

# Пример применения

**Infortrend**<sup>®</sup>

## Пример применения: iSCSI конфигурация от начала до конца

### Цель

Этот документ ведет пользователя от начала до конца процедуры настройки системы хранения с хостом iSCSI (S16E или S12E со встроенным ПО rev. 3.73). Некоторые функции, как, например, Grouping (Multiple Connections per Session) и SLP (Service Location Protocol), требуют взаимодействия с окончательными устройствами в сети iSCSI.

## Содержание

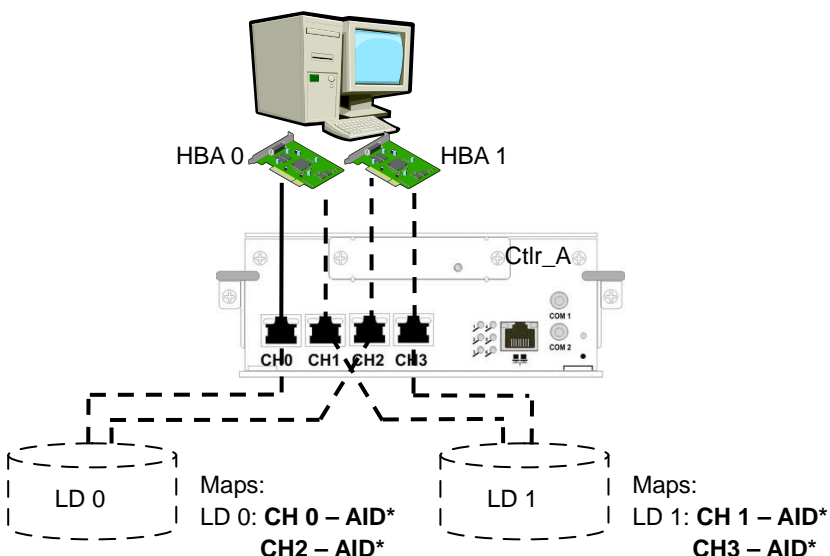
Содержание.....	1
<b>1. Варианты топологии.....</b>	<b>2</b>
Модели iSCSI DAS с одним контроллером (типа G) .....	2
iSCSI IP SAN – 1 .....	3
iSCSI IP SAN – 2 .....	4
iSCSI IP SAN – 3 .....	5
iSCSI IP SAN – 4 .....	6
<b>2. Транкинг (объединение связей).....</b>	<b>8</b>
<b>3. Настройки сетевого интерфейса .....</b>	<b>14</b>
IP адреса iSCSI хост-портов .....	14
Адресация по Internet Protocol Version 6 (IPv6).....	15
<b>4. Группирование (MC/S, множественные соединения в сеансе).....</b>	<b>18</b>
<b>5. Создание ID хост-каналов.....</b>	<b>22</b>
<b>6. Подключение LUN к хосту.....</b>	<b>22</b>
<b>7. Идентификация CHAP .....</b>	<b>25</b>
<b>8. Настройка инициатора (на примере Microsoft Software Initiator).....</b>	<b>30</b>
“channel number” - “host ID” - “LD ownership” .....	31
<b>9. Установка драйвера EopPath .....</b>	<b>37</b>
<b>10. Настройка iSNS (дополнительно ).....</b>	<b>39</b>
Пример конфигурации iSNS.....	40
<b>11. Настройка SLP (дополнительно).....</b>	<b>43</b>
<b>12. Jumbo Frame .....</b>	<b>48</b>

# 1. Варианты топологии

Примеры, приведенные ниже, начинаются с простого DAS с одним контроллером и заканчиваются сложными конфигурациями с избыточными контроллерами и распределенной нагрузкой. Будет показано, как создавать множественные логические диски, работающие под управлением двойных контроллеров, в зависимости от количества корпусов RAID массивов и JBOD.

