

28.11.2018

Сеть IP/MPLS. Анализ и предотвращение инцидентов



Ты знаешь, что можешь!

Сеть IP/MPLS. Компоненты



Firewall/VPN



RADIUS



Router



TACACS+



Switch



Fault Management
Performance Management



Admin



Security Management

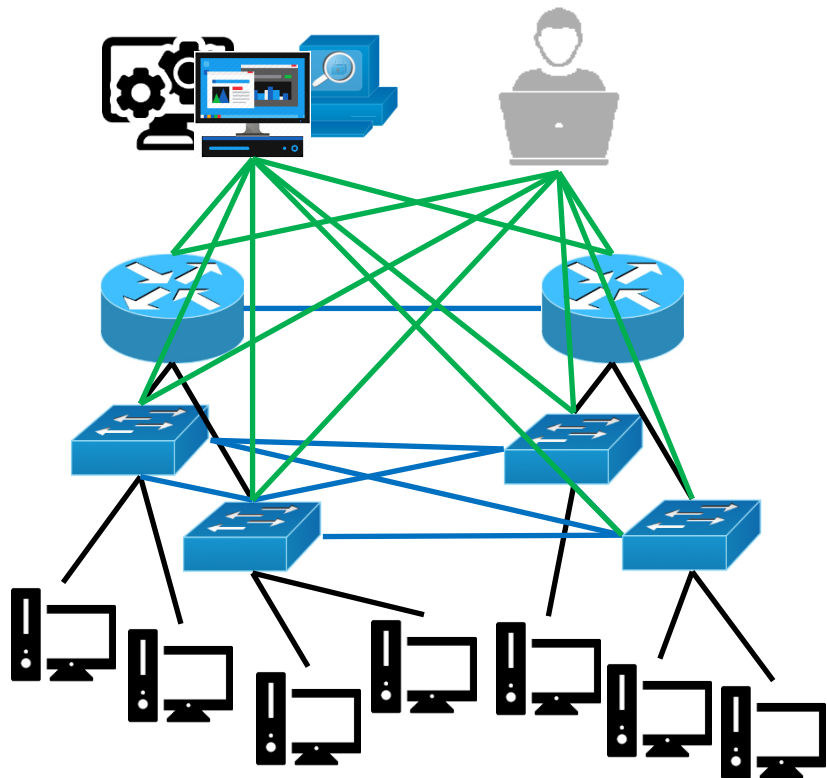


User PC



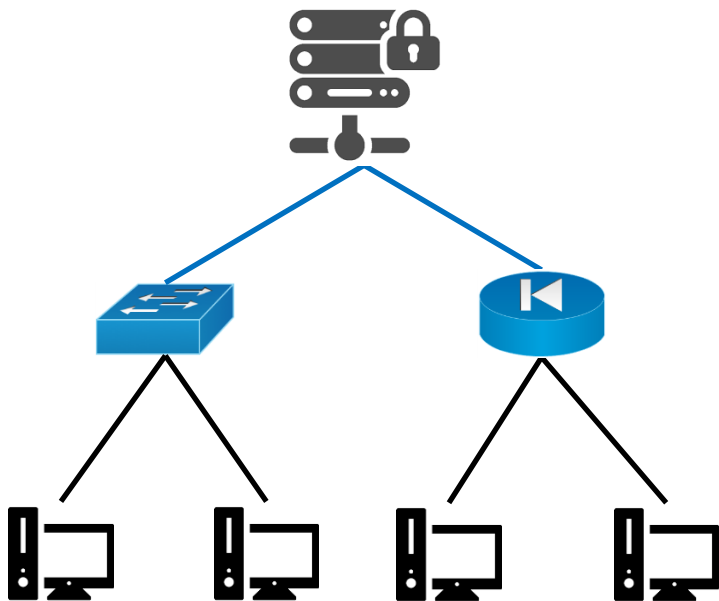
Configuration Management

Сеть IP/MPLS



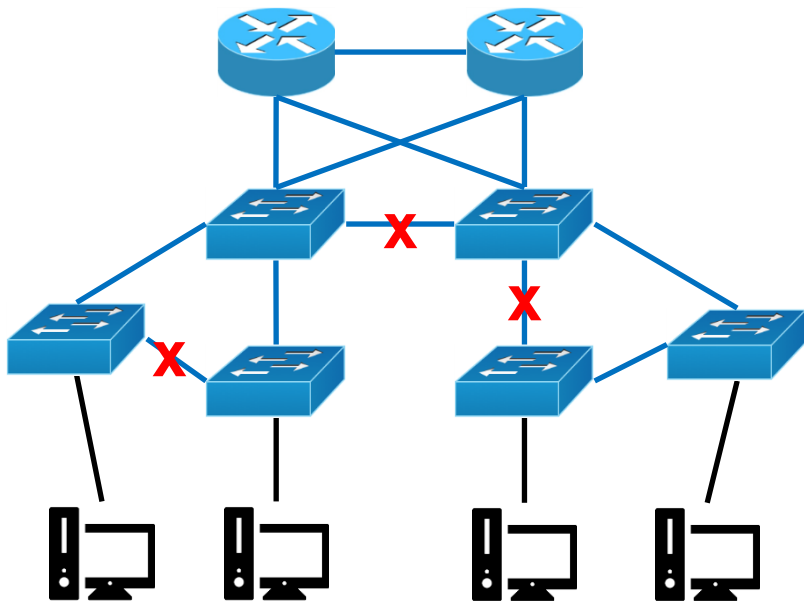
- › Data plane
- › Control plane
- › Management plane

802.1x / NAC / DAP



- AAA Server
- Network Access Server
- Supplicant/Client

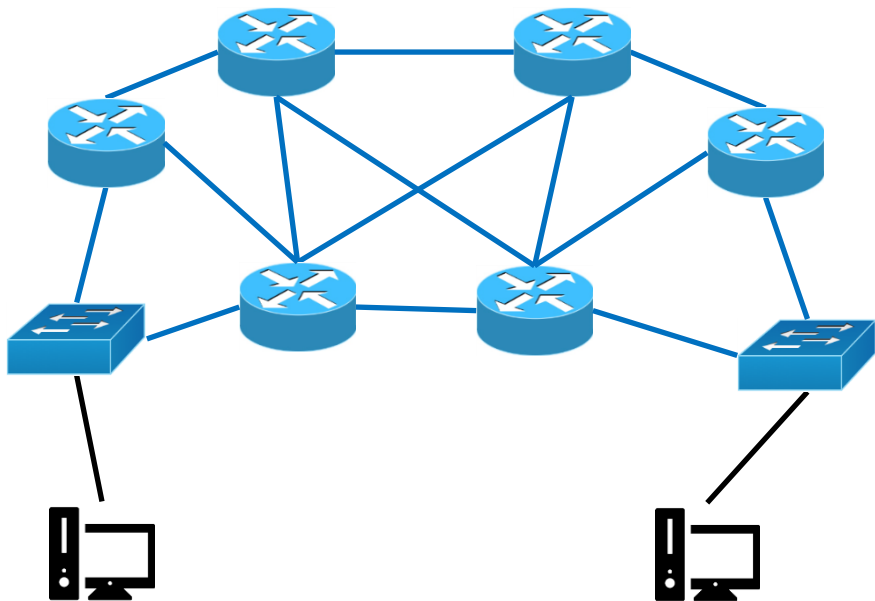
Spanning Tree Protocol



➤ 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

```
root@kali:~# shodan stats 'port:443'
Top 10 Results for Facet: country
US          38,639,772
MX          3,072,305
DE          2,359,654
NL          2,096,408
CN          1,551,633
GB          982,073
JP          929,156
FR          820,515
IT          756,496
CA          673,122

Top 10 Results for Facet: org
Akamai Technologies 7,808,736
Telmex              2,978,317
AT&T U-verse        2,026,282
Amazon.com          1,968,911
Deutsche Telekom AG 758,038
Cloudflare          555,608
Vodafone Italia DSL 392,646
CenturyLink         340,372
Microsoft Azure     324,690
HiNet               313,707

root@kali:~#
```

➤ :~\$ shodan --help

Usage: shodan [OPTIONS] COMMAND [ARGS]...

