

Контроль пользовательского доступа на основе технологии 802.1x и цифровых сертификатов

Томилко Виталий Евгеньевич
Системный архитектор



ОТКРЫТЫЕ
ТЕХНОЛОГИИ



Предоставление доступа пользователей к внутренним ресурсам

- Наличие последних обновлений антивирусных баз данных на рабочих станциях
- Контроль п/о рабочих станций (OS service pack, HotFixes)
- Контроль техно-парка оборудования (серверы, ноутбуки, рабочие станции, персональные устройства КПК, принтеры, терминалы и т.д)
- Контроль пользователей и привилегий доступа

Протокол 802.1x

- Контроль подключений персональных устройств к сети

Выбор EAP-TLS
(PKI инфраструктура)
(сертификаты X.509)

Цифровые сертификаты X.509

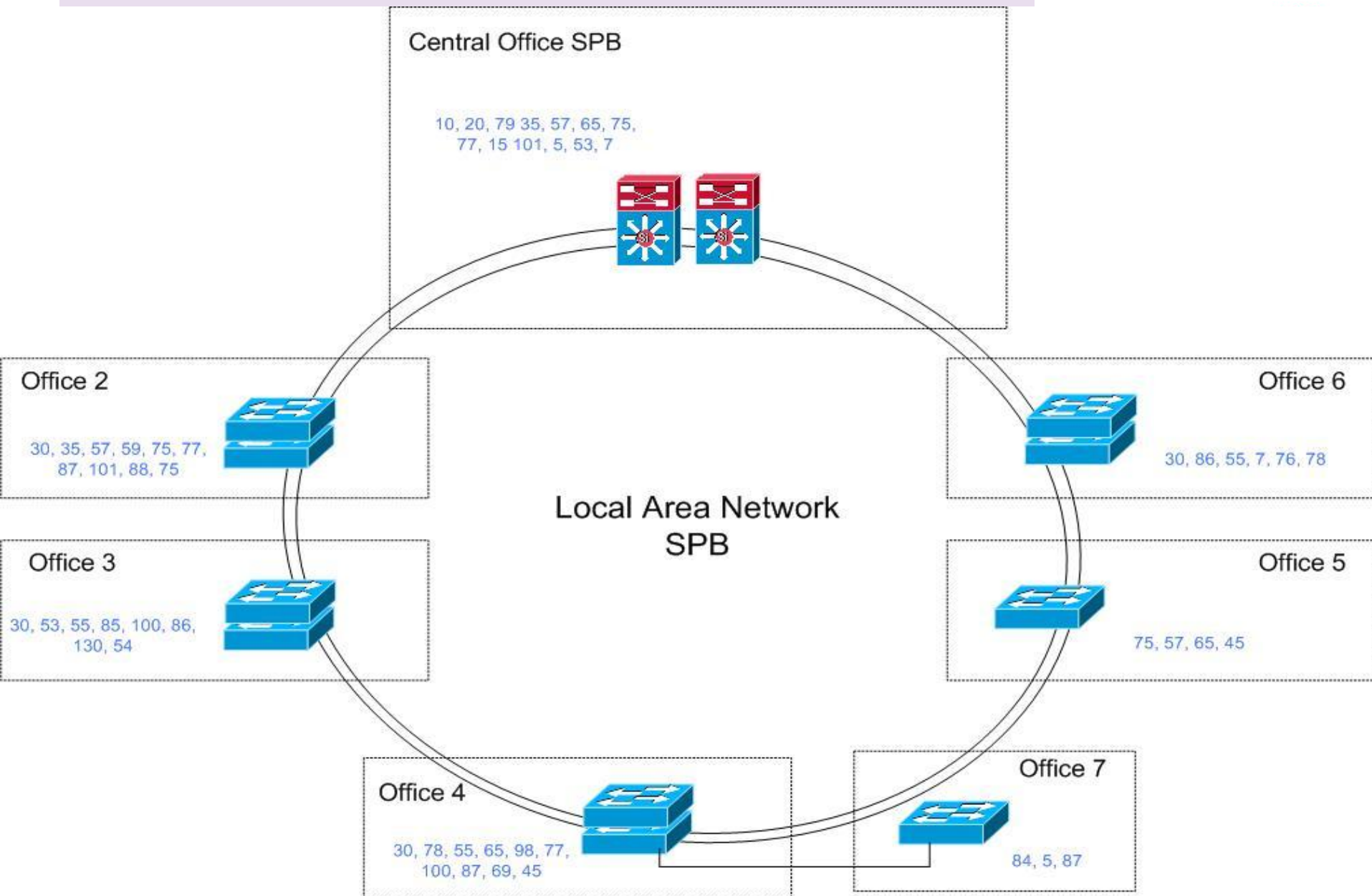
- Идентификация и авторизация сетевых устройств и пользователей при подключении к сети

