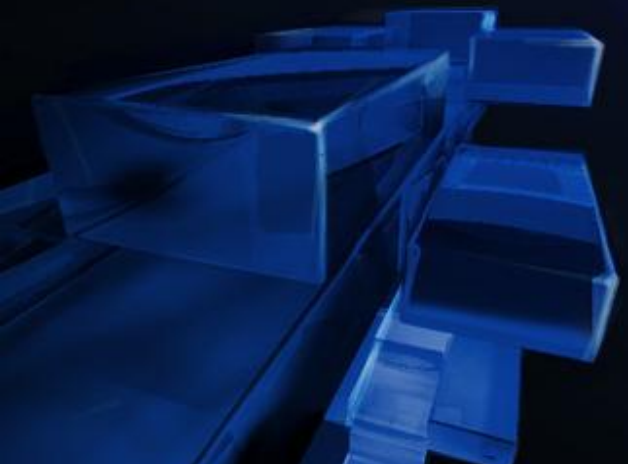
Microsoft Платформа 2008

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

Microsoft Платформа 2008

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

BOIS. История развития

- BOIS v.1 – май 2005
  - Построен на основе и как часть WSSRA
  - Windows Server 2003, SMS, MOM
  - Архитектура “Single Server”
- BOIS v.2 – февраль 2006
  - Фокус на архитектуре и проектировании распределенных сервисов.
  - Windows Server 2003 R2
  - Новые руководства по проектированию, включая DFS, PMC, VPN
- BOIS 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

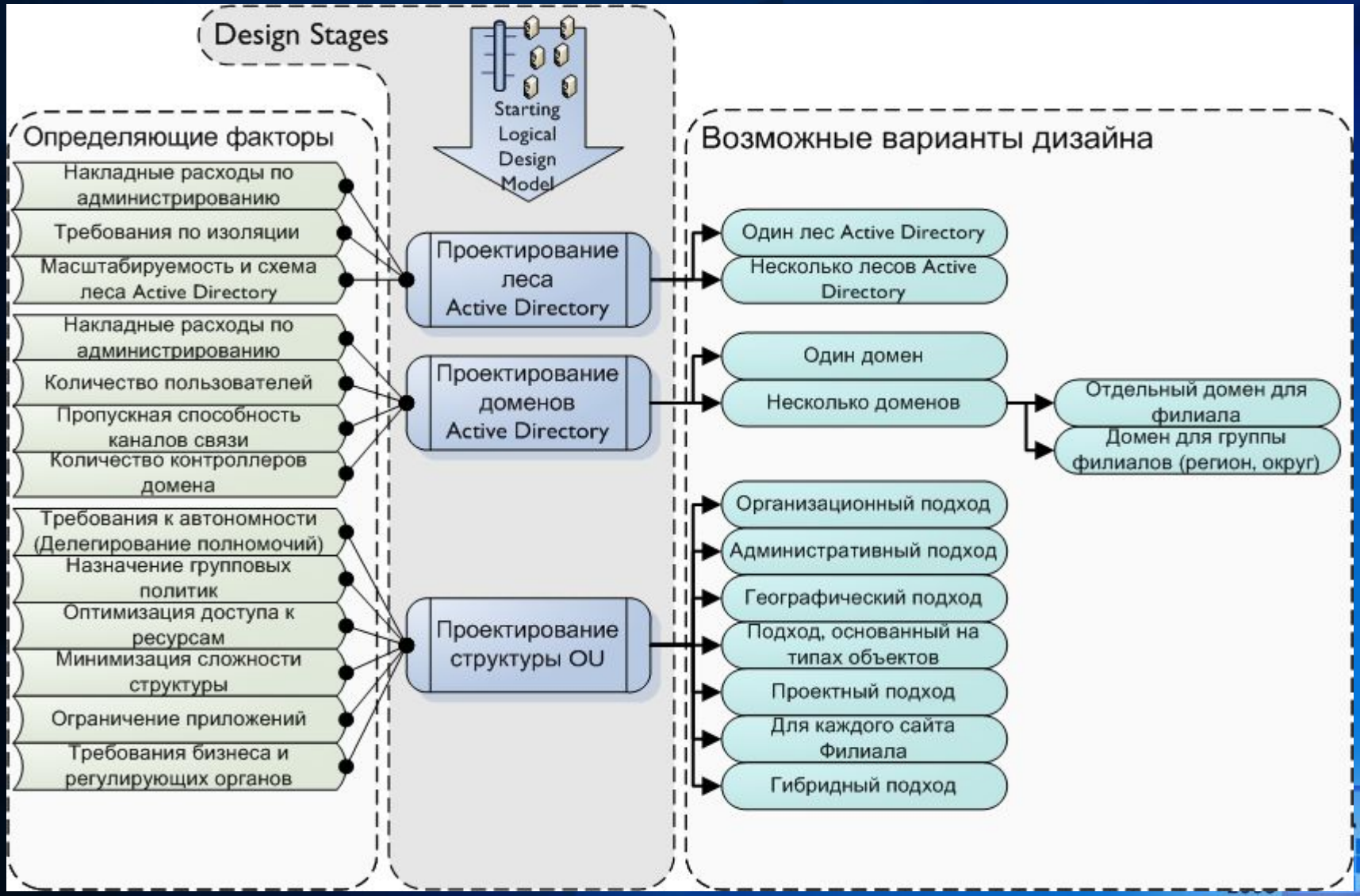
Преимущества распределенной модели

- 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

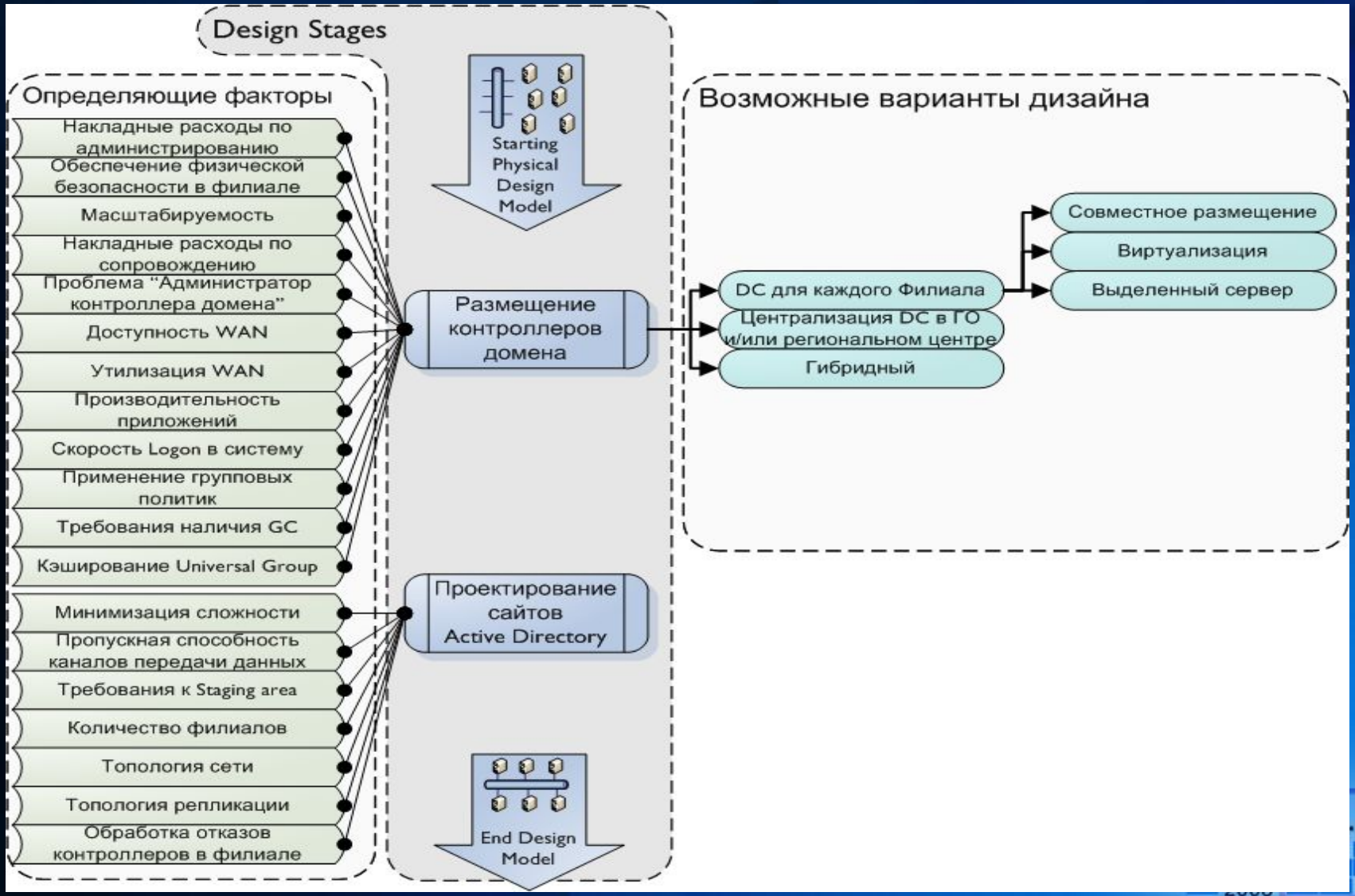
BOIS: Проектирование основных инфраструктурных сервисов

