**4. СИМВОЛЬНАЯ АДРЕСАЦИЯ В СЕТЯХ С КЛИЕНТ-СЕРВЕРНОЙ АРХИТЕКТУРОЙ**

**4.1. Символьный адрес DNS**

В стеке протоколов TCP/IP, как уже ранее говорилось, используются три типа адресов – физические, IP-адреса и символьные доменные имена. Физические адреса служат для адресации на канальном уровне. IP-адреса применяются на сетевом уровне. Доменные имена кажутся в этом ряду необязательными, ведь сеть будет работать и без них. Однако пользователю сети неудобно запоминать числовые IP-адреса, ассоциируя их с конкретными сетевыми объектами. Все привыкли к символьным именам, и именно поэтому в стек TCP/IP была введена система доменных имен DNS (Domain Name System). Она описывается в RFC 1034 и RFC 1035. Полное название доменных имен – FQDN (Fully Qualified Domain Name – полностью определенное имя домена). Кроме DNS-имен операционные системы Windows Server поддерживают символьные имена NetBIOS.

*DNS* (*Domain Name System*) – это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet.

*Служба DNS* предназначена для автоматического поиска IP-адреса по известному символьному имени узла. DNS требует статической конфигурации своих таблиц, разрешающих имена компьютеров в IP-адреса.

*Протокол DNS* является служебным протоколом прикладного уровня. Этот протокол несимметричен – в нем определены DNS-серверы и DNS-клиенты.

*DNS-серверы* хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес. Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет – то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого *доменным пространством имен*, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены.

*Имя домена* идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

*Корень базы данных DNS* управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны отвечать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций применяются следующие аббревиатуры:

* *com* – коммерческие организации (например, microsoft.com);
* *edu* – образовательные (например, mit.edu);
* *gov* – правительственные организации (например, nsf.gov);
* *org* – некоммерческие организации (например, fidonet.org);
* *net* – организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой *домен* на *поддомены* и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим полным доменным именем (Fully Qualified Domain Name, FQDN), которое включает имена всех доменов по направлению от хоста к корню.

В процессе разрешения участвуют DNS-клиент и DNS-сервер. Системный компонент DNS-клиента, называемый DNS-распознавателем, отправляет запросы на DNS-серверы. Бывает двух видов:

* интерактивный – DNS-сервер обращается к DNS-серверу с просьбой разрешить имя без обращения к другим DNS-серверам;
* рекурсивный – всю работу по разрешению имени выполняет DNS-сервер путем отправки запросов другим DNS-серверам. DNS-сервер всегда сначала ищет имя в собственной базе данных или в кэше в случае отсутствия обращается к другим серверам.

В основном DNS-клиентами используются рекурсивные запросы. На рис. 4.1 проиллюстрирован процесс разрешения доменного имени с помощью рекурсивного запроса.

