УДК 004.047

О.В.Копейка

*Государственный университет телекоммуникаций, Киев*

# СЕТЕВЫЕ СЛУЖБЫ И СЛУЖБА СЕТЕВЫХ УСТРОЙСТВ В ДАТА-ЦЕНТРАХ

*В статье рассмотрены вопросы формирования сетевых служб (DNS, DHCP, WINS) и службы сетевых устройств (маршрутизаторы, коммутаторы, балансировщики нагрузки и т.д.), которые являются типовыми для корпоративных Дата-центров.*

***Ключевые слова:*** *маршрутизаторы, коммутаторы, балансировщики нагрузки, службы сетевых устройств, сетевые службы.*

## Вступление

Службы сетевых устройств (маршрутизаторы, коммутаторы, балансировщики нагрузки и т.д.) обеспечивают построение защищенной корпоративной сети, в которой функционируют мультисервисные услуги (электронный документооборот, доступ в Интернет, IP-телефония, видеоконференции). Выход в Интернет в этом случае обеспечівается только через центральный центр обработки данных (ЦОД).

Корпоративная сеть Корпорации состоит из:

1. Транспортных составляющих ЦОД, офисов и департаментов.

2. Сервисов VPN публичной сети передачи данных Корпорации, обеспечивающих транспортировку информации между ними.

В разделе формирования сетевых служб будем рассматривать организацию базовых сетевых служб: Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Windows Internet Name Service (WINS).

Надежное обеспечение идентификации для узлов сети обеспечивает высокую доступность всех ИТ сервисов.

## Основная часть

Предварительным условием построения корпоративной сети является наличие у Корпорации публичной сети MPLS, обеспечивающей реализацию виртуальных частных сетей (VPN) одного из выбранных уровней – Layer2 (L2 VPN) или Layer3 (L3 VPN).

Концепция связности может быть одной из двух нижеперечисленных:

1. Звезда (L2 VPN) – каждый офис или департамент включен Ethernet-соединениями в один или два ЦОД (взаимодействие между офисами внутри региона запрещено). Минусами данной схемы являются:

- неоптимальная маршрутизация трафика;
- более сложная и более дорогая реализация;
- больший процент служебной информации (overhead) в трафике.

Плюсом данной схемы является больший контроль за трафиком, поскольку он весь концентрируется в ЦОД.

2. Полносвязная схема (L3 VPN) – трафик офисов и департаментов маршрутизируется в публичной сети на пути к ЦОД (как минимум, на региональном и регионально-транзитном уровне). Потенциально, все офисы, департаменты и ЦОД могут взаимодействовать друг с другом напрямую.

По сравнению с L2 VPN плюсы обращаются в минусы и наоборот.

Необходимо отметить, что при реализации любой из этих концепций выход в Интернет будет только один – на центральном узле, защищенном от внешних атак файрволлом.

Мы не рассматриваем принципы построения магистральной сети – протоколы транспорта и маршрутизации, отказоустойчивость и т.д.

**Службы сетевых устройств**

Транспортные задачи, которые выполняет ЦОД:

1. Обеспечение отказоустойчивого включения в публичную сеть.

2. Обеспечение безопасного доступа к Интернет (только центральный ЦОД).

3. Агрегацию точечных включений (в случае использования L2 VPN).

Общая схема построения транспортной составляющей ЦОД приведена на рис. 1.

Ядром ЦОД является пара коммутаторов Catalyst серии 6500, которые комплектуются центральным процессором Sup720-3B и модулями защиты корпоративной сети (Firewall Service Module (FWSM) и Intrusion Prevention System (IPS)). При этом и FWSM, и IPS функционируют в прозрачном (transparent) режиме, что позволяет скрыть факт фильтрации и анализа трафика и упростить его обработку внутри коммутатора. Отказоустойчивость решения обеспечивает использование протокола VRRP (Virtual Router Redundancy Protocol),

включенного как в сторону транспортной сети, так и в сторону локальной сети.

Интерфейс включения в MPLS Backbone – Gigabit Ethernet, внутри центрального узла – 100/1000Mbps. Абоненты локальной сети включаются в коммутаторы серии Catalyst 3560 – фиксированные коммутаторы класса Enterprise.