## iSCSI DAS модели с одиночным контроллером (типа G)

# Host	# HBA	# Channel	# Cable	# Controller	# LD	# Map	Hub status
1	2 с 2 портами	4	4	1	2	4	Нет

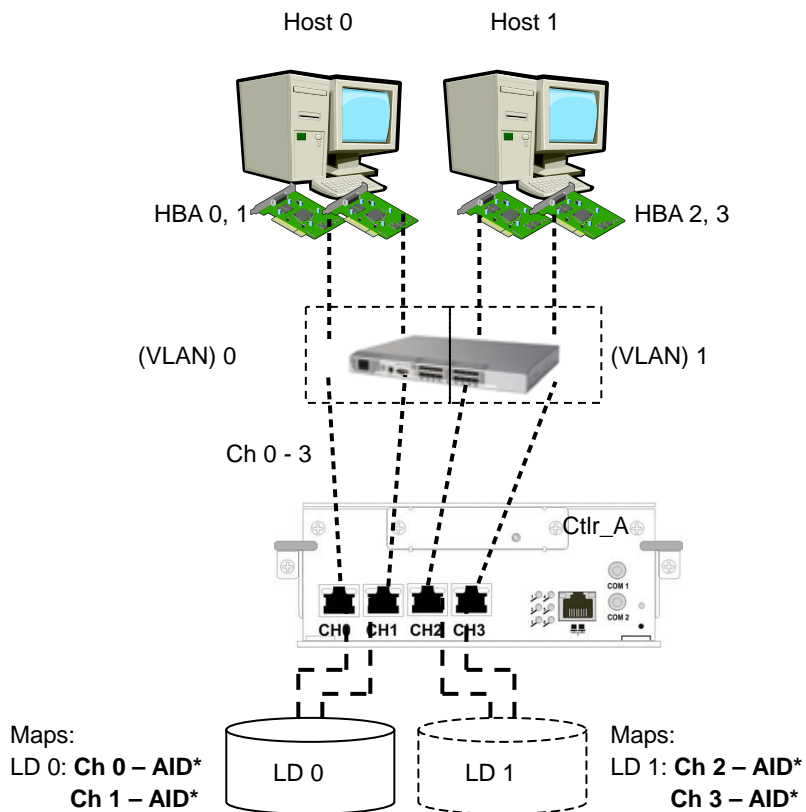


Тип отказа	Отказ	Доступный путь	MPIO
HBA	HBA 0	LD 0: HBA 1 – CH 2 – AID – LD 0	✓
		LD 1: HBA 1 – CH 3 – AID – LD 1	
Кабель	HBA 0 - CH0 - Ctrl_A	LD 0: HBA 1 – CH 2 – AID – LD 0	✓
		LD 1: HBA 0 – CH 1 – AID – LD 1	
		LD 1: HBA 1 – CH 3 – AID – LD 1	
Контроллер	Ctrl_A	X	
Нет контроллера	Ctrl_A		

# iSCSI IP SAN – 1

Модели с одиночным контроллером (типа G)