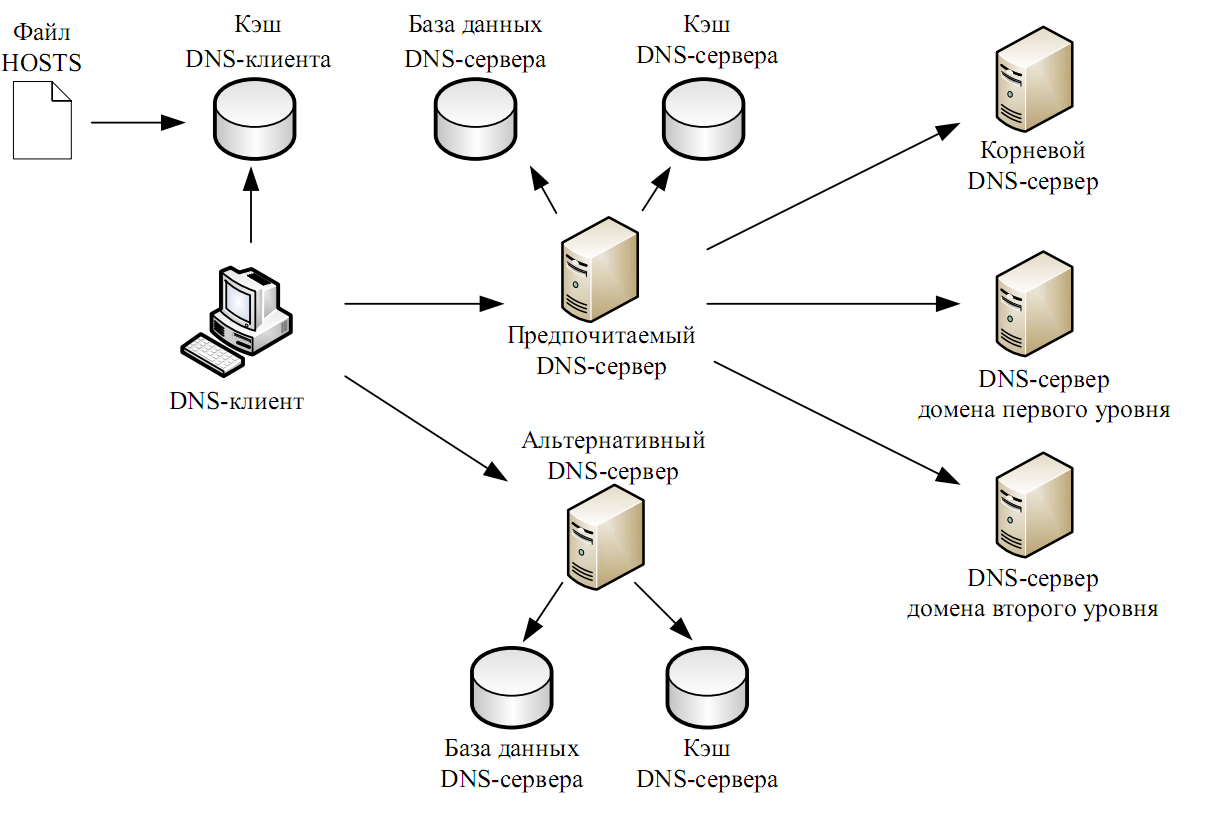
****

Рис. 4.1. Процесс рекурсивного разрешения имен

Сначала DNS-клиент осуществляет поиск в собственном локальном кэше DNS-имен. Это память для временного хранения ранее разрешенных запросов. В эту же память переносится содержимое файла hosts (каталог windows/system32/drivers/etc). Утилита IPconfig с ключом /displaydns отображает содержимое DNS-кэша. Если кэш не содержит требуемой информации, DNS-клиент обращается с рекурсивным запросом к предпочитаемому DNS-серверу (Preferred DNS server), адрес которого указывается при настройке стека TCP/IP. DNS-сервер просматривает собственную базу данных, а также кэш-память, в которой хранятся ответы на предыдущие запросы, отсутствующие в базе данных. В том случае, если запрашиваемое доменное имя не найдено, DNS-сервер осуществляет итеративные запросы к DNS-серверам верхних уровней, начиная с корневого DNS-сервера.

Рассмотрим процесс разрешения доменного имени на примере. Пусть требуется разрешить имя www.microsoft.com. Корневой домен содержит информацию о DNS-сервере, содержащем зону .com. Следующий запрос происходит к этому серверу, на котором хранятся данные о всех поддоменах зоны .com, в том числе о домене microsoft и его DNS-сервере. Сервер зоны microsoft.com может непосредственно разрешить имя www.microsoft.com в IP-адрес. Обращение к альтернативному серверу осуществляется, только если основной сервер недоступен.

Просмотр DNS-кэша осуществляется утилитой *ipconfig / displaydns*, очистка кэша – *ipconfig / flushdns*.

**4.2. Символьный адрес NETBIOS**

Протокол *NetBIOS* (Network Basic Input/Output System – сетевая базовая система ввода/вывода) был разработан в 1984 г. для корпорации IBM как сетевое дополнение стандартной BIOS на компьютерах IBM PC. В операционных системах Microsoft Windows NT, а также в Windows 98 протокол и имена NetBIOS являлись основными сетевыми компонентами. Начиная с Windows 2000, операционные системы Microsoft ориентируются на глобальную сеть Интернет, в этой связи фундаментом сетевых решений стали протоколы TCP/IP и доменные имена. Однако поддержка имен NetBIOS осталась и в операционной системе Windows Server 2008, а также Windows Server 2012.

*Система имен NetBIOS* представляет собой простое неиерархическое пространство, т. е. в имени NetBIOS отсутствует структура, деление на уровни, как в DNS-именах. Длина имени не более 15 символов (плюс один служебный).

Для преобразования NetBIOS-имен в IP-адреса в операционной системе Windows Server используется служба *WINS* – Windows Internet Naming Service (служба имен в Интернете для Windows).

Служба WINS работает, как и служба DNS, по модели клиент–сервер. WINS-клиенты используют WINS-сервер для регистрации своего NetBIOS-имени и преобразования неизвестного NetBIOS-имени в IP-адрес. Функции сервера NetBIOS-имен описаны в RFC 1001 и 1002.

Процесс разрешения имен в пространстве NetBios может быть выполнен одним из трех способов:

1. широковещательный запрос;
2. обращение к локальной базе данных NetBios-имен (LMhosts), хранящихся в папке, где файл hosts отображающий FQDN-имена;
3. обращение к централизованной базе данных имен NetBios, хранящихся на сервере WINS.

В зависимости от типа узла NetBios разрешение имен осуществляется с помощью различной комбинацией перечисленных способов. Выделяют четыре типа узла:

* b-узел (broadcast node, широковещательный) – разрешает имена в ip-адресах посредством широковещательных сообщений broadcast node;
* p-узел (peer node) – разрешает имена в IP-адреса с помощью WINS-сервера;
* m-узел (mixed node, смешанный узел) – комбинирует запросы b- и p-узлов, первоначально узел пытается применить широковещательный запрос, а в случае неудачи –обращается к WINS-серверу;
* h-узел (hybrid node*,* гибридный) – комбинирует запросы b- и p-узлов, но при этом сначала обращается к WINS-серверу, а при неудаче выполняет широковещательную рассылку.

Наиболее эффективным является h-узел. Тип узла определяется следующим образом: если в свойствах протокола TCP/IP нет адреcа WINS-сервера, то данный компьютер считается b-узлом, в противном случае является h-узлом. Использование других типов узлов настраивается через реестр Windows.

В больших сетях для распределения нагрузки по регистрации и разрешению NetBios-имен необходимо использовать несколько WINS-серверов. Считается, что один WINS-сервер должен обслуживать порядка нескольких сотен компьютеров. При использовании нескольких серверов часть клиентов настраивается на регистрацию и разрешение имен на один WINS-сервер, вторая – на другой, а между серверами, по аналогии с системой DNS, настраивается репликация.

**4.3. Настройка DNS-сервера**

Рассмотрим организацию DNS-адресации в локальной сети на примере Windows Server 2012 R2. Для организации DNS-адресации необходимо выполнить определенные действия на двух серверах (с именами Server1 и Server2) и клиенте.

*1. Установка DNS-сервера*

Установка службы DNS производится в целом аналогично установке DHCP-сервера, описанной ранее в подразделе 3.2 с той лишь разницей, что выбирается установка службы DNS.

