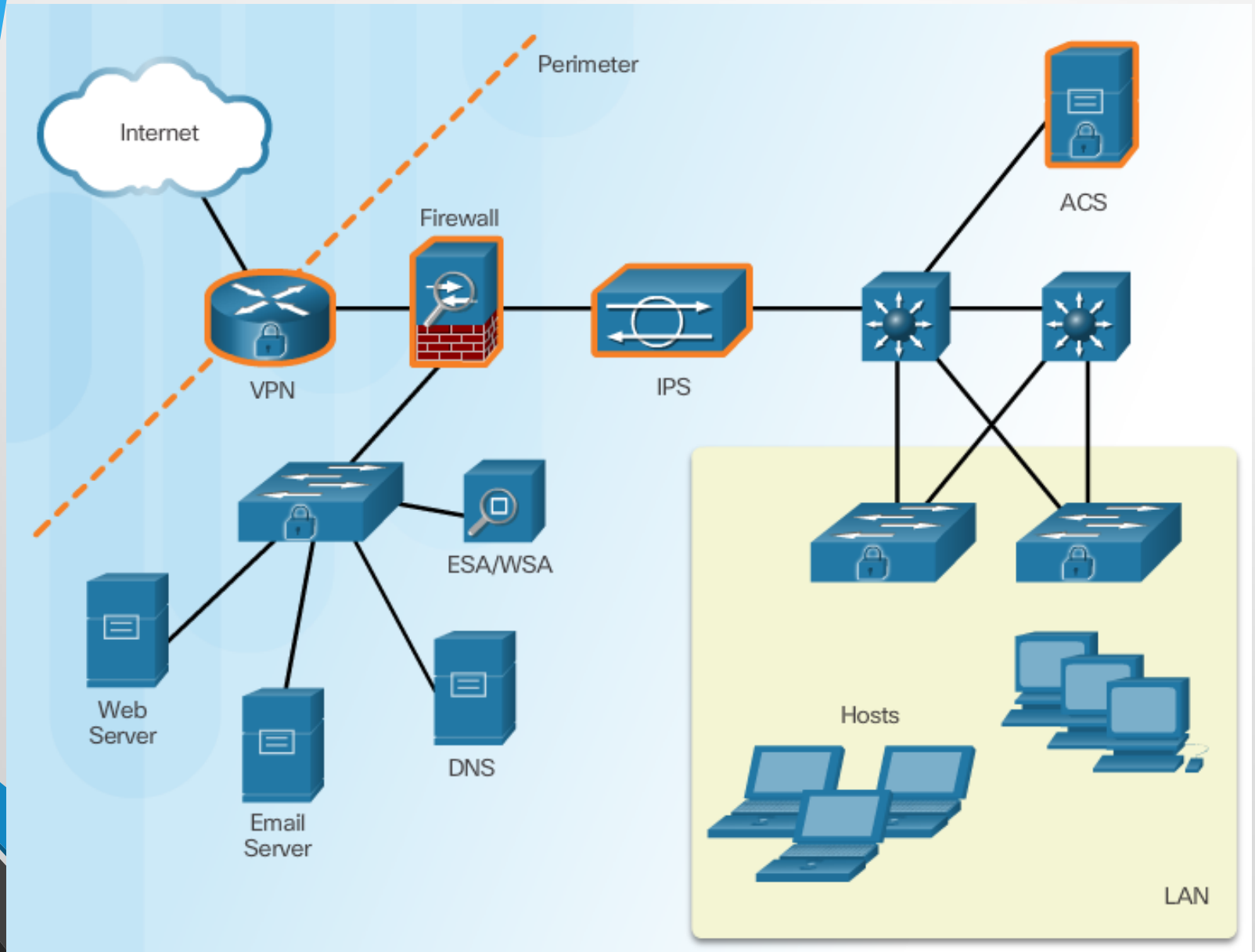
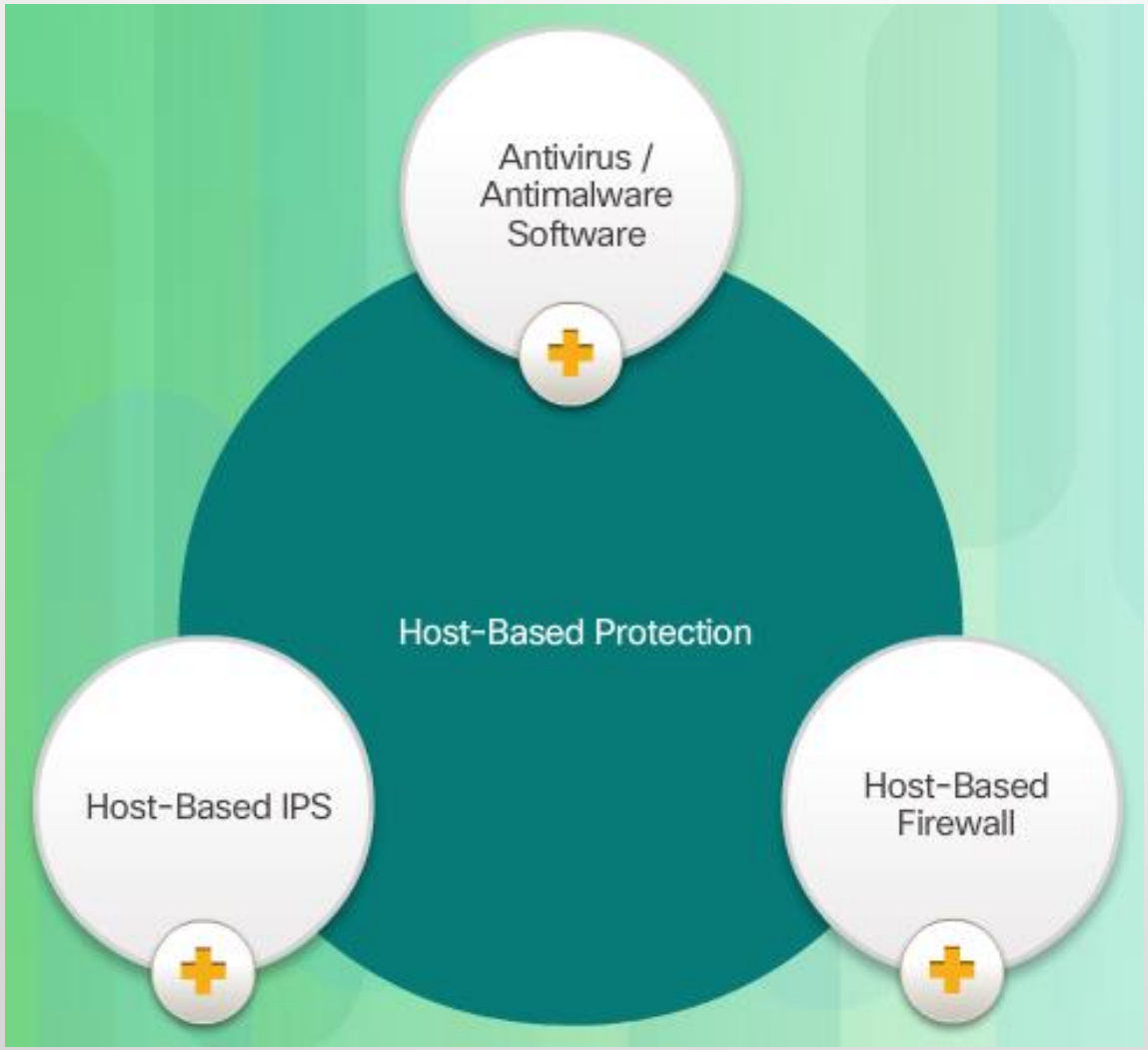
Лекция 9
Обеспечение безопасности локальной сети (LAN)

Тема Знакомство с безопасностью оконечных устройств

Защита элементов сети LAN



Обеспечение безопасности оконечных устройств традиционным способом



Сеть без границ

Обеспечение безопасности оконечных устройств в сети без границ

Вопросы, которые следует задать после вредоносной атаки:

- Откуда произошла атака?
- Каковы метод атаки и точка вторжения?
- Какие системы были затронуты?
- Что сделала угроза?
- Можно ли остановить угрозу и ее первопричину?
- Как восстановить систему?
- Как предотвратить угрозы в дальнейшем?