# Host	# HBA	# Channel	# Cable	# Controller	# LD	# Map	Hub status
2	4 с 1 портом	4	8	1	2	4	Нет

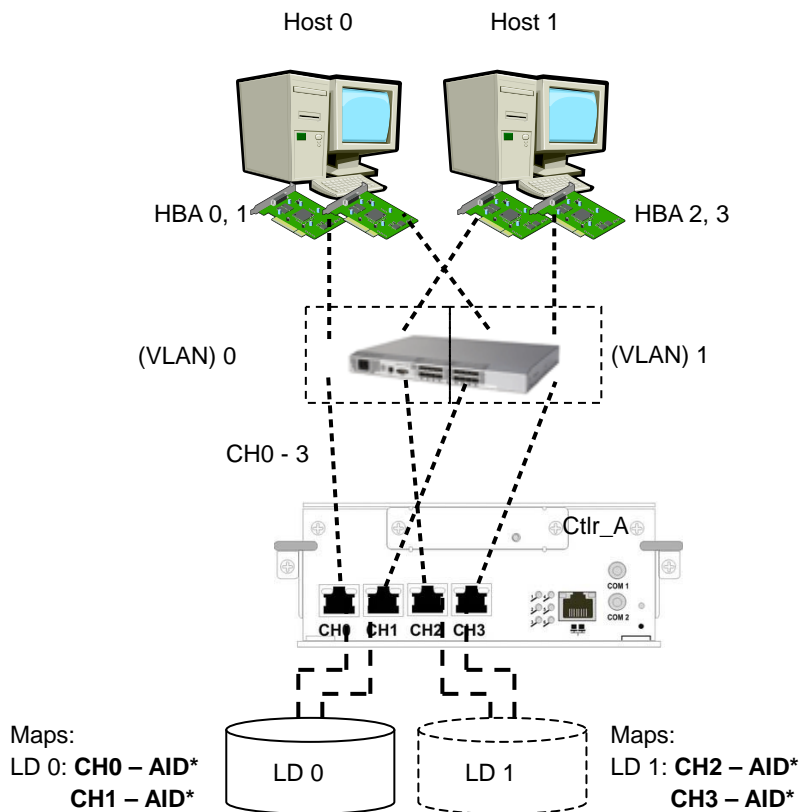


Тип отказа	Отказ	Доступный путь	MPIO
HBA	HBA 0	Host 0 -> LD 0: HBA 1 – VLAN0 – CH0 – AID – LD 0 Host 0 -> LD 0: HBA 1 – VLAN0 – CH1 – AID – LD 0	✓
	HBA 0 – VLAN0	Такой же, как при отказе HBA 0	✓
Один кабель	VLAN0 - Ctrl_A	Host 0 -> LD 0: HBA 0 – VLAN0 – CH1 – AID – LD 0 Host 0 -> LD 0: HBA 1 – VLAN0 – CH1 – AID – LD 0	✓
	Свич	Zone 0	X (Host 0 -> LD 0)
Контроллер	Ctrl_A	X	
Нет контроллера	Ctrl_A		