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

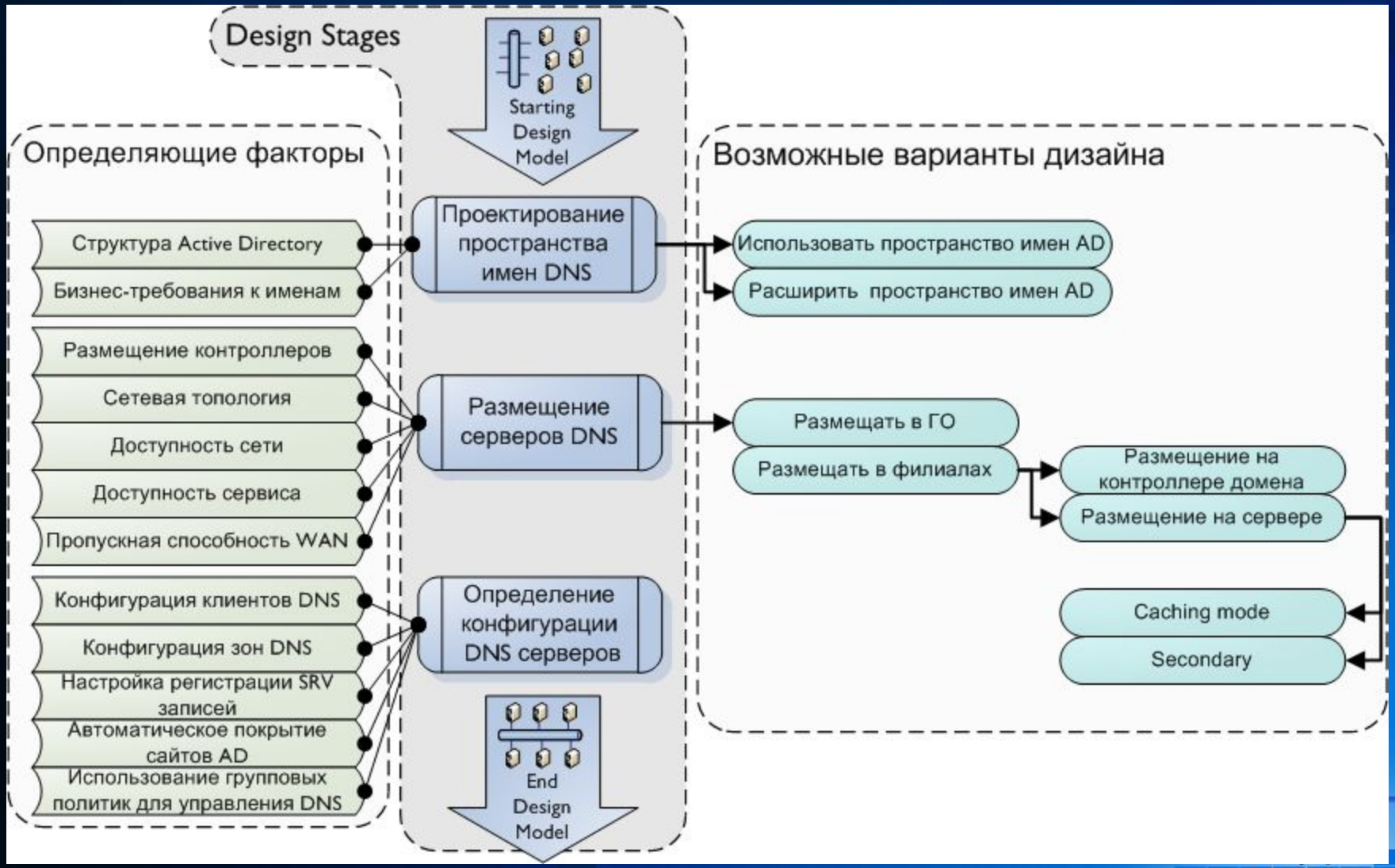
Проектирование логической топологии Active Directory