**Сеть офиса или департамента**

Задачи, которые решает транспортная составляющая регионального ЦОД, включают в себя:

1. Реализацию шлюза в корпоративную сеть.
2. Защиту локального офиса от атак, порожденных внутри корпоративной сети.

Общая схема приведена на рис. 2.

Интерфейс включения удаленного офиса или департамента – 10/100Mbps Ethernet.

Интерфейс включения департамента, находящегося в непосредственной близости к ЦОД – 1000Mbps Ethernet.

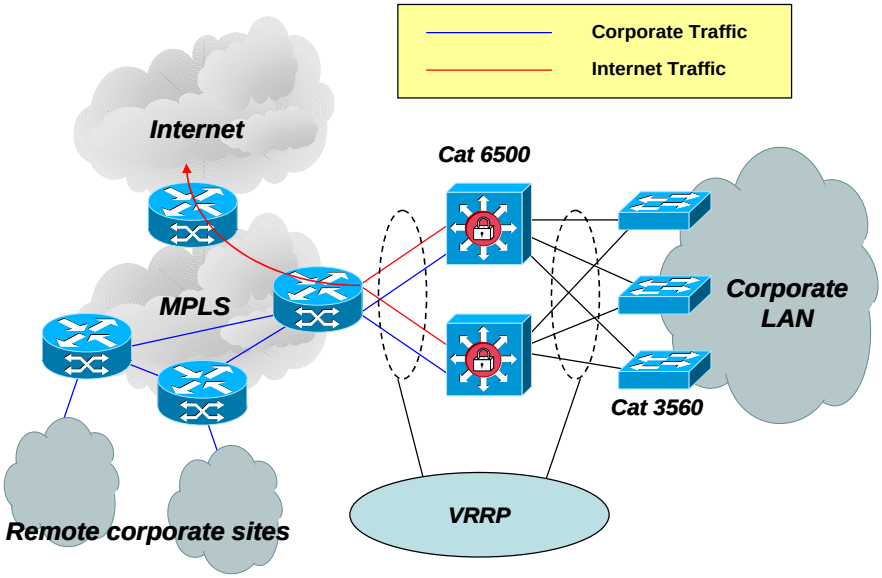


Рис. 1. Схема построения сети ЦОД в Корпорации

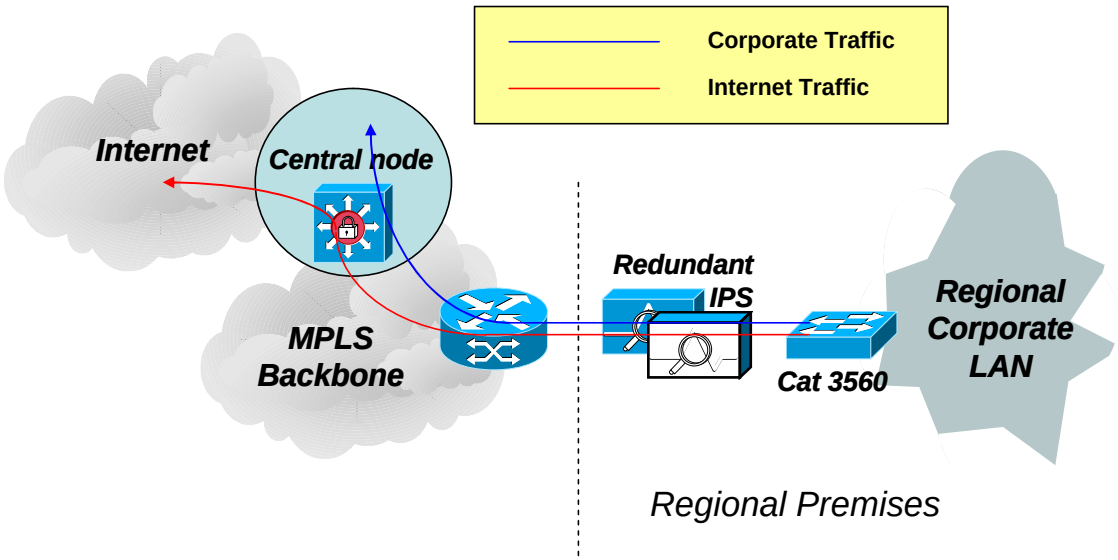


Рис. 2. Схема построения сети офиса или департамента в Корпорации

Отсутствие пакетных файрволлов в региональном офисе определяется тем, что шлюз в Интернет (на центральном узле) защищен таким оборудованием и, соответственно, возможность злонамеренных действий извне исключена. А применение Intrusion Prevention Sustem (IPS) целесообразно для защиты внутренней сети компании от атак, порожденных внутри корпоративной сети (например, программ-троянов, заразивших какой-либо служебный компьютер).

