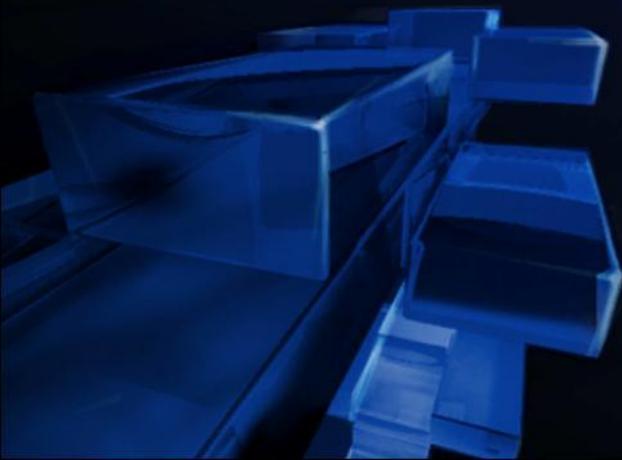




Построение эффективной ИТ инфраструктуры филиалов и дочерних предприятий

Александр Липкин
Microsoft



Региональные офисы: почему это важно

- Более 30% организаций имеют в своем составе региональные офисы
- Более 33% IT-бюджета приходится на филиалы
- В крупных организациях 55% сотрудников работают в филиалах
- Расходы на каналы связи – серьезная статья расходов для организаций
- Региональные офисы: 76% ОС Windows

Региональные офисы. Проблемы

- Каналы связи
- Предоставление сервисов для конечных пользователей филиала
- Управление и поддержка серверов
- Поддержка пользователей и защита данных

Сервера в сайте ГО?



- Эффективный процесс управления
- Каналы связи ухудшают качество предоставления сервиса в филиале

Сервера в сайте филиала?



- Предоставление сервиса вне зависимости от WAN
- Ограничены возможности управления, администрирования, а также предоставления новых сервисов для филиалов

Подходы к построению инфраструктуры дочерних предприятий

- Централизация сервисов
 - Что необходимо централизовать в первую очередь
 - Требования по изоляции и автономности
- Стандартизация серверов
 - Как обеспечить минимальное количество стандартных конфигураций серверов
- Консолидация серверов
 - Как правильно разместить сервисы
 - Виртуализация

Централизация сервисов

- Автономность – независимость, но не эксклюзивный контроль над ресурсами.
- Изоляция – независимость и эксклюзивный контроль над ресурсами.

Пример: автономность и изоляция при проектировании Active Directory

- **Обеспечение изоляции сервисов и данных**
 - формирование отдельного леса Active Directory
- **Обеспечение автономности сервисов и данных**
 - делегирование полномочий на требуемые ресурсы в рамках единого леса/домена

BOIS: Branch Office Infrastructure Solution

Основная задача – формирование эффективной инфраструктуры предприятия, имеющего распределенную филиальную сеть.

- Эффективное использование ресурсов
- Эффективная модель управления и администрирования
- Сокращение времени простоя при сбоях
- Высокий уровень унификации и стандартизации

VOIS. История развития

VOIS v.1 – май 2005

- Построен на основе и как часть WSSRA
- Windows Server 2003, SMS, MOM
- Архитектура "Single

VOIS v.2 – февраль 2006

- Фокус на архитектуре и проектировании распределенных сервисов.
- Windows Server 2003 R2
- Новые руководства по проектированию, включая DFS, PMC, VPN

VOIS v.3 – скоро

- Windows Server 2008 и Windows Vista
- Акцент на возможностях виртуализации
- Дополнительные руководства по проектированию

Региональные офисы. Логическая топология

- Модели управления
 - Централизованные сервисы
 - Распределенные сервисы
- Топология региональных офисов
 - Сателлит или микро-офис. Все ИТ – сервисы расположены в центральном офисе или региональном центре.
 - Региональный центр. Распределение сервисов между филиалом и ГО.
 - Автономный региональный офис. Сервисы расположены локально. Минимальная зависимость от ИТ головного офиса
- Проектирование сервисов
 - Основные инфраструктурные сервисы
 - Дополнительные сервисы и службы
 - Сервера приложений
 - Почтовая служба и средства совместной работы
 - Терминальные сервисы и Web caching

Типовые модели управления

- Централизованная модель администрирования и управления – централизованные сервисы
 - Единый бюджет и IT-департамент
 - Стабильная структура, четко определены процессы, регламенты и задачи
 - Высокая степень стандартизации и унификации, а также отказоустойчивости систем
- Распределенная модель администрирования и управления – распределенные сервисы
 - IT филиала автономно, локальное подчинение
 - Стандартизация в рамках филиала, структура нестабильна, возможны технологические инновации
 - Процессы и регламенты не определены

Преимущества централизованной модели

Легче гарантировать требуемый уровень безопасности

Эффективность в предоставлении новых сервисов

Легче обеспечить отказоустойчивость сервисов

Эффективность управления сервисами, а также осуществления их мониторинга

Предсказуемость и прозрачность в управлении ИТ- бюджетом

Эффективность управления ресурсами

Преимущества распределенной модели

Минимальная зависимость от каналов связи

Минимальные задержки при работе с приложениями - все сервисы в пределах LAN

Проще процесс управления изменениями

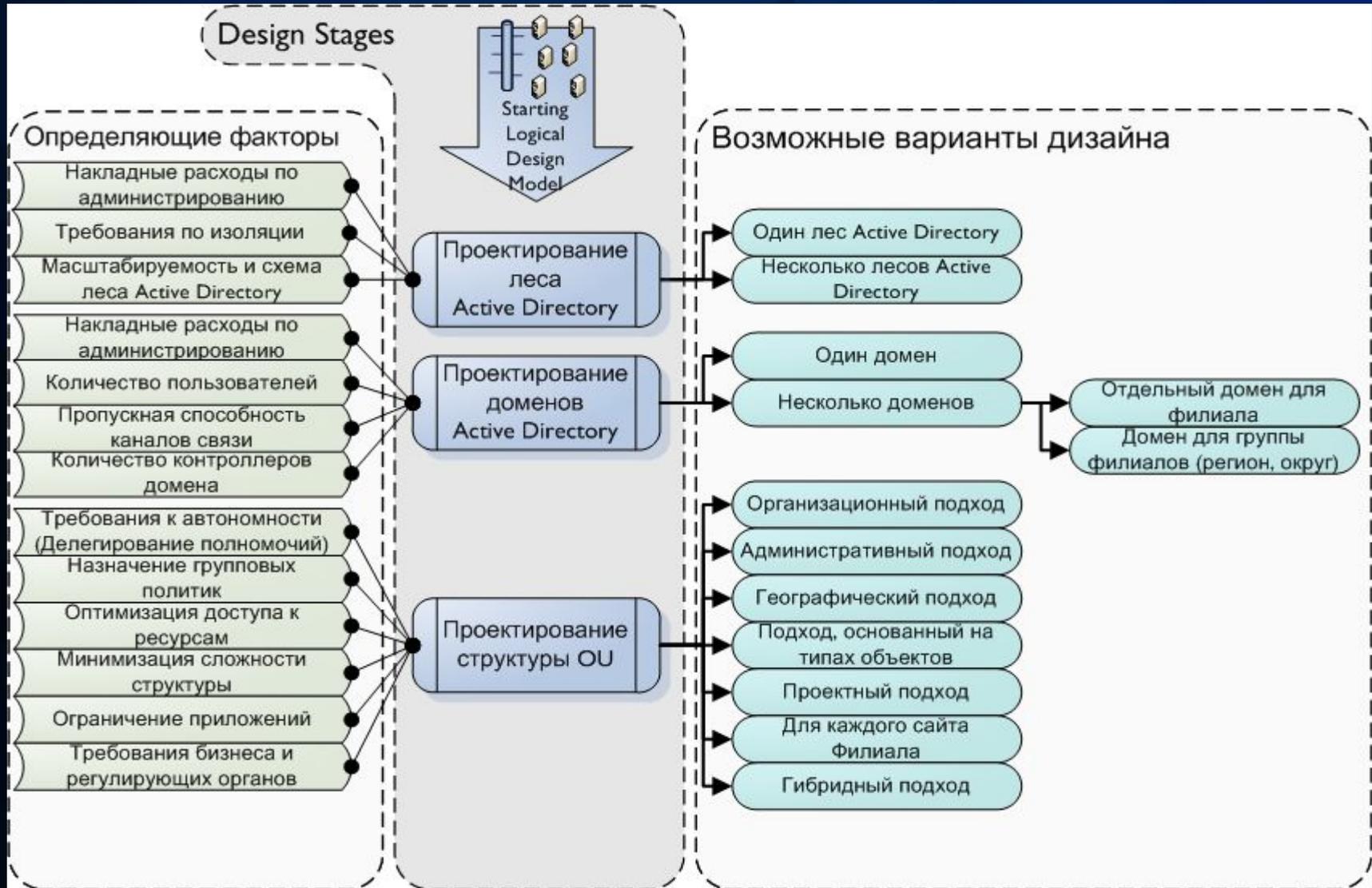
Низкие требования к пропускной способности каналов

