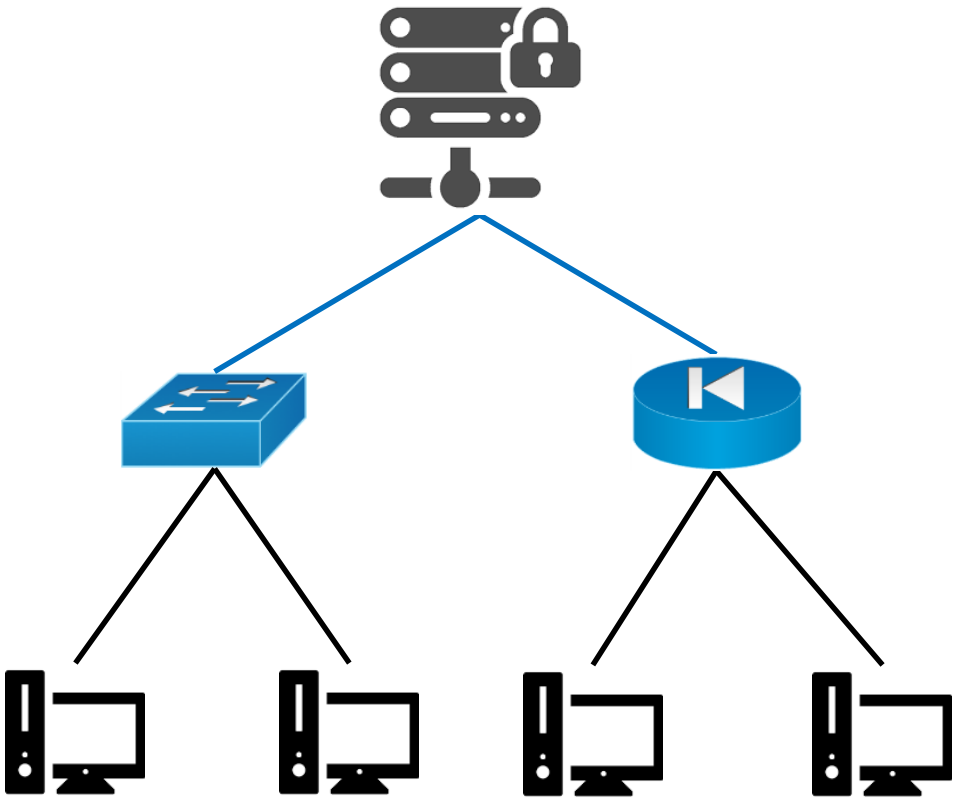


Management plane

Control plane

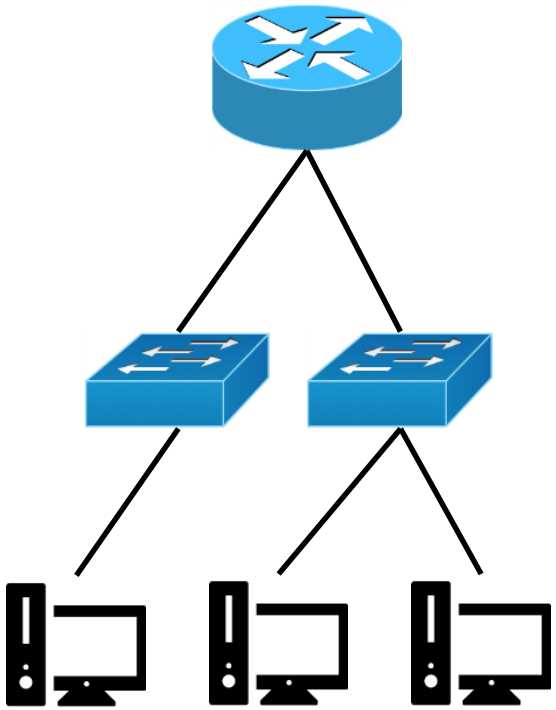
Data plane

802.1x / NAC / DAP



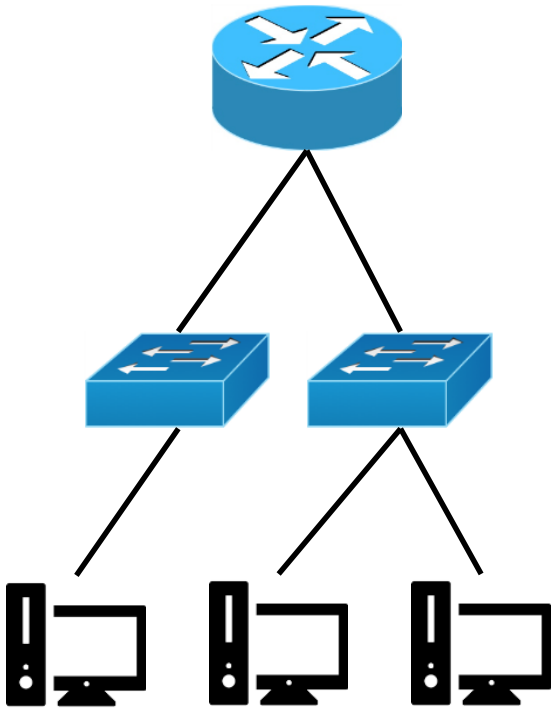
- AAA server
- Network Access Server
- Supplicant/Client

Data Plane



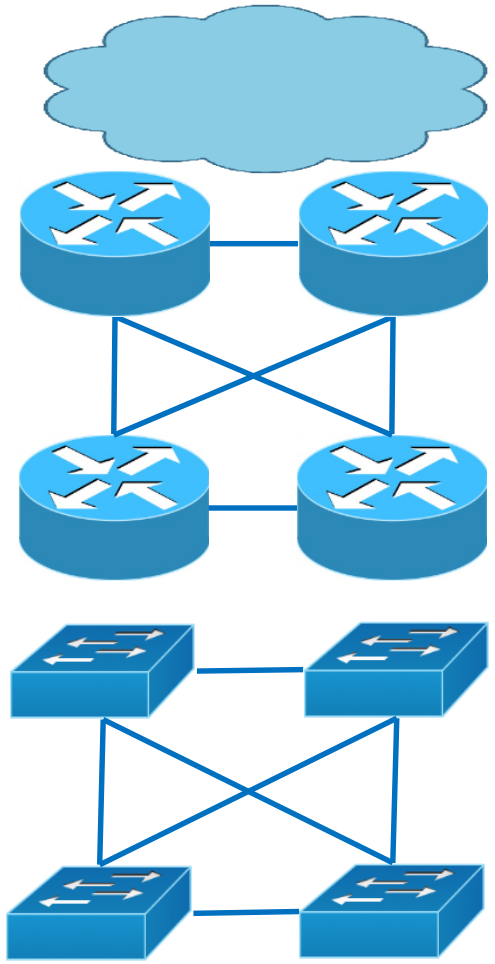
Атака	Защита
Несанкционированный доступ в сеть	802.1x
	NAC
