28.11.2018

Сеть IP/MPLS. Анализ и предотвращение инцидентов

МТС

Ты знаешь, что можешь!

Сеть IP/MPLS. Компоненты


Firewall/VPN


Router


Switch


Admin


User PC


RADIUS

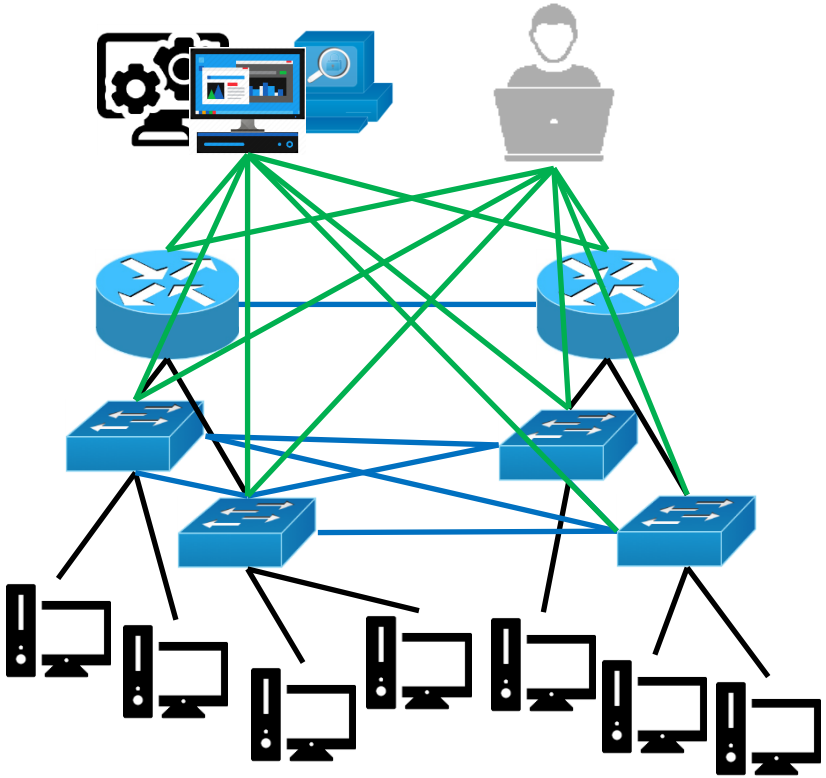

TACACS+


Fault Management
Performance Management


Security Management

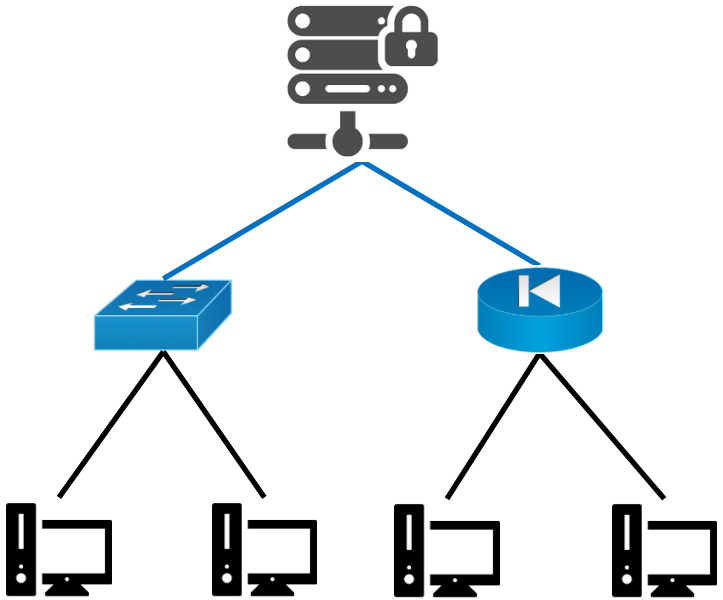

Configuration Management

Сеть IP/MPLS



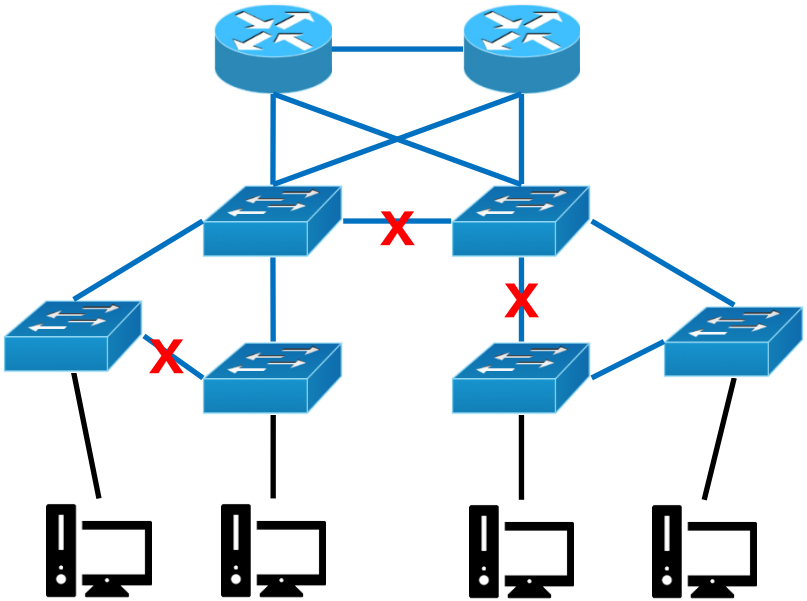