Соответствие требованиям локального бизнеса

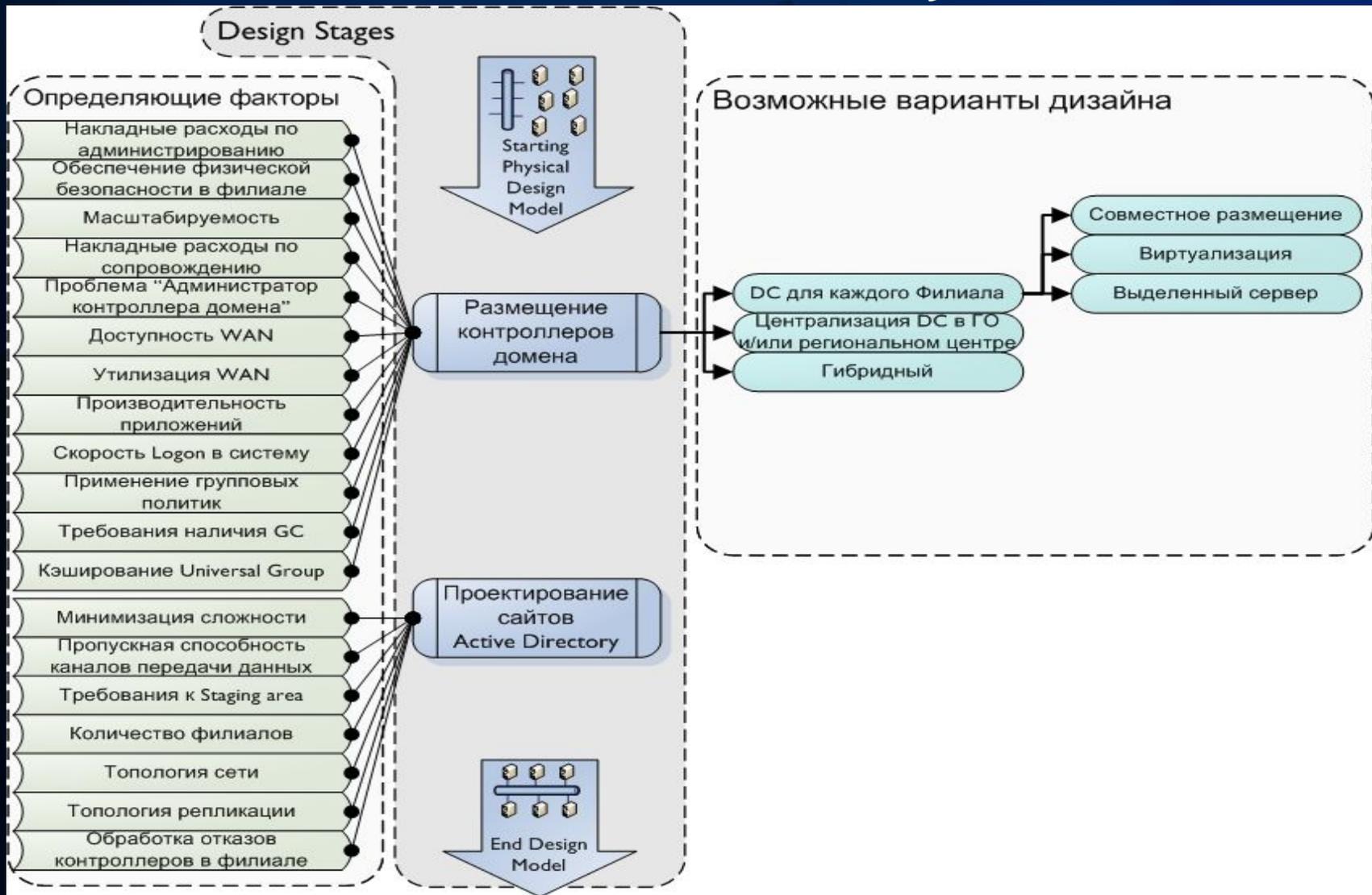
VOIS: Проектирование основных инфраструктурных сервисов

- Служба каталогов
 - Active Directory
- Сетевые службы
 - DNS
 - DHCP
 - WINS
- Файл/принт сервисы
 - DFS
 - PMS
- Сервисы управления и мониторинга
 - Обновление ПО и Patch management
 - Мониторинг и инвентаризация
 - Резервное копирование и восстановление

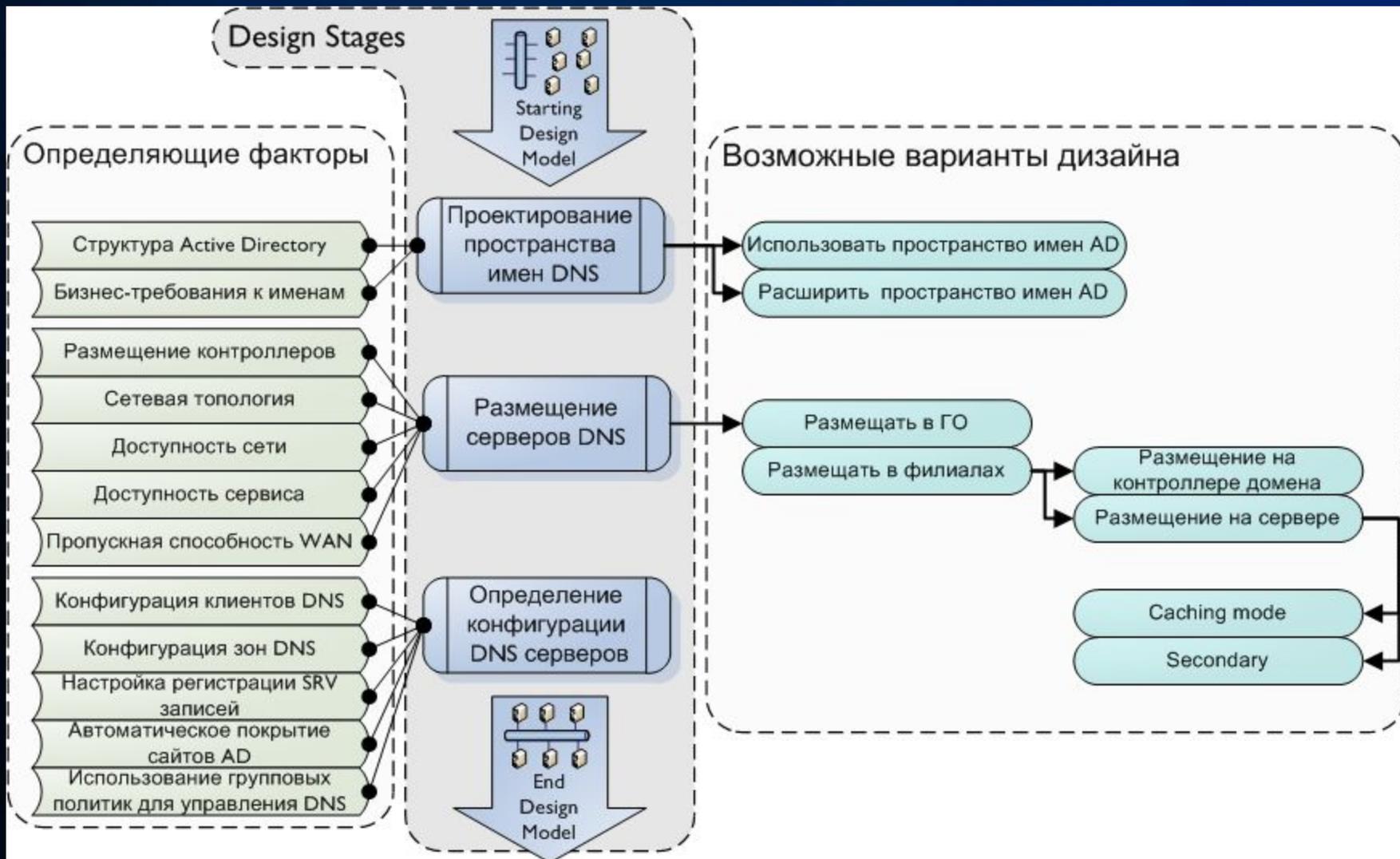
Проектирование логической топологии Active Directory



Проектирование физической топологии Active Directory



Проектирование DNS



Региональные офисы.

