Solidex

Высокая доступность DHCP и DNS

Евгений Дрыбин

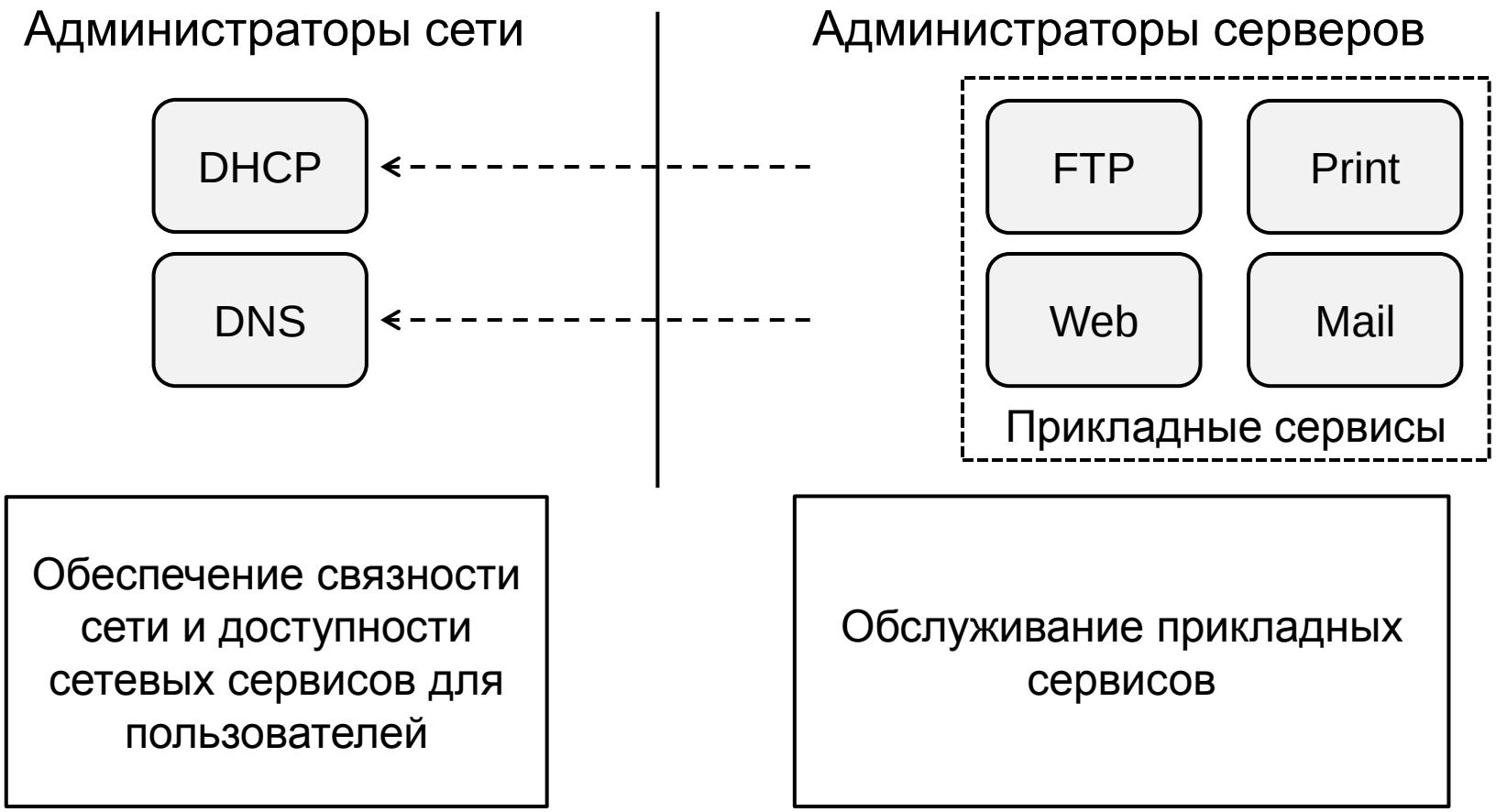
2 Октября, 2012

Слабые места существующей структуры DHCP и DNS

Solidex

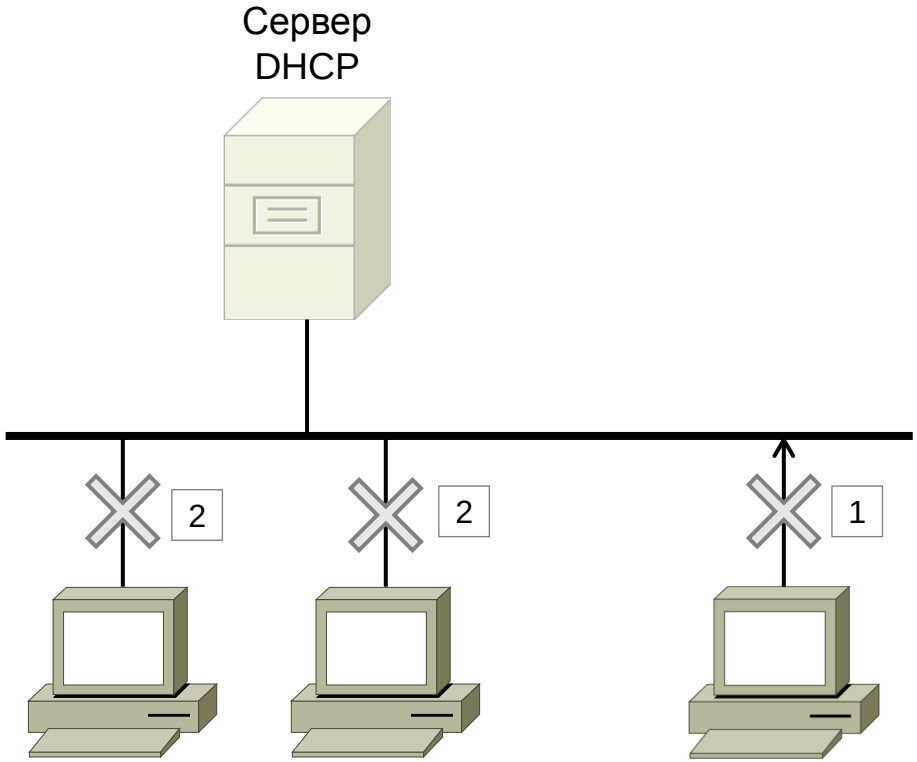
- Сервисы DHCP и DNS находятся под контролем администраторов серверов
- Сервисы DNS и DHCP управляются "независимо" друг от друга с минимальной интеграцией
- Нет резервирования сервиса DHCP

Контроль над сервисами



Для эффективного управления сетью контроль над сервисами DHCP и DNS следует передать администраторам сети

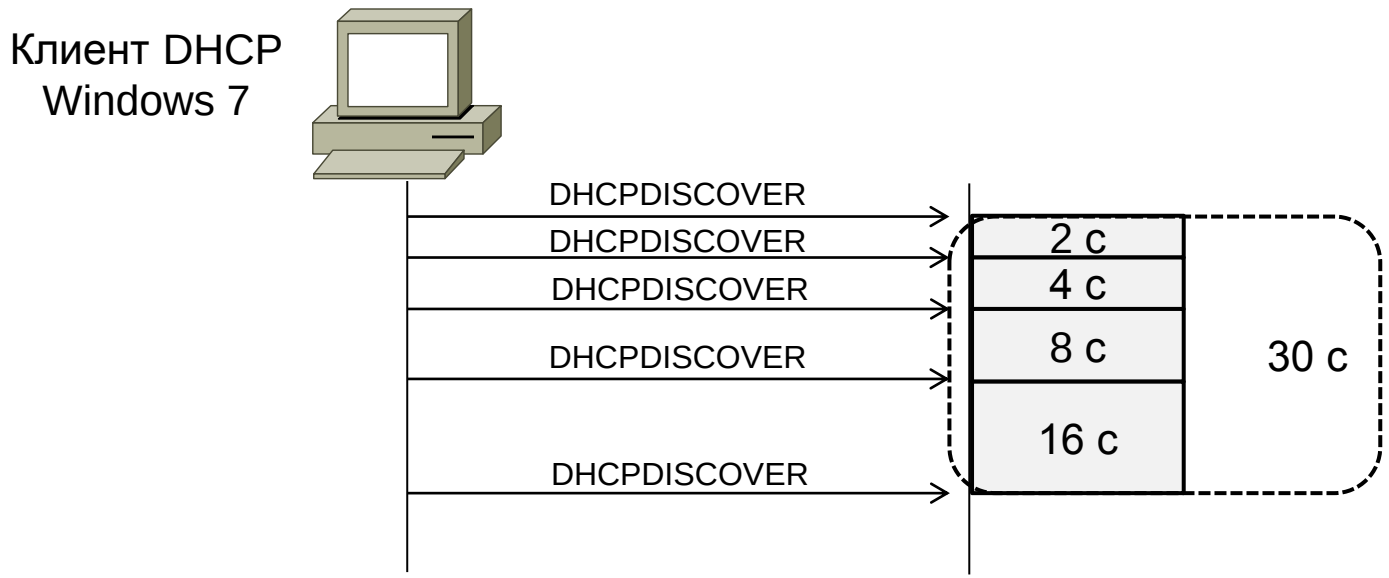
Сервис DHCP недоступен



- Новые пользователи не могут подключиться к сети (1)
- По истечении срока аренды пользователи и устройства утрачивают связь с сетью (2)

Высокая доступность сервиса DHCP

Клиенты DHCP всегда должны иметь возможность получить IP-адрес



Время восстановления сервиса менее 30 секунд

Обеспечение высокой доступности DHCP

- Вариант 1. Два сервера DHCP
- Вариант 2. DHCP Failover Protocol
- Вариант 3. Кластер высокой доступности
- Вариант 4. Средствами виртуализации вычислительных систем

Критерии

- Время восстановления сервиса DHCP менее 30 с
- Простота администрирования (определим как количество компонентов в решении)