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

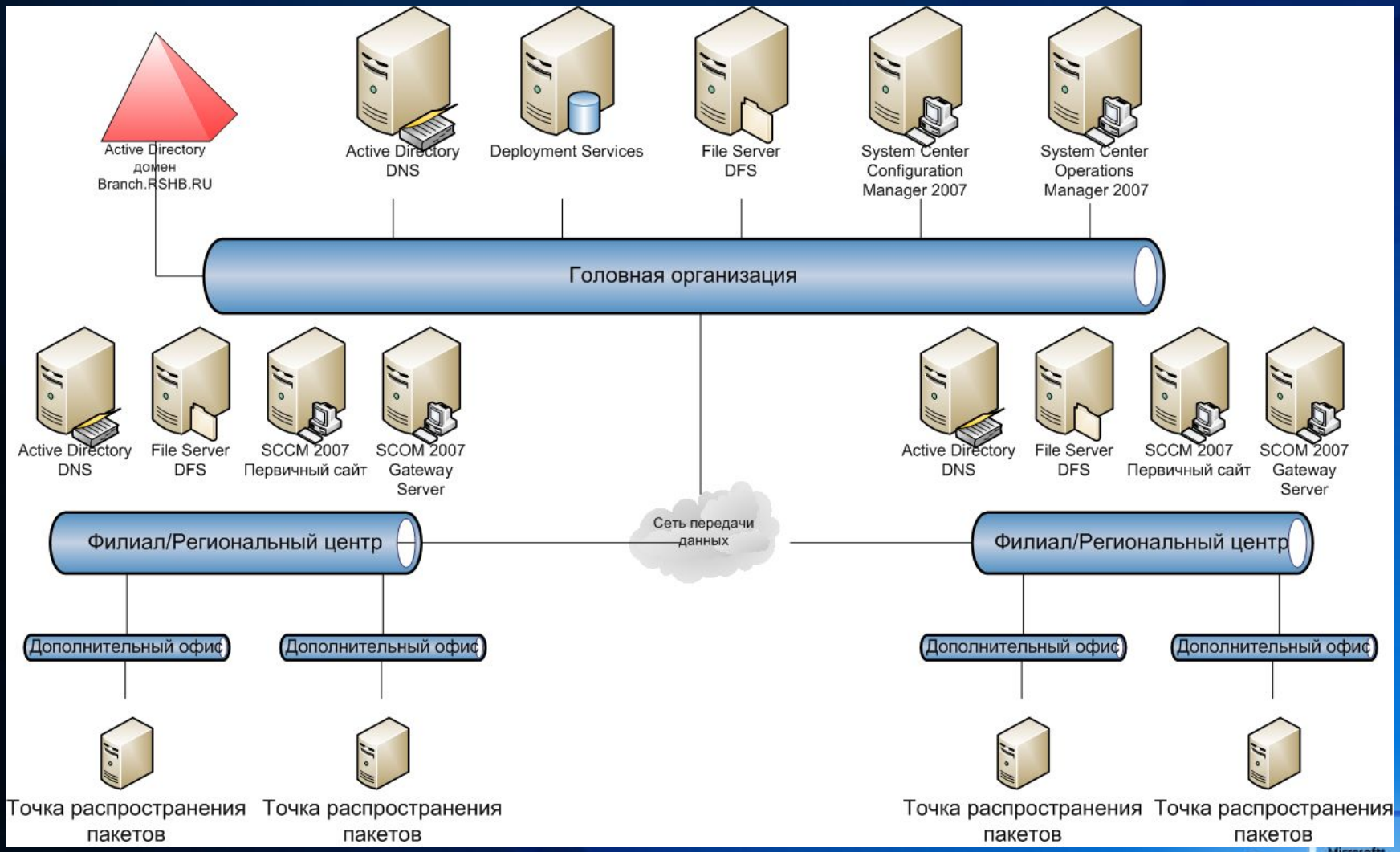
Multiple Hub

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

BOIS: 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 BOIS v2



Microsoft Платформа 2008

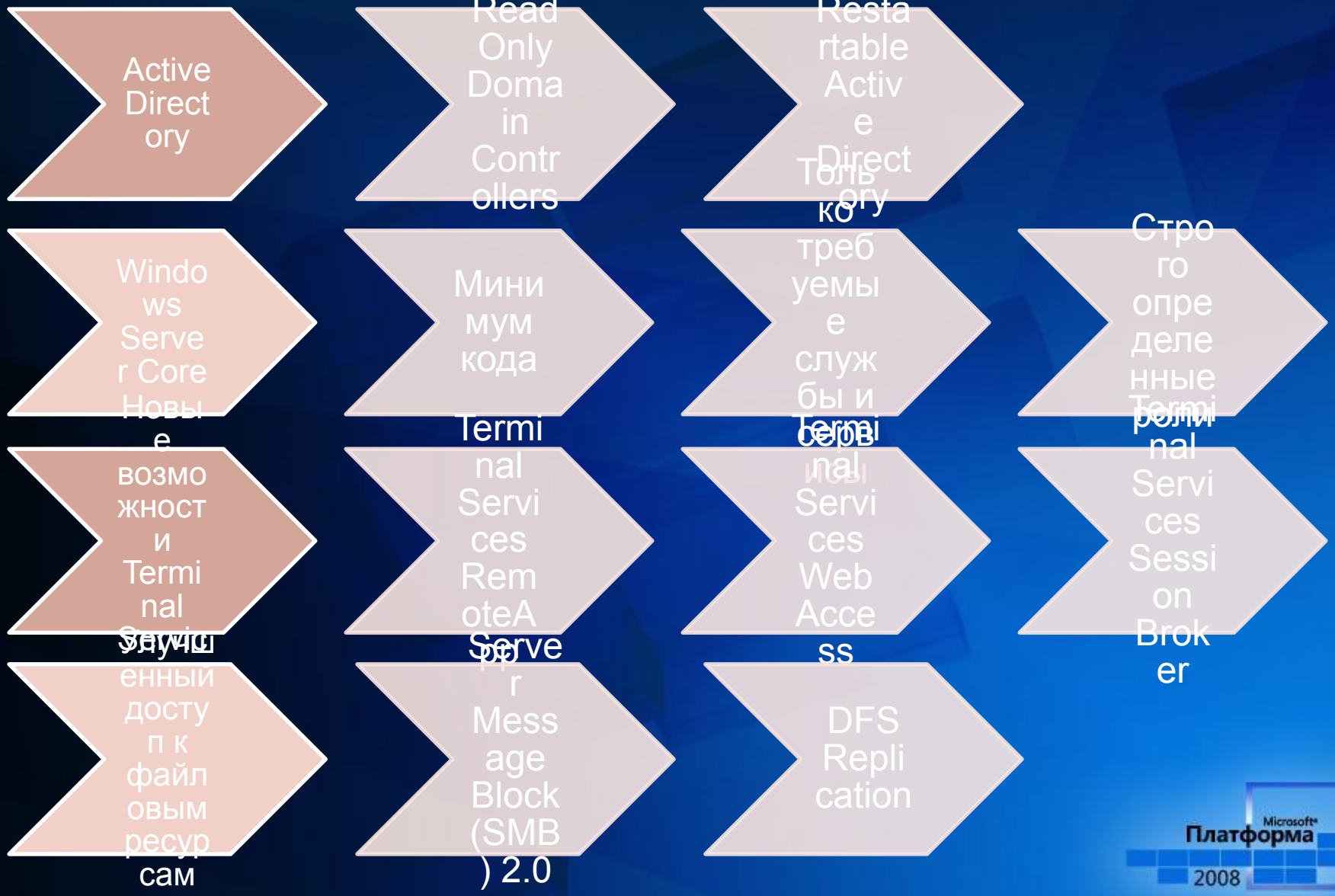
BOIS: Существующая платформа

- 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



Платформа 2008

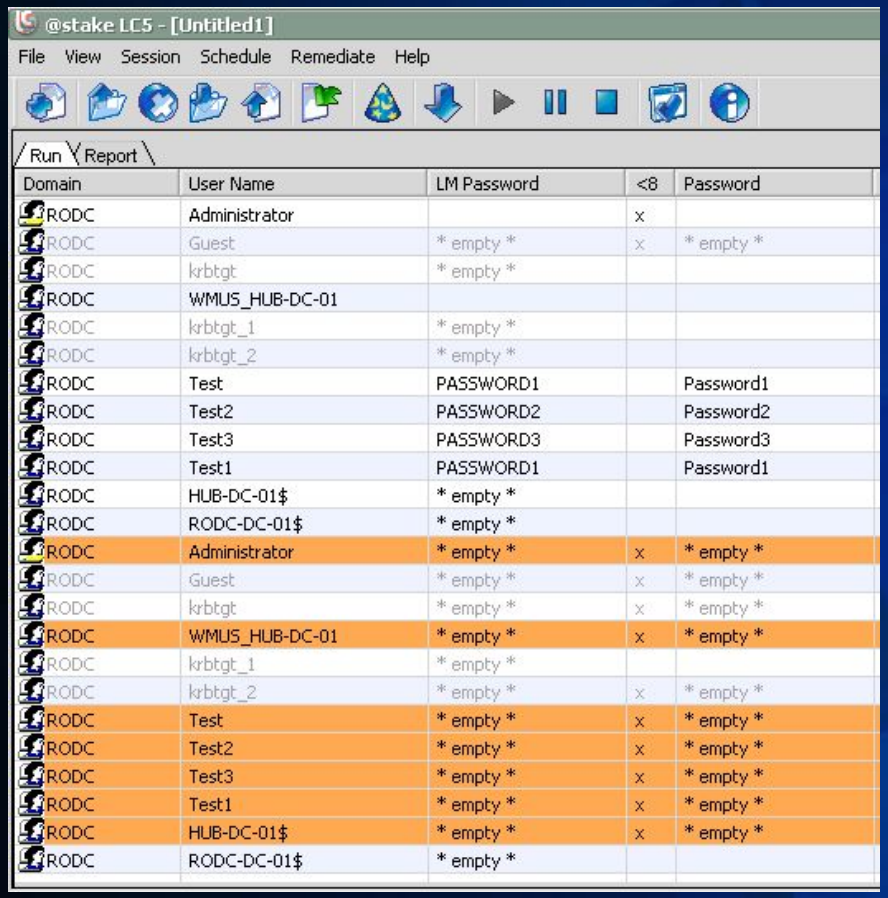
Read Only Domain Controller

- 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)

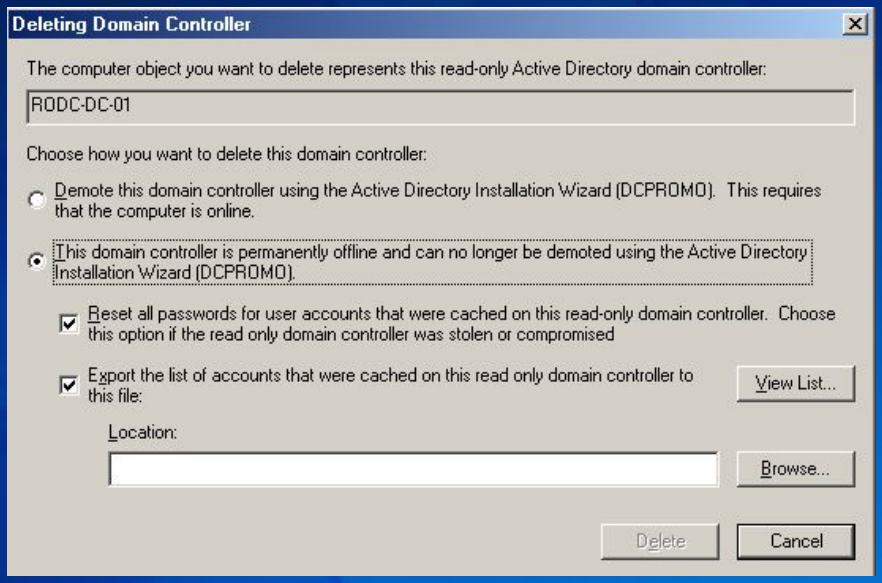
- Противостояние угрозам
  - Похищение контроллера домена

Злоумышленник:

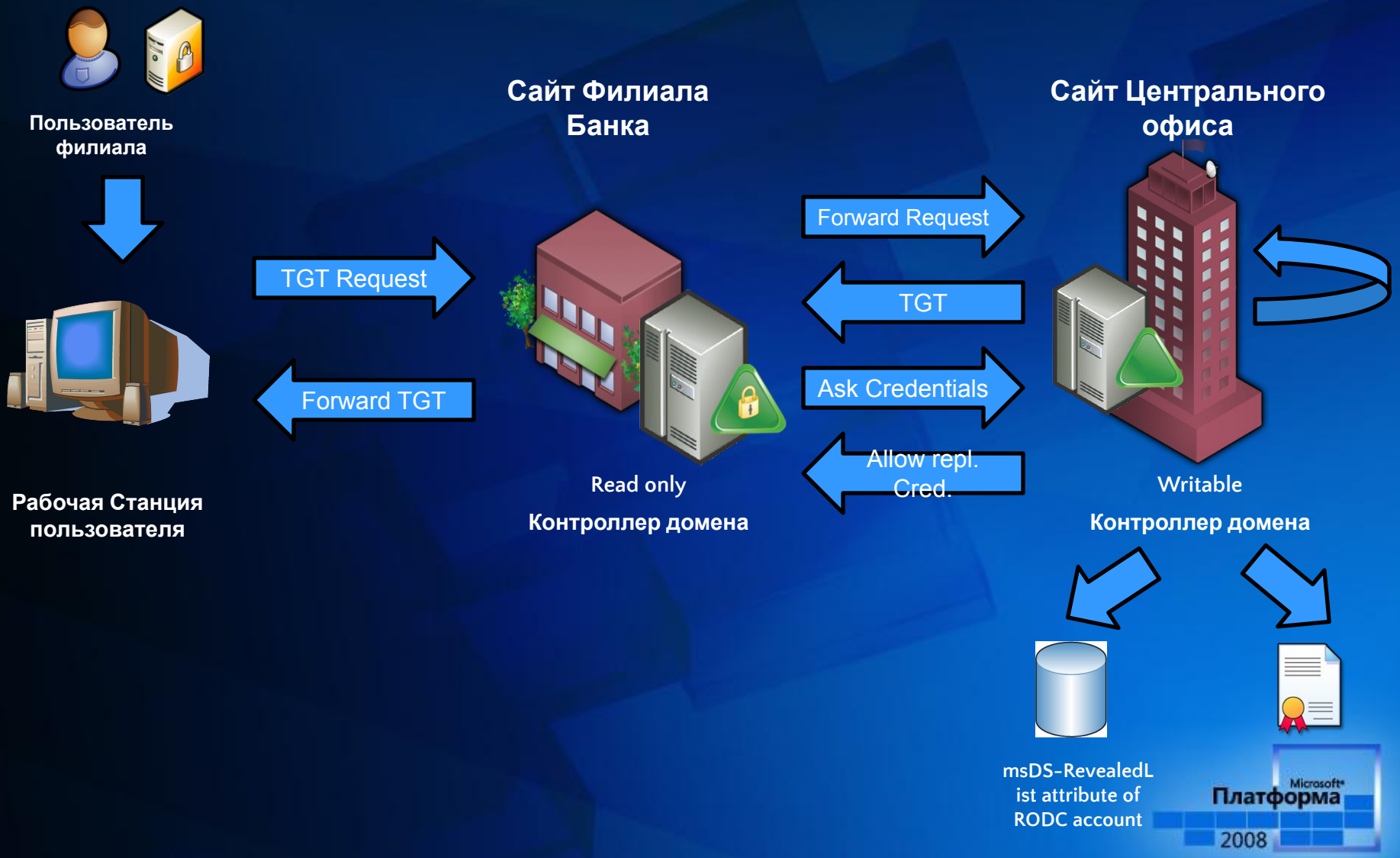


Domain	User Name	LM Password	<8	Password
RODC	Administrator		x	
RODC	Guest	* empty *	x	* empty *
RODC	krbtgt	* empty *		
RODC	WMUS_HUB-DC-01			
RODC	krbtgt_1	* empty *		
RODC	krbtgt_2	* empty *		
RODC	Test	PASSWORD1		Password1
RODC	Test2	PASSWORD2		Password2
RODC	Test3	PASSWORD3		Password3
RODC	Test1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

Администратор домена



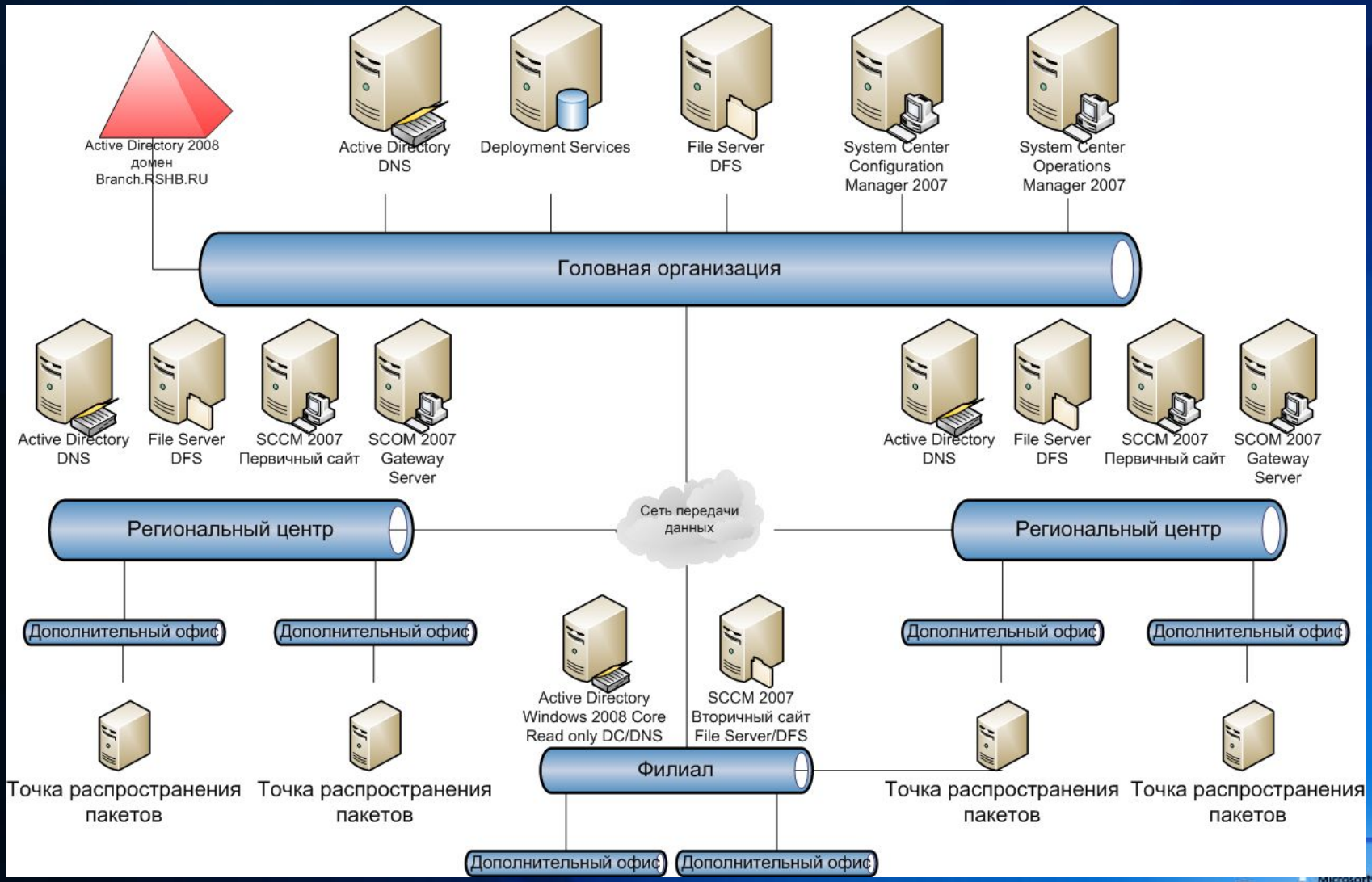
RODC Аутентификация: Запрос TGT



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 BOIS v3



Платформа 2008

Проблемы региональных офисов

Понимание процессов и условий

Мощная технологическая платформа

Методология построения решения

Мы поможем Вам построить свою эффективную инфраструктуру

Дополнительная информация

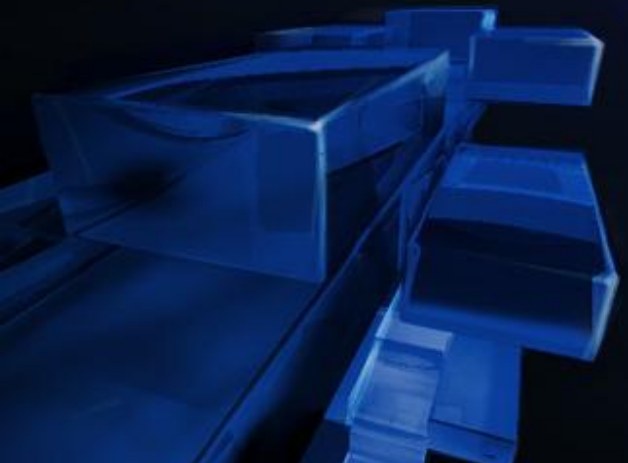
- http://www.microsoft.com/branchoffice

Microsoft Платформа 2008

Microsoft Платформа 2008

ВОПРОСЫ?