Защита от неавторизованного подключения и контроль

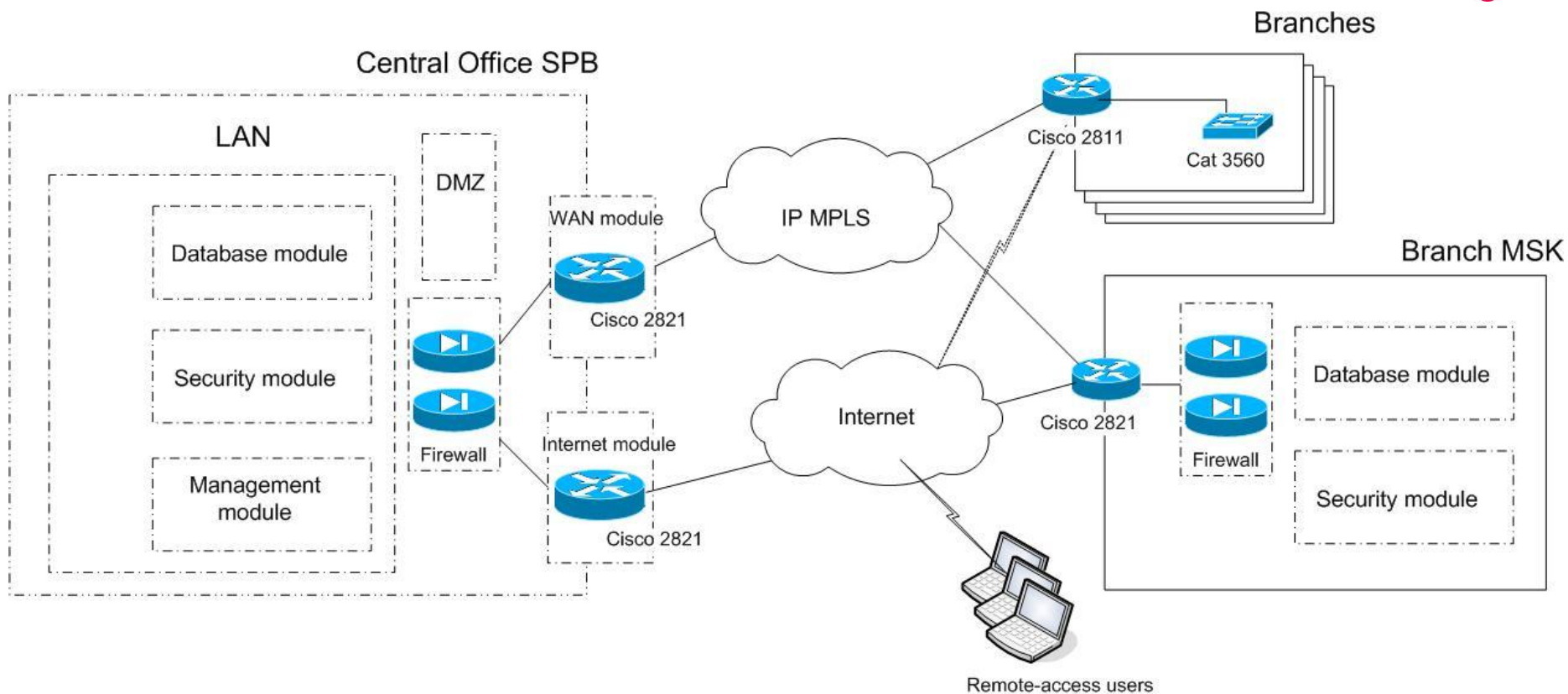
Практические аспекты внедрения решения для территориально-распределенной организации

- LAN, WAN топология
- Дизайн Active Directory
- Задачи и пути решения
- Сценарии
- Пример контроля доступа