- Data plane
- Control plane
- Management plane

802.1x / NAC / DAP



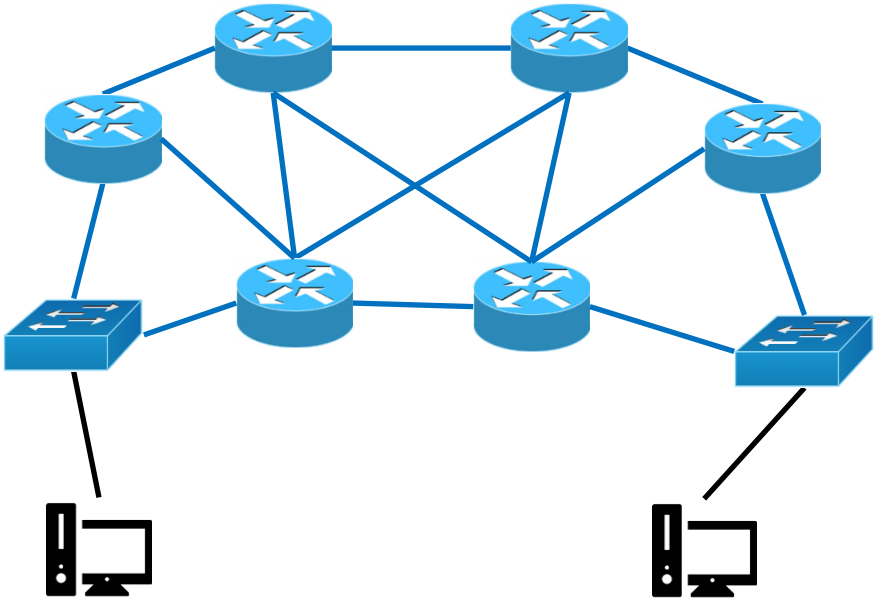
- AAA Server
- Network Access Server
- Supplicant/Client

Spanning Tree Protocol



- STP root
- STP instances

Routing protocols



- Static
- Dynamic
- MPLS L3VPN

Checker / Shodan API

- `:~$ sudo easy_install shodan #установка`
- `:~$ shodan init <API_KEY> #активация`
- `:~$ shodan myip #проверка`

