



Cisco Expo 2009



Безопасность на основе идентификации II

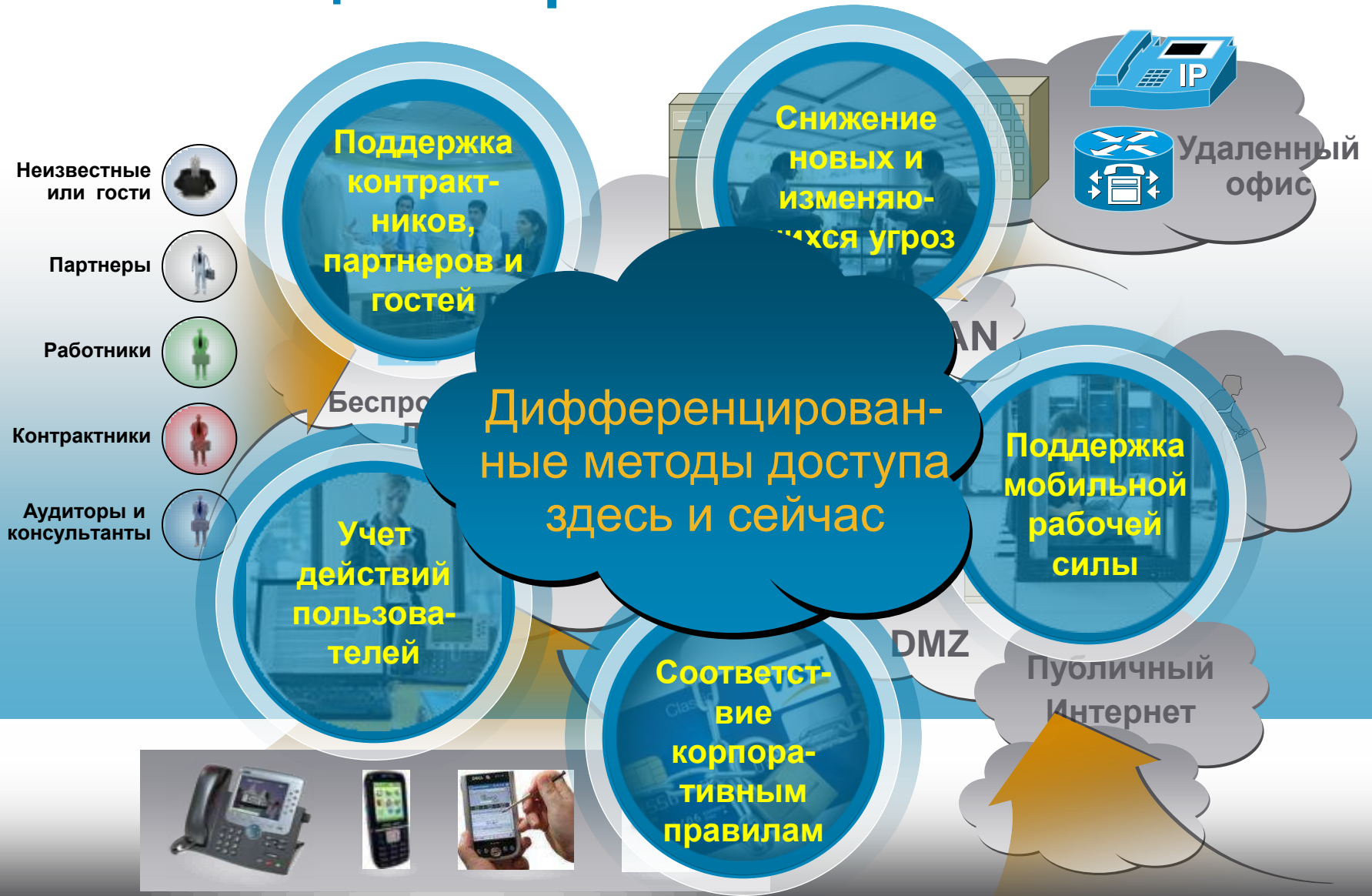
Аутентификация 802.1x

Андрей Гречин
angrechi@cisco.com

Цели данной сессии

- Узнать о преимуществах внедрения технологий аутентификации и авторизации пользователей при доступе к ЛВС
- Осветить недостатки стандартной реализации 802.1X
- Познакомиться с новыми функциями и продуктами, упрощающими внедрение 802.1X
- Обсудить особые случаи использования 802.1X и то как они могут повлиять на внедрение

Изменяющиеся требования бизнеса



Почему 802.1X так важен

1



Кто вы?

Аутентификация пользователя с использованием 802.1X (или др. техн.)

Не пускает чужих

2



Куда вы можете идти?

Основываясь на аутентификации, пользователь помещается в правильный VLAN / VRF

Контролирует честность СВОИХ

3



Какой уровень сервиса вы получаете?

Пользователь получает персональные настройки (ACL и пр.)

Персонализирует сеть

4



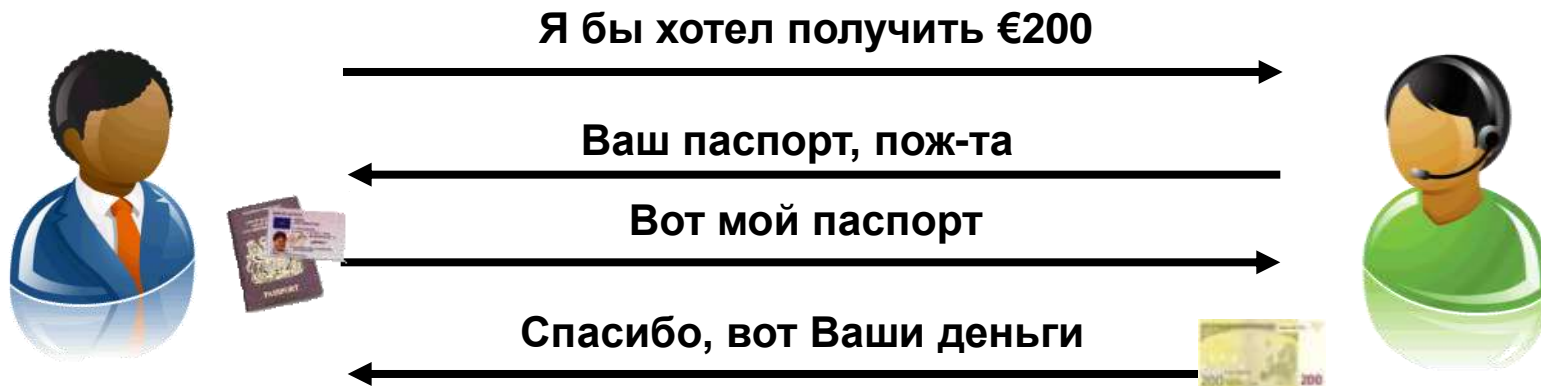
Что вы делаете?

Идентификатор пользователя и его местоположение могут быть использованы для отслеживания и учета

Повышает прозрачность использования ЛВС

Что такое аутентификация? А авторизация?

- Аутентификация это процесс установления и подтверждения личности клиента, запрашивающего сервис
- Аутентификация полезна только в случае дополнительной авторизации (проверка наличия денег на счету)



Аутентификация настолько сильна, насколько силен метод ее проверки

Модель аутентификации в сети



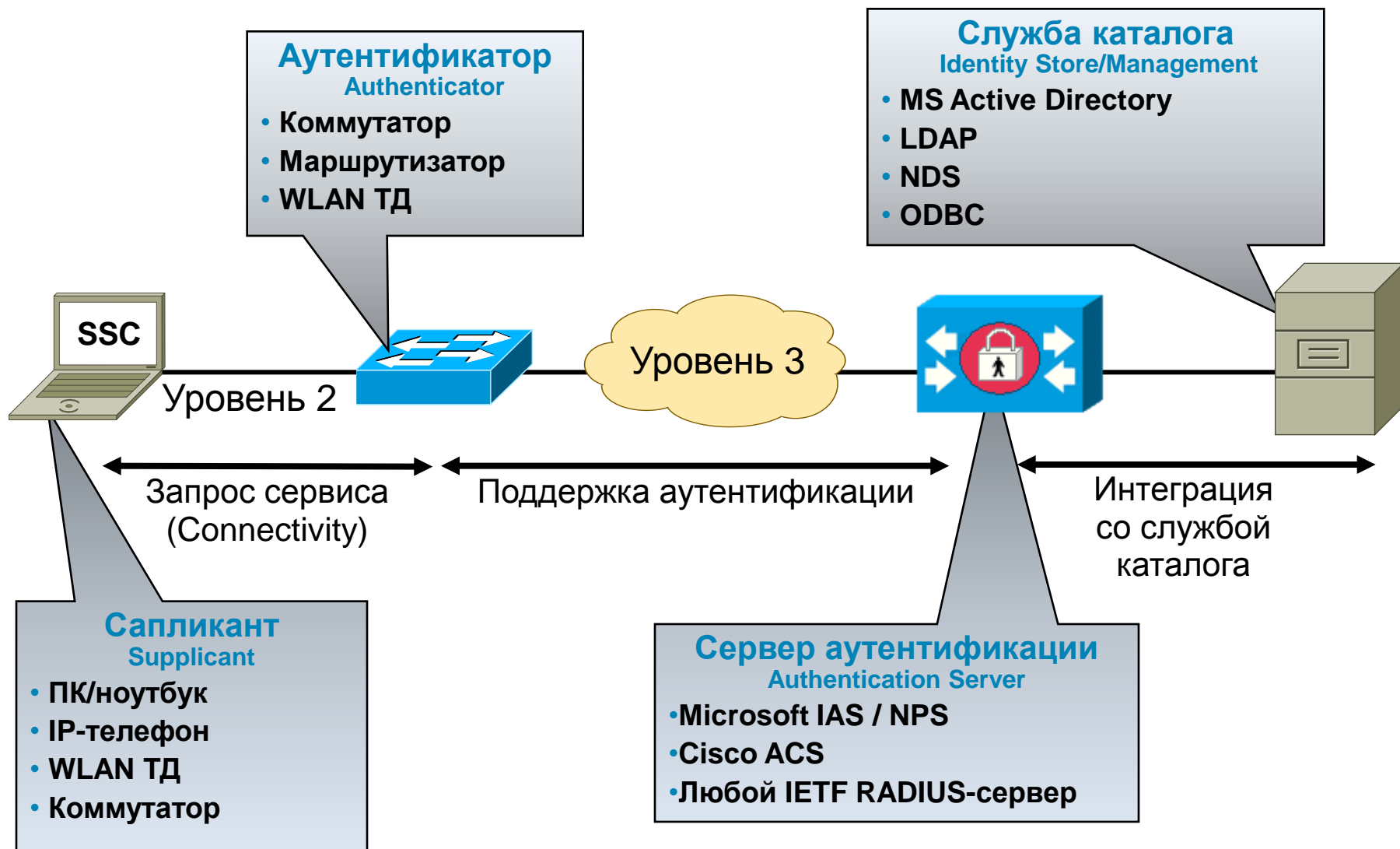
Основы стандарта 802.1X



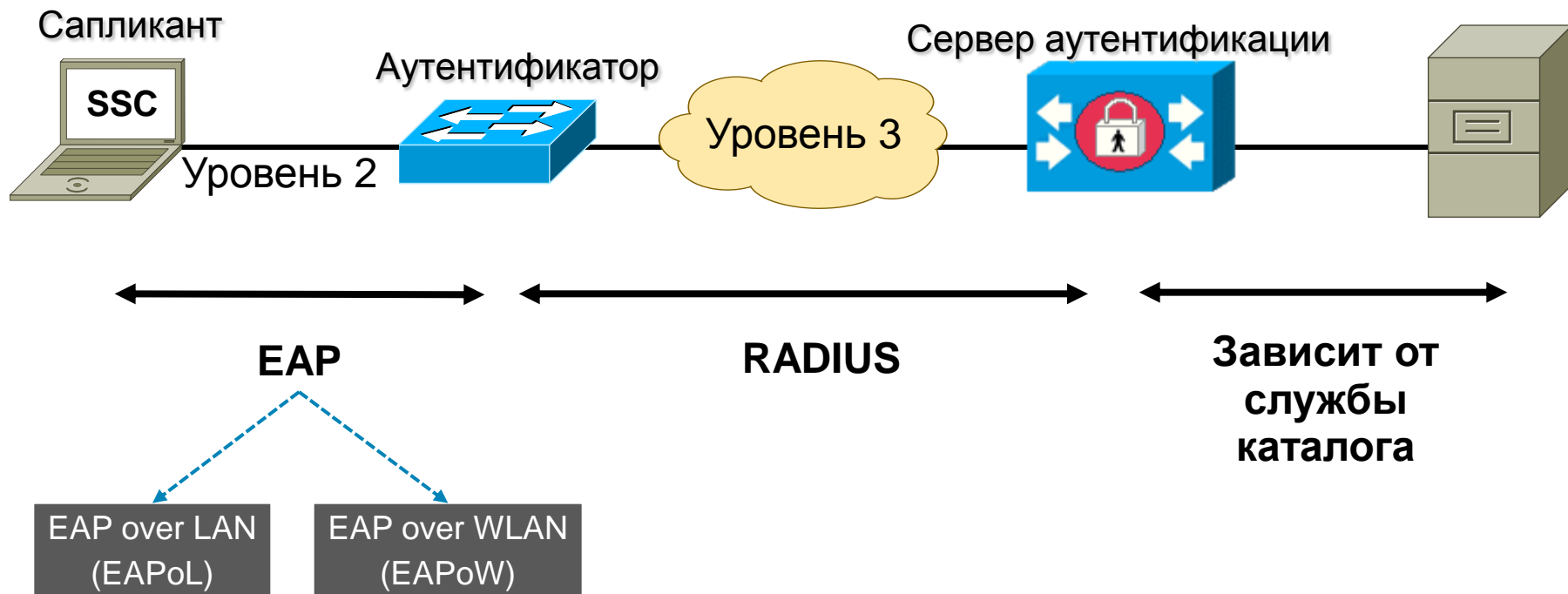
IEEE 802.1X

- Стандарт создан рабочей группой IEEE 802.1
- Спроектирован для реализации контроля доступа **на уровне порта**, используя аутентификацию
- Главным образом определяет метод инкапсуляции протокола EAP для передачи через среду IEEE 802 – EAPOL (EAP over LAN)
- Протокол второго уровня для передачи аутентификационных сообщений (EAP) между сапликантом на ПК (supplicant) и аутентификатором (authenticator) (коммутатор или ТД)
- Подразумевает защищенное подключение к порту
- **Контроль политики после аутентификации основан на фильтрации по MAC адресам и отслеживании состояния порта**