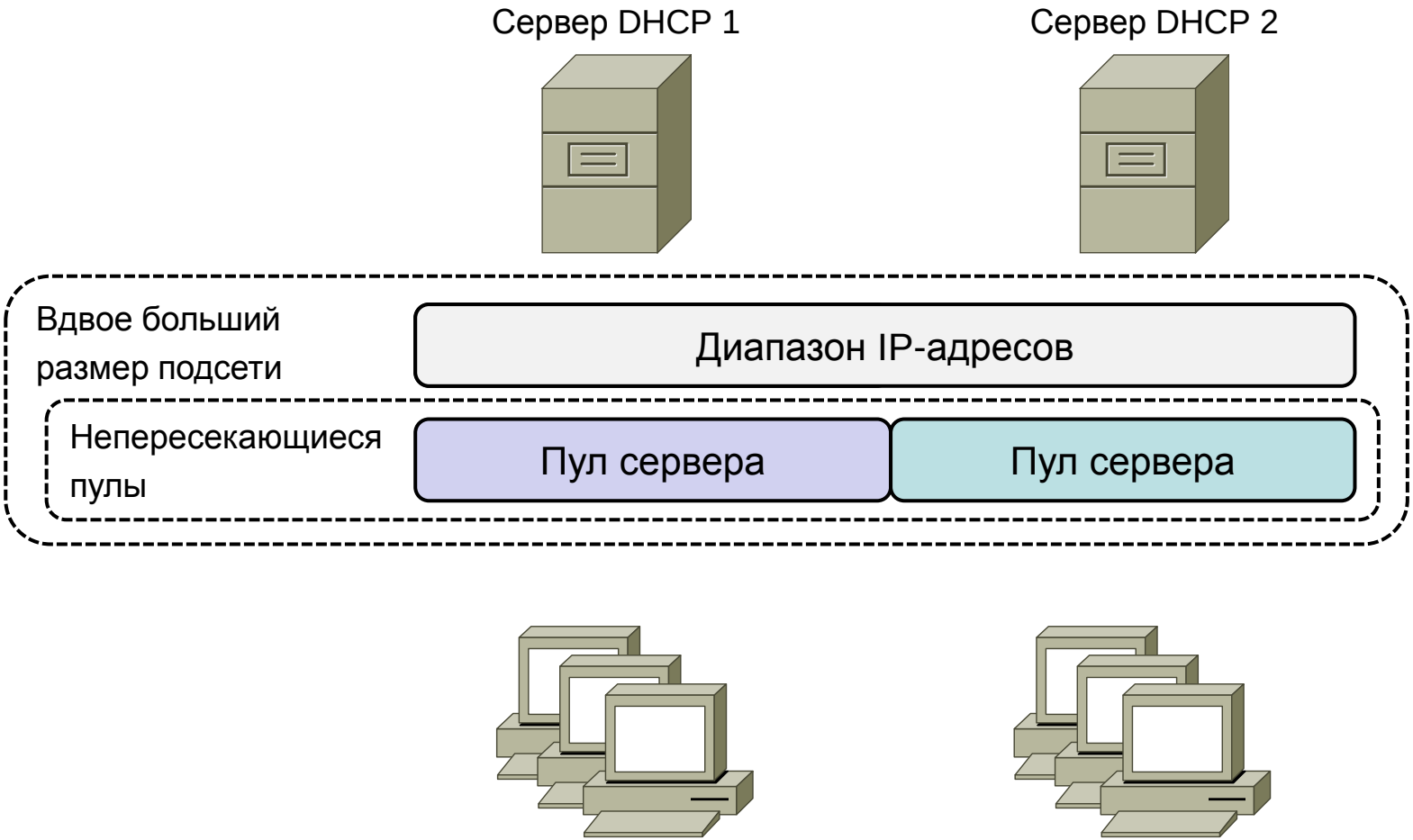
Обеспечение высокой доступности DHCP

- Вариант 1. Два сервера DHCP
- Вариант 2. DHCP Failover Protocol
- Вариант 3. Кластер высокой доступности
- Вариант 4. Средствами виртуализации вычислительных систем

Вариант 1. Два сервера DHCP

- Размещение в сети двух или более DHCP серверов с одинаковыми диапазонами (scopes) и непересекающимися пулами IP-адресов
- Все серверы отвечают на запросы клиентов
- Серверы не обмениваются информацией о выданных адресах

Диапазон IP-адресов

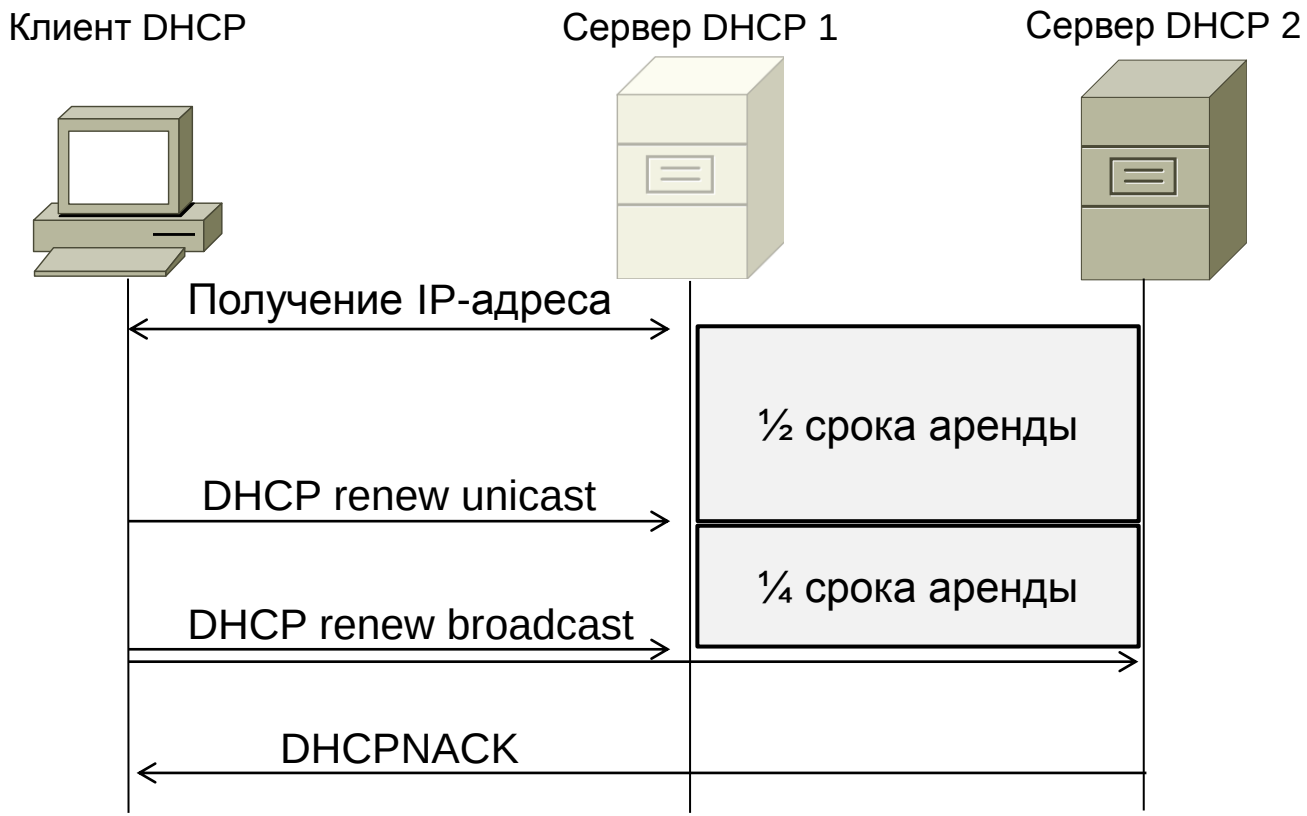


Каждый сервер способен обслужить всех клиентов сети

Отказ сервера

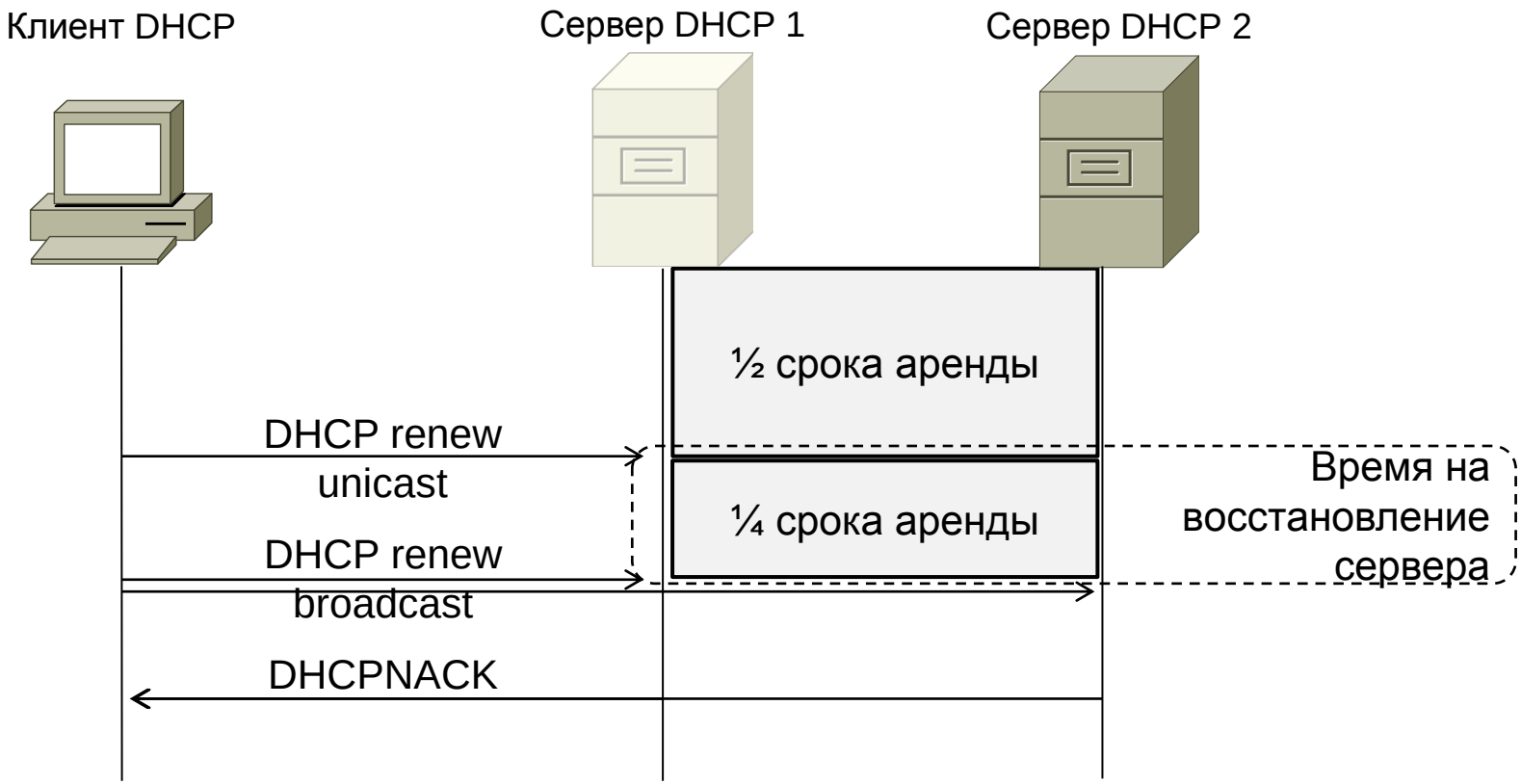
- Все запросы DHCP обрабатывает работающий сервер
- Клиенты, получившие динамический IP-адрес от вышедшего из строя сервера, не могут продлить аренду

Невозможность продлить аренду



- Изменяется IP-адрес
- Разрыв всех TCP соединений

Что делать?



