Рахман П.А.

Исследование проблемы динамических обновлений зон при работе с DNS сервером на базе системы MS Windows 2000 Advanced Server Service Pack 4

Аннотация

В ОС MS Windows 2000 динамические обновления могут выполнять 4 службы: DHCP Client, DHCP Server, NETLOGON и Cluster. Мы рассмотрим первые 3, поскольку они наиболее часто используются при построении сетевой инфраструктуры на базе серверов MS Windows 2000 и клиентов MS Windows 98/2000. Кластерные решения применяются по мере необходимости и не так уж широко. А главное, с точки зрения динамических обновлений его взаимодействие с DNS при регистрации имени кластера практически не отличается от взаимодействия с DNS таких служб как DHCP-server и DHCP-client, регистрирующих и обновляющих записи в DNS для своих клиентских машин. В этом плане службы DHCP-client и DHCP-server также во многом похожи во взаимодействии с DNS, но они еще могут взаимодействовать между собой, и мы их обеих вместе рассмотрим в первой части исследовании. Службу NETLOGON мы рассмотрим совершенно отдельно во второй части, так как она куда более сложно взаимодействует с DNS и имеет исключительную важность для служб каталога.

В данном исследовании рассматриваются гетерогенные сети, состоящие из серверов и клиентов на базе ОС MS Windows 98 SE, Windows 2000 SP3 и Windows 2000 SP4. Как увидим позже, даже сеть, состоящая только лишь из серверов на базе ОС MS Windows 2000 SP3 и серверов MS Windows 2000 SP4, также оказывается гетерогенной с точки зрения взаимодействия серверов сети с DNS при определенных условиях.

Мы будем экспериментировать только с зонами прямого просмотра, поскольку именно для них на сегодняшний день были обнаружены проблемы с динамическими обновлениями. С зонами обратного просмотра данная проблема не проявлялась.

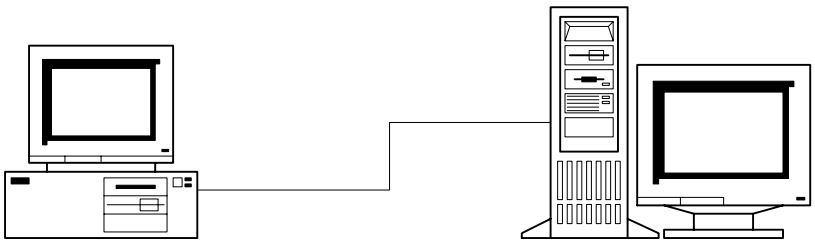
Исследование является исчерпывающим и сознательно ведется методом практически полного перебора различных сочетаний исходных условий:

- В первой части исследования это условия:
  - ОС DHCP клиента: Windows 98 SE или Windows 2000 SP3 или SP4
  - Способ получения IP-адреса: статический или аренда DHCP
  - ОС DHCP сервера: Windows 2000 SP3 или SP4
  - Размещение DHCP-сервера: Вместе с DNS сервером или на отдельной машине
  - Зона прямого просмотра: DNS Zone 1, 2, 3, 4-го уровня
  - Клиент регистрируется в: DNS Node 1, 2, 3, 4-го уровня (макс. – уровень зоны)
- Во второй части исследования это условия:
  - Зона прямого просмотра: DNS Zone 1 или 2-го уровня
  - ОС контроллера корневого AD-домена: Windows 2000 SP3 или SP4
  - ОС контроллера дочернего AD-домена: отсутствует или Windows 2000 SP3 или SP4

Разумеется, для получения выводов, нет необходимости в полном переборе. Обнаружив те или иные характерные признаки можно обобщить вывод, сделанный по нескольким экспериментам, и с некоторой достоверностью распространить его на все остальные случаи. Однако, интересны не только сами выводы, но и дополнительные моменты, которые проявляются только при определенных условиях (заранее неизвестных) и имеют свою немаловажную практическую ценность. Кроме того, это превращает материалы узкоспециализированного исследования в практическое пособие если и далеко не на все, то на достаточно многие проверенные случаи жизни.

Часть 1. Эксперименты с зонами прямого просмотра и службами DHCP Client и DHCP Server

1. DHCP-клиент на базе ОС MS Windows 98 SE
Объединенный DHCP, DNS сервер MS Windows 2000 AS SP4
Разрешены только безопасные динамические обновления зон



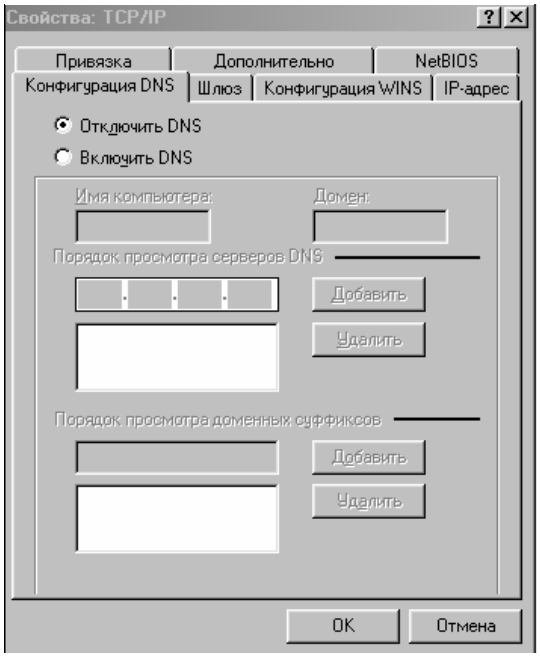
CLIENT9X
Windows 98 SE
DHCP Client

ROOTDCSP4.TEST.LOCAL
IP: 10.0.5.1
Windows 2000 SP4
ROOT DC

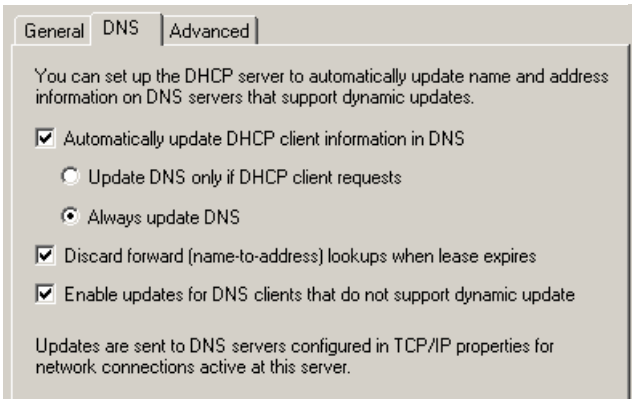
DNS Server
Zones with secure updates only:
FLZ: TEST.LOCAL & experimental zones
RLZ: 5.0.10.IN-ADDR.ARPA

DHCP Server
Scope: 10.0.5.1 - 10.0.5.254
Exclusion: 10.0.5.1 - 10.0.5.20
Reservation 10.0.5.100 for CLIENT9X with experimental DNS Domain Names

DNS-настройки клиента

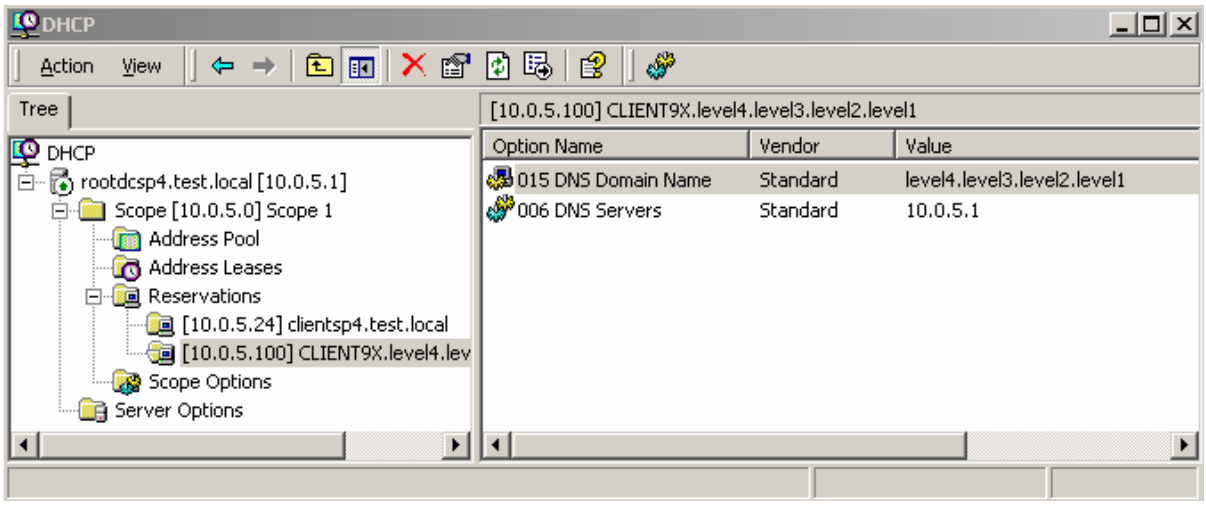


Настройки DHCP сервера для работы с DNS

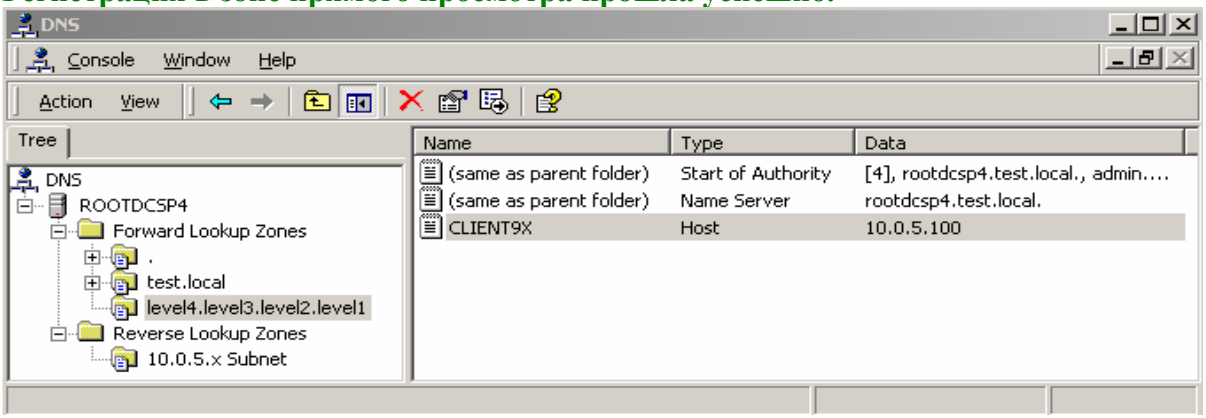


1.1. Зона прямого просмотра: LEVEL4.LEVEL3.LEVEL2.LEVEL1.
Зона обратного просмотра: 5.0.10.IN-ADDR.ARPA.

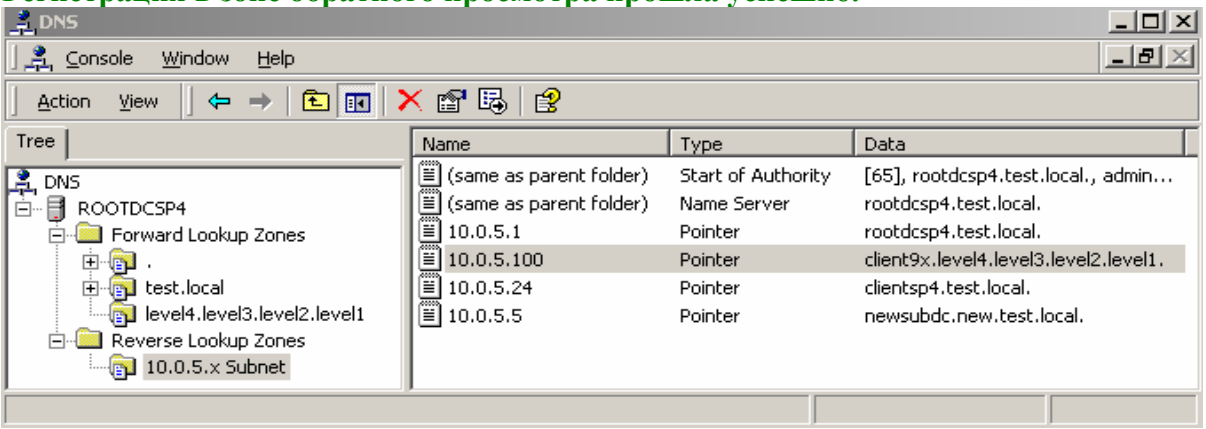
1.1.1. DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL4 с IP: 10.0.5.100



Регистрация в зоне прямого просмотра прошла успешно.

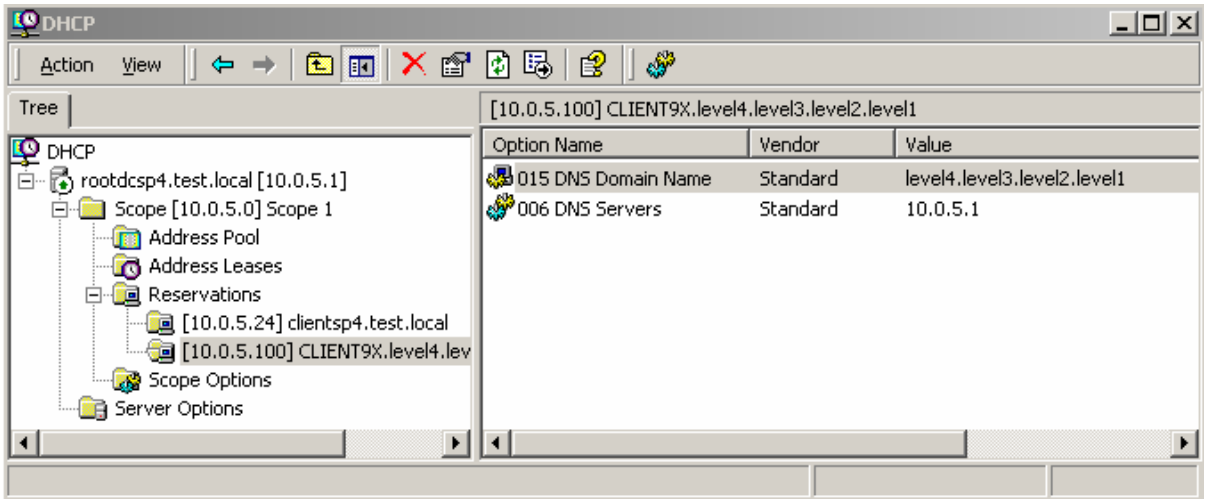


Регистрация в зоне обратного просмотра прошла успешно.

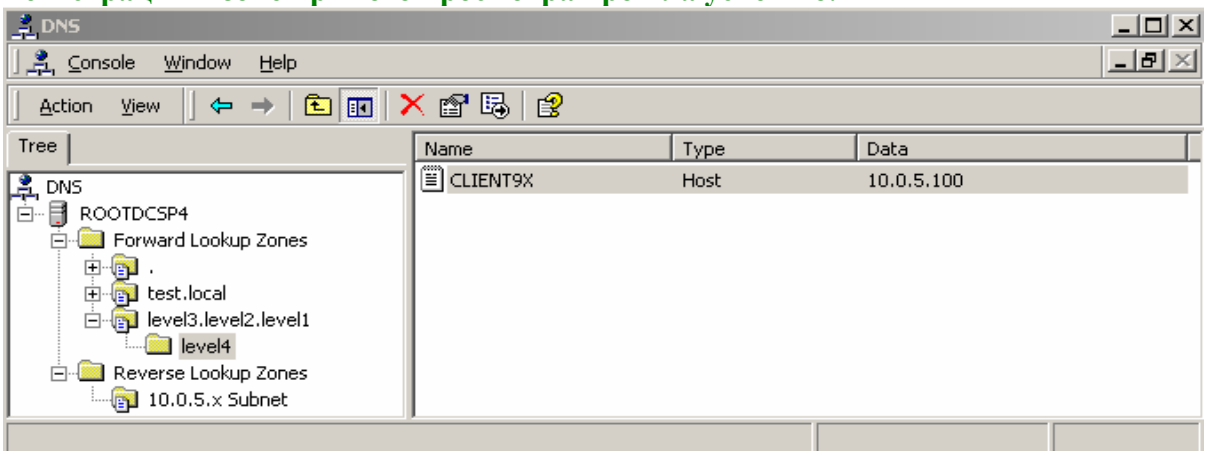


1.2. Зона прямого просмотра: LEVEL3.LEVEL2.LEVEL1.
В этой зоне создается DNS-поддомен LEVEL4
Зона обратного просмотра: 5.0.10.IN-ADDR.ARPA.

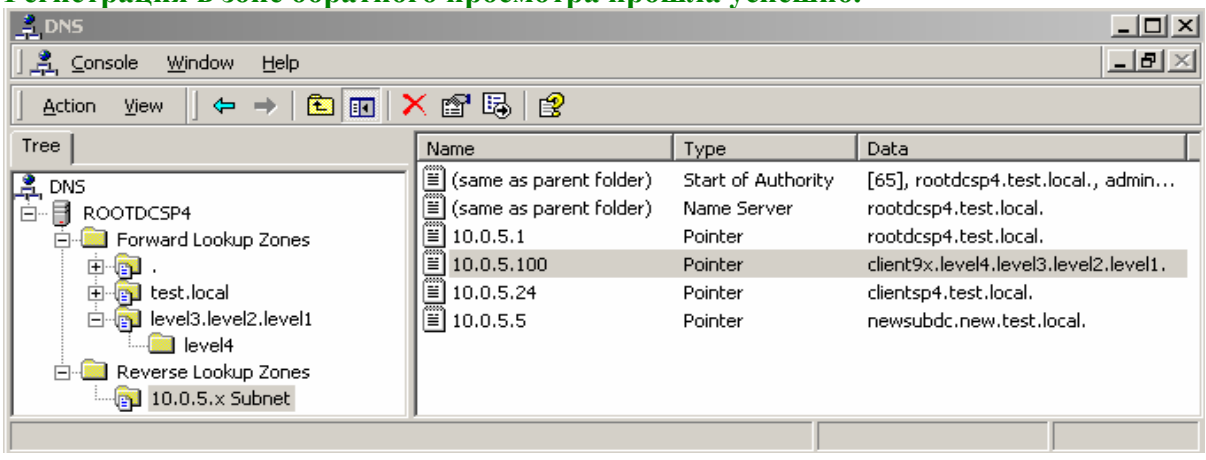
1.2.1. DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL4 с IP: 10.0.5.100



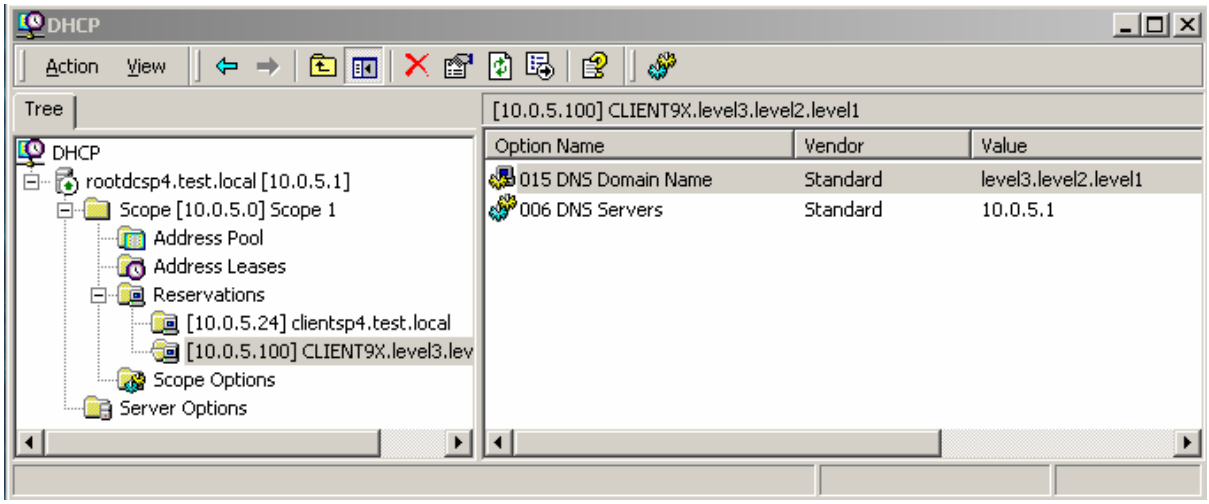
Регистрация в зоне прямого просмотра прошла успешно.



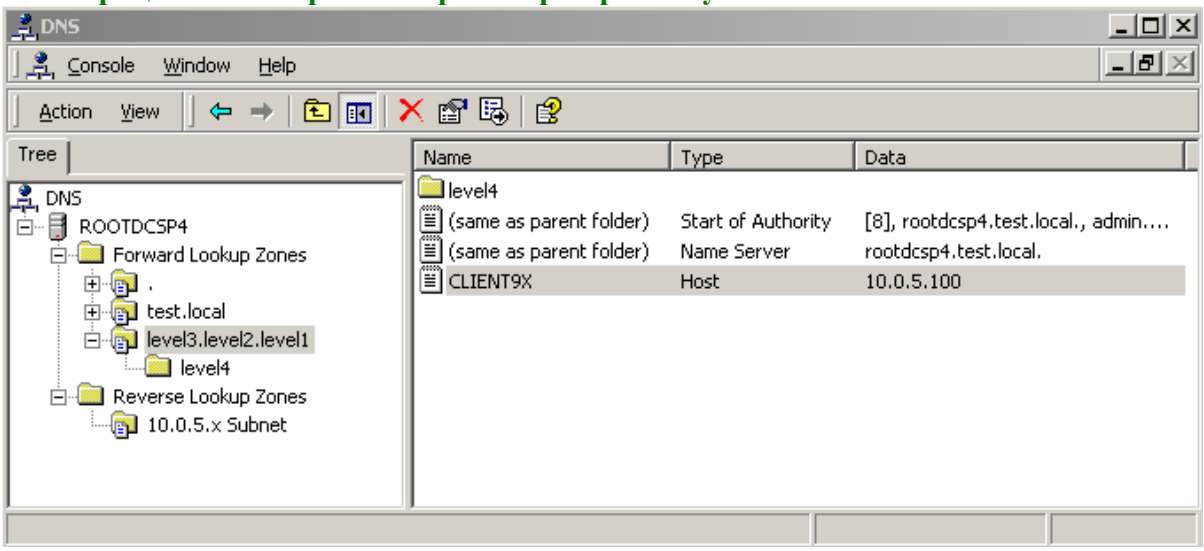
Регистрация в зоне обратного просмотра прошла успешно.



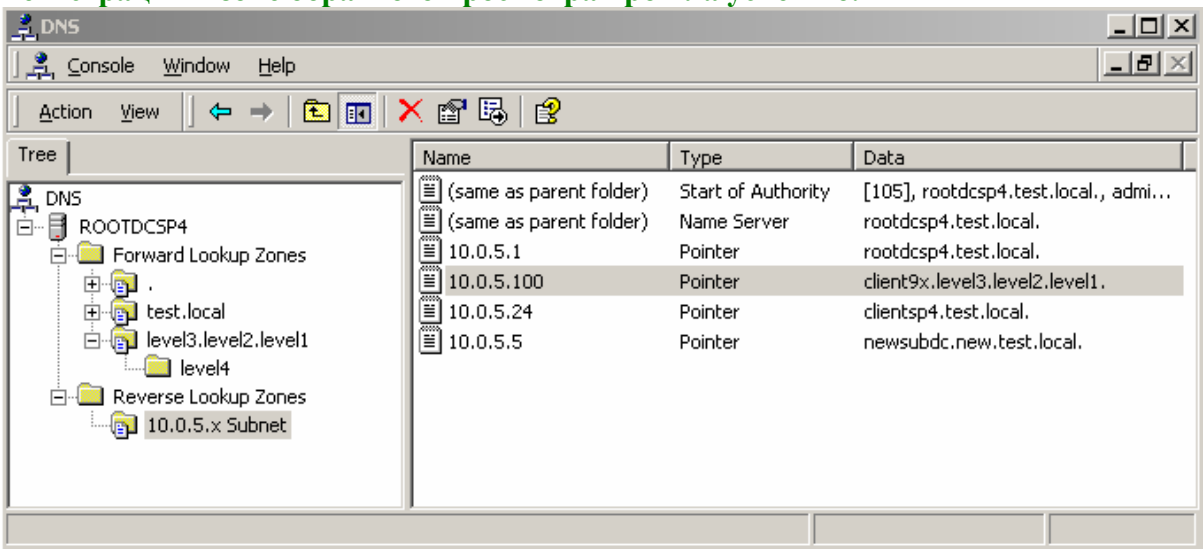
1.2.2. DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL3 с IP: 10.0.5.100



Регистрация в зоне прямого просмотра прошла успешно.

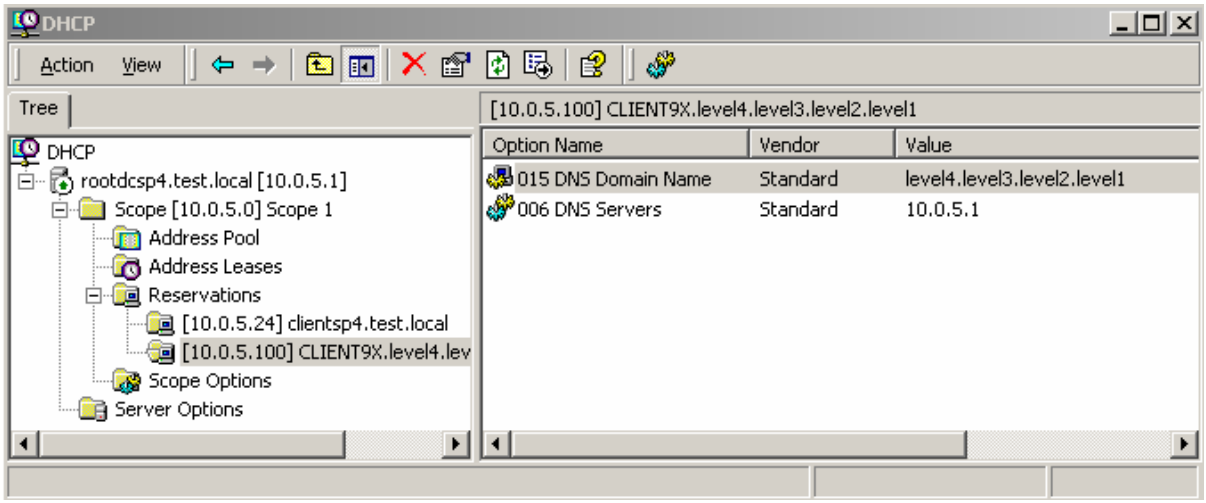


Регистрация в зоне обратного просмотра прошла успешно.

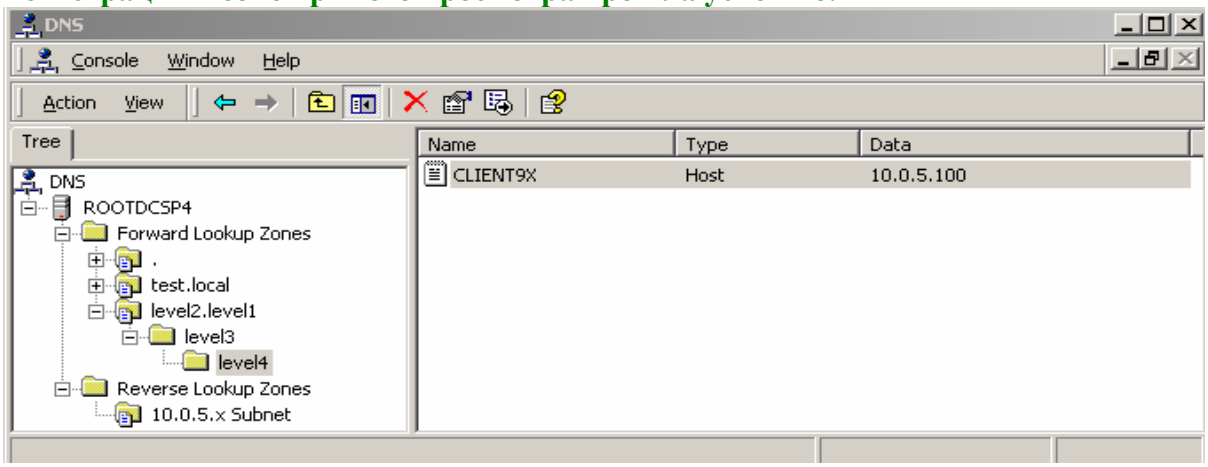


1.3. Зона прямого просмотра: LEVEL2.LEVEL1.
В этой зоне создается DNS-поддомен LEVEL3.
В свою очередь, в DNS-домене LEVEL3 создается DNS-поддомен LEVEL4
Зона обратного просмотра: 5.0.10.IN-ADDR.ARPA.

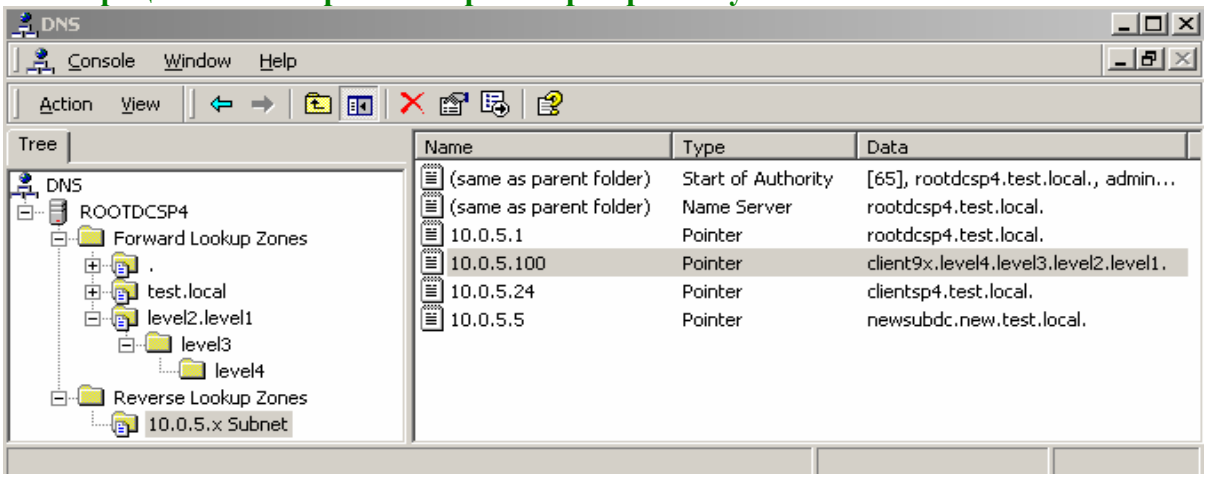
1.3.1. DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL4 с IP: 10.0.5.100



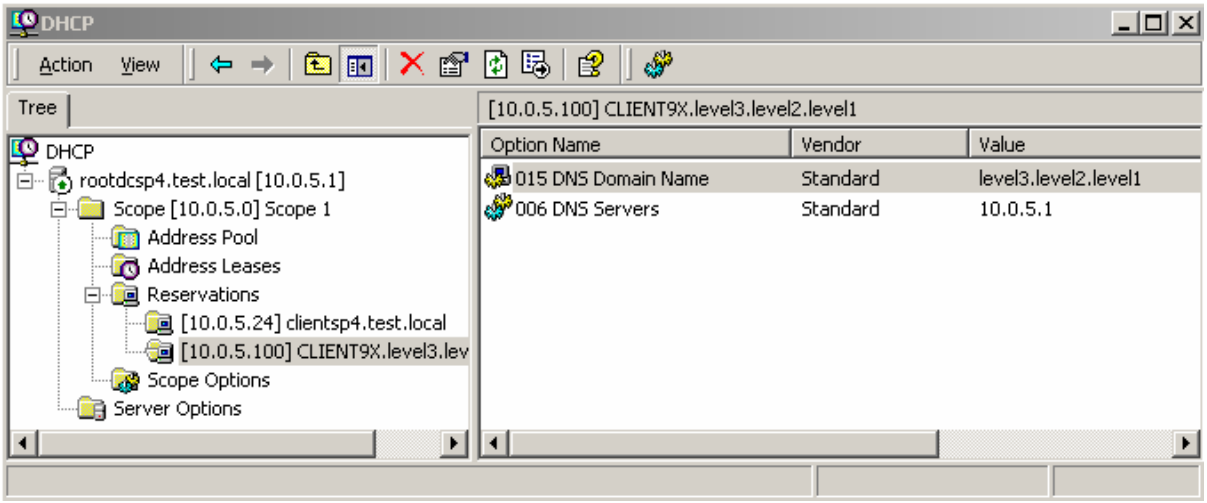
Регистрация в зоне прямого просмотра прошла успешно.



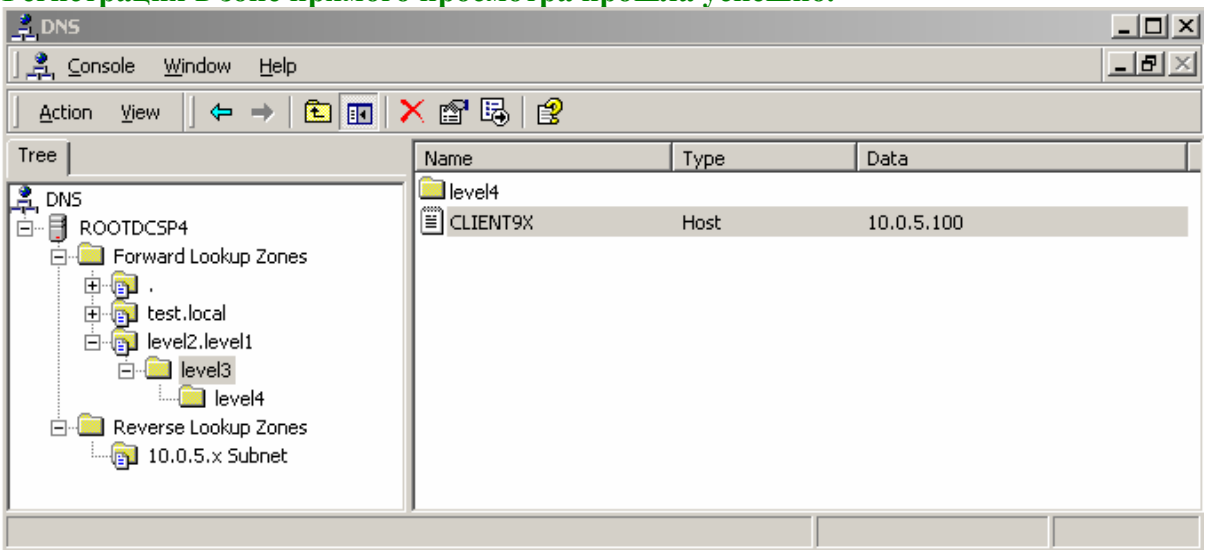
Регистрация в зоне обратного просмотра прошла успешно.