	DAP
	DHCP MAC filtering
Несанкционированный доступ к ресурсам	Firewall/ACL
	IPS
Сетевой червь	PVLAN
	Protected port

Data Plane



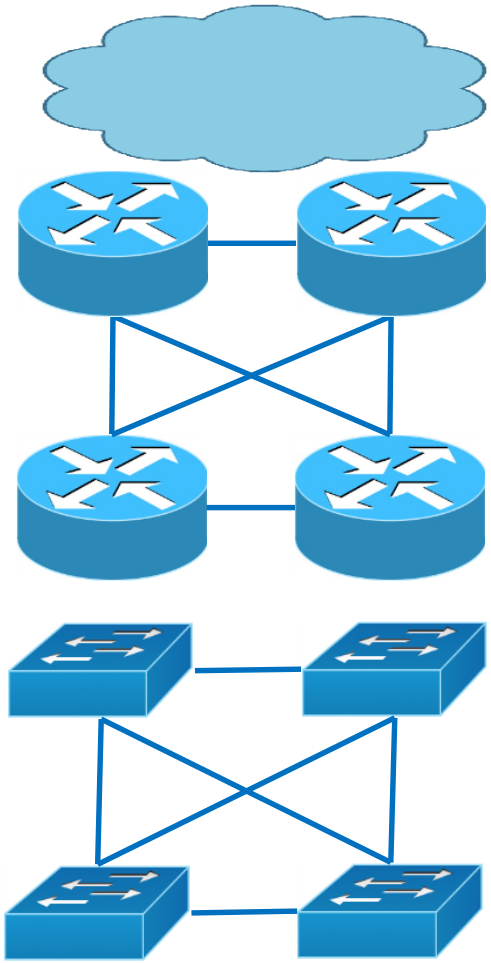
Атака	Защита
Исчерпание CAM	802.1x
	Port security
DHCP starvation	DHCP snooping limit rate
Ложный DHCP	DHCP snooping trusted/untrusted port
ARP spoofing	DAI
IP spoofing	IP source guard
	RPF