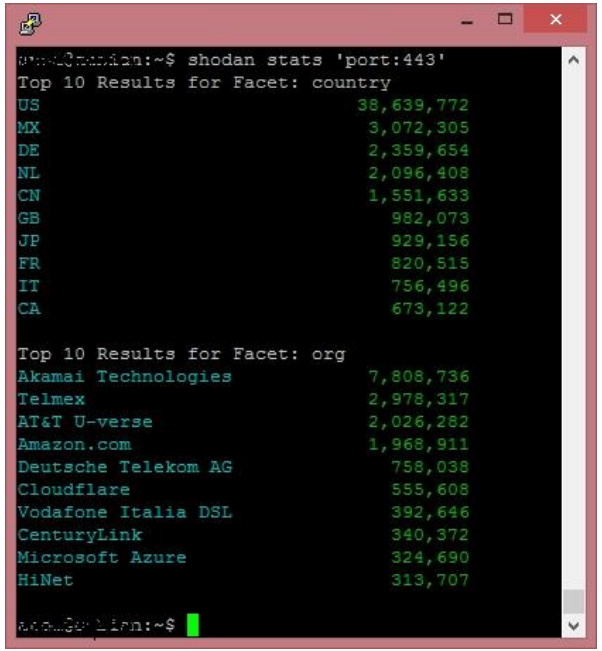
`<IP-address>`

- `:~$ shodan info #проверка`

`Query credits available: <count>`

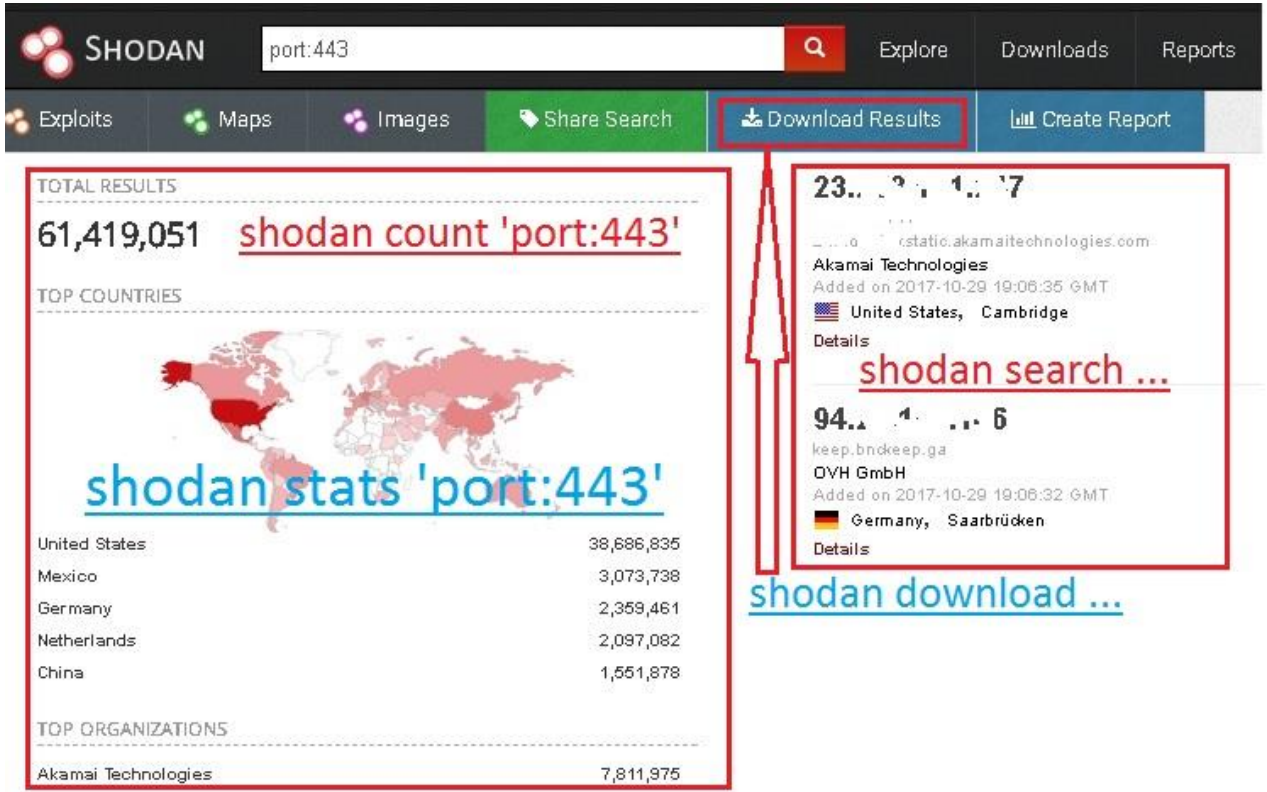
`Scan credits available: <count>`

Shodan API

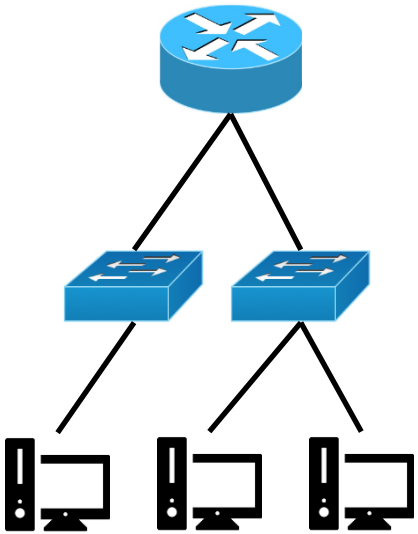



```
:~$ shodan --help
Usage: shodan [OPTIONS] COMMAND [ARGS]...
...
Commands:
...
  count          <описание>
  ...
  host           <описание>