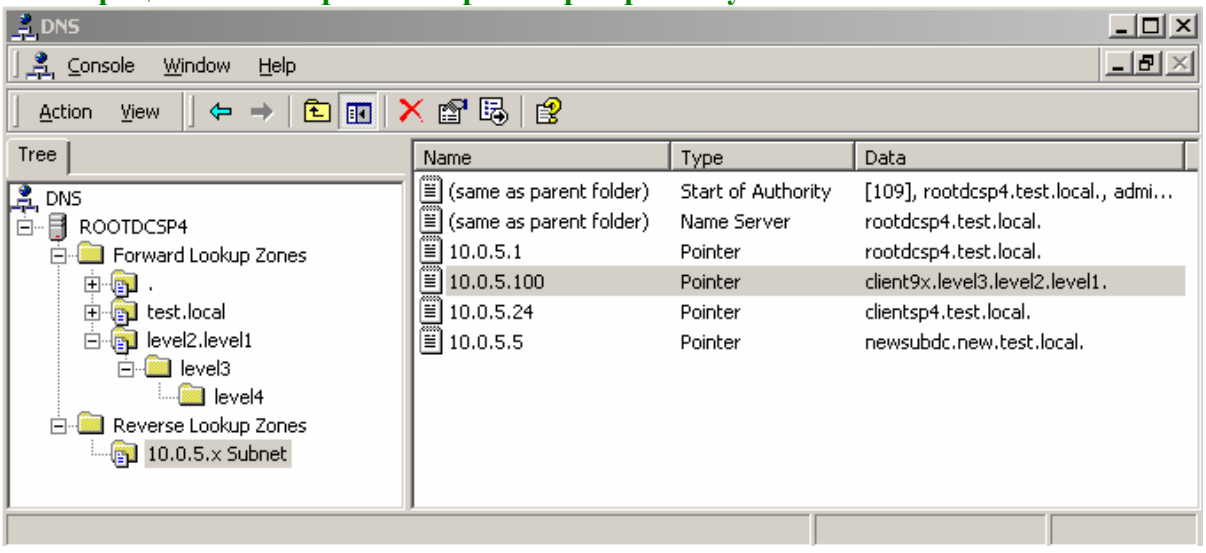
1.3.2. DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL3 с IP: 10.0.5.100



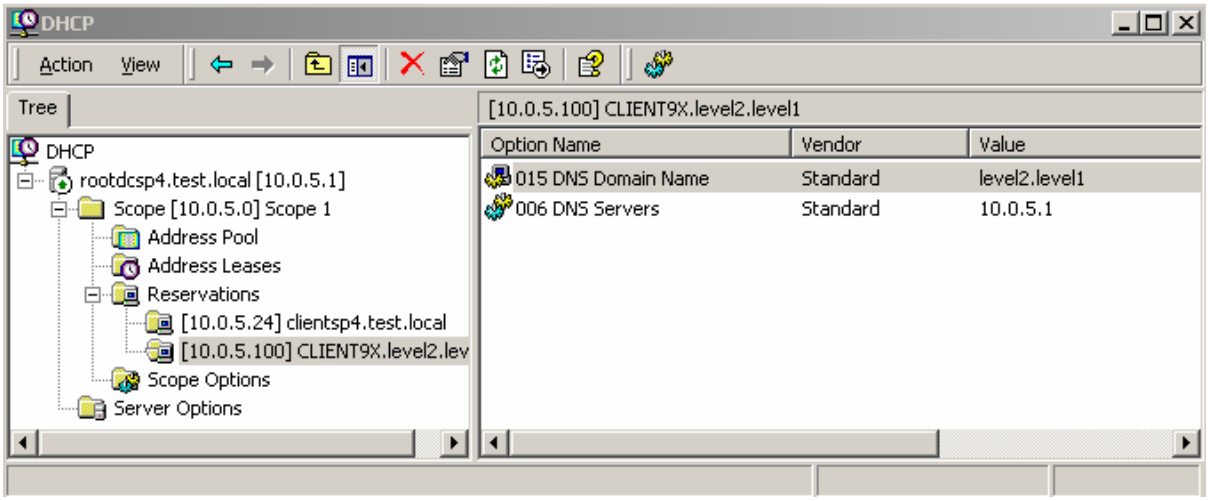
Регистрация в зоне прямого просмотра прошла успешно.



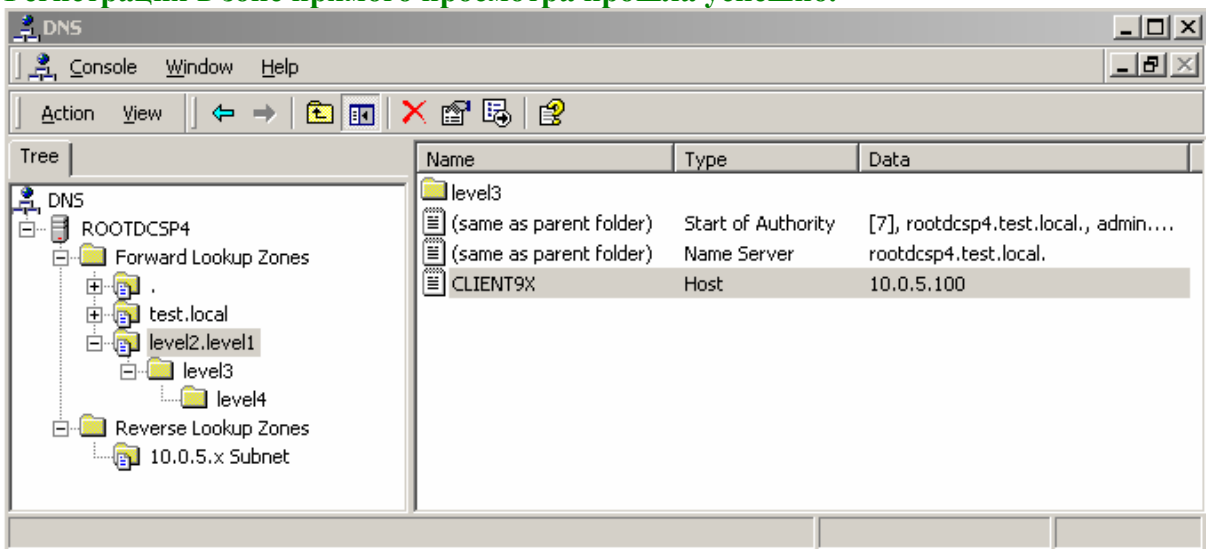
Регистрация в зоне обратного просмотра прошла успешно.



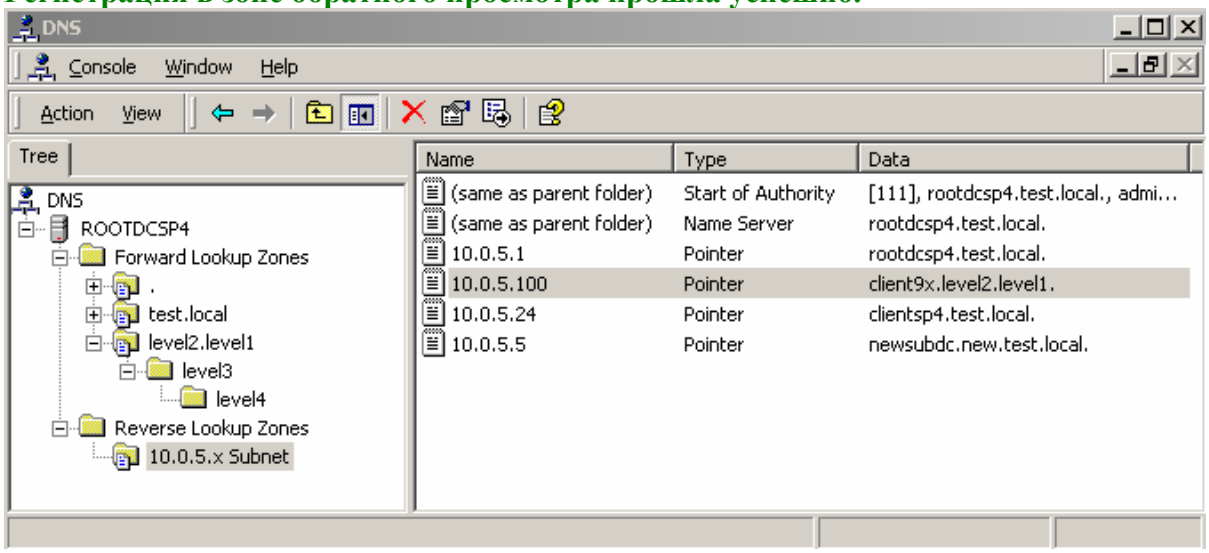
1.3.3. DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL2 с IP: 10.0.5.100



Регистрация в зоне прямого просмотра прошла успешно.

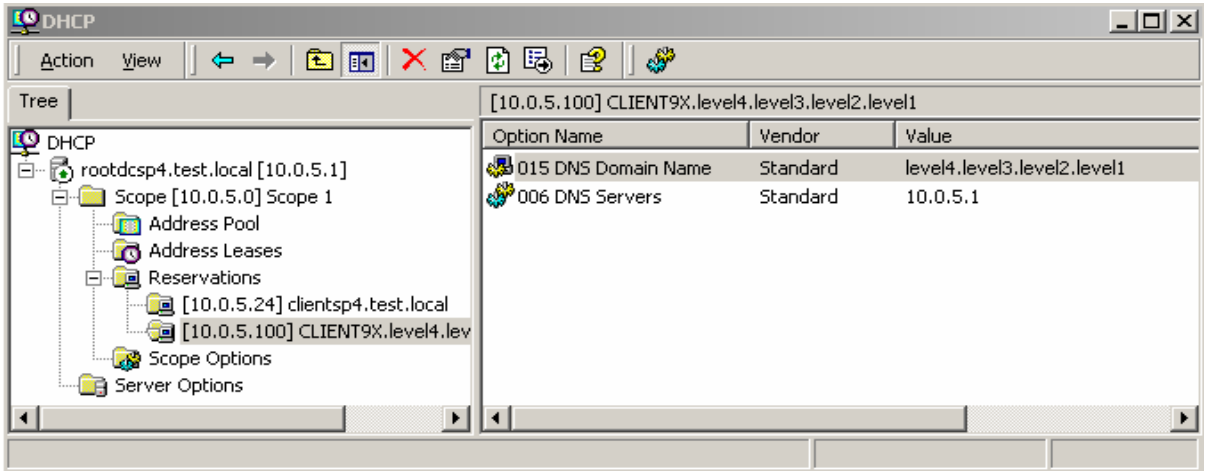


Регистрация в зоне обратного просмотра прошла успешно.

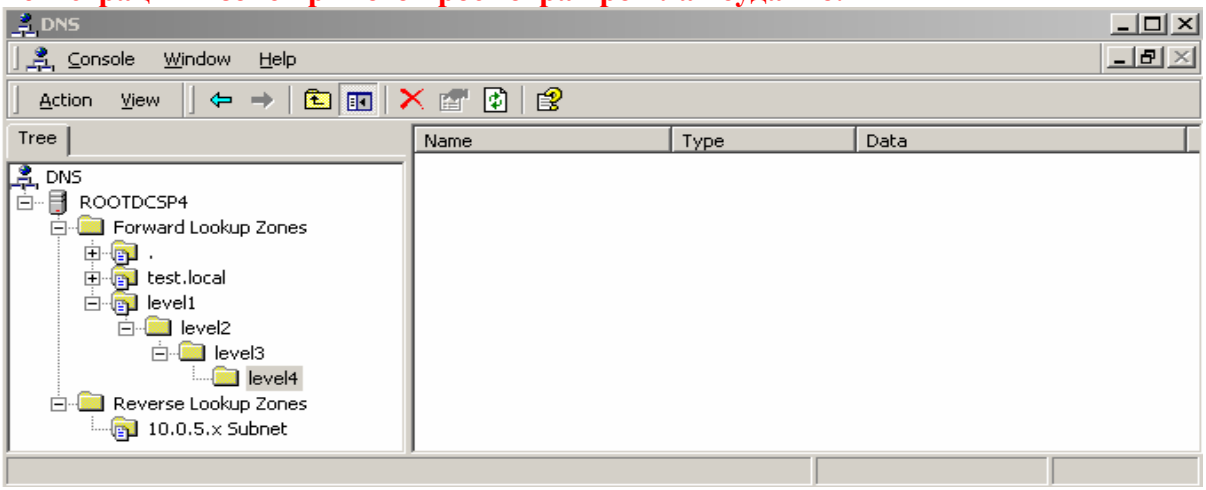


1.4. Зона прямого просмотра: LEVEL1.
В этой зоне создается DNS-поддомен LEVEL2, а в нем,
В свою очередь, в DNS-домене LEVEL2 создается DNS-поддомен LEVEL3.
Наконец, в DNS-домене LEVEL3 создается DNS-поддомен LEVEL4.
Зона обратного просмотра: 5.0.10.IN-ADDR.ARPA.

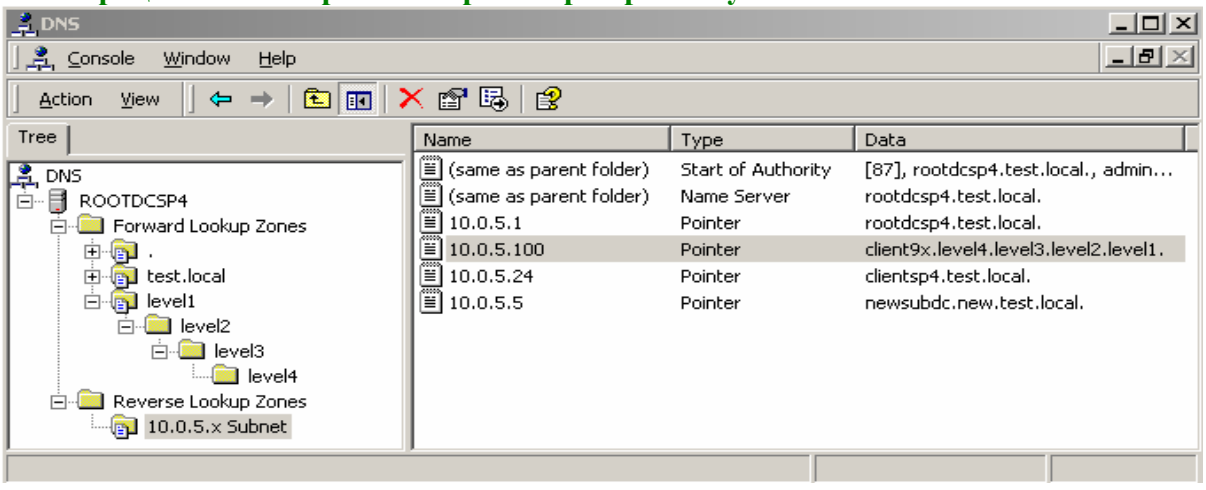
1.4.1. DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL4 с IP: 10.0.5.100



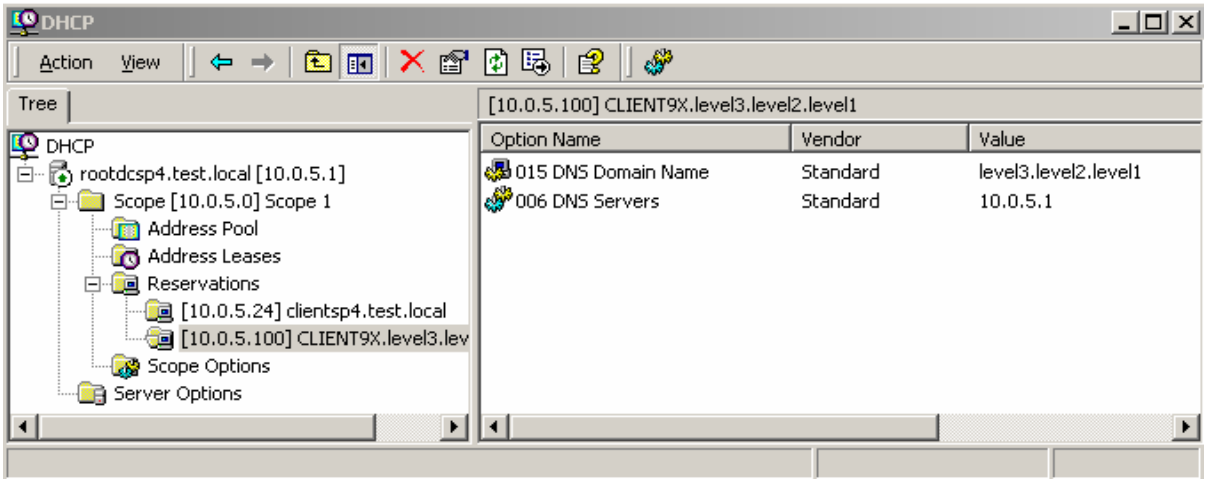
Регистрация в зоне прямого просмотра прошла неудачно.



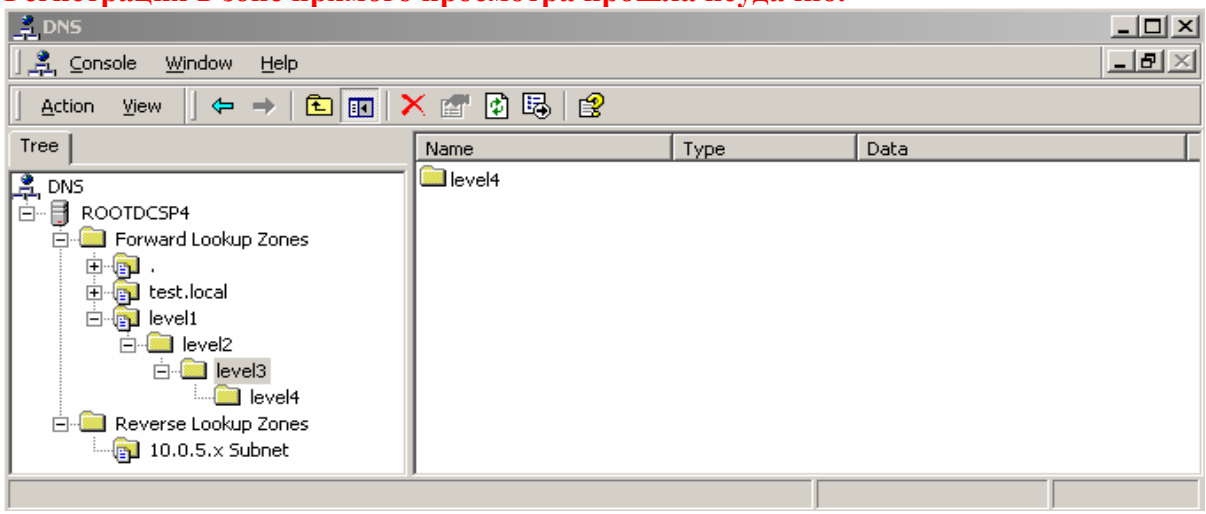
Регистрация в зоне обратного просмотра прошла успешно.



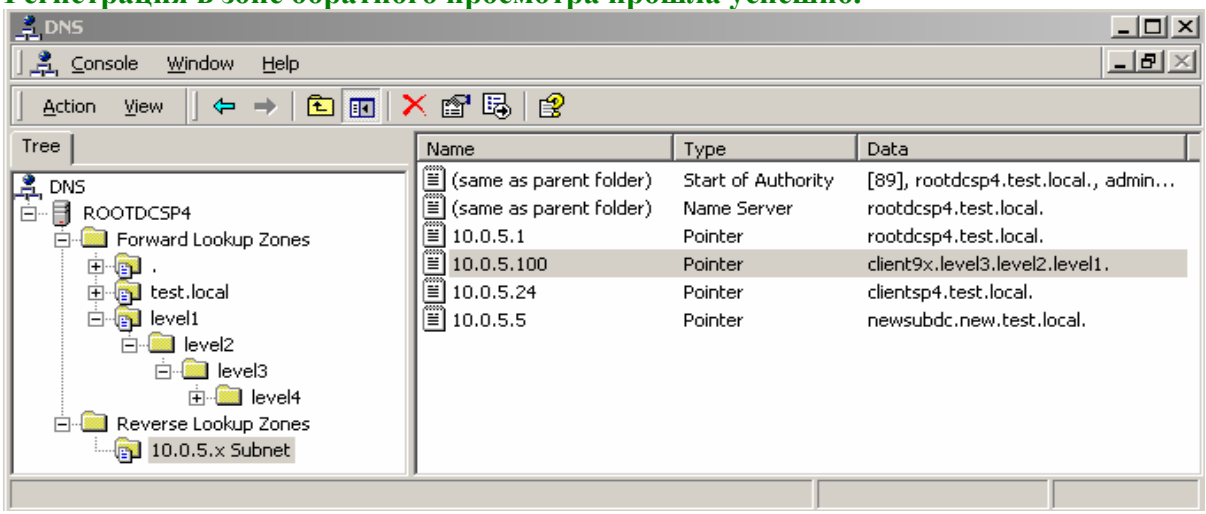
1.4.2. DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL3 с IP: 10.0.5.100



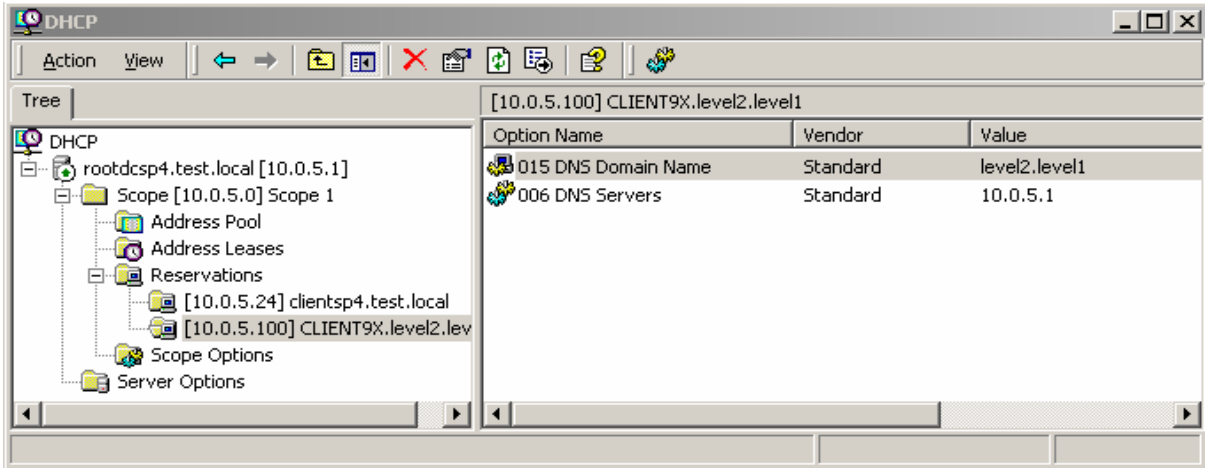
Регистрация в зоне прямого просмотра прошла неудачно.



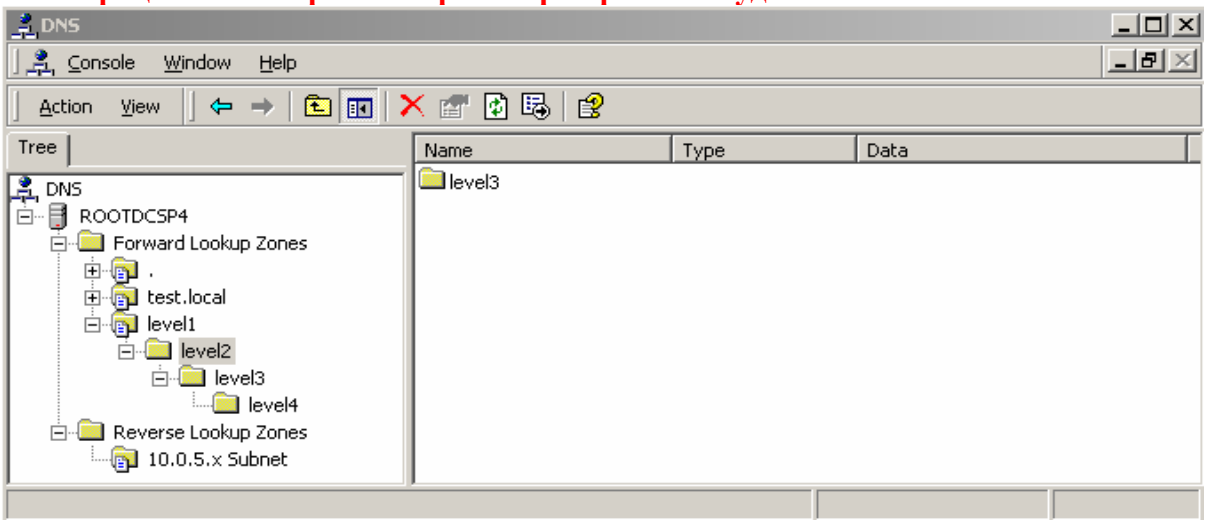
Регистрация в зоне обратного просмотра прошла успешно.



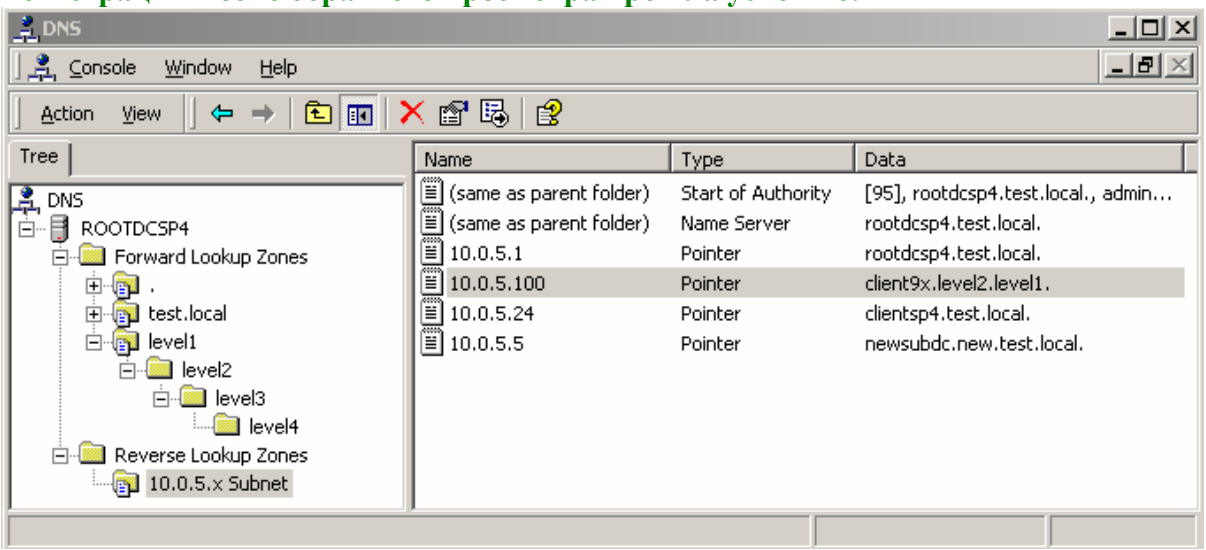
1.4.3. DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL2 с IP: 10.0.5.100



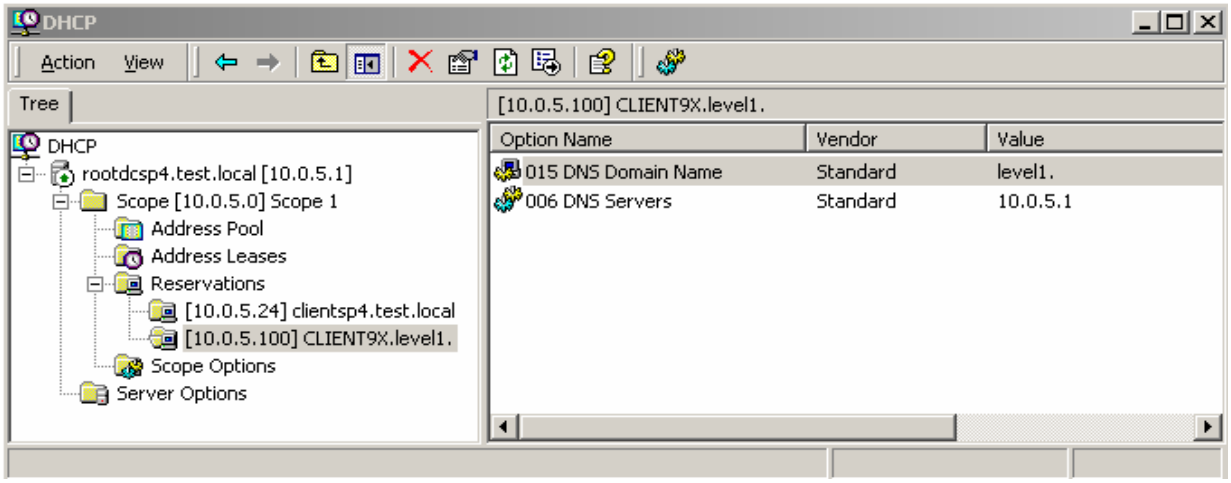
Регистрация в зоне прямого просмотра прошла неудачно.



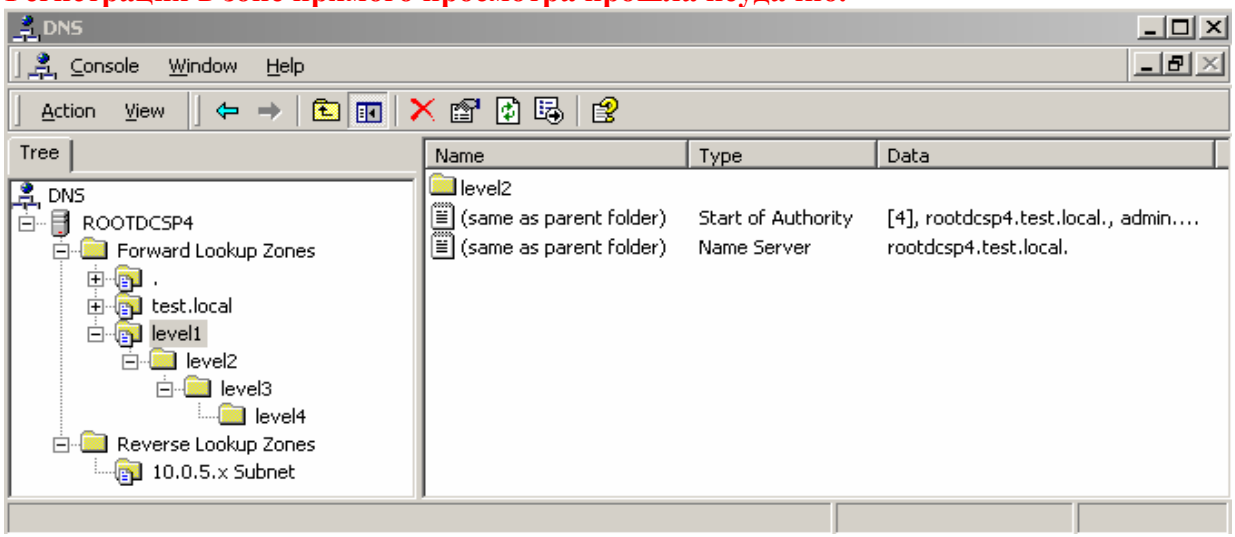
Регистрация в зоне обратного просмотра прошла успешно.



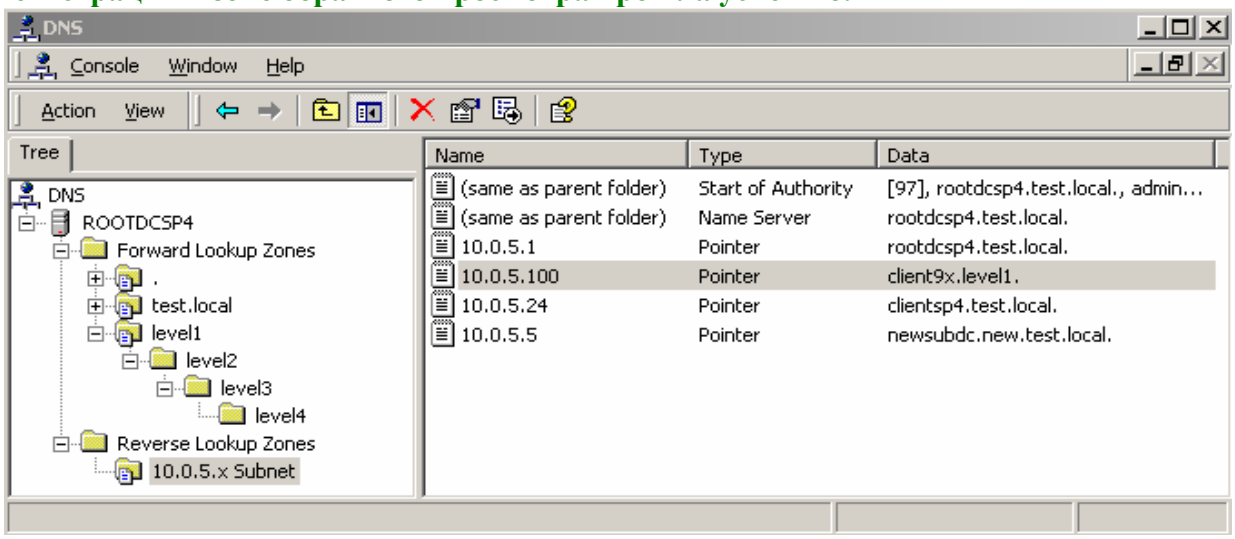
1.4.4. DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL1 с IP: 10.0.5.100



Регистрация в зоне прямого просмотра прошла неудачно.