## iSCSI IP SAN – 2

Модели с одиночным контроллером (типа G) для кластерного окружения

# Host	# HBA	# Channel	# Cable	# Controller	# LD	# Map	Hub status
2	4 с 1 портом	4	8	1	2	4	Нет

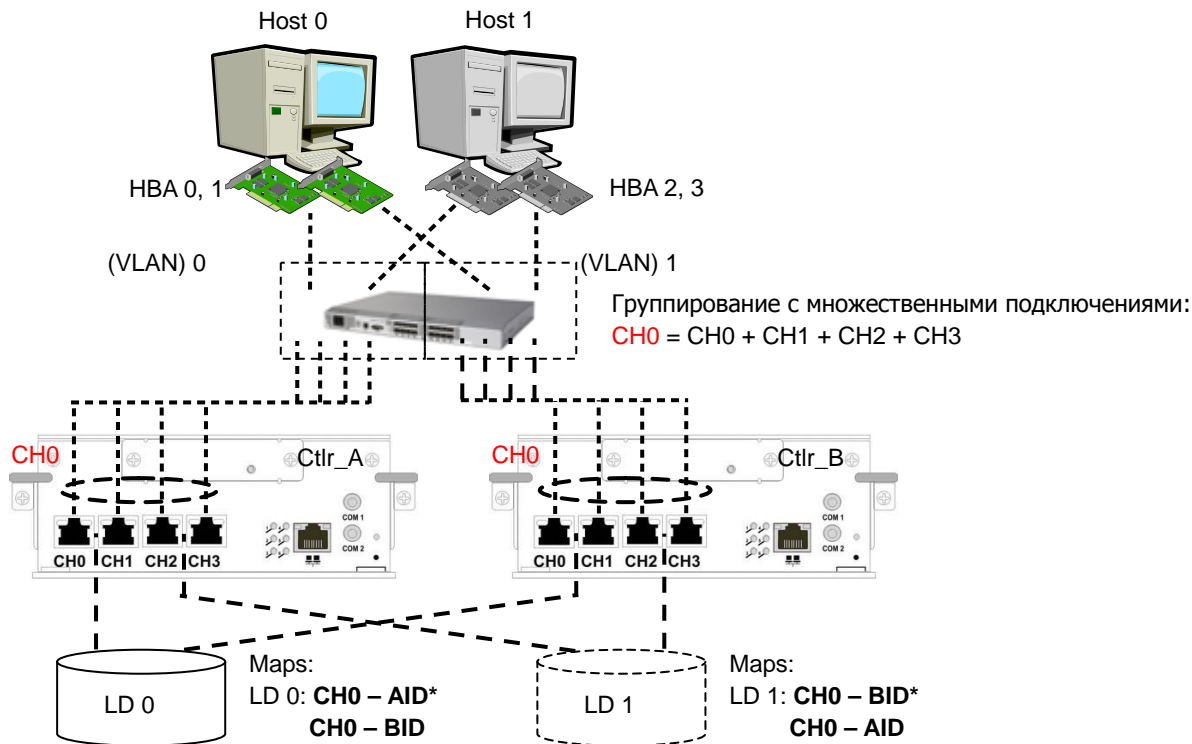


Тип отказа	Отказ	Доступный путь	MPIO
НБА	HBA 0	X (Обработка кластерной ОС)	✓
Один кабель	HBA 0 – VLAN0	Такой же, как при отказе HBA 0	✓
	VLAN0 - Ctlr_A	Host 0 -> LD 0: HBA 1 – VLAN1 – CH1 – AID – LD 0 Host 1 -> LD 0: HBA 3 – VLAN1 – CH1 – AID – LD 0	✓
Свич	VLAN0	Такой же, как при отказе кабеля VLAN0 – Ctlr_A	✓
Контроллер	Ctlr_A	X	
Нет контроллера	Ctlr_A		

### iSCSI IP SAN – 3

Модели с избыточным контроллером, один хост, два хоста или кластер

# Host	# HBA	# Channel	# Cable	# Controller	# LD	# Map	Hub status
2 (1)	4 с 1 портом	2	12 (10)	2	2	4	Нет



Пользователь может также настроить хост 1 как внекластерный сервер.