*2. Создание основной зоны прямого просмотра*

На сервере DC1 создадим стандартную основную зону, например, с именем world.ru:

* откройте консоль DNS (рис. 4.2);
* выберите раздел *Forward Lookup Zones (Зоны прямого просмотра)* изапустите мастер создания зоны (тип зоны – *Primary (Основная)*, динамические обновления – *разрешить*, остальные параметры – по умолчанию) (рис. 4.3);

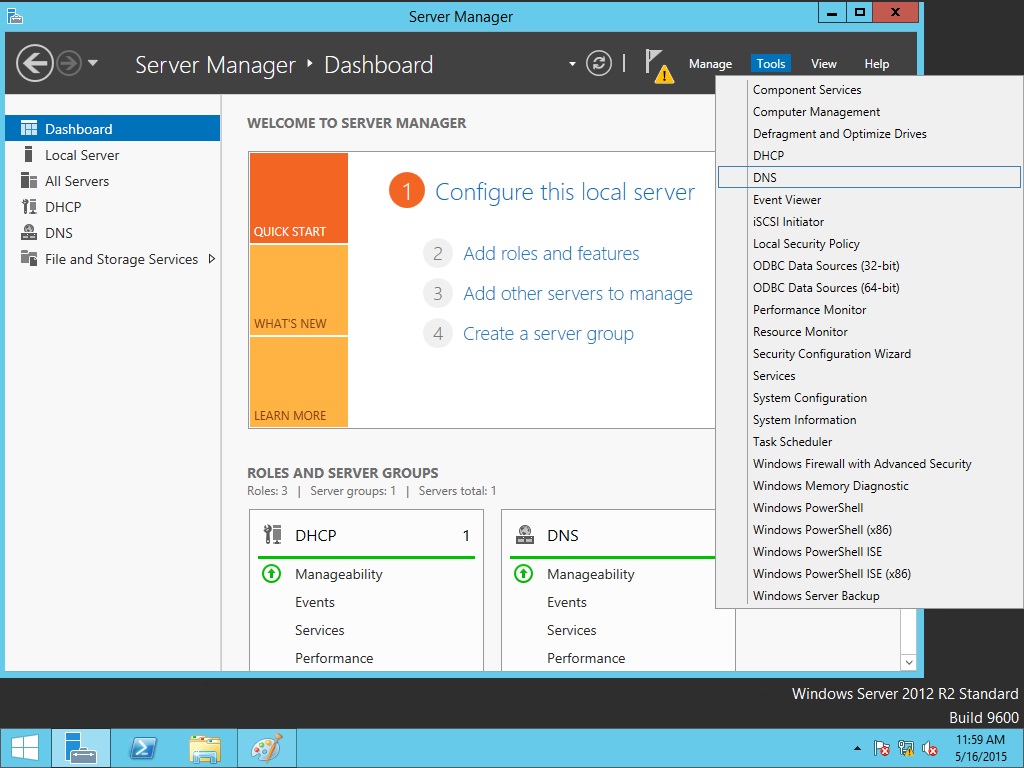


Рис. 4.2. Открытие консоли DNS-сервера

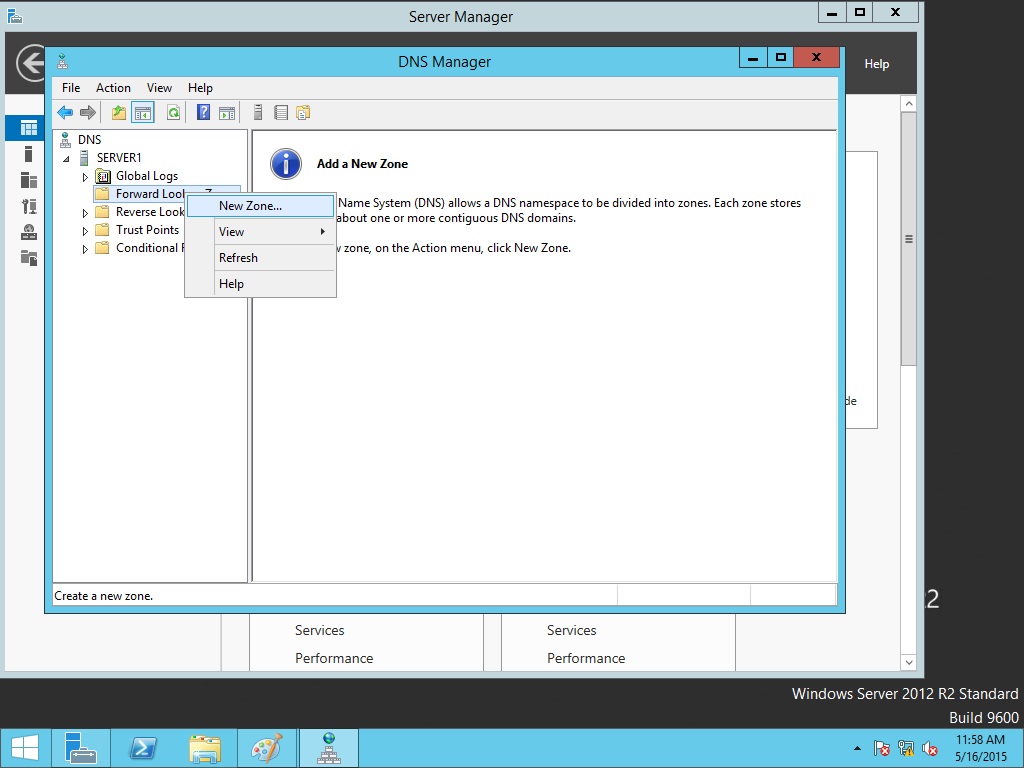


Рис. 4.3. Запуск мастера для создания новой зоны DNS-сервера

* введите тип зоны и имя – в примере используется название   
  local.by (рис. 4.4 и 4.5); имя файла, хранящего информацию о зоне, сформируется автоматически (рис. 4.6);