Поскольку политика безопасности определяется службой безопасности компании, то подбор оборудования должен производиться на основании этой политики и может включать в себя как пакетные фильтры, так и системы предотвращения атак.

**Физическая реализация сети ЦОД**

Сеть центра обработки данных должна отвечать следующим требованиям:

1. Надежность – критичные узлы должны быть зарезервированы.

2. Высокая производительность.

3. Защищенность – сервера, размещенные в датацентре, должны быть защищены от:

- атак из Интернета (файрволлом, системой предотвращения атак);

- перегрузки трафиком (системой балансировки нагрузки).

Исходя из этих требований, схема построения сети центра обработки данных приведена на рис. 3.

**Уровень агрегации**

Выполняется на коммутаторах Catalyst 6500 с центральным процессором Sup720-3B, обеспечивающими пропускную способность до 30Mpps. Каждый из коммутаторов комплектуется следующими модулями:

1. Firewall (FWSM).

2. Intrusion Prevention System (IDSM-2).

3. Content Switching Module (CSM).

Эти модули могут обслуживать различные группы серверов, обеспечивая таким образом максимальную гибкость для предоставления сервисов.

Для включения в Core Network могут быть использованы как 1Gbps, так и 10Gbps порты. Включение в опорную сеть – резервируемое.

В общем случае, последовательность прохождения трафика через коммутатор соответствует приведенному выше порядку перечисления модулей:

1. Firewall FWSM - отсеивание изначально нежелательного трафика.

2. Intrusion Prevention System IDSM-2 - анализ и отсеивание более сложных атак.

3. Content Switching Module CSM - балансировка рабочего трафика между серверами дата-центра.

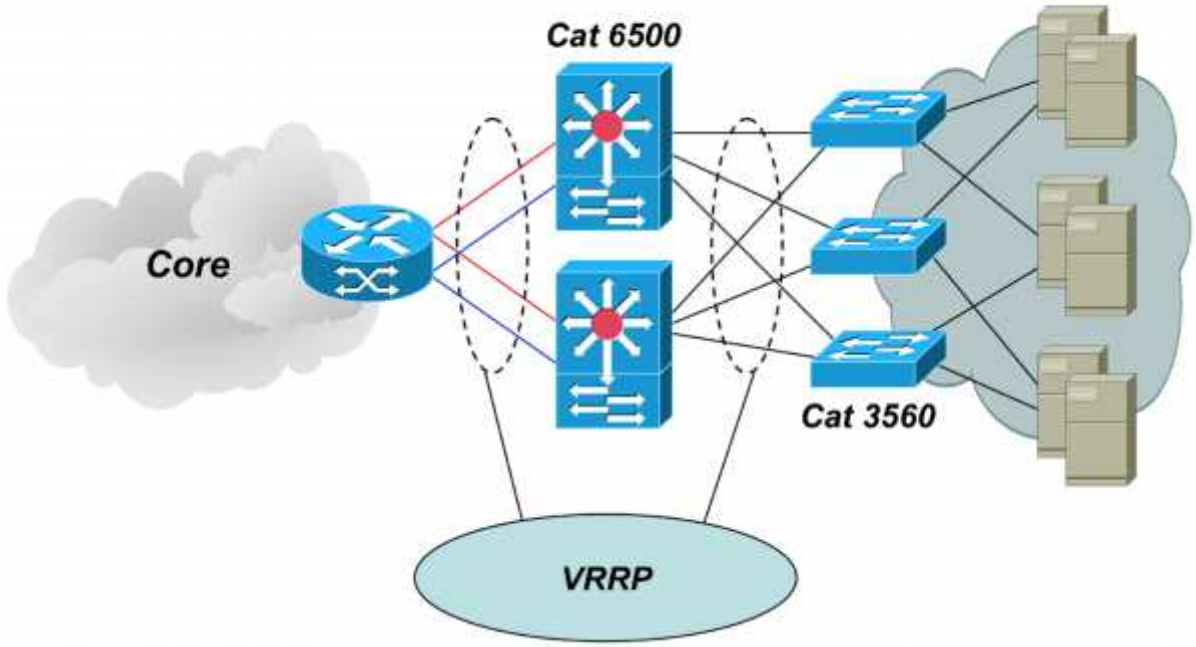


Рис. 3. Уровни в сети ЦОД в Корпорации

В схеме присутствуют два уровня.