Регистрация в зоне обратного просмотра прошла успешно.



Для наглядности сведем результаты экспериментов в таблицу.

#	Зона прямого просмотра	DNS Node клиента	Обновление A-записи	Обновление PTR-записи
1.1.1	**LEVEL4.LEVEL3.LEVEL2.LEVEL1**	LEVEL4		
1.2.1	**LEVEL3.LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4	LEVEL4		
1.2.2		LEVEL3		
1.3.1	**LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3	LEVEL4		
1.3.2		LEVEL3		
1.3.3		LEVEL2		
1.4.1	**LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3 в DNS-поддомене LEVEL2	LEVEL4		
1.4.2		LEVEL3		
1.4.3		LEVEL2		
1.4.4		LEVEL1		

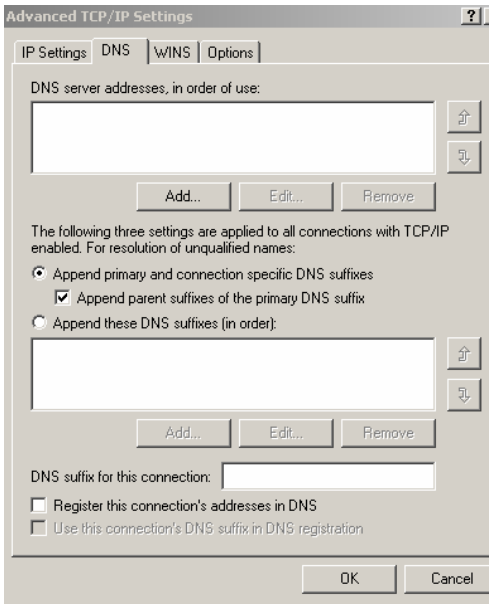
Обновляется практически мгновенно и всегда

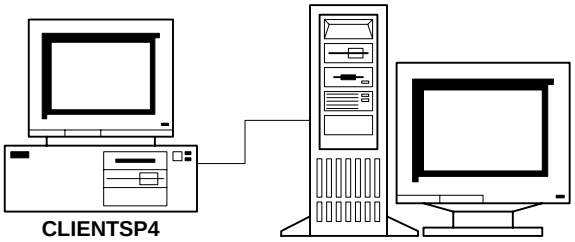
Вообще не обновляется никак и никогда

Обновляется либо мгновенно либо в течение 5 минут после нескольких попыток обновить аренду: ipconfig /renew

2. DHCP-клиент на базе ОС MS Windows 2000 AS SP4
Объединенный DHCP, DNS сервер MS Windows 2000 AS SP4
Разрешены только безопасные динамические обновления зон

DNS-настройки клиента





CLIENTSP4
Windows 2000 AS SP4
DHCP Client

ROOTDCSP4.TEST.LOCAL
IP: 10.0.5.1
Windows 2000 AS SP4
ROOT DC

DNS Server
Zones with secure updates only:
FLZ: TEST.LOCAL & experimental zones
RLZ: 5.0.10.IN-ADDR.ARPA

DHCP Server
Scope: 10.0.5.1 - 10.0.5.254
Exclusion: 10.0.5.1 - 10.0.5.20
Reservation 10.0.5.100 for CLIENTSP4 with experimental DNS Domain Names

Настройки DHCP-сервера такие же, как в 1-й серии 10-ти экспериментов

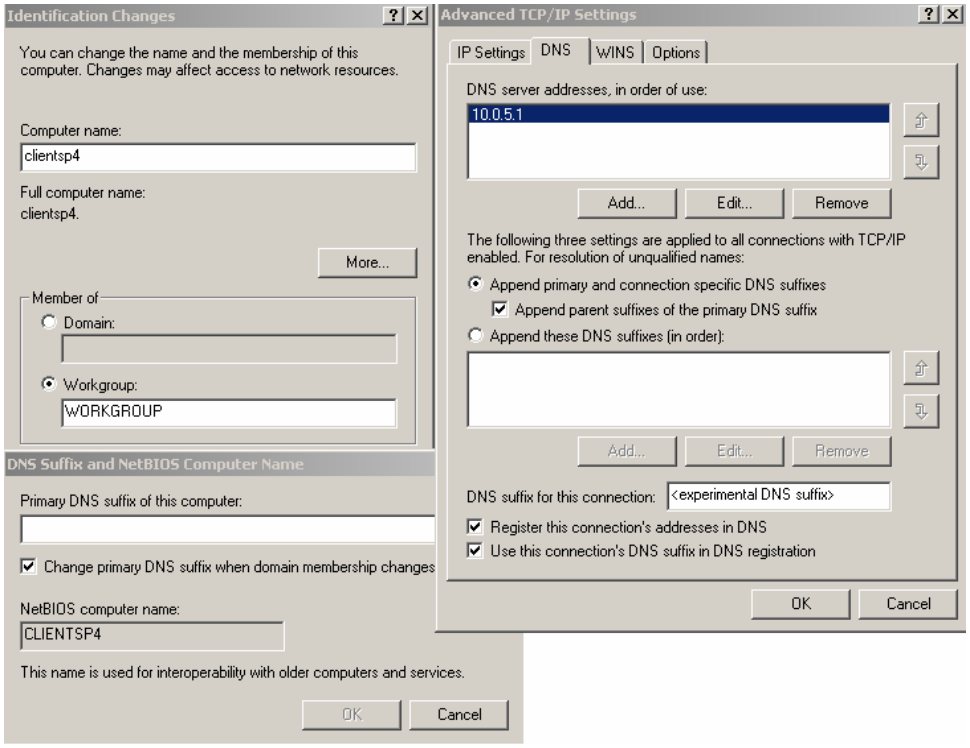
Повторим эксперименты (1.1.1 – 1.4.4) для DHCP-клиента MS Windows AS SP4 и без лишних снимков экрана сведем результаты 10-ти экспериментов в таблицу.

#	Зона прямого просмотра	DNS Node клиента	Обновление A-записи	Обновление PTR-записи
2.1.1	**LEVEL4.LEVEL3.LEVEL2.LEVEL1**	LEVEL4		
2.2.1	**LEVEL3.LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4	LEVEL4		
2.2.2		LEVEL3		
2.3.1	**LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3	LEVEL4		
2.3.2		LEVEL3		
2.3.3		LEVEL2		
2.4.1	**LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3 в DNS-поддомене LEVEL2	LEVEL4		
2.4.2		LEVEL3		
2.4.3		LEVEL2		
2.4.4		LEVEL1		

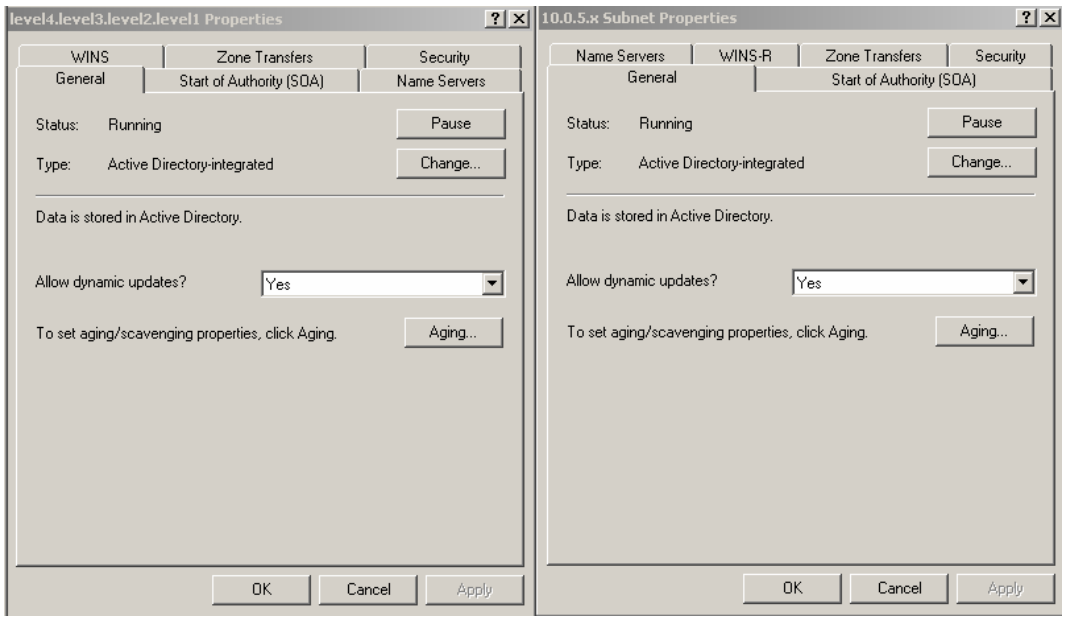
Результаты идентичны с предыдущими экспериментами.

3. Клиент со статическим адресом на базе ОС MS Windows 2000 AS SP4
Объединенный DHCP, DNS сервер MS Windows 2000 AS SP4
Разрешены любые динамические обновления зон

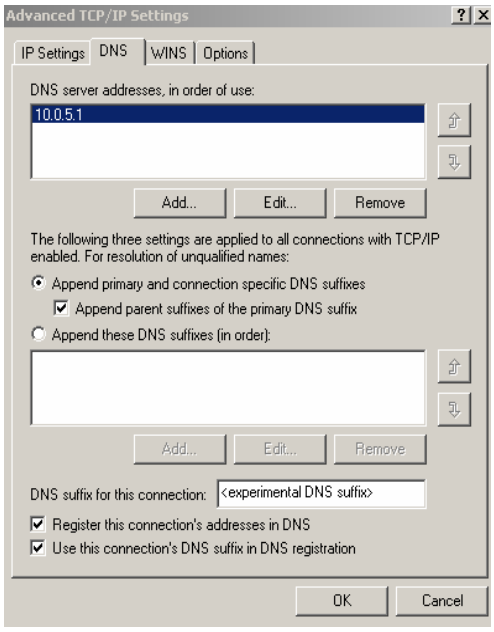
Как известно, клиенты Windows 2000 могут сами обновлять свои записи при явно указанном DNS-суффиксе подключения и при установленных флажках для регистрации на DNS сервере с использованием заданного суффикса.

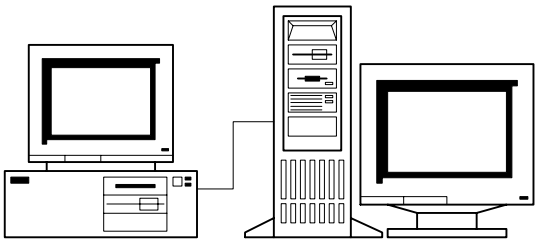


Однако, если клиент не входит ни в какой AD-домен, то он не будет распознан DNS сервером как Authenticated User, имеющий право на создание объектов с полными правами на эти объекты в дальнейшем. Поэтому для упрощения экспериментов, зонам временно разрешаем любые обновления. Тем более что, Security не имеет никакого отношения к проблеме.



DNS-настройки клиента





CLIENTSP4
Windows 2000 AS **SP4**
Static Address Client
experimental DNS Suffixes

ROOTDCSP4.TEST.LOCAL
IP: 10.0.5.1
Windows 2000 AS **SP4**
ROOT DC

DNS Server
None-secure updates are allowed
FLZ: TEST.LOCAL & experimental zones
RLZ: 5.0.10.IN-ADDR.ARPA

DHCP Server
Scope: 10.0.5.1 - 10.0.5.254
Exclusion: 10.0.5.1 - 10.0.5.20

Настройки DHCP-сервера такие же, как в 1-й серии 10-ти экспериментов (здесь они не имеют значения)

Результаты экспериментов.

#	Зона прямого просмотра	DNS Node клиента	Обновление A-записи	Обновление PTR-записи
3.1.1	**LEVEL4.LEVEL3.LEVEL2.LEVEL1**	LEVEL4		
3.2.1	**LEVEL3.LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4	LEVEL4		
3.2.2		LEVEL3		
3.3.1	**LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3	LEVEL4		
3.3.2		LEVEL3		
3.3.3		LEVEL2		
3.4.1	**LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3 в DNS-поддомене LEVEL2	LEVEL4		
3.4.2		LEVEL3		
3.4.3		LEVEL2		
3.4.4		LEVEL1		

Результаты идентичны с предыдущими экспериментами.

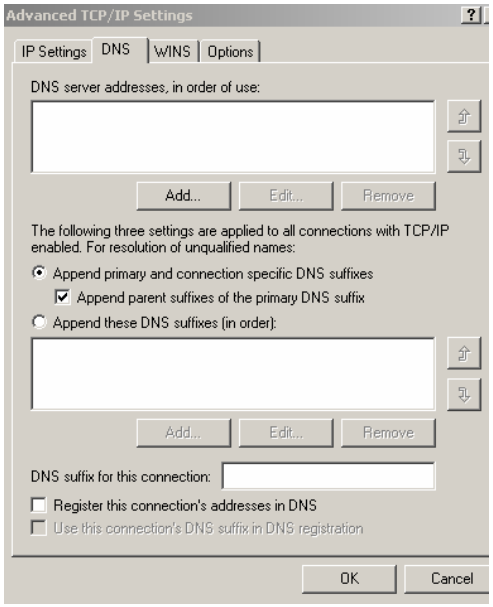
Обновляется практически мгновенно и всегда

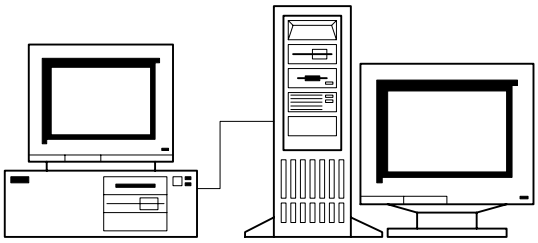
Вообще не обновляется никак и никогда

Обновляется либо мгновенно либо в течение 5 минут после нескольких попыток ipconfig /registerdns

4. DHCP-клиент на базе ОС MS Windows 2000 AS SP3
Объединенный DHCP, DNS сервер MS Windows 2000 AS SP4
Разрешены только безопасные динамические обновления зон

DNS-настройки клиента





CLIENTSP3
Windows 2000 AS SP3
DHCP Client

ROOTDCSP4.TEST.LOCAL
IP: 10.0.5.1
Windows 2000 AS SP4
ROOT DC

DNS Server
Zones with secure updates only:
FLZ: TEST.LOCAL & experimental zones
RLZ: 5.0.10.IN-ADDR.ARPA

DHCP Server
Scope: 10.0.5.1 - 10.0.5.254
Exclusion: 10.0.5.1 - 10.0.5.20
Reservation 10.0.5.100 for CLIENTSP3 with experimental DNS Domain Names

Настройки DHCP-сервера такие же, как в 1-й серии 10-ти экспериментов

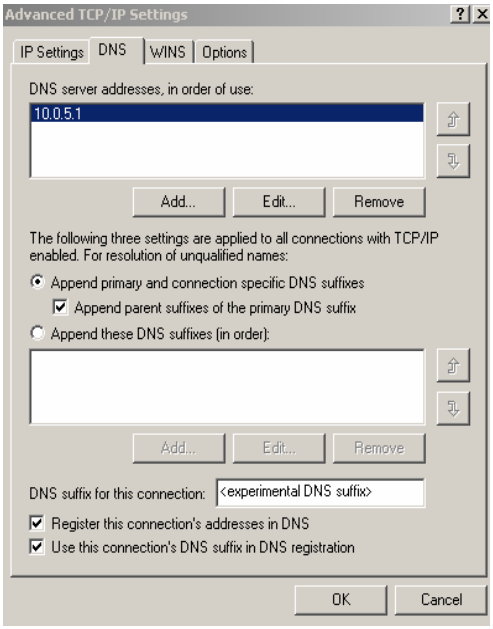
Результаты экспериментов.

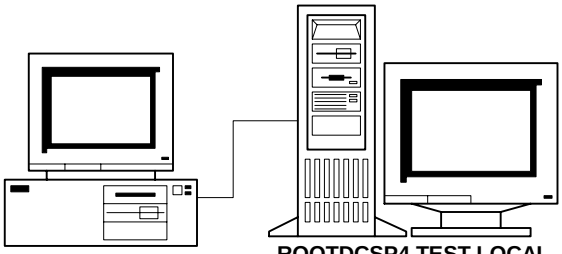
#	Зона прямого просмотра	DNS Node клиента	Обновление A-записи	Обновление PTR-записи
4.1.1	**LEVEL4.LEVEL3.LEVEL2.LEVEL1**	LEVEL4		
4.2.1	**LEVEL3.LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4	LEVEL4		
4.2.2		LEVEL3		
4.3.1	**LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3	LEVEL4		
4.3.2		LEVEL3		
4.3.3		LEVEL2		
4.4.1	**LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3 в DNS-поддомене LEVEL2	LEVEL4		
4.4.2		LEVEL3		
4.4.3		LEVEL2		
4.4.4		LEVEL1		

Результаты идентичны с предыдущими экспериментами.

5. Клиент со статическим адресом на базе ОС MS Windows 2000 AS SP3 Объединенный DHCP, DNS сервер MS Windows 2000 AS SP4 Разрешены любые динамические обновления зон

DNS-настройки клиента





CLIENTSP3
Windows 2000 AS SP3
Static Address Client
experimental DNS Suffixes

ROOTDCSP4.TEST.LOCAL
IP: 10.0.5.1
Windows 2000 AS SP4
ROOT DC

DNS Server
None-secure updates are allowed
FLZ: TEST.LOCAL & experimental zones
RLZ: 5.0.10.IN-ADDR.ARPA

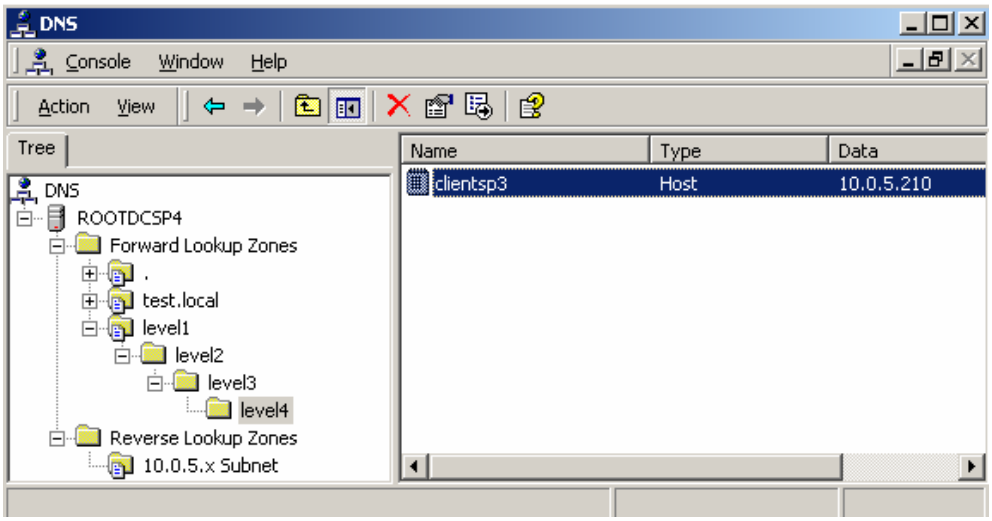
DHCP Server
Scope: 10.0.5.1 - 10.0.5.254
Exclusion: 10.0.5.1 - 10.0.5.20

Настройки DHCP-сервера такие же, как в 1-й серии 10-ти экспериментов (здесь они не имеют значения)

Результаты экспериментов.

#	Зона прямого просмотра	DNS Node клиента	Обновление A-записи	Обновление PTR-записи
5.1.1	**LEVEL4.LEVEL3.LEVEL2.LEVEL1**	LEVEL4		
5.2.1	**LEVEL3.LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4	LEVEL4		
5.2.2		LEVEL3		
5.3.1	**LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3	LEVEL4		
5.3.2		LEVEL3		
5.3.3		LEVEL2		
5.4.1	**LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3 в DNS-поддомене LEVEL2	LEVEL4		
5.4.2		LEVEL3		
5.4.3		LEVEL2		
5.4.4		LEVEL1		

Наконец! Первый полностью положительный результат! В качестве примера снимок успешного обновления зоны прямого просмотра в проблемном случае – зоны “LEVEL1” (эксперимент 5.4.1, для сравнения посмотрите эксперимент 1.4.1):



После 4-х серий по 10 экспериментов с частично положительными результатами, в 5-й серии мы получили полностью положительные результаты. Какие выводы можно сделать?

- Проблемы возникают только с зоной 1-го уровня LOCAL1, представляющей собою дерево вершин (DNS Nodes) с корнем, являющимся DNS Node первого уровня, за исключением тех вершин, где настроено делегирование: такие вершины являются корнем поддеревьев, делегированных DNS серверам для хранения в виде отдельных самостоятельной зон.
- Судя по сериям 1-4, можно было сказать, что проблема в службе DNS, точнее в ее неспособности обновлять зоны первого уровня. Однако 5-я серия опровергает такую гипотезу. Необходимо посмотреть на то, кто с кем взаимодействовал, и, самое главное, вспомнить о том, кто именно занимается обновлением записей в зонах в каждом случае.

Итак, акцентируем внимание на экспериментах X.4.1 – X.4.4 всех серий (X – ее номер):

№ серии	DHCP-сервер	Клиент	Служба, обращающаяся к DNS с запросом на обновление A-записи
1	Windows 2000 SP4	Аренда по DHCP Windows 98 SE	Сервер DHCP
2	Windows 2000 SP4	Аренда по DHCP Windows 2000 SP4	Сервер DHCP
3	Windows 2000 SP4	Статический адрес Windows 2000 SP4	Служба DHCP на клиентской стороне
4	Windows 2000 SP4	Аренда по DHCP Windows 2000 SP3	Сервер DHCP
5	Windows 2000 SP4	Статический адрес Windows 2000 SP3	Служба DHCP на клиентской стороне

Примечание 1. DHCP-сервер на базе ОС Windows 98 SE не встречается. Служба клиента DHCP в этой ОС не способна производить динамические обновления, поэтому:

- В случае статического адреса, ее A и PTR записи для клиента Windows 98 SE могут быть обновлены только вручную.
- В случае аренды адреса за нее это делает DHCP-сервер, если он настроен для динамических обновлений, и он также настроен для поддержки Pre-Windows 2000 клиентов (в экспериментах 1-й серии именно такие настройки, важно было проверить работу DHCP сервера).

Примечание 2. В Windows 2000 именно служба DHCP Client, а не служба DNS Client выполняет динамические обновления в DNS. DNS Client – это всего лишь Name Resolver и только. Другое дело, кто именно непосредственно взаимодействует с DNS сервером:

- В случае статического адреса DHCP Client напрямую работает с DNS сервером для обновления A и PTR записей, если это разрешено в TCP/IP настройках клиента (в экспериментах 3-й и 5-й серии именно такие настройки, важно было проверить службу клиента DHCP Client).
- В случае аренды адреса, если:
  - DHCP-сервер не настроен для динамических обновлений, то служба клиента DHCP Client обновляет A и PTR записи.
  - DHCP-сервер настроен для обновлений по запросу клиента, то DHCP сервер обновляет PTR-запись, а служба клиента DHCP Client обновляет A-запись.
  - DHCP-сервер настроен для безусловных динамических обновлений, то DHCP сервер обновляет A и PTR записи, служба клиента DHCP Client при этом не пытается ничего обновлять (в экспериментах 2-й и 4-й серии именно такие настройки, важно было проверить работу DHCP сервера).

Итак, на данном этапе делаем следующий вывод – проблеме появляется при двух условий:

- DHCP служба (клиента или сервера), непосредственно посылающая запрос DNS серверу на обновление данных в зоне прямого просмотра, работает под управлением системы MS Windows 2000 Service Pack 4
- Зона, в которой производятся обновления, является зоной 1-го уровня (назовем такую зону для краткости “проблемной”).

Теперь, посмотрим на то, какие вообще могут варианты сочетания условий и то, какие из них и в каких экспериментах они были рассмотрены:

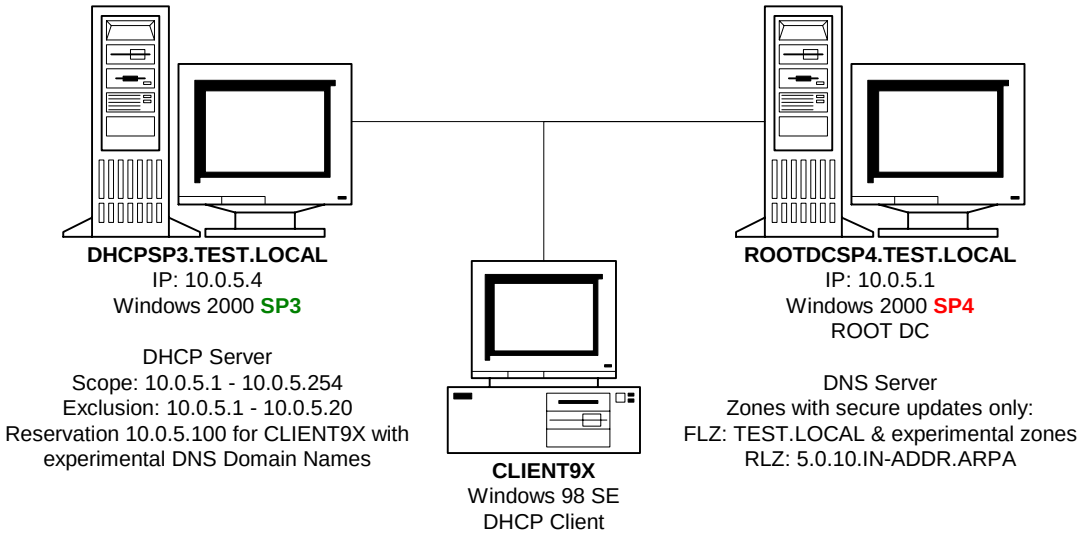
№	Служба, обращающаяся к DNS с запросом на обновление A-записи	ОС службы	Категория зоны	Эксперименты
1	Служба DHCP клиента	Service Pack 3	Не проблемная зона	5.1.1 – 5.3.3
2	Служба DHCP клиента	Service Pack 3	Проблемная зона	5.4.1 – 5.4.4
3	Служба DHCP клиента	Service Pack 4	Не проблемная зона	3.1.1 – 3.3.3
4	Служба DHCP клиента	Service Pack 4	Проблемная зона	3.4.1 – 3.4.4
5	Сервер DHCP	Service Pack 3	Не проблемная зона	не рассмотрены
6	Сервер DHCP	Service Pack 3	Проблемная зона	не рассмотрены
7	Сервер DHCP	Service Pack 4	Не проблемная зона	1.1.1 – 1.3.3 2.1.1 – 2.3.3 4.1.1 – 4.3.3
8	Сервер DHCP	Service Pack 4	Проблемная зона	1.4.1 – 1.4.4 2.4.1 – 2.4.4 4.4.1 – 4.4.4

Не проверены варианты 5 и 6. Можно предположить то, что в обоих вариантах будут положительные результаты. Однако, это необходимо проверить.

Очевидно, что для проверки вариантов 5 и 6 необходим сервер DHCP на базе ОС MS Windows 2000 AS Service Pack 3. DNS-сервер должен оставаться на старой машине под управлением ОС MS Windows 2000 SP4, как это было изначально. Поэтому DHCP-сервер будет разворачиваться на отдельной машине DHCPSP3. Для чистоты экспериментов БД DHCP не переносится со старого DHCP сервера на DHCPSP3, новый сервер DHCP создается и настраивается заново.

Нет необходимости проводить эксперименты типа 3-й и 5-й серии, поскольку они касаются статического назначения адреса клиентам, а цель – проверить DHCP сервер.

6. DHCP-клиент на базе ОС MS Windows 98 SE
DNS сервер MS Windows 2000 AS SP4
Отдельный DHCP сервер MS Windows 2000 AS SP3
Разрешены только безопасные динамические обновления зон



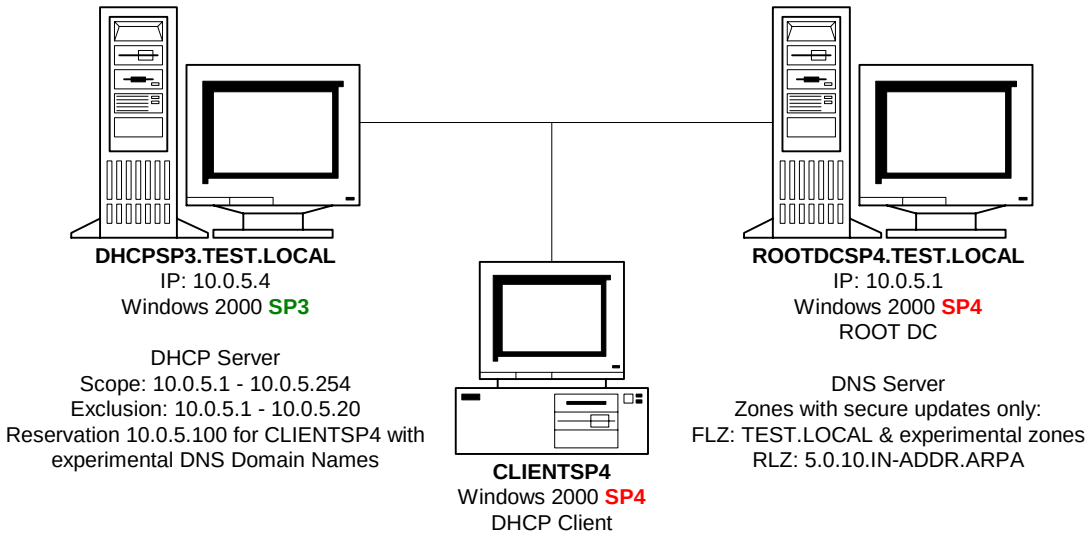
DNS-настройки клиента такие же, как в 1-й серии 10-ти экспериментов
Настройки DHCP-сервера такие же, как в 1-й серии 10-ти экспериментов

Результаты экспериментов.

#	Зона прямого просмотра	DNS Node клиента	Обновление A-записи	Обновление PTR-записи
6.1.1	**LEVEL4.LEVEL3.LEVEL2.LEVEL1**	LEVEL4		
6.2.1	**LEVEL3.LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4	LEVEL4		
6.2.2		LEVEL3		
6.3.1	**LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3	LEVEL4		
6.3.2		LEVEL3		
6.3.3		LEVEL2		
6.4.1	**LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3 в DNS-поддомене LEVEL2	LEVEL4		
6.4.2		LEVEL3		
6.4.3		LEVEL2		
6.4.4		LEVEL1		

Все четко, как и ожидалось.

7. DHCP-клиент на базе ОС MS Windows 2000 AS SP4
DNS сервер MS Windows 2000 AS SP4
Отдельный DHCP сервер MS Windows 2000 AS SP3
Разрешены только безопасные динамические обновления зон



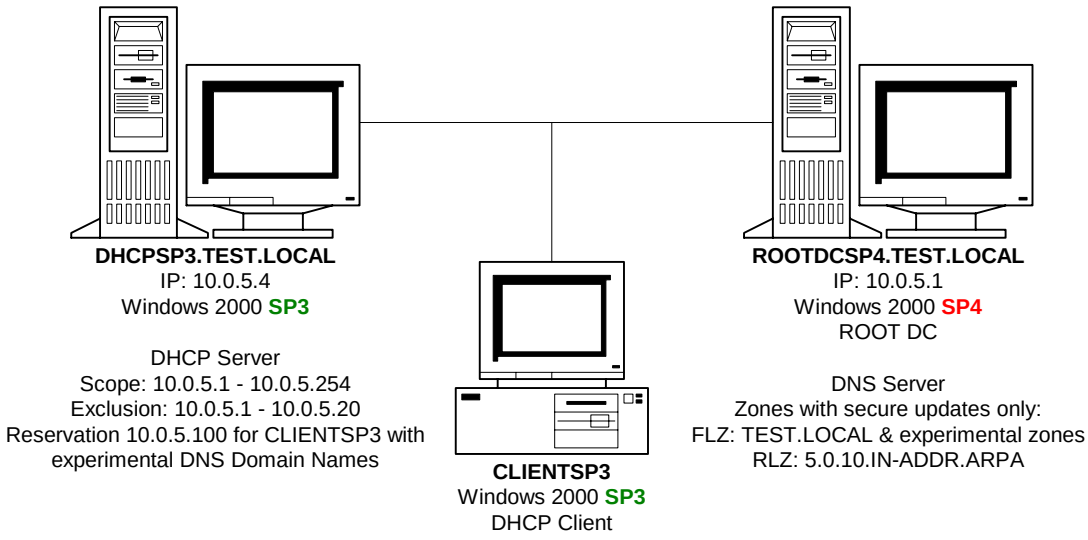
DNS-настройки клиента такие же, как во 2-й и 4-й серии 10-ти экспериментов
Настройки DHCP-сервера такие же, как в 1-й серии 10-ти экспериментов

Результаты экспериментов.

#	Зона прямого просмотра	DNS Node клиента	Обновление A-записи	Обновление PTR-записи
7.1.1	**LEVEL4.LEVEL3.LEVEL2.LEVEL1**	LEVEL4		
7.2.1	**LEVEL3.LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4	LEVEL4		
7.2.2		LEVEL3		
7.3.1	**LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3	LEVEL4		
7.3.2		LEVEL3		
7.3.3		LEVEL2		
7.4.1	**LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3 в DNS-поддомене LEVEL2	LEVEL4		
7.4.2		LEVEL3		
7.4.3		LEVEL2		
7.4.4		LEVEL1		

Все четко. Лишнее подтверждение тому, что именно DHCP сервер (Win2K AS SP3) взаимодействовал с DNS сервером, а не служба DHCP клиента (Win2K AS SP4)

8. DHCP-клиент на базе ОС MS Windows 2000 AS SP3
DNS сервер MS Windows 2000 AS SP4
Отдельный DHCP сервер MS Windows 2000 AS SP3
Разрешены только безопасные динамические обновления зон



DNS-настройки клиента такие же, как во 2-й и 4-й серии 10-ти экспериментов
Настройки DHCP-сервера такие же, как в 1-й серии 10-ти экспериментов

Результаты экспериментов.