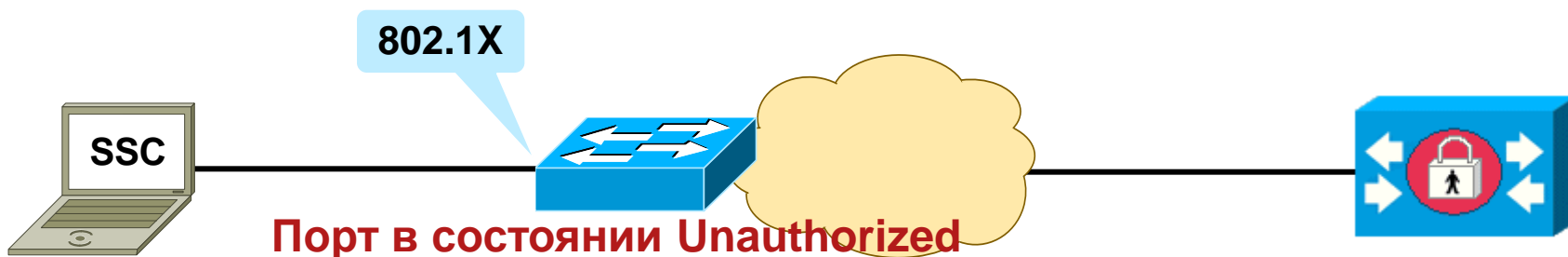
Модель контроля доступа 802.1X



Протоколы 802.1X



Конфигурация IOS коммутатора



Cisco IOS

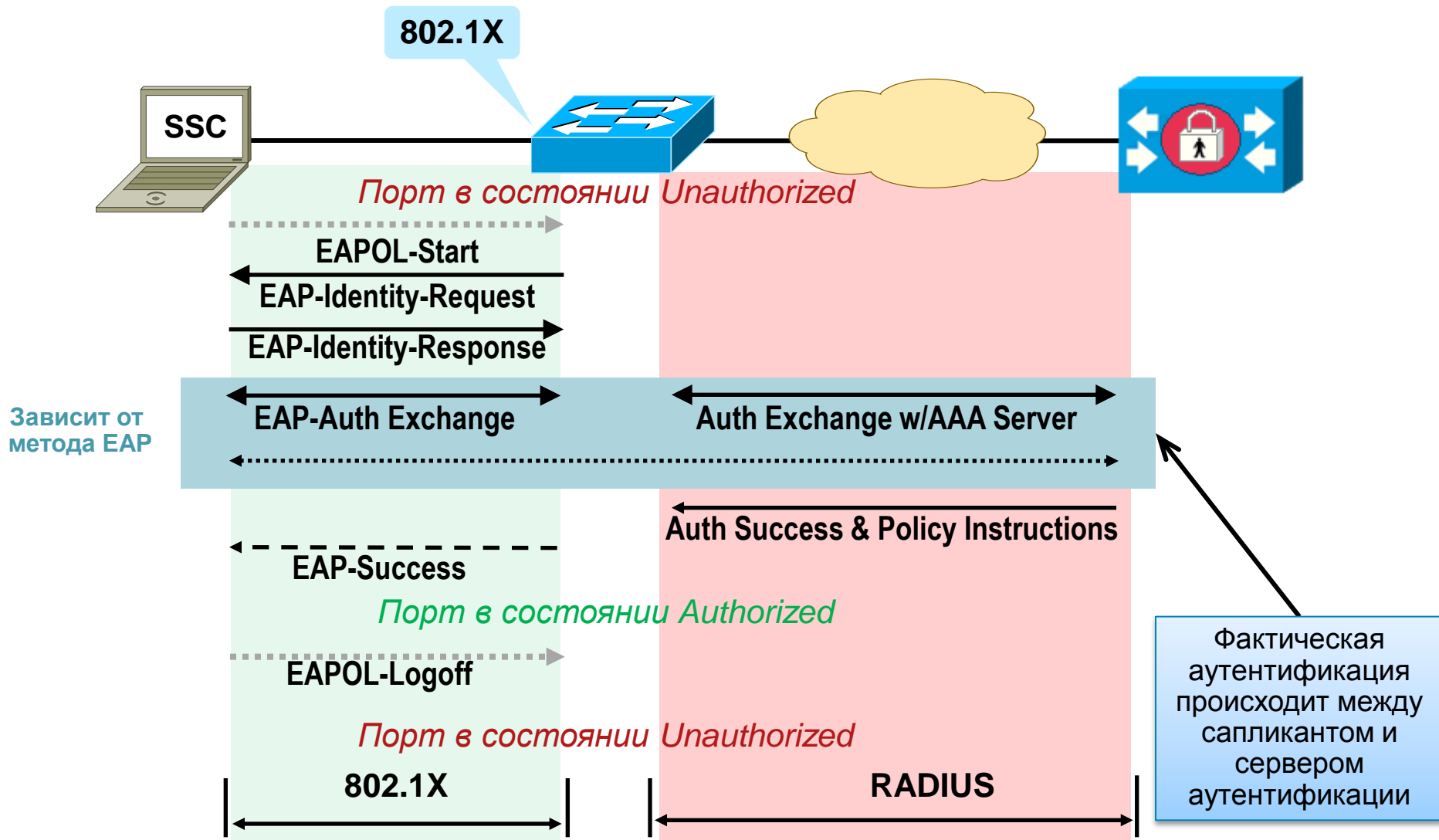
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius

radius-server host 10.100.100.100
radius-server key cisco123

dot1x system-auth-control

interface GigabitEthernet1/0/1
 authentication port-control auto
 dot1x pae authenticator
```

Процесс аутентификации и авторизации



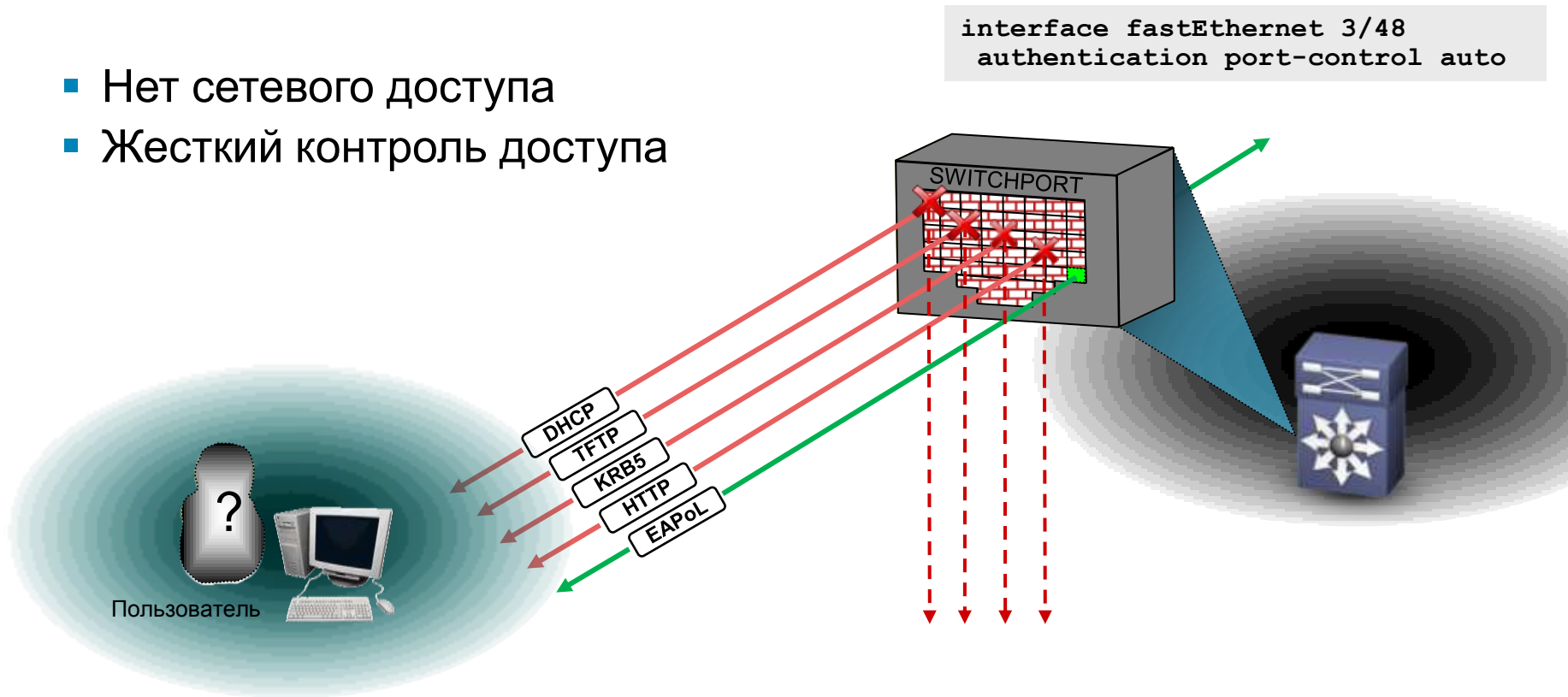
Проблематика внедрений 802.1X



Стандартная реализация 802.1X

До аутентификации

- Нет сетевого доступа
- Жесткий контроль доступа



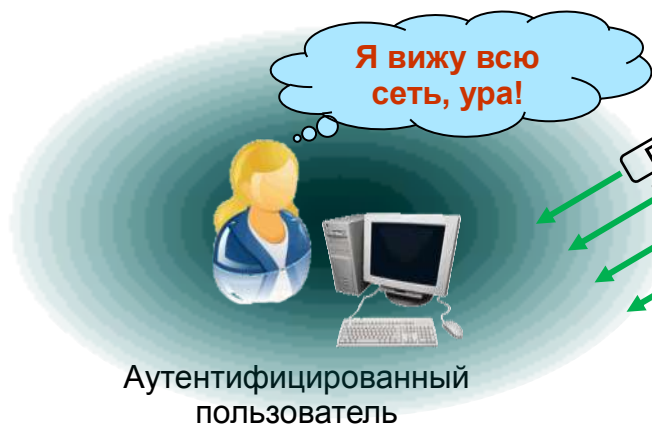
Весь трафик *кроме EAPoL* сбрасывается

Стандартная реализация 802.1X

После аутентификации

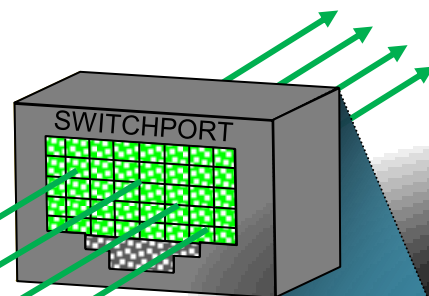
- Пользователь/устройство опознаны
- Контроль доступа на основе идентификатора

Один MAC на порт



DHCP
TFTP
KRB5
HTTP