**Уровень доступа**

Выполнен на коммутаторах серии Catalyst 3560 (производительность – от 7Mpps до 39Mpps), обеспечивающих высокую концентрацию портов для подключения серверов дата-центра. Включение в уровень агрегации – резервируемое, для обеспечения надежной связи с опорной сетью.

**Дополнительные меры по обеспечению безопасности сети центра обработки данных и корпоративной сети в целом**

Существует ряд атак, которые в последнее время находят все большее применение и при этом не могут быть отфильтрованы упомянутыми ранее средствами (пакетный файрволл и система предотвращения атак). Это – так называемые Denial of Service (а также – Distributed DoS) атаки. Целью такой атаки является не взлом системы для получения какой-либо информации, а приведение узла (или совокупности узлов) к неработоспособному состоянию – путем или перегрузки процессора, или полного исчерпания канальной емкости, соединяющей узел с сетью.

Во избежание подобного рода атак применяется специальная система Cisco Guard, состоящая из двух компонентов:

1. Cisco Detector – самообучающееся устройство, анализирующее поток трафика и при появлении каких-либо аномалий принимающее решение о начале атаке.

2. Cisco Guard – устройство, пропускающее через себя поток трафика, которое отсекает трафик атаки и передает на узел назначения рабочий трафик.

Схема работы комплекса показана на рис. 4.

В нормальном состоянии трафик проходит напрямую между Интернет и корпоративной сетью (или дата-центром), но при этом он постоянно анализируется устройством Cisco Detector. Если это устройство замечает какую-либо аномалию, оно дает команду на Cisco Guard и тот заворачивает весь трафик, предназначенный атакуемому узлу на себя, отфильтровывает трафик атаки, а рабочий трафик – отправляет по назначению.

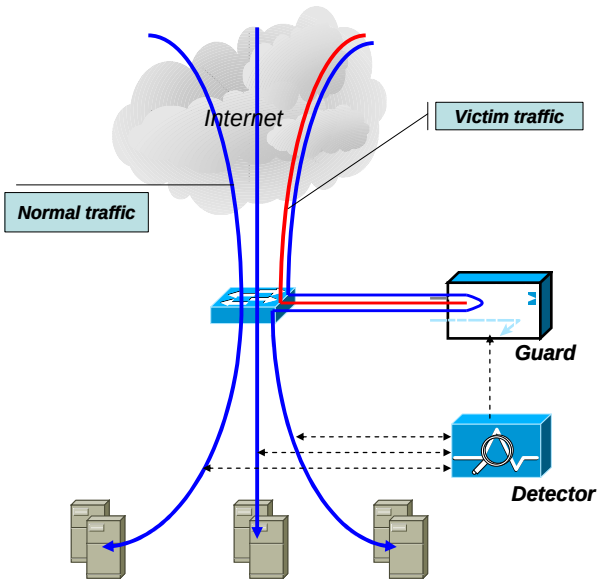


Рис. 4. Контроль траффика в корпоративной сети в Корпорации

Далее рабочий трафик будет проверен системами безопасности, перечисленными ранее (FWSM и IDSM-2), и передан тому серверу, которому предназначался.

Таким образом обеспечивается комплексная защита узла от всех видов атак, включая атаки Denial of Service, что позволяет предоставить бесперебойное функционирование всех служб, размещенных на узле.

## Сетевые службы

Данный раздел рассматривает организацию базовых сетевых служб: Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Windows Internet Name Service (WINS).

Надежное обеспечение идентификации для узлов сети обеспечивает высокую доступность всех ИТ сервисов.

**Сервис DNS**

DNS сервис представляет собой иерархически организованную базу данных обеспечивающую разрешение доменных имен в IP адреса и наоборот. Служба DNS используется в том числе для:

1. Поиска сервисов аутентификации и контролеров доменов.
2. Поиска сервисов приложений.
3. Поиска партнеров для репликации данных.
4. Поиска адресов Интернет ресурсов.