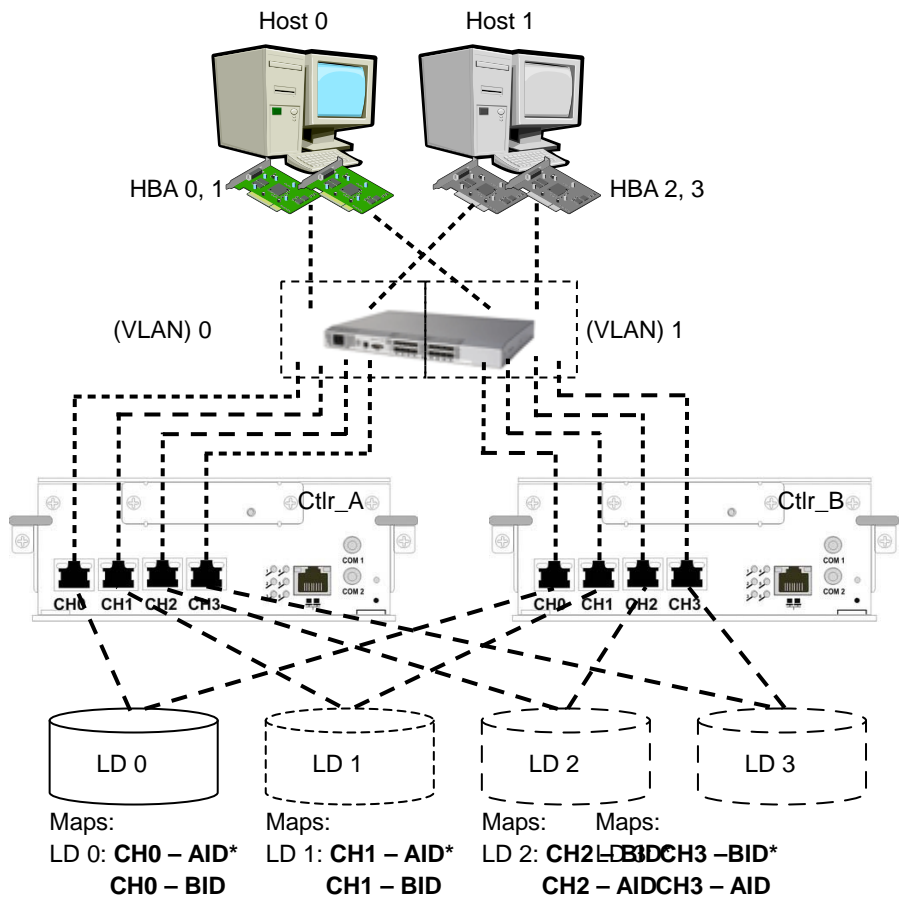
Тип отказа	Отказ	Доступный путь	MPIO
HBA	HBA 0	Host 0 -> LD 0: HBA 1 – VLAN1 – CH0 – BID – LD 0 (re-route)	✓
		Host 0 -> LD 1: HBA 1 – VLAN1 – CH0 – BID – LD 1	
Кабель	HBA 0 – VLAN0	Такой же, как при отказе HBA 0	✓
	VLAN0 - CH0 - Ctr_A	Отказ одного кабеля не влияет, при отказе двух: Host 0 -> LD 0: HBA 1 – VLAN1 – CH0 – BID – LD 0 (re-route) Host 0 -> LD 1: HBA 1 – VLAN1 – CH0 – BID – LD 1	
Свич	VLAN0	Такой же, как при отказе HBA 0	✓
Контроллер	Ctr_A	Host 0 -> LD 0: HBA 1 – VLAN1 – CH0 – AID – LD 0	✓
		Host 0 -> LD 1: HBA 1 – VLAN1 – CH0 – BID – LD 1	
Нет контроллера	Ctr_A	Тот же, что при отказе контроллера А	✓

ПРИМЕЧАНИЕ: В конфигурации с двумя серверами приложений, не объединенных в кластер, пользователь должен применять блокировку файлов, закрытие портов, маскирование LUN или VLAN, чтобы не допустить доступа разных хостов к одному и тому же LD и смешивания данных.

## iSCSI IP SAN – 4

Модели с избыточным контроллером, один хост, два хоста или кластер

# Host	# HBA	# Channel	# Cable	# Controller	# LD	# Map	Hub status
2 (1)	4 с 1 портом	4	12 (10)	2	4-8	8-16	Нет



Примечание: чтобы получить все, что можно, от этой конфигурации, пользователь должен создать 4 или больше LD (LD4, LD5, LD6 и LD7) и определить пассивные пути как активные пути данных следующим образом:

LD 4: CH2 – AID\*  
CH2 – BID

LD 5: CH3 – AID\*  
CH3 – BID

LD 6: CH0 – BID\*  
CH0 – AID

LD 7: CH1 – BID\*  
CH1 – AID

Пользователь может также настроить хост 1 как внекластерный сервер.