Физическая топология

- Топология среды передачи данных
 - Характеристики и требования к каналам связи
 - Сегментация локальной сети филиала



Single hub



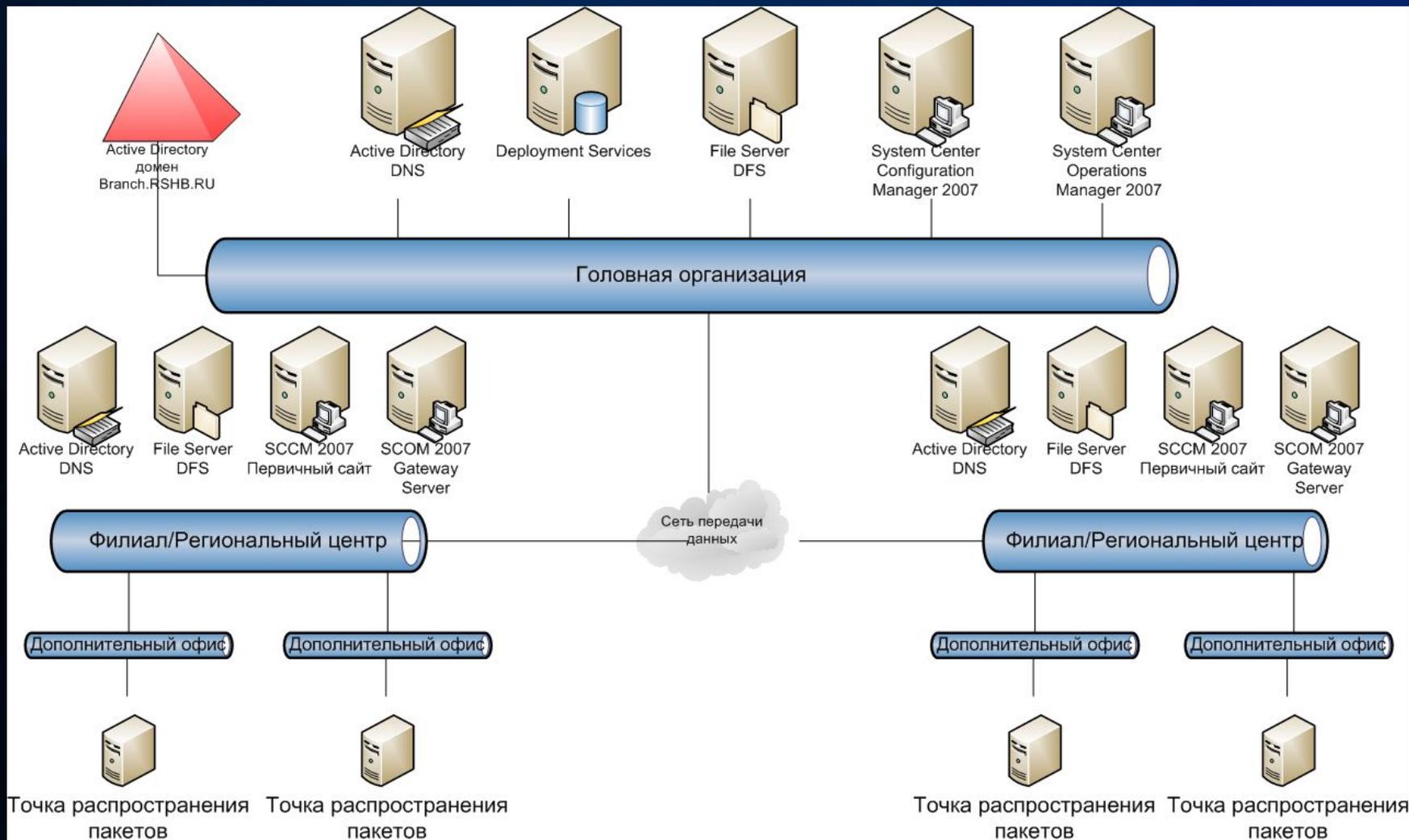
Multiple Hub

- Планирование серверов и размещение служб
 - ❖ Консолидация сервисов
 - ❖ Размещение на выделенном сервере
 - ❖ Виртуализация

VOIS: Методология построения инфраструктуры

- Методология проектирования логической и физической топологии
- Руководства по планированию инфраструктурных сервисов
- Руководства по развертыванию инфраструктурных сервисов
- Описания эксплуатационных процессов, включая мониторинг, резервное копирование и восстановление

Пример реализации VOIS v2



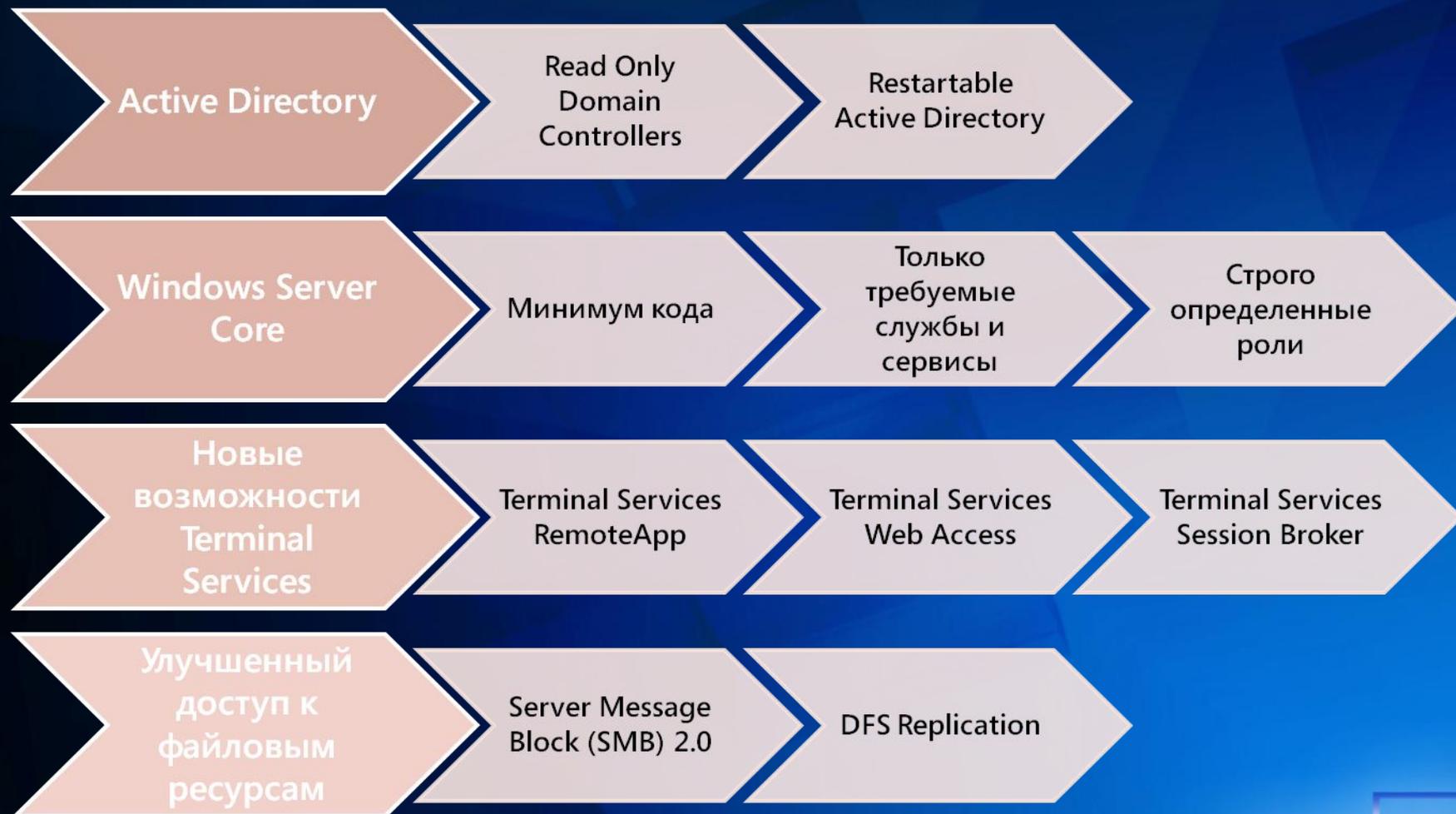
VOIS: Существующая платформа

- Windows Server 2003 R2
- Virtual Server 2005 R2
- Internet Security and Acceleration Server 2006
- System Center
 - Operations Manager 2007
 - Configuration Manager 2007
 - Data Protection Manager 2007

Особенности SCCM 2007 для предприятий с распределенной структурой

- Построение иерархии на основании административной модели, а также географического распределения
- Полностью централизованное управление с широкими возможностями делегирования полномочий
- Branch distribution point в том числе на Windows XP Pro
- Wake on LAN
- Новый модуль Remote Tools на базе RDP

Развитие платформы: возможности Windows Server 2008 для филиалов



Read Only Domain Controller

- Содержит все объекты каталога кроме “хэша” паролей учетных записей
- Доступен только для чтения
- Криптографическая изоляция: отдельный kbrtgt
- Возможность кэширования “account’s credentials”, определяемая политикой репликации паролей
- Удаление скомпрометированного RODC приведет к автоматическому сбросу паролей для кэшированных учетных записей
- Возможность делегирования полномочий локального администратора для DC