Защита на хосте:

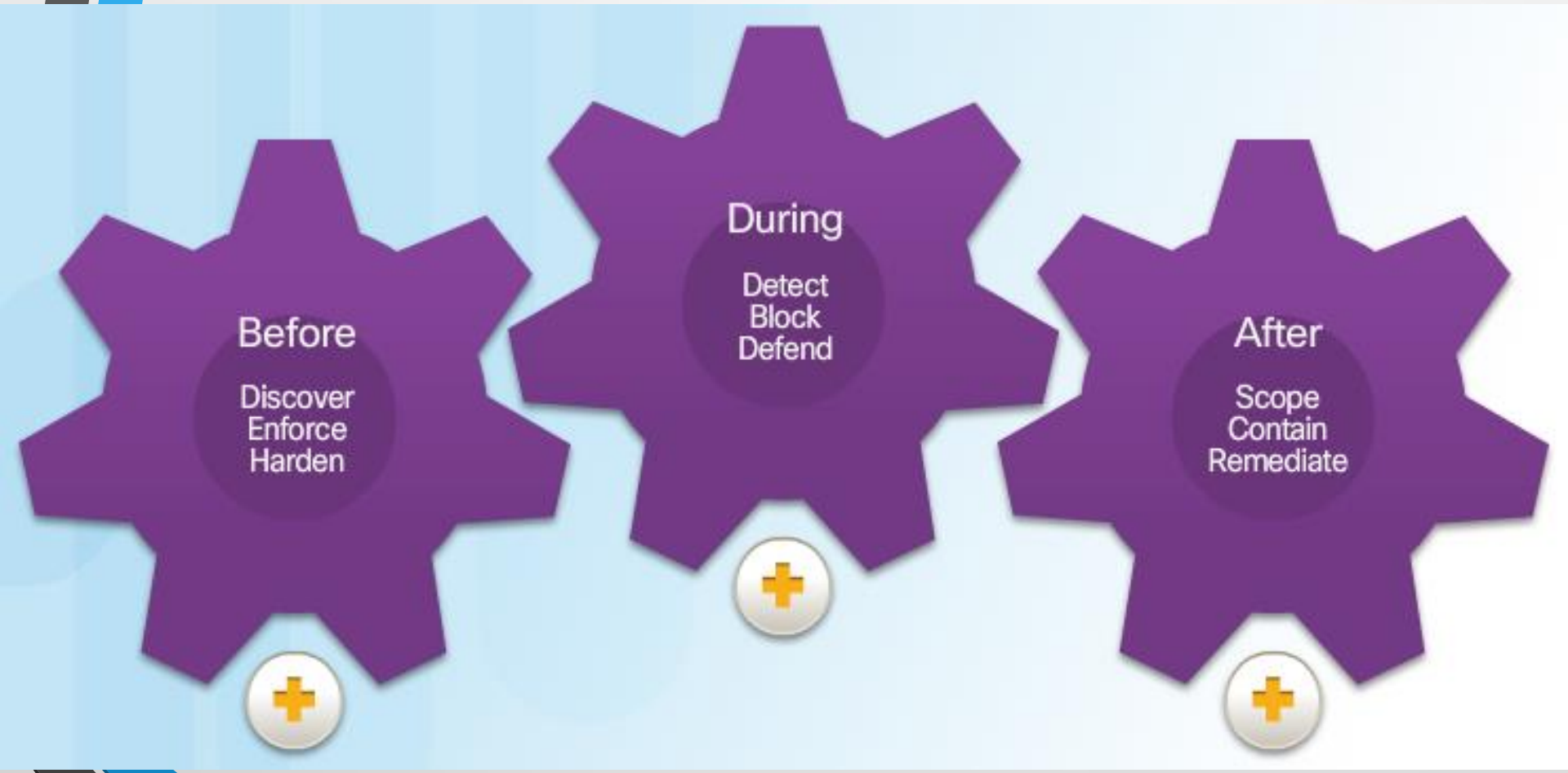
- Антивирус/антивредоносное ПО
- Фильтрация спама
- Фильтрация URL-адресов
- Черные списки
- Предотвращение потери данных (DLP)

Современные решения для безопасности оконечных устройств

Аппаратное и программное шифрование локальных данных

Тема Защита от вредоносного ПО

Усовершенствованная защита от вредоносного ПО



AMP и управляемая защита от угроз

Команды Talos собирают аналитические данные об угрозах в реальном времени из разных источников:

- 1,6 миллиона развернутых устройств обеспечения безопасности, включая межсетевые экраны, IPS, решения защиты веб-трафика и устройства обеспечения безопасности электронной почты
- 150 млн оконечных устройств

Затем они анализируют эти данные:

- 100 ТБ ежедневной аналитики безопасности
- 13 млрд веб-запросов в день
- 35% мирового корпоративного трафика электронной почты

AMP для оконечных устройств

- **AMP для оконечных устройств** (AMP for Endpoints) интегрируется с решением Cisco AMP для сетей (Cisco AMP for Networks), чтобы обеспечить комплексную защиту по всей распределенной сети и оконечным устройствам.
- **AMP для сетей** (AMP for Networks) представляет собой сетевое решение и интегрируется в самостоятельные устройства сетевой безопасности Cisco ASA Firewall и Cisco FirePOWER.
- **AMP для защиты контента** (AMP for Content Security) представляет собой функцию, интегрированную в устройства Cisco Cloud Web Security или устройства Cisco Web и Email Security для защиты от вредоносных атак через электронную почту или веб-трафик.

Тема
Защита электронной почты и веб-трафика

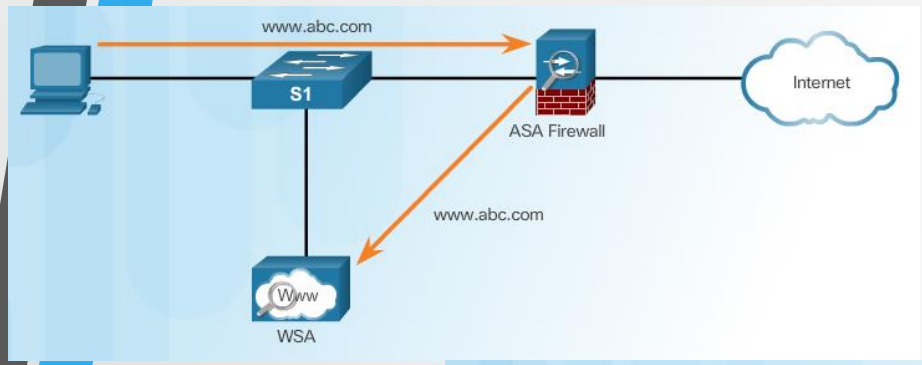
Защита электронной почты и веб-трафика

Устройство защиты электронной почты Cisco ESA

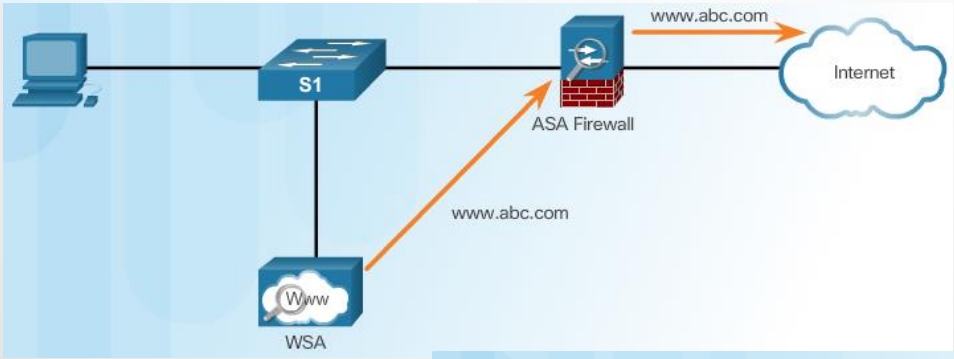
Функции и преимущества решений Cisco для защиты электронной почты:

- Глобальные аналитические данные по угрозам
- Блокировка спама
- Усовершенствованная защита от вредоносного ПО
- Средства управления исходящими сообщениями