...

Commands:

...

count <описание>

...

host <описание>

...

search <описание>

stats <описание>

...

Shodan WEB & API

The screenshot displays the Shodan search interface. At the top, the search bar contains 'port:443'. Below the search bar, there are navigation tabs: Exploits, Maps, Images, Share Search, Download Results (highlighted with a red box), and Create Report. The main content area is divided into two sections. The left section, titled 'TOTAL RESULTS', shows '61,419,051 shodan count 'port:443'' and 'TOP COUNTRIES' with a world map and a table of countries. The right section, titled '23.. .. 1.. .. 17', shows details for a specific result, including the domain 'static.akamai technologies.com', organization 'Akamai Technologies', location 'United States, Cambridge', and a link to 'shodan search ...'. Below this, another result is shown for '94.. .. 6' with domain 'keep.bnkeep.ga', organization 'OVH GmbH', location 'Germany, Saarbrücken', and a link to 'shodan download ...'.

TOTAL RESULTS

61,419,051 shodan count 'port:443'

TOP COUNTRIES

shodan stats 'port:443'

United States	38,686,835
Mexico	3,073,738
Germany	2,359,461
Netherlands	2,097,082
China	1,551,878

TOP ORGANIZATIONS

Akamai Technologies	7,811,975
---------------------	-----------

23.. .. 1.. .. 17

static.akamai technologies.com

Akamai Technologies

Added on 2017-10-29 19:06:35 GMT

United States, Cambridge

Details

shodan search ...

94.. .. 6

keep.bnkeep.ga

OVH GmbH

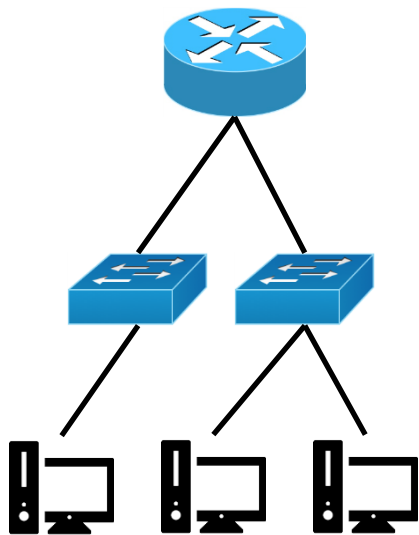
Added on 2017-10-29 19:06:32 GMT

Germany, Saarbrücken

Details

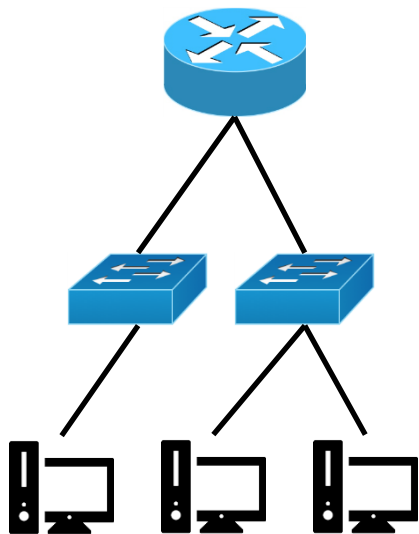
shodan download ...

Data plane



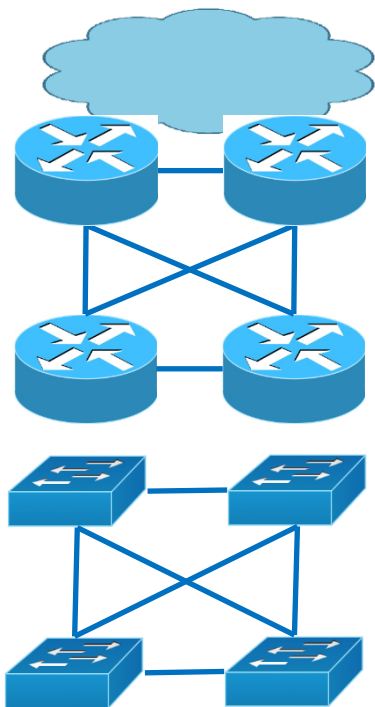
Инцидент	Предотвращение
Несанкционированный доступ в сеть	802.1x
	NAC
	DAP
	DHCP MAC filtering
Несанкционированный доступ к ресурсам	Firewall/ACL
	IPS
Сетевой червь	PVLAN
	Protected port