```
interface fastEthernet 3/48
 authentication port-control auto
 dot1x pae authenticator
```



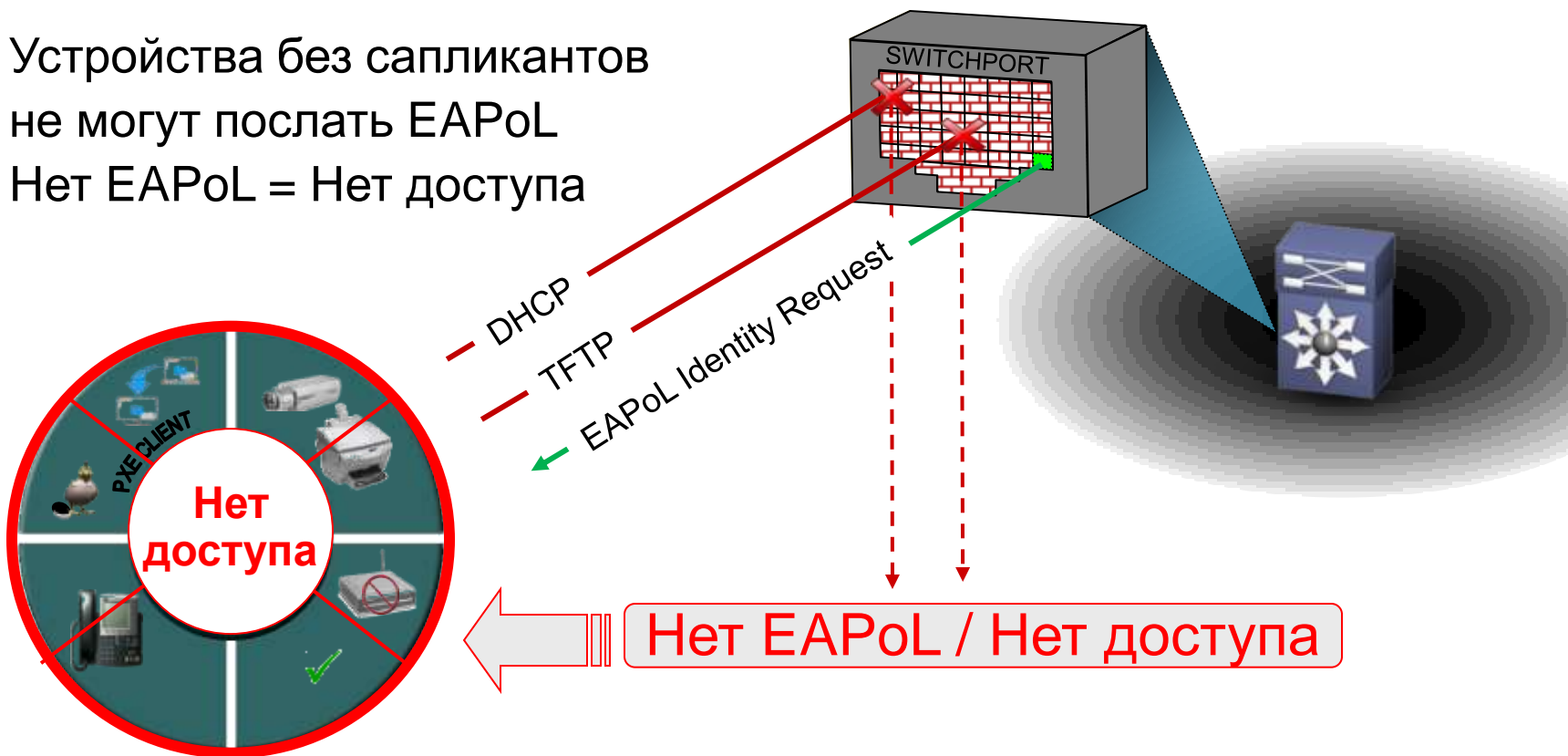
Динамические VLANы или ACLи могут быть использованы для дополнительного ограничения доступа в качестве средств авторизации.

Ограничения стандартной реализации 802.1X (1/2)

Стандартное ограничение 802.1X

- Устройства без сапликантов не могут послать EAPoL
- Нет EAPoL = Нет доступа

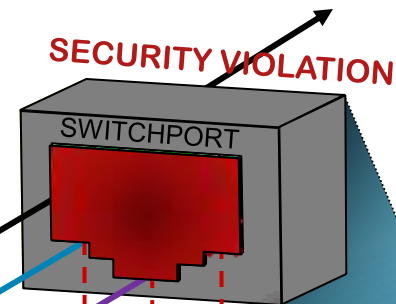
```
interface fastEthernet 3/48
authentication port-control auto
dot1x pae authenticator
```



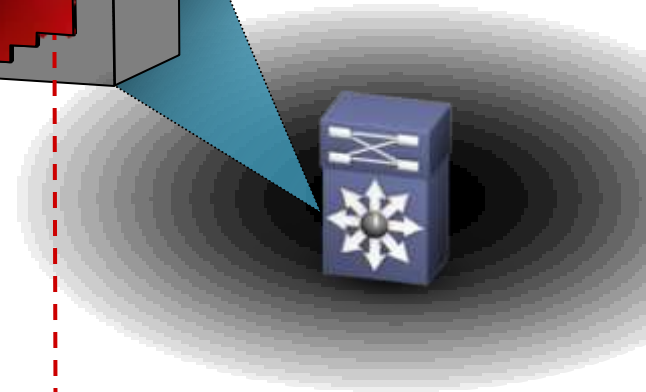
Ограничения стандартной реализации 802.1X (2/2)

Несколько MAC'ов на порту

- Предполагается злой умысел
На самом деле это хабы, VMWare, IPT и др.



```
interface fastEthernet 3/48
authentication port-control auto
dot1x pae authenticator
```



Новая методология внедрения 802.1X



Фазы внедрения 802.1X

Режим мониторинга

Основные технологии

- Open mode

Преимущества

- Свободный доступ
- Нет влияния на сеть
- Логи и отчеты для анализа



Режим ограниченного доступа

Основные технологии

- Open mode
- ACL загружаемые и на уровне порта

Преимущества

- Базовая связность по-прежнему доступна
- Повышенная безопасность доступа
- Разграничение доступа



Безопасный режим

Основные технологии

- Стандартный закрытый режим
- Назначение динамических VLANов (опция)

Преимущества

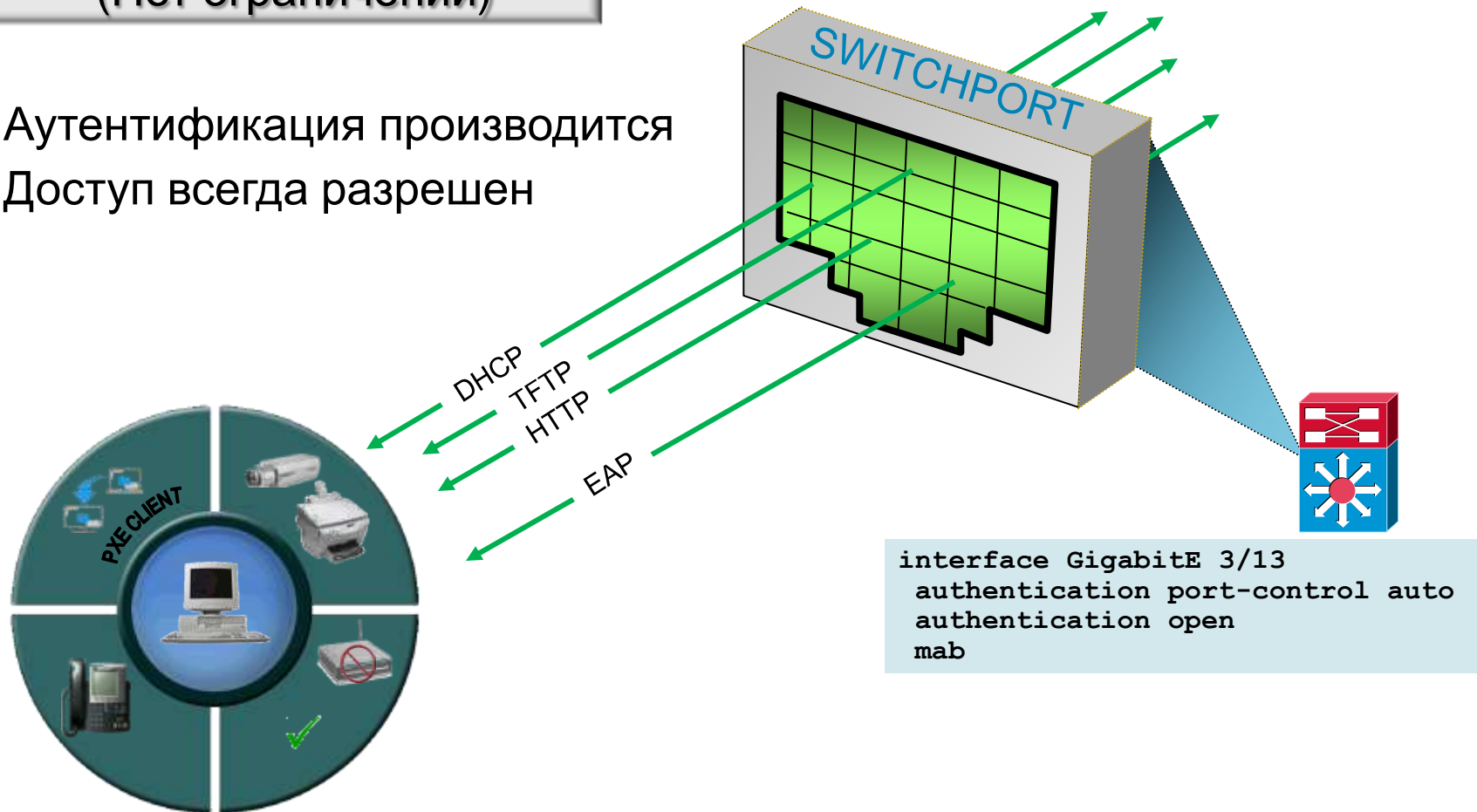
- Строгий контроль доступа



Изменение авторизации по умолчанию: Open Mode

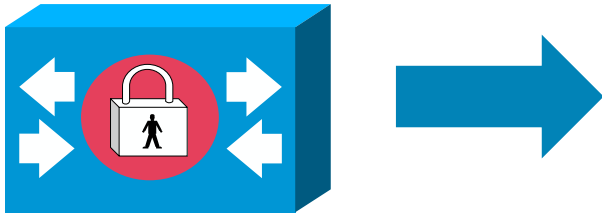
Open Mode
(Нет ограничений)

- Аутентификация производится
- Доступ всегда разрешен



Мониторинг

Мониторинг сети для определения неправильно настроенных ПК, неправильных аутентификационных данных, создания БД MAC адресов



Логи RADIUS сервера позволяют выявить:

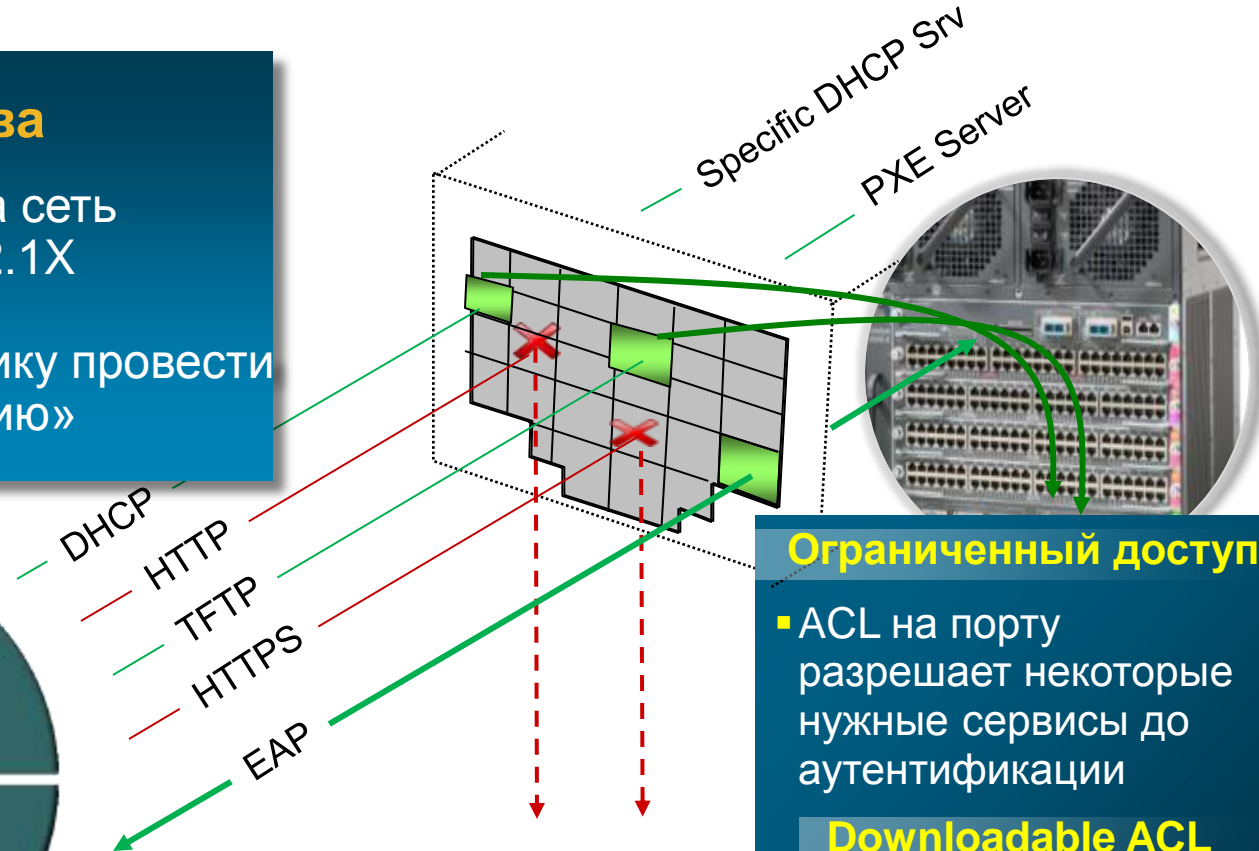
- Попытки аутентификации 802.1X/EAP
 - Список устройств 802.1X
 - Список устройств без 802.1X сапликанта
- Попытки аутентификации MAB
 - Список правильных MAC
 - Список неправильных или неизвестных MAC
- Подготовиться к другим этапам

Open Mode с ограничением доступа

Баланс между безопасностью и доступностью

Преимущества

- Уменьшает влияние на сеть при развертывании 802.1X
- Поддерживает PXE
- Предоставляет заказчику провести «генеральную репетицию»



Ограниченный доступ

- ACL на порту разрешает некоторые нужные сервисы до аутентификации

Downloadable ACL

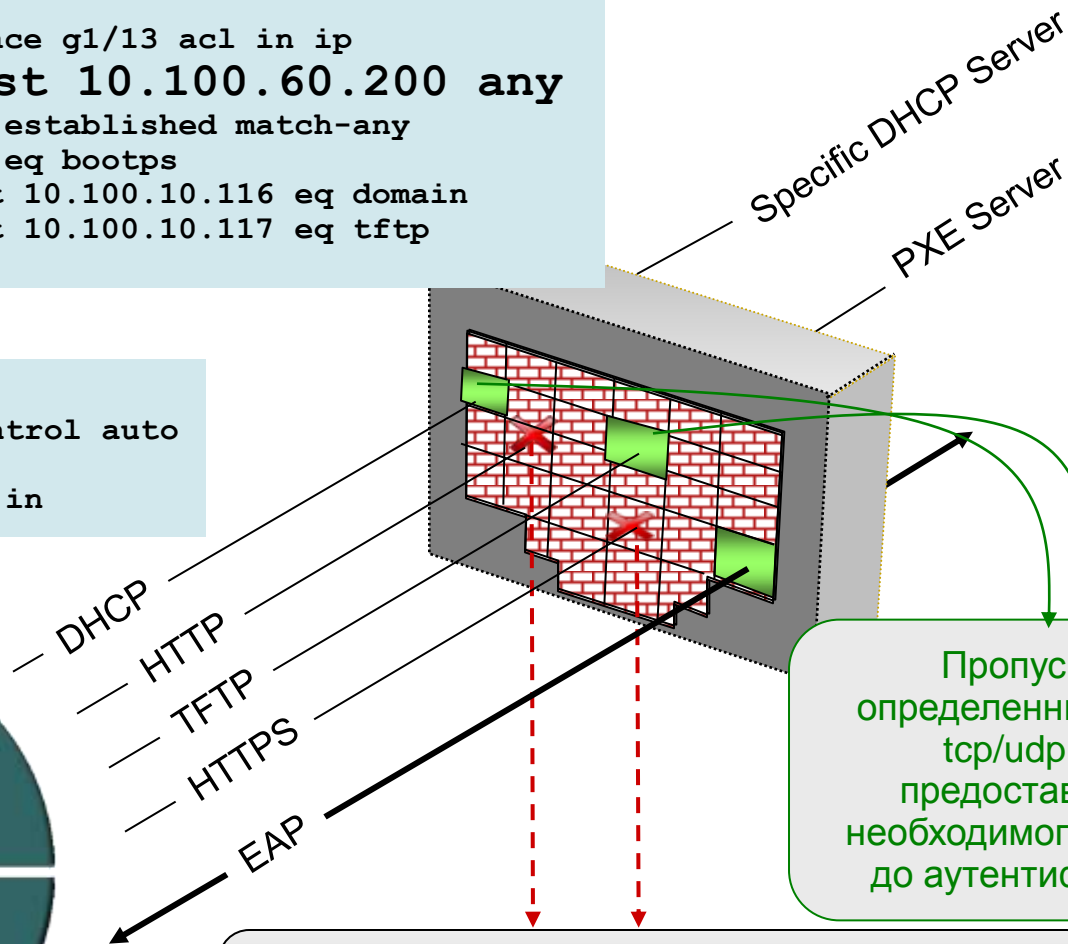
- После аутентификации на порт назначаются dACL полученные от ACS

Open Mode с ограничением доступа

(After Authentication)