Тип отказа	Отказ	Доступный путь	MPIO
HBA	HBA0	Host 0 -> LD 0: HBA 1 – VLAN1 – CH0 – BID – LD 0 (re-route)	✓
		Host 0 -> LD 1: HBA 1 – VLAN1 – CH1 – BID – LD 1 (re-route)	
		Host 0 -> LD 2: HBA 1 – VLAN1 – CH2 – BID – LD 2	
		Host 0 -> LD 3: HBA 1 – VLAN1 – CH3 – BID – LD 3	
Кабель	HBA0 – VLAN0	Такой же, как при отказе HBA 0	✓
	VLAN0 – CH0 –	Host 0 -> LD0: HBA 1 – VLAN1 – CH0 – BID – LD 0 (re-route) Host 0 -> LD1: HBA 0 – VLAN0 – CH1 – AID – LD 1	✓

	Ctrl_A	Host 0 -> LD2: HBA 1 – VLAN1 – CH2 – BID – LD 2	
		Host 0 -> LD3: HBA 1 – VLAN1 – CH3 – BID – LD 3	
Свич	VLAN0	Такой же, как при отказе HBA 0	✓
Контроллер	Ctrl_A	Host 0 -> LD0: HBA 1 – VLAN1 – CH0 – AID – LD 0	✓
		Host 0 -> LD1: HBA 1 – VLAN1 – CH1 – AID – LD 1	
		Host 0 -> LD2: HBA 1 – VLAN1 – CH2 – BID – LD 2	
		Host 0 -> LD3: HBA 1 – VLAN1 – CH3 – BID – LD 3	
Нет контроллера	Ctrl_A	Тот же, что при отказе контроллера A	✓

ПРИМЕЧАНИЕ: В конфигурации с двумя серверами приложений, не объединенных в кластер, пользователь должен применять блокировку файлов, закрытие портов, маскирование LUN или VLAN, чтобы не допустить доступа разных хостов к одному и тому же LD и смешивания данных.



## 2. Транкинг (объединение связей)

Транкинг осуществляется в соответствии со стандартом IEEE 802.3.

### Обратите внимание:

#### 1. Ограничения использования:

##### a. ID канала:

Если объединяются несколько портов хоста, все ID будут доступны как будто по одному каналу.

##### b. Назначение IP адресов:

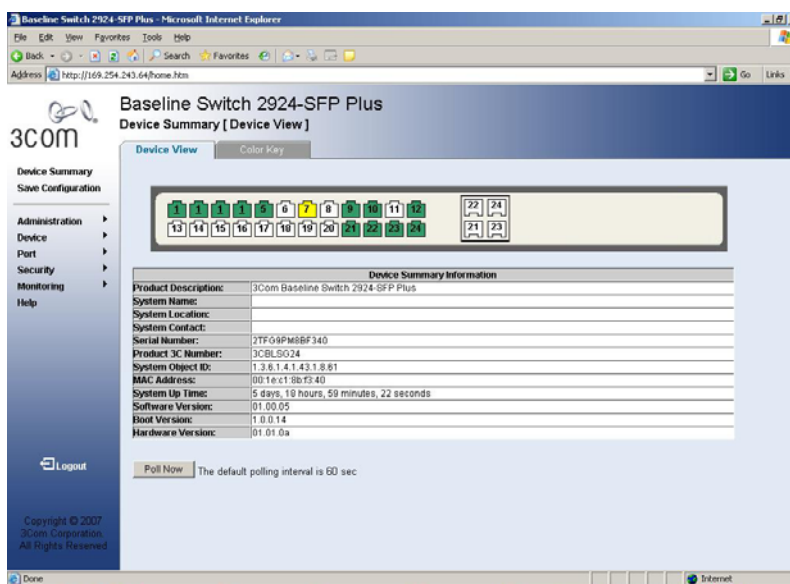
Объединенные порты будут иметь один IP. Объединенные порты будут принадлежать одной и той же подсети