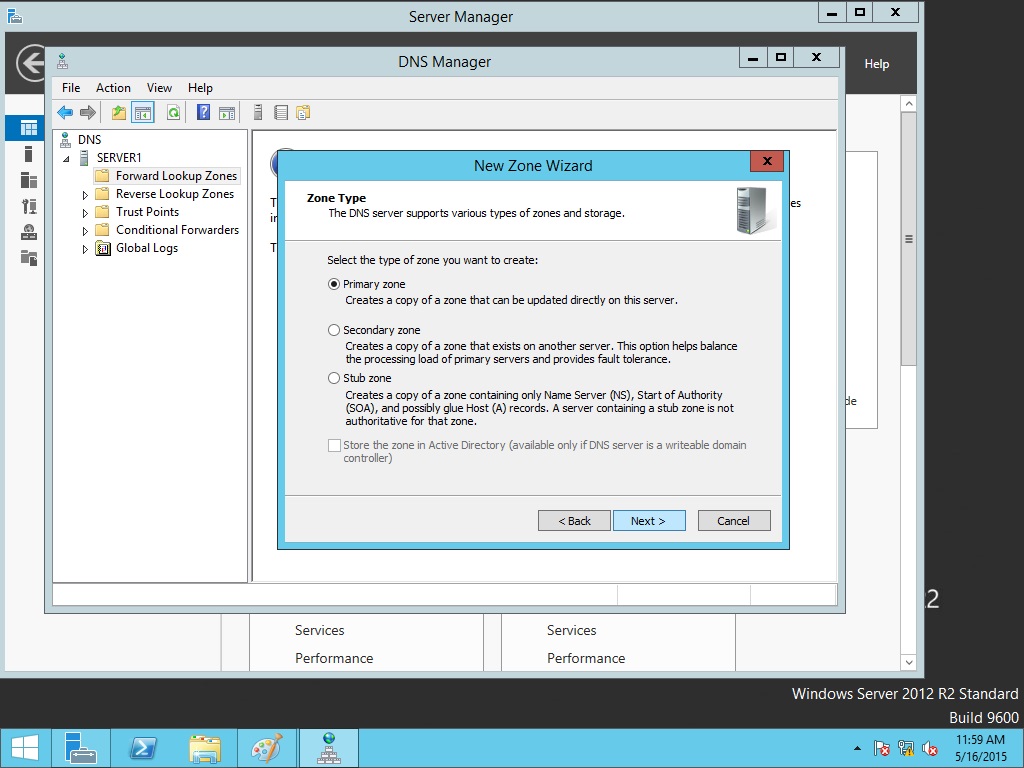


Рис. 4.4. Выбор типа новой зоны DNS-сервера

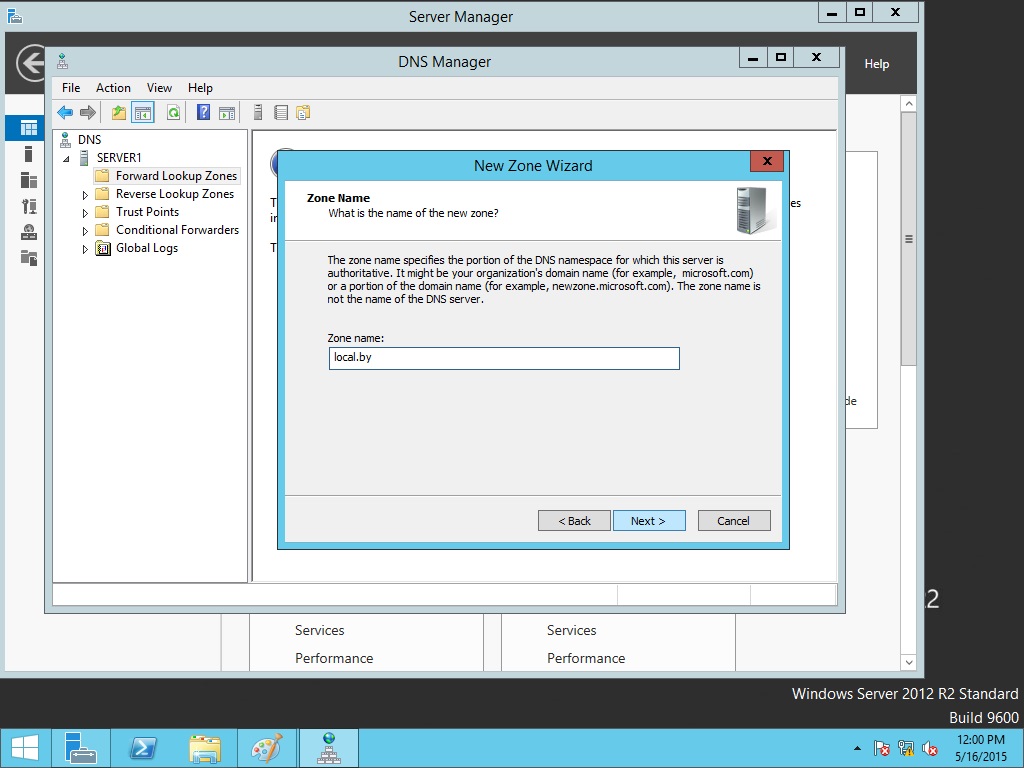


Рис. 4.5. Выбор названия новой зоны DNS-сервера

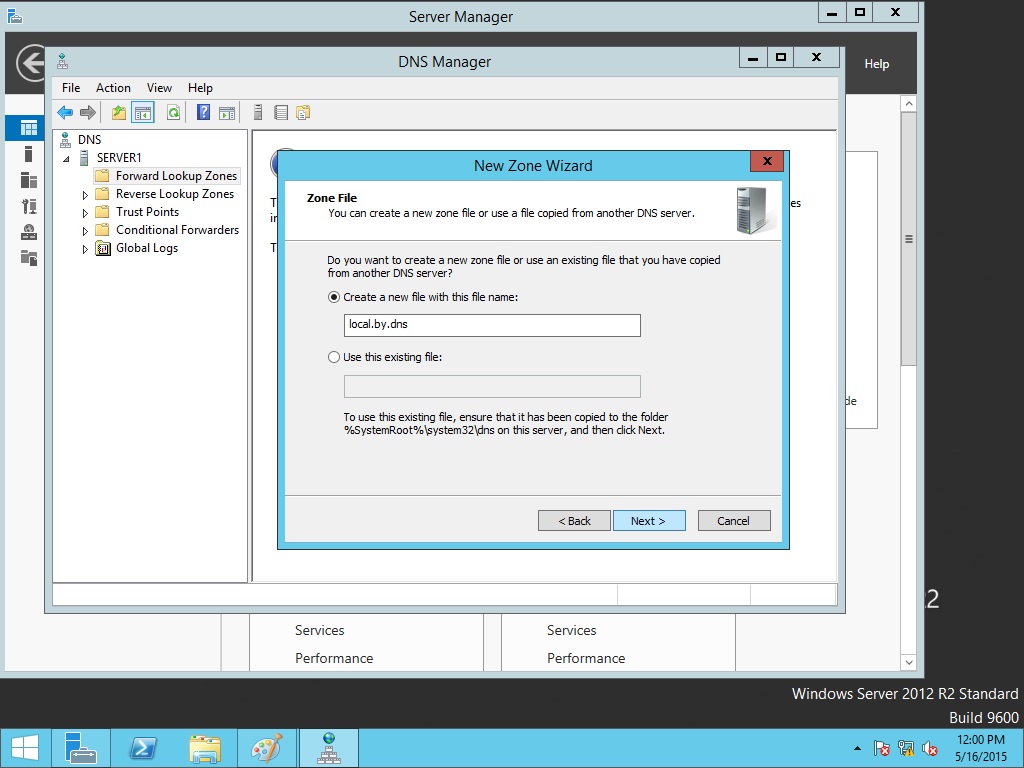


Рис. 4.6. Название файла новой зоны DNS-сервера

* разрешите передачу данной зоны на любой сервер DNS (*консоль DNS* – зона local.by – *Properties (Свойства)* – закладка *Zone Transfers (Передачи зон)* – Отметьте *Allow zone transfers (Разрешить передачи)* и *To any server (На любой сервер*)) (рис. 4.7).

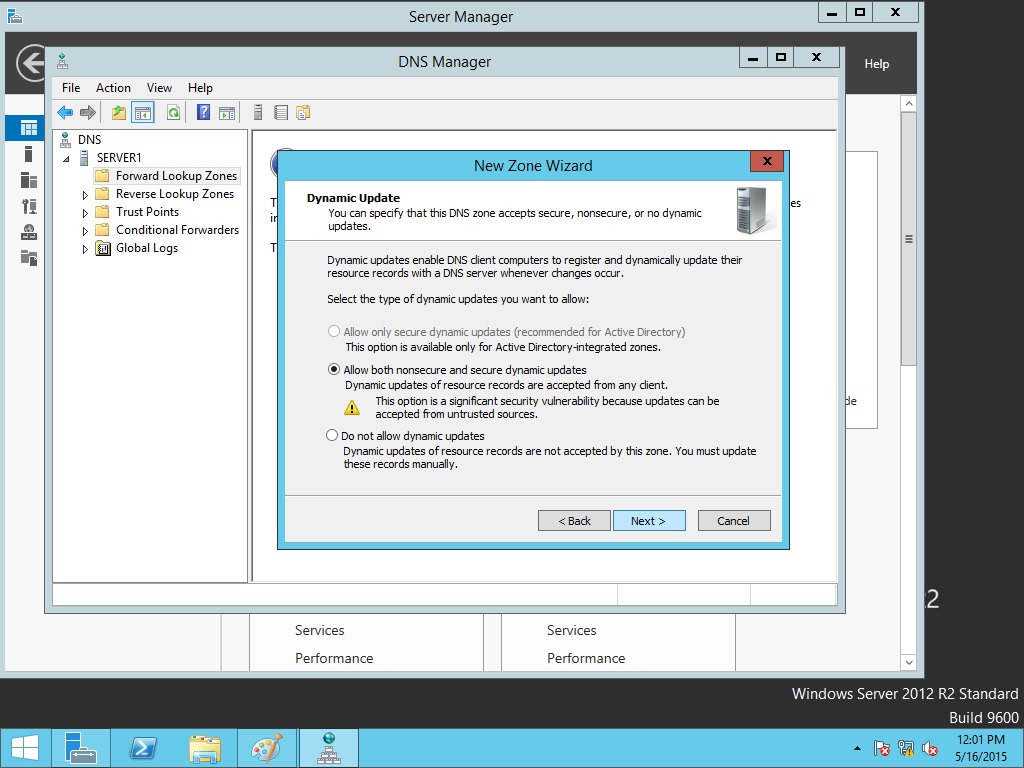


Рис. 4.7. Разрешение на передачу зоны на другой сервер

* в итоге получим зону прямого просмотра DNS-сервера, как показано на рис. 4.8.