```
Switch#show tcam interface g1/13 acl in ip
  permit ip host 10.100.60.200 any
  permit tcp any any established match-any
  permit udp any any eq bootps
  permit udp any host 10.100.10.116 eq domain
  permit udp any host 10.100.10.117 eq tftp
  deny ip any any
```

```
interface GigabitE 3/13
  authentication port-control auto
  authentication open
  ip access-group UNAUTH in
```



Пропускает определенные порты tcp/udp для предоставления необходимого доступа до аутентификации

Блокирует определенные ресурсы до прохождения полной аутентификации 802.1X, MAB или WebAuth

Особые случаи использования 802.1X



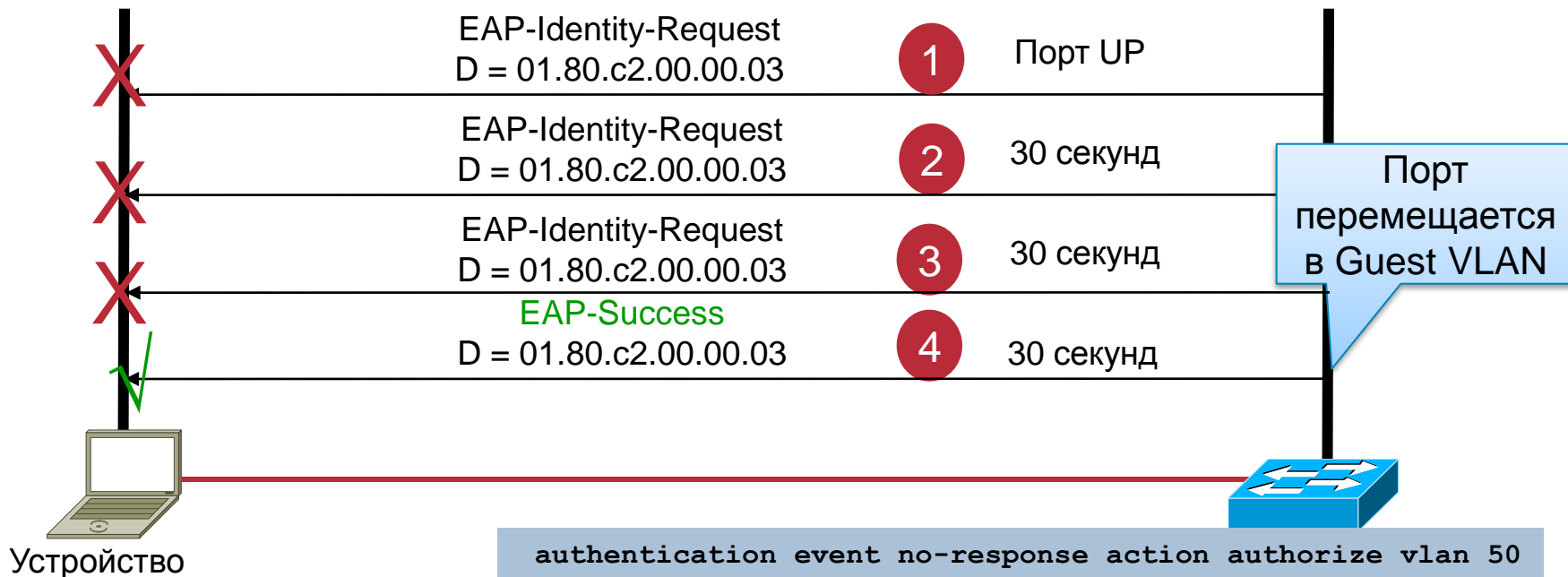
Особые случаи использования 802.1X

- Устройства без 802.1X сапликанта и гостевой доступ
- Обработка неудачных аутентификаций
- Последовательность методов аутентификации Flexible-Authentication
- Несколько устройств на порту
- Сапликанты
- 802.1X и Microsoft Windows

Устройства без 802.1X сапликанта и гостевой доступ

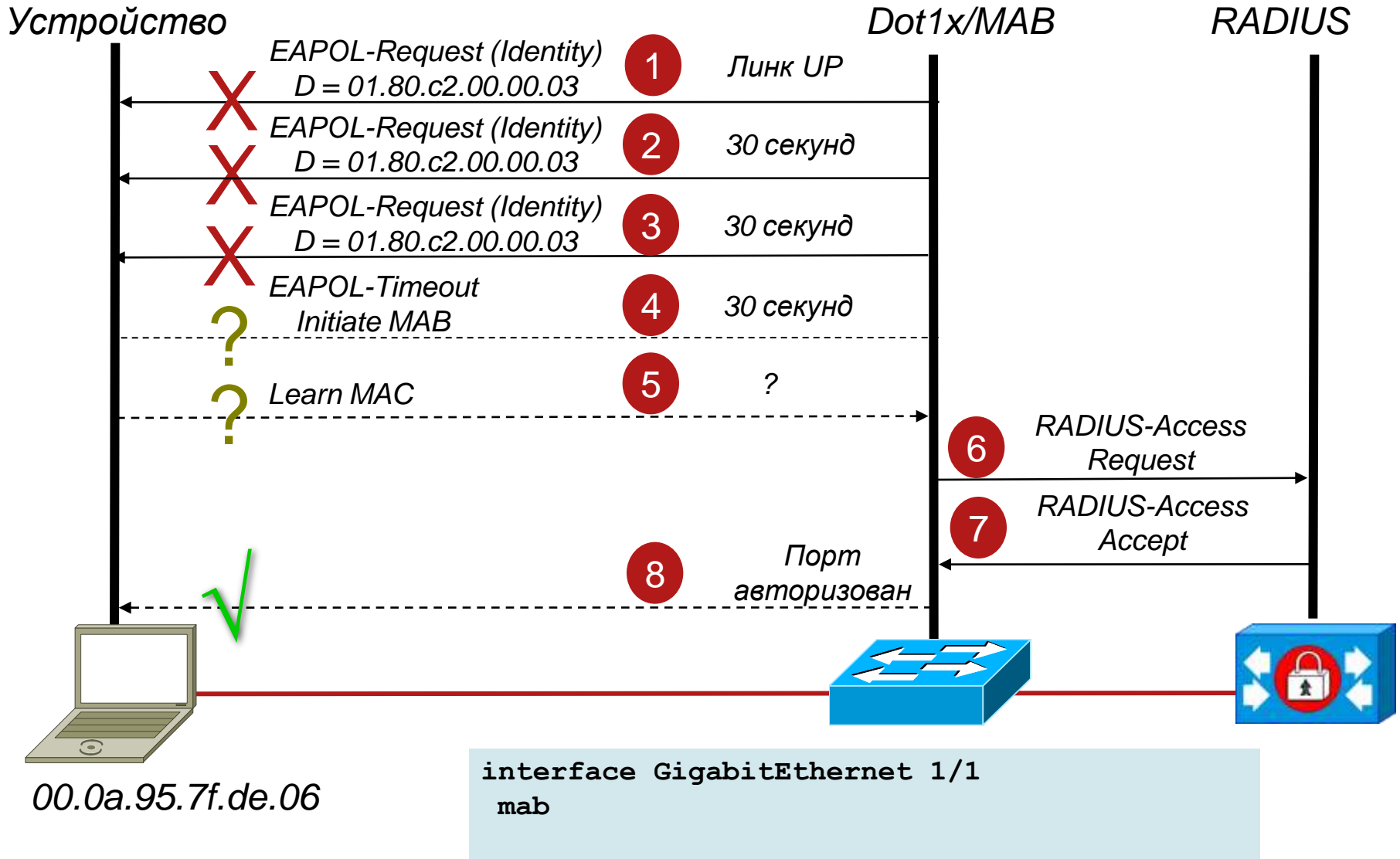
- Аутентифицировать через менее безопасный метод
 - MAC Authentication Bypass (MAB)
 - Web Auth (клиент должен использовать браузер)
- Предоставить ограниченный доступ в случае отсутствия ответа сапликанта
 - Guest VLAN
- Предоставлять только беспроводной доступ вместо проводного
 - Или использовать статическую конфигурацию портов в конференц-комнатах

802.1X и Guest VLAN



- Любой 802.1X порт будет посылать фреймы EAPOL-Identity-Request (в независимости есть на другой стороне сапликант или нет)
- Устройство перемещается в Guest VLAN только в случае его не ответа на фреймы EAP-Request-Identity
- Другие методы аутентификации или авторизации не могут быть применены, номер VLAN'а задается жестко на коммутаторе
- Таймаут = 90 секунд, что больше чем MS DHCP таймаут

MAC Authentication Bypass (MAB)



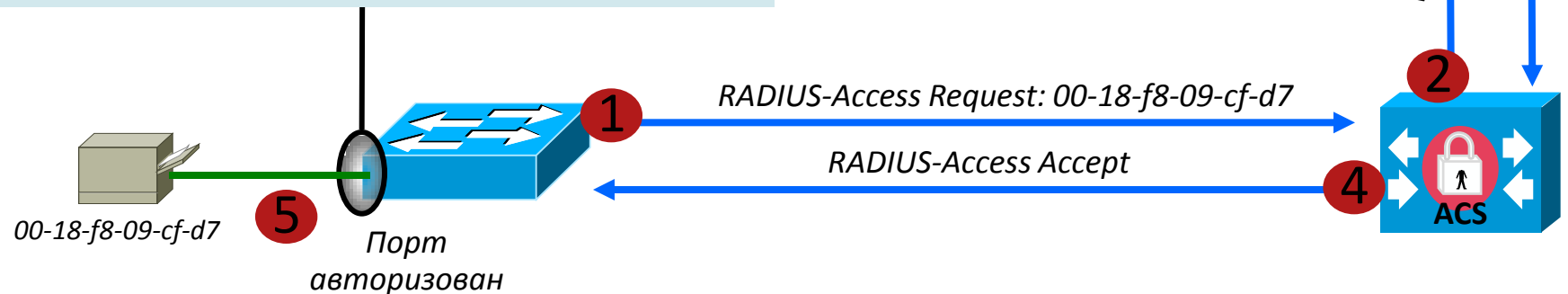
Ограничения MAB

- MAB требует создания и поддержки БД MAC адресов
- По умолчанию таймаут 802.1X = 90 секундам
 - 90 сек > таймаута по умолчанию для MS DHCP
 - 90 сек > таймаута по умолчанию для PXE
- Не самый лучший способ исправления: Настройка таймеров, что всегда требует дополнительного тестирования
 - max-reauth-req**: максимальное кол-во раз, которое коммутатор будет перепосылать фрейм EAP-Identity-Request (по умолчанию: 2)
 - tx-period**: кол-во секунд, в течении которых коммутатор будет ожидать ответа на фрейм EAP-Identity-Request до начала его перепосылки (по умолчанию: 30)
 - Таймаут 802.1X** == $(\text{max-reauth-req} + 1) * \text{tx-period}$

Упрощение развертывания MAB с использованием NAC Profiler

- 1) 802.1X таймаут, коммутатор инициирует MAB
- 2) ACS запрашивает БД NAC Profiler используя LDAP
- 3) NAC Profiler подтверждает MAC адрес
- 4) ACS посылает подтверждение аутентификации
- 5) Коммутатор авторизует порт (с возможным ограничением доступа)