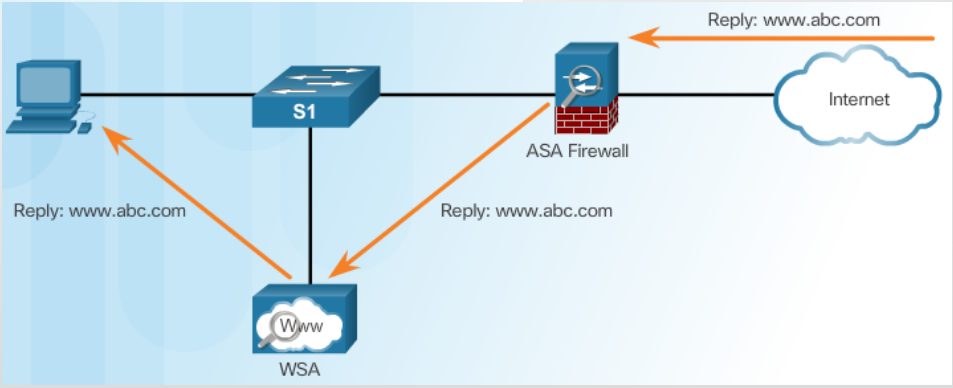
Устройство защиты веб-трафика Cisco WSA



Клиент инициирует веб-запрос



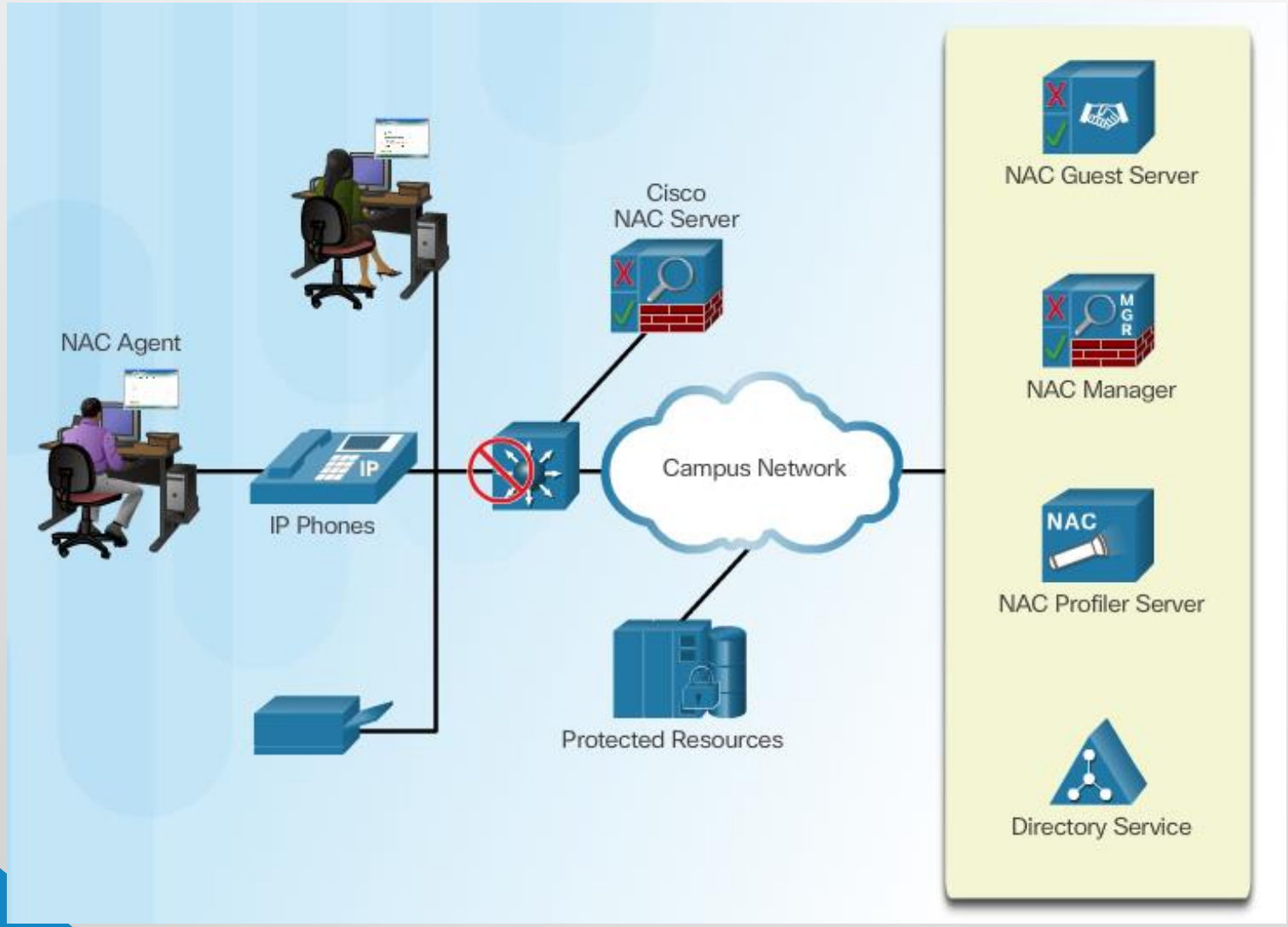
WSA пересылает запрос



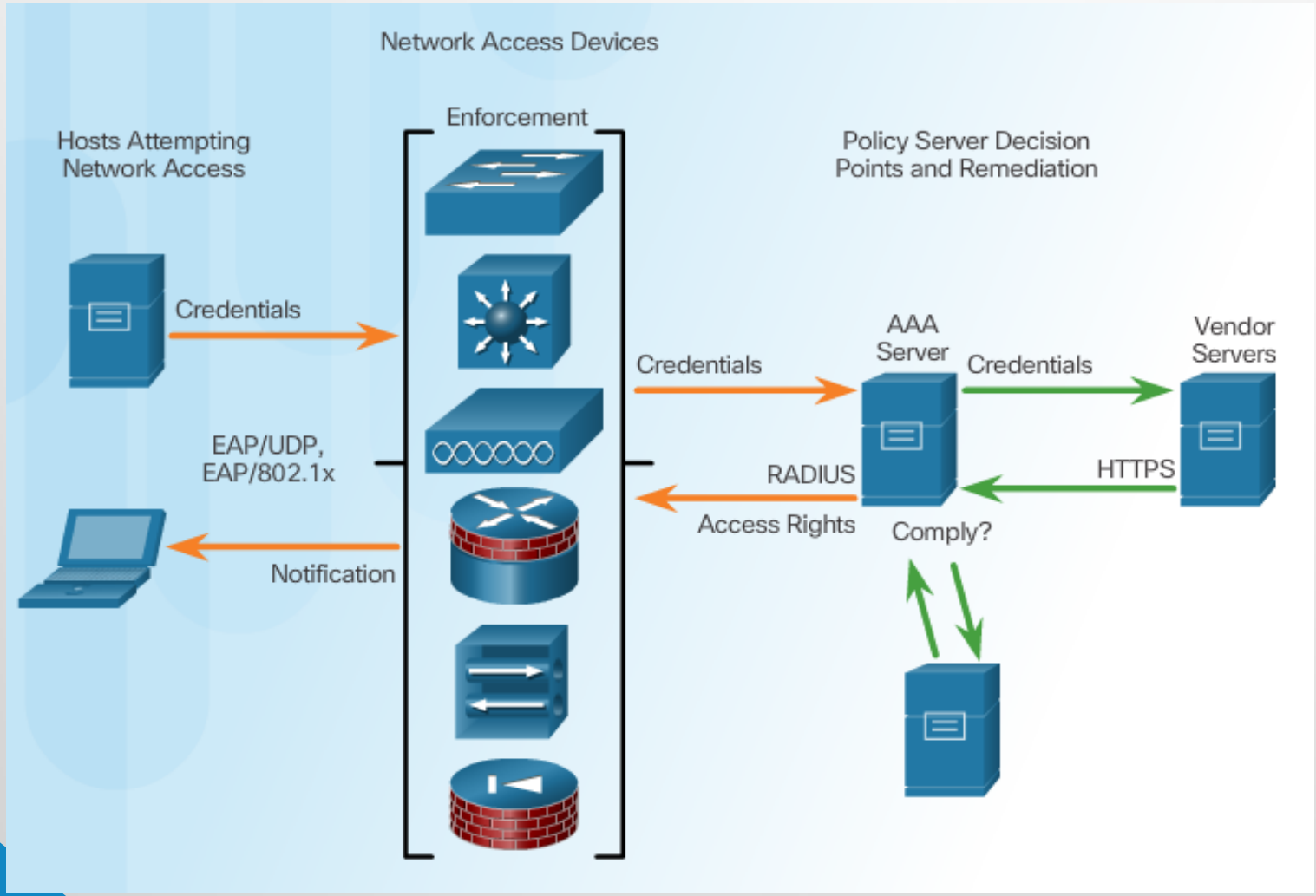
Ответ отправляется на WSA, а затем на клиента

Тема
Контроль сетевого доступа

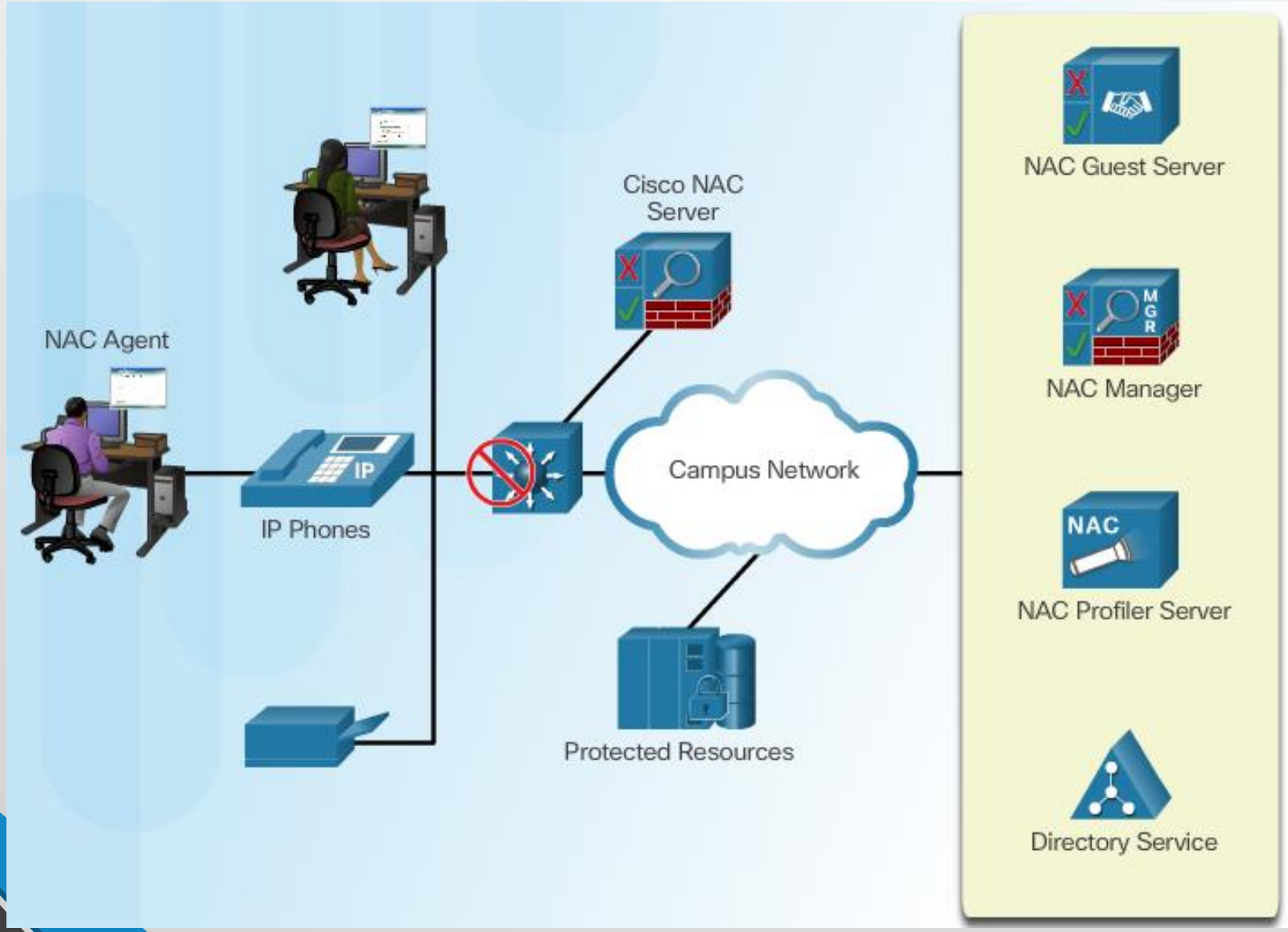
Решения Cisco для контроля доступа к сети