  ...
  search         <описание>
  stats          <описание>
  ...
```

Shodan WEB & API

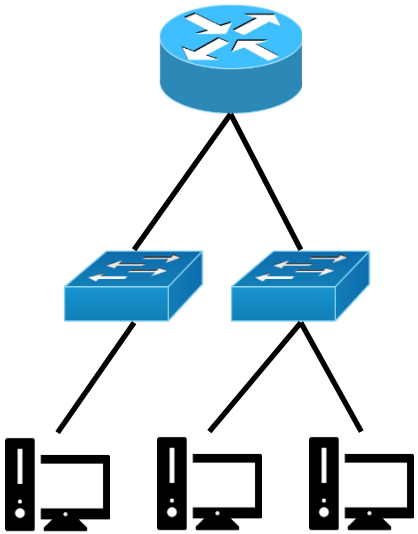


Data plane



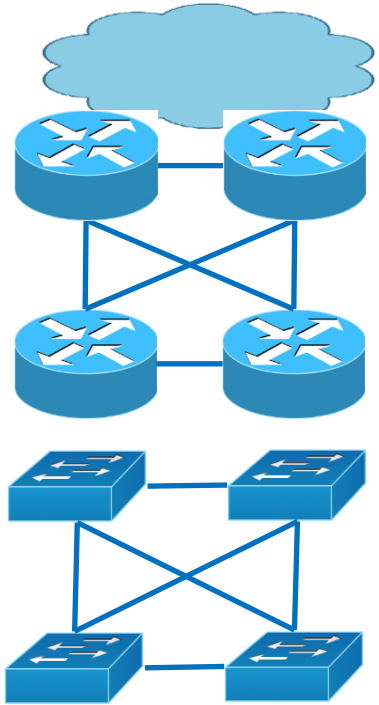
Инцидент	Предотвращение
Несанкционированный доступ в сеть	802.1x
	NAC
	DAP
	DHCP MAC filtering
Несанкционированный доступ к ресурсам	Firewall/ACL
	IPS
Сетевой червь	PVLAN
	Protected port