```
interface range gigE 1/0/1 - 24
 switchport access vlan 30
 switchport voice vlan 31
 authentication port-control auto
 mab
```

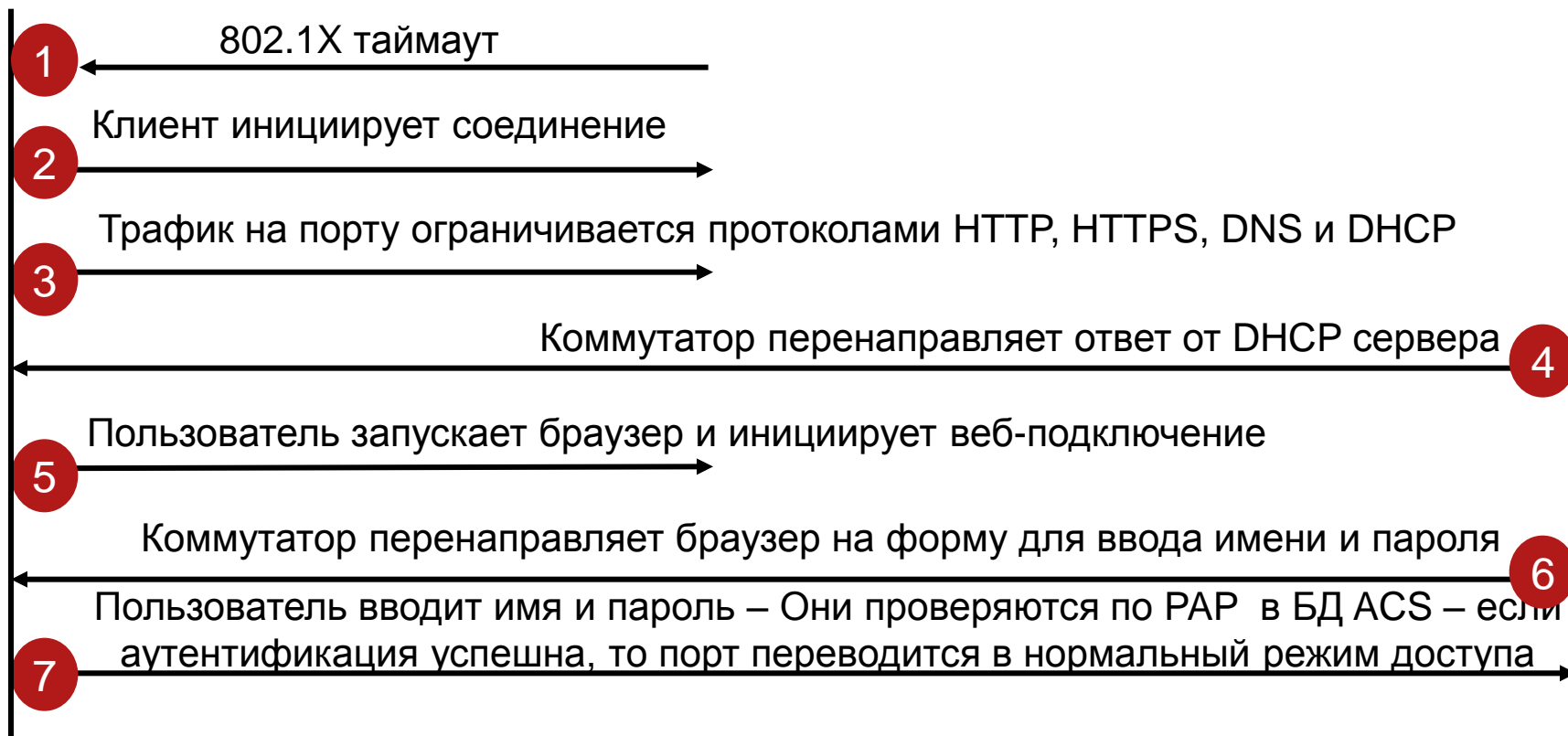
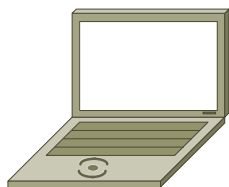


Веб-аутентификация

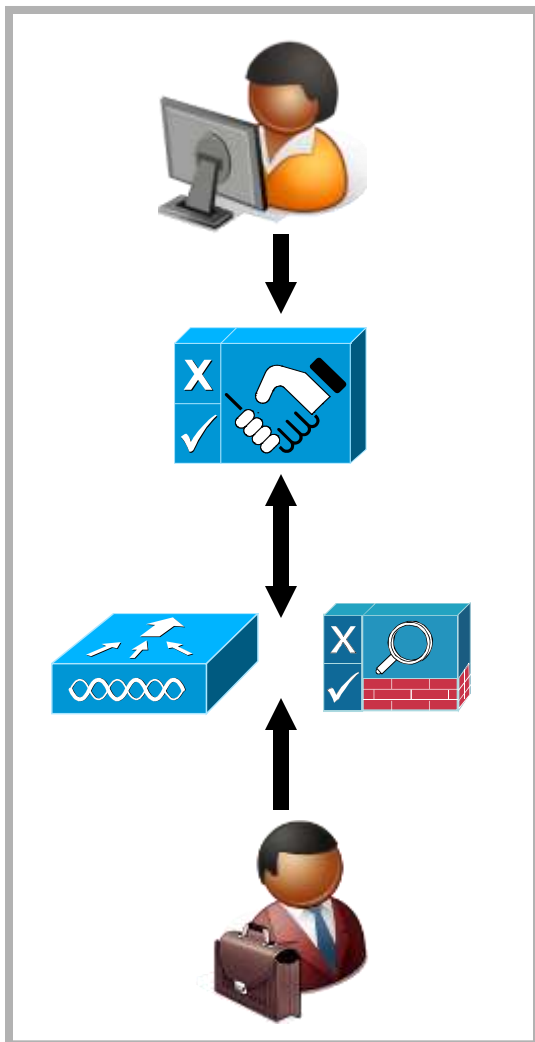
Нет EAPOL

Процесс 802.1X

RADIUS процесс



Интеграция с NAC Guest Server



СПОНСОР

Внутренний пользователь, желающий предоставить доступ в Интернет своим гостям

NAC GUEST SERVER

Позволяет спонсору создать гостевую учетную запись; провести аудит; контролировать доступ

УСТРОЙСТВО СЕТЕВОГО ДОСТУПА

Перенаправление Web, аутентификация и обеспечение доступа. WLAN Controller или NAC Appliance

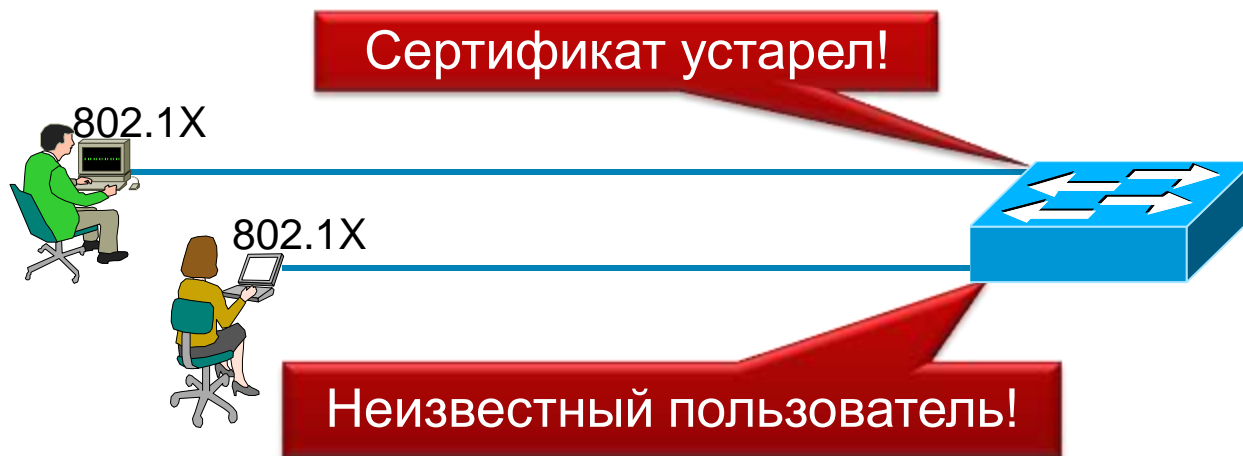
ГОСТЬ

Посетитель, которому нужен доступ в Интернет (обычно Интернет, но может и не только)

Особые случаи использования 802.1X

- Устройства без 802.1X сапликанта и гостевой доступ
- **Обработка неудачных аутентификаций**
- Последовательность методов аутентификации Flexible-Authentication
- Несколько устройств на порту
- Сапликанты
- 802.1X и Microsoft Windows

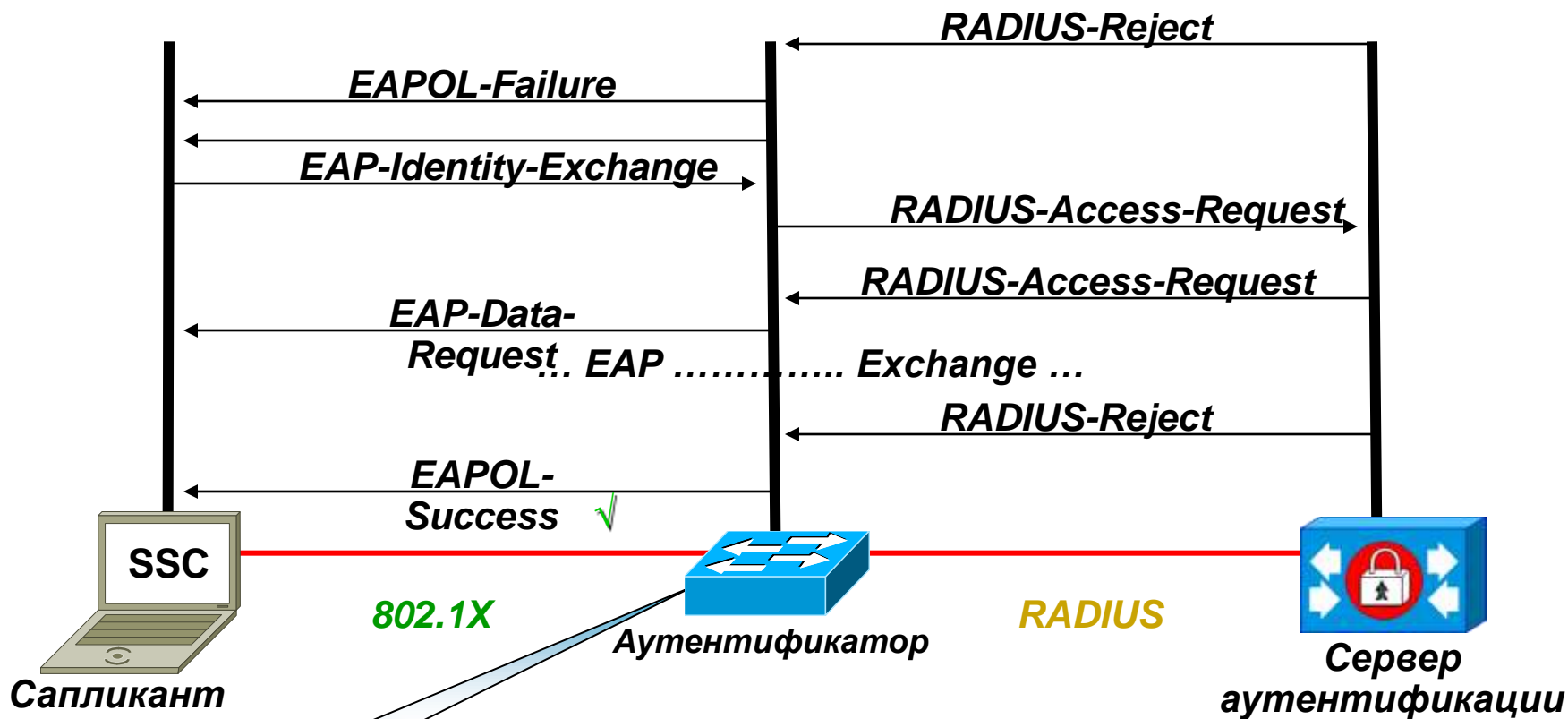
Зачем нужен доступ устройствам, которые не прошли аутентификацию?



- Аутентификационная информация устарела или введена неправильно
- На многих компьютерах 802.1X включен по умолчанию – пользователи не смогут попасть в Guest VLAN
- Многие компании требуют наличия ограниченного доступа к необходимым ресурсам для восстановления доступа

Неудачная аутентификация: Решение 1

Auth-Fail-VLAN



Доступ разрешен