Функции Cisco NAC



Компоненты Cisco NAC

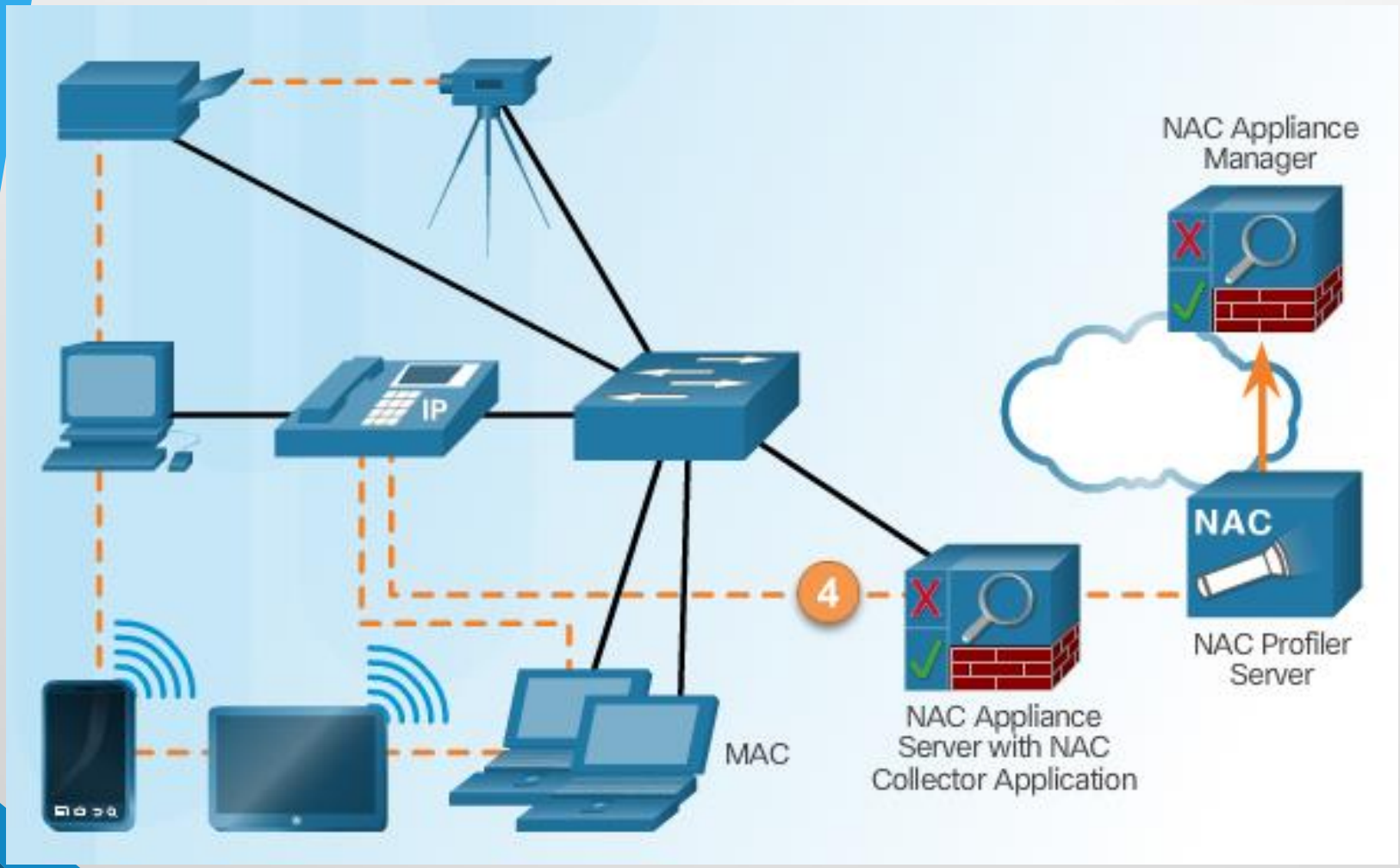


Сетевой доступ для гостей

Предоставлять полномочия спонсора можно тремя способами:

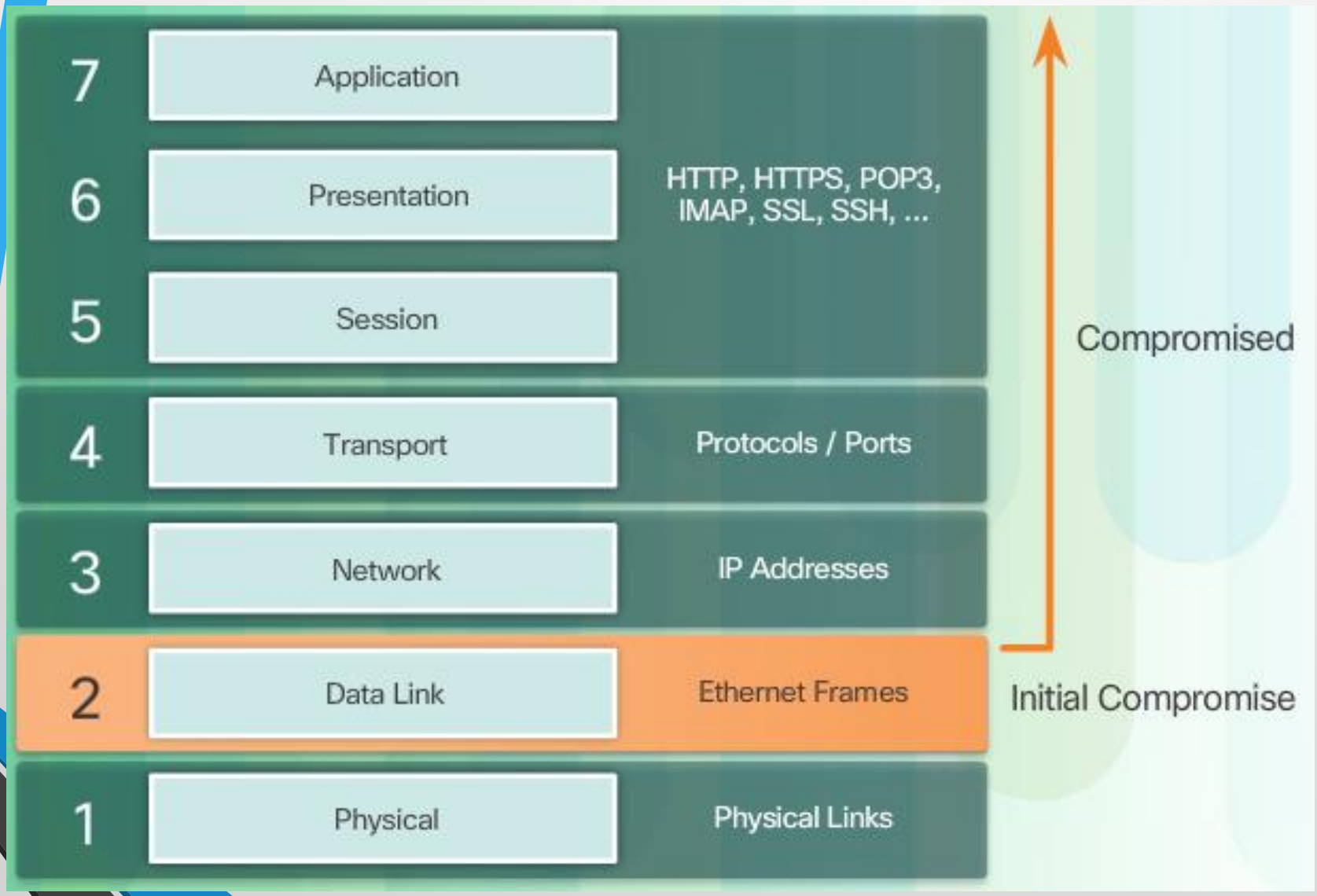
- только учетным записям, созданным спонсором
- всем учетным записям
- никаким учетным записям (т. е. пользователи не смогут изменять никакие полномочия)