Александр Липкин
Microsoft
alipkin@microsoft.com



Microsoft®

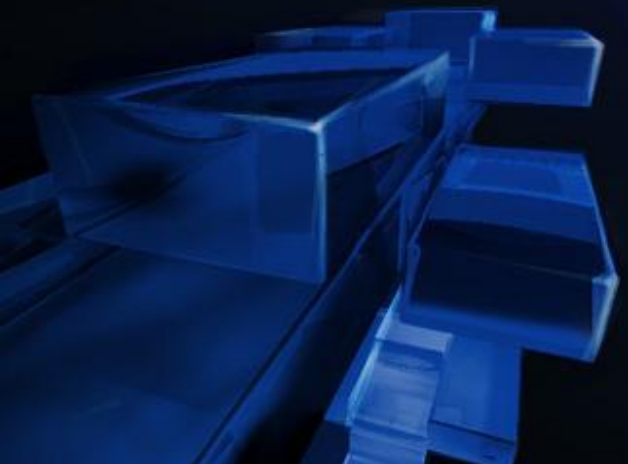
Your potential. Our passion.™

Microsoft Платформа 2008

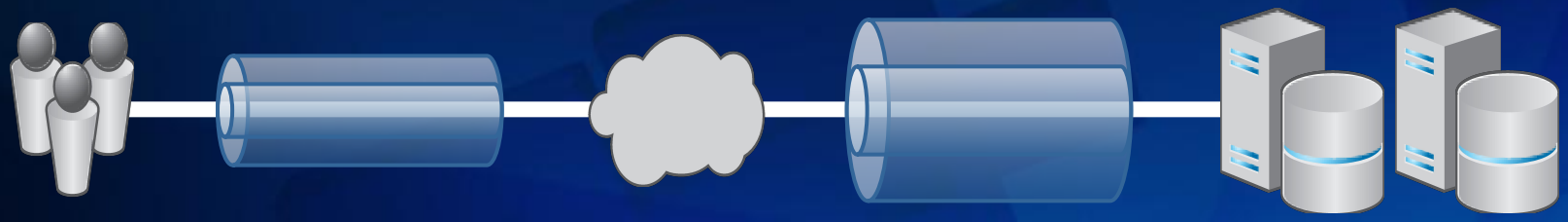
Microsoft Платформа 2008

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

Сергей Халяпин
Citrix Systems



Традиционный Подход



Пользователи Филиалов
Мобильные Пользователи

Купить более широкий канал

Головной Центр Обработки Данных

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

Пользователи филиалов

Улучшаем производительность мобильных пользователей

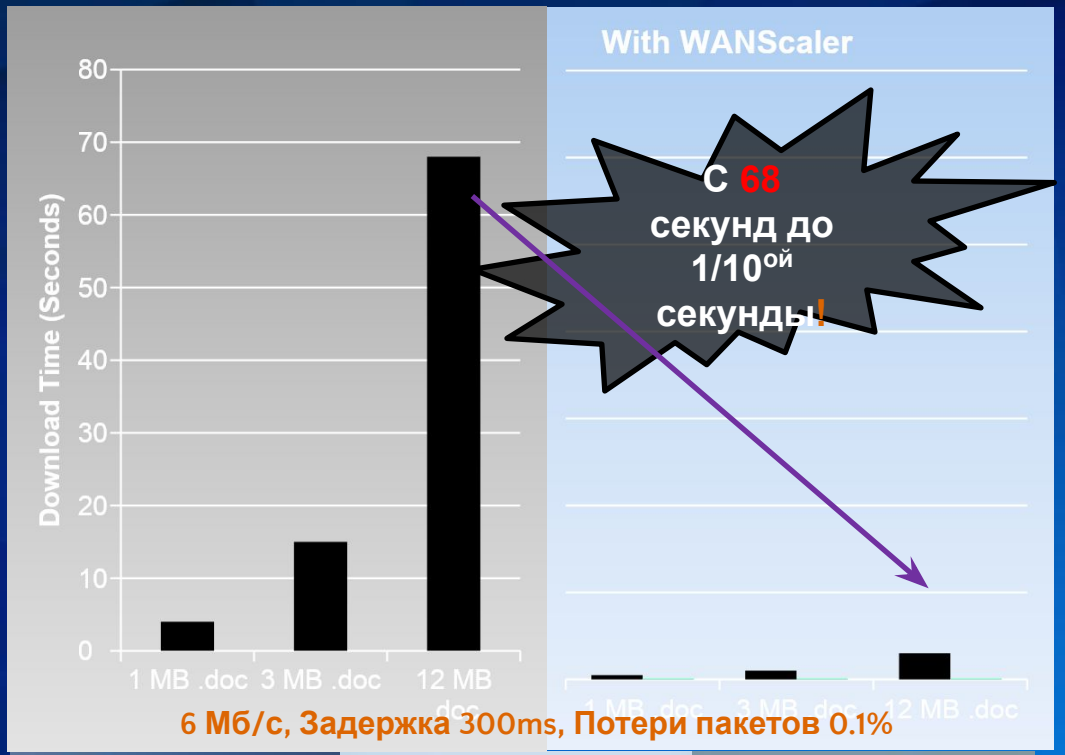
Центр обработки данных

Результат: ✔Эффективно ✔Просто ✔Отлично Масштабируется

Microsoft Платформа 2008

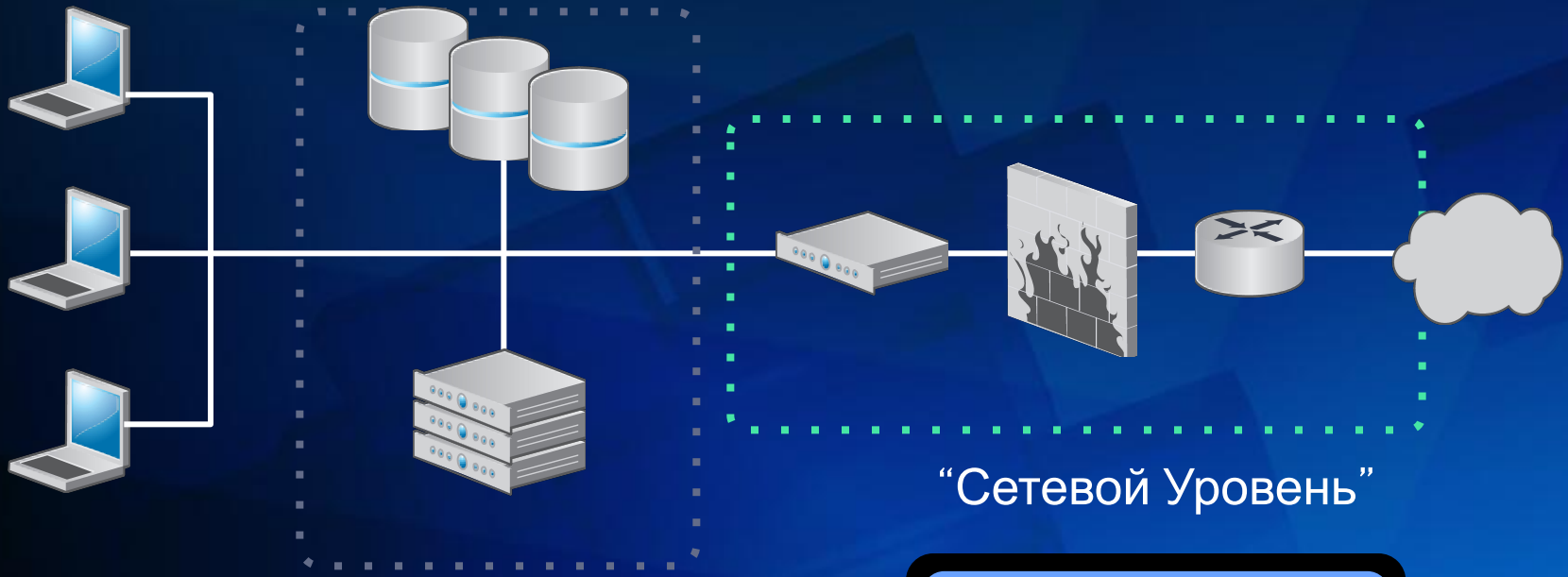
Сценарии с Большими Задержками

- **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 Платформа 2008

Инфраструктура Филиала



"Сетевой Уровень"