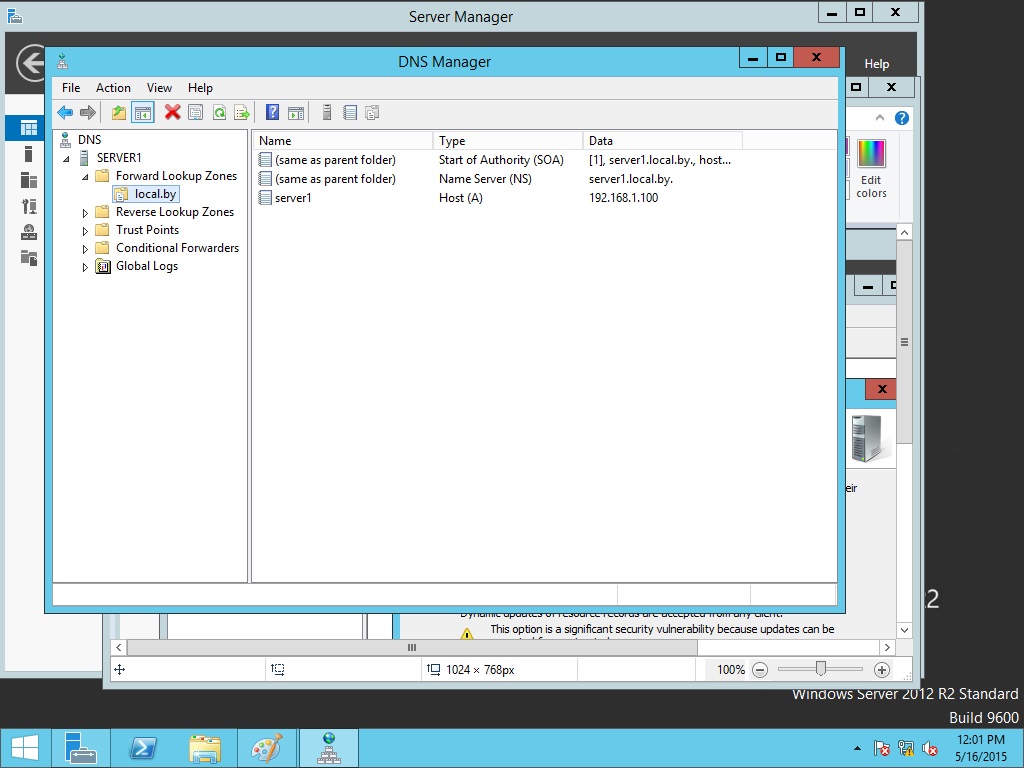


Рис. 4.8. DNS-сервер с созданной зоной прямого просмотра

Чтобы на DNS-сервере автоматически зарегистрировалось имя сервера (в нашем случае server1), необходимо указать в свойствах компьютера DNS-суффикс (рис. 4.9), а также в IP-конфигурации должен быть указан адрес DNS-сервера (в нашем случае это все тот же 192.168.1.100).

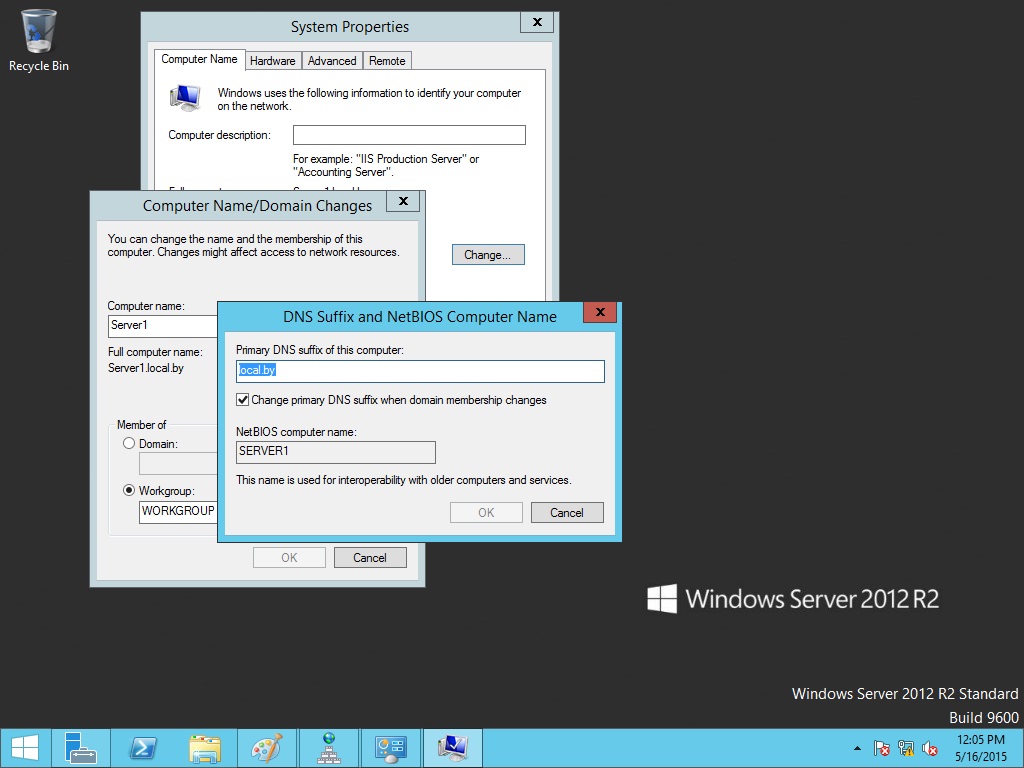


Рис. 4.9. DNS-суффикс для символьного имени компьютера

*3. Создание дополнительной зоны прямого просмотра*

На втором сервере создадим стандартную дополнительную зону с именем local.by (все действия выполняются на втором сервере аналогично установке службы DNS на первом сервере с отличием типа зоны прямого просмотра):

* откройте консоль DNS;
* выберите раздел *Primary Zone (Зоны прямого просмотра)*;
* запустите мастер создания зоны (выберите: тип зоны –*Secondary Zone (Дополнительная зона)*, IP-адрес master-сервера (с которого будет копироваться зона) – адрес сервера *server1*, остальные параметры – по умолчанию);
* введите имя зоны – local.by.

В итоге получим совместную работу DNS-серверов с реализации функции резервирования.

*4. Настройка узлов для выполнения динамической регистрации на сервер DNS*

Для выполнения данной задачи нужно выполнить ряд действий как на серверах (если требуемые настройки не были выполнены ранее), так и в настройках клиента DNS. Рассмотрим пример настройки клиента с его регистрацией в DNS-сервере.

На сервере *DNS*  должна быть создана соответствующая зона, а также разрешены динамические обновления.

На клиенте *DNS* необходимо сделать следующее:

* указать в настройках протокола TCP/IP адрес предпочитаемого DNS-сервера – тот сервер, на котором разрешены динамические обновления (в нашем примере – сервер с адресом 192.168.1.100);
* в полном имени компьютера указать соответствующий DNS-суффикс (в нашем примере – local.by). Для этого последовательно инициировать: *Мой компьютер – Свойства* – закладка *Имя компьютера* – кнопка *Изменить* – Кнопка *Дополнительно* – в пустом текстовом поле вписать название домена local – кнопка *ОK* (3 раза)) (рис. 4.10).