Профайлер Cisco NAC



Тема Угрозы безопасности уровня 2

Описание уязвимостей на 2-м уровне



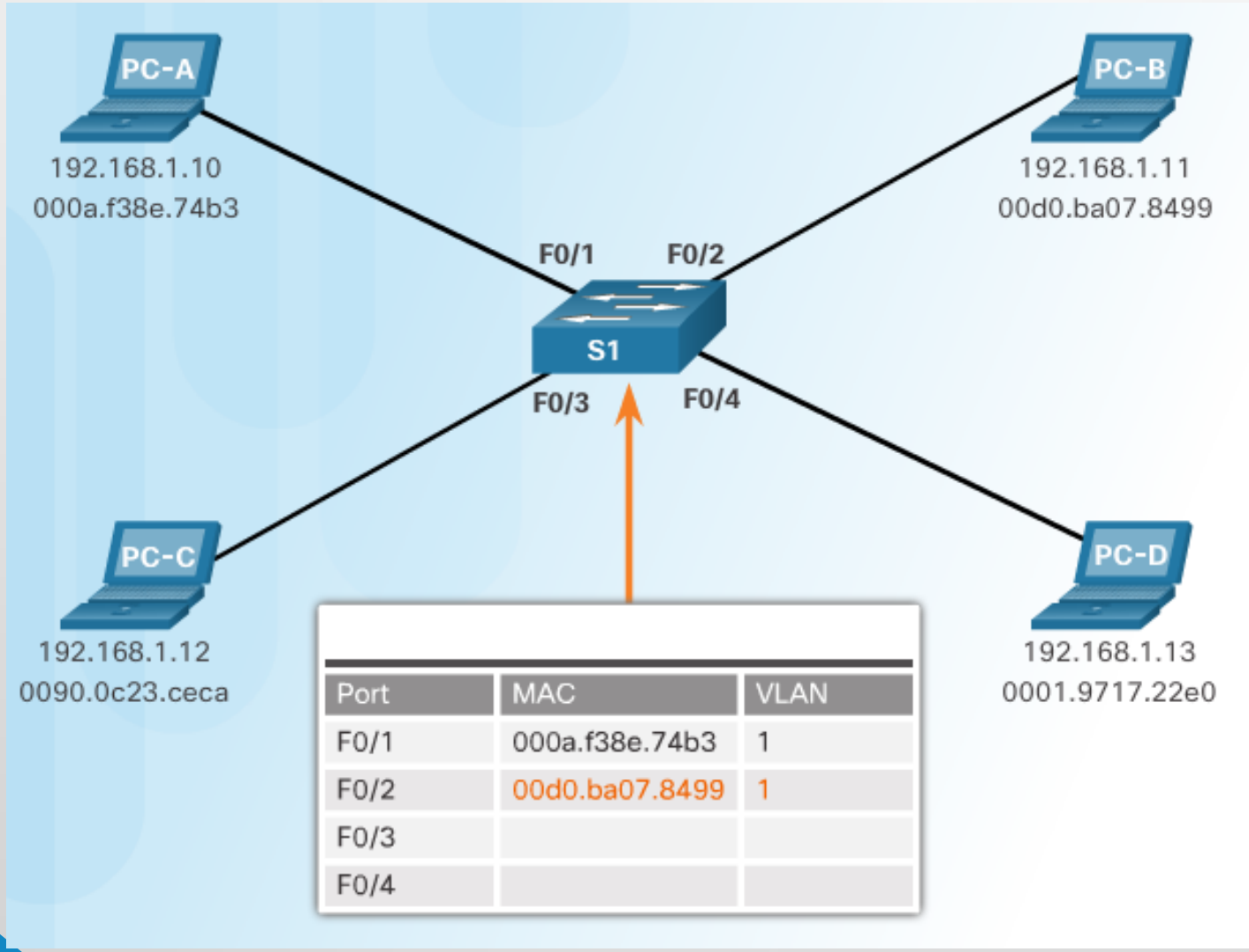
Категории атак на коммутаторы

Тема Атаки на таблицы CAM

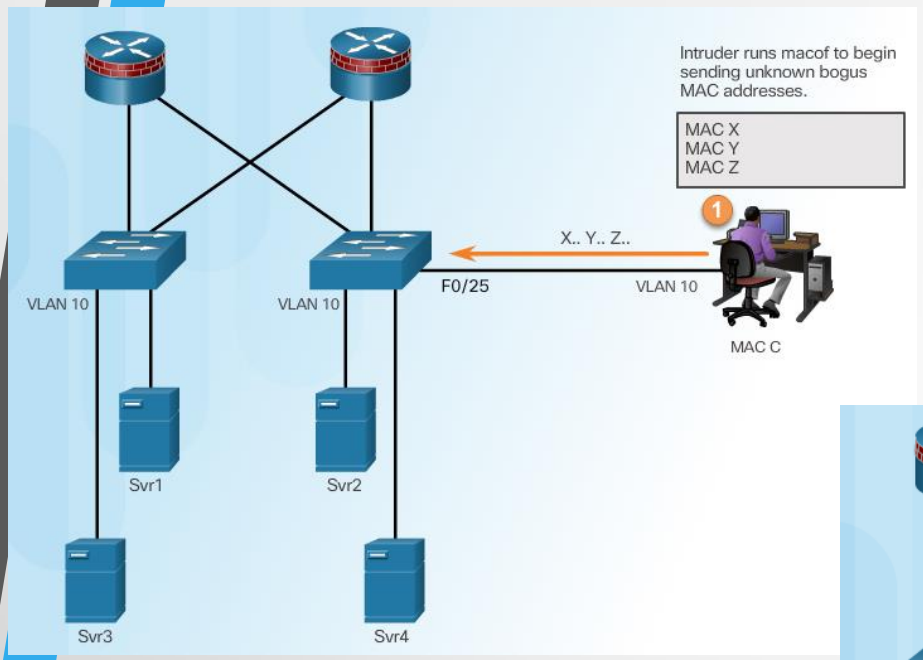
Базовый режим работы коммутатора

```
S1# show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
Sw1#
```