Control Plane



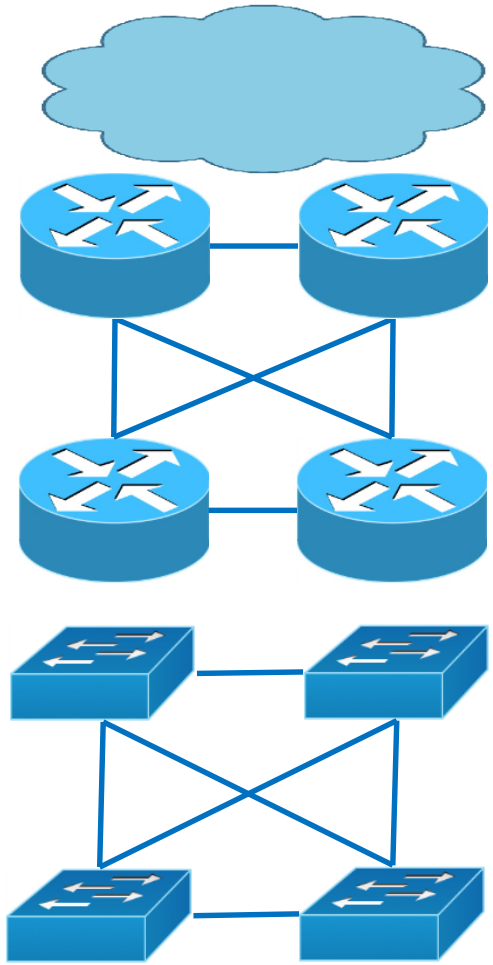
Атака	Защита
L2-петля	STP
	STP-free (VSS+VPC)
Несанкционированное изменение топологии STP	BPDUfilter
	BPDUguard
	Rootguard
	Loopguard
L3-петля	TTL
	Протоколы маршрутизации

Control Plane



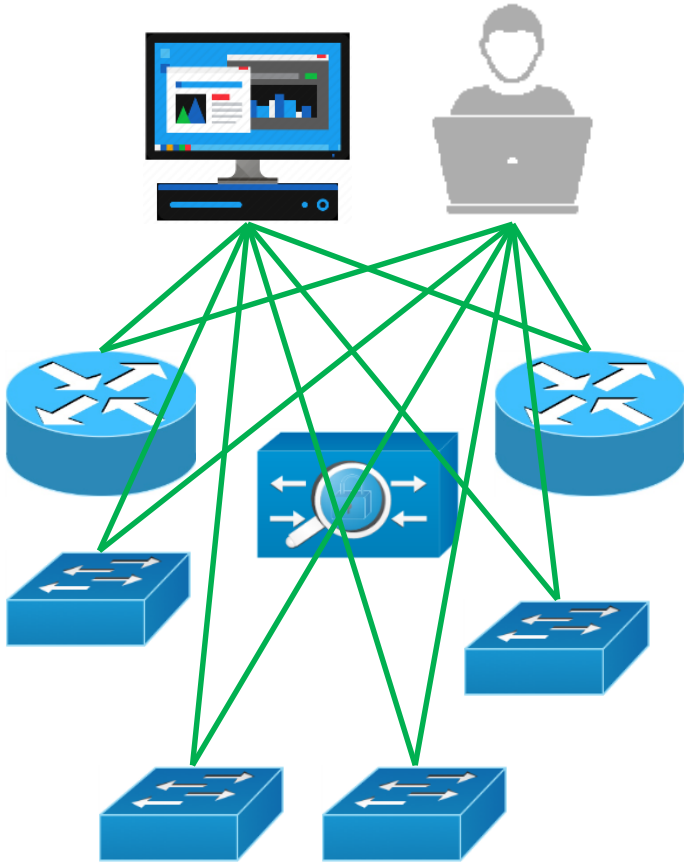
Атака	Защита
Подмена маршрута	Prefix-list
	Аутентификация протоколов маршрутизации
Переполнение таблицы маршрутизации	Prefix-list
	Maximum-prefix