Read-only Domain Controller (RODC)

• Протиповане контролера домена

Злоумышленник:

Администратор домена

| Domain | User Name | LM Password | <8 | Password |
|--------|----------------|-------------|----|-----------|
| RODC | Administrator | | x | |
| RODC | Guest | * empty * | x | * empty * |
| RODC | krbtgt | * empty * | | |
| RODC | WMJS_HUB-DC-01 | | | |
| RODC | krbtgt_1 | * empty * | | |
| RODC | krbtgt_2 | * empty * | | |
| RODC | Test | PASSWORD1 | | Password1 |
| RODC | Test2 | PASSWORD2 | | Password2 |
| RODC | Test3 | PASSWORD3 | | Password3 |
| RODC | Test1 | PASSWORD1 | | Password1 |
| RODC | HUB-DC-01\$ | * empty * | | |
| RODC | RODC-DC-01\$ | * empty * | | |
| RODC | Administrator | * empty * | x | * empty * |
| RODC | Guest | * empty * | x | * empty * |
| RODC | krbtgt | * empty * | x | * empty * |
| RODC | WMJS_HUB-DC-01 | * empty * | x | * empty * |
| RODC | krbtgt_1 | * empty * | | |
| RODC | krbtgt_2 | * empty * | x | * empty * |
| RODC | Test | * empty * | x | * empty * |
| RODC | Test2 | * empty * | x | * empty * |
| RODC | Test3 | * empty * | x | * empty * |
| RODC | Test1 | * empty * | x | * empty * |
| RODC | HUB-DC-01\$ | * empty * | x | * empty * |
| RODC | RODC-DC-01\$ | * empty * | | |

The computer object you want to delete represents this read-only Active Directory domain controller:

RODC-DC-01

Choose how you want to delete this domain controller:

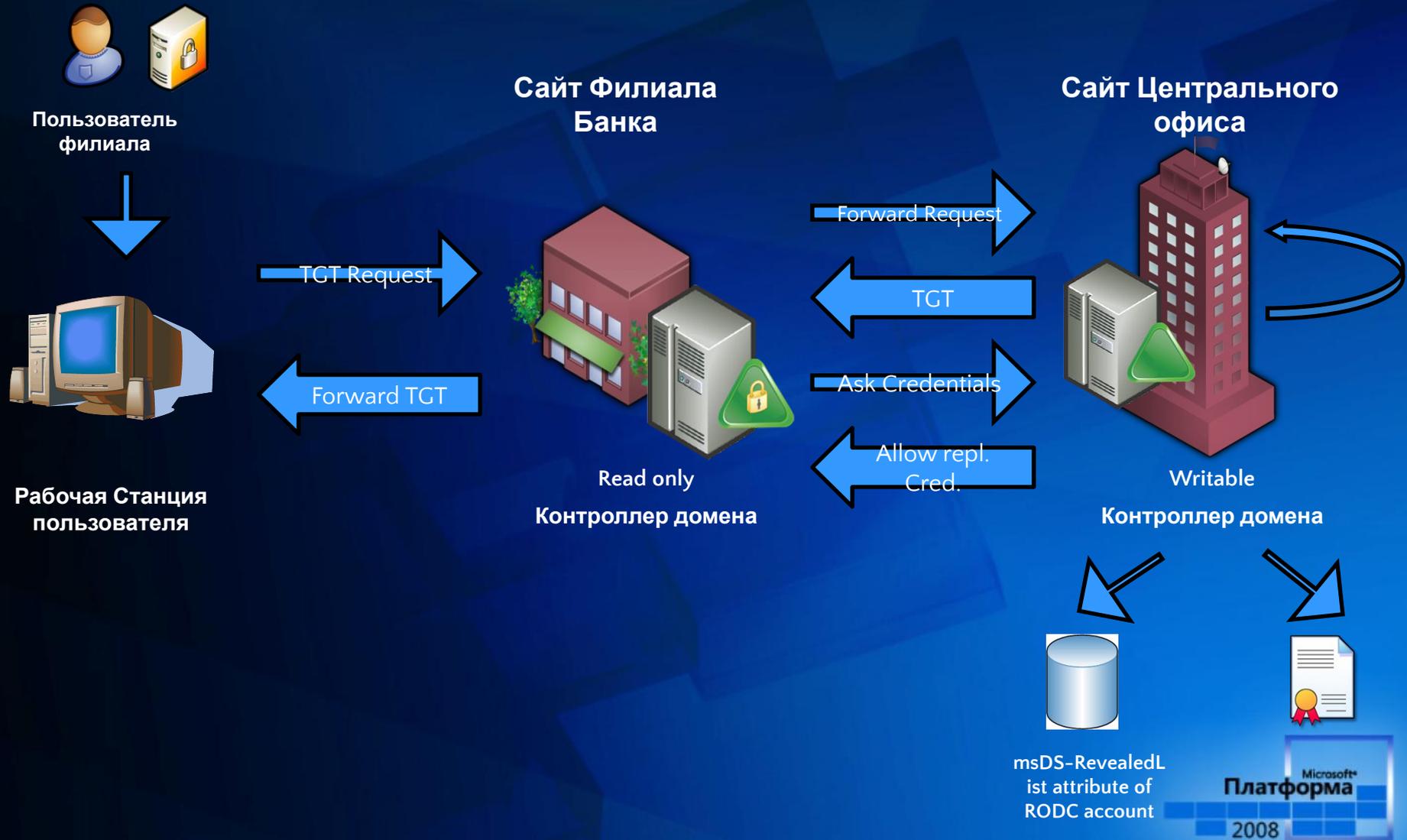
- Demote this domain controller using the Active Directory Installation Wizard (DCPROMO). This requires that the computer is online.
- This domain controller is permanently offline and can no longer be demoted using the Active Directory Installation Wizard (DCPROMO).

Reset all passwords for user accounts that were cached on this read-only domain controller. Choose this option if the read only domain controller was stolen or compromised

Export the list of accounts that were cached on this read only domain controller to this file:

Location:

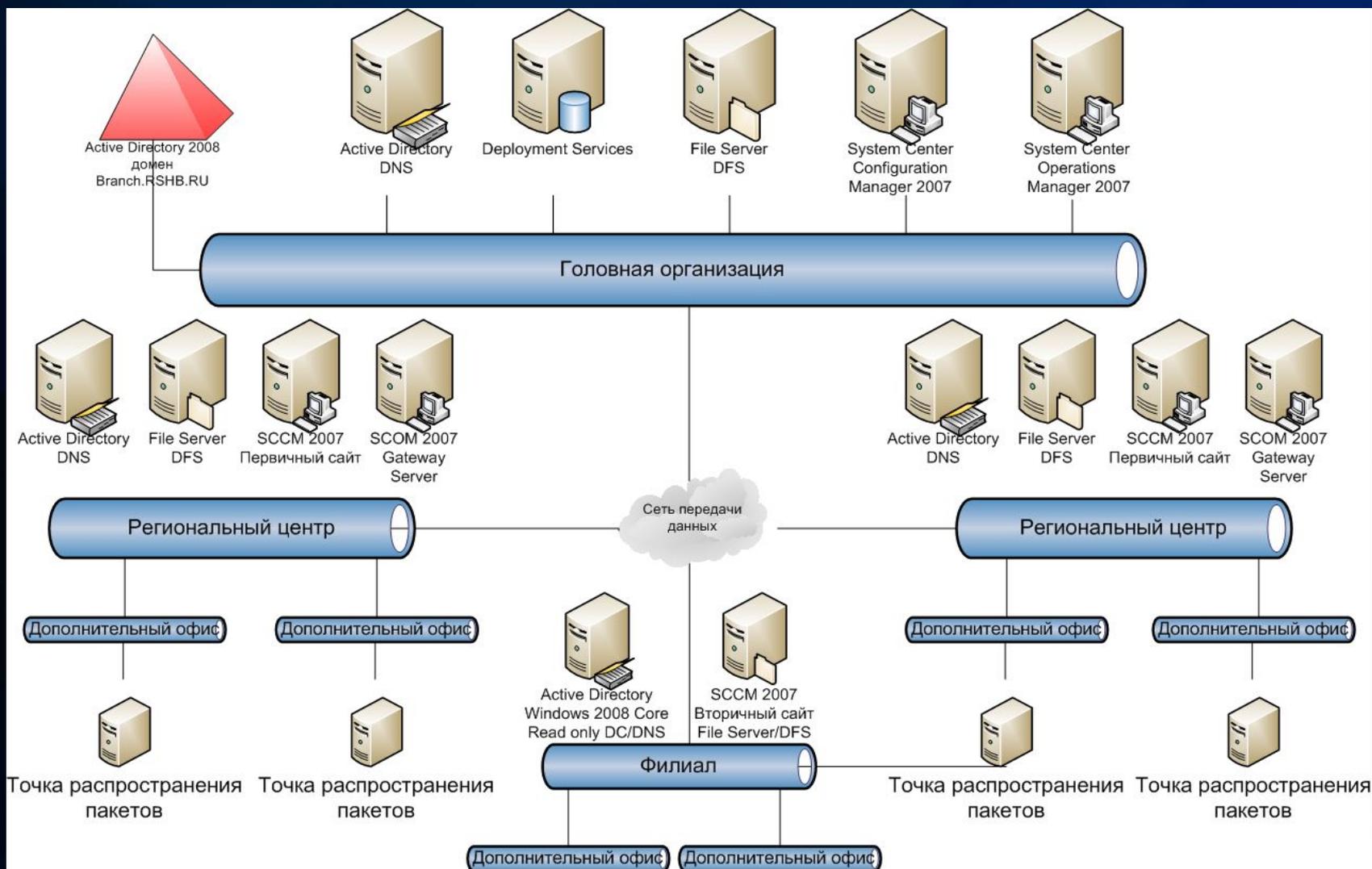
RODC Аутентификация: Запрос TGT



Windows Server 2008 Core

- Установка минимального окружения, в соответствии с заданной ролью:
 - File/Print
 - DHCP/DNS/WINS
 - Active Directory, включая AD LDS (ADAM) и read only DC
 - Failover clustering
- Интерфейс управления – командная строка
- Локальное администрирование при помощи:
 - Command prompt
 - Scripts

Пример реализации VOIS v3



Проблемы региональных офисов

Понимание процессов и условий

Мощная технологическая платформа

Методология построения решения

Мы поможем Вам построить свою
эффективную инфраструктуру

Дополнительная информация

- <http://www.microsoft.com/branchoffice>



ВОПРОСЫ?

Александр Липкин
Microsoft
alipkin@microsoft.com

Microsoft[®]

Your potential. Our passion.[™]

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.



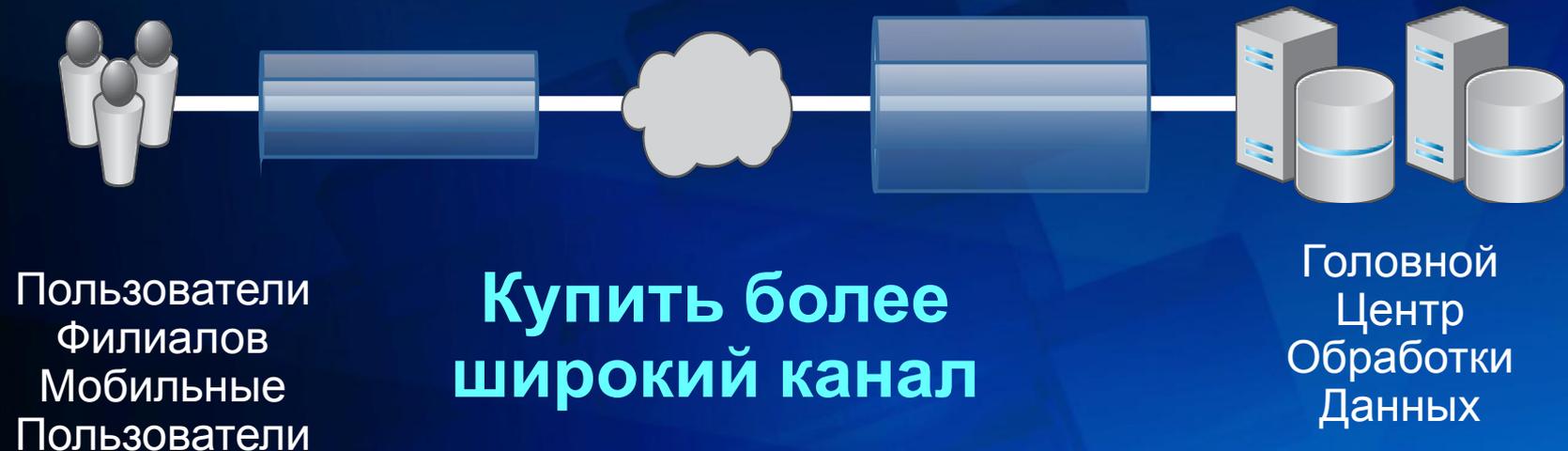


WANScaler и проект Evergreen как средство для обеспечения работы удалённого филиала.

Сергей Халяпин
Citrix Systems



Традиционный Подход



Результат

- Дорого
- Приложения по прежнему работают медленно
- Не масштабируемо

Требования к решению

- Глобальные сети должны просто РАБОТАТЬ
- Не должно требоваться никаких изменений в инфраструктуре
- Время отклика как в локальной сети..
..в не зависимости от того где Вы находитесь..