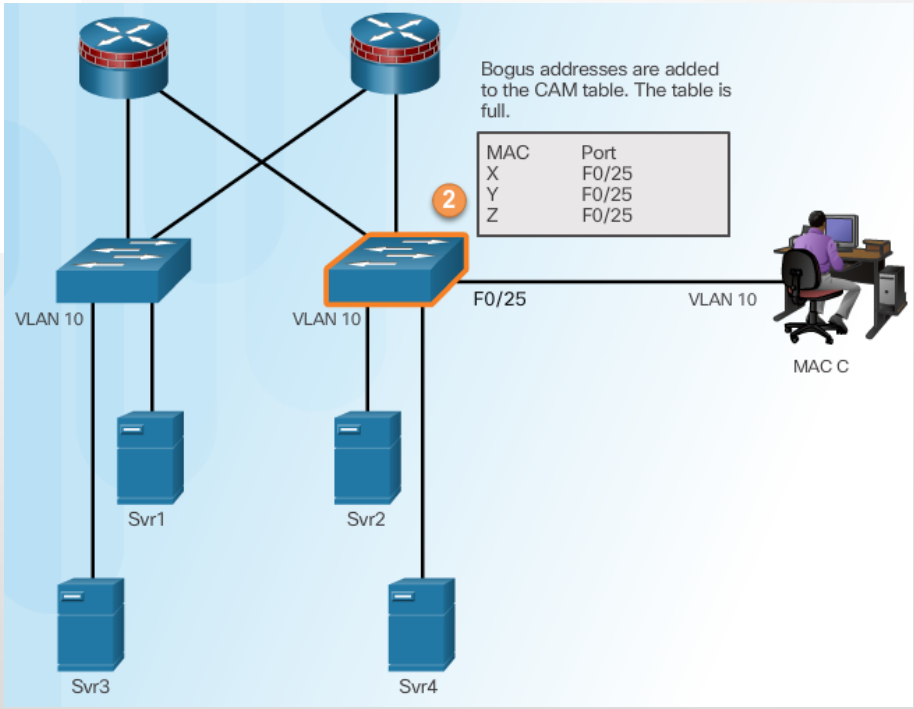
Пример использования таблицы CAM



Атака на таблицу CAM

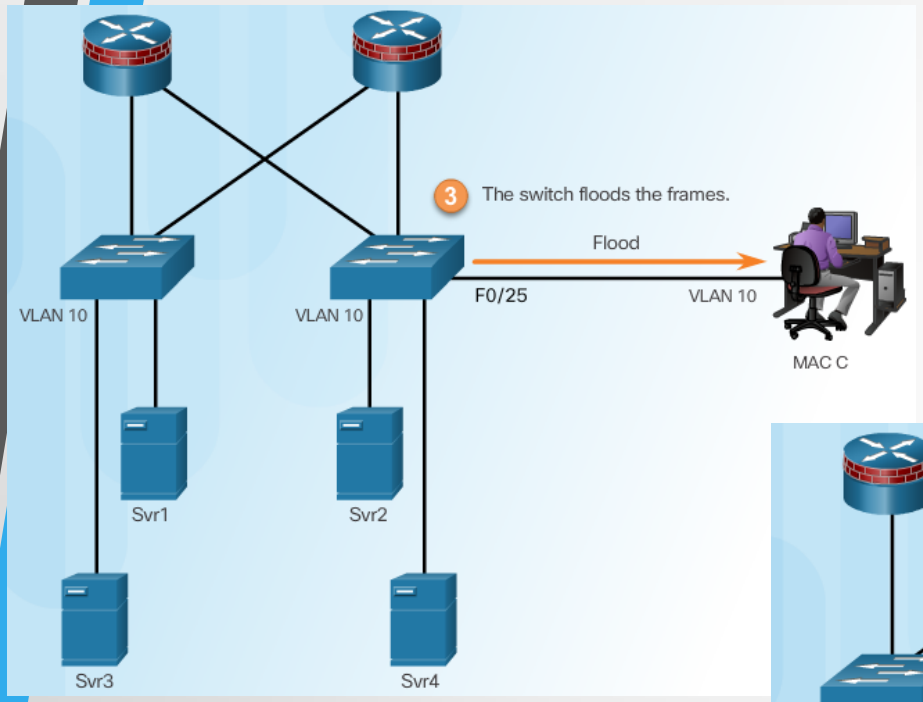


Злоумышленник запускает инструмент атаки



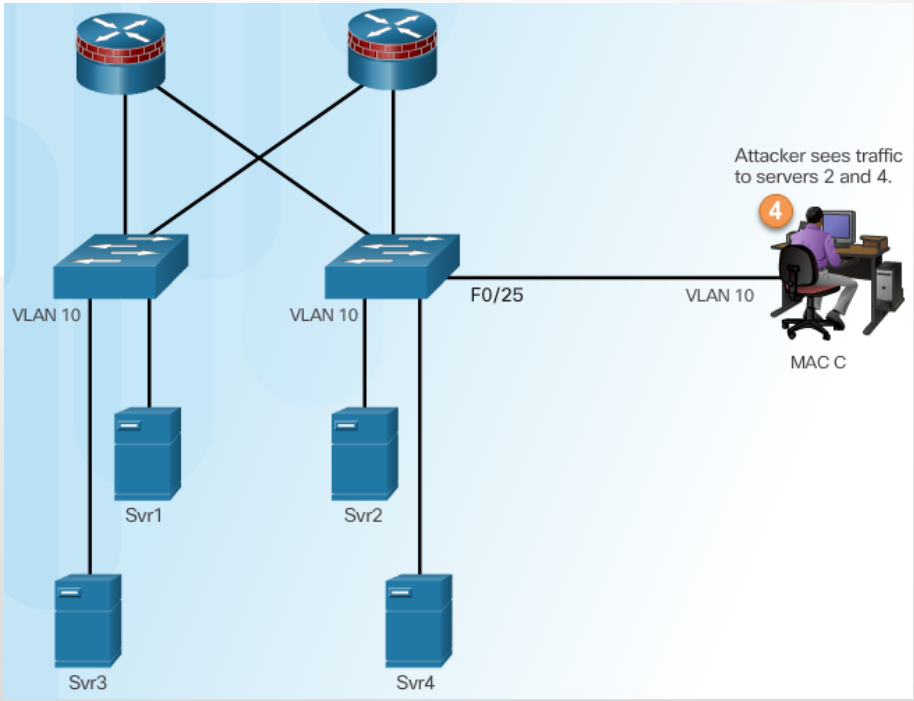
Заполнение таблицы CAM

Атака на таблицу CAM



Коммутатор передает весь трафик

Злоумышленник захватывает трафик

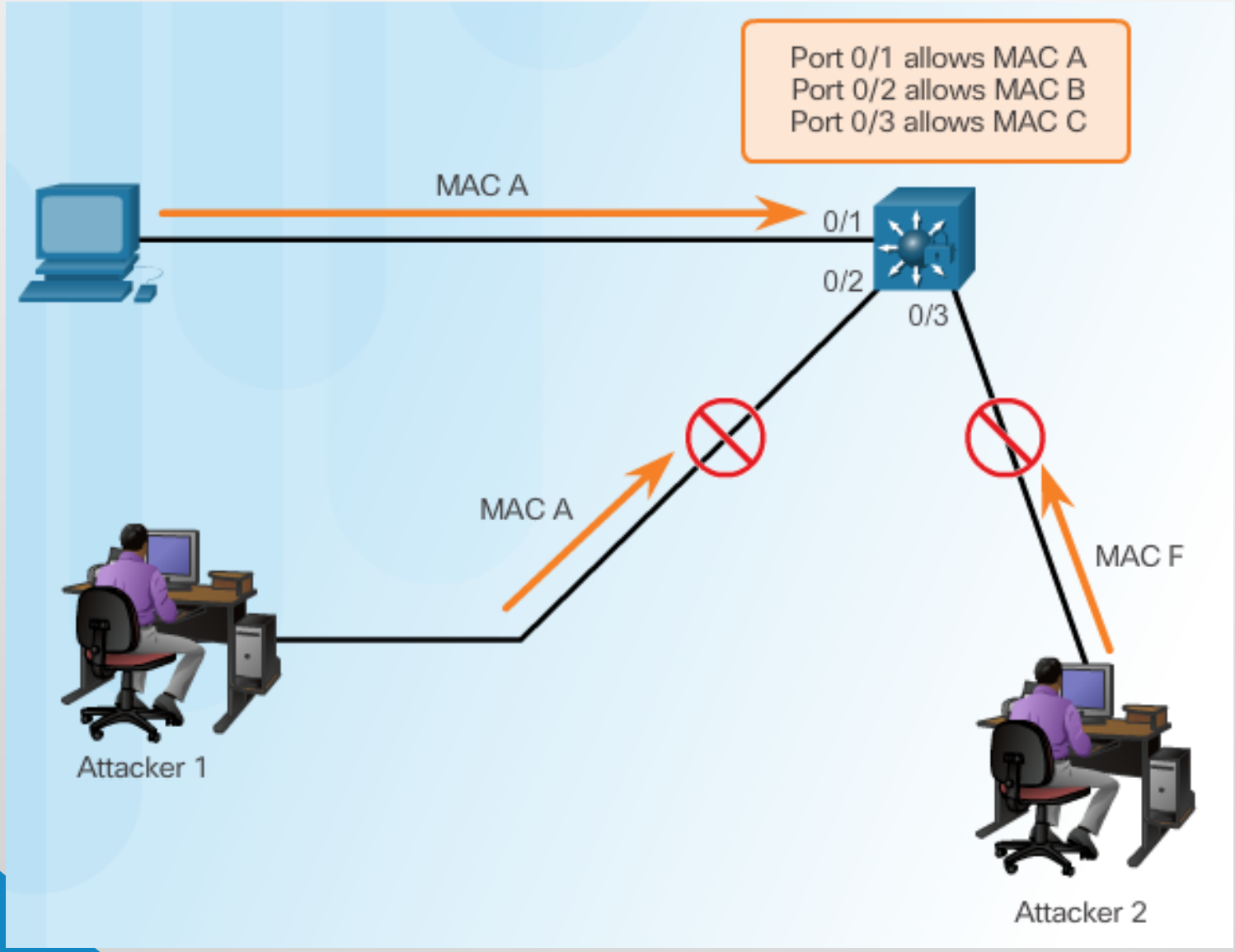


Инструменты атаки на таблицу CAM

```
macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

Тема Нейтрализация атаки на таблицу CAM

Способы борьбы с атаками на таблицу CAM



Защита портов

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

Включение функции защиты портов

Проверка работы функции защиты портов

```
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Опции защиты портов

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
  <cr>

S1(config-if)# switchport port-security
```

Включение опций защиты портов

Настройка максимального числа MAC-адресов

```
Switch(config-if)
switchport port-security maximum value
```

Конфигурирование MAC-адресов вручную

```
Switch(config-if)
switchport port-security mac-address mac-address {vlan | {access | voice}}
```

Динамическое изучение подключенных MAC-адресов