**Логическая организация сервиса**

Рассмотрим организацию сервиса DNS Корпорации на примере ПАТ «Укртелеком», где поддерживается 5-ть доменов имен. Четыре домена имен зарегистрированы в сети Интернет: ukrtelecom.net, ukrtel.net, ukrpost.net и ukrtelecom.ua.

**Первый домен является корневым доменом службы каталогов, однако используется только для хранения ограниченного числа записей (контролеры доменов, MX запись, и запись администратора зоны). Второй, третий и четвертый домены используются для доступа к Интернет сервисам ЦОД.**

**Пятый домен ПАО «Укртелеком» corp.ukrtelecom.net является подчиненным Ukrtelecom.net** и содержит все записи об узлах и сервисах корпоративной сети.

Для обеспечения высокого уровня защиты DNS сервиса, сервера поддерживающие домен ukrtelecom.net разделены на три группы (Split-Split DNS model):

1. Сервера DNS домена Ukrtelecom.net, которые находятся в зоне периметра и обслуживают внешние запросы – advertisers. Они не поддерживают рекурсию и поддерживают ограниченный набор запросов.
2. Сервера DNS домена Ukrtelecom.net, которые находятся в зоне периметра и обслуживают внутренний запросы от внутренних серверов DNS – resolvers.
3. Сервера DNS Ukrtelecom.net которые обслуживают только внутренних клиентов и находятся в зоне Инфраструктурных ИТ сервисов.

DNS сервис внутренних доменов ukrtelecom.net и corp.ukrtelecom.net интегрирован в сервис Active Directory. Каждый сервер контролера домена является сервером DNS. Такая модель обеспечит следующие преимущества:

1. Автоматизация операций путем интеграции с DHCP.
2. Защищенная и быстрая репликация зон.
3. Оптимизация нагрузки на сеть.
4. Репликация с множеством мастеров зон.
5. Контроль доступа у каждой из DNS записей.
6. Автоматическое резервирование.
7. Упрощенное эксплуатирование.

Рабочие станции и устройства пользователей будут получать информацию о DNS серверах из трех источников:

1. Все узлы сети, которые находятся в зоне пользователей обслуживаются службой DHCP.
2. Резервная система назначения IP конфигурации - Active Directory Group Policy.
3. Все браузеры получают конфигурационную информацию в INF, Web Proxy AutoDiscovery (WPAD), или PAC файлах. Таким образом количество запросов на разрешение Интернет адресов на внутренние DNS сервера минимально.

## Физическая организация

### Серверное обеспечение

Четыре сервера в каждом из 7 опорных ЦОД. Сервера двух процессорные с 1 Гб памяти и 8 Гб дискового пространства. Шесть серверов в Интернет Дата Центре, в зоне периметра. Сервера двух процессорные с 1 Гб памяти и 4 Гб дискового пространства. Модель сервера уровня - HP DL380.

Один DNS сервер на базе Windows Server 2003 способен обрабатывать 10 000 запросов в секунду на процессоре Pentium III 700 Мгц и поддерживать 200 000 зон с шестью записями каждая.

### Коммуникационная сеть

В ЦОД настраиваются:

1. Коммутатор Внутренней Интеграции – используются функции VLAN и Firewall.
2. Центральный Коммутатор ЦОД – используются функции VLAN и Firewall.
3. Коммутатор Периметра – используются функции VLAN и Firewall.
4. Оборудование Границы сети.