Data plane



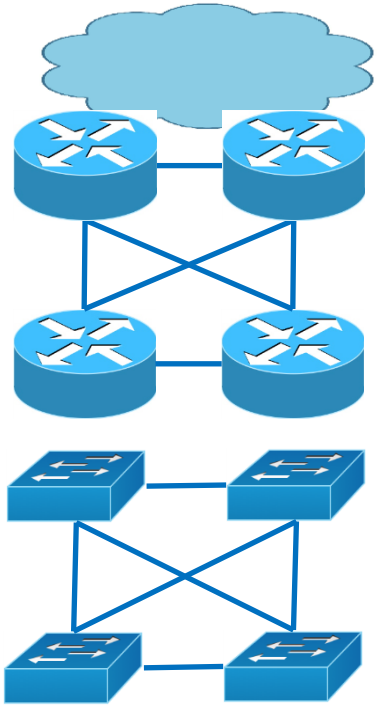
Инцидент	Предотвращение
Исчерпание CAM	802.1x
	Port security
DHCP starvation	DHCP snooping limit rate
Ложный DHCP	DHCP snooping trusted/untrusted port
ARP spoofing	DAI
IP spoofing	IP source guard
	RPF

Control plane



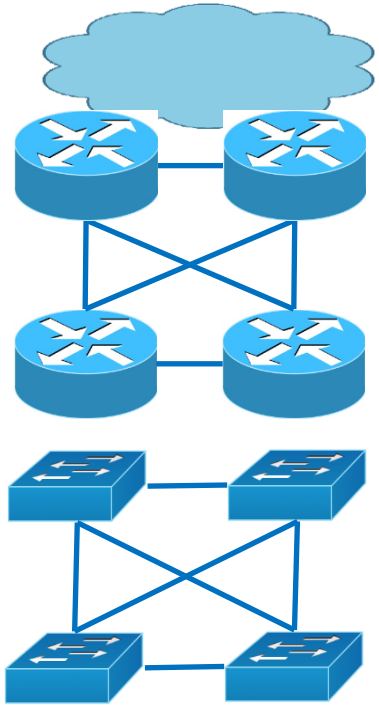
Инцидент	Предотвращение
L2-петля	STP
	STP-free (VSS+VPC)
Несанкционированное изменение топологии STP	BPDUfilter
	BPDUguard
	Rootguard
	Loopguard
L3-петля	TTL
	Протоколы маршрутизации

Control plane



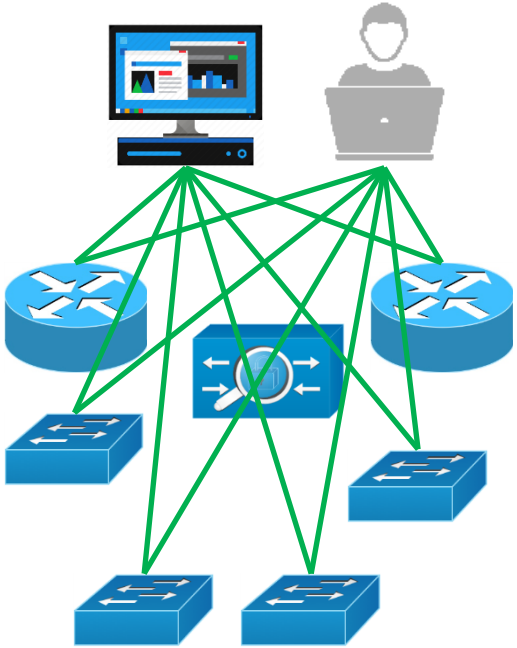
Инцидент	Предотвращение
Подмена маршрута	Prefix-list
	Аутентификация протоколов маршрутизации
Переполнение таблицы маршрутизации	Prefix-list
	Maximum-prefix

Control plane



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

Management plane



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

Management plane control

- **:~$ shodan search '<syntax_as_web>'**

<вывод результатов>

OR Security_scanner

- **Парсинг результатов в SIEM:**
  - **Управляющие протоколы (telnet, ssh, snmp, http, https, API)**
  - **Сервисы с настройками по умолчанию**
  - **Уязвимые сервисы (SMI)**
- **Генерация инцидента**

Incident generation algo

- **IF**
  - **Scanner OR Shodan scan results**
  - **AND dst port [22 | 23 | 80 | 161 | 443 | 4786]**
  - **AND service eq [ssh | telnet | http | https | snmp | API | SMI]**
  - **AND host in [MTS NET_MGMT_IFACES]**
- **THEN**
  - **INCIDENT**

МТС Ты знаешь, что можешь!