```
Switch(config-if)
switchport port-security mac-address sticky
```

Нарушение защиты портов

Режимы нарушения защиты:

- Защита
- Ограничение
- Отключение

Security Violation Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No
Restrict	No	Yes	Yes	No
Shutdown	No	Yes	Yes	Yes

Устаревание данных защиты портов

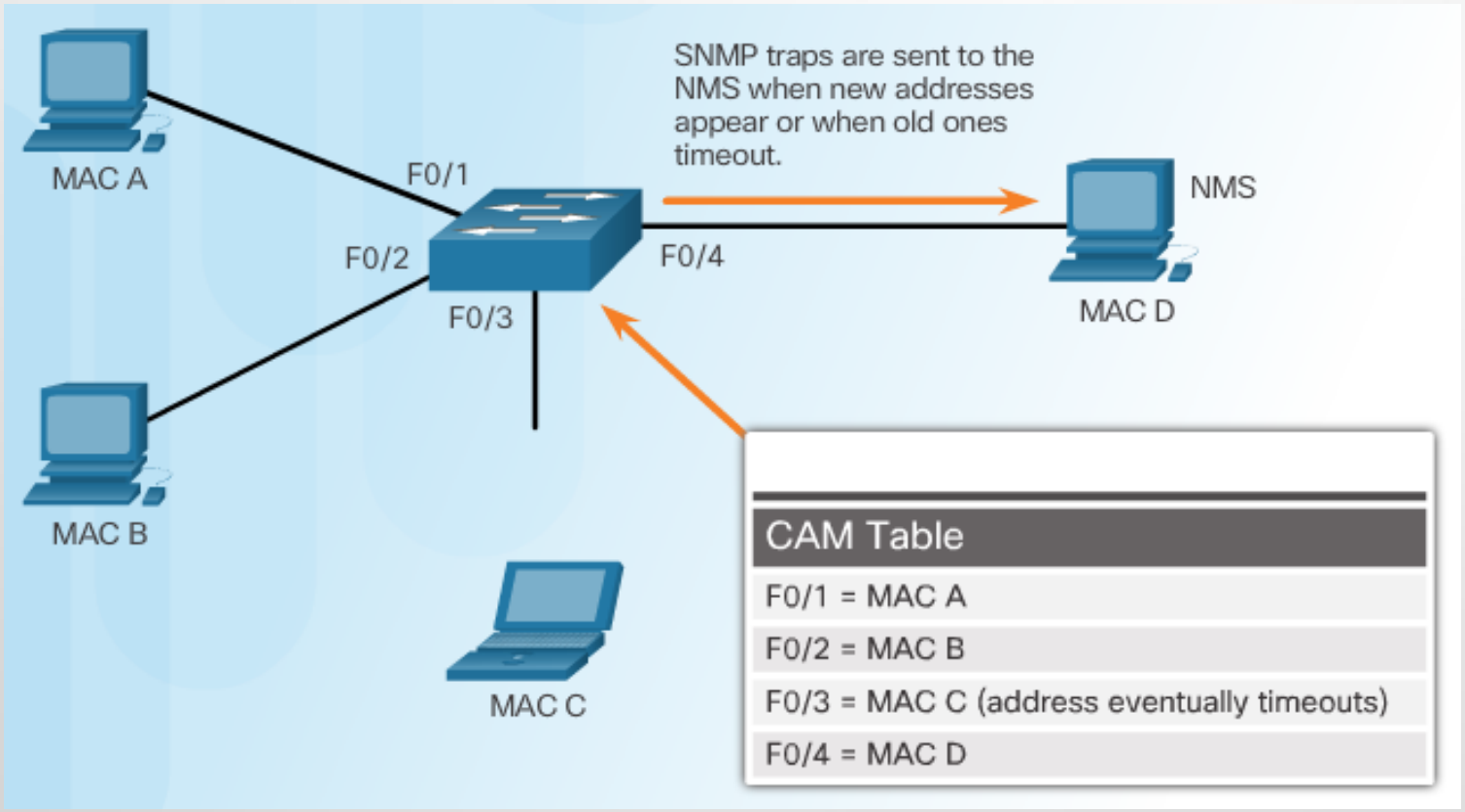
```
Switch(config-if)
switchport port-security aging {static | time time| type {absolute | inactivity}}
```

Parameter	Description
static	• Enable aging for statically configured secure addresses on this port.
time time	• Specify the aging time for this port. • The range is 0 to 1440 minutes. • If the time is 0, aging is disabled for this port.
type absolute	• Set the absolute aging time. All the secure addresses on this port age out exactly after the time (in minutes) specified and are removed from the secure address list.
type inactivity	• Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Работа защиты портов совместно с IP-телефонами

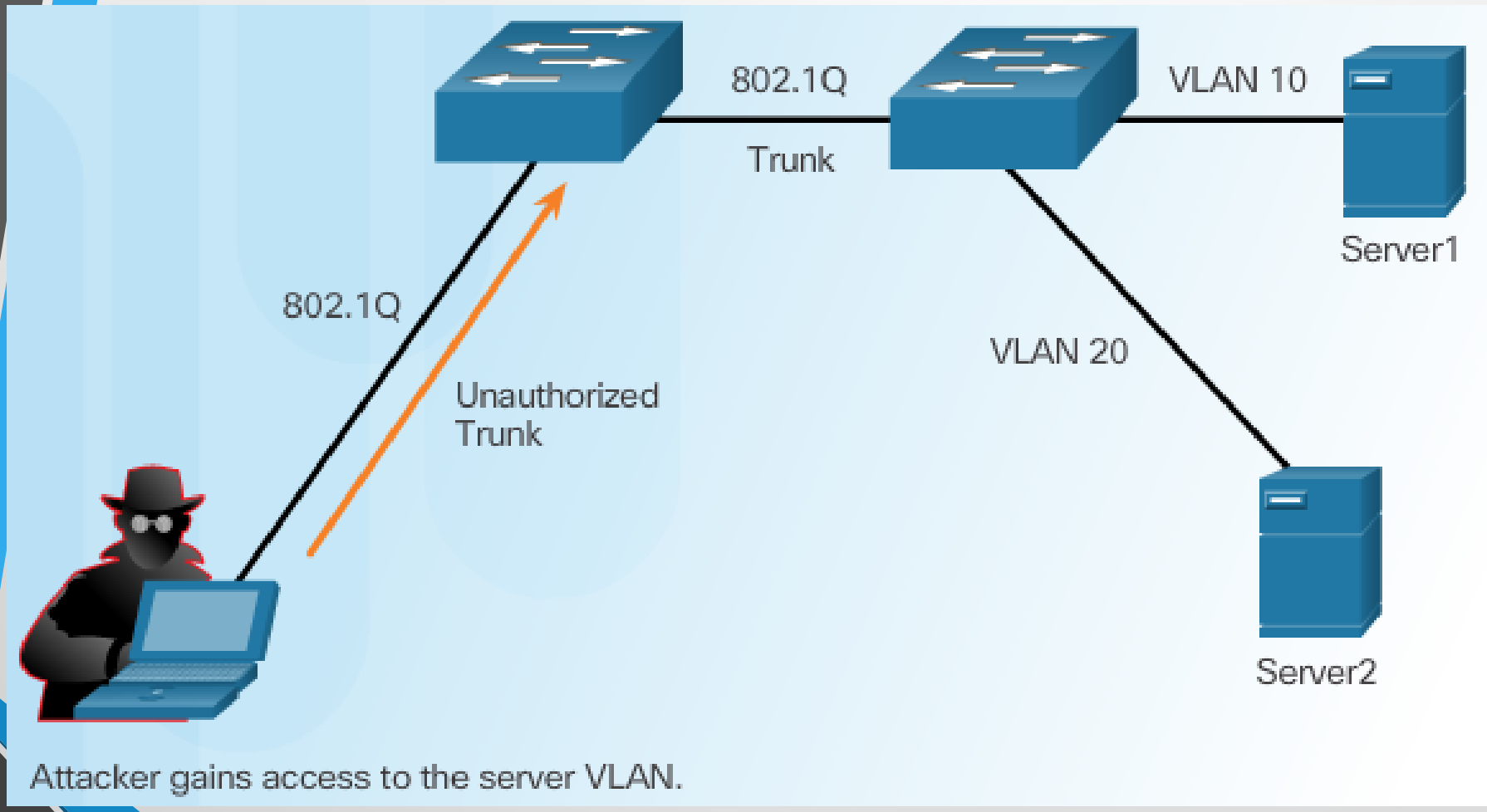

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 3
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# switchport port-security aging time 120
S1(config-if)#
```