- Восстановить сервер за ¼ срока аренды
- Определить срок аренды таким, чтобы пользователи не пытались продлить аренду в течение рабочего дня

Вариант 1. Соответствие критериям

	Два сервера DHCP
Время восстановления	Сервис не прерывается
Простота эксплуатации	2 сервера

Вариант 1. Недостатки решения

Solidex

- Требуется изменение плана IP-адресации (вдвое больший диапазон адресов)

Обеспечение высокой доступности DHCP

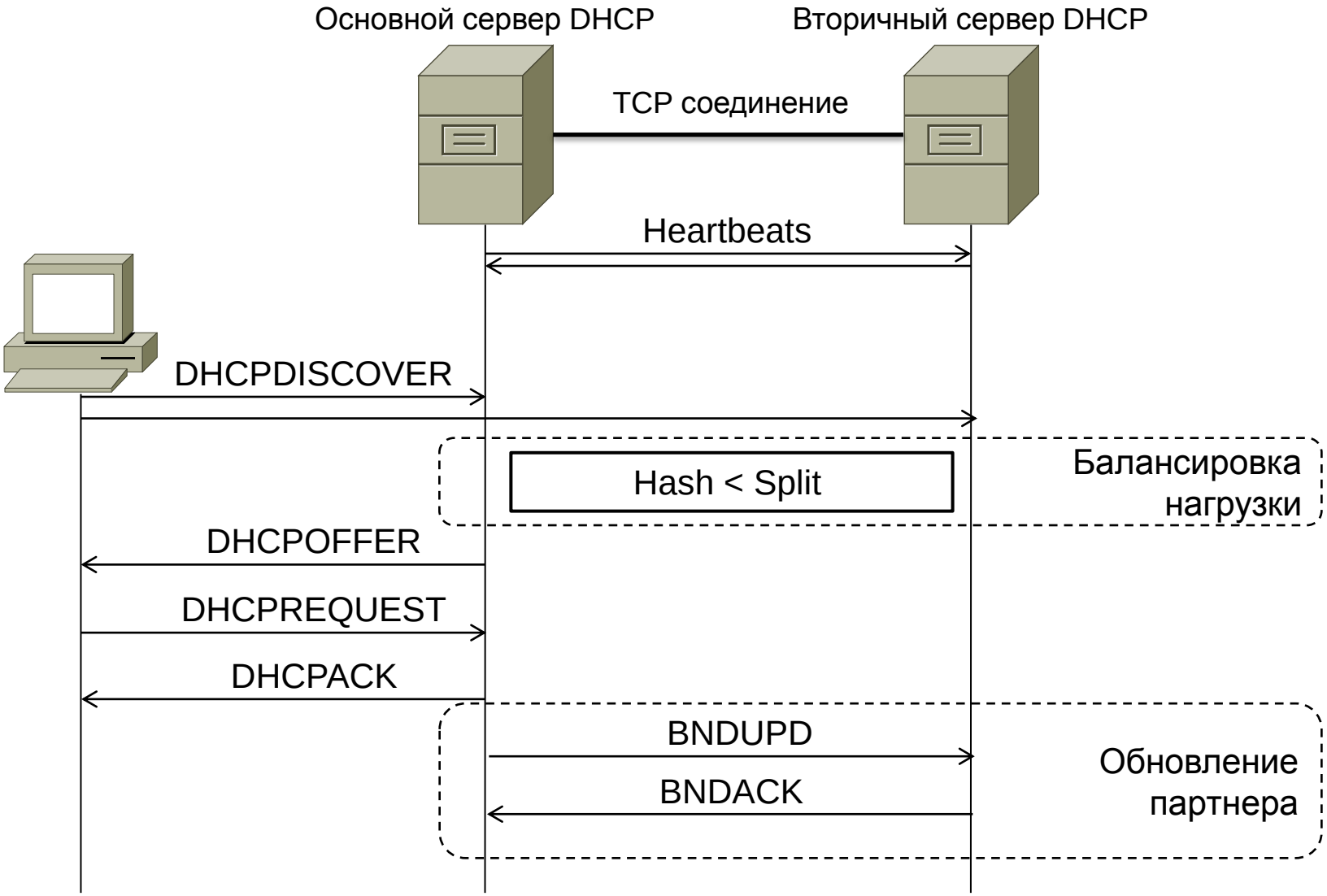
Solidex

- Вариант 1. Два сервера DHCP
- Вариант 2. DHCP Failover Protocol
- Вариант 3. Кластер высокой доступности
- Вариант 4. Средствами виртуализации вычислительных систем

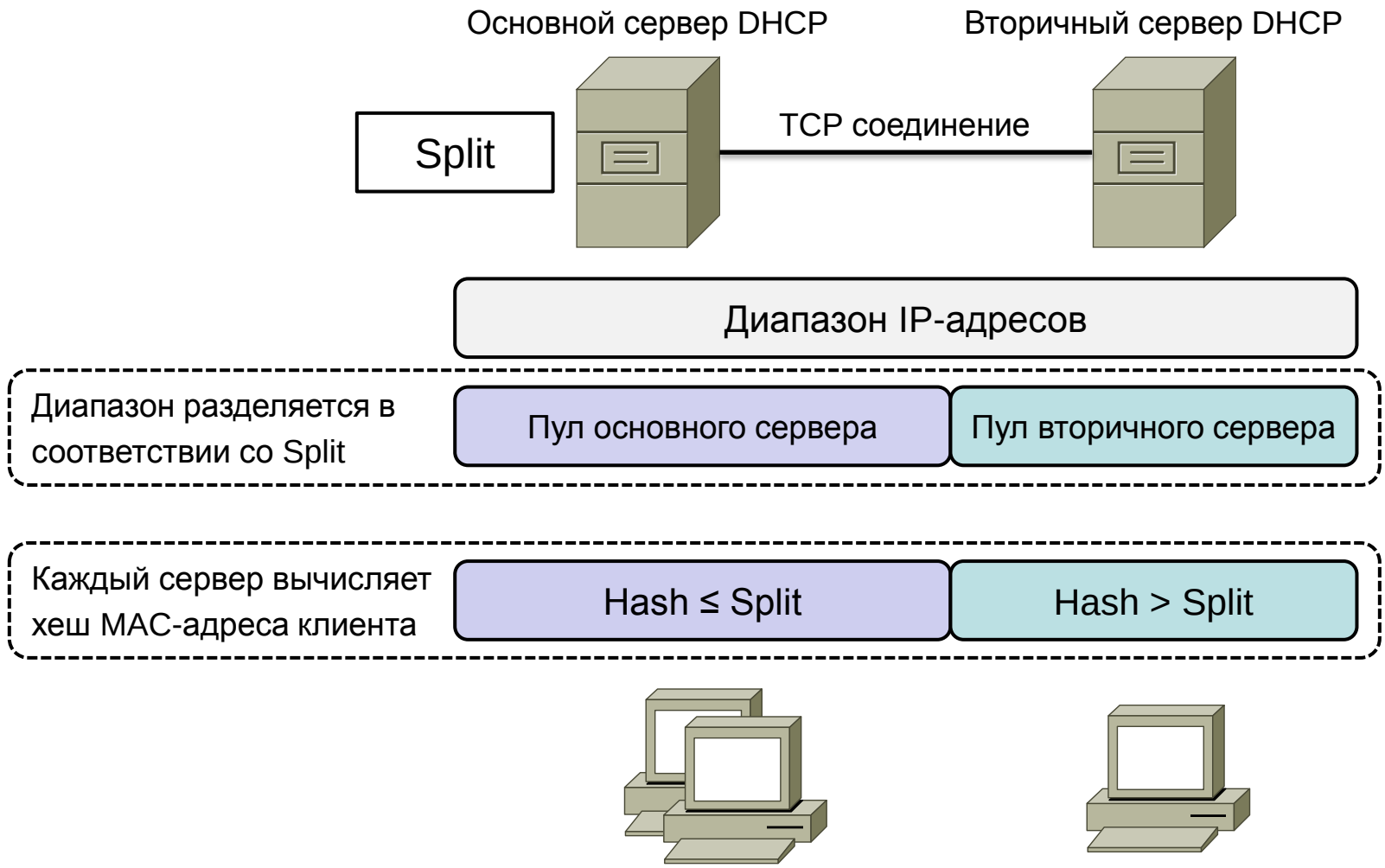
Вариант 2. DHCP Failover Protocol

- На двух серверах DHCP настраиваются одинаковые диапазоны и взаимодействие по протоколу DHCP Failover (IETF Internet Draft)
- Серверы обмениваются информацией о выданных IP-адресах и клиентах
- Балансировка нагрузки
- DHCP Failover поддерживается в реализациях DHCP сервера Win2008R2, Win2012, ISC DHCP v.3 и старше