Data plane



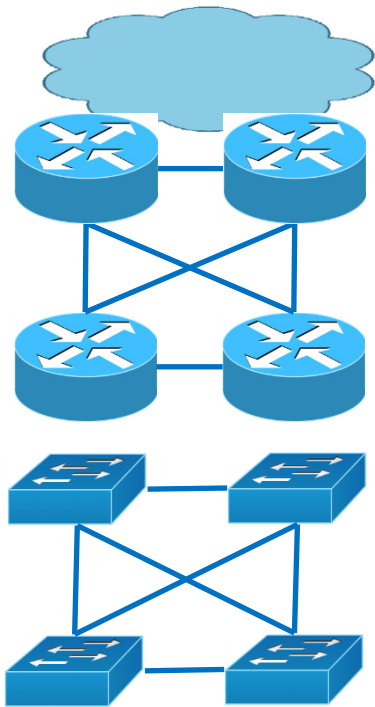
Инцидент	Предотвращение
Исчерпание CAM	802.1x
	Port security
DHCP starvation	DHCP snooping limit rate
Ложный DHCP	DHCP snooping trusted/untrusted port
ARP spoofing	DAI
IP spoofing	IP source guard
	RPF

Control plane



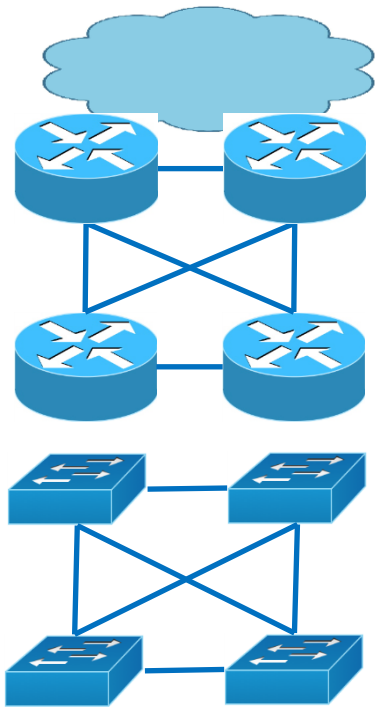
Инцидент	Предотвращение
L2-петля	STP
	STP-free (VSS+VPC)
Несанкционированное изменение топологии STP	BPDUfilter
	BPDUguard
	Rootguard
	Loopguard
L3-петля	TTL
	Протоколы маршрутизации

Control plane



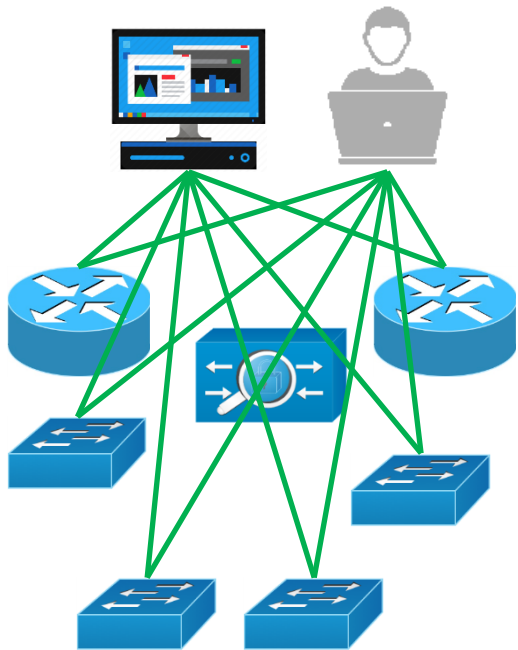
Инцидент	Предотвращение
Подмена маршрута	Prefix-list
	Аутентификация протоколов маршрутизации
Переполнение таблицы маршрутизации	Prefix-list
	Maximum-prefix

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**



Ты знаешь, что можешь!