#	Зона прямого просмотра	DNS Node клиента	Обновление A-записи	Обновление PTR-записи
8.1.1	**LEVEL4.LEVEL3.LEVEL2.LEVEL1**	LEVEL4		
8.2.1	**LEVEL3.LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4	LEVEL4		
8.2.2		LEVEL3		
8.3.1	**LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3	LEVEL4		
8.3.2		LEVEL3		
8.3.3		LEVEL2		
8.4.1	**LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3 в DNS-поддомене LEVEL2	LEVEL4		
8.4.2		LEVEL3		
8.4.3		LEVEL2		
8.4.4		LEVEL1		

Все четко. Возможно, данная проверка была избыточной, но для полноты исследования была необходима.

Итак, после дополнительных экспериментов с отдельным DHCP сервером на базе ОС MS Windows 2000 AS SP4, можем пополнить сводную таблицу по экспериментам X.4.1 – X.4.4 всех серий (X – номер серии):

№ серии	DHCP-сервер	Клиент	Служба, обращающаяся к DNS с запросом на обновление А-записи
1	Windows 2000 SP4	Аренда по DHCP Windows 98 SE	Сервер DHCP (объединен с DNS, DC)
2	Windows 2000 SP4	Аренда по DHCP Windows 2000 SP4	Сервер DHCP (объединен с DNS, DC)
3	Windows 2000 SP4	Статический адрес Windows 2000 SP4	Служба DHCP на клиентской стороне
4	Windows 2000 SP4	Аренда по DHCP Windows 2000 SP3	Сервер DHCP (объединен с DNS, DC)
5	Windows 2000 SP4	Статический адрес Windows 2000 SP3	Служба DHCP на клиентской стороне
6	Windows 2000 SP3	Аренда по DHCP Windows 98 SE	Сервер DHCP (отдельный)
7	Windows 2000 SP3	Аренда по DHCP Windows 2000 SP4	Сервер DHCP (отдельный)
8	Windows 2000 SP3	Аренда по DHCP Windows 2000 SP3	Сервер DHCP (отдельный)

Также пополняется таблица по различным вариантам сочетания условий:

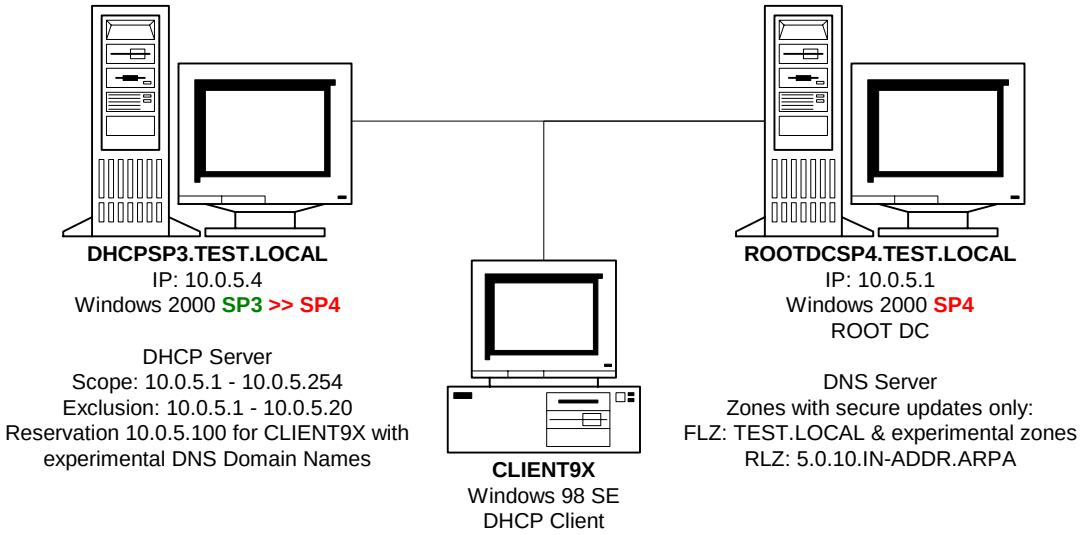
№	Служба, обращающаяся к DNS с запросом на обновление А-записи	ОС службы	Категория зоны	Эксперименты
1	Служба DHCP клиента	Windows 2000 Service Pack 3	Не проблемная зона	5.1.1 – 5.3.3
2	Служба DHCP клиента	Windows 2000 Service Pack 3	Проблемная зона	5.4.1 – 5.4.4
3	Служба DHCP клиента	Windows 2000 Service Pack 4	Не проблемная зона	3.1.1 – 3.3.3
4	Служба DHCP клиента	Windows 2000 Service Pack 4	Проблемная зона	3.4.1 – 3.4.4
5	Сервер DHCP (отдельный)	Windows 2000 Service Pack 3	Не проблемная зона	6.1.1 – 6.3.3 7.1.1 – 7.3.3 8.1.1 – 8.3.3
6	Сервер DHCP (отдельный)	Windows 2000 Service Pack 3	Проблемная зона	6.4.1 – 6.4.4 7.4.1 – 7.4.4 8.4.1 – 8.4.4
7	Сервер DHCP (объединен с DNS, DC)	Windows 2000 Service Pack 4	Не проблемная зона	1.1.1 – 1.3.3 2.1.1 – 2.3.3 4.1.1 – 4.3.3
8	Сервер DHCP (объединен с DNS, DC)	Windows 2000 Service Pack 4	Проблемная зона	1.4.1 – 1.4.4 2.4.1 – 2.4.4 4.4.1 – 4.4.4

9. DHCP-клиент на базе ОС MS Windows 98 SE (W2K SP3, SP4)
DNS сервер MS Windows 2000 AS SP4
Отдельный DHCP сервер MS Windows 2000 AS SP4
Разрешены только безопасные динамические обновления зон

Остался последний спорный момент. Интуитивно понятно, что отдельный сервер DHCP (DHCPSP3) на базе ОС MS Windows 2000 AS SP3 работает корректно не потому, что он находится отдельно от DNS-сервера (он же и контроллер домена), а именно по причине работы в условиях Service Pack 3. На эту мысль наталкивает тот факт, что при статическом назначении адресов на Windows 2000 машинах CLIENTSP3 и CLIENTSP4 корректность работы службы DHCP-клиента зависела только от версии Service Pack той ОС, в которой она работала (варианты №2 и №4 сочетания условий). Служба DHCP-клиента всегда находилась на клиентских машинах, которые ничем кроме версии Service Pack не различались. Проведя аналогию, можно было бы сказать, что это касается и службы DHCP-сервера: неважно то, на какой машине она работает, важно какой версии Service Pack той ОС, под управлением которой служба работает.

Для того чтобы достоверно проверить этот момент, достаточно установить Service Pack 4 на DHCPSP3 и проверить корректность его работы с проблемной зоной, взяв любого из DHCP-клиентов. То есть необходимо рассмотреть следующее сочетания:

9	Сервер DHCP (отдельный)	Windows 2000 Service Pack 4	Не проблемная зона	не рассмотрены
10	Сервер DHCP (отдельный)	Windows 2000 Service Pack 4	Проблемная зона	не рассмотрены



DNS-настройки клиента такие же, как в 1-й серии 10-ти экспериментов
Настройки DHCP-сервера такие же, как в 1-й серии 10-ти экспериментов

Итак, после установки Service Pack 4 на DHCP-сервер, повторяем эксперименты 6.1.1 – 6.4.4 и получаем результаты:

#	Зона прямого просмотра	DNS Node клиента	Обновление A-записи	Обновление PTR-записи
9.1.1	**LEVEL4.LEVEL3.LEVEL2.LEVEL1**	LEVEL4		
9.2.1	**LEVEL3.LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4	LEVEL4		
9.2.2		LEVEL3		
9.3.1	**LEVEL2.LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3	LEVEL4		
9.3.2		LEVEL3		
9.3.3		LEVEL2		
9.4.1	**LEVEL1** с DNS-поддоменом LEVEL4 в DNS-поддомене LEVEL3 в DNS-поддомене LEVEL2	LEVEL4		
9.4.2		LEVEL3		
9.4.3		LEVEL2		
9.4.4		LEVEL1		

Другого результата и не должно было быть. После установки Service Pack 4 на DHCPSP3 (теперь это уже отдельно стоящий сервер DHCP), он стал некорректно работать с проблемной зоной.

Нет смысла проводить аналогичные эксперименты с DHCP-клиентами Windows 2000 SP3 и Windows 2000 SP4. Результаты будут идентичны.

Соответственно, теперь заполняем 9-ю и 10-ю строки таблицы сочетаний условий:

9	Сервер DHCP (отдельный)	Windows 2000 Service Pack 4	Не проблемная зона	9.1.1 – 9.3.3
10	Сервер DHCP (отдельный)	Windows 2000 Service Pack 4	Проблемная зона	9.4.1 – 9.4.4

И видим то, результат такой же, что и в 7-й и 8-й строках таблицы сочетаний условий, где DHCP сервер так работал под управлением ОС MS Windows 2000 SP4, но располагался вместе с DNS, DC.

Отсюда делаем вывод о том, что местоположение службы сервера DHCP не имеет никакого значения. Неважно то, на какой машине она работает, важно какой версии Service Pack той ОС, под управлением которой служба работает

Заключение по проведенным экспериментам со службами DHCP

Запишем окончательно эмпирические знания в табличном виде:

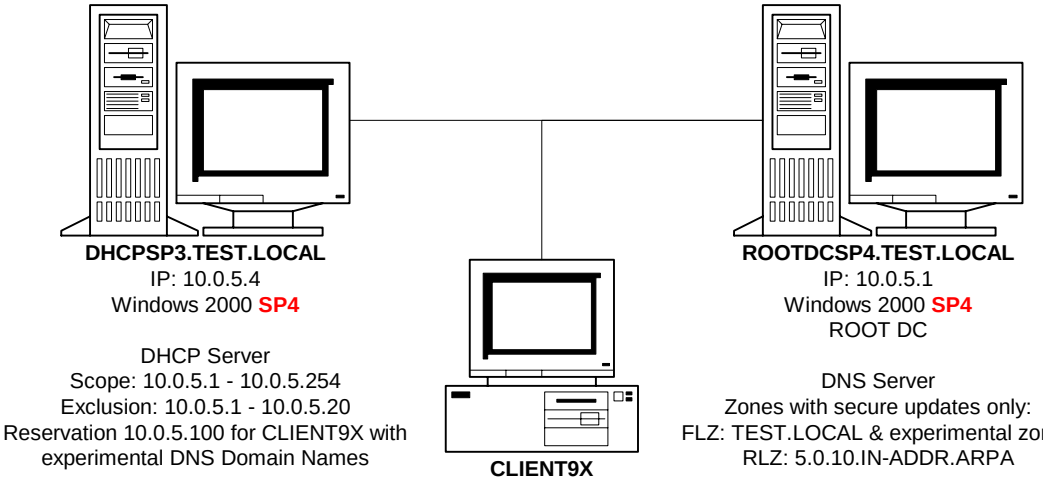
№	Служба, обращающаяся к DNS с запросом на обновление A-записи	ОС службы	Категория зоны	Запись “A” автоматически обновляется?
1	Служба DHCP клиента	Windows 2000 Service Pack 3	Не проблемная зона	Да
2	Служба DHCP клиента	Windows 2000 Service Pack 3	Проблемная зона	Да
3	Служба DHCP клиента	Windows 2000 Service Pack 4	Не проблемная зона	Да
4	Служба DHCP клиента	Windows 2000 Service Pack 4	Проблемная зона	Нет
5	Служба сервера DHCP (отдельный)	Windows 2000 Service Pack 3	Не проблемная зона	Да
6	Служба сервера DHCP (отдельный)	Windows 2000 Service Pack 3	Проблемная зона	Да
7	Служба сервера DHCP (объединен с DNS, DC)	Windows 2000 Service Pack 4	Не проблемная зона	Да
8	Служба сервера DHCP (объединен с DNS, DC)	Windows 2000 Service Pack 4	Проблемная зона	Нет
9	Сервер DHCP (отдельный)	Windows 2000 Service Pack 4	Не проблемная зона	Да
10	Сервер DHCP (отдельный)	Windows 2000 Service Pack 4	Проблемная зона	Нет

Вывод:

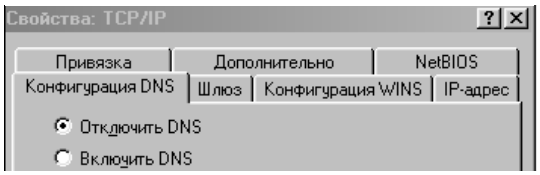
- Для появления проблемы необходимы два условия:
  - DHCP служба (клиента или сервера), непосредственно посылающая запросы к DNS серверу работает под управлением системы Windows 2000 Service Pack 4.
  - Зона, в которой должны производится обновления, является зоной 1-го уровня.
- При иных сочетаниях условий проблема не проявляется.
- Не имеет никакого значения то, располагается ли служба сервера DHCP на отдельной машине или вместе с DNS и DC. Важна только версия Service Pack ОС.

Анализ журнала сервера DNS для одного успешного и одного неудачного обновления зоны прямого просмотра

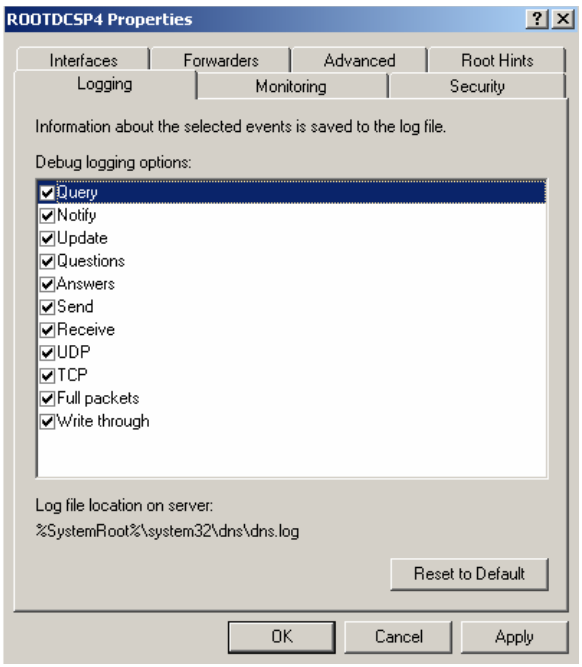
10. DHCP-клиент на базе ОС MS Windows 98 SE
DNS сервер MS Windows 2000 AS SP4 с ведением журнала
Отдельный DHCP сервер MS Windows 2000 AS SP4
Разрешены только безопасные динамические обновления зон



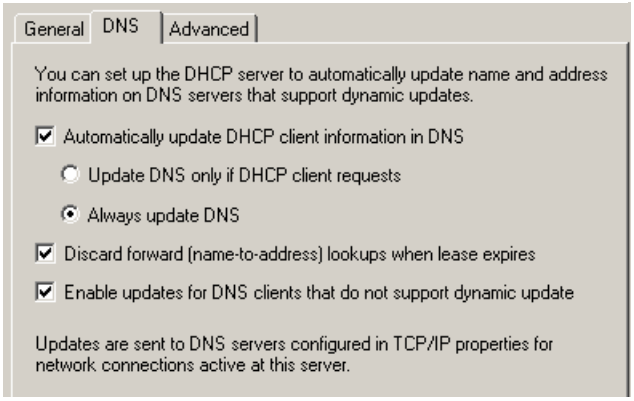
DNS-настройки клиента



Настройка ведения журнала DNS сервера

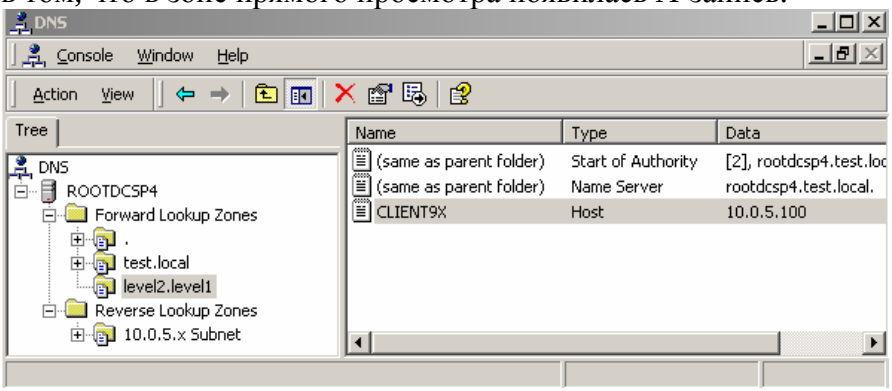


Настройки DHCP сервера для работы с DNS

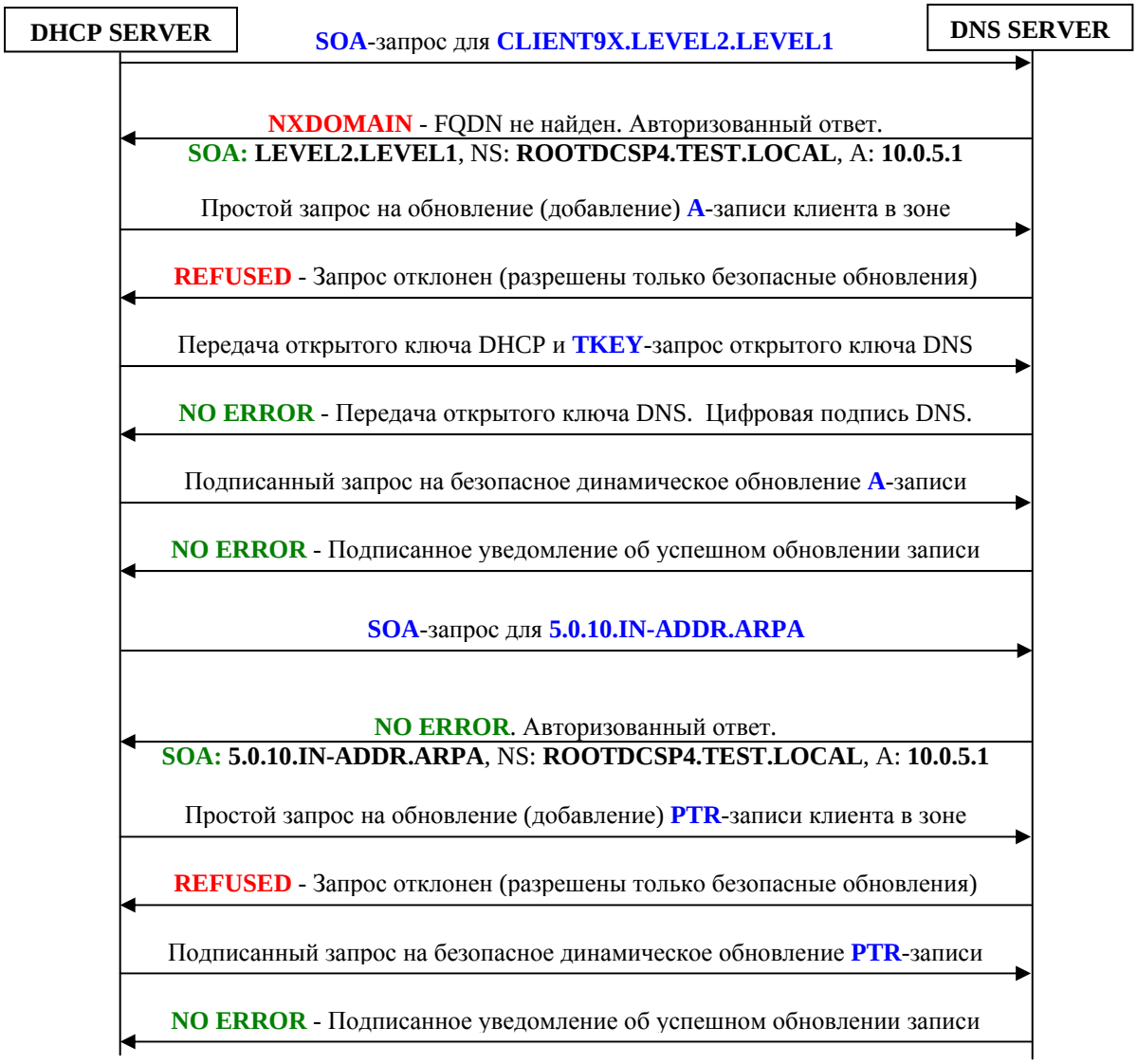


10.1. Зона прямого просмотра: LEVEL2.LEVEL1.
Зона обратного просмотра: 5.0.10.IN-ADDR.ARPA.
DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL2 с IP: 10.0.5.100

- Создаем AD-Integrated зону прямого просмотра **LEVEL2.LEVEL1**
- Создаем резервацию 10.0.5.100 для CLIENT9X и настраиваем опцию DNS Domain Name – LEVEL2.LEVEL1. Обновляем аренду на клиентской стороне и убеждаемся в том, что в зоне прямого просмотра появилась A-запись:

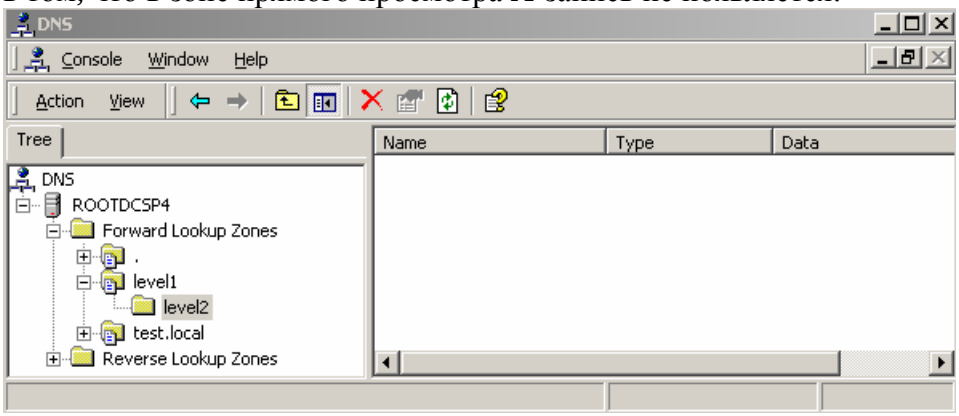


- Анализируем журнал DNS сервера. Записываем в виде протокола взаимодействие DHCP сервера (Windows 2000 Service Pack 4) с сервером DNS (Windows 2000 Service Pack 4) при успешном обновлении записей в не проблемной зоне.

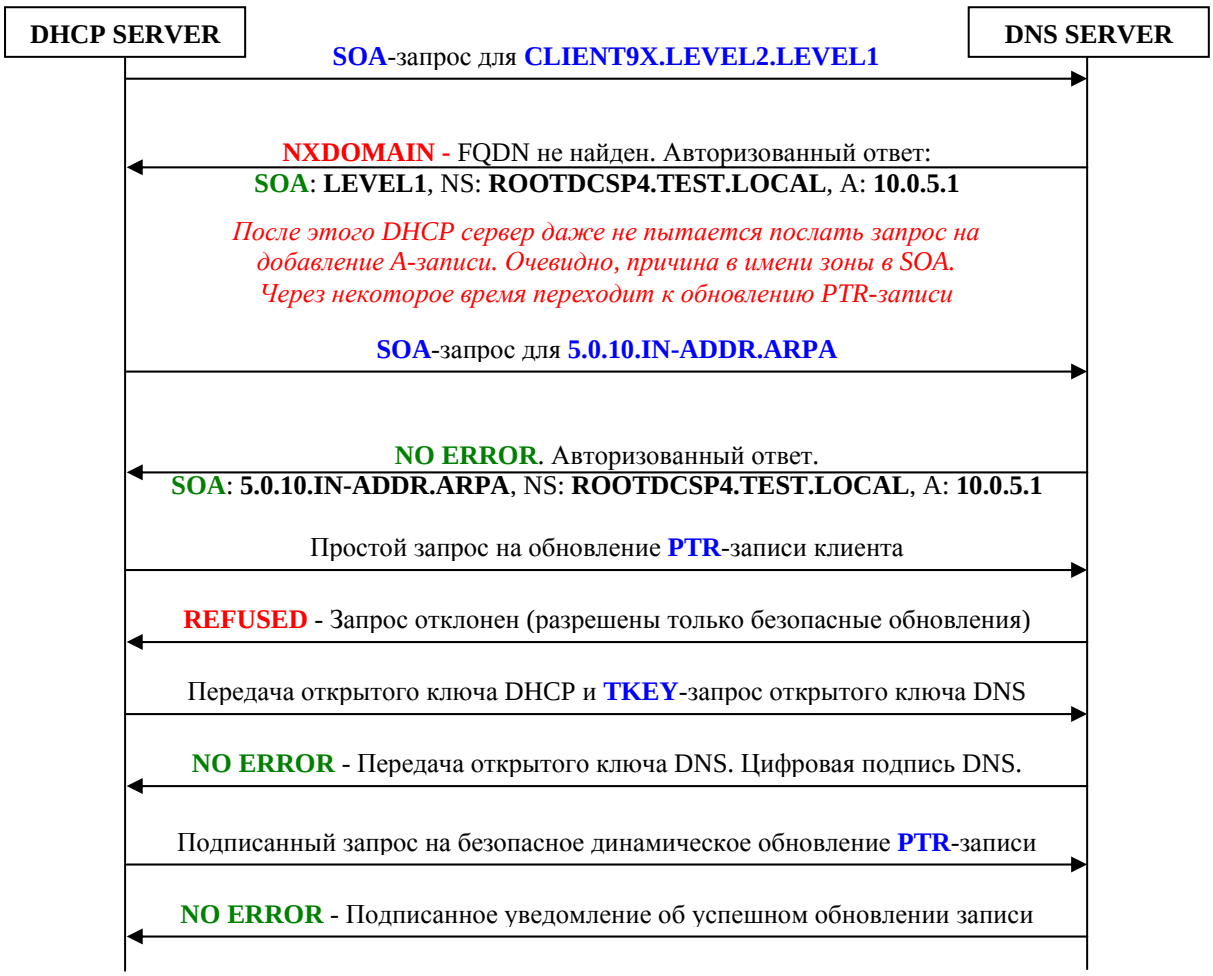


10.2. Зона прямого просмотра: LEVEL1.
В этой зоне создается DNS-поддомен LEVEL2
Зона обратного просмотра: 5.0.10.IN-ADDR.ARPA.
DHCP-сервер регистрирует CLIENT9X в DNS Node LEVEL2 с IP: 10.0.5.100

- Создаем AD-Integrated зону **LEVEL1**. В нем создаем DNS-поддомен LEVEL2.
- Создаем резервацию 10.0.5.100 для CLIENT9X и настраиваем опцию DNS Domain Name – LEVEL2.LEVEL1. Обновляем аренду на клиентской стороне и убеждаемся в том, что в зоне прямого просмотра A-запись не появляется:



- Анализируем журнал DNS сервера. Записываем в виде протокола взаимодействие DHCP сервера (Windows 2000 Service Pack 4) с сервером DNS (Windows 2000 Service Pack 4) при неудачном обновлении A-записи в проблемной зоне.



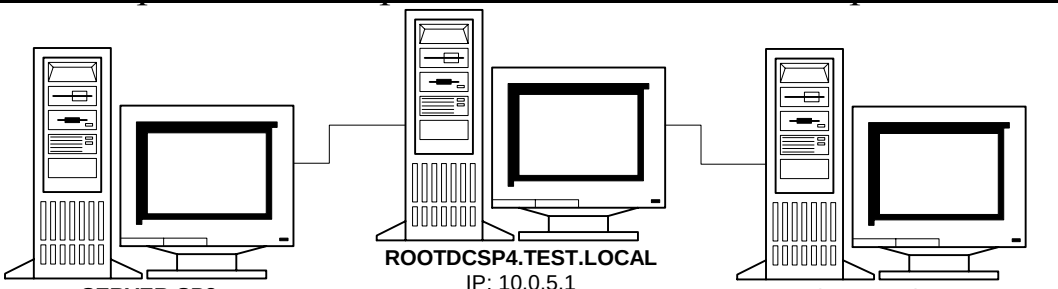
Заключение по анализу журнала службы DNS при успешном и неудачном обновлениях A-записи в зоне прямого просмотра.

По результатам анализа можно сделать вывод о том, что служба сервера DNS не является причиной некорректной работы с проблемными зонами служб DHCP Server и DHCP Client, работающих под управлением ОС MS Windows 2000 SP4. Причина в том, что службы DHCP (под W2K AS SP4), получив в ответе на SOA-запрос имя зоны первого уровня, отказываются дальше с ней работать. Такова особенность этих служб в ОС MS Windows 2000 SP4.

Часть 2. Эксперименты с зонами прямого просмотра и службой NETLOGON контроллеров AD-домена

1. DNS сервер MS Windows 2000 AS SP4
Создание контроллеров корневых доменов отдельных несвязанных лесов на базе Windows 2000 AS SP3 и Windows 2000 AS SP4

1.1. Эксперименты с корневыми доменами в не проблемных зонах

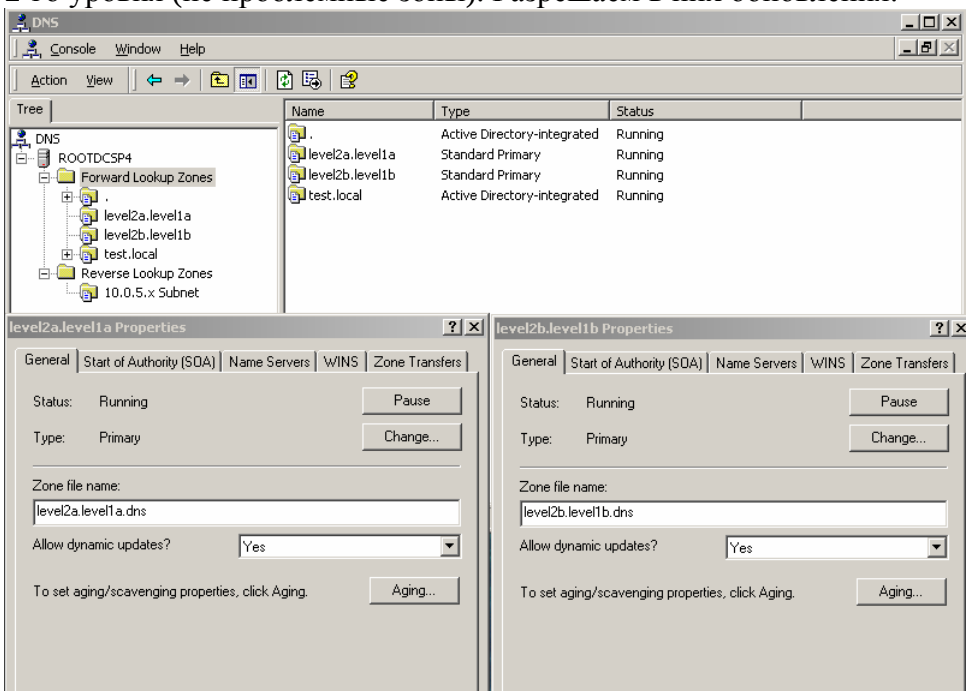


SERVER-SP3
IP: 10.0.5.6
Windows 2000 **SP3**
Stand-Alone Server
We'll try to promote it to
DC for the FOREST ROOT DOMAIN
LEVEL2A.LEVEL1A

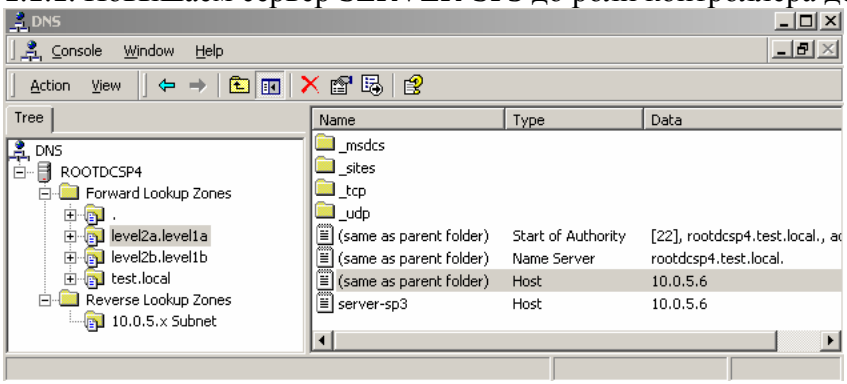
ROOTDCSP4.TEST.LOCAL
IP: 10.0.5.1
Windows 2000 **SP4**
FOREST **TEST.LOCAL** ROOT DC
DNS Server:
AD-zones with secure updates only:
FLZ: **TEST.LOCAL**
RLZ: **5.0.10.IN-ADDR.ARPA**
Experimental Standard
Primary Zones with enabled updates
LEVEL2A.LEVEL1A , LEVEL2B.LEVEL1B

SERVER-SP4
IP: 10.0.5.7
Windows 2000 **SP4**
Stand-Alone Server
We'll try to promote it to
DC for the FOREST ROOT DOMAIN
LEVEL2B.LEVEL1B

Нам важно проверить работу службы NETLOGON именно тестовых серверов, поэтому для чистоты эксперименты будем создавать новые леса, а не поддомены в лесу TEST.LOCAL. Тогда очевидно то, что тестовые контроллеры доменов не будут авторизованы в домене TEST.LOCAL и не смогут безопасно обновлять какие-либо AD integrated зоны, созданные на DNS сервере. По этой причине, для 100% гарантий того, что права доступа не будут причиной проблем обновлений, создаем две стандартные основные зоны прямого просмотра: LEVEL2A.LEVEL1A и LEVEL2B.LEVEL1B. Это зоны 2-го уровня (не проблемные зоны). Разрешаем в них обновления:

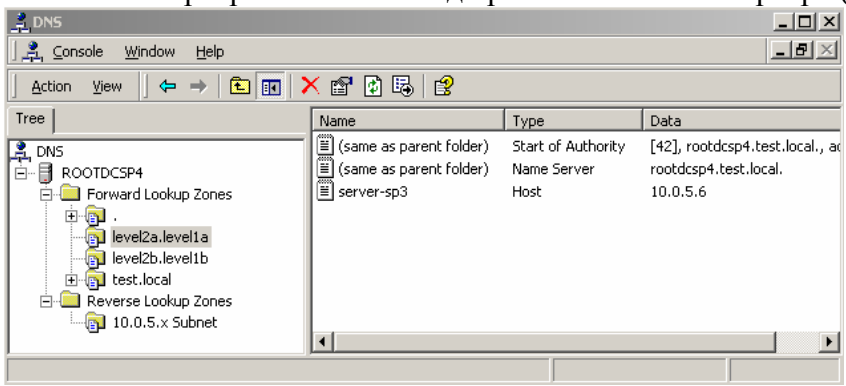


1.1.1. Повышаем сервер SERVER-SP3 до роли контроллера домена LEVEL2A.LEVEL1A:



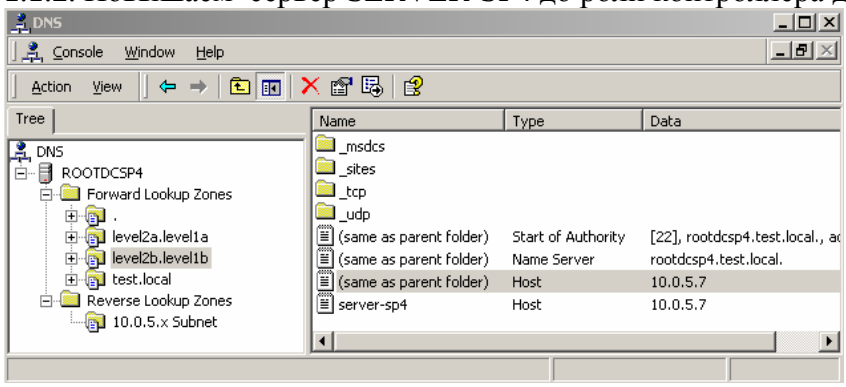
Служба NETLOGON сервера SERVER-SP3 успешно зарегистрировала SRV-записи.