LAN топология



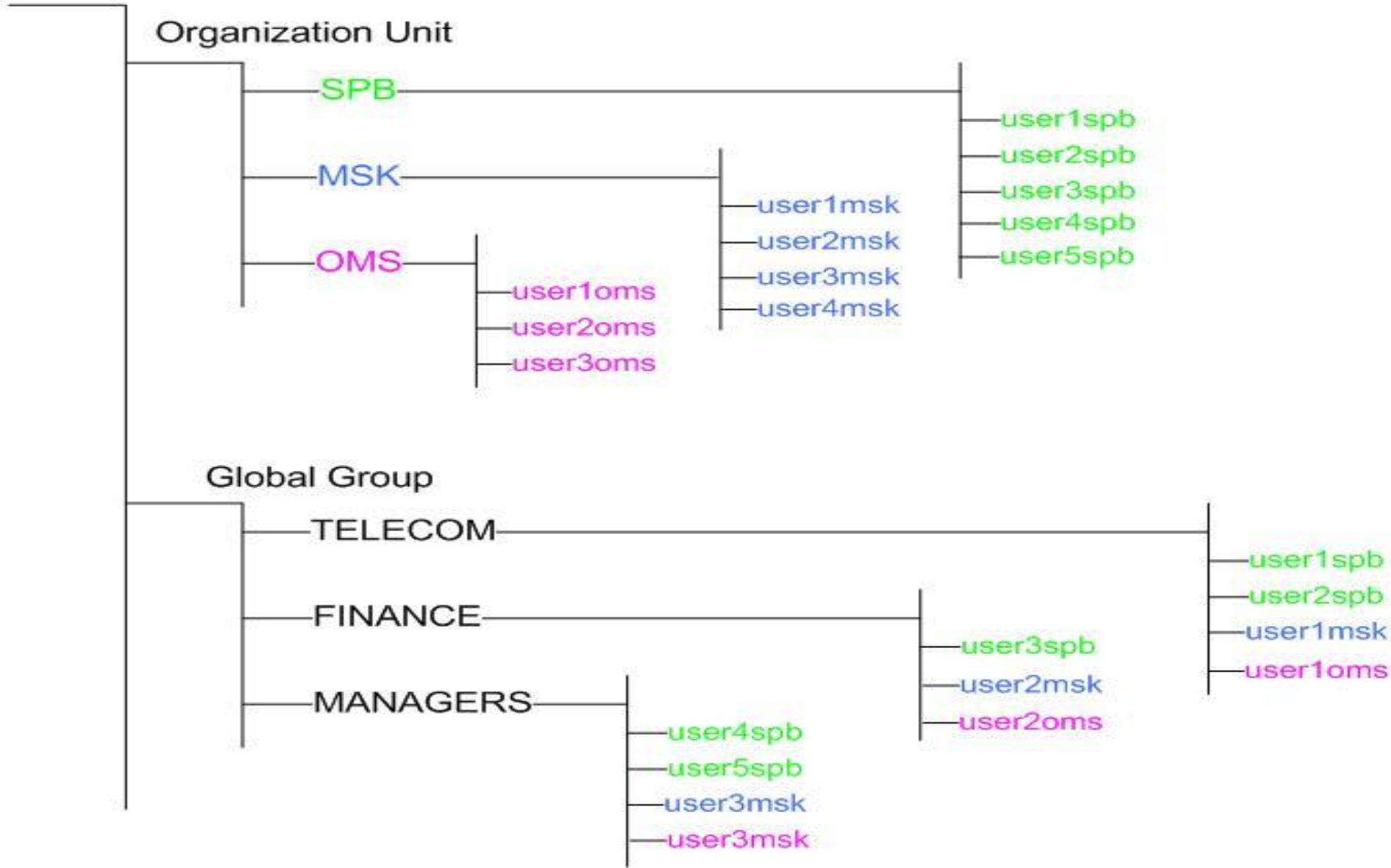
WAN топология



Дизайн Active Directory



Domain Controller – Sky.lan



Задачи и пути решения

□ Задачи

□ Сетевой дизайн

Снижение затрат на управление IT

Идентификация и авторизация

Общее повышение защищенности

Единый носитель сертификата

Диагностика и анализ событий

□ Достигаемый результат

Интеграция с Active Directory

Внедрение Certification Authority

AAA на базе RADIUS

Идентификация на уровне подключения

Использование Dot1X инфраструктуры
Назначение VLAN ID на порт

Назначение IP адреса на рабочую станцию

Мониторинг и сбор статистики

Сценарии

- Переезды пользователей. Концепция свободного рабочего места.