```
interface GigabitE 3/13
authentication port-control auto
authentication event fail action authorize vlan 51
```

После трех последовательных неудачных аутентификаций порт будет переведен в авторизованное состояние

Auth-Fail VLAN

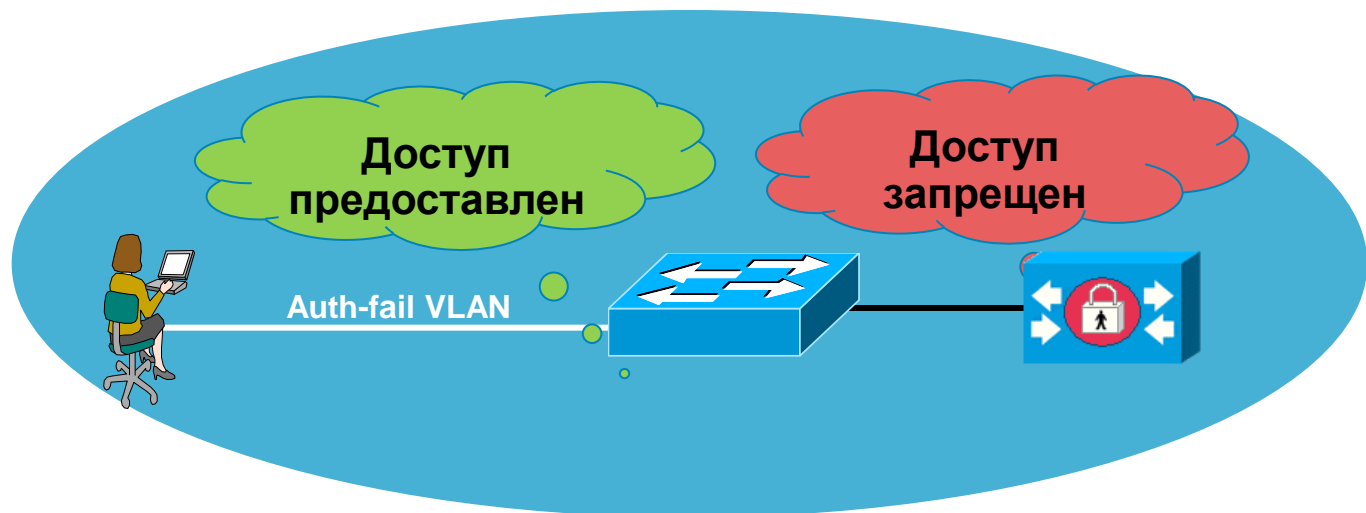
Замечания по применению

1. Сампликант не может выйти из Auth-Fail VLAN

Можно только: re-authentication (60 минут) или отключение порта

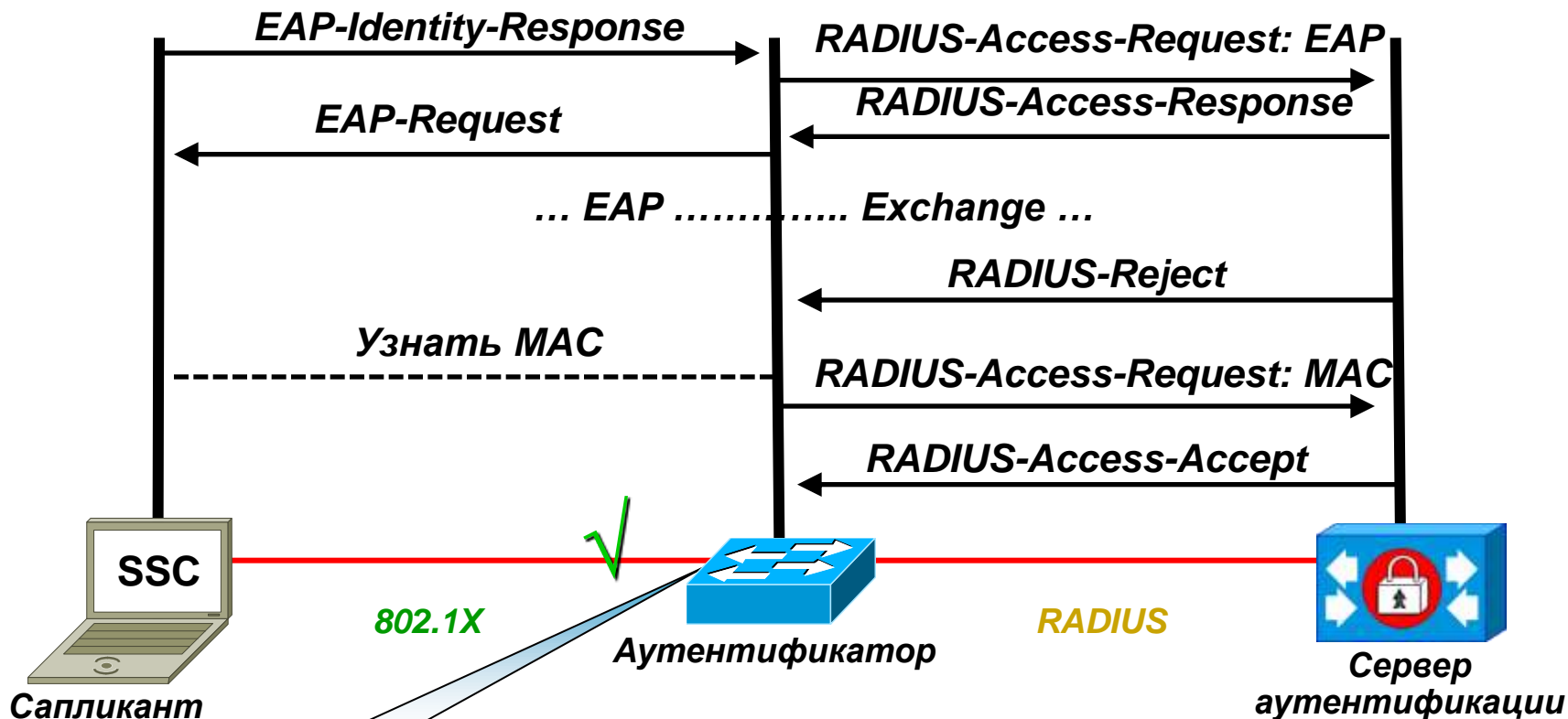
2. Auth-Fail VLAN, так же как и Guest VLAN, настраивается локально на коммутаторе

3. Коммутатор и сервер аутентификации имеют разное представление о событии



Неудачная аутентификация: Решение 2

Flex-auth: следующий метод



Доступ разрешен после MAB

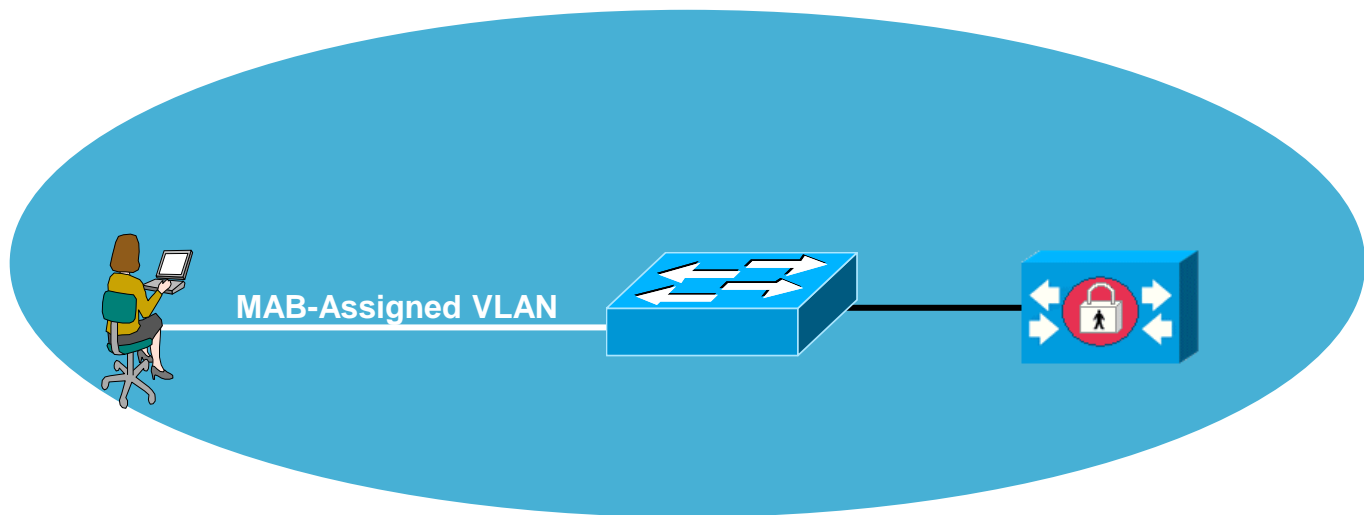
```
interface GigabitE 3/13
authentication port-control auto
authentication order dot1x mab
mab
authentication event fail action next-method
```

После неудачной аутентификации 802.1X, порт переходит к аутентификации с использованием следующего метода (MAB)

Next-Method MAB

Замечания по применению

- По прежнему нужно поддерживать БД MAC адресов
- Компромисс с безопасностью: должны ли 802.1X устройства получать тот же уровень доступа через MAB, если они не прошли 802.1X аутентификацию?



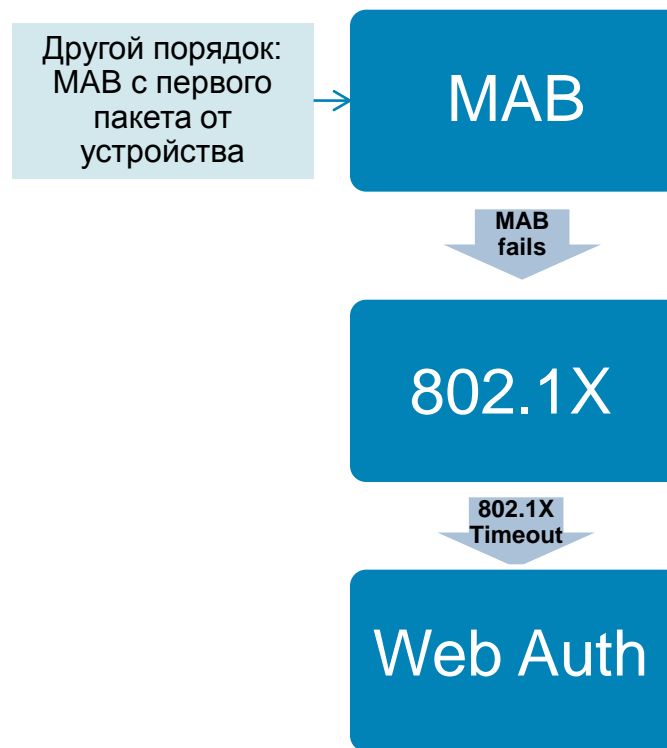
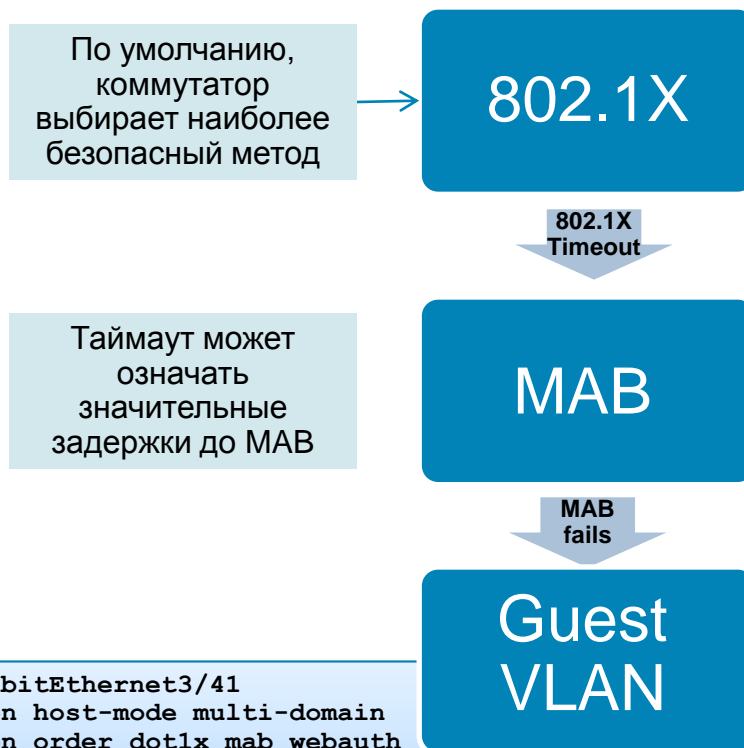
Особые случаи использования 802.1X

- Устройства без 802.1X сапликанта и гостевой доступ
- Обработка неудачных аутентификаций
- Последовательность методов аутентификации Flexible-Authentication
- Несколько устройств на порту
- Сапликанты
- 802.1X и Microsoft Windows

Последовательность методов аутентификации Flexible-Authentication

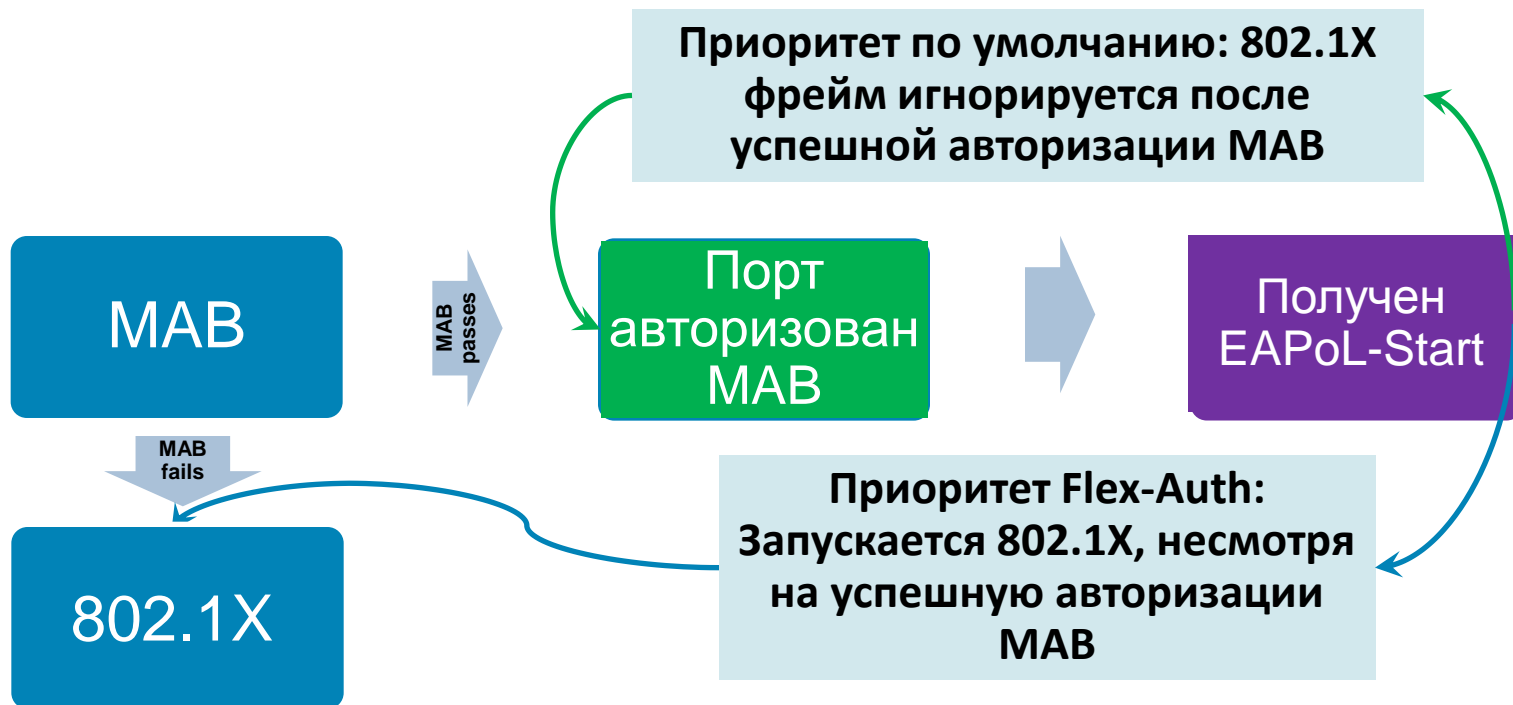
По умолчанию
Сначала 802.1X

Новый порядок
Сначала MAB