Понижаем сервер SERVER-SP3 до роли Stand Alone сервера (удаляем тестовый лес):



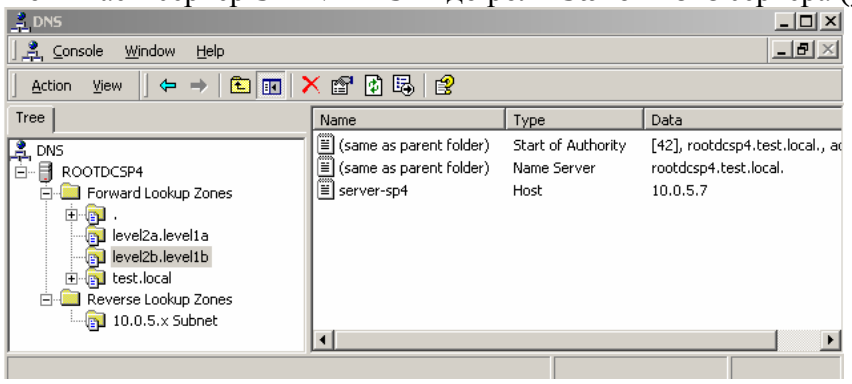
Служба NETLOGON сервера SERVER-SP3 успешно удалила SRV-записи.

1.1.2. Повышаем сервер SERVER-SP4 до роли контроллера домена LEVEL2B.LEVEL1B:



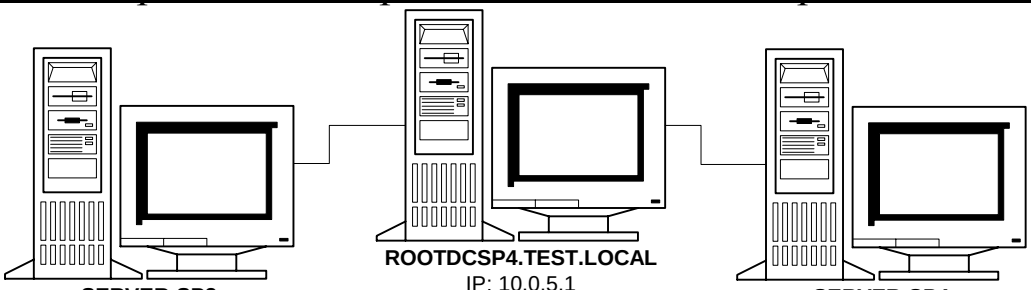
Служба NETLOGON сервера SERVER-SP4 успешно зарегистрировала SRV-записи.

Понижаем сервер SERVER-SP4 до роли Stand Alone сервера (удаляем тестовый лес):



Служба NETLOGON сервера SERVER-SP4 успешно удалила SRV-записи.

1.2. Эксперименты с корневыми доменами в проблемных зонах

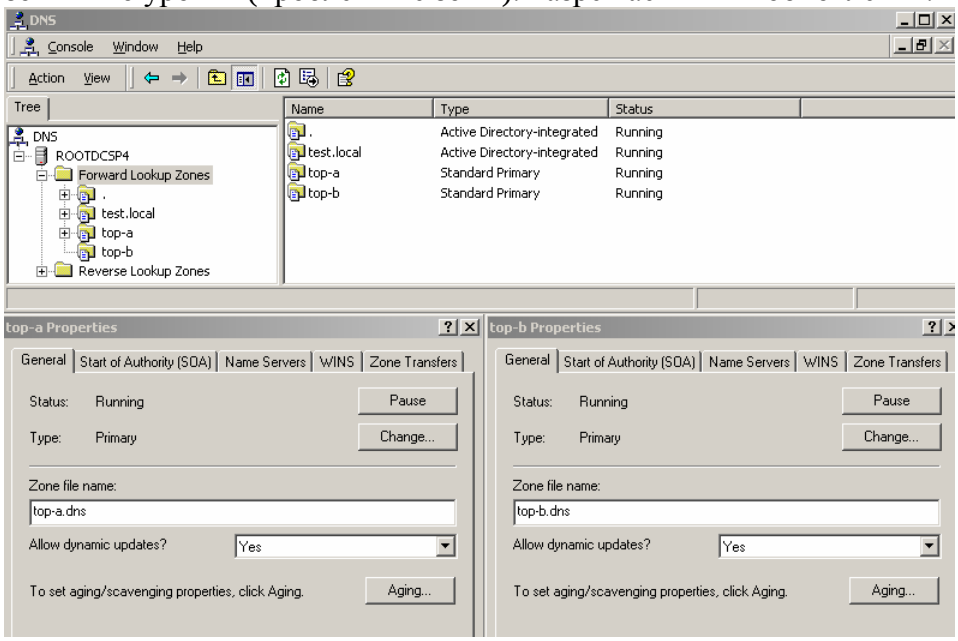


SERVER-SP3
IP: 10.0.5.6
Windows 2000 **SP3**
Stand-Alone Server
We'll try to promote it to
DC for the FOREST ROOT DOMAIN
TOP-A

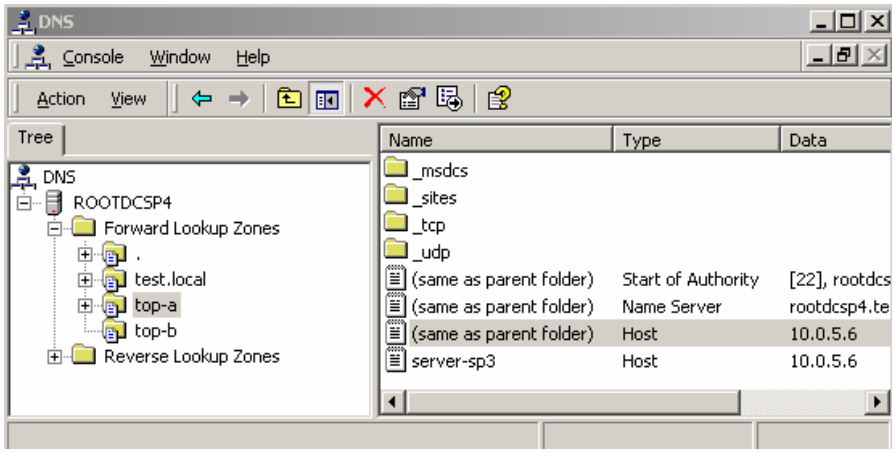
ROOTDCSP4.TEST.LOCAL
IP: 10.0.5.1
Windows 2000 **SP4**
FOREST **TEST.LOCAL** ROOT DC
DNS Server:
AD-zones with secure updates only:
FLZ: **TEST.LOCAL**
RLZ: **5.0.10.IN-ADDR.ARPA**
Experimental Standard
Primary Zones with enabled updates
TOP- A , TOP- B

SERVER-SP4
IP: 10.0.5.7
Windows 2000 **SP4**
Stand-Alone Server
We'll try to promote it to
DC for the FOREST ROOT DOMAIN
TOP-B

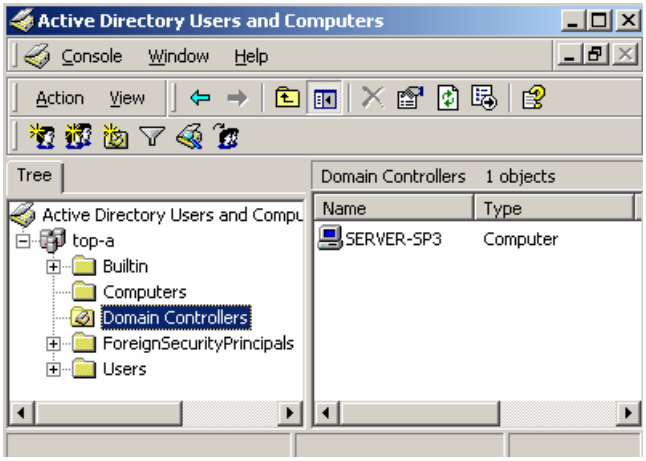
Создаем две стандартные основные зоны прямого просмотра: TOP-A и TOP-B. Это зоны 1-го уровня (проблемные зоны). Разрешаем в них обновления.



1.2.1. Повышаем сервер SERVER-SP3 до роли контроллера домена TOP-A нового дерева нового леса. После успешной операции повышения и перезагрузки, проверяем DNS:



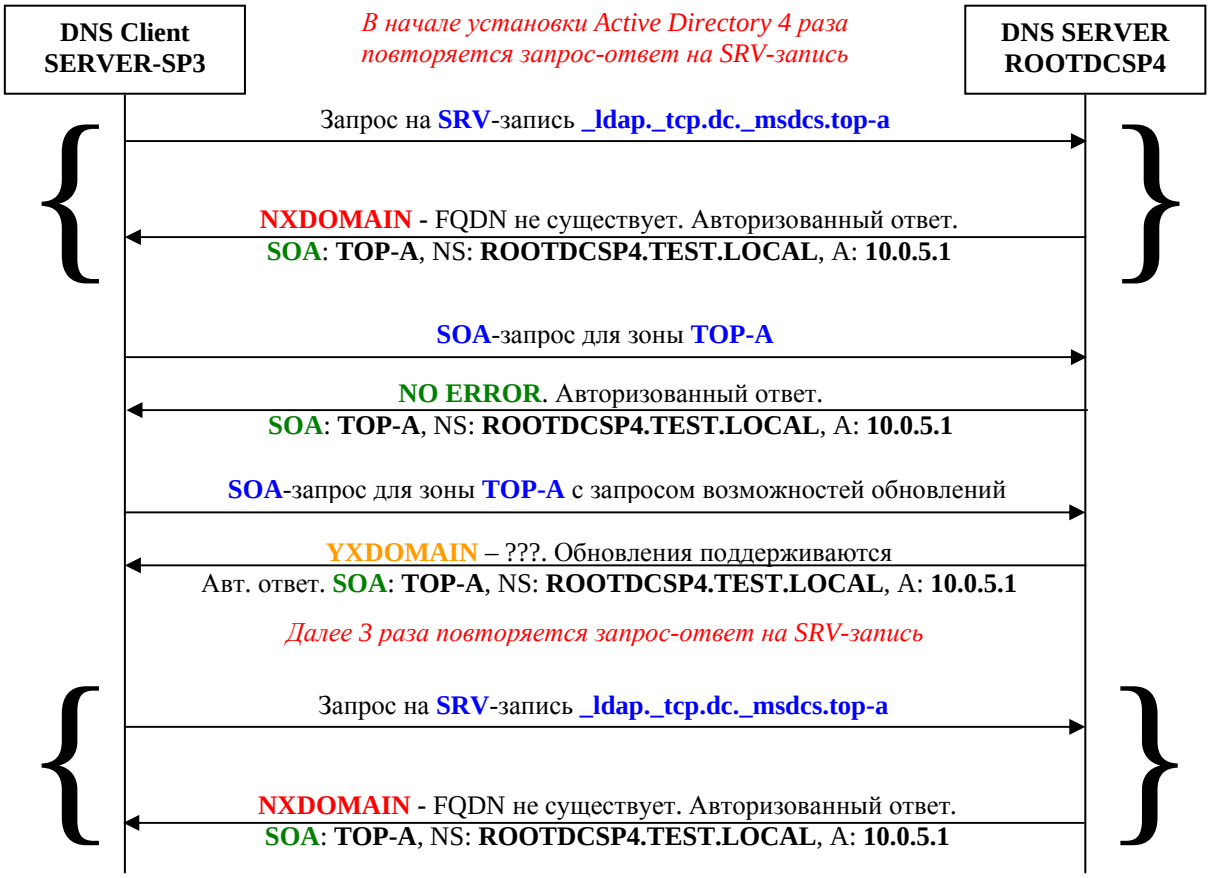
Служба NETLOGON сервера SERVER-SP3 успешно зарегистрировала SRV-записи.



AD-домен первого уровня TOP-A, действительно, успешно создался.

Посмотрим в журнале DNS то, как происходило взаимодействие с SERVER-SP3 с DNS.

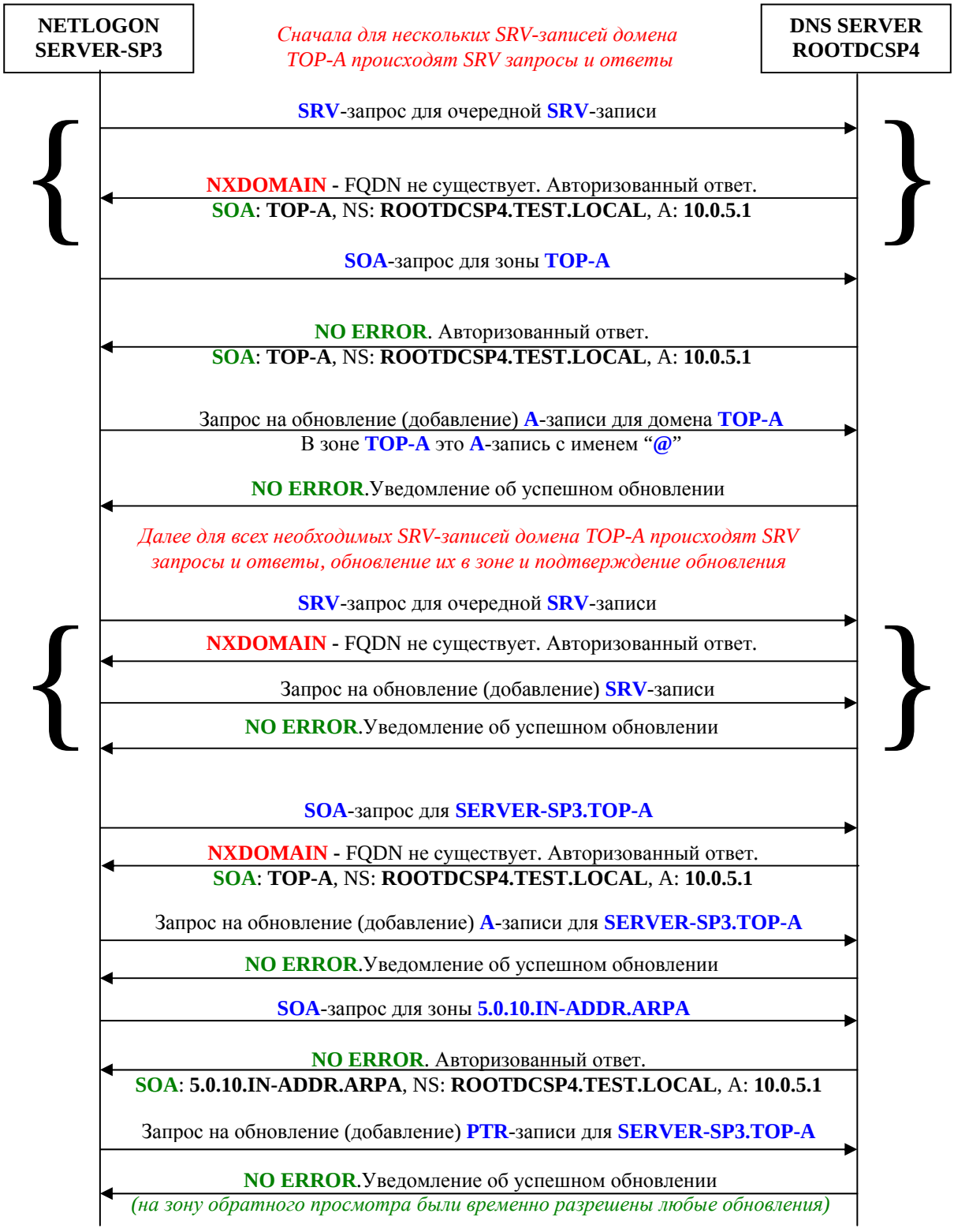
Фаза 1: Установка Active Directory (до перезагрузки SERVER-SP3):



Далее до перезагрузки SERVER-SP3, взаимодействие с DNS-сервером отсутствует.

Примечание. На запрос о возможности обновления в зоне в случае, когда зона не поддерживает обновления, DNS-сервер возвращает ответ **NOTIMP** (not implemented), а если поддерживает – то **NO ERROR**. **YXDOMAIN** означает существование DNS-домена, которого не должно быть, что это значит в данной ситуации – неизвестно, но в любом случае SERVER-SP3 не считает это негативным ответом, он выводит ошибку только в случае получения ответа **NOTIMP** (проверено экспериментально).

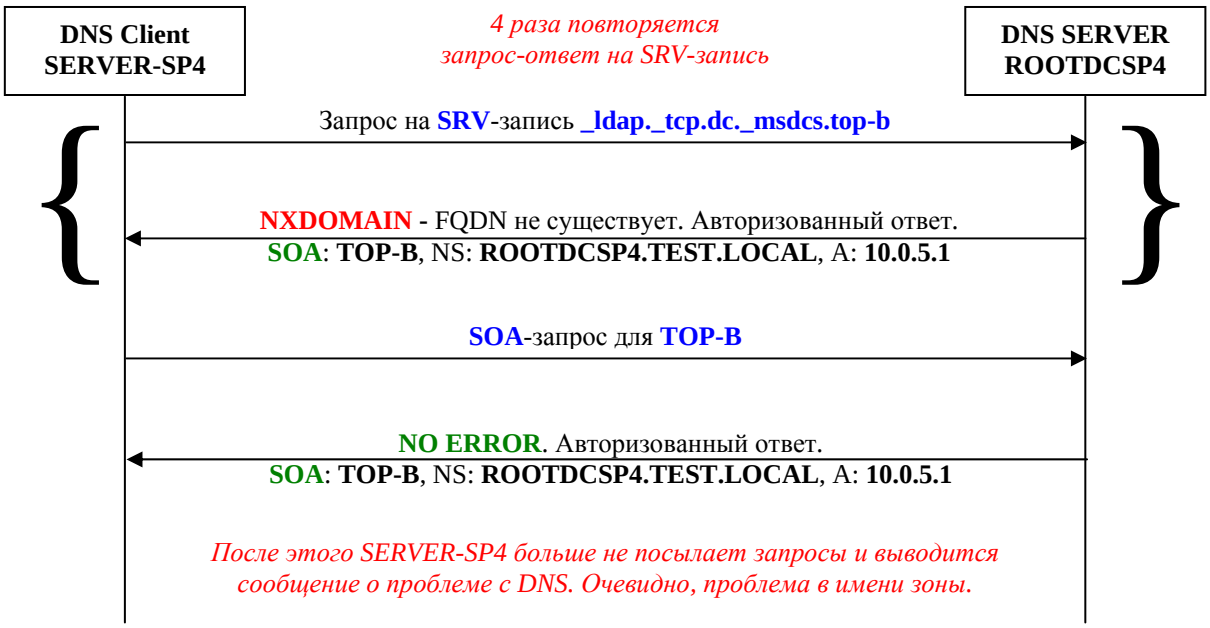
Фаза 2: Автоматическое создание SRV-записей в DNS (после перезагрузки SERVER-SP3):



Таким образом, корневой домен TOP-A нового дерева нового леса TOP-A успешно создан и все A и SRV записи успешно зарегистрированы в зоне TOP-A. Службы DNS Client и NETLOGON контроллера корневого домена SERVER-SP3 на базе ОС MS Windows 2000 AS SP3 с проблемной зоной отработали четко и корректно.

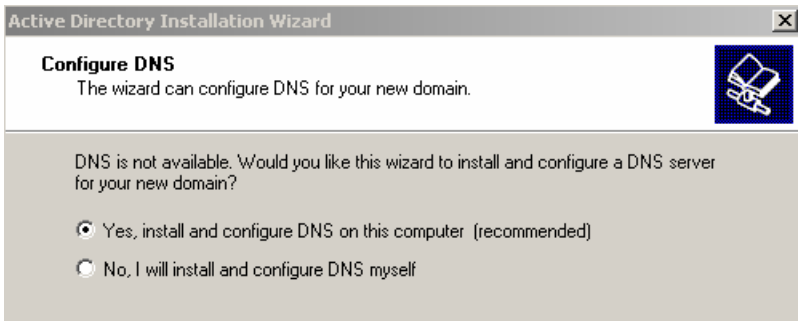
1.2.2. Пытаемся повысить сервер SERVER-SP4 до роли контроллера домена TOP-B нового дерева нового леса, и получаем следующую ошибку:

Анализ журнала DNS-сервера ROOTDCSP4 дает следующую картину (запрос делает служба DNS Client, служба NETLOGON в это время вообще не работает):

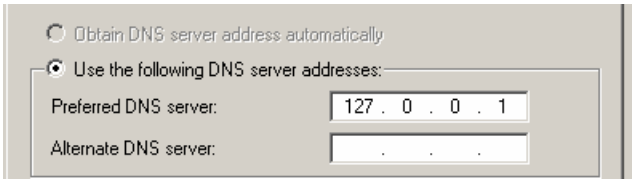


Серверу SERVER-SP4 не устраивает имя зоны “TOP-B” в SOA-ответе DNS-сервера, она решает, что зоны вообще нет на DNS-сервере! Сравнивая протокол взаимодействия с протоколом успешного повышения SERVER-SP3 до роли контроллера корневого домена (фаза до перезагрузки) в предыдущем эксперименте (1.2.1) легко замечаем, что SERVER-SP4 даже не доходит до проверки зоны на возможность обновлений, его сама по себе зона не устраивает.

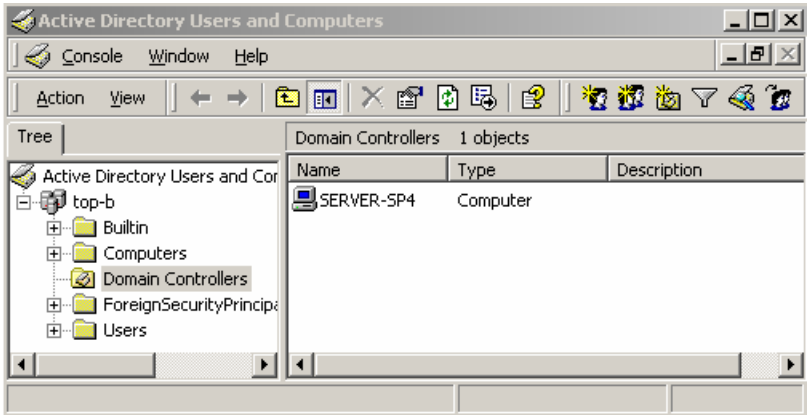
Дальше нам предлагают 2 возможных сценариев повышения SERVER-SP4: установка и использование локального DNS-сервера или отказ от его установки:



Сценарий 1. Локальный DNS сервер: Пусть на сервере SERVER-SP4 автоматически установится локальный DNS-сервер. При этом скорректируем настройки TCP/IP, чтобы SERVER-SP4 использовал не ROOTDCSP4, а локальный DNS-сервер:

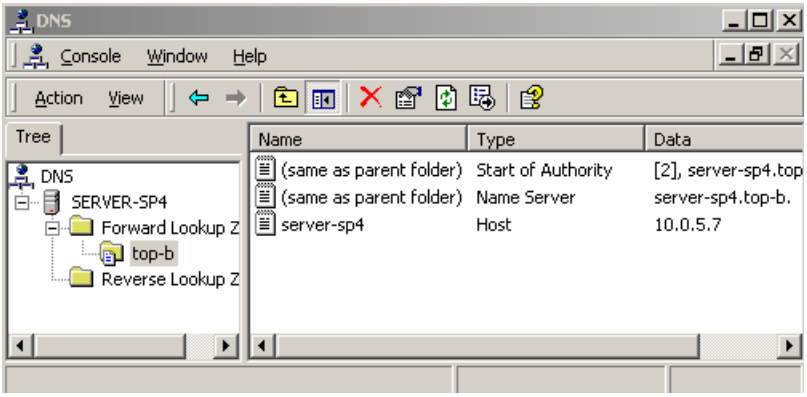


В результате домен успешно создается, после перезагрузки видим следующее:



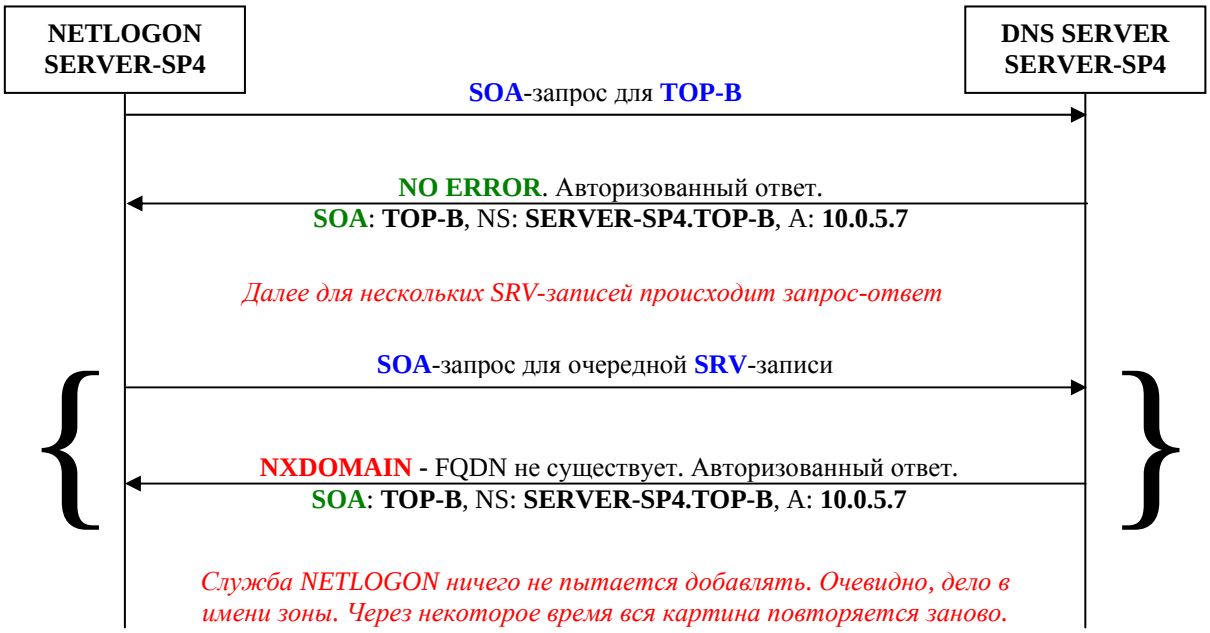
AD-домен первого уровня TOP-B, действительно, успешно создался.

На локальном сервере DNS автоматически создалась AD-Integrated зона **TOP-B**, с разрешенными безопасными динамическими обновлениями, и тем не менее:



Служба NETLOGON не добавила SRV-записи.

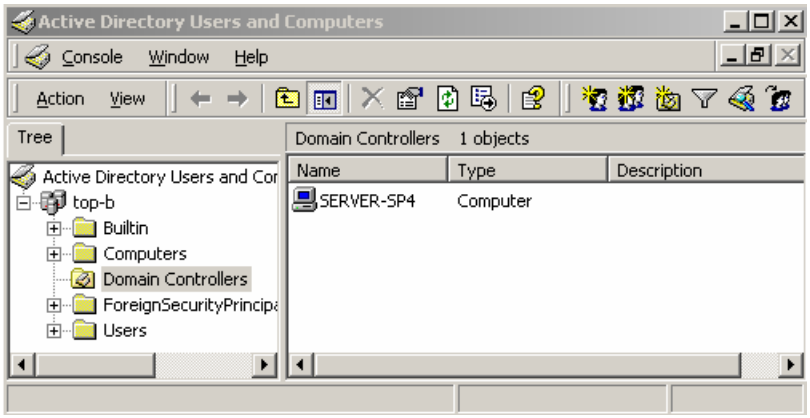
Анализ журнала DNS-сервера SERVER-SP4 дает следующую картину:



Служба NETLOGON получает отрицательные ответы на запросы на SRV-записи, но это означает то, что SRV-записи нет и ее необходимо создать, ведь запись должна быть в зоне TOP-B и SERVER-SP4 полномочный DNS-сервер для этой зоны. Просматривая протокол (фаза после перезагрузки) предыдущего эксперимента (1.2.1), видим то, что сервер SERVER-SP3, не найдя необходимые A и SRV-записи, без проблем создал их в зоне TOP-A, в которой полномочным серверов является корневой DNS-сервер ROOTDCSP4.

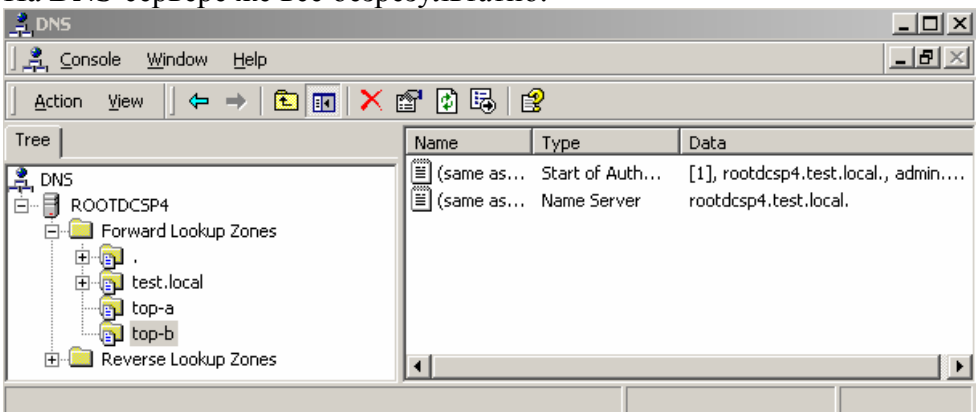
Сценарий 2. Отказ от локального DNS сервера: Мы откажемся от установки локального сервера DNS, и в TCP/IP настройках SERVER-SP4 в качестве DNS-сервера останется исходно назначенный DNS-сервер, полномочный в зоне **TOP-B –** ROOTDCSP4. Так или иначе, сервер SERVER-SP4 будет взаимодействовать с этим DNS-сервером.

В результате домен успешно создается, после перезагрузки видим следующее:



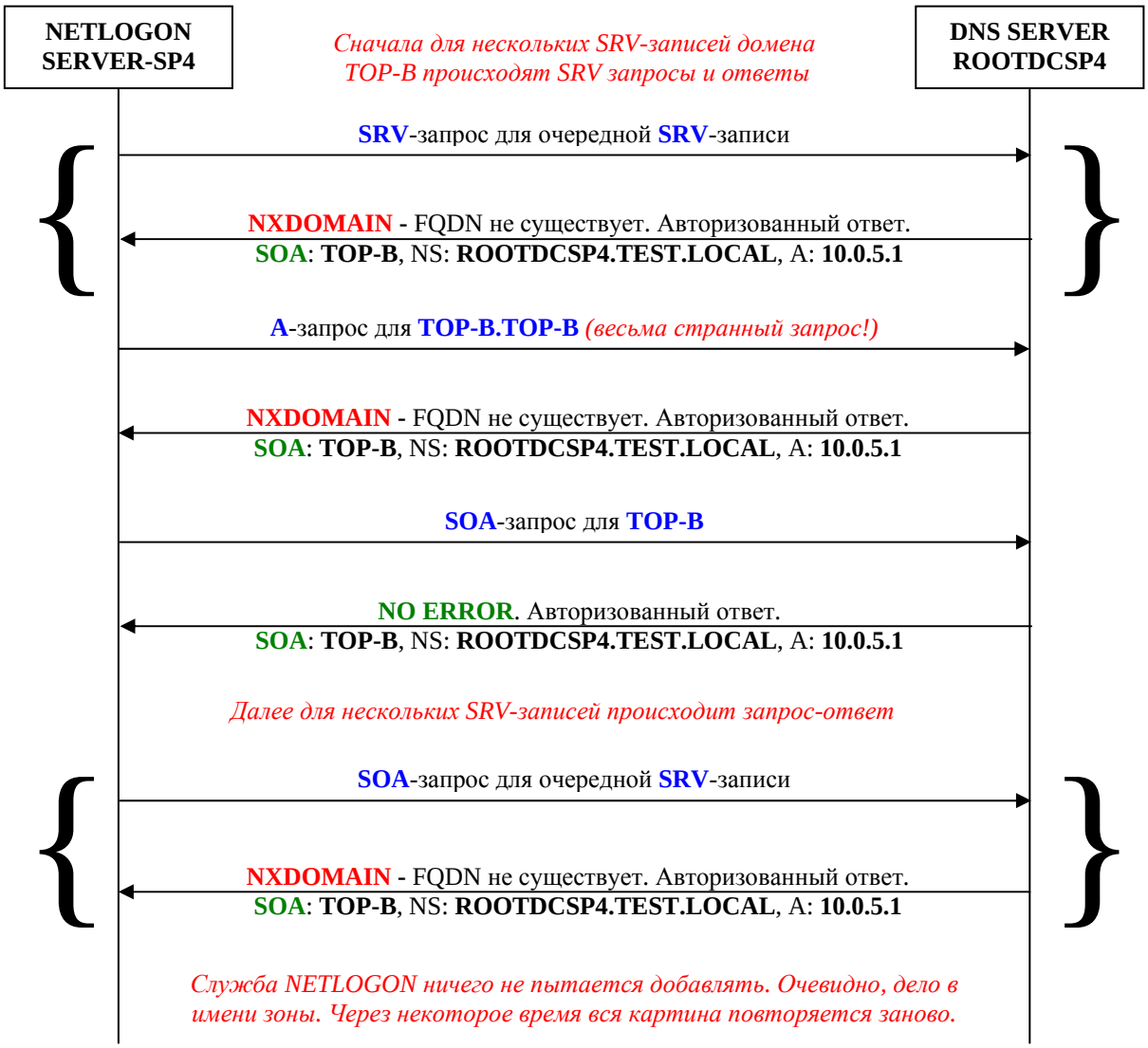
AD-домен первого уровня TOP-B, действительно, успешно создался.