- Посменная работа операторов, кассиров и т. д. Многопользовательская среда.

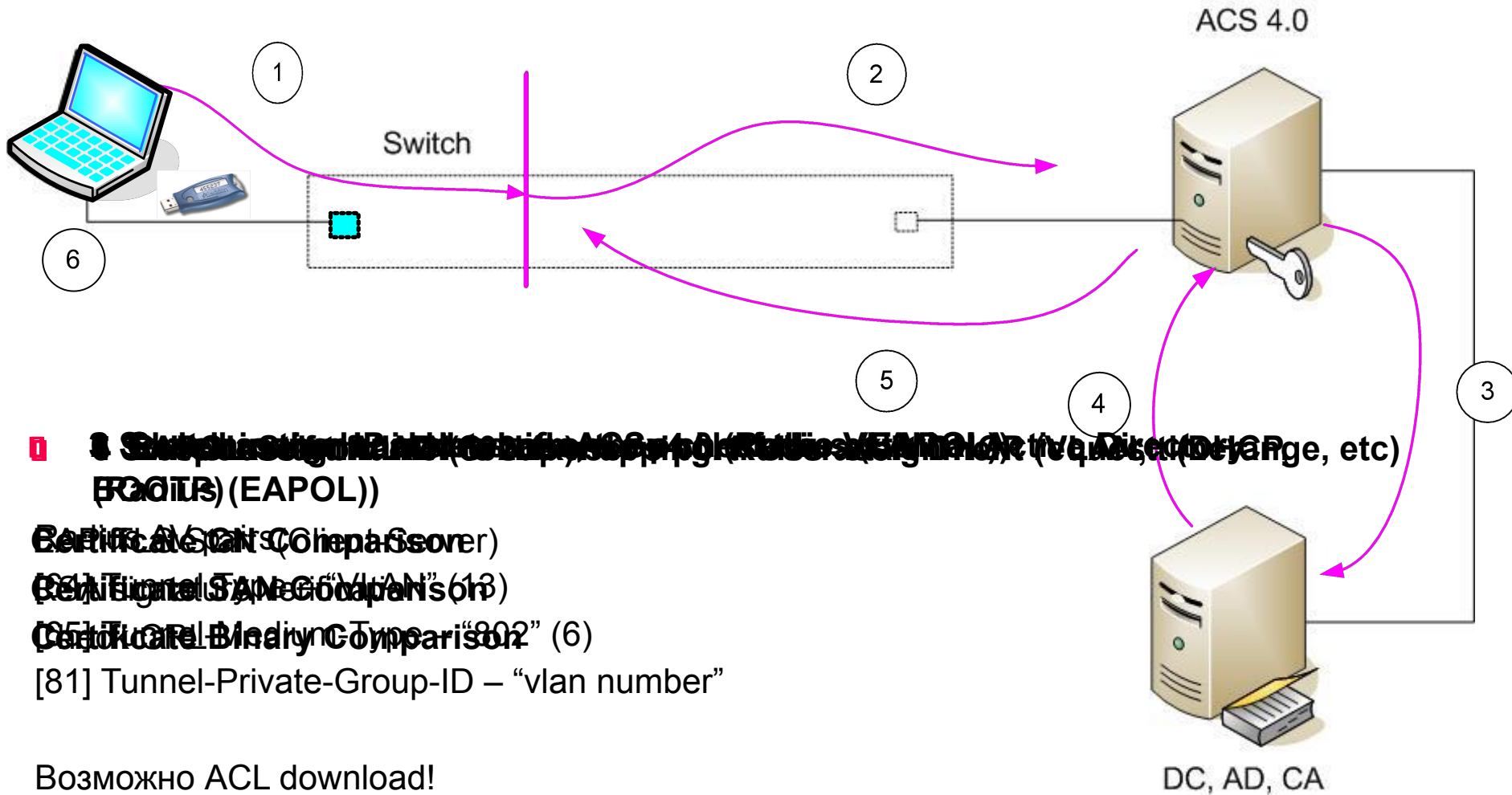
- Удаленный доступ к ресурсам (из гостиницы, дома). Установление VPN, авторизация на уровне сети и на уровне приложений

- Предоставление гостевого входа (доступ в интернет для заказчика, партнера)

- Подключение принтеров, терминалов и других устройств, не поддерживающих 802.1x

Защита от неавторизованного подключения и контроль

Пример контроля доступа



1. Subsequent RADIUS requests (e.g., RADIUS Accounting) to a Director (or RADIUS) (EAPOL)

2. RADIUS Accounting (over)

3. RADIUS Accounting (over)

4. RADIUS Accounting (over) (6)

[81] Tunnel-Private-Group-ID – "vlan number"

Возможно ACL download!