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

"Уровень Сервисов"

1. WAN Оптимизация
2. Сервисы Windows

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

Microsoft Платформа 2008

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

(Улучшение не эффективных протоколов)

(Сокращение передаваемых данных)

(Борьба с потерями/штрафами задержки)

(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 Дисковую 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

X = Потеря пакета

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

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

TCP в глобальных сетях (WAN)

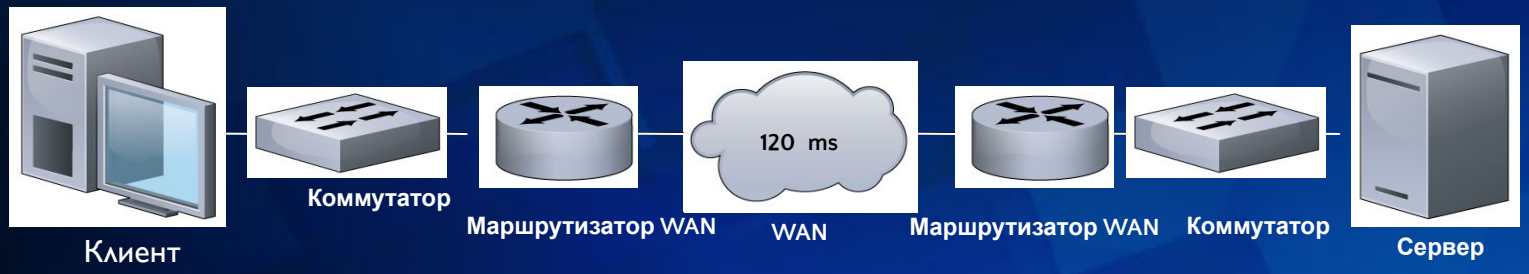
X = Потеря пакета

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

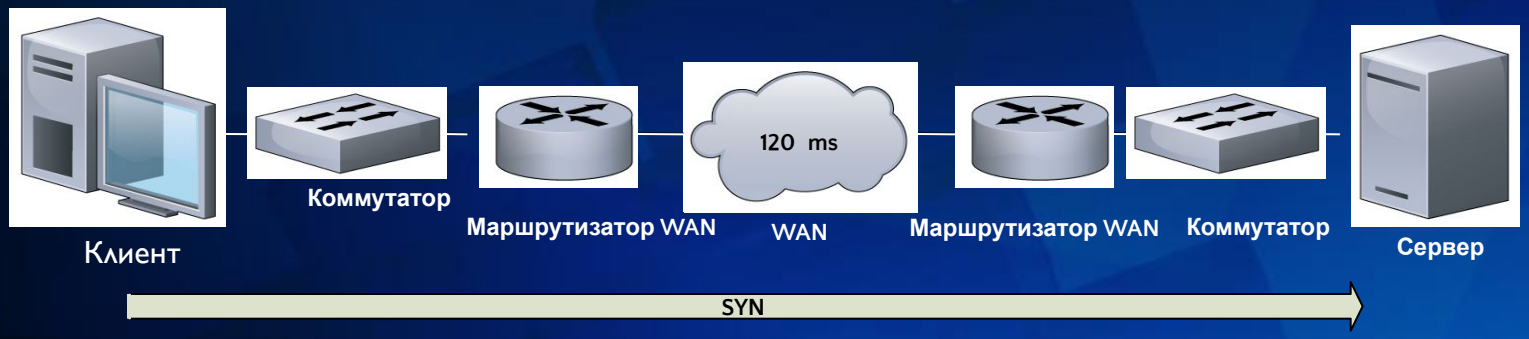
2
Потеря пакетов очень нерегулярна и временами сомнительна, чтобы быть предсказуемой.

TCP в глобальных сетях (WAN)

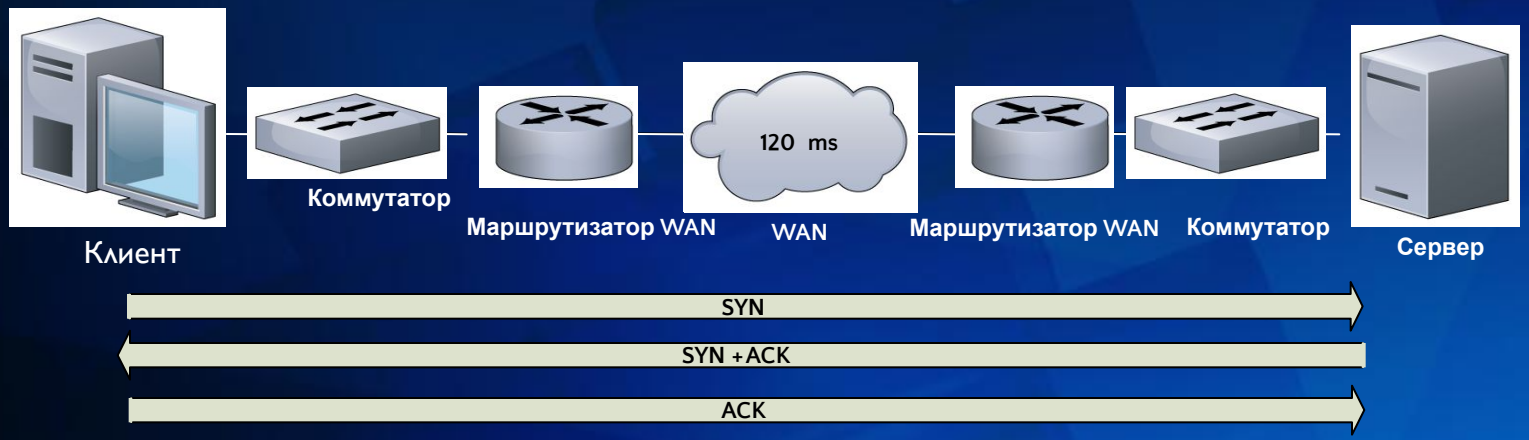
Стандартное управление TCP потоком в WAN