Решение – Citrix WANScaler

Используем
те же каналы



Взаимодействуем
с большим
количеством
филиалов

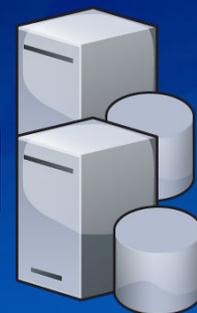


Поддерживаем
больше
пользователей



Улучшаем
производительность
мобильных пользователей

Пользователи
филиалов



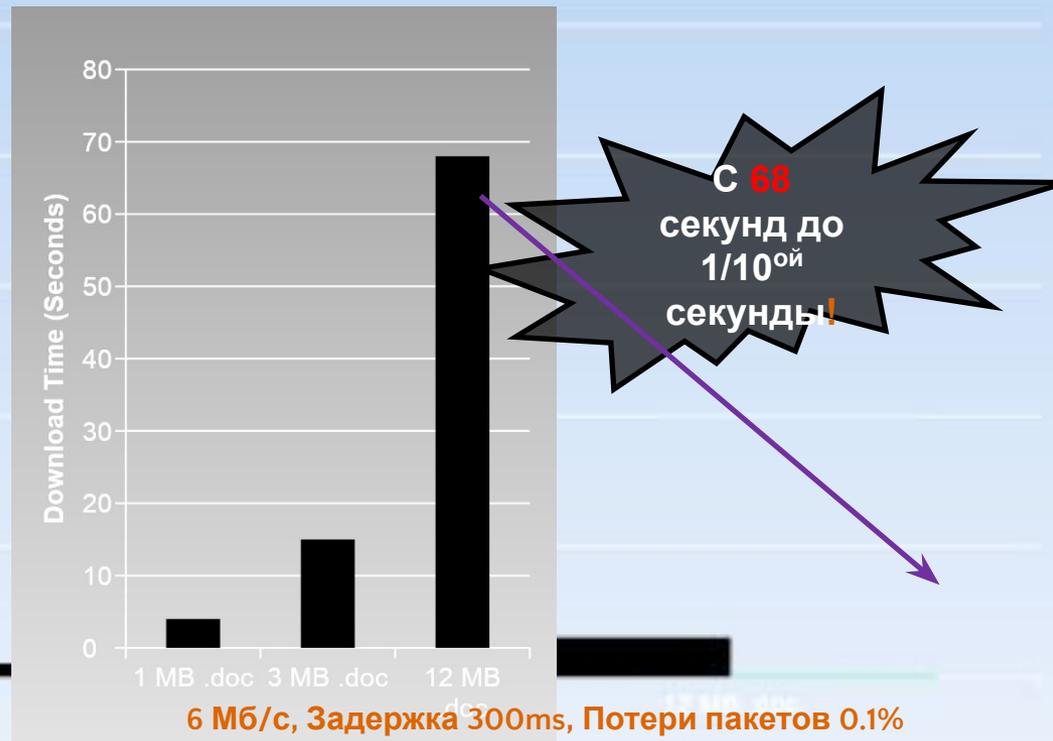
Центр
обработки
данных

Результат: ✓ Эффективно ✓ Просто
✓ Отлично Масштабируется

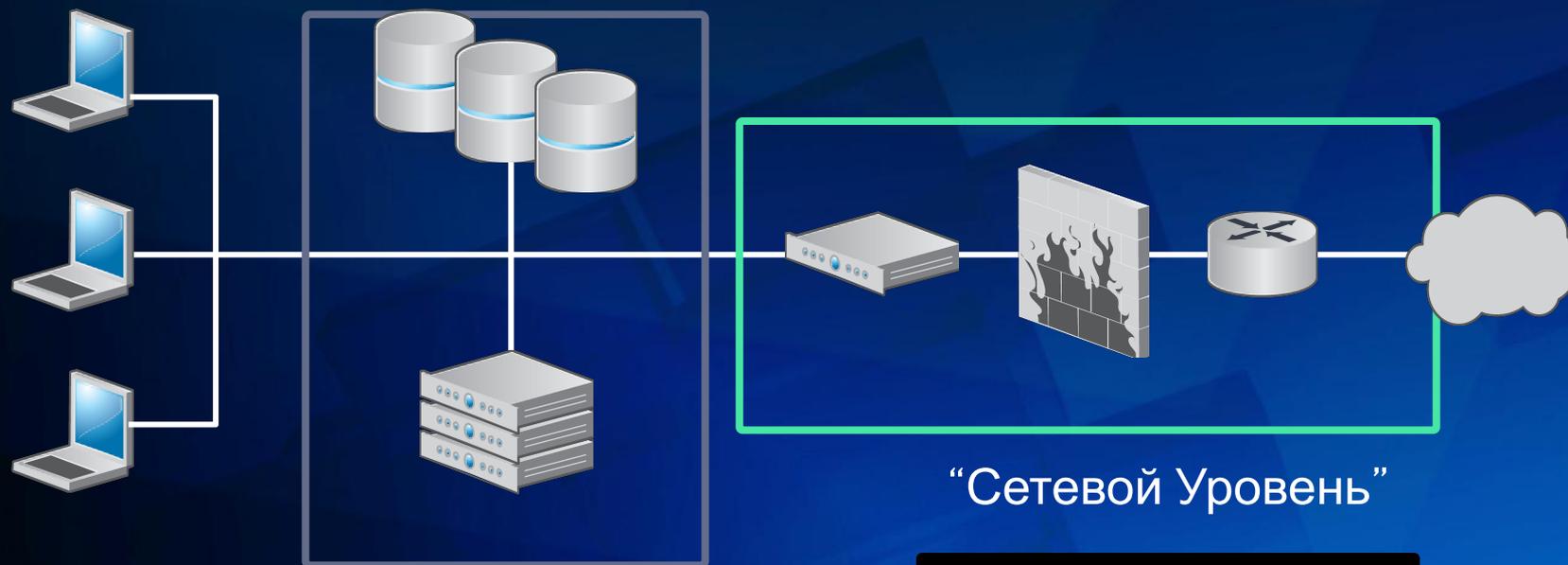
Сценарии с Большими Задержками

- Низкая пропускная способность, высокие задержки и потери пакетов, всё это вносит свой вклад в плохую производительность
- Быть “соединённым” не означает быть “производительным”
- Citrix WANScaler убирает эти барьеры за счёт управления передачей данных и оптимизацией производительности

Microsoft®



Инфраструктура Филиала



“Уровень Сервисов”

1. WAN Оптимизация
2. Сервисы Windows

“Сетевой Уровень”

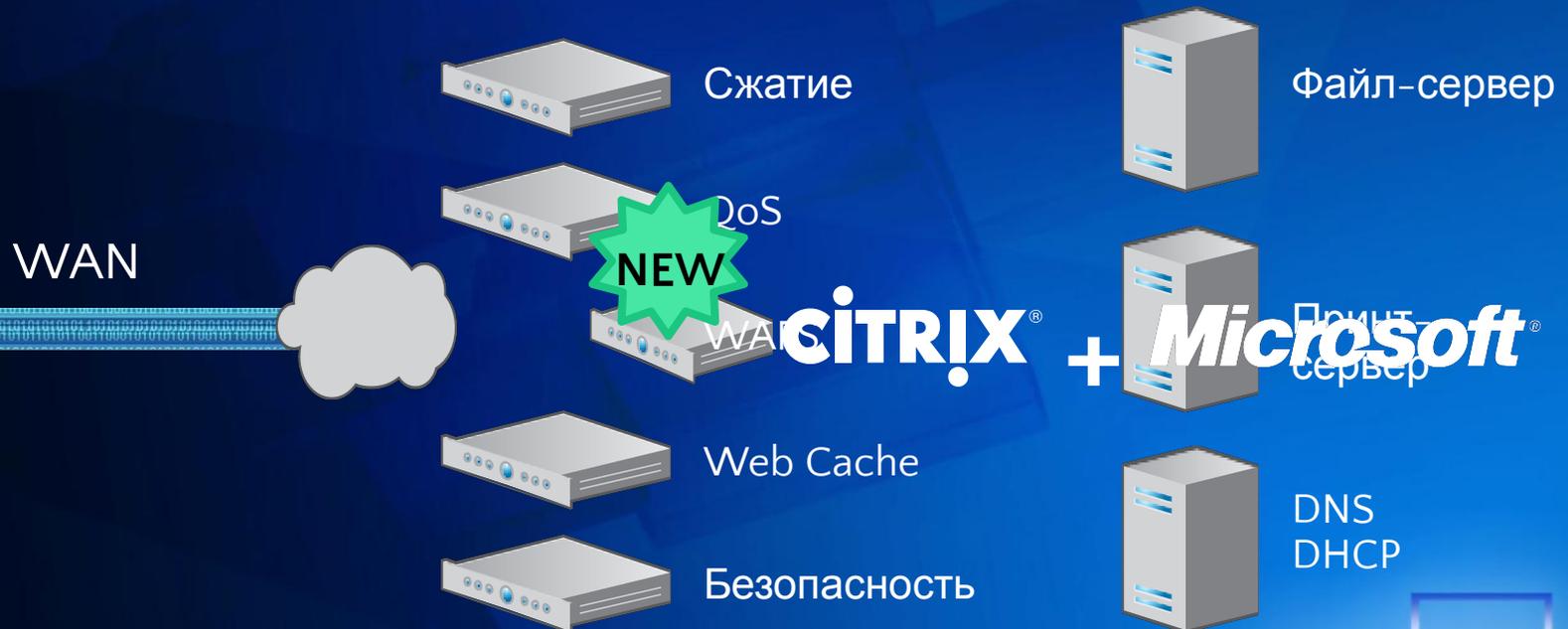
1. Маршрутизация/
Коммутация
2. Firewall/VPN/IPS

1. File/Print Службы
2. DNS/WINS/DHCP/AAA
3. Приложения Microsoft

Следующее Поколение – Evergreen

Новый тип “Офис из Коробки”

- Объединяет WAN оптимизацию и сервисы филиала
- Citrix WANScaler + Microsoft ISA Server + Windows Server 2003 R2
- Простота развёртывания plug-and-play, простота удалённого управления



Архитектура WANScaler

Ускорение протоколов

(Улучшение не эффективных протоколов)

Многоуровневое сжатие

(Сокращение передаваемых данных)

Управление потоком TCP

(Борьба с потерями/штрафами задержки)

Управление трафиком (QoS)

(Выставление приоритетов критичному трафику)

Проблемы CIFS



Автоматически Оптимизированное Ускорение CIFS



Как работает сжатие в WANScaler?

- Сжатие
 - Заменяет большие куски повторяющихся данных небольшим токеном. Токен работает как указатель
 - Используемые в WANScaler методы:
 - Сжатие, используя Дисктовую память
 - Сжатие, используя Оперативную память
- В отличие от кэширования web, WANScaler не оперирует понятиями объект или файл. Он работает только с битовым потоком TCP соединения.
- При заполнении истории, автоматически очищается память по принципу FIFO.

Стандартное управление потоком TCP

Ethernet LAN, 10Mb/s, маленькие задержки и потери

Performance (Mbs)



1 TCP Slow Start – скорость передачи пакетов увеличивается после каждого подтверждения.

2 TCP Congestion Control – Штраф за потерю пакета = скорость передачи снижается на 50%.

X = Потеря пакета

ТСР в глобальных сетях (WAN)

T3, 45Mb/s, высокие задержки и потери

Performance (Mbs)