Control Plane



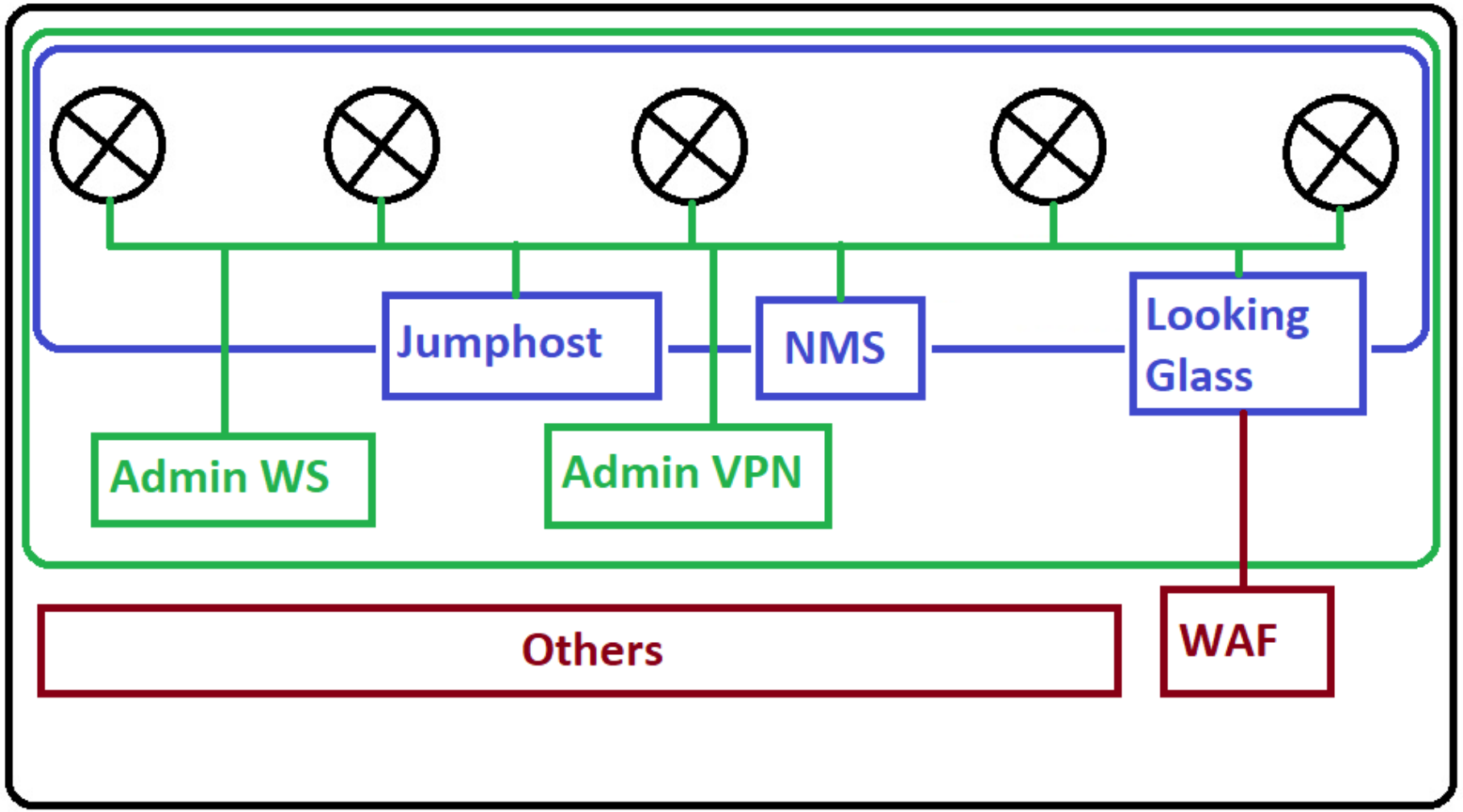
Атака	Защита
Изменение базы VLAN	Nonegotiate
	VTPv3
	no vtp (if)
	VTP password hidden
	VTP domain
	Отказ от VTP в пользу CM

Management Plane



Атака	Защита
Подбор пароля, SNMP community	ACL
	Management interface/VLAN/VRF
	SNMPv3 authpriv
	Password policy
	Scan/check
SMI RCE	no vstack
	Scan/check

Management Plane



Q&A