Стандартное управление TCP потоком в WAN

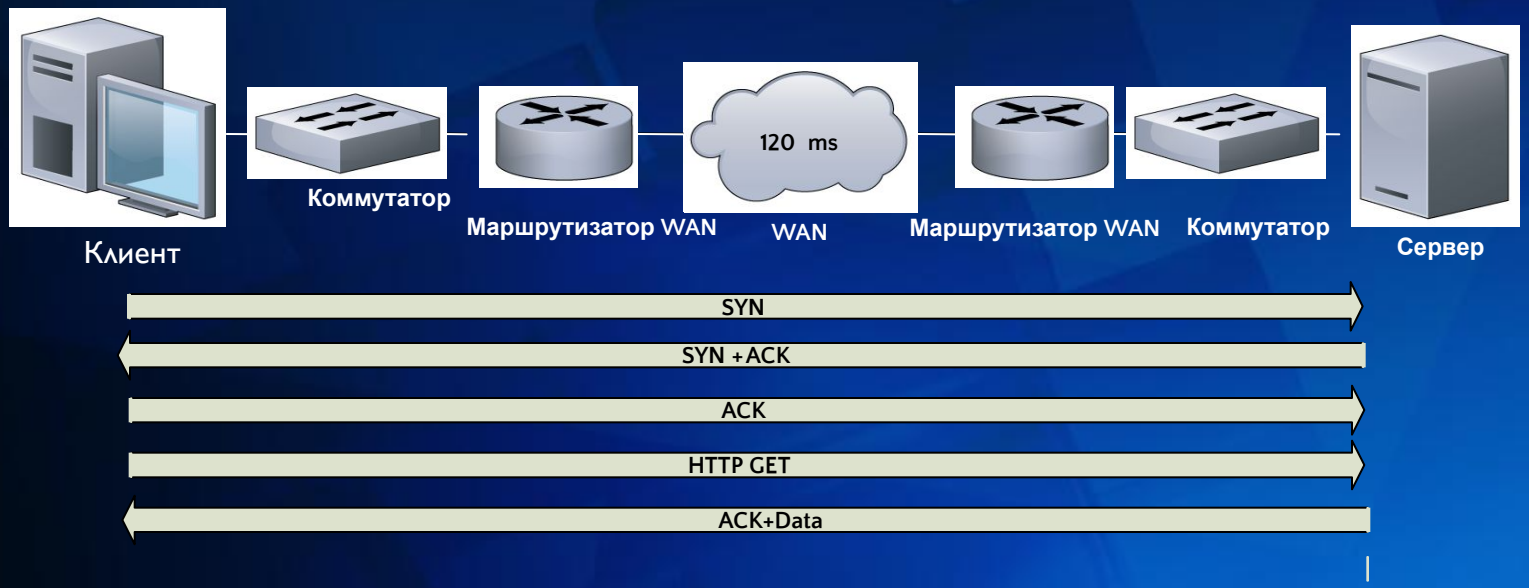


Стандартное управление TCP потоком в WAN

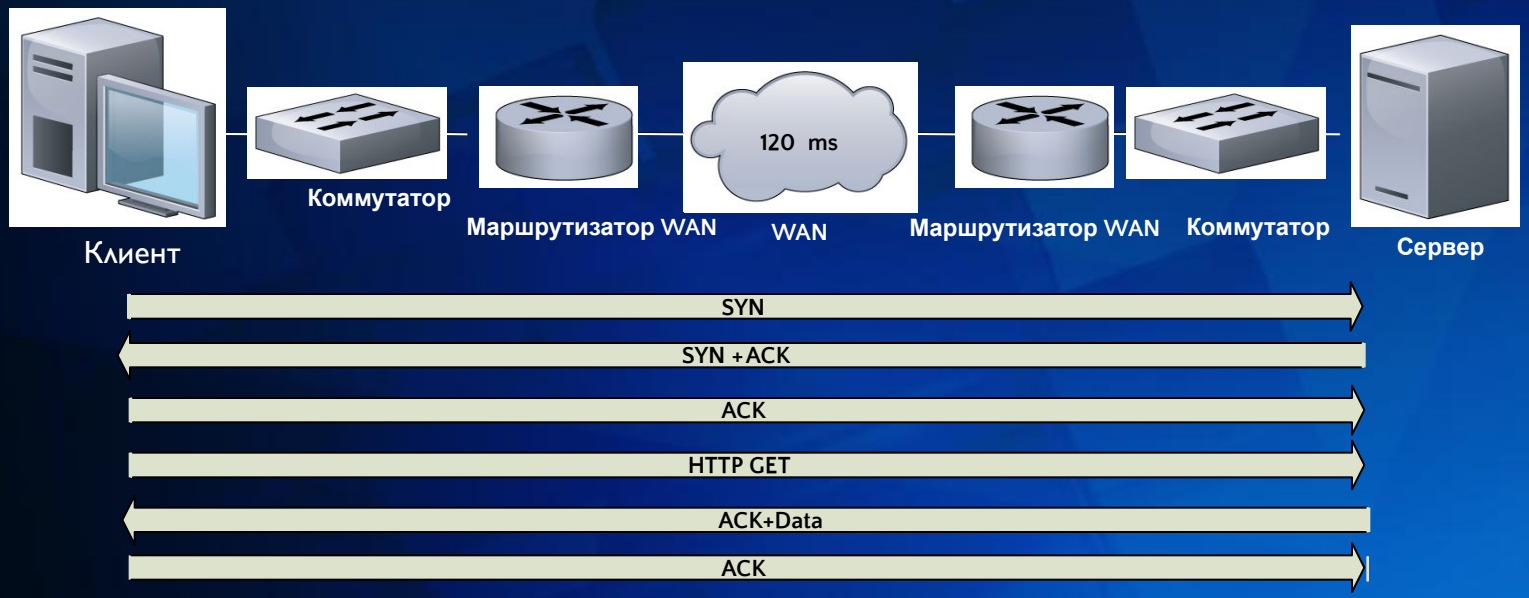


Стандартное управление TCP потоком в WAN

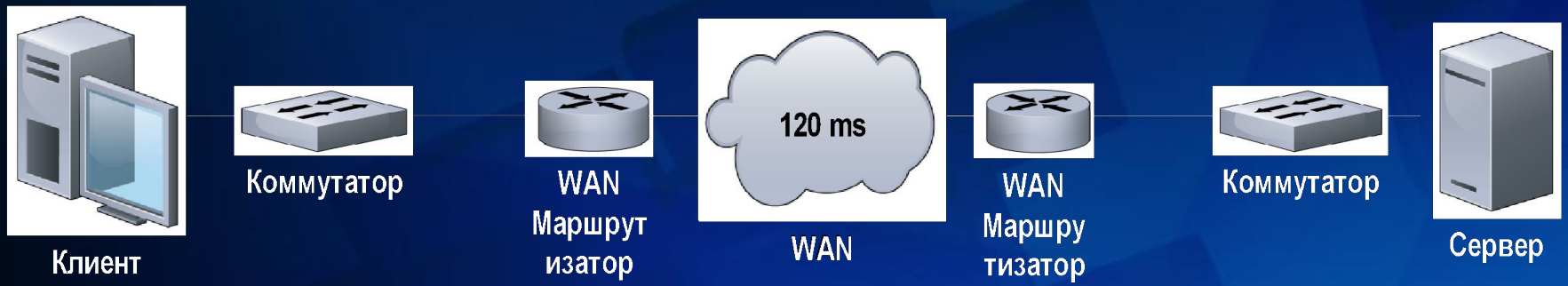
Стандартное управление TCP потоком в WAN



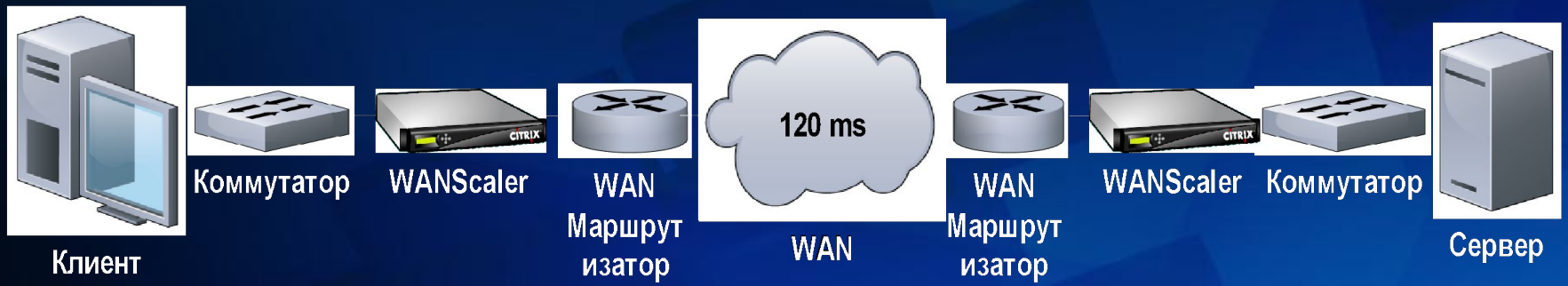
Стандартное управление TCP потоком в WAN