[009/001] cisco-av-pair

Защита от неавторизованного подключения и контроль

AD. Users and Computers.

Групповые политики

Users

- Remote access permission (Dial-up or VPN)
- Groups membership (Domain administrators, Domain users, Telecom)

Computers

- Autoenrollment settings (Enroll certificate automatically)
- Smart card removal behavior (Lock Workstation)
- Control local devices (USB, COM, IrDA, Bluetooth, Wi-Fi т. д.)

Развитие. Комплексное решение на основе агентского П/О

Подключение к сети

Сканирование стека TCP/IP

Анализ реестра

Сбор версий OS, hotfixs, версии антивирусного п/о

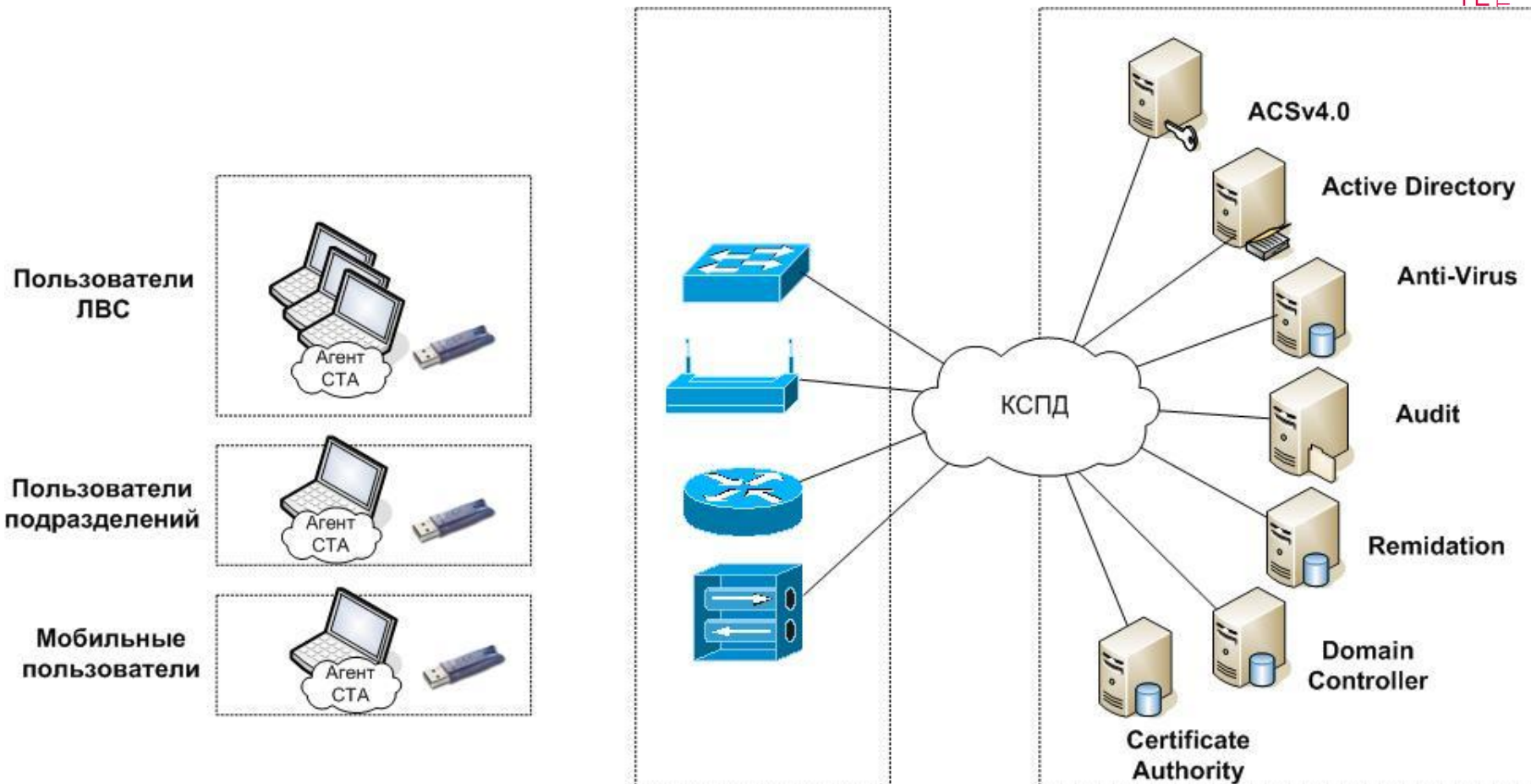
Загрузка обновлений

Повторный аудит

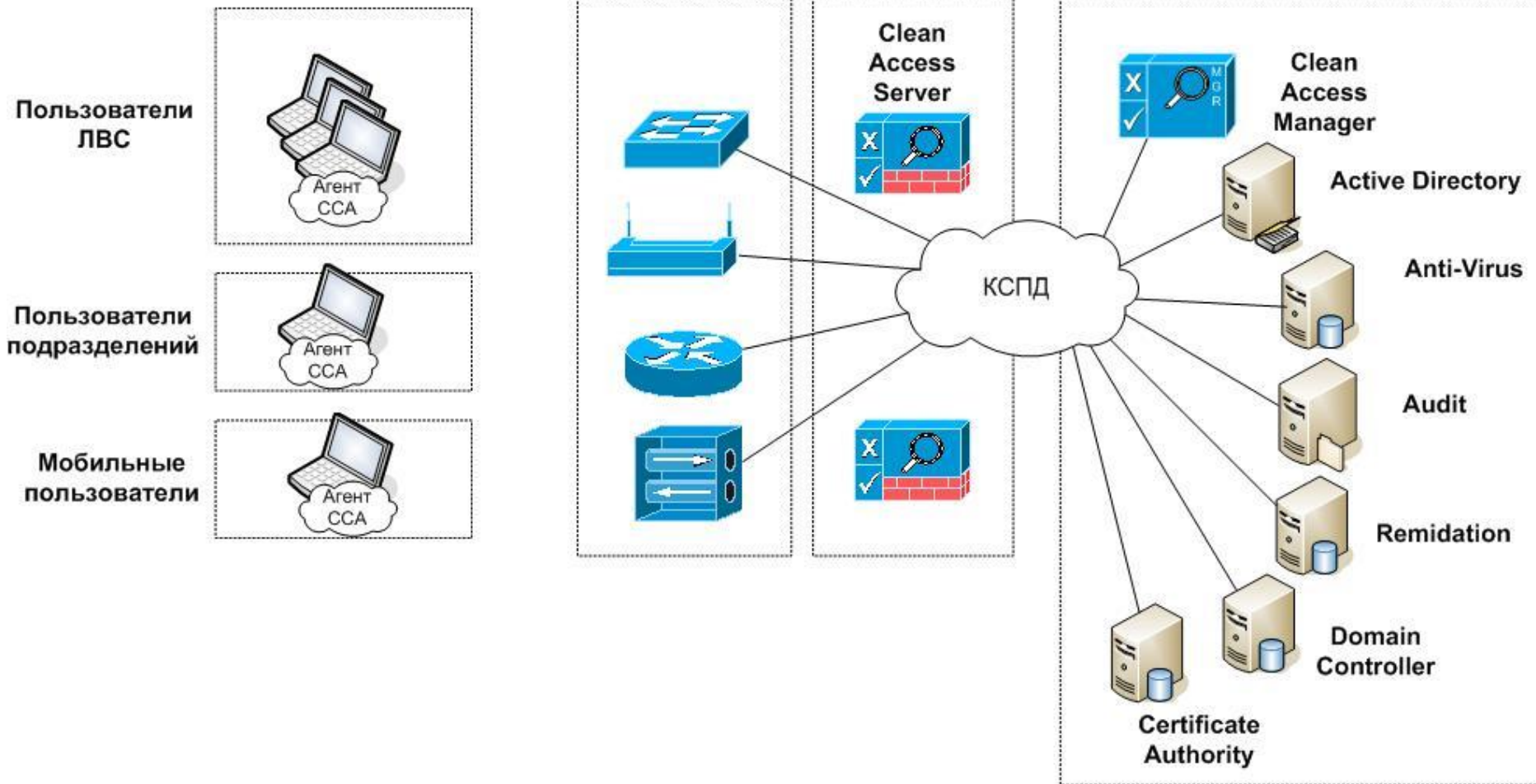
Предоставление доступа

Защита от неавторизованного подключения и контроль

Решения на основе 802.1x инфраструктуры