##### c. Подключение LUN:

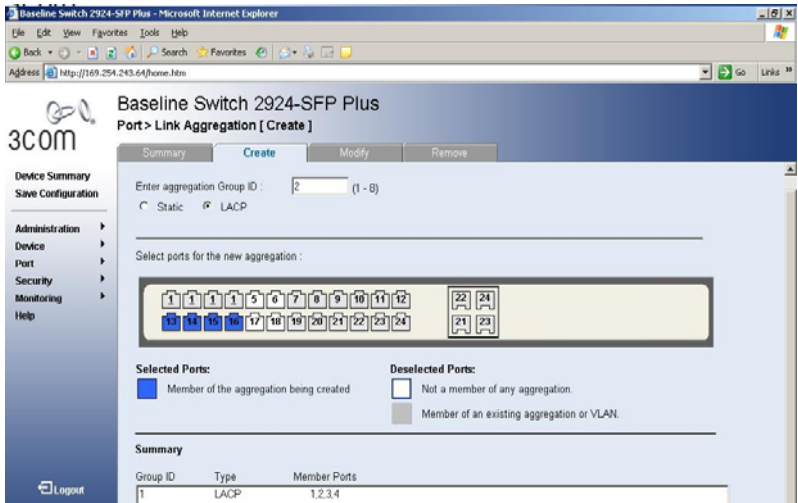
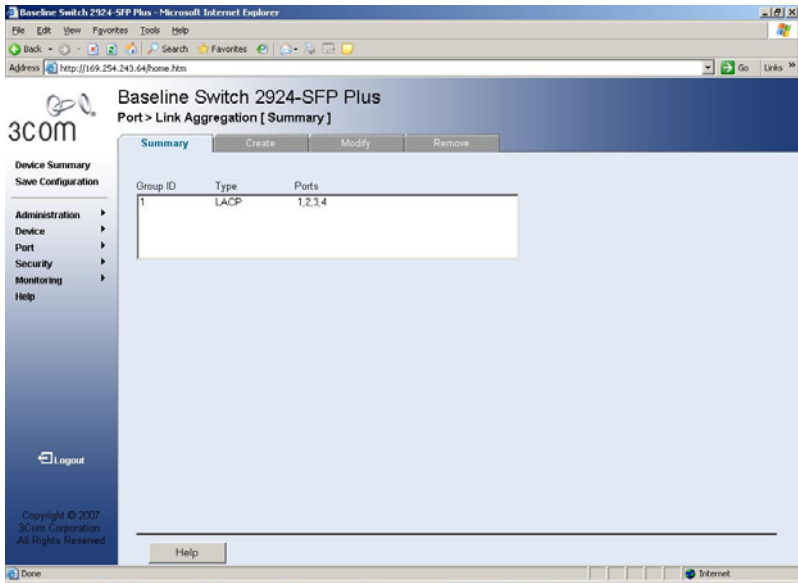
Подключение LUN к объединенной группе портов выполняется так же, как подключение к одиночному порту хоста.

##### d. Настройка свича:

Порты свича также должны быть настроены соответствующим образом, рекомендуется сделать это до изменения настроек системы. Пример настройки транкинговых портов свича (3COM 2924-SFP Plus) показан ниже:



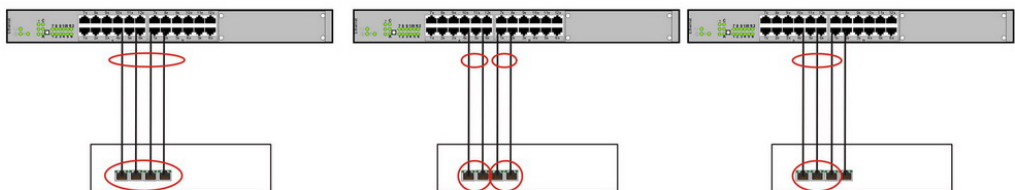
Настройка выполняется посредством Port -> Link Aggregation -> Aggregation group ID. Выбор порта производится с помощью LACP -> Select port.



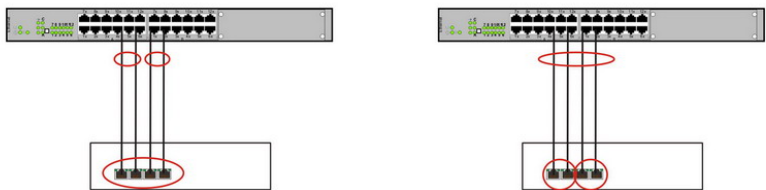
Изучите документацию на ваши Ethernet свичи и ознакомьтесь с инструкциями по настройке транкинговых портов.