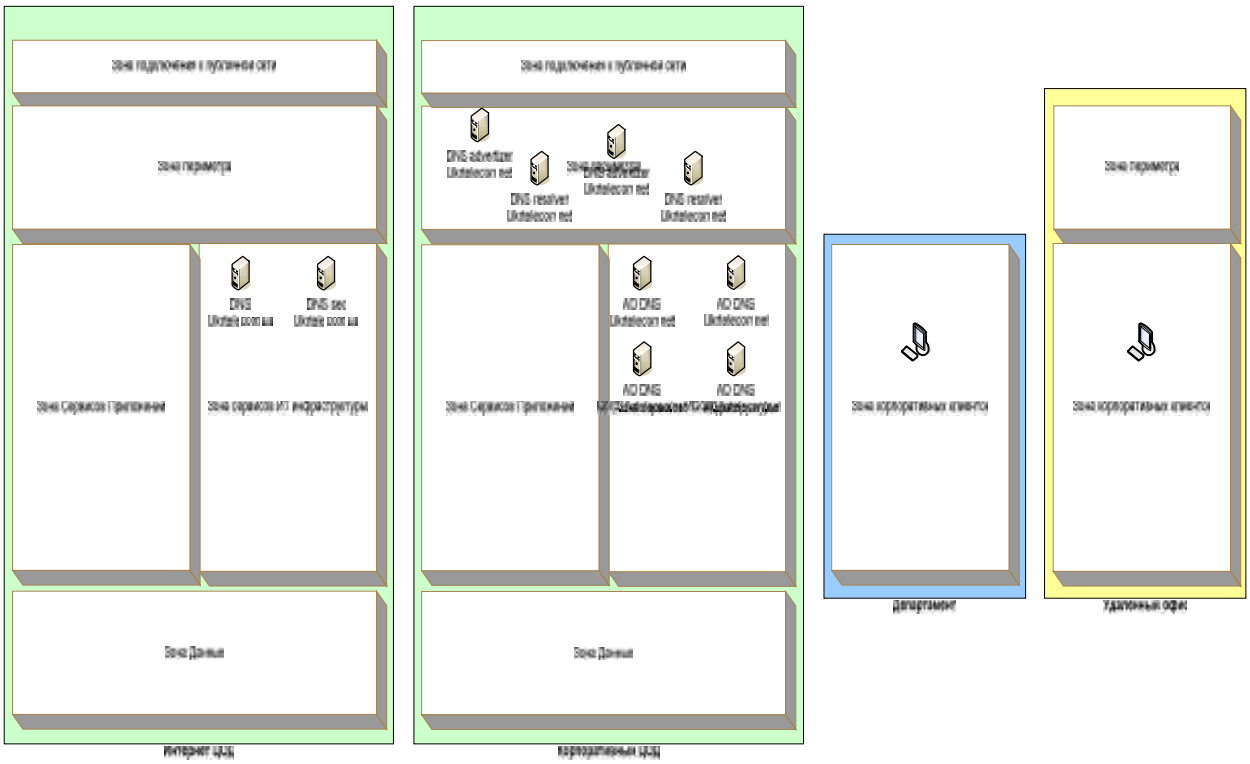


Рис. 6. Организация сервиса поддержки пространства доменных имен в ПАО «Укртелеком»

### Доступность

Доступность обеспечивается дублированием серверных компонентов. Клиенты получают по 2 адреса DNS сервера посредством службы DHCP.

### Безопасность

Протокол сервиса DNS разрабатывался как открытый и поэтому требуется отдельно рассматривать конфигурацию DNS в ЦОД и Интернет ЦОД. Внутренний DNS сервер разделяется на три составляющих: advertiser, resolver, core DNS, каждая из которых дублируется.

Внешний DNS организован по упрощенной схеме.

**Масштабируемость**

При необходимости DNS служба наращивается горизонтально, путем добавления серверов и внедрение NLB кластеризации.

**Управление**

Инструментарий управления – графический на базе консоли MMC и командный на базе **dnscmd** оболочки.

За эксплуатацию DNS отвечает согласно MOF роль – DNS owner.

Администратор отвечает за выполнение следующих функций:

1. Управление учетными записями и пуском системы.
2. Создание метрик производительности и отчетов.
3. Управление сетевыми операциями и сервисом каталога.
4. Создание и управление пользовательскими учетными записями и разрешениями.
5. Управление эксплуатацией службы каталога.
6. Управление защитой службы DNS.
7. Поддержка базы данных DNS.

**Консолидация**

Служба DNS консолидируется со службой каталога.

**Сервис DHCP**

Сервис DHCP обеспечивает назначение адресов и параметров IP протокола на пользовательские устройства в ИТ инфраструктуре.

**Логическая организация**

DHCP сервис обслуживает только системы из зон Корпоративных клиентов. Системы в ЦОД имеют статическую IP конфигурацию.

Организация параметров DHCP scope включает:

1. Длительность аренды – 16 дней.
2. Scope, Server, Class и Reservation параметры включают в себя обязательно – routers, DNS servers, DNS domain, WINS node type, WINS server.