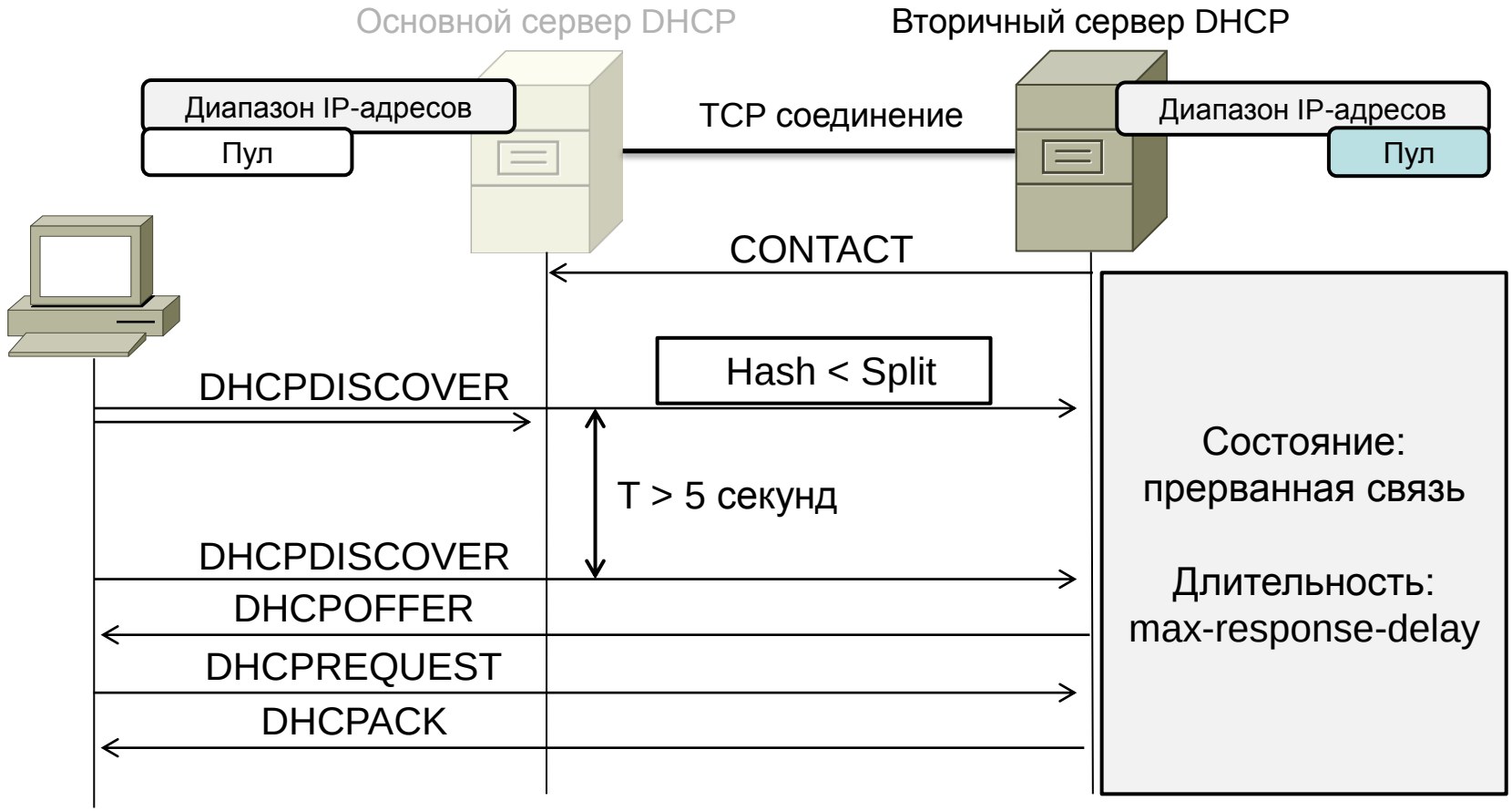
Взаимодействие серверов



Балансировка нагрузки

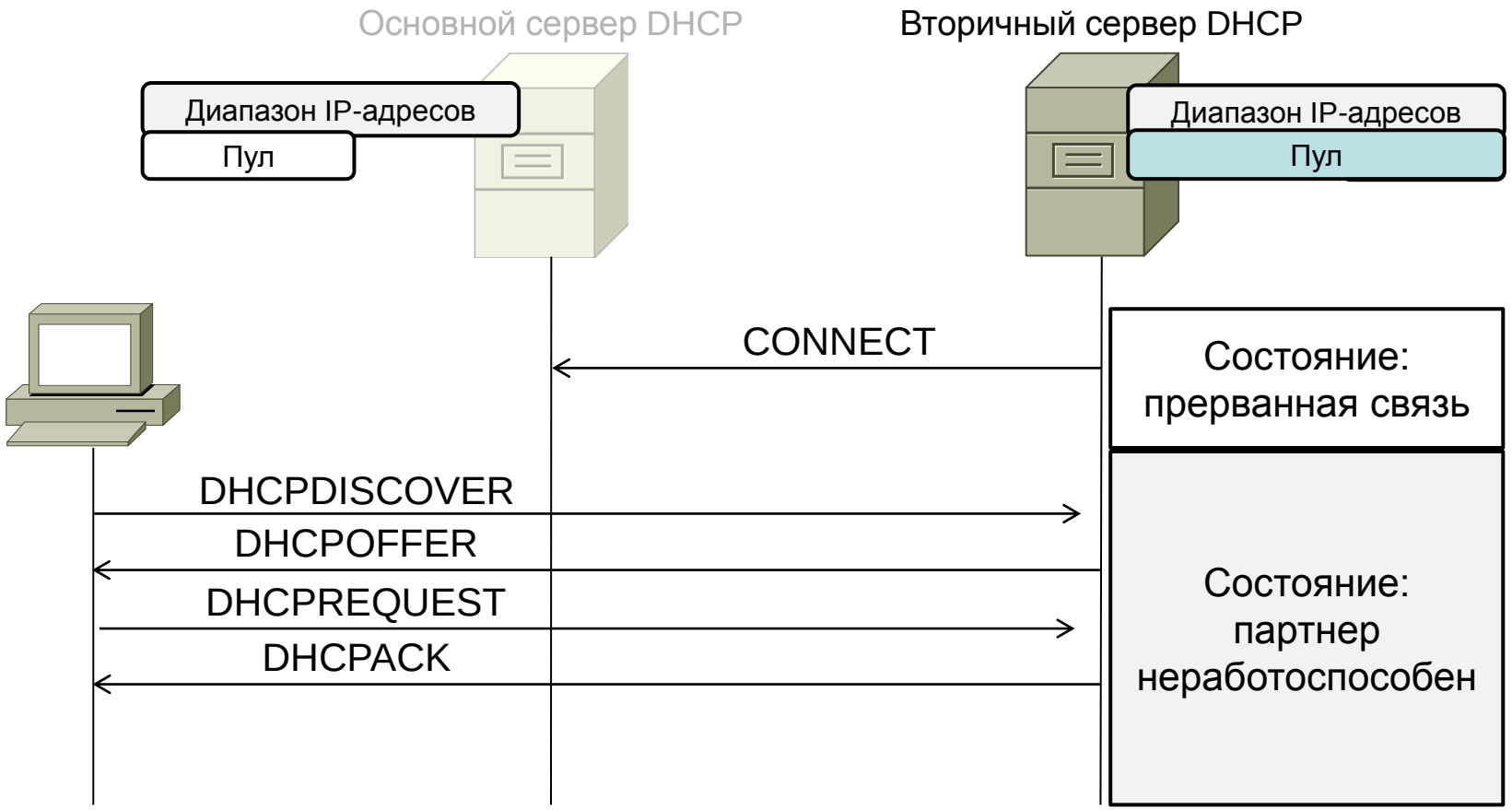


Отказ сервера. Состояние прерванной связи



Вторичный сервер обслужит повторный запрос клиента независимо от хеша (повторность запроса определяется на основании времени между запросами)

Отказ сервера. Состояние неработоспособен партнер



Вторичный сервер обслуживает все запросы клиентов

Вариант 2. Соответствие критериям

	Два сервера DHCP	Протокол DHCP Failover
Время восстановления	Сервис не прерывается	Сервис не прерывается
Простота эксплуатации	2 сервера	2 сервера

Вариант 2. Недостатки решения

Solidex

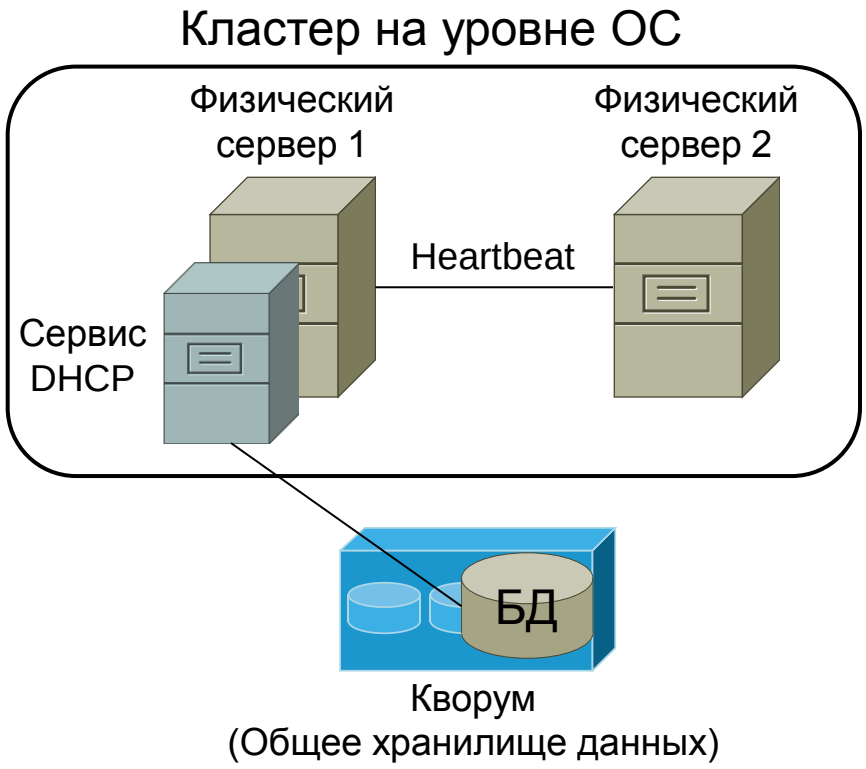
- Протокол DHCP Failover не является стандартом (Internet Draft)

Обеспечение высокой доступности DHCP

Solidex

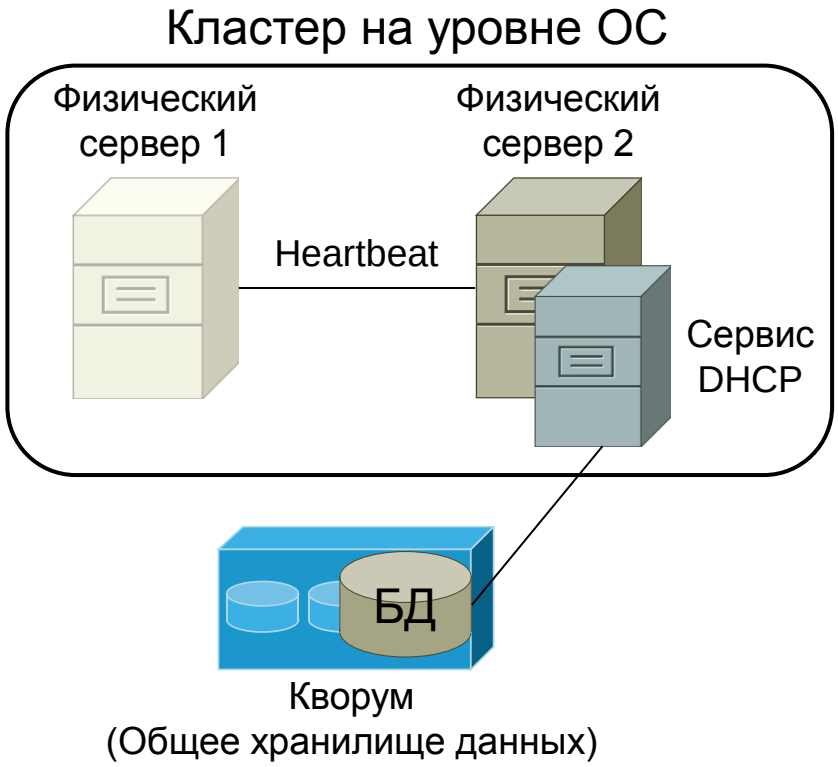
- Вариант 1. Два сервера DHCP
- Вариант 2. DHCP Failover Protocol
- Вариант 3. Кластер высокой доступности
- Вариант 4. Средствами виртуализации вычислительных систем

Вариант 3: Кластер высокой доступности



Информация о выданных IP-адресах хранится в базе данных на диске кворума

Отказ сервера



Время восстановления = время детектирования отказа + запуск службы DHCP

≈ несколько секунд

Недостаток кластера

- Общее хранилище данных является единой точкой отказа
- Необходимо решение для резервирования СХД, что увеличит общую стоимость решения

Вариант 3. Соответствие критериям

Solidex

	Два сервера DHCP	Протокол DHCP Failover	Кластер высокой доступности
Время восстановления	Сервис не прерывается	Сервис не прерывается	Несколько секунд
Простота эксплуатации	2 сервера	2 сервера	2 сервера + СХД + кластер

Вариант 3. Недостатки решения

Solidex

- Дополнительные денежные расходы на ПО кластеризации
- Необходимо решение для резервирования СХД