SNMP-уведомление об изменениях MAC-адресов

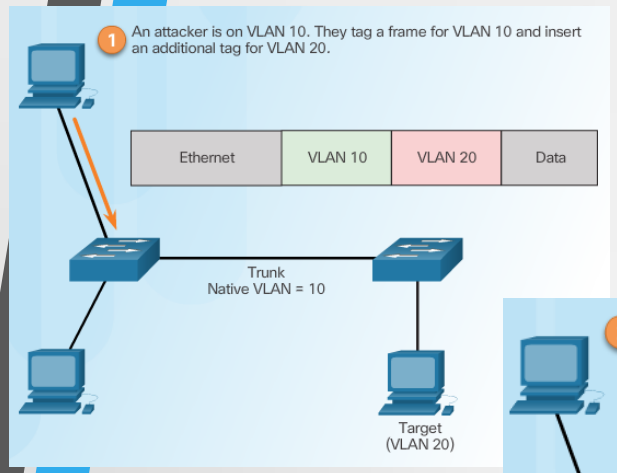


Тема
Нейтрализация атак на VLAN

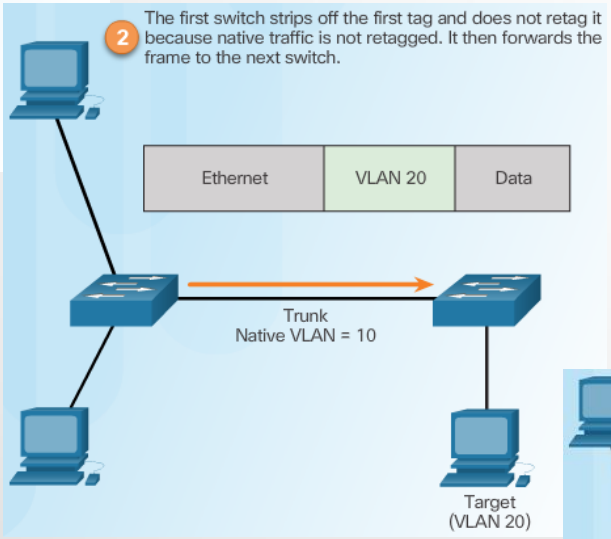
Атаки перехода (Hopping) VLAN



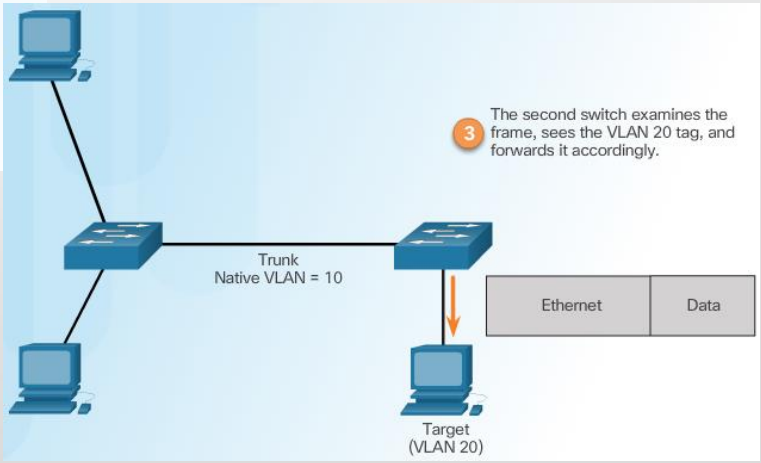
Атака VLAN Double-Tagging



Шаг 1 – атака Double Tagging

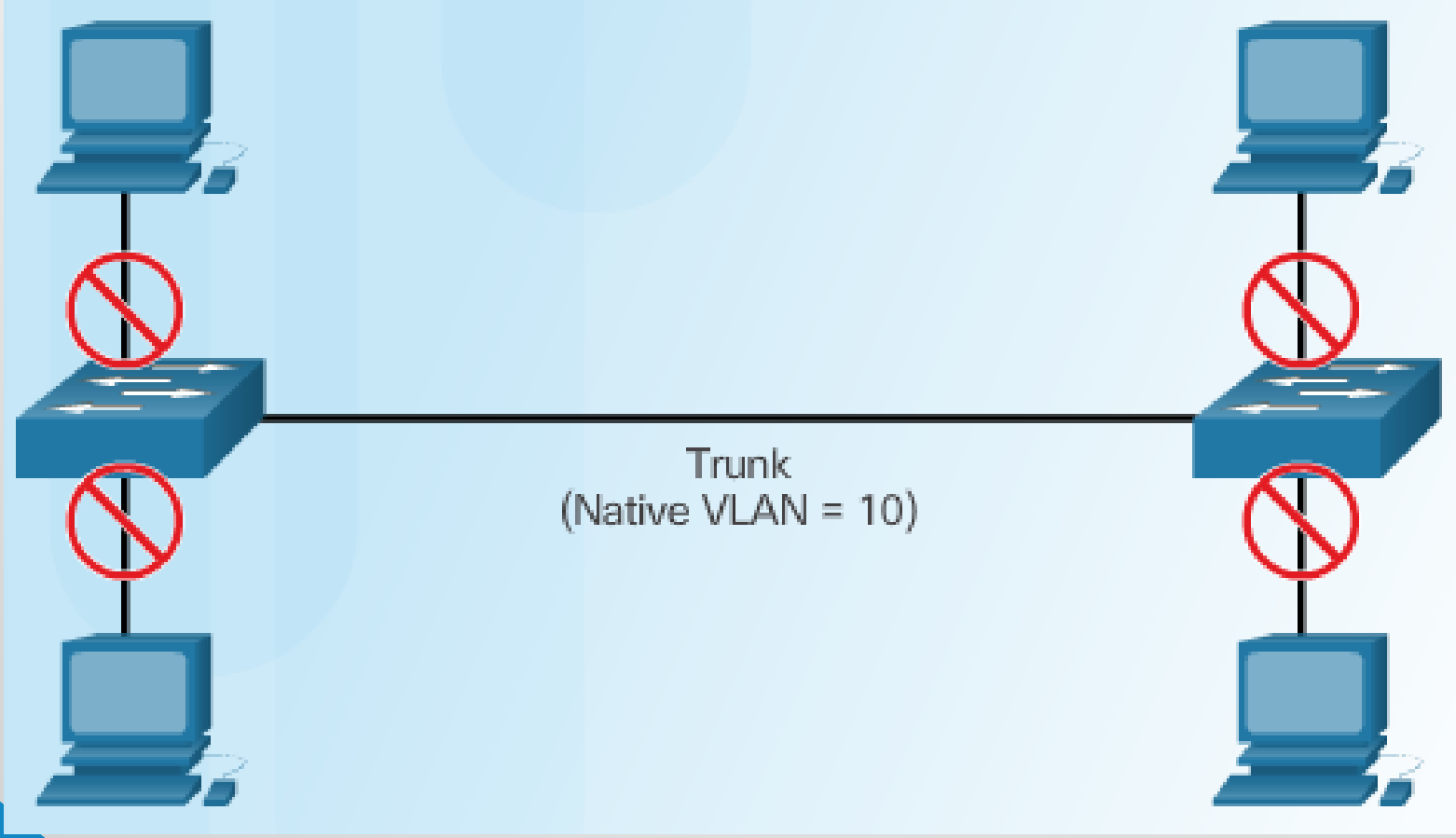


Шаг 2 – атака Double Tagging

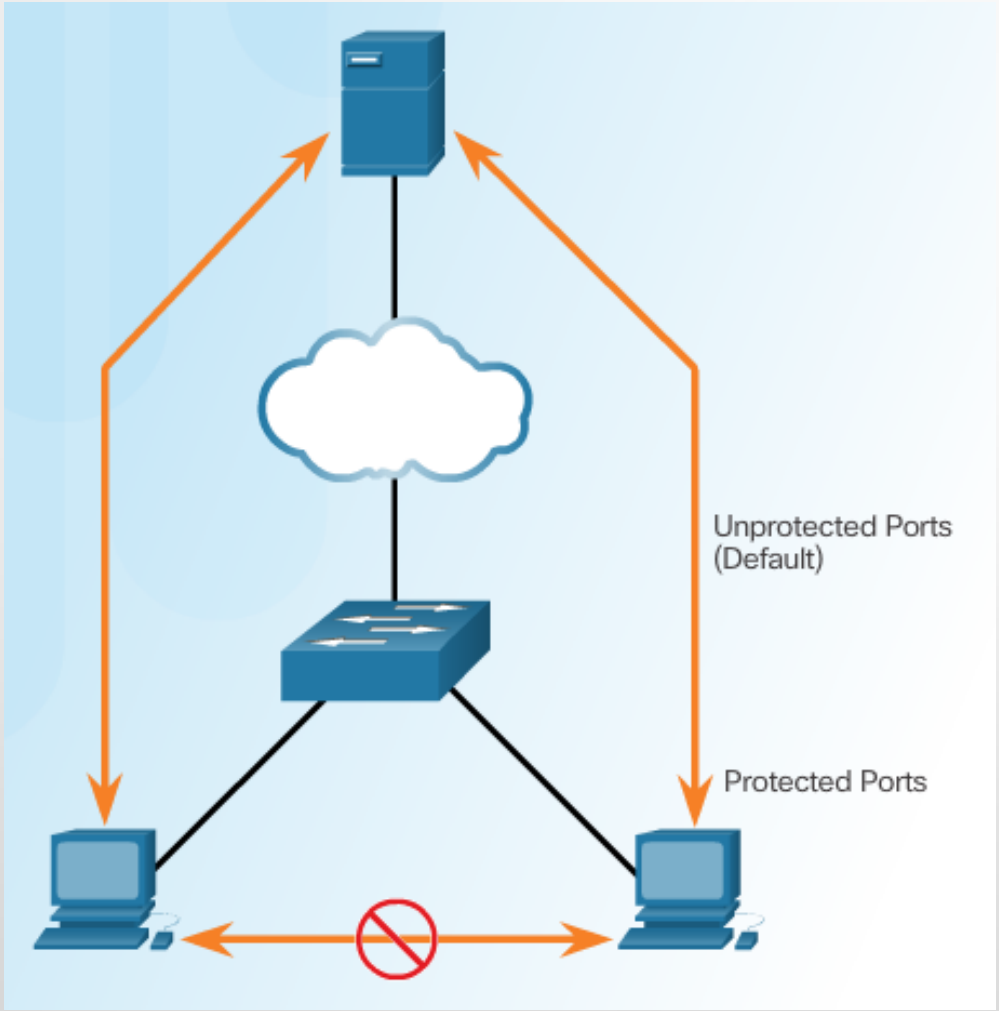


Шаг 3 – атака Double Tagging

Нейтрализация атак перехода VLAN



Функция PVLAN Edge



Проверка защищенных портов

```
Switch# show interfaces gigabitethernet1/0/1 switchport
Name: G1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
<output omitted >
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
```

Частные сети VLAN