DHCP сервис в Центре Обработки Данных организован в качестве отказоустойчивого кластера. Для работы в маршрутизируемых сетях используются DHCP relay agents. Каждая подсеть должна иметь по 2 relay агента. В качестве резервного варианта предлагается рассмотреть возможность активации опции DHCP Forwarding на маршрутизаторах.

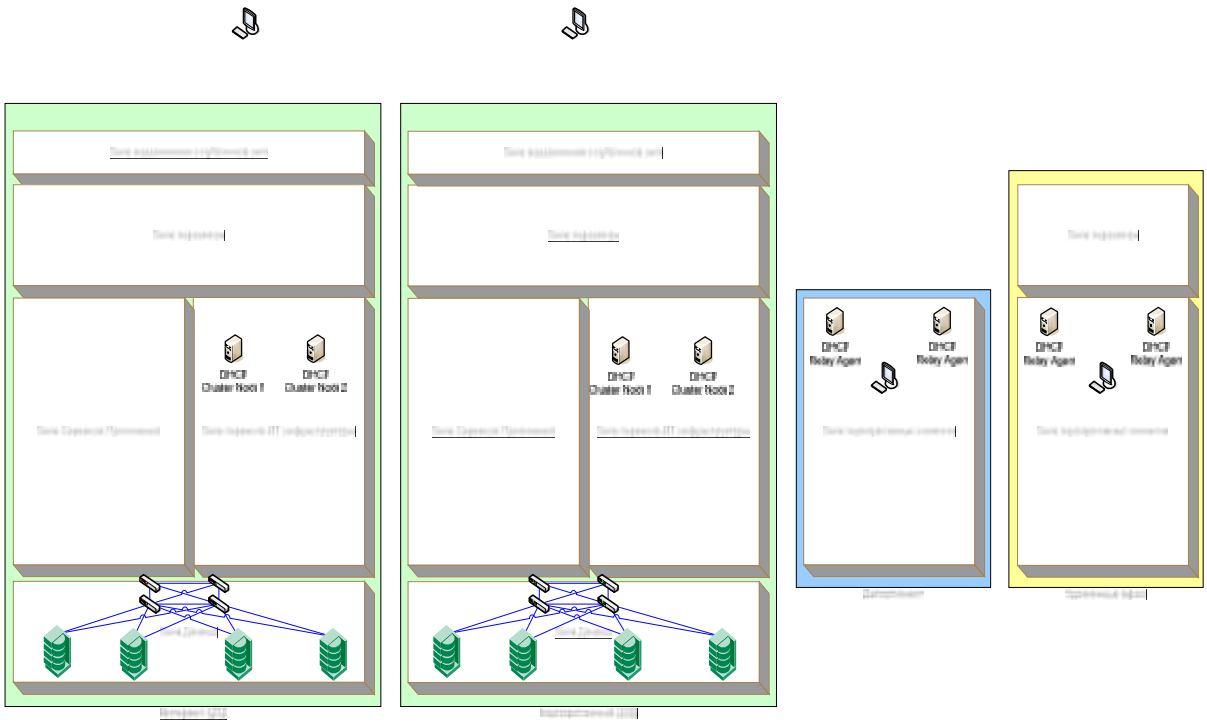

Рис. 7. Организация сервиса DHCP в ПАО «Укртелеком»

### Физическая реализация

**Серверное обеспечение**

Два сервера объединенных в кластер в каждом из 7 опорных ЦОД. Сервера двух процессорные с 1Гб памяти и 8 Гб дискового пространства. Два сервера (кластер) в каждом из двух Интернет Дата Центров, в зоне ИТ инфраструктуры. Сервера двух процессорные с 1 Гб памяти и 4 Гб дискового пространства. Модель сервера уровня - HP DL380.

**Сеть хранения данных**

Используется для хранения базы данных IP адресов. Поэтому сервера DHCP оборудованы двумя HBA адаптерами для подключения к сети хранения данных.

**Коммуникационная сеть**

В ЦОД настраиваются:

1. Коммутатор Внутренней Интеграции – используются функции VLAN и Firewall.
2. Центральный Коммутатор ЦОД – используются функции VLAN и Firewall.
3. Коммутатор Периметра – используются функции VLAN и Firewall.
4. Оборудование Границы сети.