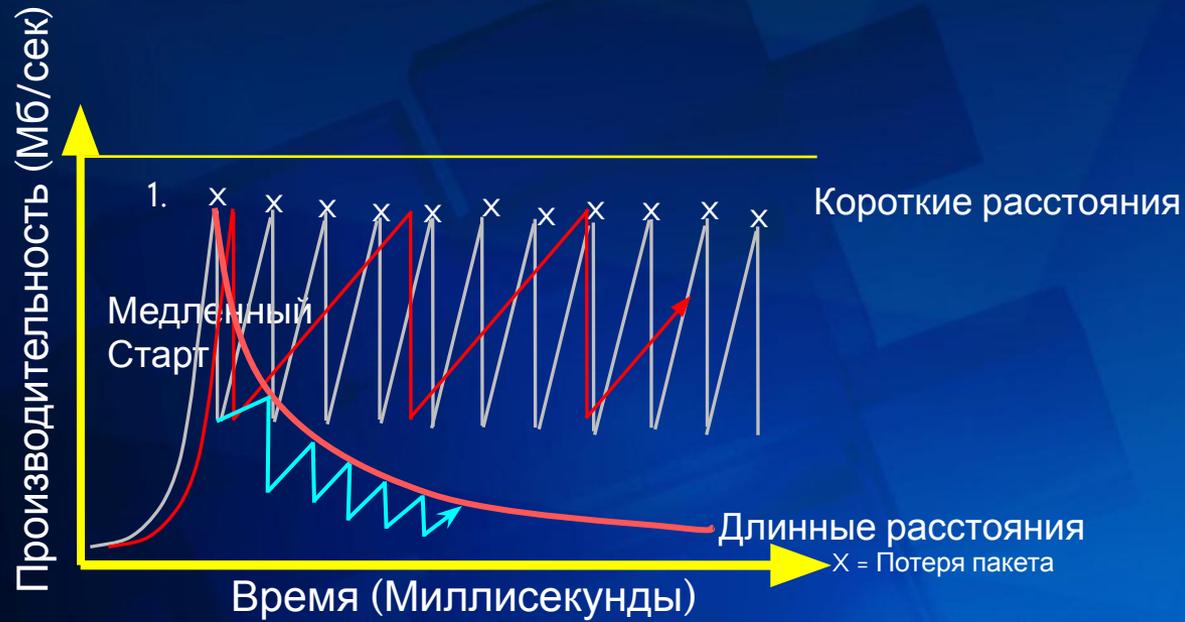


X = Потеря пакета

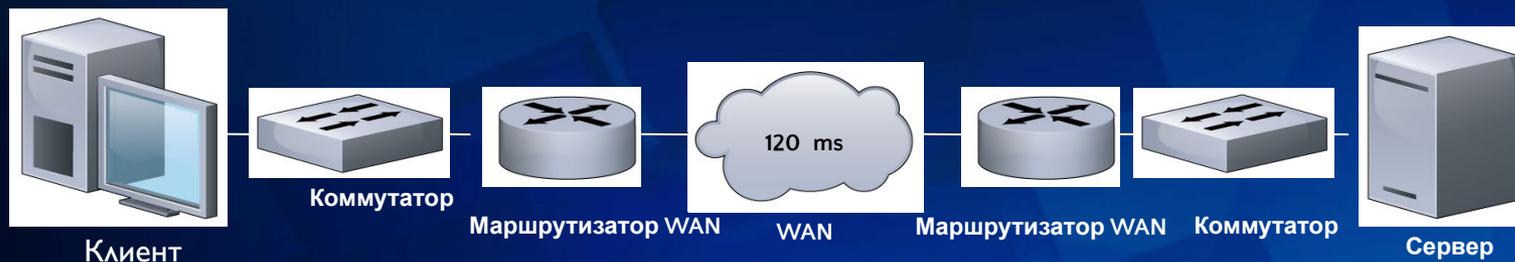
1
Высокие задержки означают более медленный период восстановления после потери пакета.

2
Потеря пакетов очень нерегулярна и временами сомнительна, чтобы быть предсказуемой.

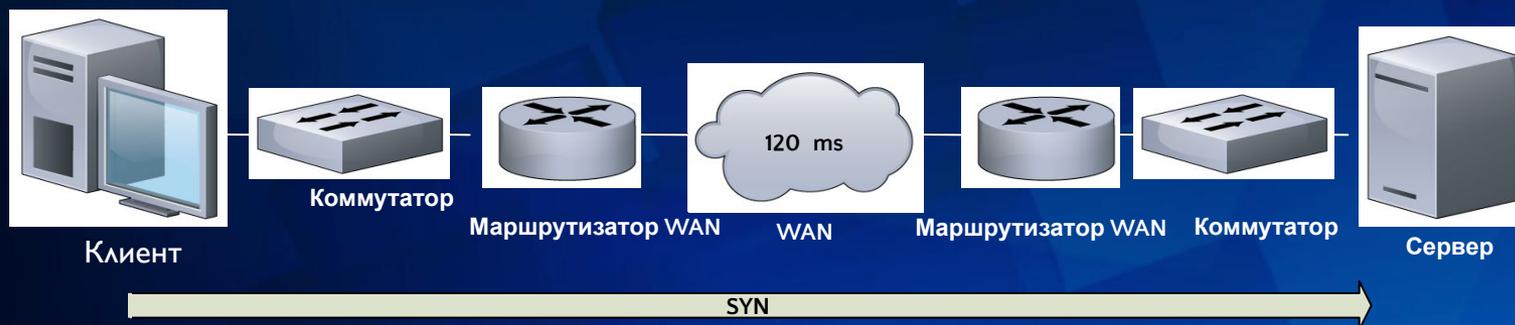
ТСР в глобальных сетях (WAN)



Стандартное управление ТСР ПОТОКОМ В WAN



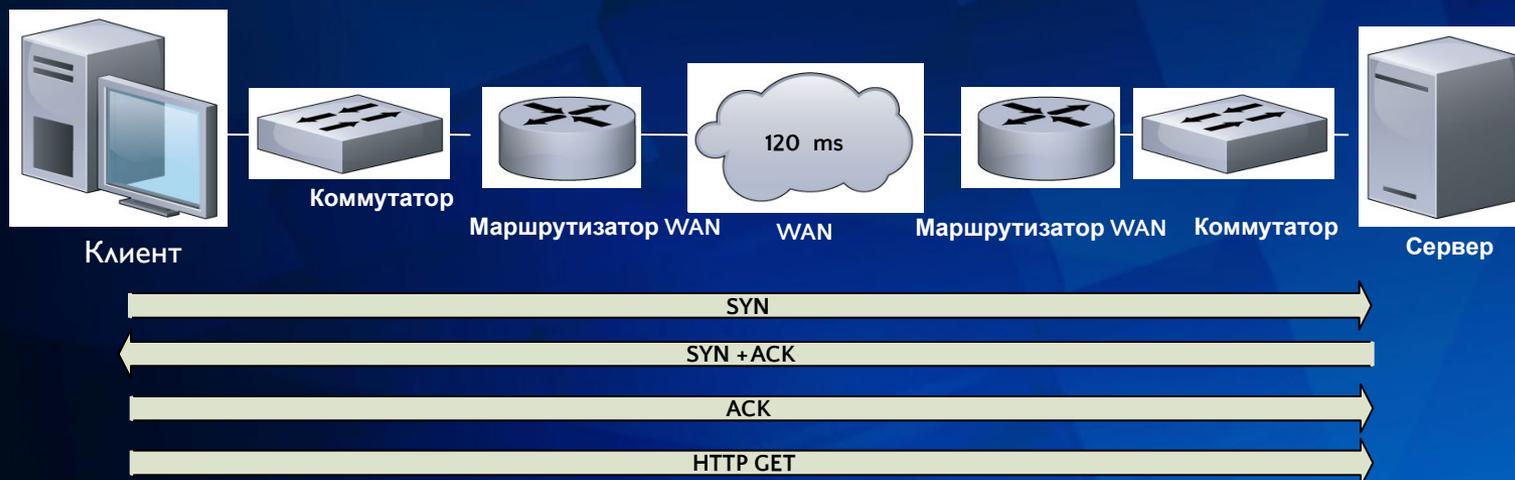
Стандартное управление ТСР ПОТОКОМ В WAN



Стандартное управление ТСР ПОТОКОМ В WAN



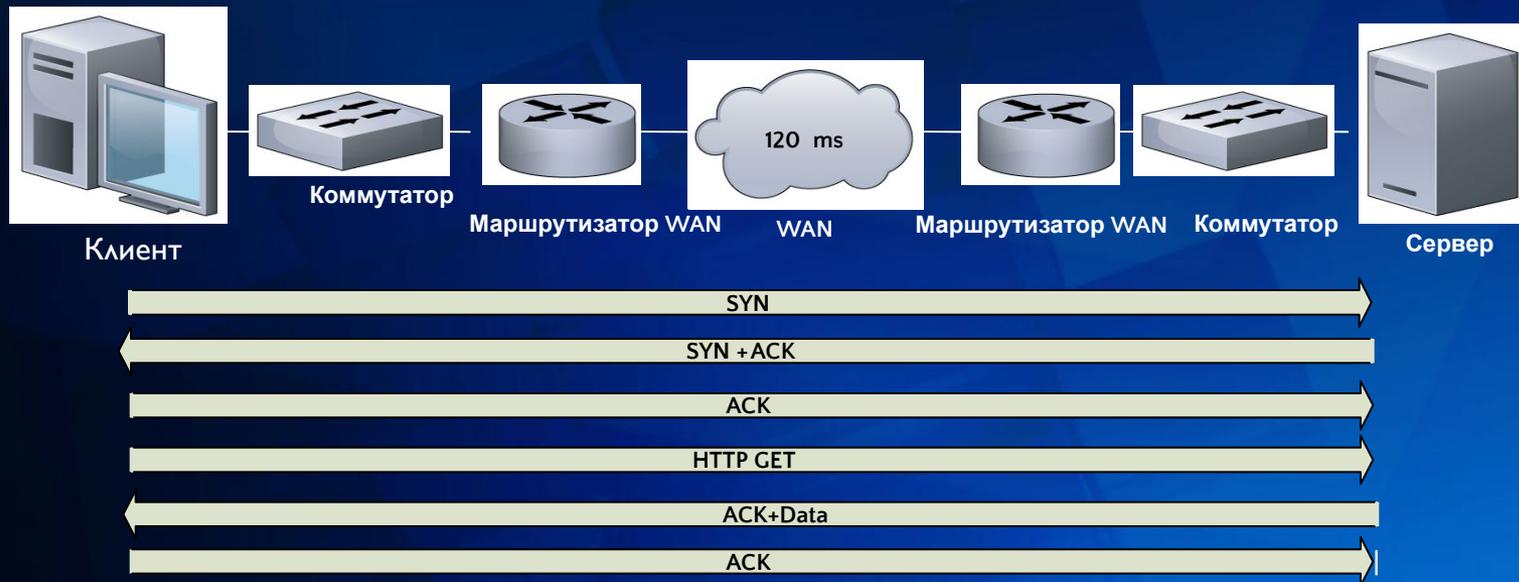
Стандартное управление ТСР ПОТОКОМ В WAN