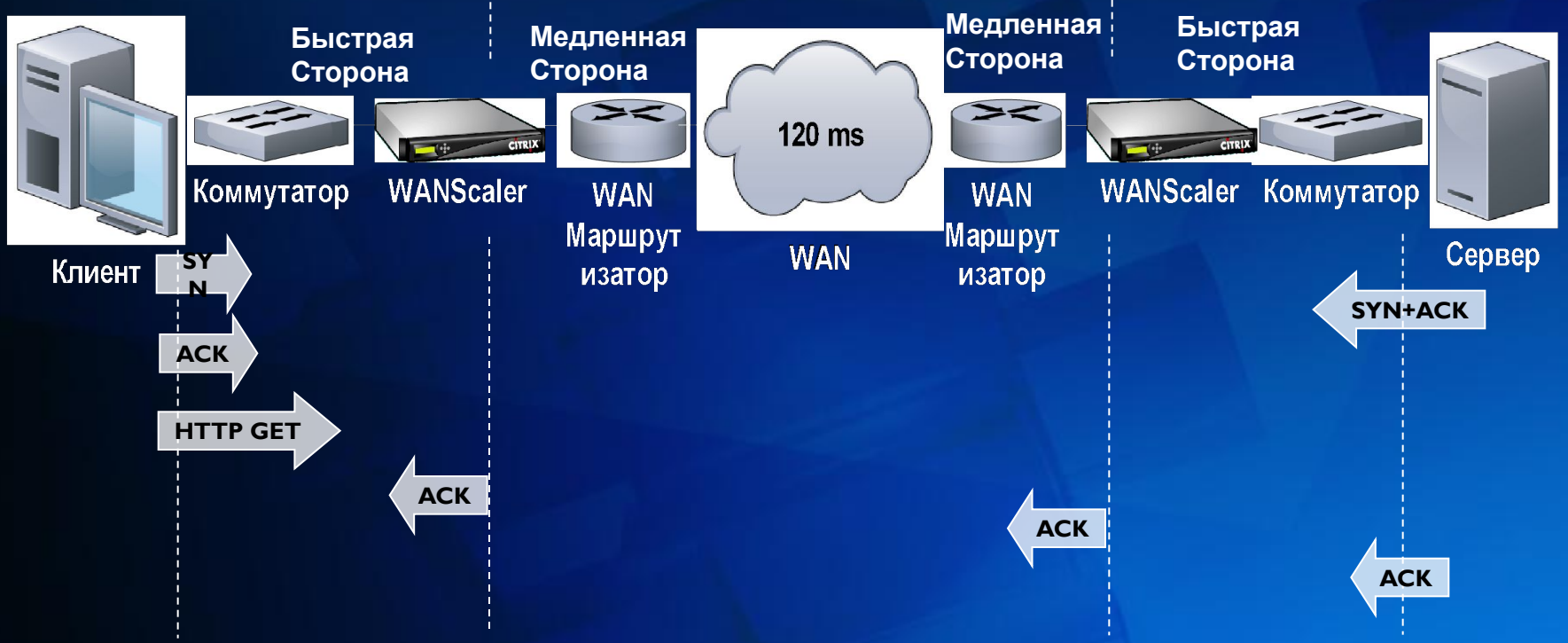
Управление TCP потоком WANScaler



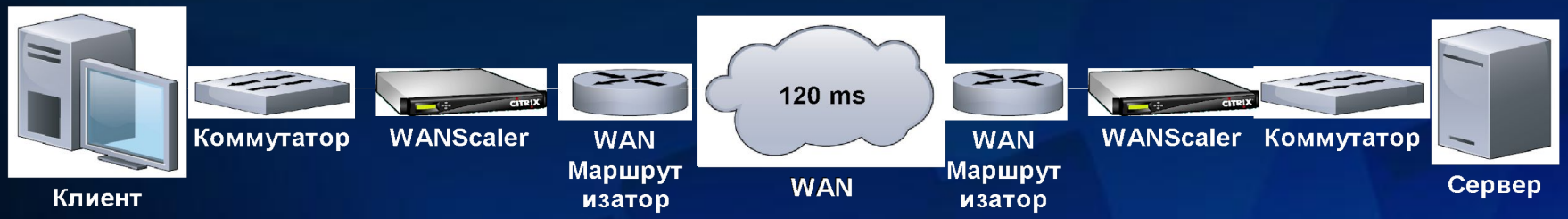
Управление TCP потоком WANScaler



Управление TCP потоком WANScaler

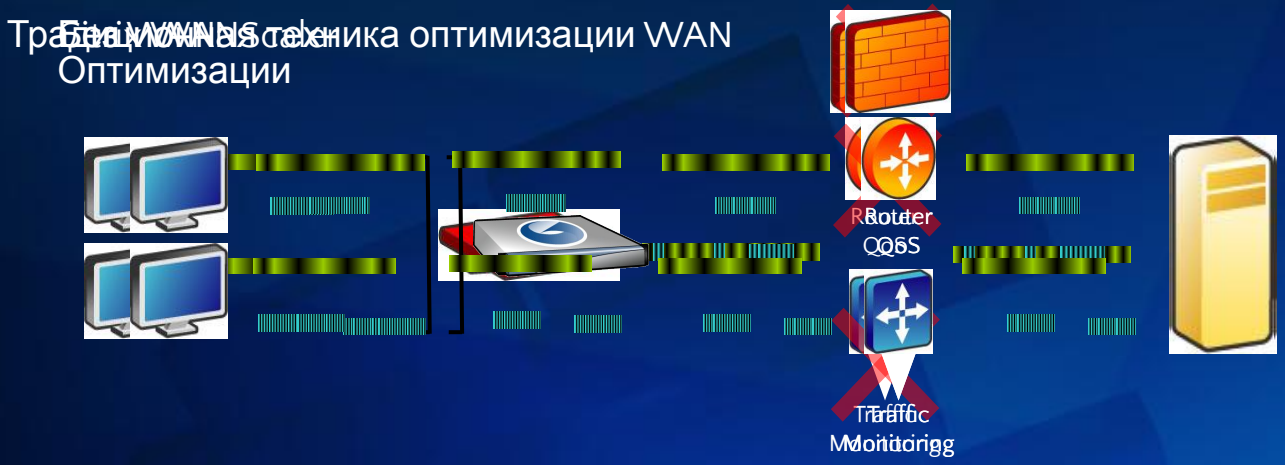


Управление TCP потоком WANScaler



- 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



- Оптимизация трафика TCP не изменяет заголовоков 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

Платформа 2008

QoS – Как это работает

- Цель: Полностью заполнить канал
  - QoS наводит порядок в трафике, заполняющим канал
- Существует Пять классов трафика (От “A” до “E”. 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

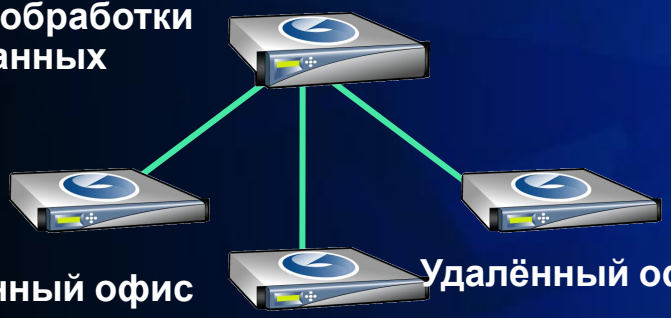
Варианты внедрения WANScaler

Точка – Точка

Центр обработки данных

Удалённый офис

Звезда



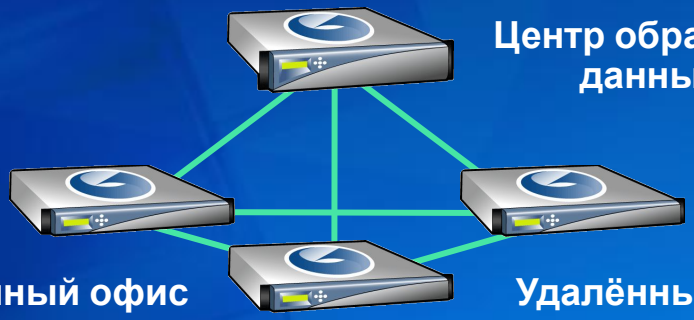
Центр обработки данных

Удалённый офис

Удалённый офис

Удалённый офис

Смешанный



Центр обработки данных

Удалённый офис

Удалённый офис

Удалённый офис

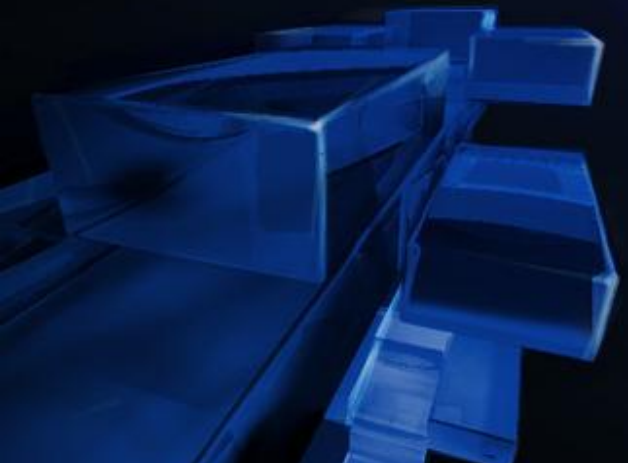
Microsoft Платформа 2008

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

Microsoft® Платформа 2008

ВОПРОСЫ?



Сергей Халяпин
Citrix Systems
sergey.khalyapin@eu.citrix.com


CITRIX®

Microsoft®

Your potential. Our passion.™

Microsoft Платформа 2008