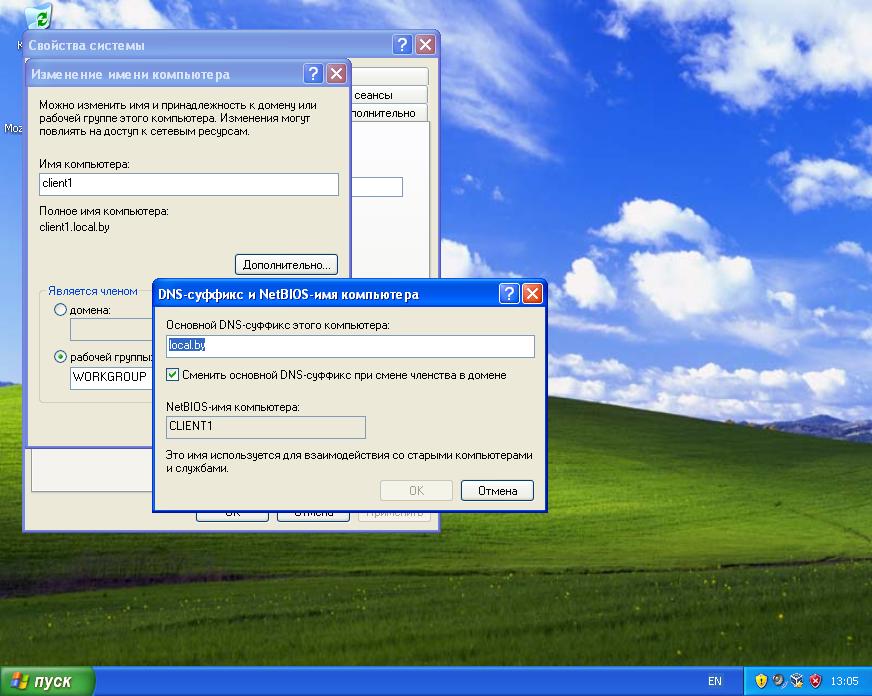


Рис. 4.10. Заполнение поля *DNS-суффикс* на клиенте

После этого система предложит перезагрузить компьютер. После выполнения перезагрузки на сервер DNS в зоне loсal.by автоматически создадутся записи типа A для наших серверов (рис. 4.11). В случае не создания записи для клиента (в нашем примере это client1) можно на стороне клиента в командной строке выполнить команду *ipconfig / registerdns.*

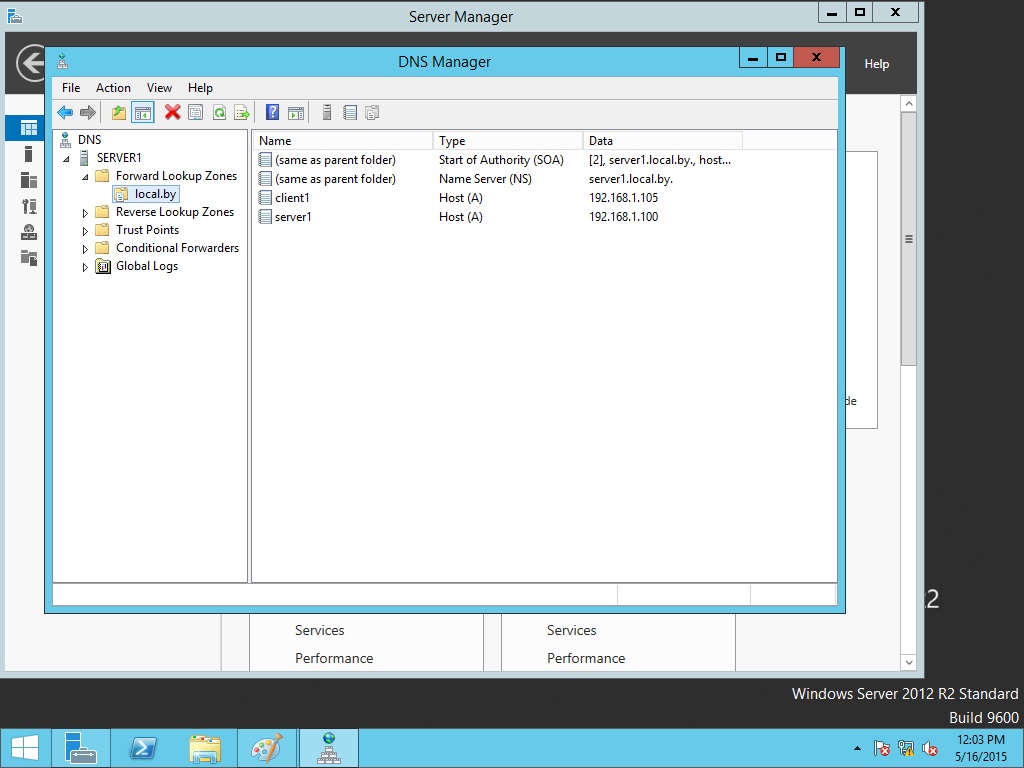


Рис. 4.11. Пример DNS-сервера с записями для клиента и сервера

Аналогичные операции необходимо выполнить на всем компьютерах сети.

Если автоматически записи не создались, то их можно создать вручную (рис. 4.12), однако при этом могут возникнуть сложности с автоматическим обновлением записей при изменении IP-адресов.

*5. Создание зоны обратного просмотра*

Выполняется по следующим шагам:

* откройте консоль DNS;
* выберите раздел *Reverse Lookup Zone (Зоны обратного просмотра)*;
* запустите мастер создания зоны (выберите: тип зоны – *Primary* *(Основная)*, динамические обновления – разрешить, остальные параметры – по умолчанию) (рис. 4.13);
* в поле *Код сети* (*ID*) введите параметры идентификатора сети – «192.168.1», а затем выполните команду принудительной регистрации компьютеров на сервере DNS – *ipconfig* / *registerdns*.

В итоге компьютеры зарегистрируются в обратной зоне DNS.