Обеспечение высокой доступности DHCP

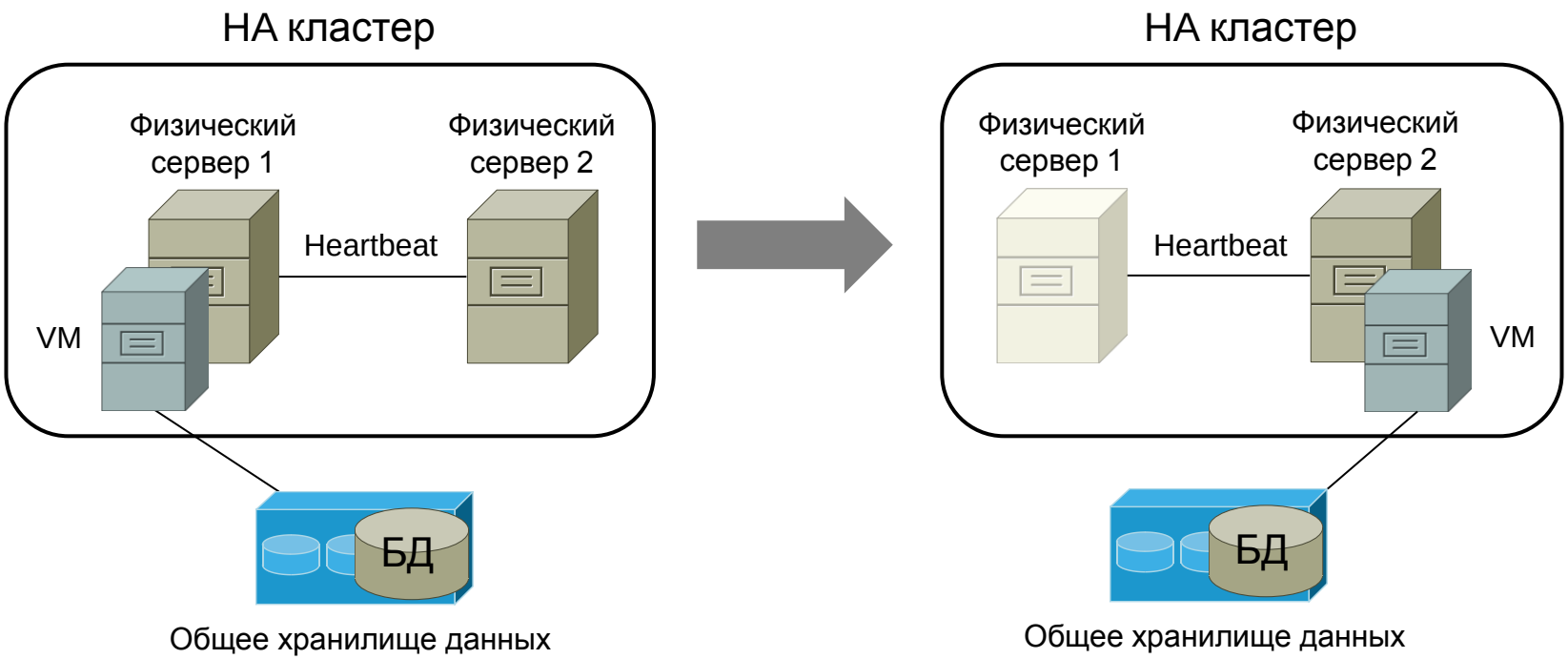
Solidex

- Вариант 1. Два сервера DHCP
- Вариант 2. DHCP Failover Protocol
- Вариант 3. Кластер высокой доступности
- Вариант 4. Средствами виртуализации вычислительных систем

Вариант 4: Средствами виртуализации

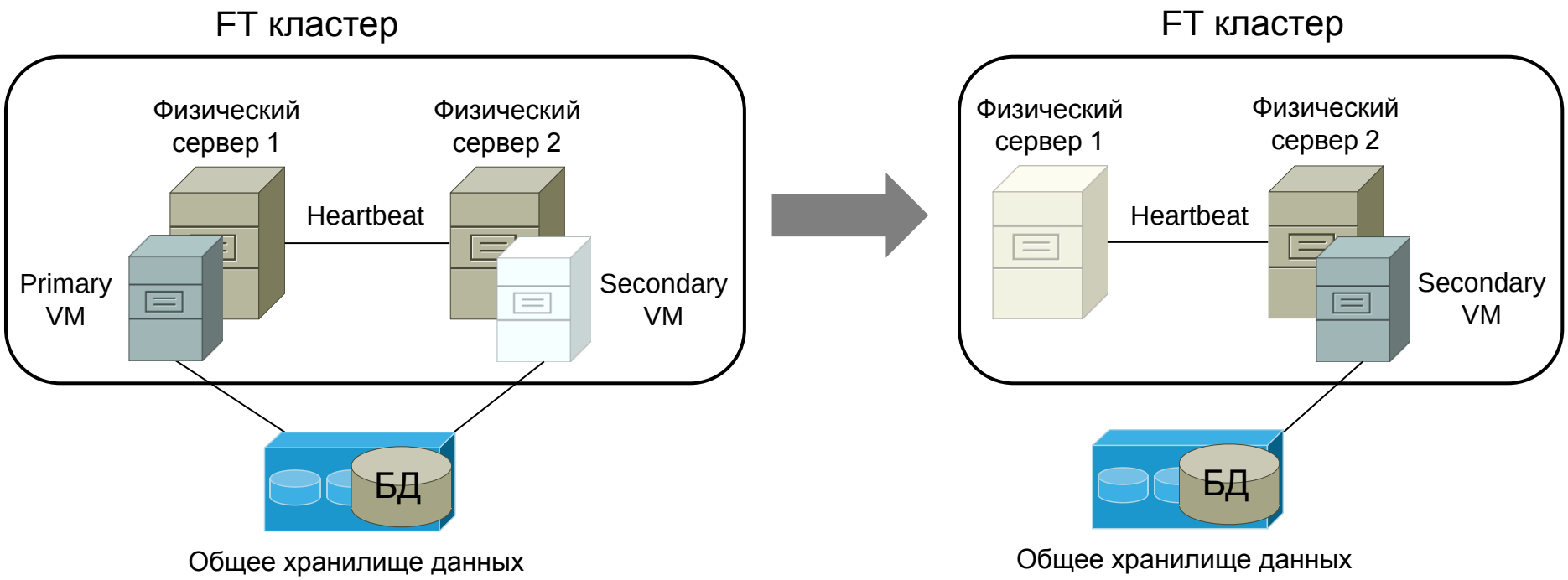
- Объединение нескольких физических серверов в кластер высокой доступности средствами гипервизора вычислительных систем

Отказ сервера. High Availability



Перезапуск ВМ занимает порядка минуты > 30с

Отказ сервера. Fault Tolerance



Перезапуск ВМ не требуется

Время детектирования отказа ≈ 1 мс

Вариант 4. Соответствие критериям

Solidex

	Два сервера DHCP	Протокол DHCP Failover	Кластер высокой доступности	Средствами виртуализации
Время восстановления	Сервис не прерывается	Сервис не прерывается	Несколько секунд	Около миллисекунды
Простота эксплуатации	2 сервера	2 сервера	2 сервера + СХД + кластер	2 сервера + СХД

Вариант 4. Недостатки решения

Solidex

- Дополнительные денежные расходы на ПО виртуализации
- Необходимо решение для резервирования СХД
- Не защищает от сбоев гостевой операционной системы или виртуальной машины

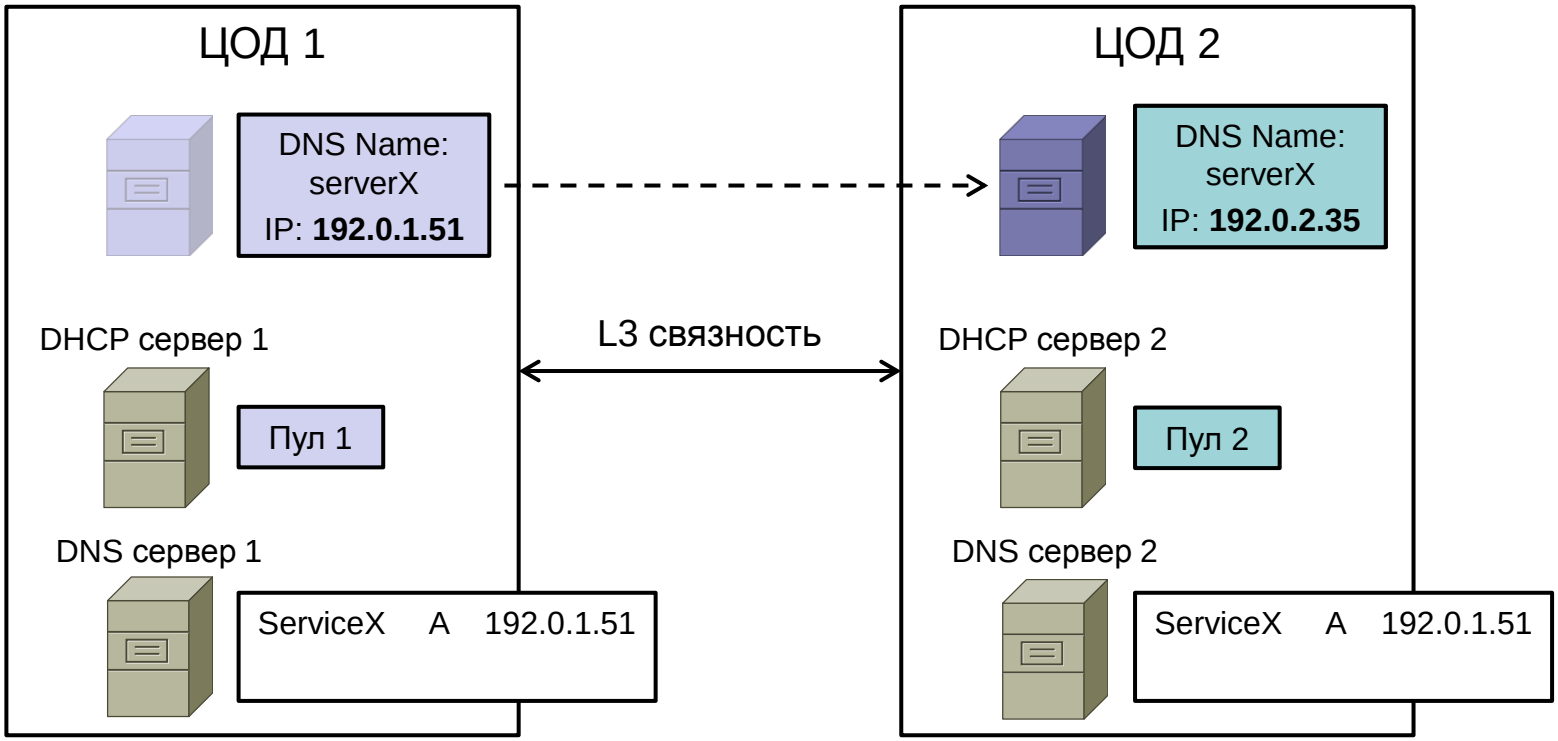
Интеграция DHCP и DNS

Использование DHCP

- Сервис DHCP обычно используется для динамического назначения IP-адресов рабочим станциям