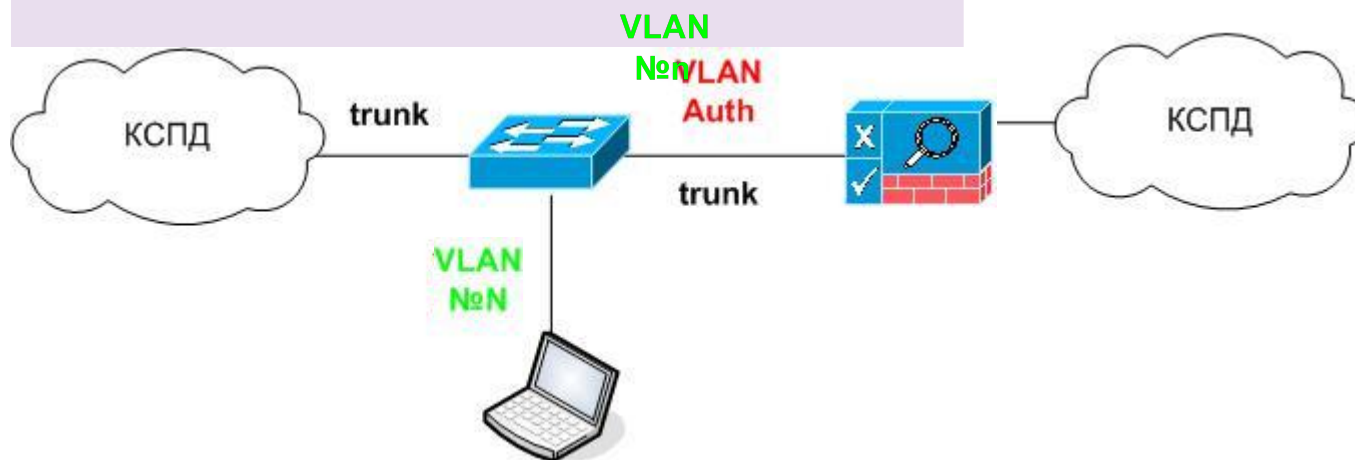


Решения независимые от 802.1x инфраструктуры



Архитектура решения

Внутри полосы (in-band)



Решения на основе 802.1x инфраструктуры

Преимущества

Недостатки

Контроль доступа к сетевым ресурсам
с рабочей станции

Нет SSO (Single Sign-On)

При физическом подключении к сети сразу

высылается запрос на авторизацию

Не все операционные системы и

пользователи поддерживают сертификаты для

идентификации пользователя или рабочей

станции

Решения на основе агентского п/о

Преимущества

- Контроль подключения к сетевым ресурсам вплоть до уровня приложений
- Недостатки
 - Независимость от типа операционных систем на рабочих станциях
 - Очень высокие требования к централизованной проверке состояния рабочей отказоустойчивости инфраструктуры сети станций на соответствие корпоративным правилам
 - Централизованное управление всеми коммутаторами (настройки вплоть до порта)
 - Возможность реализации SSO (Single Sign-On)

Защита от неавторизованного подключения и контроль



ОТКРЫТЫЕ
ТЕХНОЛОГИИ

ТЕХНОЛОГИИ ОТКРЫТИЙ

Россия, 117997, Москва, ул. Обручева, 30, стр. 2

Тел.: (495) 787-08-88, 787-70-27

Факс: (495) 787-70-28, 225-23-58

E-mail: info@ot.ru

www.ot.ru

Table 1-3 EAP Authentication Protocol and User Database Compatibility

Database	LEAP	EAP-MD5	EAP-TLS	PEAP (EAP-GTC)	PEAP (EAP-MS CHAPv2)	EAP-FAST Phase Zero	EAP-FAST Phase Two
ACS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes	Yes	Yes
Windows AD	Yes	No	Yes	Yes	Yes	Yes	Yes
LDAP	No	No	Yes	Yes	No	No	Yes
ODBC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	No	Yes	Yes	Yes	Yes
All Token Servers	No	No	No	Yes	No	No	No