На DNS-сервере же все безрезультатно:



Служба NETLOGON не добавила SRV-записи.

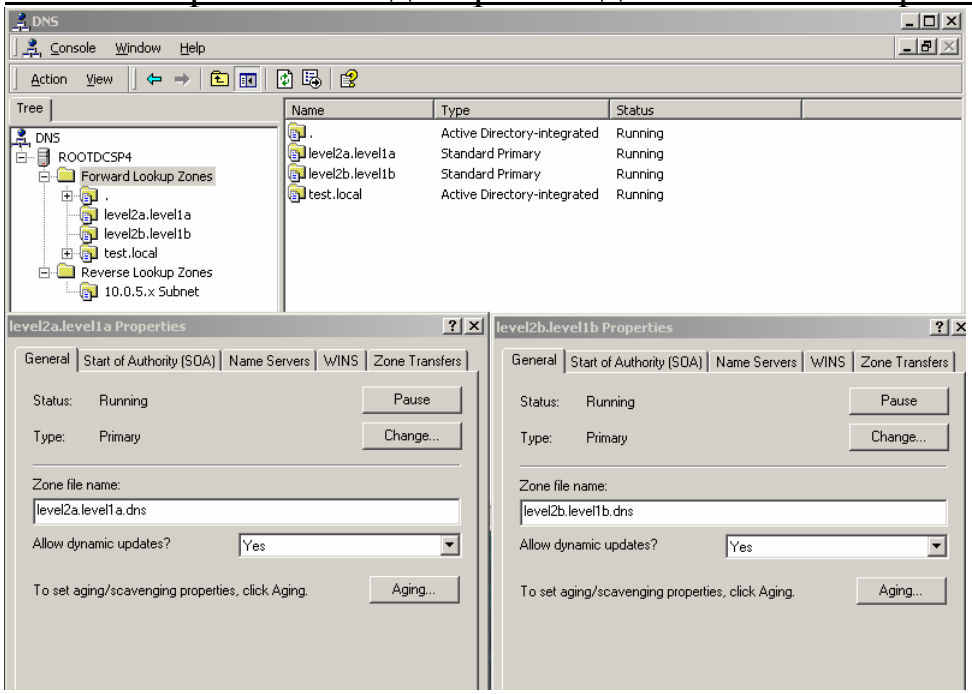
Анализ журнала DNS-сервера SERVER-SP4 дает следующую картину:



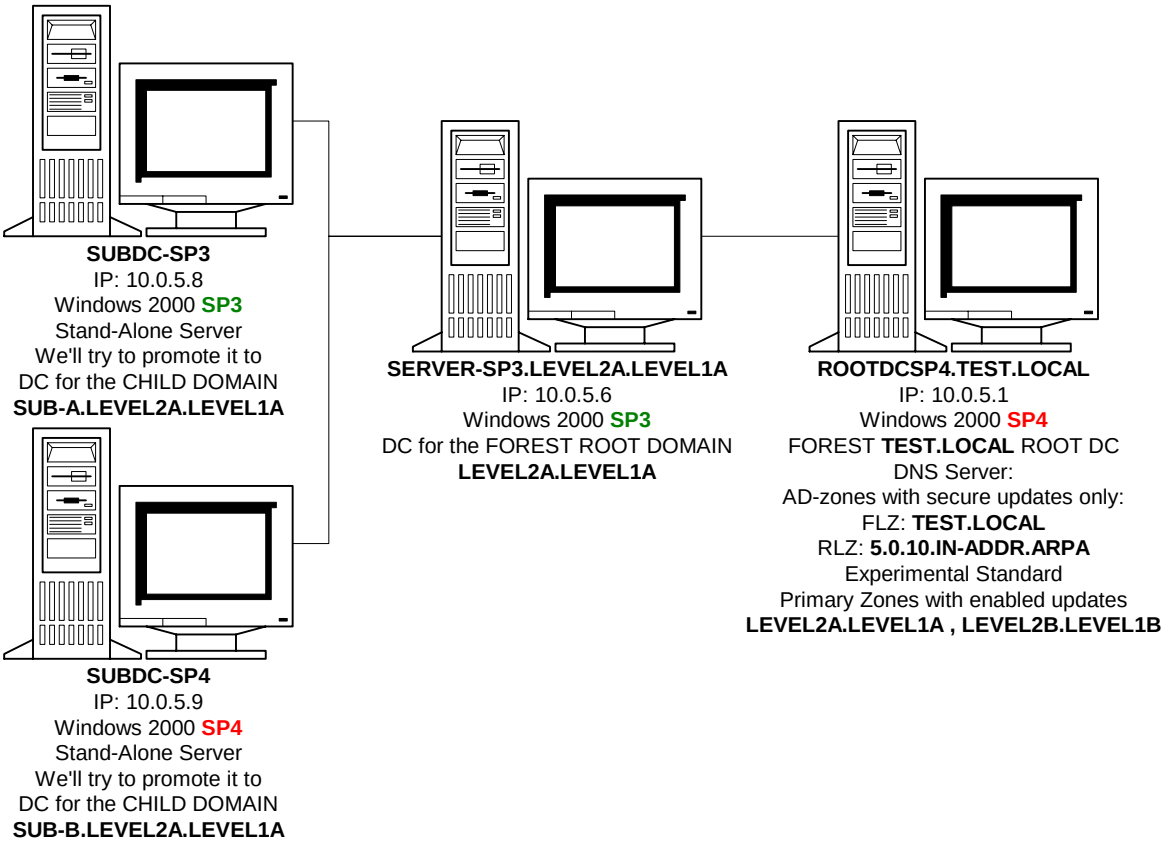
Что же, результат по второму сценарию по существу не отличается от результатов первого: служба NETLOGON не создает необходимые A и SRV-записи, и с таким контроллером домена вряд ли можно нормально в дальнейшем работать и взаимодействовать. Можно, конечно, вручную создать SRV-записи, но обновляться они не будут автоматически, и это будет вызывать массу проблем.

2. DNS сервер MS Windows 2000 AS SP4
Использование контроллеров корневых доменов отдельных несвязанных лесов на базе Windows 2000 AS SP3 и Windows 2000 AS SP4 для создания в корневых доменах контроллеров дочерних доменов на базе Windows 2000 AS SP3 и Windows 2000 AS SP4

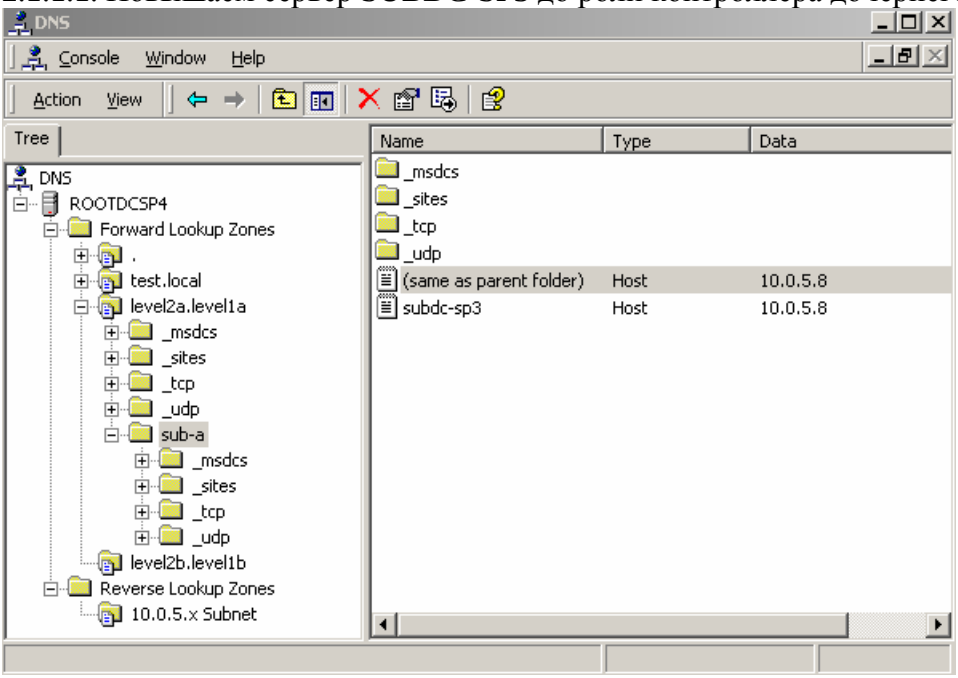
2.1. Эксперименты с дочерними доменами в не проблемных зонах



2.1.1 Контроллер корневого домена на базе ОС MS Windows 2000 AS SP3

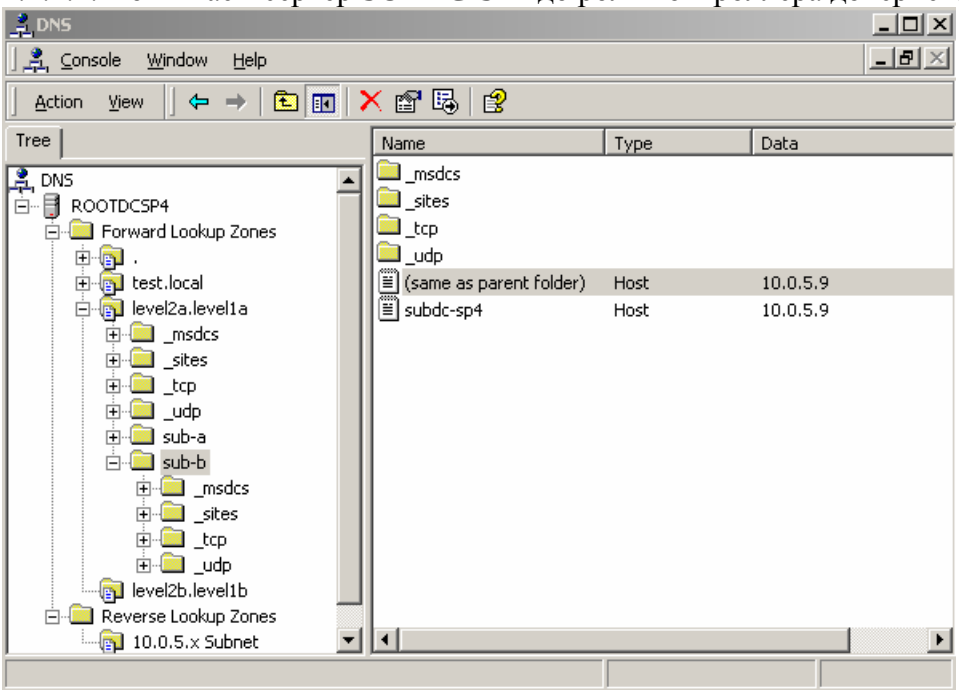


2.1.1.1. Повышаем сервер SUBDC-SP3 до роли контроллера дочернего домена SUB-A:

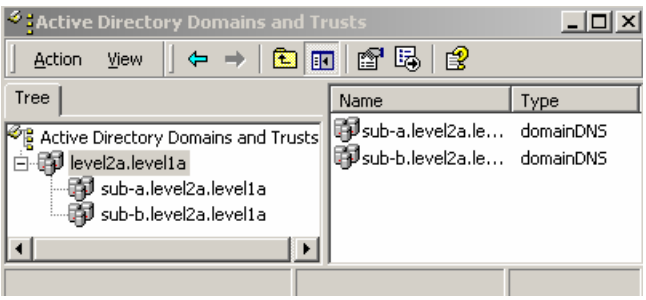


Служба NETLOGON сервера SUBDC-SP3 успешно зарегистрировала SRV-записи.

2.1.1.2. Повышаем сервер SUBDC-SP4 до роли контроллера дочернего домена SUB-B:

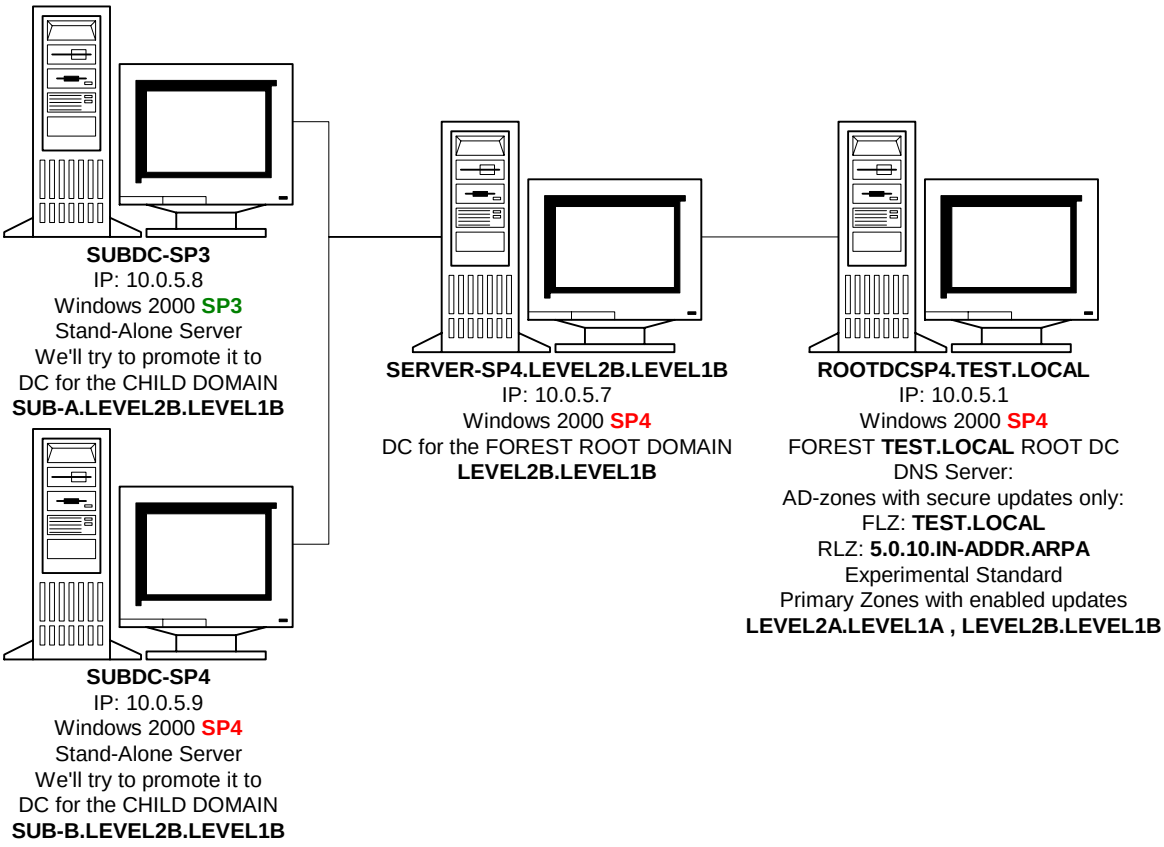


Служба NETLOGON сервера SUBDC-SP4 успешно зарегистрировала SRV-записи.

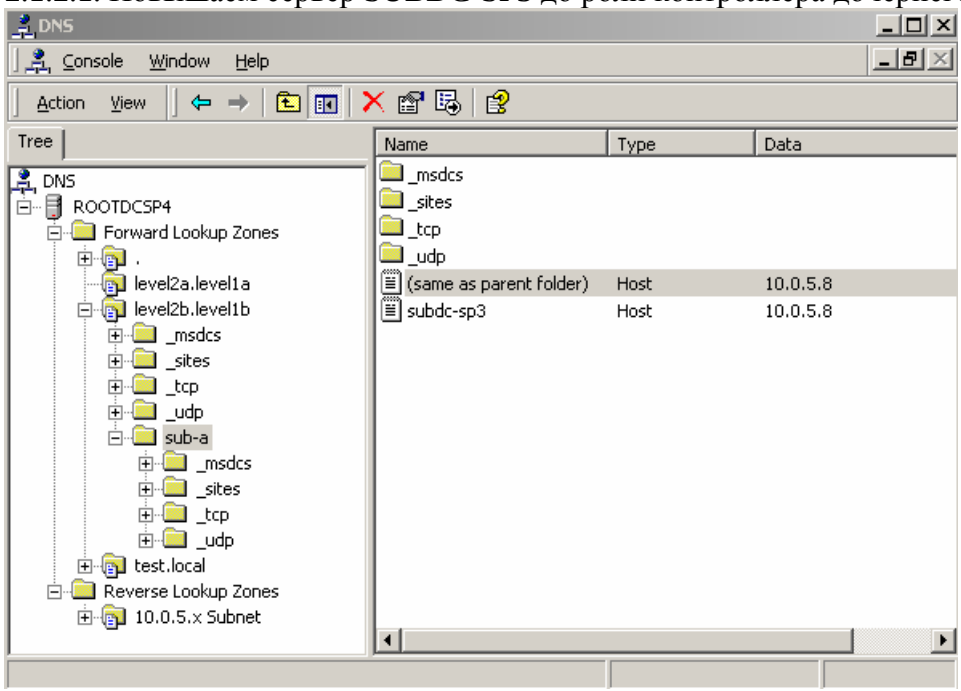


Дочерние домены присутствуют в Active Directory

2.1.2 Контроллер корневого домена на базе ОС MS Windows 2000 AS SP4

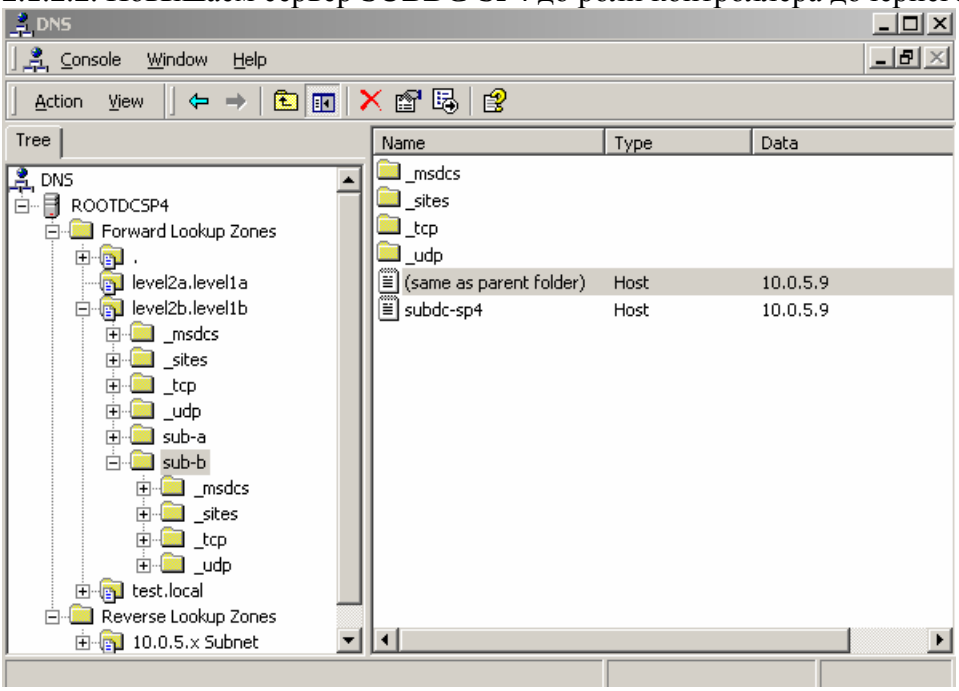


2.1.2.1. Повышаем сервер SUBDC-SP3 до роли контроллера дочернего домена SUB-A:

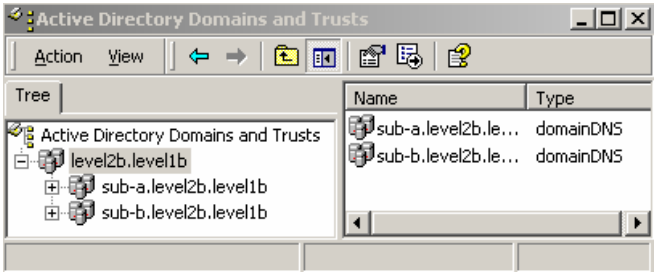


Служба NETLOGON сервера SUBDC-SP3 успешно зарегистрировала SRV-записи.

2.1.2.2. Повышаем сервер SUBDC-SP4 до роли контроллера дочернего домена SUB-B:

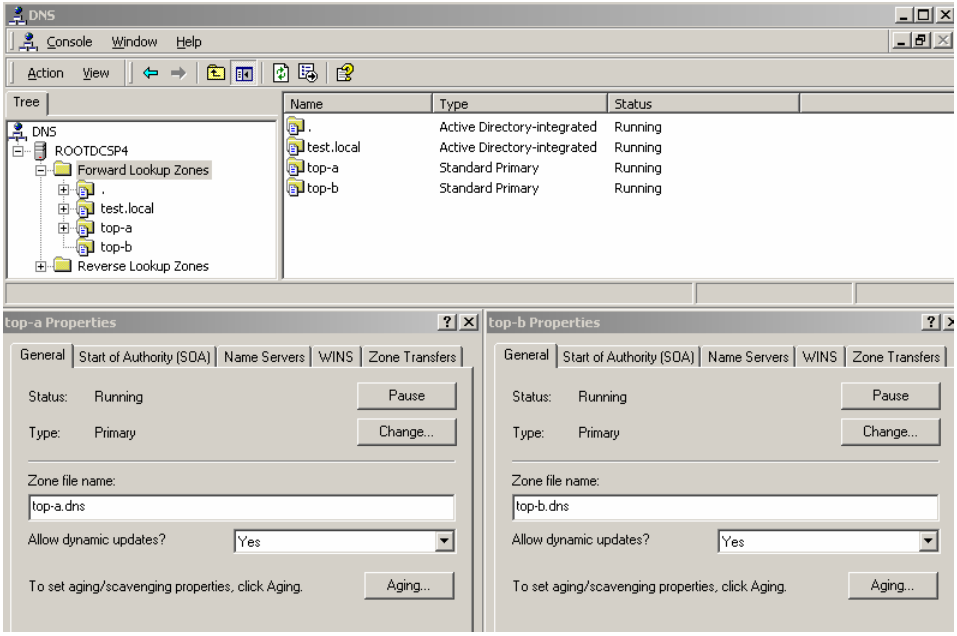


Служба NETLOGON сервера SUBDC-SP4 успешно зарегистрировала SRV-записи.

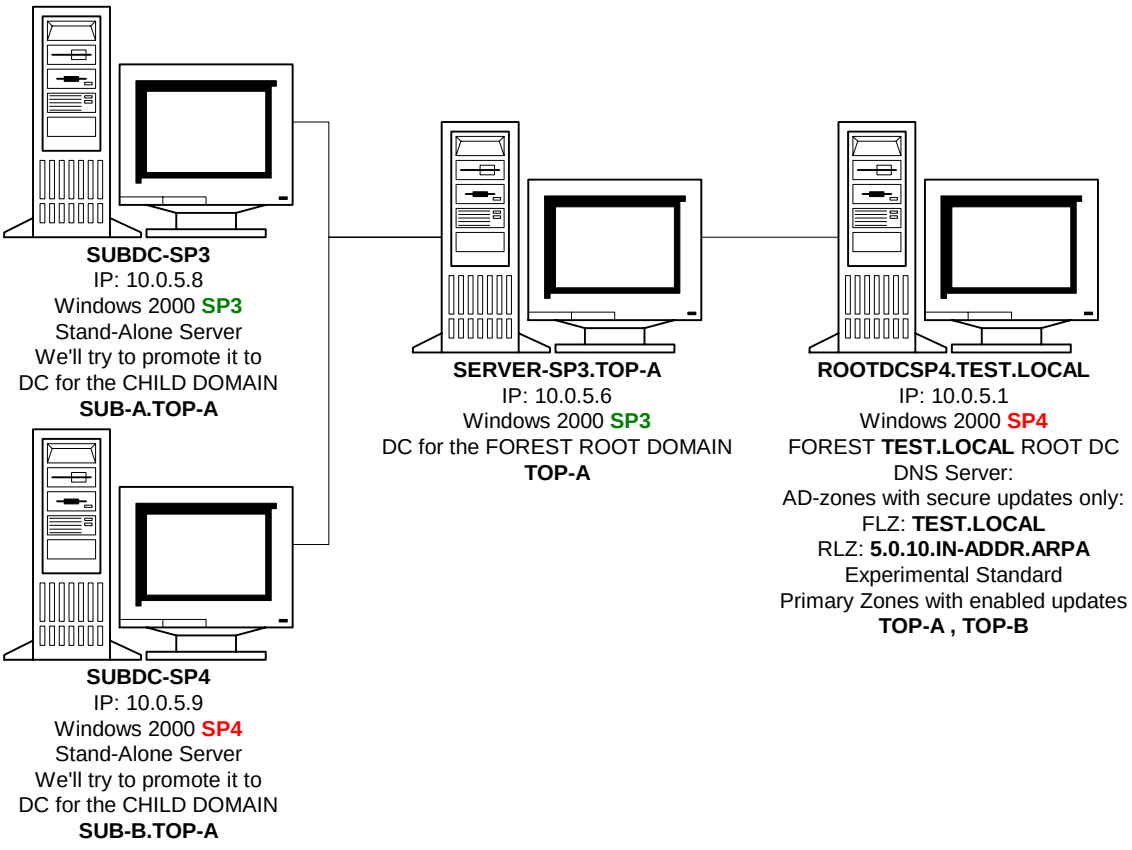


Дочерние домены присутствуют в Active Directory

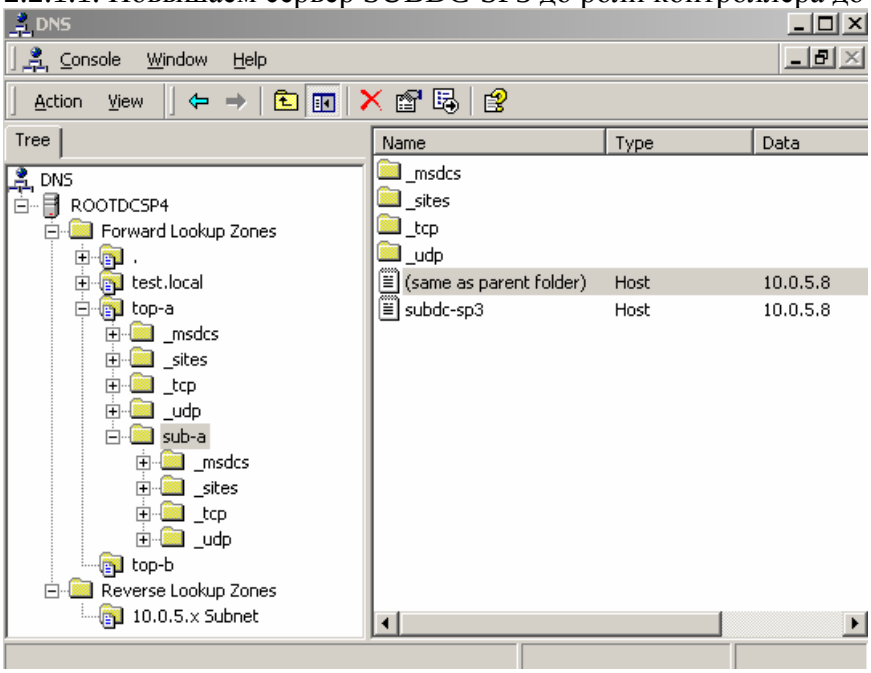
2.2. Эксперименты с дочерними доменами в проблемных зонах



2.2.1 Контроллер корневого домена на базе ОС MS Windows 2000 AS SP3



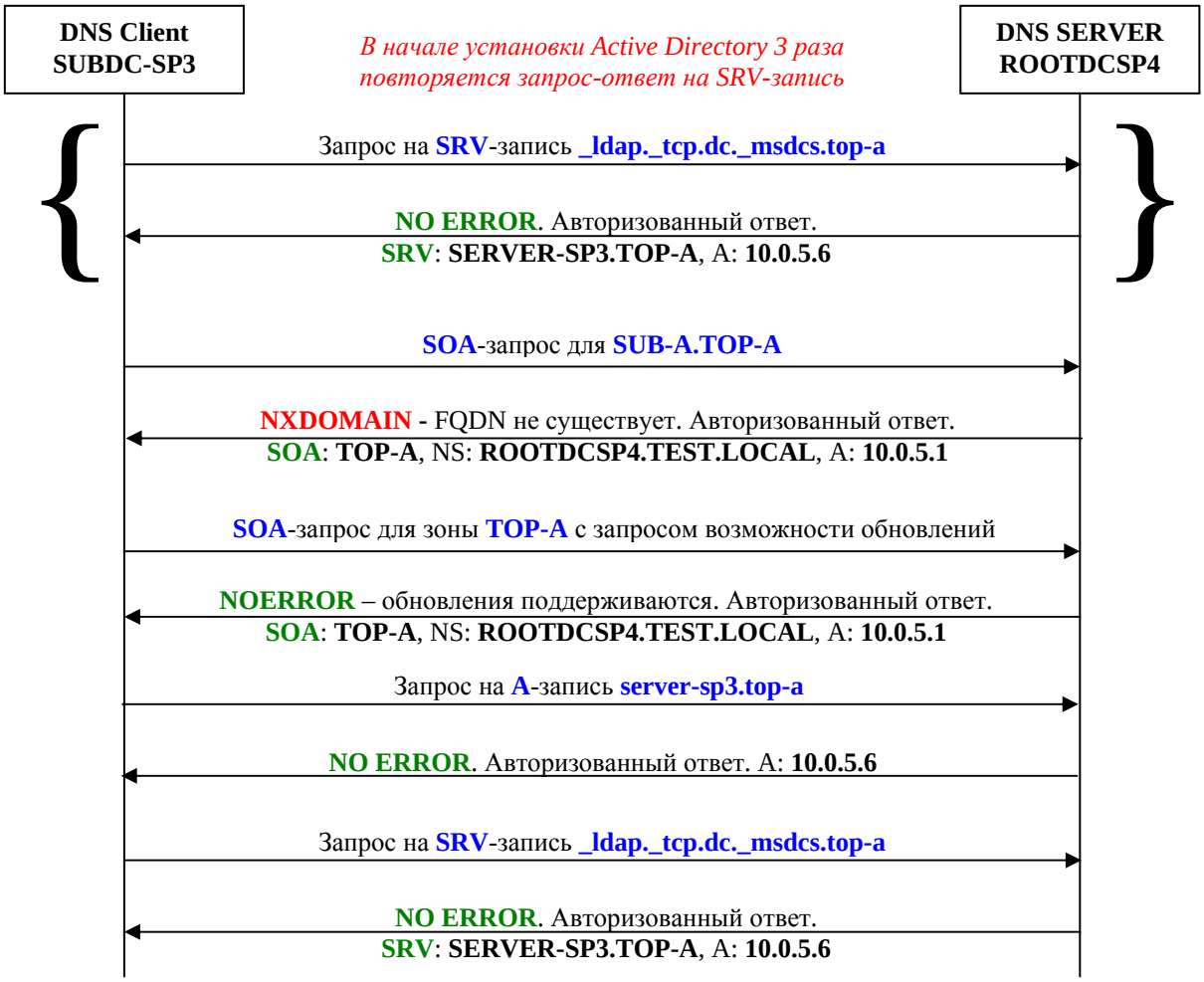
2.2.1.1. Повышаем сервер SUBDC-SP3 до роли контроллера дочернего домена SUB-A:



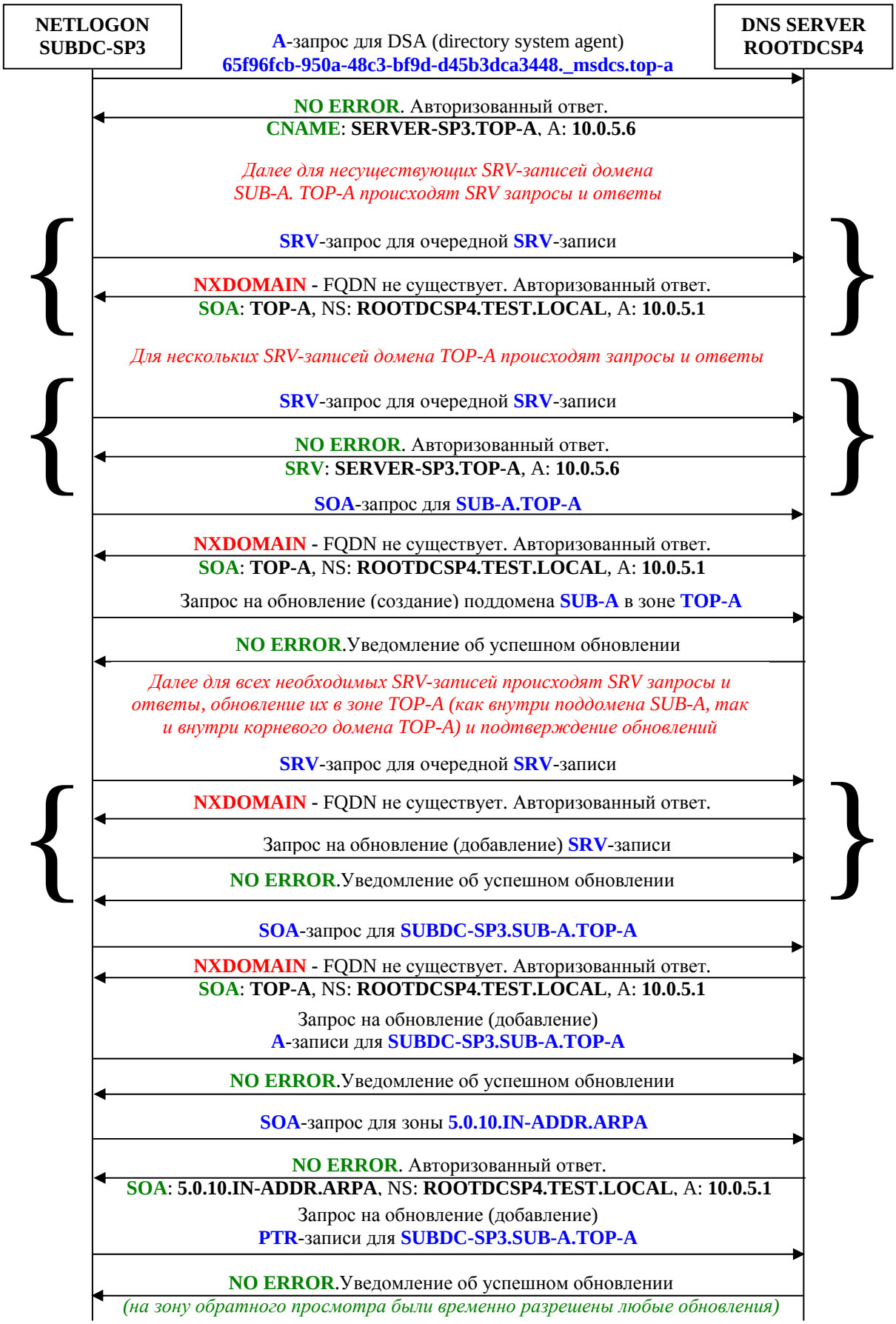
Служба NETLOGON сервера SUBDC-SP3 успешно зарегистрировала SRV-записи.