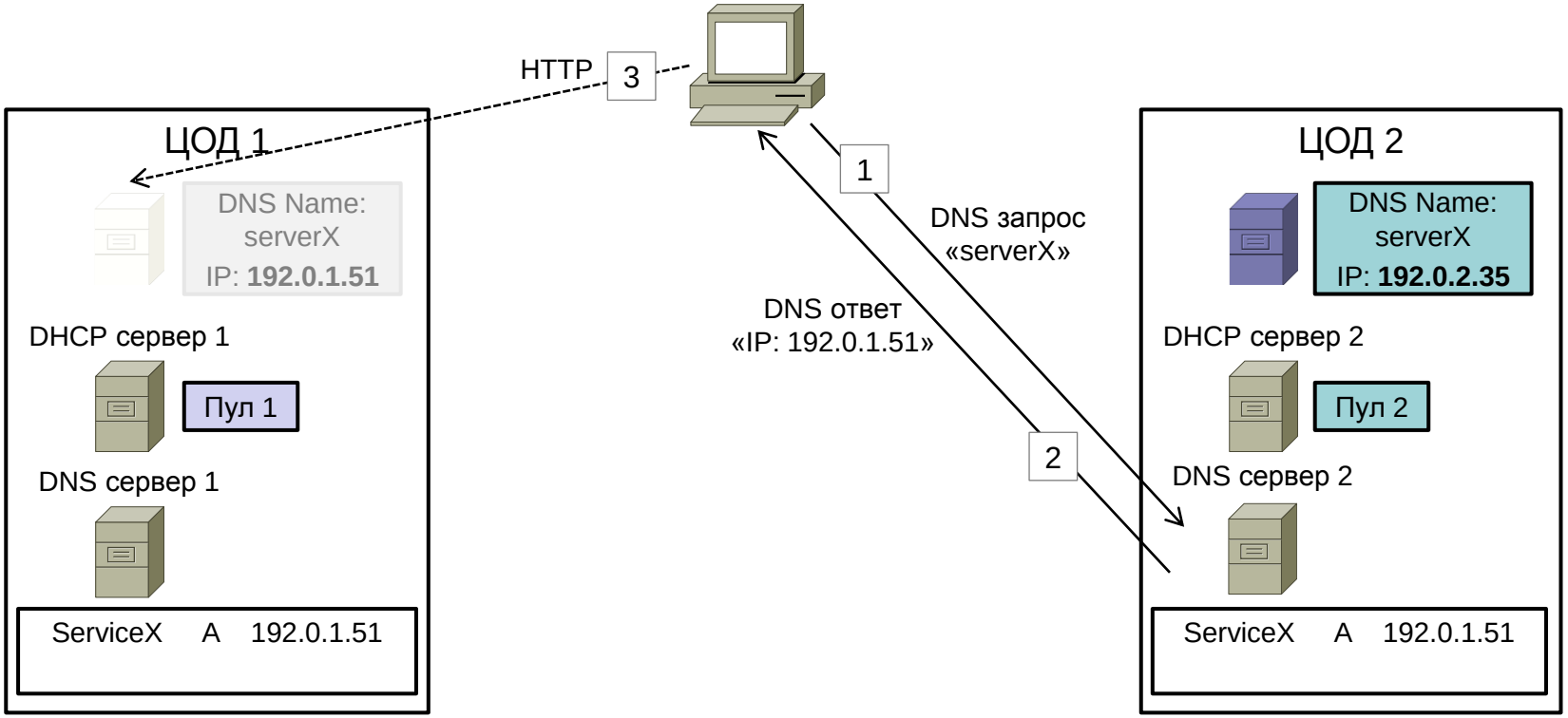
- Есть ли смысл использовать DHCP для серверов?

Перезапуск сервера в другом ЦОДе



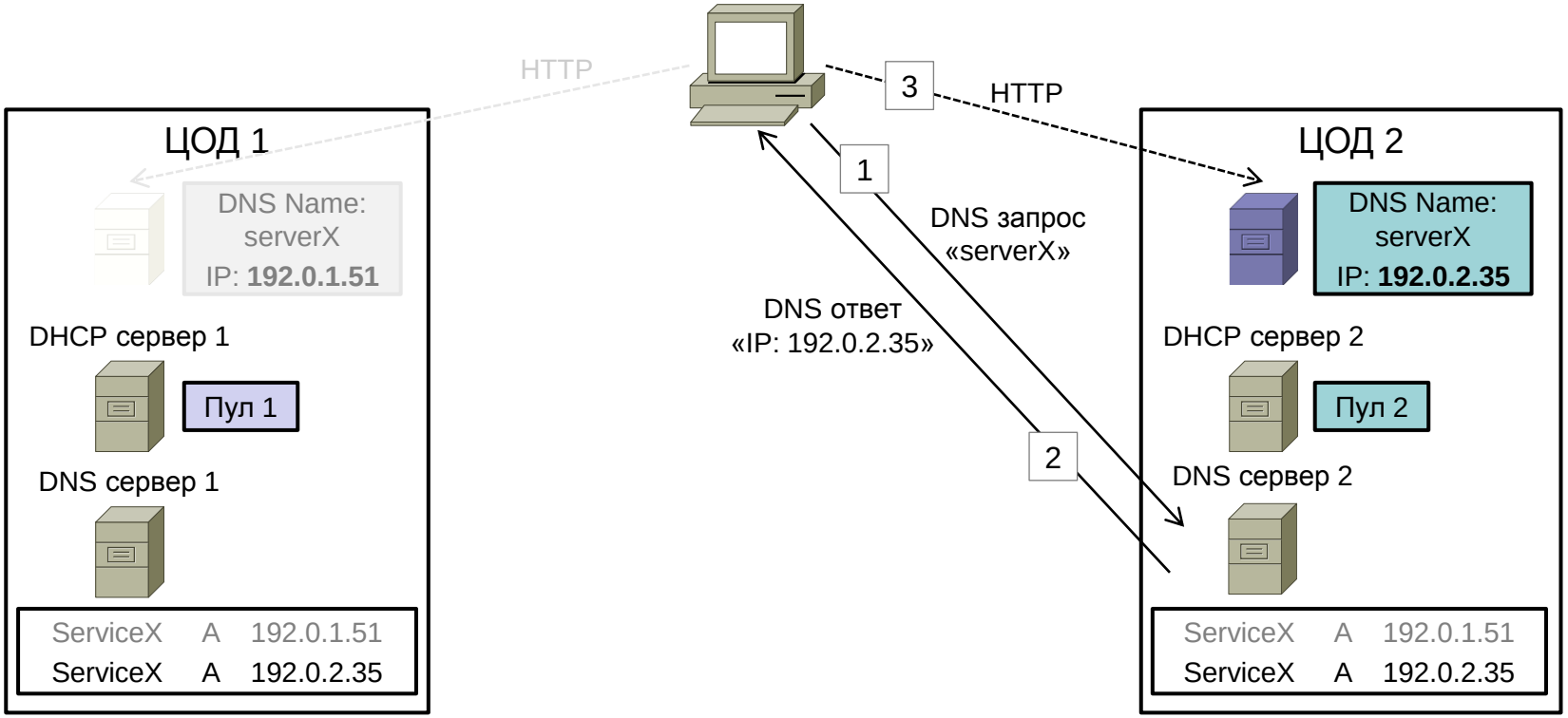
DHCP назначит серверу IP-адрес из подсети ЦОДа 2

Перезапуск сервера в другом ЦОДе (2)



- Клиенты обращаются к серверу по DNS имени
- IP-адрес сервера изменился

Перезапуск сервера в другом ЦОДе (3)



- Клиенты обращаются к серверу по DNS имени
- IP-адрес сервера изменился
- Необходимо обновить записи DNS

Обновление записей DNS вручную администратором

Solidex

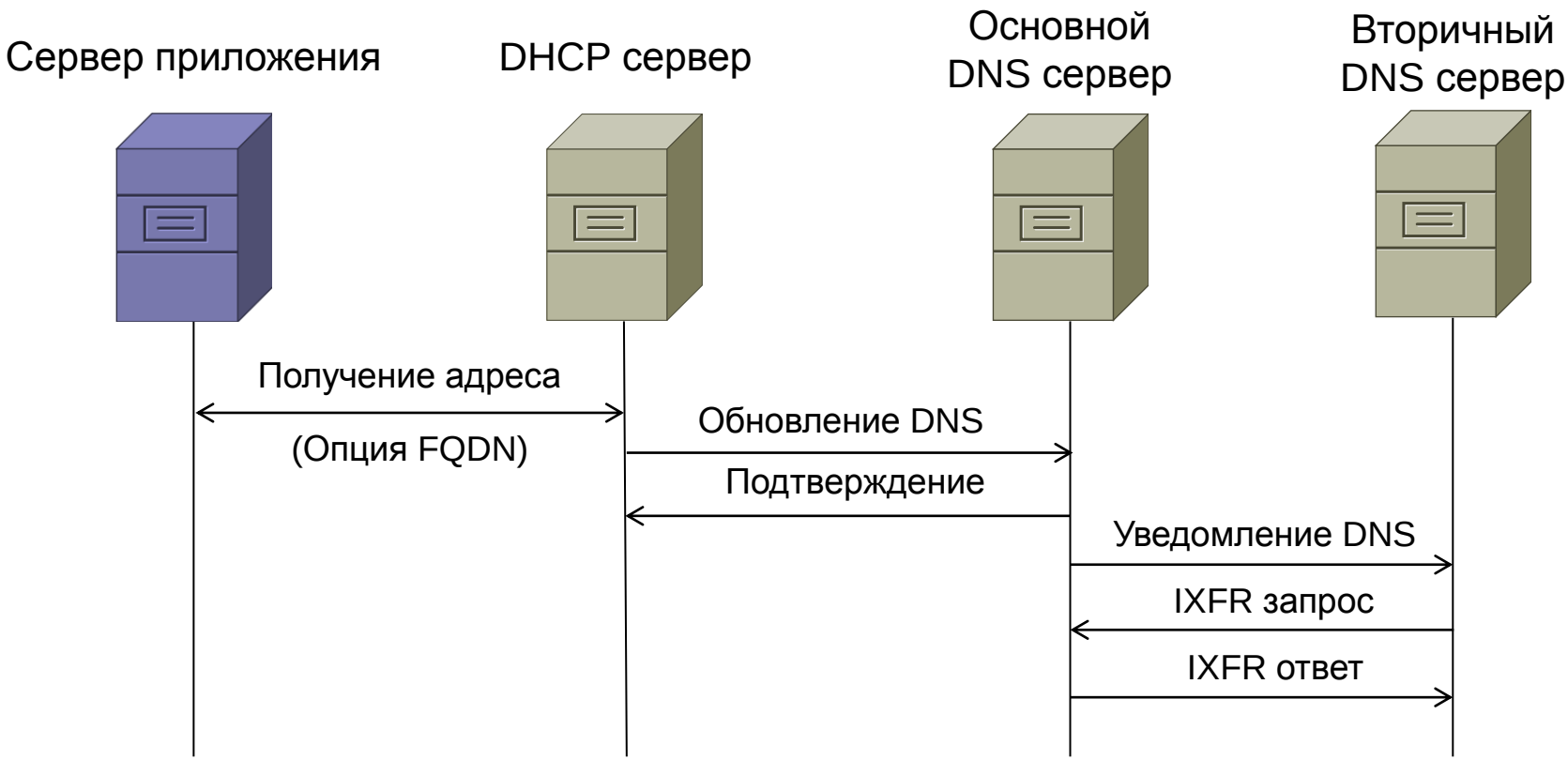
```
$ORIGIN example.com.     ; designates the start of this zone file in the namespace
$TTL 1h
example.com.  IN  SOA  ns.example.com. username.example.com. (
              2012091710 ; serial number of this zone file
              1d         ; slave refresh
              2h         ; slave retry time
              4w         ; slave expiration time
              1h         ; maximum caching time
              )
example.com.  NS    ns                    ; ns.example.com is a nameserver for example.com
example.com.  NS    ns.somewhere.example. ; ns.somewhere.example is a backup nameserver
example.com.  MX    10 mail.example.com.  ; mail.example.com is the mailserver for example.com
@             MX    20 mail2.example.com. ; equivalent to above line, "@" represents zone origin
@             MX    50 mail3              ; equivalent to above line, but using a relative host name
; server host definitions
example.com.  A     192.0.2.1             ; IPv4 address for example.com
ns            A     192.0.2.2             ; IPv4 address for ns.example.com
www           CNAME example.com.          ; www.example.com is an alias for example.com
wwwtest       CNAME www                   ; wwwtest.example.com is another alias for www.example.com
ftp           CNAME www.example.com.      ; ftp server definition
mail          A     192.0.2.3             ; IPv4 address for mail.example.com,
mail2         A     192.0.2.4             ; IPv4 address for mail2.example.com
mail3         A     192.0.2.5             ; IPv4 address for mail3.example.com
; non server domain hosts
bill          A      192.0.1.10
fred          A      192.0.1.12
```