```
interface GigabitEthernet3/41
 authentication host-mode multi-domain
 authentication order dot1x mab webauth
 authentication priority dot1x mab webauth
 authentication port-control auto
 authentication violation restrict
 authentication fallback WEB-AUTH
 mab
```

Порядок методов Flex-Auth с указанием приоритета



- Приоритет определяет, какой метод преобладает над другими методами
- По умолчанию, очередность указания методов определяет приоритет (первый метод имеет высший приоритет)
- Если MAB имеет приоритет, то фреймы EAPoL-Starts будут игнорироваться после успешной авторизации MAB

Особые случаи использования 802.1X

- Устройства без 802.1X сапликанта и гостевой доступ
- Обработка неудачных аутентификаций
- Последовательность методов аутентификации Flexible-Authentication
- Несколько устройств на порту
- Сапликанты
- 802.1X и Microsoft Windows

Multi-Domain Authentication (MDA)

Решает проблему: два устройства на одном порту

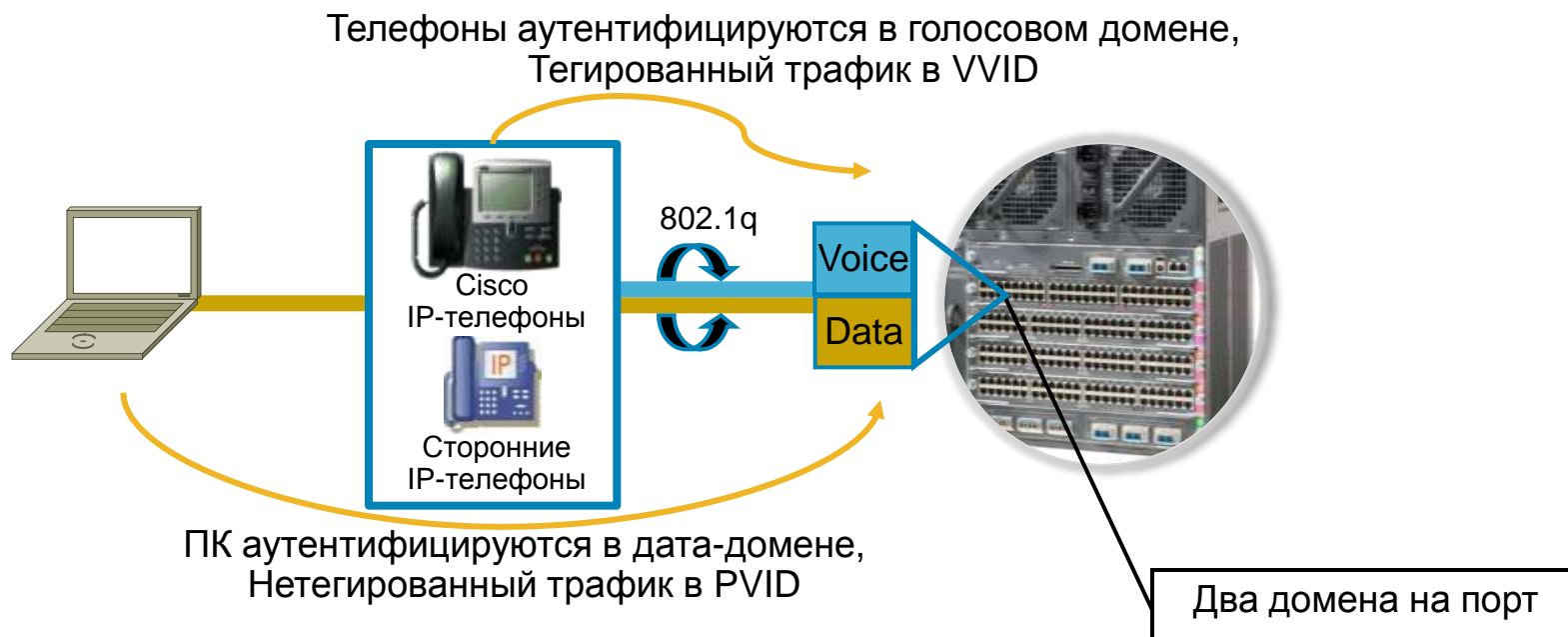
IEEE 802.1X

Одно устройство на порт



MDA

Одно устройство в домене на порт



- MDA заменяет CDP Bypass
- Поддерживает Cisco IP-телефоны и сторонние
- Телефоны и ПК используют 802.1X или MAB

Проблемы с использованием ИРТ

1) Легальные пользователи могут вызвать срабатывания защиты

Порт авторизован
для 0011.2233.4455



2) Неавторизованный доступ, используя MAC spoofing



Решая проблему с перемещением MAC адресов

Proxy EAPoL-Logoff



Сессия обнуляется сразу посылкой EAPoL-Logoff

Работает только с 802.1X устройствами и определенными телефонами*

802.1x/MAB Inactivity Timeout



Есть возможность подключения до истечения таймера и очистки сессии

Некоторым устройствам может понадобиться повторная аутентификация

CDP 2nd Port Notification



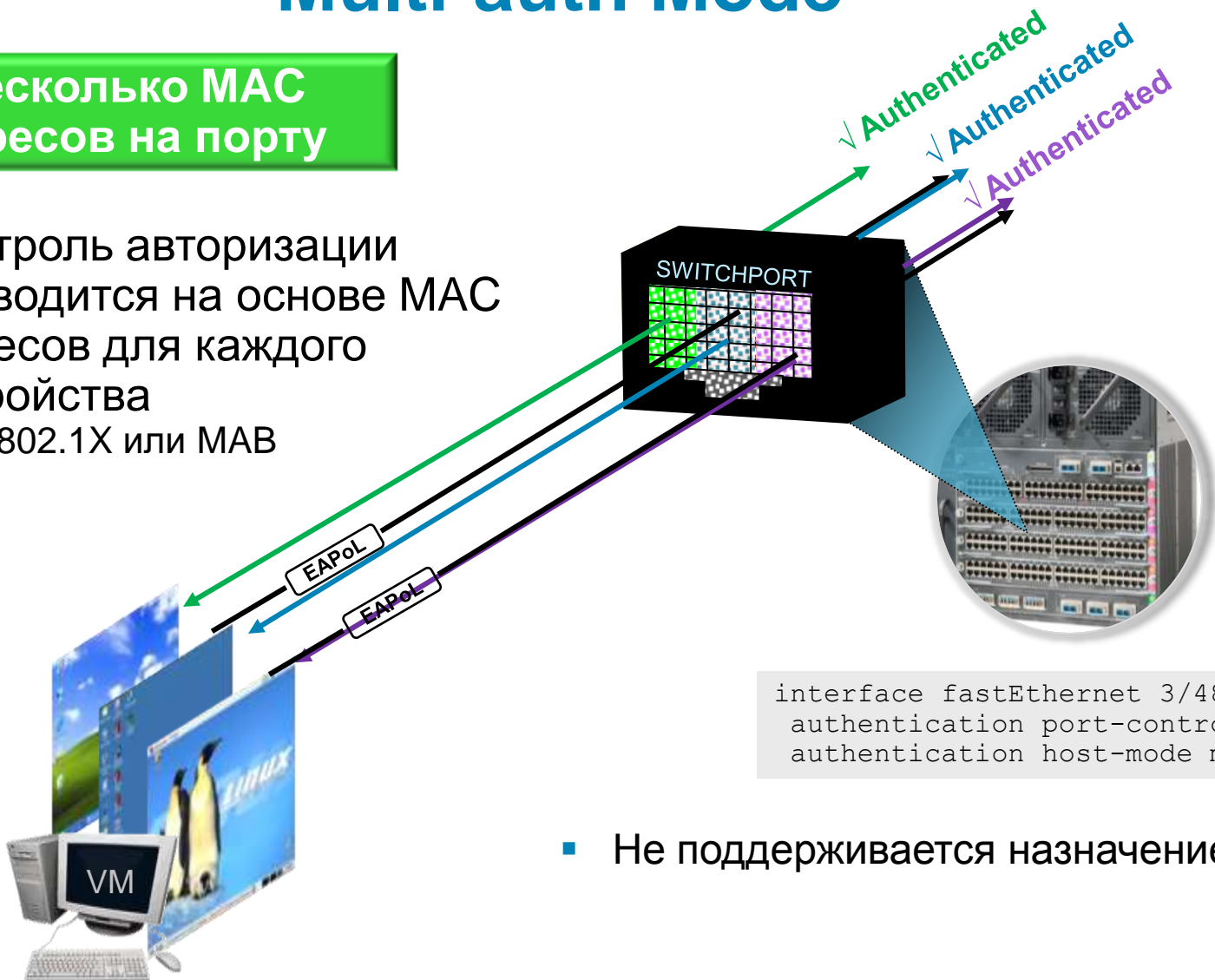
Сессия обнуляется сразу посылкой CDP Link Down

- ✓ Работает с MAB, 802.1X, и Webauth.
- ✓ Не требует настройки

Multi-auth Mode

Несколько MAC адресов на порту

- Контроль авторизации проводится на основе MAC адресов для каждого устройства
 - 802.1X или MAB



- Не поддерживается назначение VLAN

Особые случаи использования 802.1X

- Устройства без 802.1X сапликанта и гостевой доступ
- Обработка неудачных аутентификаций
- Последовательность методов аутентификации Flexible-Authentication
- Несколько устройств на порту
- Сапликанты
- 802.1X и Microsoft Windows

Cisco Secure Services Client (SSC)

- Поддерживает функции встроенных сапликантов и даже больше

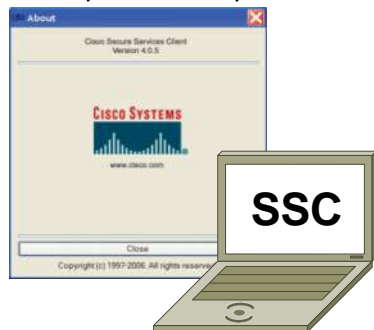
Типы EAP

PEAP, TLS, FAST, и др.

Интерфейс управления

Автоматическое
установление VPN туннеля

Windows XP, 2003, Vista



Secure Services Client

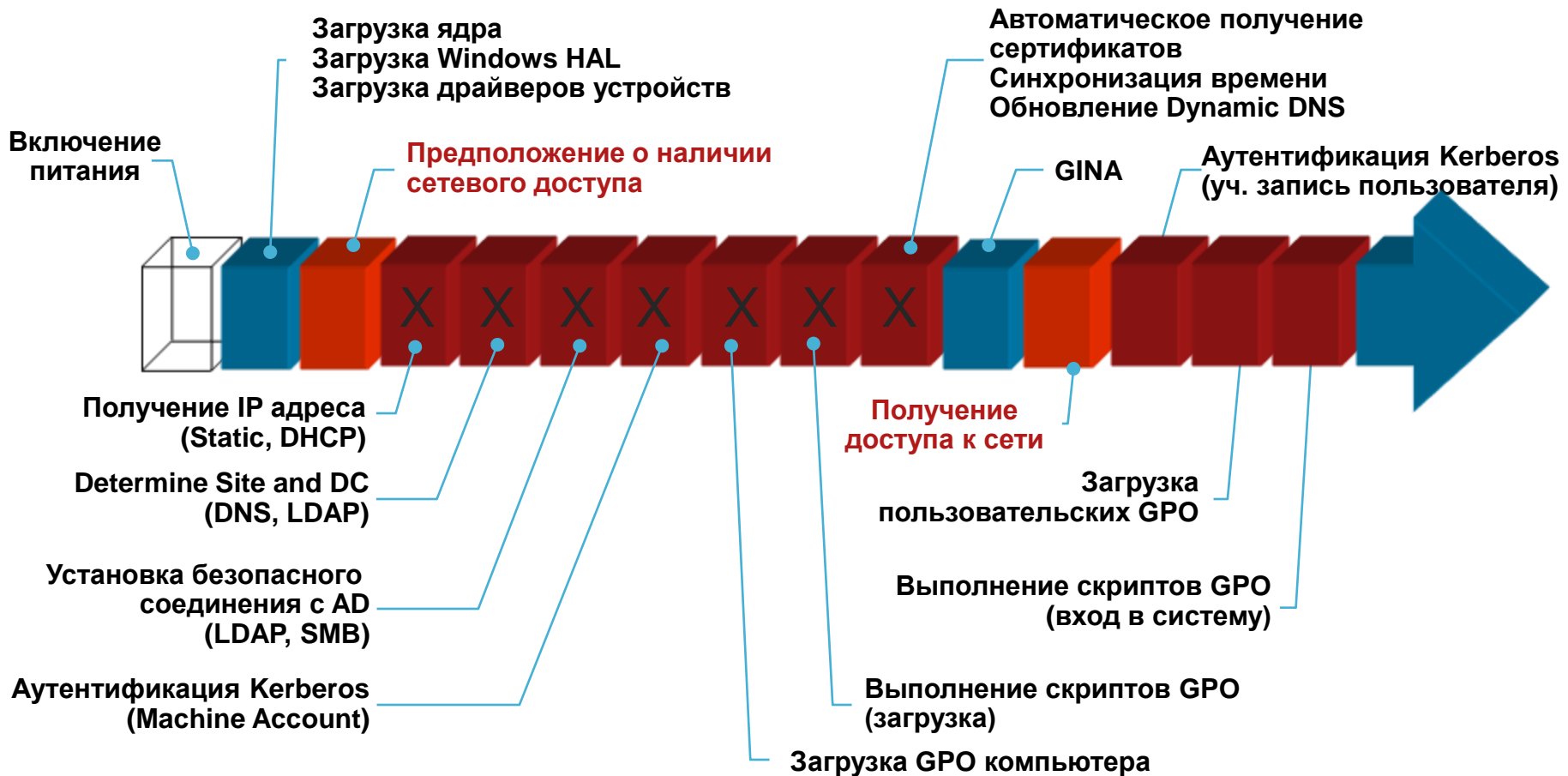
Функции

- Поддержка проводных и беспроводных интерфейсов
- Стандартное поведение для всех ОС Windows
- Управление профайлами подключений
- Запрет определенных подключение на основе политик
- Поддержка стандартов
- Поддержка Single sign-on
- Бесплатен для проводных подключений

Особые случаи использования 802.1X

- Устройства без 802.1X сапликанта и гостевой доступ
- Обработка неудачных аутентификаций
- Последовательность методов аутентификации Flexible-Authentication
- Несколько устройств на порту
- Сапликанты
- 802.1X и Microsoft Windows

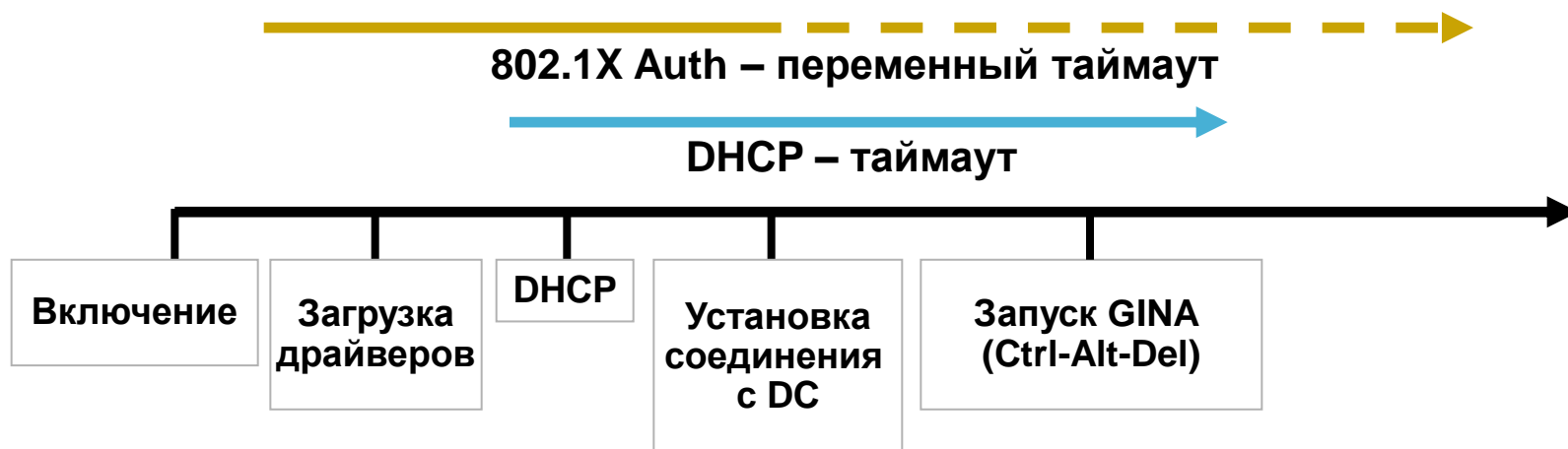
Процесс загрузки ОС Windows



Проблема 1: Microsoft и DHCP

DHCP это параллельный процесс, независимый от аутентификации 802.1X

- На проводных интерфейсах успешная аутентификация 802.1X **не запускает** процесс DHCP address discovery
- DHCP запускается как только подключается физический уровень
- Если аутентификации 802.1X занимает много времени, то адрес по DHCP может быть не получен



Проблема 2: Машинные групповые политики GPO

Что такое групповая политика?

- **Групповая политика** — это набор правил, в соответствии с которыми производится настройка рабочей среды Windows в окружении Active Directory
- **Типы групповых политик**
 - Политика на основе реестра
 - Опции безопасности
 - Установка и обслуживание ПО
 - Скрипты
 - Перенаправление папок

Решение: Машинная аутентификация

- Что такое машинная аутентификация?

Возможность Windows-компьютера аутентифицироваться используя собственную учетную записку, независимо от сессии пользователя

- Для чего она используется?

Машинная аутентификация используется в момент загрузки операционной системы, для того, чтобы аутентифицироваться и взаимодействовать с контролерами домена для получения машинных групповых политик.

- Почему нужно это использовать?

802.1X блокирует сетевой доступ до завершения аутентификации и мешает получению IP адреса, и скачиванию машинных групповых политик. Используйте машинную аутентификацию для исправления этой ситуации.

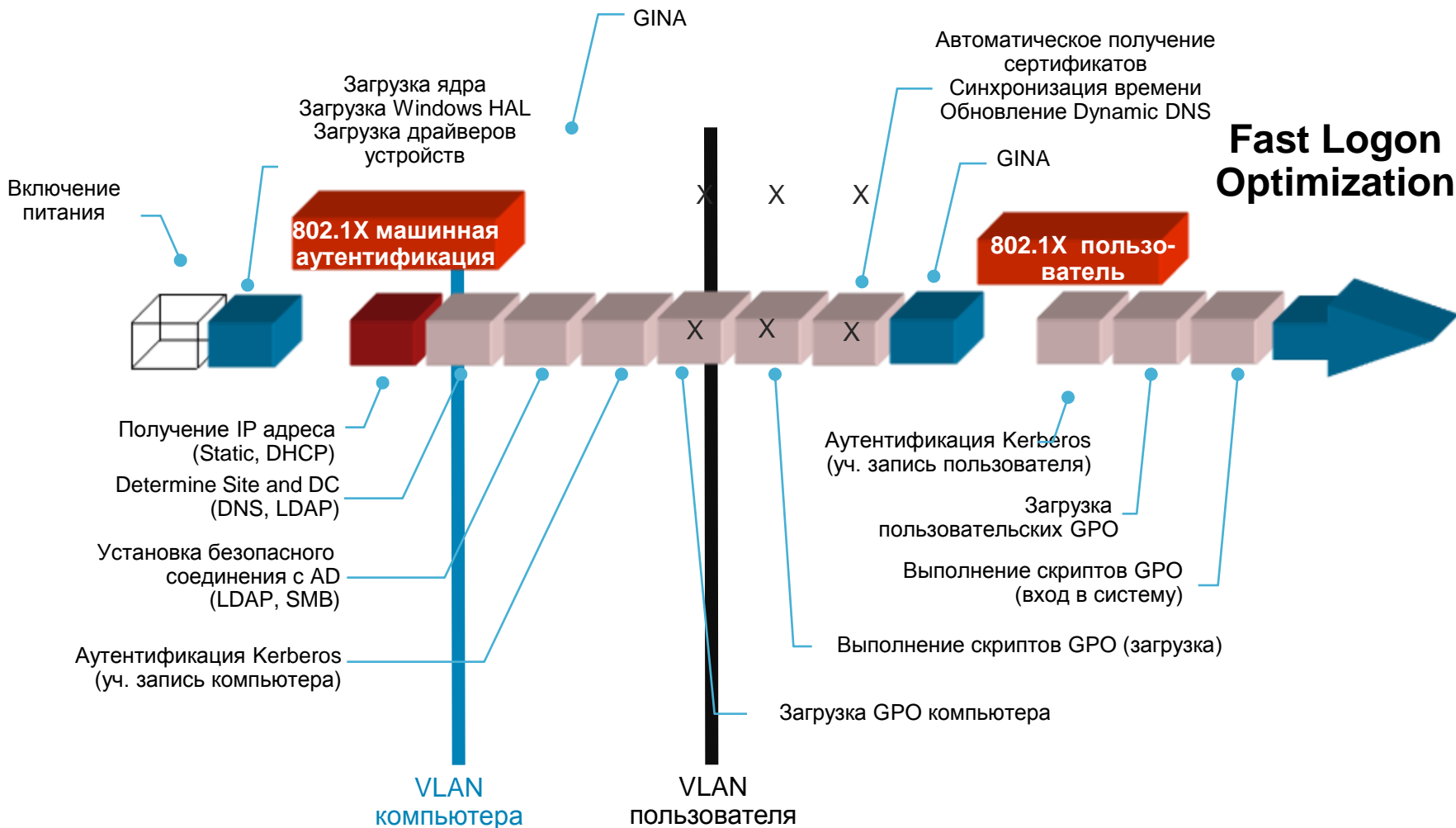
802.1X: Назначение VLAN

DHCP Renewal

- При назначении динамического VLAN с использованием пользовательской и машинной аутентификации, VLAN может смениться после аутентификации пользователя.
 - IP адрес так же должен быть сменен
- Поведение сапликанта было исправлено
 - Windows XP: service pack 1a + KB 826942
 - Windows 2000: service pack 4
 - Необходимо для присвоения VLAN с использованием сервиса Wireless Zero Config