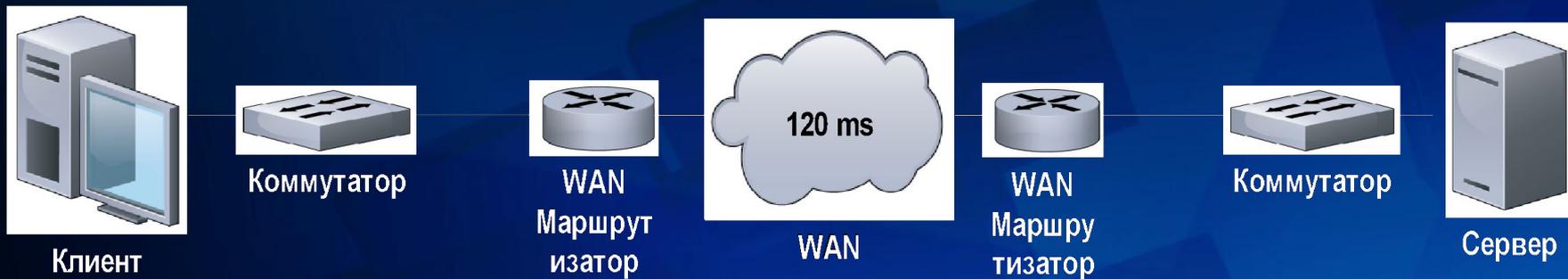
Стандартное управление ТСР ПОТОКОМ В WAN



Стандартное управление ТСР ПОТОКОМ В WAN



Управление TCP потоком WANScaler



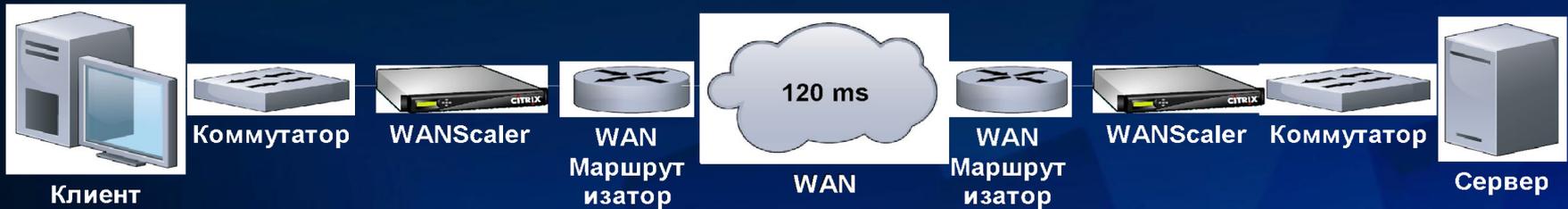
Управление TCP потоком WANScaler



Управление TCP потоком WANScaler



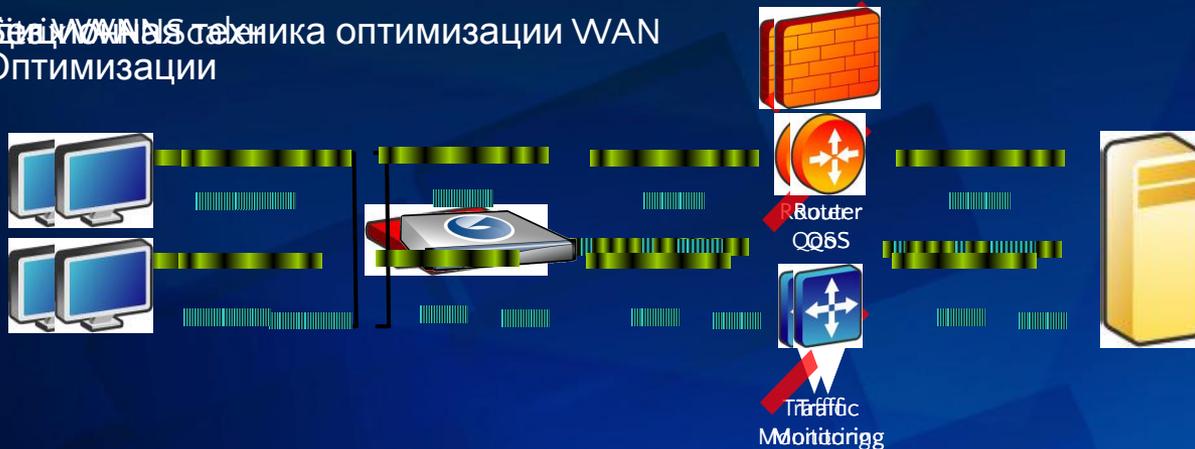
Управление TCP потоком WANScaler



- Каждый Сегмент имеет своё управление ПОТОКОМ:
 - Обычный размер окна TCP максимум 64Кб.
 - На стороне WAN, WANScaler увеличивает окно до 8Мб (RFC 1323)
 - WANScaler отправляет подтверждения на стороне LAN, таким образом сервер продолжает передачу
- В сегменте WAN всегда происходит передача данных с определённой скоростью. Нет передачи быстрее, чем настроенная скорость канала.

Сетевая Прозрачность

Трафик WAN-сетей
Оптимизации



- Оптимизация трафика TCP не изменяет заголовков пакетов.
 - Заголовки IP и TCP остаются не тронутыми
- Не требуется перенастройки приложений или клиентской части
 - Например шлюзы и настройки прокси не изменяются
- Существующее сетевое оборудование НЕ затрагивается
 - Например – файерволы, маршрутизаторы с QoS, и средства сетевого мониторинга

QoS – Как это работает

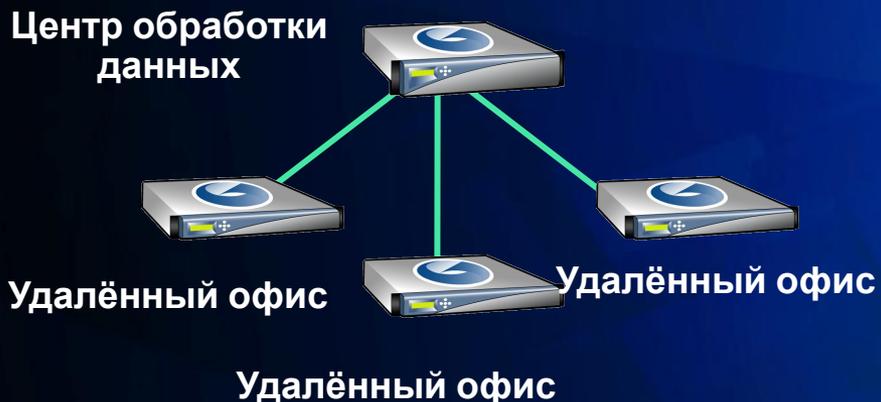
- Цель: Полностью заполнить канал
 - QoS наводит порядок в трафике, заполняющим канал
- Существует Пять классов трафика (От “А” до “Е”. Имена можно изменить)
- Каждой очереди может быть назначен процент трафика
 - Если трафика не достаточно до заявленного процентного соотношения, может использоваться другой трафик, таким образом WANScaler всегда будет заполнять канал
- Каждый очереди может быть назначен Класс
- Доступны отчёты специфичные для очередей

Варианты внедрения WANScaler

Точка – Точка



Звезда



Смешанный



Дополнительная информация

- <http://www.citrix.com/wanscaler/>
- <http://www.citrix.com/mycitrix/>
- <http://www.citrix.ru>
- <http://www.citrixnews.ru>
- <http://www.citrixeducation.com>
- <http://citrixcommunity.com>



ВОПРОСЫ?

Сергей Халяпин

Citrix Systems

sergey.khalyapin@eu.citrix.com

CITRIX[®]

Microsoft[®]

Your potential. Our passion.[™]

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