Редактирование записей DNS вручную требует определенных знаний, времени и может вести к ошибкам

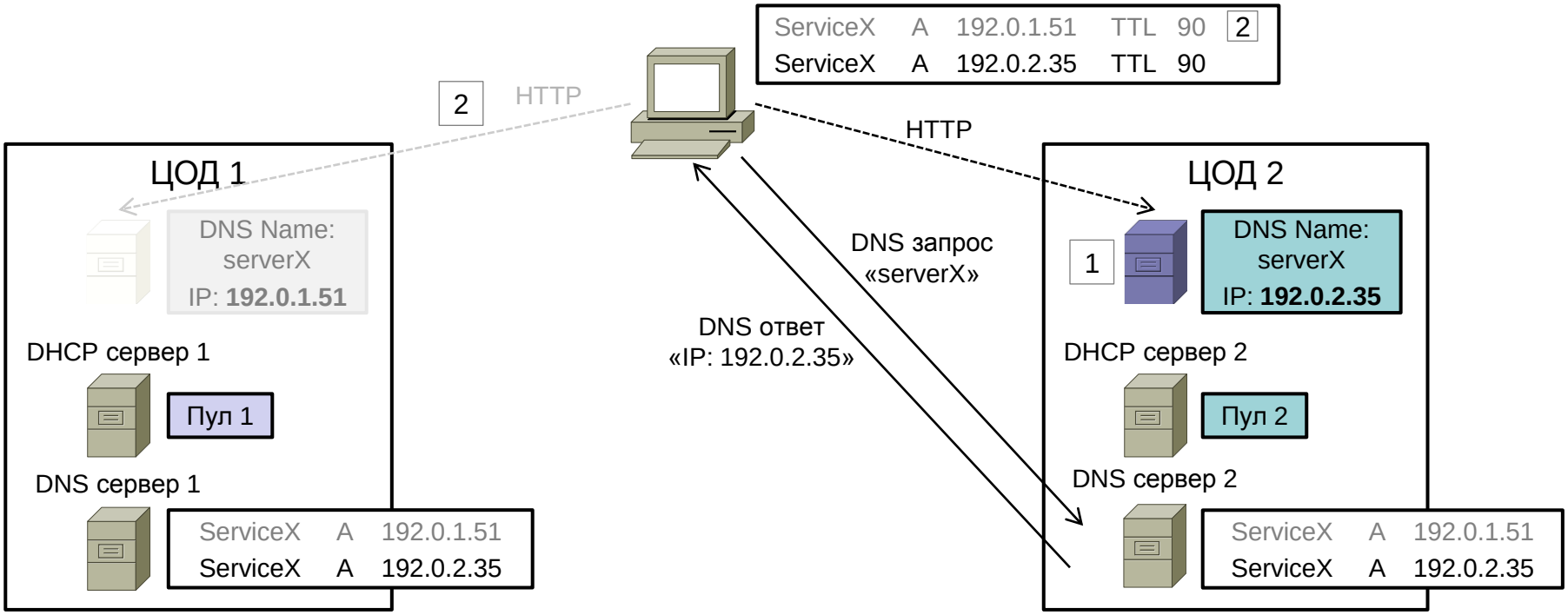
Динамическое обновление DNS (RFC 2136)

Записи DNS обновляет DHCP сервер:

- Не требуется редактировать записи DNS вручную
- Обновления происходят своевременно

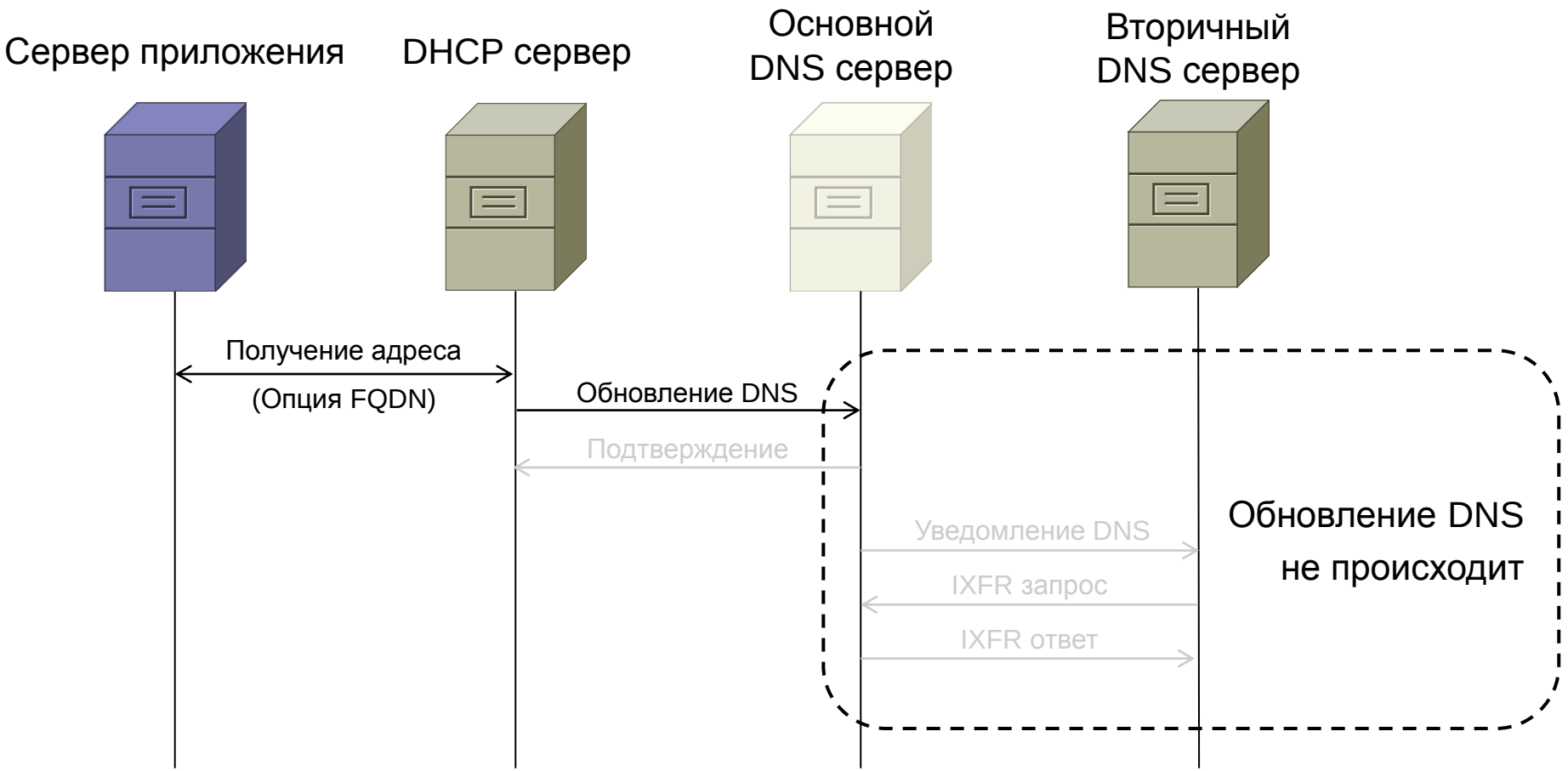


Локальное кеширование DNS



- Перезапуск сервера длится порядка минуты (1)
- Время жизни (TTL) для динамических записей следует задавать порядка минуты, иначе клиенты будут использовать устаревшую информацию (2)