- Исправленный сапликант запрашивает обновленный IP адрес через DHCP
 - Успешная аутентификация заставляет клиента три раза пропинговать шлюз по умолчанию, с интервалом менее секунды
 - Отсутствие ответа запускает обновление IP адреса через DHCP
 - Если шлюз отвечает, то IP адрес не меняется

Процесс загрузки ОС Windows

Назначение VLAN и Fast Logon Optimization



802.1X и Windows: Рекомендации

- Машинная аутентификация обязательна в большинстве случаев
- Рассмотрите вариант использования только машинной аутентификации
- По возможности используйте встроенные в AD средства
 - Компьютеры инициализируются автоматически с использованием машинного пароля
 - Возможен автоматически выпуск сертификатов посредством GPO AD

VLAN'ы и Windows: Рекомендации

- Используя динамические VLANы:
 - Выключите Fast Logon Optimization
 - Используйте один и тот же VLAN для машинной и пользовательской аутентификации
 - Назначение VLANов требует изменений в AD, DHCP, IP адресации, и сетевой инфраструктуре – подумайте прежде чем делать это
- Листы контроля доступа (ACL) – альтернатива использованию VLANов, но учитывайте ограничение TCAM
 - Старайтесь использовать как можно более простые ACL, привязанные к группам
- Используйте имена VLAN'ов, а не их номера
- Не используйте VLAN'ы для компьютеров без сапликантов

Другие задачи..

- Доступность RADIUS сервера

Проблема: невозможность получения доступа к сети в случае отказа сервера аутентификации

Решение: Резервирование серверов аутентификации

Решение: Inaccessible Authentication Bypass – назначение определенного VLAN на порт

- Remote Desktop Connect (RDC)

Проблема: в Windows XP после удаленного входа посылается команда EAP-Logoff

Решение: Использовать сапликант Cisco (CSSC)

Другие задачи..

- Pre eXecution Boot Environment (PXE)

Проблема: невозможно получить доступ к сети для загрузки ОС

Решение: Используйте MAB и настройку 802.1X timeout

Решение: Используйте Open Mode + ACL

- Wake On Lan (WOL)

Проблема: Невозможность отправки magic packet на неавторизованный порт

Решение: Выключите контроль для исходящего с порта трафика

Решение: Intel Advanced Management Technology (сапликант на сетевой карте)

Заключение



Фазы внедрения 802.1X

Режим мониторинга

Основные технологии

- Open mode

Преимущества

- Свободный доступ
- Нет влияния на сеть
- Логи и отчеты для анализа



Режим ограниченного доступа

Основные технологии

- Open mode
- ACL загружаемые и на уровне порта

Преимущества

- Базовая связность по-прежнему доступна
- Повышенная безопасность доступа
- Разграничение доступа



Безопасный режим

Основные технологии

- Стандартный закрытый режим
- Назначение динамических VLANов (опция)

Преимущества

- Строгий контроль доступа



Новый функционал 802.1X на коммутаторах позволяет..

- Обеспечивать поддержку различного типа пользователей и хостов
 - Корпоративные пользователи (с 802.1X)
 - Корпоративные хосты и пользователи (без 802.1X)
 - Гостевые пользователи
 - Поддержка WoL, VMWare, PXE, IP телефония, и др.
- На одном порту
- И без его перенастройки!

Заключение

- 802.1X улучшает безопасность
- 802.1X повышает прозрачность использования ЛВС
- 802.1X это платформа для других мер по обеспечению безопасности
- 802.1X действительно можно внедрить (теперь)
- Новая функциональность в коммутаторах ЛВС существенно упрощает развертывание 802.1X
- **Cisco 802.1X (IBNS) > 802.1X**

Доступность новой функциональности в Cisco IOS

	Catalyst 6500 series	Catalyst 4500 series	Catalyst 36xx, 37xx, 2960
Open Mode	12.2(33)SXI	12.2(50)SG	12.2(50)SE
Flex-Auth	12.2(33)SXI	12.2(50)SG	12.2(50)SE
Multi-Auth	12.2(33)SXI	12.2(50)SG	12.2(50)SE
dACL	12.2(33)SXI	12.2(50)SG	12.2(50)SE
CDP 2 nd port	12.2(33)SXI	12.2(50)SG	12.2(50)SE
Enhanced syslogs	12.2(33)SXI	12.2(50)SG	12.2(50)SE

Вопросы и Ответы



Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com или по телефону: +7 (495) 961-1410

Мы хотели бы узнать Ваше мнение

Пожалуйста,
заполните анкету



Дополнительная литература

- Краткое техническое описание Identity-Based Networking Services
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/data_sheet_c78-542121.html
- Пошаговое внедрение IBNS/802.1X, описание методологии
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/whitepaper_C11-530469.html
- Пошаговое внедрение IBNS/802.1X, пример настройки
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/Whitepaper_c11-532065.html

Дополнительная литература

- Настройка 802.1X на коммутаторах серии Catalyst 2960
http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_50_se/configuration/guide/sw8021x.html
- Настройка 802.1X на коммутаторах серии Catalyst 3560
http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_50_se/configuration/guide/sw8021x.html
- Настройка 802.1X на коммутаторах серии Catalyst 3750
http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_50_se/configuration/guide/sw8021x.html
- Настройка 802.1X на коммутаторах серии Catalyst 4500
<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/50sg/configuration/guide/dot1x.html>
- Настройка 802.1X на коммутаторах серии Catalyst 6500
<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html>