Для исключения широковещательного трафика в сетях корпоративных клиентов, устанавливаются DHCP relay агенты.

**Доступность**

Доступность обеспечивается с помощью fail-over кластеризации и дублированием элементов сети хранения данных.

## Выводы

При организации службы сетевых устройств обеспечивается построение защищенной корпоративной сети, в которой функционируют мультисервисные услуги (электронный документооборот, доступ в Интернет, IP-телефония, видеоконференции). Выход в Интернет в этом случае обеспечивается только через центральный ЦОД. Таким образом обеспечивается комплексная защита узла от всех видов атак, включая атаки Denial of Service, что позволяет предоставить бесперебойное функционирование всех служб, размещенных на узле.

В разделе формирования сетевых служб рассмотрено организацию базовых сетевых служб:

1. Domain Name System (DNS) и Windows Internet Name Service (WINS). При этом, обеспечивается:

- **Доступность.** Доступность обеспечивается дублированием серверных компонентов. Клиенты получают по 2 адреса DNS сервера посредством службы DHCP.
- **Безопасность.** Протокол сервиса DNS разрабатывался как открытый и поэтому требуется отдельно рассматривать конфигурацию DNS в ЦОД и Интернет ЦОД. Внутренний DNS сервер разделяется на три составляющих: advertiser, resolver, core DNS, каждая из которых дублируется. Внешний DNS организован по упрощенной схеме.
- **Масштабируемость.** При необходимости DNS служба наращивается горизонтально, путем добавления серверов и внедрение NLB кластеризации.
- **Управление.**Инструментарий управления – графический на базе консоли MMC и командный на базе **dnscmd** оболочки.
- **Консолидация.** Служба DNS консолидируется со службой каталога.

2. Dynamic Host Configuration Protocol (DHCP). При этом, обеспечивается:

- **Доступность.** Доступность обеспечивается с помощью fail-over кластеризации и дублированием элементов сети хранения данных.

## Список литературы

*1. Еталонні архітектури MSA. – К.: Майкрософт Україна; К.: Видавнича група BHN, 2005. – 352 с.*

*2. Засади регіональної інформатизації/ Довгий С.О., Копійка О.В., Черепін Ю.Т.- К.:ВПЦ «ТИРАЖ», 2004.-304с.*

*3. Новые технологии в телекоммуникации: выбор технологической архитектуры. Современные тенденции развития/ С.А.Довгий, О.В.Копейка, С.П.Поленок. – К.:Укртелеком,2001.- 281 с.*

4. *O.Kopeika, I.Tarasenko, A.Kisselevskiy, A.Karichenskiy, T.Valiulin Softline applies TMF standards as a guide when building Resource Inventory solution for nation-wide carrier Ukraine Telecom// TM Forum Case Study Handbook, Volume* 3, May 2007 – S. 27

*5. http://www.tiaonline.org/standards/*

*6. Jew, Jonathan. BICSI Data Center Standard: A Resource for Today's Data Center Operators and Designers // BICSI News Magazine, May/June 2010- page 28.*

*7. Niles, Susan. Standardization and Modularity in Data Center Physical Infrastructure // 2011, Schneider Electric – page 4.*

*Поступила в редакцию 14.11.2013*

**Рецензент:** д-р техн. наук, проф. Л.Н.Беркман, Государственный университет телекоммуникаций, Киев.

**МЕРЕЖЕВІ СЛУЖБИ І СЛУЖБА МЕРЕЖЕВИХ ПРИСТРОЇВ В ДАТА-ЦЕНТРАХ**

О.В. Копійка

*У статті розглянуті питання формування мережевих служб (DNS, DHCP, WINS) і служби мережевих пристроїв (маршрутизатори, комутатори, балансувальники навантаження і т.п.), які є типовими для корпоративних Дата-центрів.*
***Ключові слова:*** *маршрутизатори, комутатори, балансувальники навантаження, служби мережевих пристроїв, мережеві служби.*

**NETWORK SERVICES AND NETWORK DEVICES SERVICE IN THE DATA CENTER**

O.V. Kopiyka

*The article studies the matters of network services formation (DNS, DHCP, WINS) and network devices services (routers, switches, load balancers, etc.), which are typical for corporate data centers.*
***Keywords:*** *routers, switches, load balancers, network devices services, network service.*