Приведем протокол взаимодействия SUBDC-SP3 с DNS, когда создается поддомен SUB-A, выбросив все лишние запросы на несуществующие SRV-записи и негативные ответы (NXDOMAIN) на них, чтобы не загромождать протокол:

Фаза 1: Установка Active Directory (до перезагрузки SUBDC-SP3):

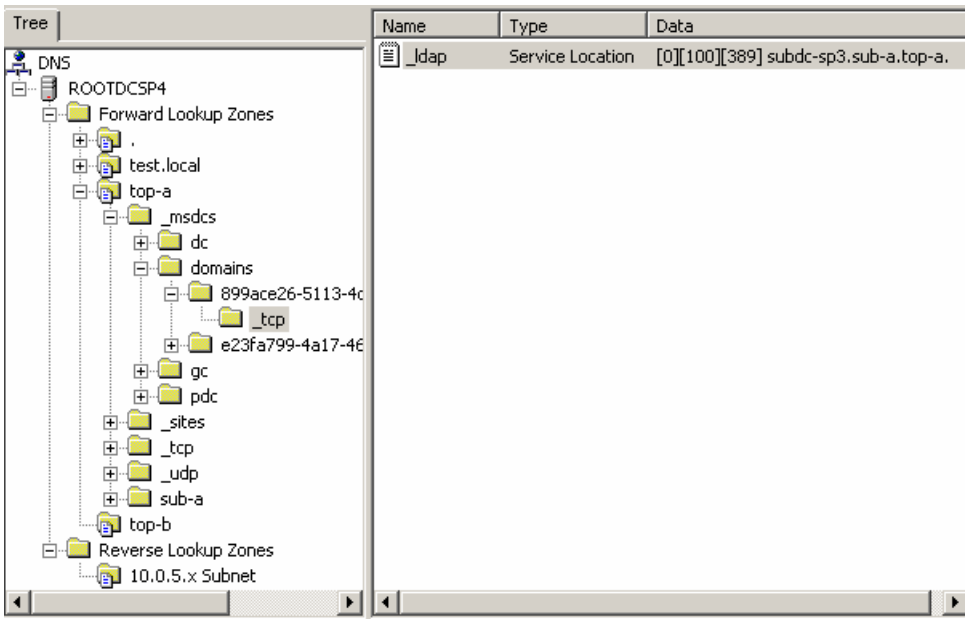


Фаза 2: Автоматическое создание SRV-записей в DNS (после перезагрузки SUBDC-SP3):



Таким образом, дочерний домен SUB-A в корневом домене TOP-A успешно создан и все A и SRV записи успешно зарегистрированы в зоне TOP-A. Службы DNS Client и NETLOGON контроллера дочернего домена – SUBDC-SP3 на базе ОС MS Windows 2000 AS SP3 – с проблемной зоной отработали четко и корректно.

Важное примечание. Именно служба NETLOGON контроллера дочернего домена обновляет все SRV-записи в зоне как внутри своего DNS Node (и привязанных к нему 4-х специальных поддеревьев для хранения SRV-записей), так и внутри корневого DNS Node зоны. Служба NETLOGON контроллера родительского домена не создает и не обновляет записи для контроллеров дочерних доменов. Это было установлено экспериментально в ходе анализа журналов DNS: в ходе повышения сервера SUBDC-SP3 до роли контроллера дочернего домена SUB-A, от контроллера родительского домена SERVER-SP3 не было зафиксировано ни одного запроса на обновление каких-либо записей, все необходимые SRV записи без исключения создал SUBDC-SP3. Кроме того, тщательный анализ запросов от SUBDC-SP3 также показал, что именно он создал все без исключения записи, которые появились в зоне TOP-A после перезагрузки SUBDC-SP3. Так, например, на снимке ниже, выделенная SRV-запись находится в корневом DNS Node TOP-A зоны TOP-A., но создана и обновляется службой NETLOGON именно сервера SUBDC-SP3 – контроллера дочернего домена SUB-A:



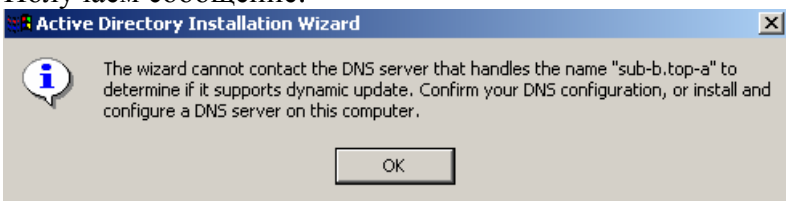
Этот момент имеет принципиально важное значение, поскольку он означает:

При создании дочерних доменов каждый контроллер только сам регистрирует и обновляет необходимые A, CNAME и SRV-записи как в своем DNS Node (и в 4-х привязанных к нему специальных поддеревьях), так и внутри корневого DNS Node зоны. Контроллеры родительских доменов заботятся только о своих записях в DNS и только. Контроллеры корневого домена, создают свои записи только внутри корневого DNS Node зоны.

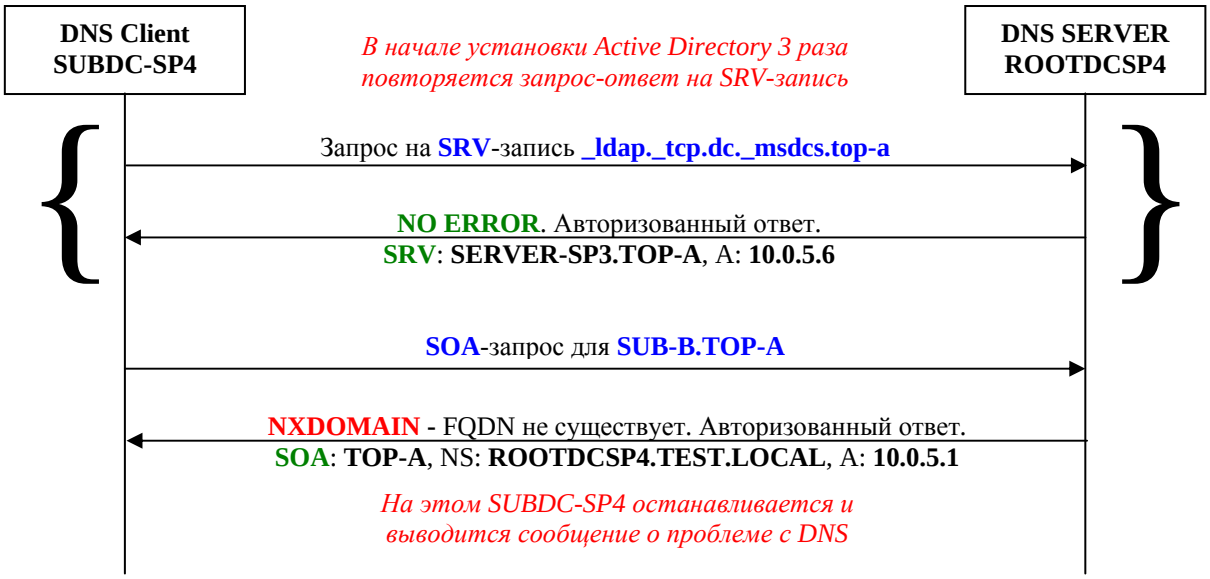
Так что, некорректно работающая с проблемной зоной служба NETLOGON контроллера родительского или корневого домена не может быть причиной проблем с созданием и динамическим обновлением необходимых A, CNAME и SRV-записей контроллеров дочерних доменов.

2.2.1.2. Повышаем сервер SUBDC-SP4 до роли контроллера дочернего домена SUB-B:

Получаем сообщение:



Анализ журнала DNS-сервера ROOTDCSP4 дает следующую картину (выбросим все лишние запросы на несуществующие SRV-записи и негативные ответы (NXDOMAIN) на них, чтобы не загромождать протокол):

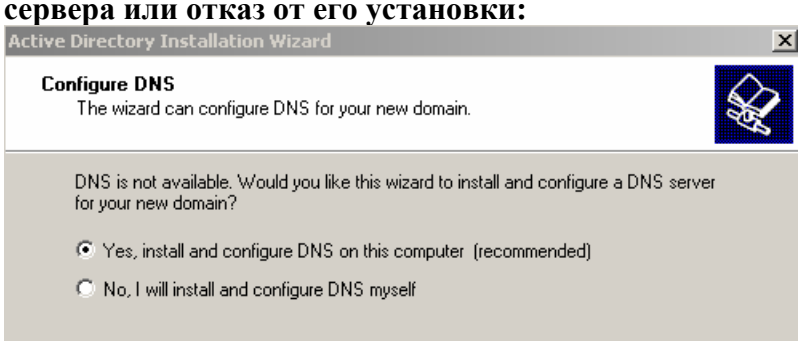


Сравниваем этот небольшой протокол с протоколом на фазе 1 (до перезагрузки) предыдущего эксперимента (2.2.1.1) и видим то, что в начале картины идентичны. Дальше, в случае SUBDC-SP3 – получив отрицательный ответ, он проверяет зону TOP-A на возможность обновления, становится контроллером дочернего домена и регистрирует все необходимые SRV-записи, а SUBDC-SP4 – ничего не делает.

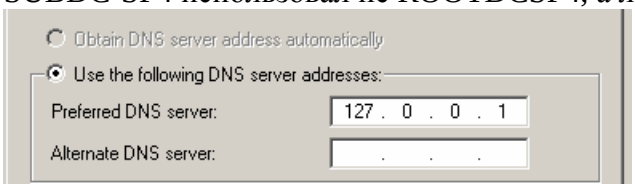
Что же, такое сообщение мы уже видели с контроллером корневого домена – SERVER-SP4 (эксперимент 1.2.2). Дальше последуют два возможных сценария – это создания локального DNS-сервера или отказ от установки локального DNS с продолжением использования ROOTDCSP4. Текущий эксперимент отличается от (1.2.2) только тем, что там мы работали с контроллером корневого домена, а здесь мы работаем с будущим контроллером дочернего домена. Однако, как было выяснено в предыдущем эксперименте (2.2.1.1), контроллер корневого домена не регистрирует в зоне SRV-записи контроллеров дочерних доменов, этим занимаются они каждый самостоятельно. Грубо говоря, контроллер SERVER-SP3 корневого домена, корректно работающий с проблемными зонами, “не поможет” контроллеру дочернего домена SUBDC-SP4, когда тот не сможет зарегистрировать ни одной SRV-записи в DNS. Но мы в любом случае проведем эксперименты.

Тем более что интересным будет то, что именно создаст SUBDC-SP4 на своем локальном сервере DNS, когда мы пойдем по первому сценарию: новую зону он создаст, но ведь он не может же стать контроллером корневого домена зона, он же контроллер дочернего домена.

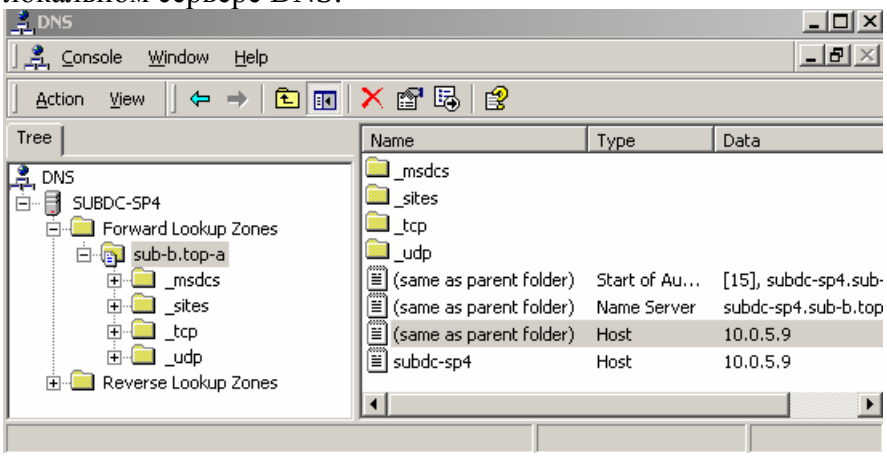
После вышеприведенного сообщения об ошибке нам предлагают 2 возможных сценариев повышения SUBDC-SP4: установка и использование локального DNS-сервера или отказ от его установки:



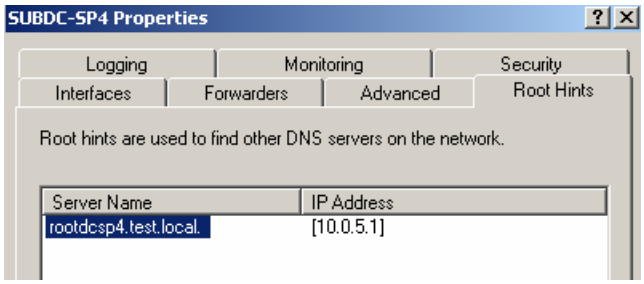
<u>Сценарий 1. Локальный DNS сервер</u>: Пусть на сервере SUBDC-SP4 автоматически установится локальный DNS-сервер. При этом скорректируем настройки TCP/IP, чтобы SUBDC-SP4 использовал не ROOTDCSP4, а локальный DNS-сервер:



В результате домен успешно создается, после перезагрузки видим следующее на локальном сервере DNS:

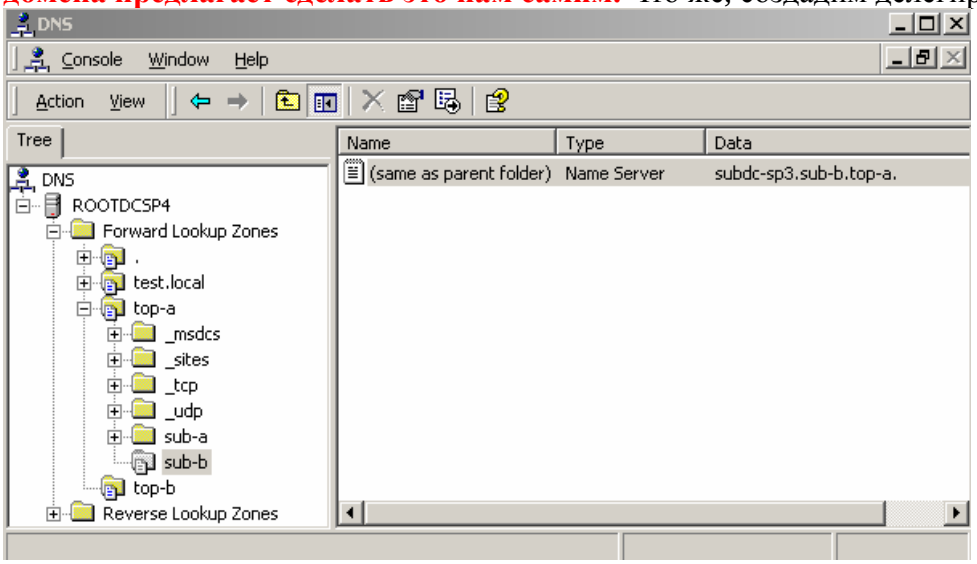


Удивительный результат! Сервер SUBDC-SP4 создал свою собственную зону SUB-B.TOP-A второго уровня (не проблемная зона) и успешно в ней зарегистрировал свои SRV-записи. Что же, похоже, контроллер домена дочернего домена выбрал решение, предполагающий то, что на основном DNS-сервере будет создано делегирование поддерева SUB-B.TOP-A. в зоне TOP-A. на DNS-сервер SUBDC-SP4. Более того, заглянем в Root Hints DNS-сервера SUBDC-SP4, и увидим то, что в нем автоматически создана ссылка на корневой DNS-сервер:

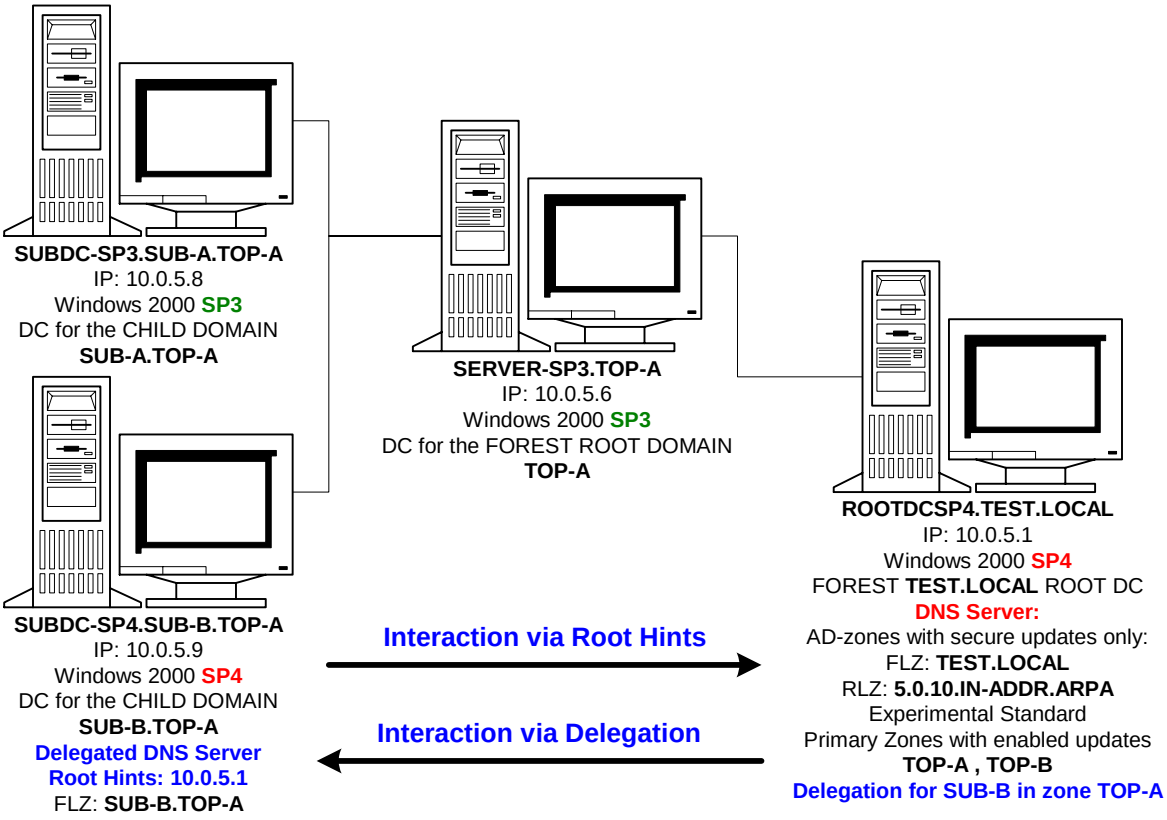


Это логично и правильно.

Однако, создать делегирование SUB-B.TOP-A. в зоне TOP-A контроллер дочернего домена предлагает сделать это нам самим. Что же, создадим делегирование:



Получается следующая структура серверов и взаимодействие DNS-серверов:



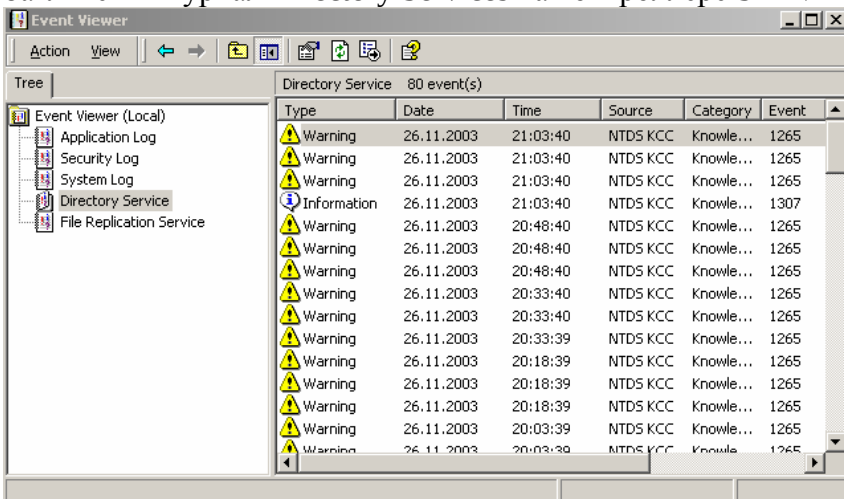
На первый взгляд кажется, что мы нашли идеальное решение проблемы обновлений в случае, когда нам необходимо создать в проблемной зоне (зоне первого уровня) дочерний домен с контроллером на базе ОС Windows 2000 AS SP4:

- Идем по сценарию 1 создания на контроллере дочернего домена своего DNS сервера, на котором автоматически создается зона ***<имя дочернего домена>.<родительский суффикс>.*** и в Root Hints добавляется адрес корневого DNS.
- Настраиваем контроллер дочернего домена для использования своего сервера DNS.
- На корневом DNS сервере создаем делегирование поддерева ***<имя дочернего домена>.<родительский суффикс>.*** в проблемной зоне.

После этого мы будем иметь контроллер дочернего домена на базе ОС Windows 2000 AS SP4, который без проблем будет обновлять SRV-записи в своей локальной зоне (не проблемной). В проблемной же зоне на корневом DNS сервере, свои SRV-записи будет обновлять контроллер корневого домена на базе ОС Windows 2000 AS SP3. Контроллер корневого домена без проблем найдет SRV-записи контроллера дочернего домена через запись делегирования на корневом DNS-сервере, а контроллер дочернего домена найдет SRV-записи контроллера корневого домена через Root Hints.

Вроде все продумано, но есть очень опасный подводный камень. Мы забыли про то, что некоторые ключевые SRV-записи контроллера дочернего домена также должны регистрироваться внутри корневого DNS Node зоны, на которую отображается дерево AD-доменов.

Заглянем в журнал Directory Services на контроллере SERVER-SP3 корневого домена:

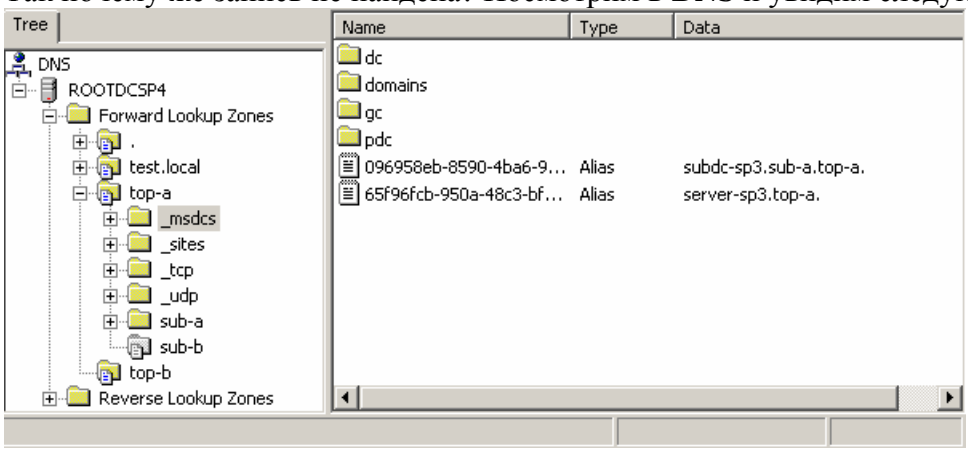


Журнал заполнен ошибками от службы проверки целостности инфраструктуры на базе Active Directory. Посмотрим содержимое ошибки:

Event Type: Warning
Event Source: NTDS KCC
Event Category: Knowledge Consistency Checker
Event ID: 1265
Date: 26.11.2003
Time: 20:33:40
User: N/A
Computer: SERVER-SP3
Description:
The attempt to establish a replication link with parameters
Partition: DC=sub-b, DC=top-a
Source DSA DN: CN=NTDS Settings, CN=SUBDC-SP4, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=top-a
Source **DSA Address: 91d19ea9-15ad-4a1e-aab4-98fb7c91fa27.msdcs.top-a**
Inter-site Transport (if any):
failed with the following status:
The DSA operation is unable to proceed because of a DNS lookup failure.
The record data is the status code. This operation will be retried.

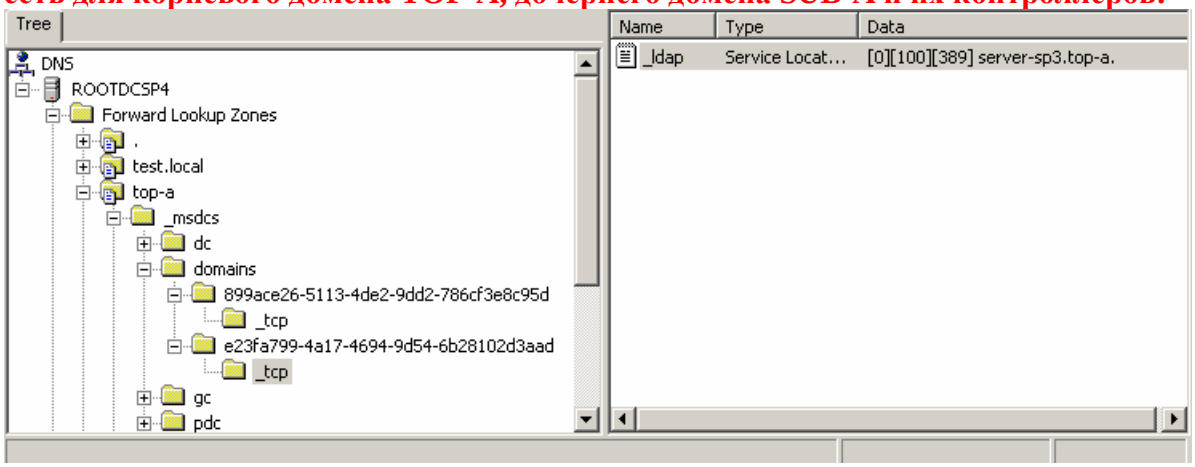
Итак, в DNS в зоне TOP-A не найдена ключевая запись DSA (directory system agent) для контроллера домена SUB-B и невозможно установление репликации с этим контроллером. Нет необходимости пояснять к чему это приводит: нарушение синхронизации данных об объектах и их атрибутах в Active Directory, проблемы с включением клиентских ПК в домен, проблемы с аутентификацией в доменах и т.д.

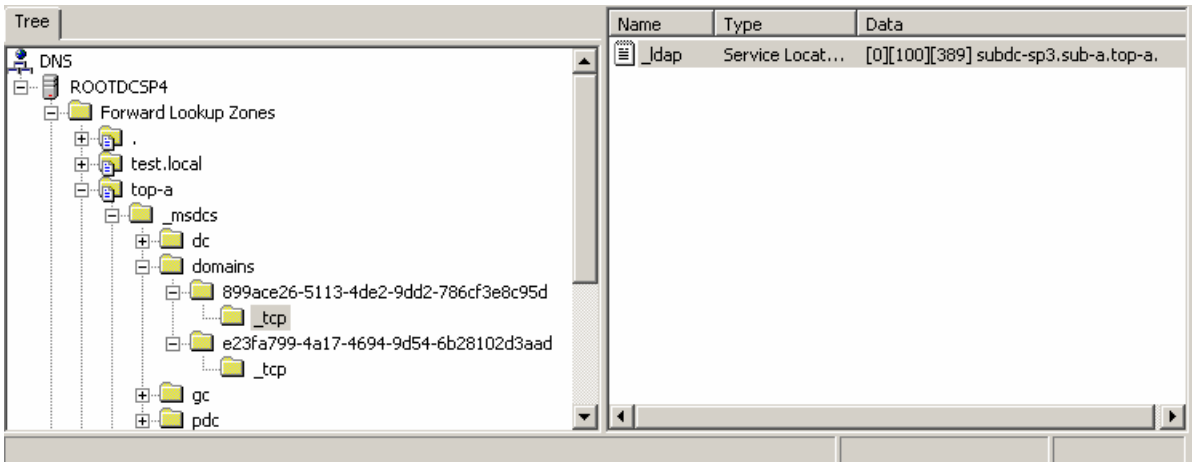
Так почему же запись не найдена? Посмотрим в DNS и увидим следующее:



Действительно, запись DSA для контроллера SUBDC-SP4 отсутствует. Самое главное то, что он должна находится здесь, и его должен был создать именно сервер SUBDC-SP4, но он не смог это сделать, так как зона TOP-A – проблемная, и его служба NETLOGON (ОС Win2K 2000 SP4) не может обновлять данные в такой зоне.

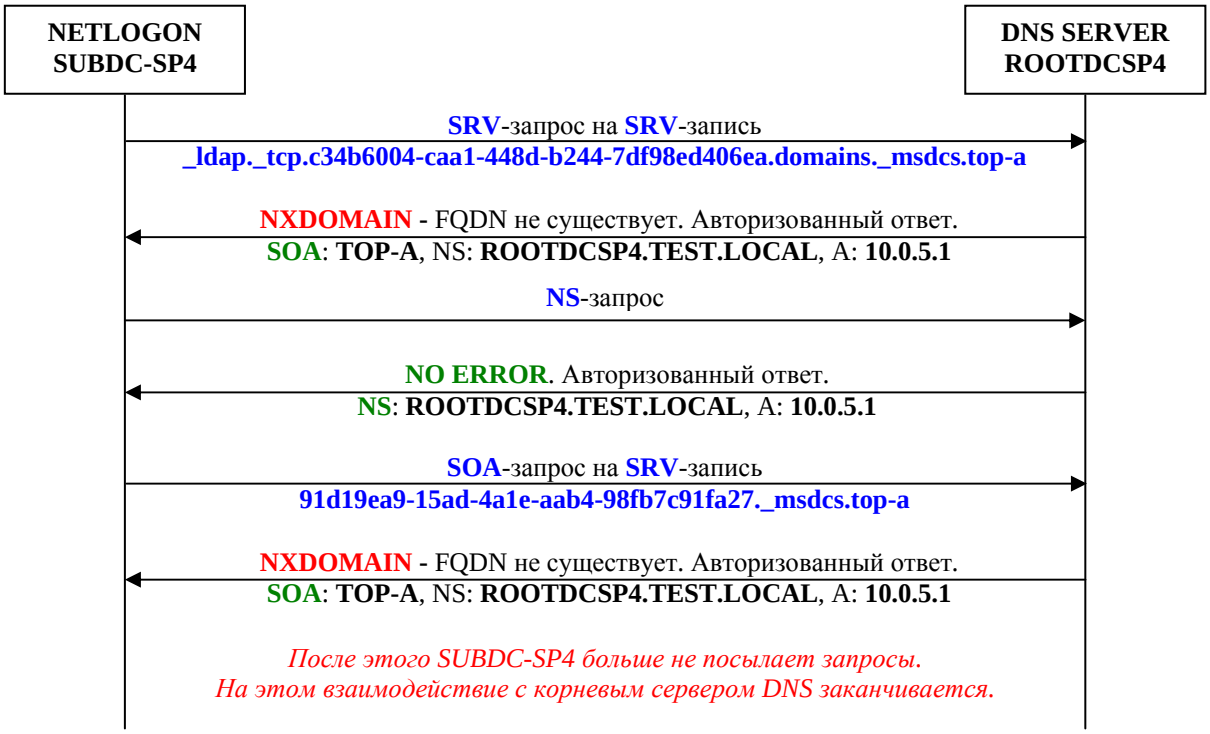
И это еще не все, в зоне TOP-A вообще нет информации о GUID (globally unique identifier) домена SUB-B и соответствующей SRV-записи для контроллера, которые есть для корневого домена TOP-A, дочернего домена SUB-A и их контроллеров:





Что же, SUBDC-SP4 без проблем регистрируют SRV-записи в своем домене своей локальной зоны, делегированной от корневого DNS сервера, но этого недостаточно, SUBDC-SP4 не регистрирует важнейшие записи в зоне TOP-A., на которую отображается дерево AD-доменов.

Посмотрим журнал в DNS на предмет того, пытался ли сервер SUBDC-SP4 после повышения до роли контроллера дочернего домена и перезагрузки что-либо делать в корневой зоне TOP-A. Картина получается следующая:

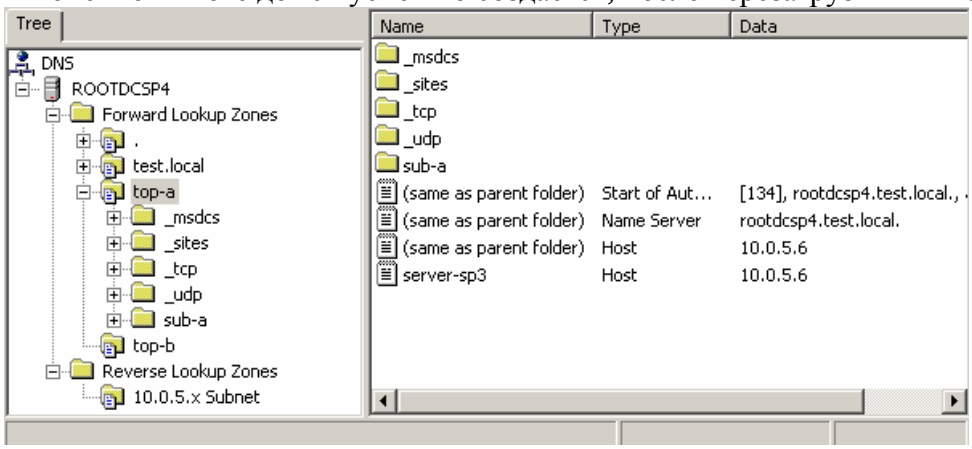


Очевидно, длинный шестнадцатеричный код в первом запросе – это GUID для домена SUB-B. В третьем запросе длинный код – это и есть тот самый ключевой DSA адрес, который тщетно пытался выяснить контроллер корневого домена SERVER-SP3. Сервер SUBDC-SP4 не находит необходимых записей, но и не пытается их создать.