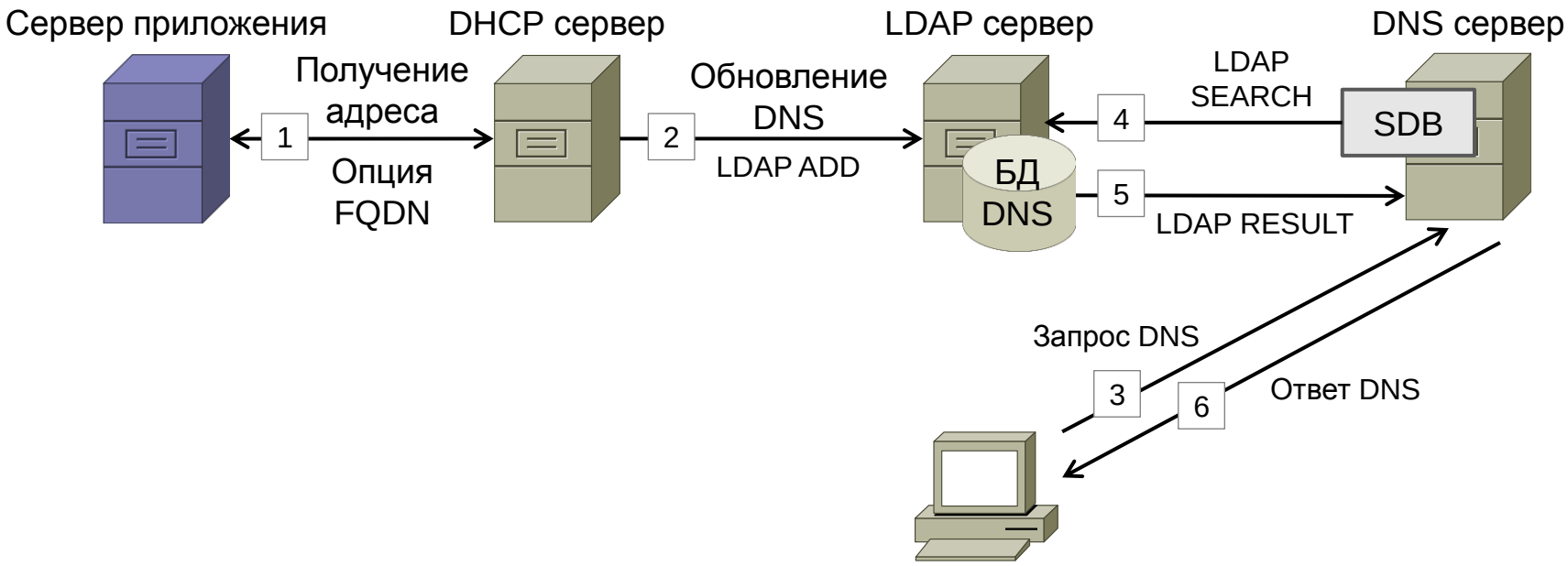
Отказ основного DNS сервера



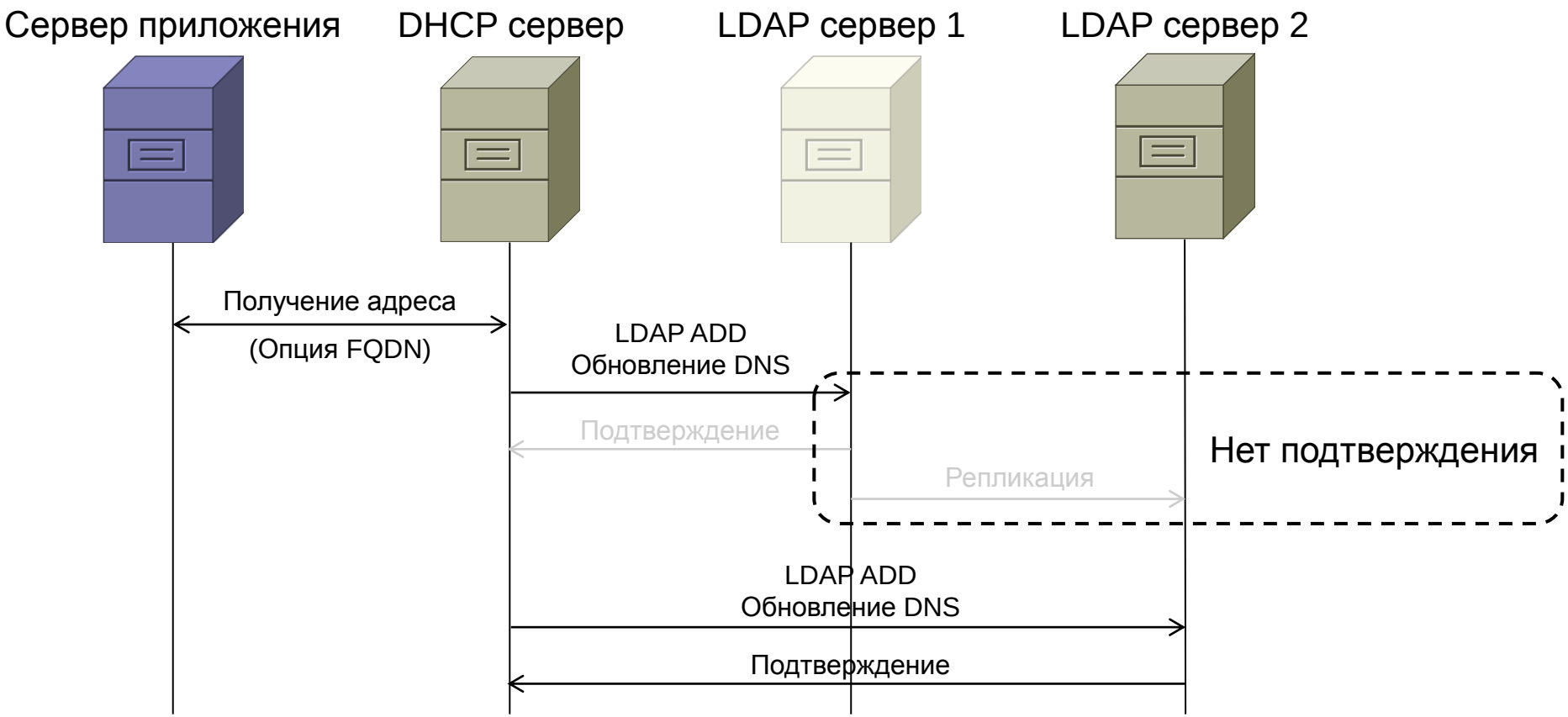
Новый сервер недоступен для клиентов по DNS имени

Интеграция DNS с LDAP

- Зоны DNS хранятся на сервере службы каталогов
- Сервер DNS использует программный интерфейс Simplified Database Backend для работы с LDAP

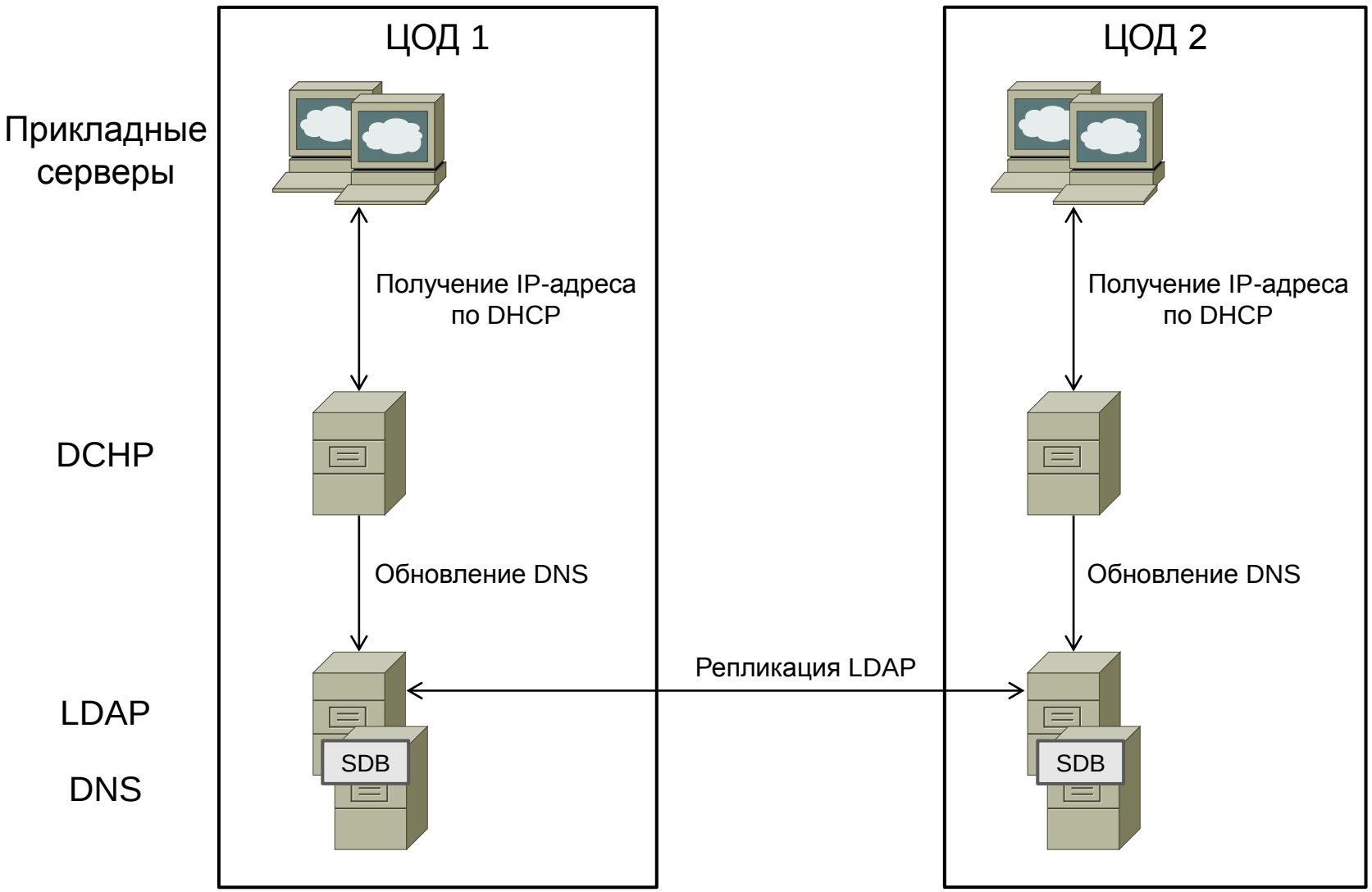


LDAP репликация динамических обновлений DNS



Обновления DNS не теряются

Итого


ЦОД 1
ЦОД 2
Прикладные серверы
Получение IP-адреса по DHCP
Получение IP-адреса по DHCP
DCHP
Обновление DNS
Обновление DNS
Репликация LDAP
LDAP
DNS
SDB
SDB

Анализ решения

- Не требуется L2 связность между ЦОДами
- После перезапуска сервера в другом ЦОДе клиенты могут обращаться к нему по DNS имени

Высокая доступность DHCP и DNS

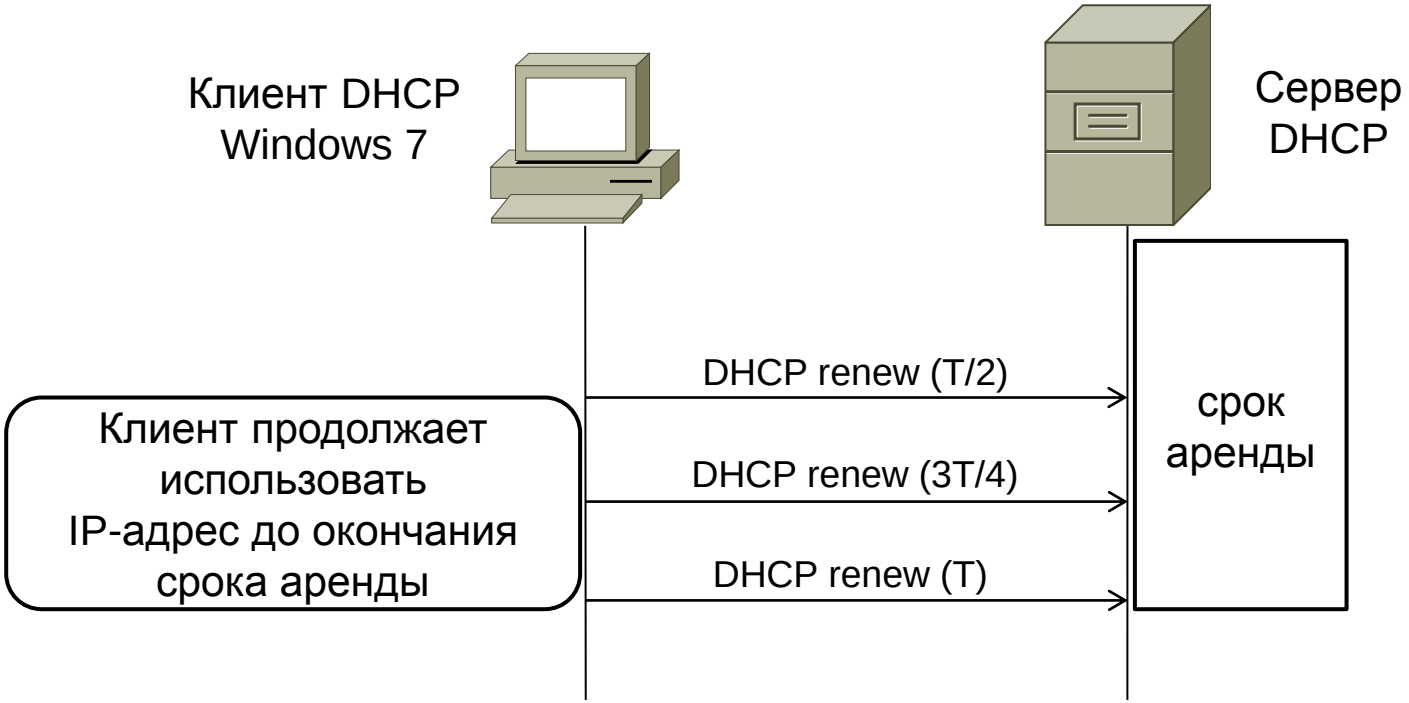
Вопросы?

Евгений Дрыбин

edrybin@solidex.by

Back Slides

Продление аренды



TCP соединение не разрывается

- Если клиенту удается продлить аренду за вторую половину срока (leasetime/2 > 30c), то он продолжает использовать IP-адрес на протяжение еще одного срока аренды
- => TCP соединение не является критерием для определения времени восстановления сервиса DHCP

Relay Agent и DHCP Failover

Solidex

- DHCP Relay Agent необходимо настроить пересылать пакеты на оба сервера
- Большинство реализаций DHCP Relay Agent позволяют такое дублирование пакетов