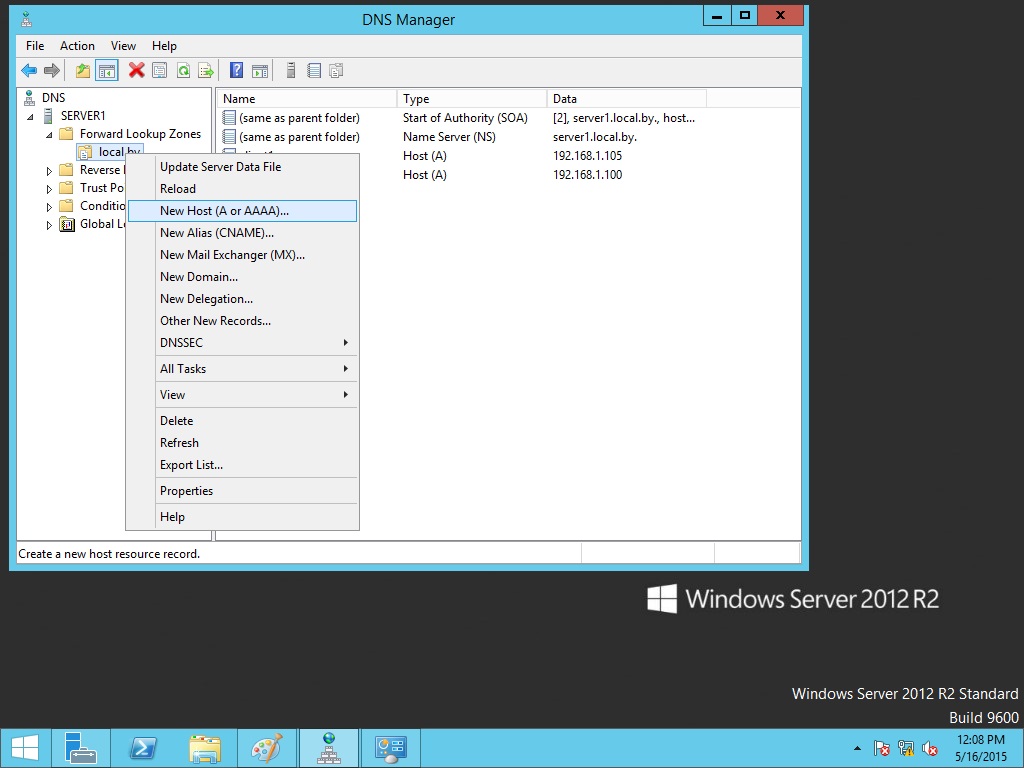


Рис. 4.12. Создание записи типа А на DNS-сервере вручную

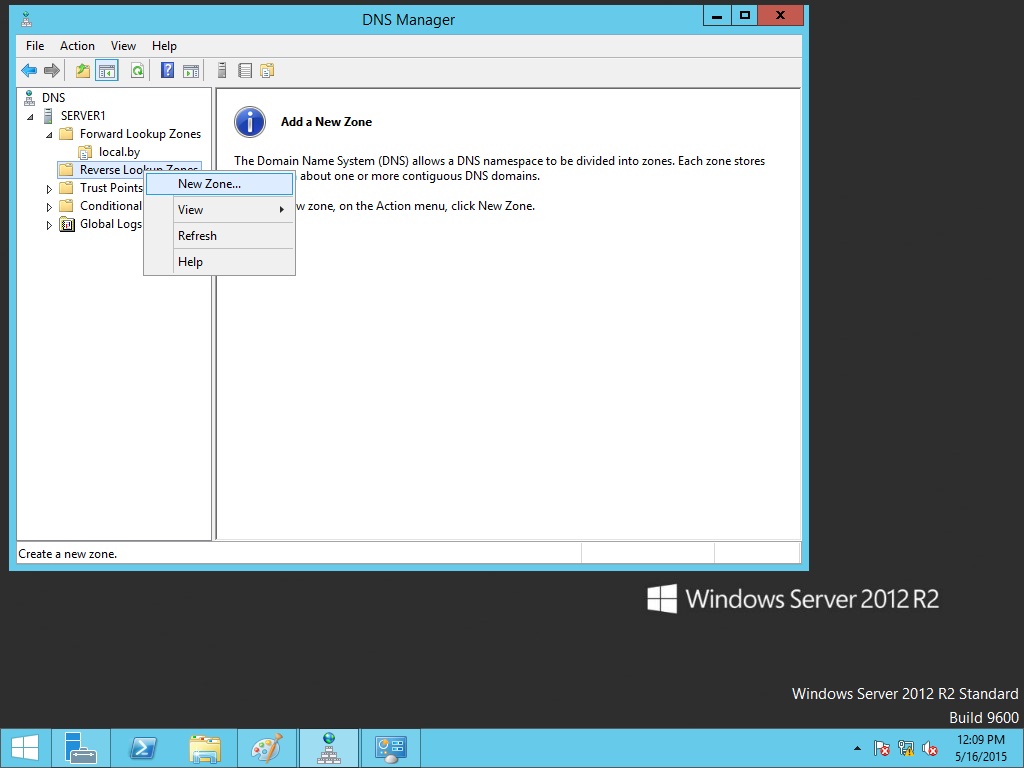


Рис. 4.13. Создание зоны обратного просмотра

**4.3. Лабораторная работа № 6**

**Цель:** изучение методов организации символьной адресации в клиент-серверной сети на базе операционных систем Windows с использованием DNS-сервера.

**Задание:** лабораторная работа представляет собой настройку в сети с клиент-серверной архитектурой, организованной при выполнении лабораторной работы №4-5, DNS-сервера и регистрации DNS-клиентов. В качестве хостов должны выступать виртуальные операционные системы типа Windows с организованной динамической адресацией. DNS-сервер должен использовать статический адрес (согласно лабораторной работе №4-5). Имена доменов выбрать согласно варианту (табл. 4.1).

Таблица 4.1

**Варианты заданий для лабораторной работы №6**

|  |  |
| --- | --- |
| № варианта | Наименование домена |
| 1 | ISiT1.by |
| 2 | ISiT2.by |
| 3 | ISiT3.by |
| 4 | ISiT4.by |
| 5 | ISiT5.by |
| 6 | ISiT6.by |
| 7 | ISiT7.by |
| 8 | ISiT8.by |
| 9 | ISiT9.by |
| 10 | ISiT10.by |
| 11 | ISiT11.by |
| 12 | ISiT12.by |
| 13 | ISiT13.by |
| 14 | ISiT14.by |
| 15 | ISiT15.by |