Таким образом, дочерний домен SUB-A в корневом домене TOP-A успешно создан и часть SRV записей успешно зарегистрировались в делегированной зоне SUB-A.TOP-A. Однако в зоне TOP-A. ни одной из необходимых SRV записи нет. Службы DNS Client и NETLOGON контроллера дочернего домена – SUBDC-SP4 на базе ОС MS Windows 2000 AS SP4 – с проблемной зоной отработали некорректно.

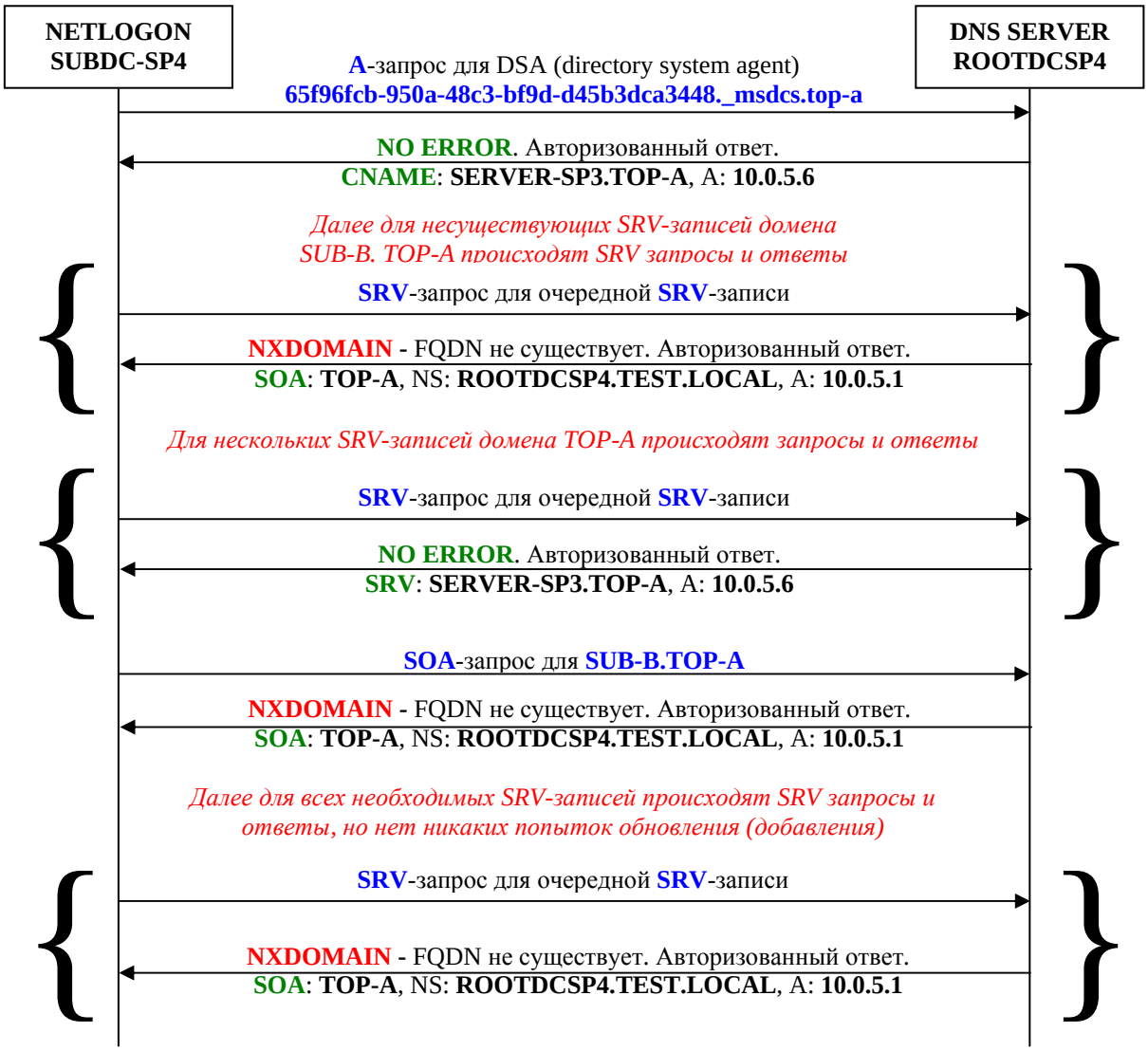
Сценарий 2. Отказ от локального DNS сервера: Мы откажемся от установки локального сервера DNS, и в TCP/IP настройках SUBDC-SP4 в качестве DNS-сервера останется исходно назначенный DNS-сервер, полномочный в зоне **TOP-A –** ROOTDCSP4.

В конечном итоге домен успешно создается, после перезагрузки в DNS видим следующее:



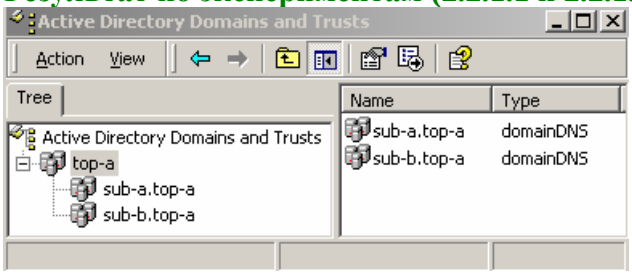
Служба NETLOGON не добавила SRV-записи. Поддомен SUB-B даже не появился.

Проанализировав взаимодействие контроллера SUBDC-SP4 с DNS-сервером, получаем следующую картину:



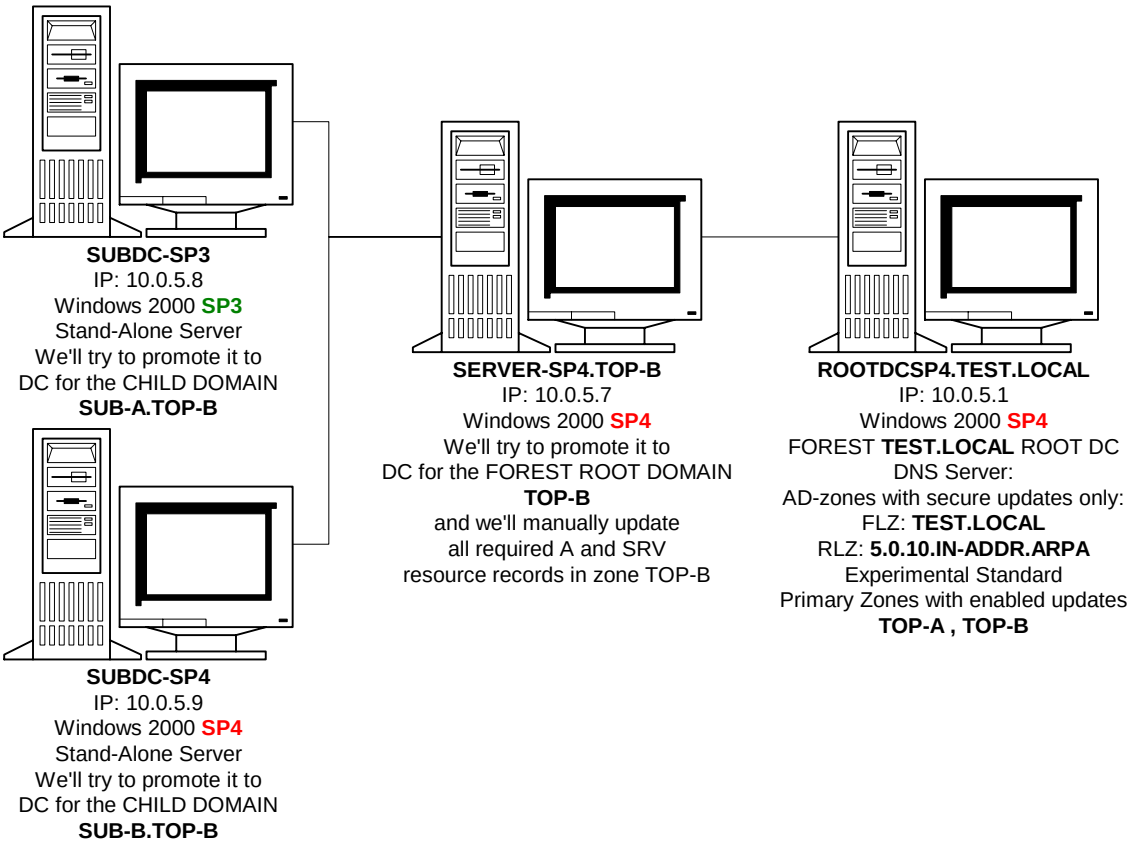
Таким образом, оба сценария хотя и существенно различались по результатам и возможностям экспериментирования, но тем нее менее, оба работали некорректно с проблемной зоной TOP-A. В сценарии 1 при использовании локального DNS сервера удалось получить немного более выгодную картину за счет того, что на локальном сервере DNS автоматически создается зона 2-го уровня (не проблемная) и контроллеру домена удается успешно зарегистрировать часть необходимых записей. Однако в проблемной зоне TOP-A., как и в сценарии 2, никакие записи не добавляются, а именно там находятся наиболее важные записи, используемые при взаимодействии контроллеров различных доменов и репликации.

Результат по экспериментам (2.2.1.1 и 2.2.1.2) в Active Directory:



Дочерние домены присутствуют в Active Directory

2.2.2 Контроллер корневого домена на базе ОС MS Windows 2000 AS SP4

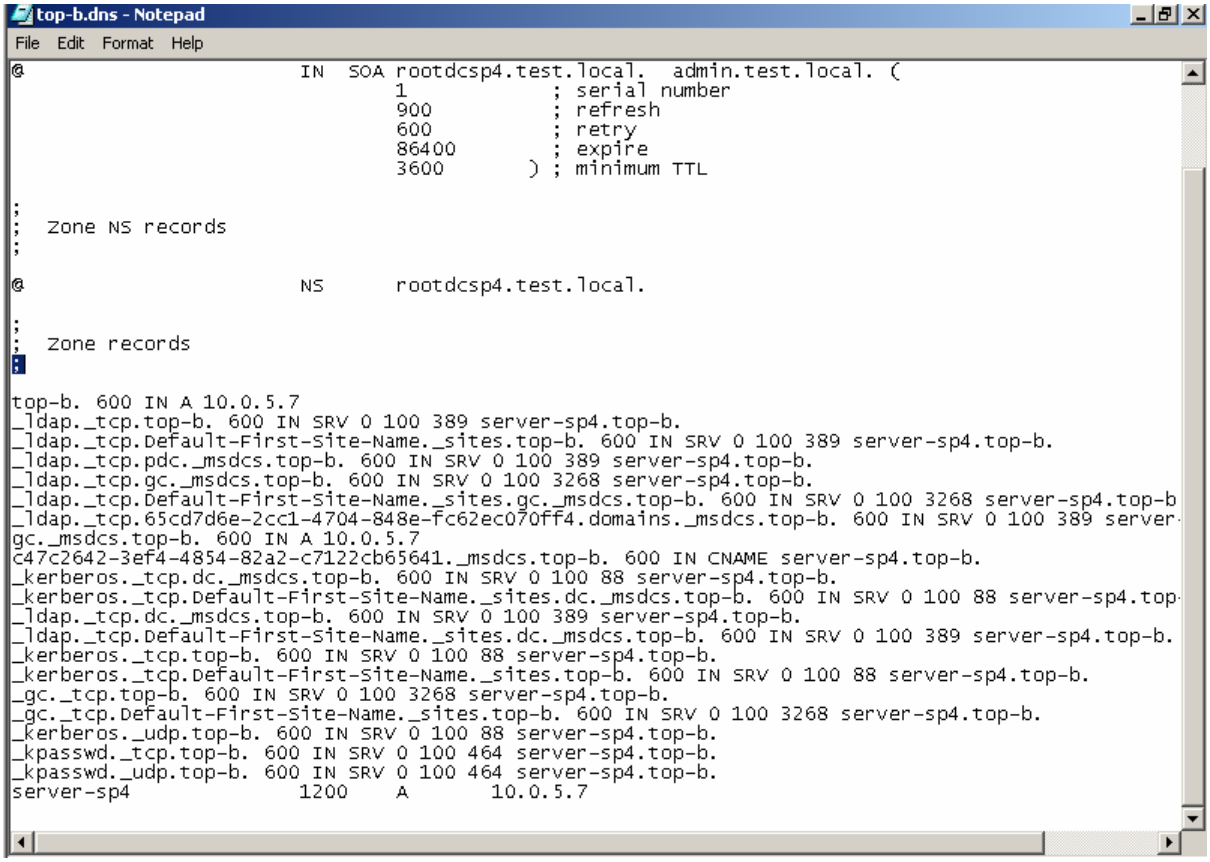


В ранее проведенном эксперименте (1.2.2) с контроллером SERVER-SP4 на базе ОС MS Windows 2000 AS SP4 корневого домена TOP-B были проблемы: сервер SERVER-SP4 не хотел корректно работать с проблемной зоной TOP-B. При попытке установки Active Directory выводилась ошибка о недоступности DNS сервера, содержащего зону TOP-B с поддерживаемыми динамическими обновлениями. Далее предлагались два сценария (с локальным сервером DNS и без него, при использовании основного ROOTDCSP4). Оба сценария были подробно рассмотрены, и было установлено то, что как в случае работы с зоной TOP-B на локальном сервере DNS, так и в случае использования зоны TOP-B на основном DNS сервере (ROOTDCSP4), контроллер корневого домена не регистрирует свои SRV-записи, что делает его неприемлемым для взаимодействия.

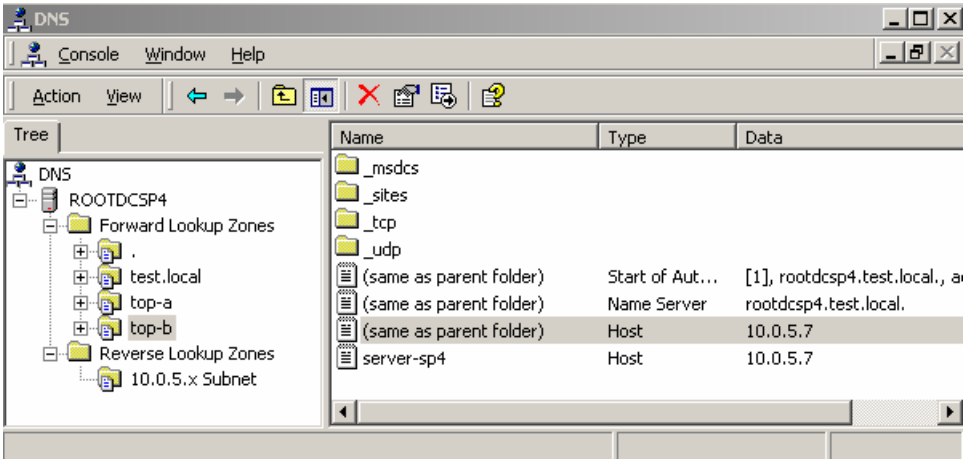
Однако, для проведения двух дополнительных экспериментов с контроллерами дочерних доменов нам на данном этапе необходим контроллер корневого домена TOP-B в проблемной зоне TOP-B, развернутый на базе ОС MS Windows 2000 AS SP4. Для этого мы можем его развернуть по второму сценарию (без своей локальной службы DNS сервера, вместо этого использование основного ROOTDCSP4). Разумеется, в зоне TOP-B, хранящейся на DNS-сервере ROOTDCSP4, необходимые A и SRV-записи автоматически не создадутся. Нам остается их только создать вручную.

Но где взять информацию о необходимых A и SRV-записях? Здесь к нам на помощь приходит файл NETLOGON.DNS, хранящийся у каждого контроллера домена в папке %SYSTEMROOT%\SYSTEM32\CONFIG. В нем хранятся все записи, регистрируемые в DNS службой NETLOGON контроллера домена. Поскольку зона TOP-B – стандартная основная, то она хранится в виде файла TOP-B.DNS на сервере DNS в папке %SYSTEMROOT%\SYSTEM32\DNS, и нам проще простого скопировать необходимые данные в конец этого файла, предварительно остановив DNS сервер, а после копирование запустить его снова. Однако, в файле NETLOGON.DNS нет A-записи для DNS-имени контроллера домена. Это логично, регистрация A и PTR записей для машины – это забота служб DHCP. Мы же их просто вручную создадим.

Итак, повышаем сервер SERVER-TOP4 до роли контроллера корневого домена TOP-B, отказавшись от установки локального DNS-сервера (второй сценарий). После перезагрузки убеждаемся в том, на сервере SERVER-SP4 находим файл NETLOGON.DNS и копируем его содержимое в конец файла TOP-B.DNS на DNS-сервере, предварительно остановив его, также в конец добавляем A-запись для DNS-имени контроллера домена:



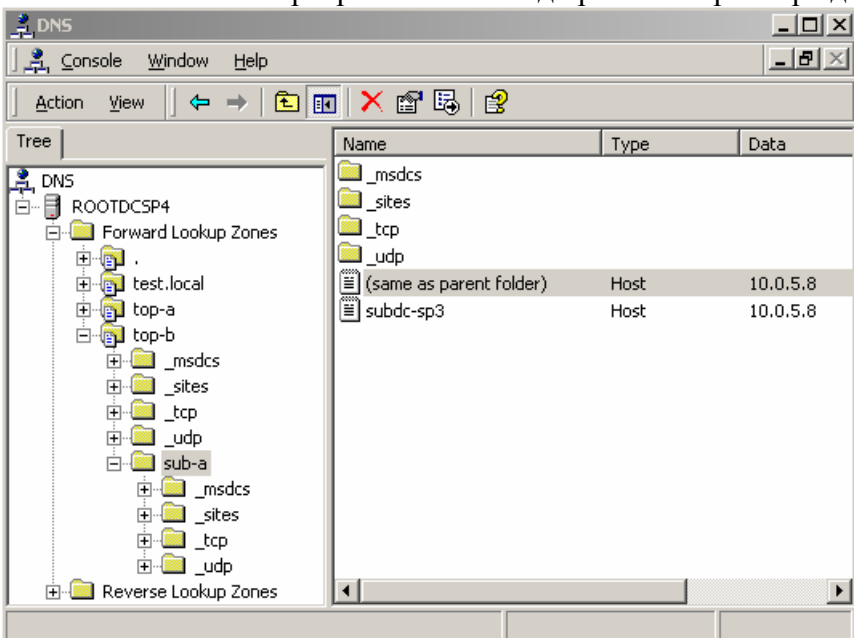
Запускаем службу сервера DNS и смотрим на результат:



Все необходимые A и SRV-записи добавились (искусственным путем). Обновляться они, разумеется, автоматически не будут.

Теперь можно приступать к экспериментированию с дочерними доменами.

2.2.2.1. Повышаем сервер SUBDC-SP3 до роли контроллера дочернего домена SUB-A:



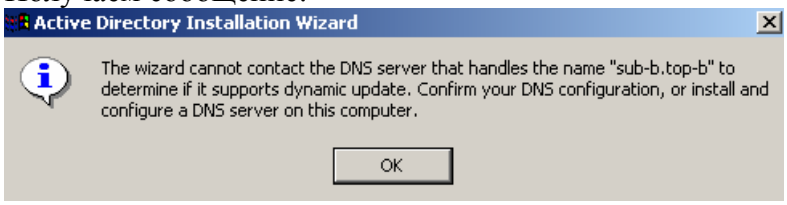
Служба NETLOGON сервера SUBDC-SP3 успешно зарегистрировала SRV-записи.

Нет смысла анализировать журнал DNS: картина взаимодействия контроллера дочернего домена с сервером DNS такая же, как и в эксперименте (2.2.1.1).

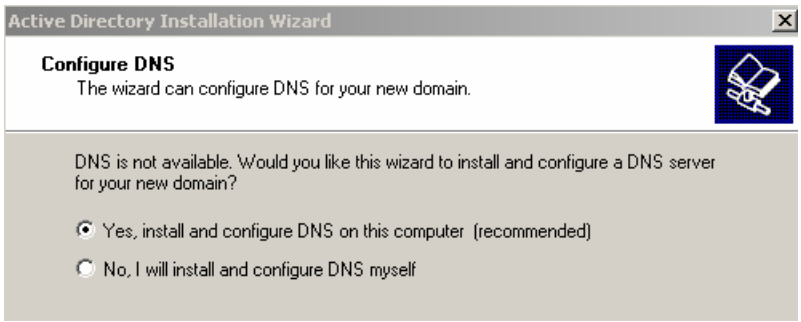
Однако, хотя дочерний домен SUB-A без проблем создался, нельзя забывать то, что корневой домен TOP-B создан на базе контроллера, неспособного обновлять автоматически свои записи в проблемной зоне TOP-B, и это будет приводить к проблемам и требовать ручного слежения и коррекции записей контроллера SERVER-SP4. В противном случае неверные устаревшие данные в корневом домене TOP-B зоны TOP-B будут резко негативно сказываться на работе всего леса доменов.

2.2.2.2. Повышаем сервер SUBDC-SP4 до роли контроллера дочернего домена SUB-B:

Получаем сообщение:

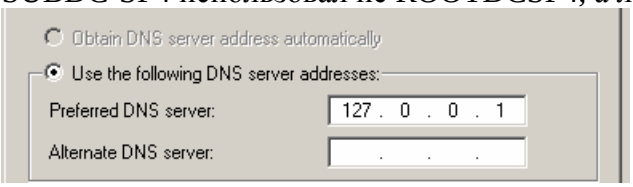


Этого и следовало ожидать, все повторяется как в эксперименте (2.2.1.2). Здесь мы, как и ранее, столкнемся с 2-мя возможными сценариями продолжения установки Active Directory на сервер SUBDC-SP4 (с локальным сервером DNS и без него):

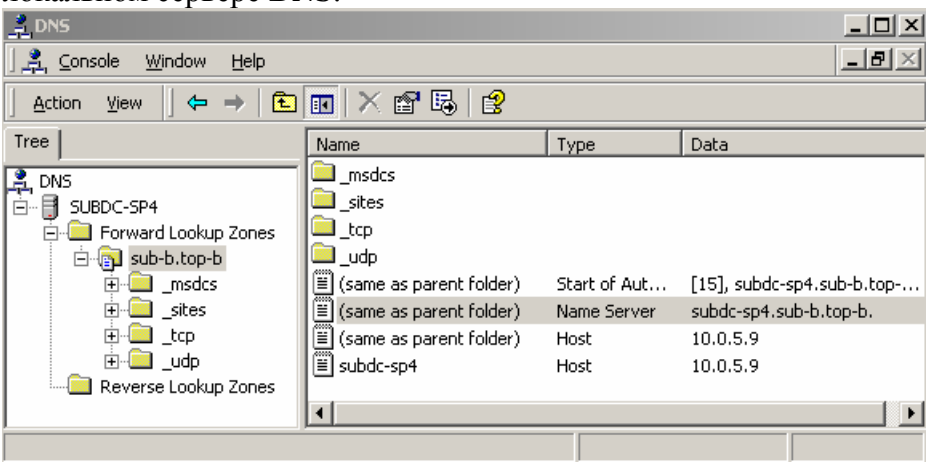


Мы рассмотрим эти сценарии, но не будем подробно анализировать результаты и журналы DNS. Поставим эксперименты по обоим сценариям только лишь для того, чтобы убедится в том, что, действительно, все будет так, как было в эксперименте (2.2.1.2).

Сценарий 1. Локальный DNS сервер: Пусть на сервере SUBDC-SP4 автоматически установится локальный DNS-сервер. При этом скорректируем настройки TCP/IP, чтобы SUBDC-SP4 использовал не ROOTDCSP4, а локальный DNS-сервер:

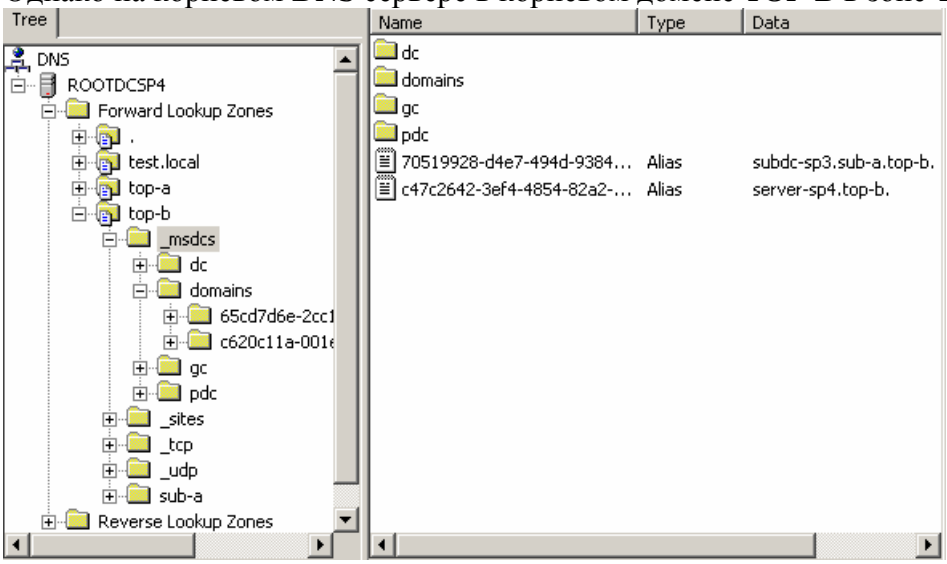


В результате домен успешно создается, после перезагрузки видим следующее на локальном сервере DNS:



Как и ожидалось, в своем домене SUB-B в локальной зоне SUB-B.TOP-B (не проблемной) контроллер SUBDC-SP4 все необходимые записи зарегистрировал.

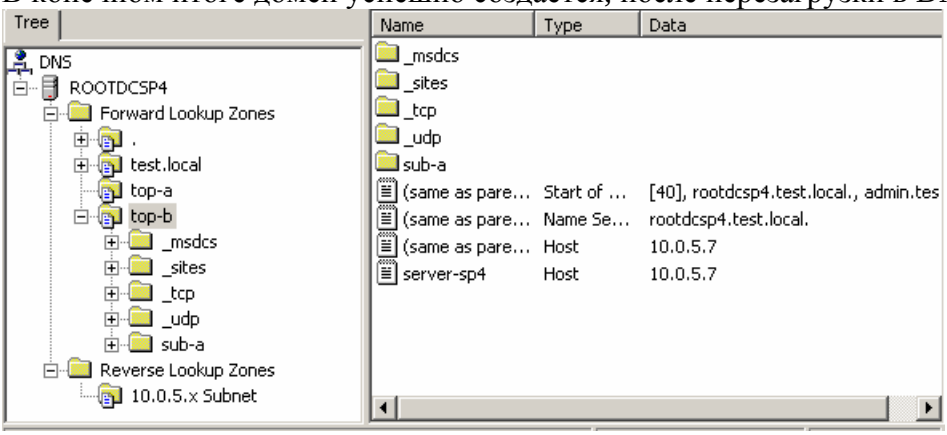
Однако на корневом DNS сервере в корневом домене TOP-B в зоне TOP-B:



Необходимая ключевая DSA-запись для SUBDC-SP4 не зарегистрировалась.
В папке Domains третий Domain GUID поддомена SUB-B не появился (первый для корневого домена TOP-B, второй – для поддомена SUB-A).
Кроме того, требуется вручную делегирование SUB-B в зоне TOP-B.

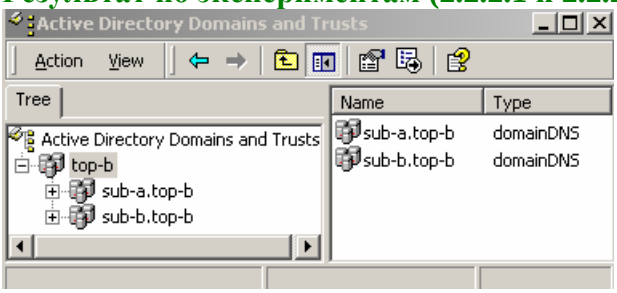
<u>Сценарий 2. Отказ от локального DNS сервера</u>: Мы откажемся от установки локального сервера DNS, и в TCP/IP настройках SUBDC-SP4 в качестве DNS-сервера останется исходно назначенный DNS-сервер, полномочный в зоне **TOP-B –** ROOTDCSP4.

В конечном итоге домен успешно создается, после перезагрузки в DNS видим следующее:



Служба NETLOGON не добавила SRV-записи. Поддомен SUB-B даже не появился.

Результат по экспериментам (2.2.2.1 и 2.2.2.2) в Active Directory:



Дочерние домены присутствуют в Active Directory

Заключение по проведенным экспериментам со службой NETLOGON

Запишем окончательно эмпирические знания в табличном виде:

№	Зона	Контроллер корневого домена		Контроллер дочернего домена		
		ОС	Обновления внутри корневого DNS Node	ОС	Обновления внутри корневого DNS Node	Обновления внутри дочернего DNS Node
1.1.1	Не проблемная	W2K SP3	Да	-	-	-
1.1.2	Не проблемная	W2K SP4	Да	-	-	-
1.2.1	Проблемная	W2K SP3	Да	-	-	-
1.2.2	Проблемная	W2K SP4 (сценарий 1)	Нет [1]	-	-	-
		W2K SP4 (сценарий 2)	Нет	-	-	-
2.1.1.1	Не проблемная	W2K SP3	Да	W2K SP3	Да	Да
2.1.1.2	Не проблемная	W2K SP3	Да	W2K SP4	Да	Да
2.1.2.1	Не проблемная	W2K SP4	Да	W2K SP3	Да	Да
2.1.2.2	Не проблемная	W2K SP4	Да	W2K SP4	Да	Да
2.2.1.1	Проблемная	W2K SP3	Да	W2K SP3	Да	Да
2.2.1.2	Проблемная	W2K SP3	Да	W2K SP4 (сценарий 1)	Нет	Да [2]
				W2K SP4 (сценарий 2)	Нет	Нет
2.2.2.1	Проблемная	W2K SP4 [3]	Нет	W2K SP3	Да	Да
2.2.2.2	Проблемная	W2K SP4 [3]	Нет	W2K SP4 (сценарий 1)	Нет	Да [2]
				W2K SP4 (сценарий 2)	Нет	Нет

1 – на локальном сервере DNS создается зона 1-го уровня, и она также оказывается проблемной.

2 – на локальном сервере DNS создается зона *<имя дочернего домена>.<родительский суффикс>*, и она уже не является проблемной. Контроллер домена успешно регистрирует в своей локальной зоне необходимые A и SRV записи, а в корневом DNS Node проблемной зоны ничего не создает, хотя в Root Hints у нее автоматически присутствует ссылка на корневой DNS-сервер.

3 – Контроллер корневого домена создан по второму сценарию. Все необходимые записи взяты из файла NETLOGON.DNS и вручную добавлены в файл проблемной зоны на корневом сервере DNS. После этого становится временно возможным взаимодействие с контроллером корневого домена.

Выводы:

- Для появления проблемы необходимы два условия:
  - Служба NETLOGON (контроллера корневого либо дочернего домена), непосредственно посылающая запросы к DNS серверу работает под управлением системы Windows 2000 Service Pack 4
  - Зона, в которой должны производится обновления, является зоной 1-го уровня (проблемная зона).
- При иных сочетаниях условий проблема не проявляется.
- При установке Active Directory на сервер, работающего под управлением Windows 2000 Service Pack 4, в случае проблемной зоны выводится ошибка о невозможности определения DNS-сервера, полномочного за зону и поддерживающего обновления. Далее возможны два сценария:

1) Создание локального DNS сервера:
   - Если создается контроллер корневого домена, то на локальном сервере DNS будет создана требуемая зона (опять же 1-го уровня, а значит – проблемная) и никакие записи не будут автоматически добавляться или обновляться.
   - Если создается контроллер дочернего домена, то на локальном сервере DNS будет создана зона с именем ***<имя дочернего домена>.<родительский суффикс>.***, и она уже не является проблемной, и контроллер успешно регистрирует часть необходимых записей в этой зоне. Однако, часть записей, которые должны регистрироваться в корневом DNS Node, находящемся в проблемной зоне на корневом сервере DNS, остаются незарегистрированными. Связь с корневым сервером DNS осуществляется за счет автоматически созданной ссылки на корневой сервер DNS в Root Hints локального сервера DNS. А обратная связь – делегирование поддерева ***<имя дочернего домена>.<родительский суффикс>.*** в проблемной зоне на корневом сервере DNS – не создается, это требуется сделать вручную.

2) Отказ от создания локального DNS-сервера (продолжение использования корневого сервера DNS). В этом случае в проблемной зоне ни внутри корневого DNS Node, ни внутри дочернего DNS Node никакие из необходимых записей не будут автоматически добавляться или обновляться.

   Так или иначе, AD-домен можно сделать работоспособным до первых изменений, которые могут потребовать изменения SRV-записей в своем и корневом DNS Node (для контроллеров корневых доменов – только в корневом DNS Node). Это делается ручным добавлением необходимых записей, взятых из файла NETLOGON.DNS в папке %SYSTEMROOT%\SYSTEM32\CONFIG на системном диске контроллера домена. Далее, рано или поздно начнутся проблемы, если постоянно не следить за всеми изменениями и своевременно вручную не синхронизировать это с SRV-записями контроллера домена.

Важное примечание.

При создании дочерних доменов каждый контроллер только сам регистрирует и обновляет необходимые A и SRV-записи как в своем DNS Node, так и в корневом DNS Node зоны. Контроллеры родительских доменов заботятся только о своих записях в DNS. Контроллеры корневого домена, создают свои записи только в корневом DNS Node.

Заключение: Службы DHCP Client, DHCP Server и NETLOGON в Windows 2000 Service Pack 4 не выполняют обновления в зонах первого уровня.