Убедитесь, что вы правильно настроили вашу iSCSI систему и Ethernet свичи. Иначе неизбежен отказ в работе сети.

### Supported Configurations



### Unsupported Configurations



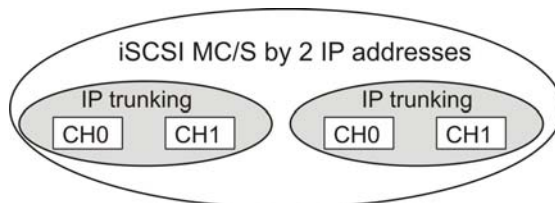
#### Ограничения [Условия и ограничения]

1. Объединенные интерфейсы должны быть подключены в одной и той же сети через один и тот же Ethernet свич, чтобы ограничить физическую изоляцию множественных путей.
2. Возможность транкинга зависит от наличия допускающих транкинг устройств и свичей.
3. Все порты должны быть объединены и иметь единственный IP, или несколько IP. Например, пусть имеется 4 GbE порта в iSCSI системе хранения и пользователь может настроить эти 4 порта так, чтобы они имели один IP, или два IP каждый, объединяя два физических порта. Если взять для примера избыточный контроллер S16E-R, то получим следующие комбинации портов:

	Объединенные порты		
Порты контроллера A	4	3 + 1	2 + 2
Порты контроллера B	4	3 + 1	2 + 2

4. Если транкинговая комбинация окажется неправильной, будет выдано сообщение об ошибке. Например, с 4 GbE портами в группе в iSCSI системе, в то время как соответствующие порты GbE свича не объединены в группу. В этом случае настройка транкинга не завершена, последует приглашение продолжить ее. Пользователь должен задать настройки свича и перезагрузить iSCSI систему снова.
5. Перезагрузка системы после изменения транкинговой конфигурации:
  - a. Создать новые транкинговые группы или изменить состав групп портов
  - b. Изменить ID транкинговой группы
  - c. Изменить IP адрес: Сбросить (как обычно, iSCSI хост-порты и 10/100BaseT mgmt. port)

6. Транкинг и iSCSI MC/S (Multiple Connections per Session):
  - 6-1. Настроить транкинговые порты перед настройкой MC/S.
  - 6-2. Если уже имеются какие-нибудь сконфигурированные MC/S группы, когда вы организываете IP транкинг, удалите их.



7. В соответствии с IEEE 802.3, объединение связей неприменимо в следующих случаях:
  - ... Объединение связей между несколькими системами
 

Методика, описанная в этой статье, неприменима, если речь идет об объединении связей между более, чем двумя системами.
  - ... Различные протоколы
 

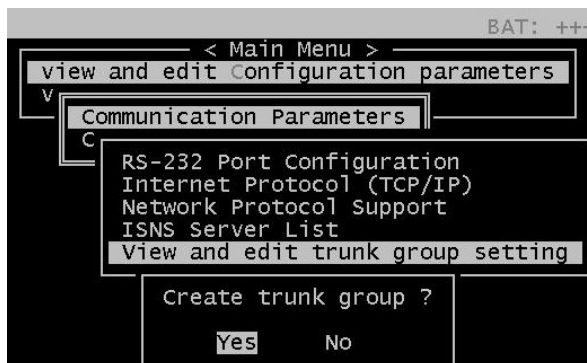
Транкинг применим только для связей, использующих протокол IEEE 802.3 (Gigabit Ethernet и FDDI не поддерживаются параллельно, однако различные физические среды, как, например, медные провода и оптоволокно, допускаются)
  - ... Полудуплексный режим
 

Объединение связей поддерживается только для двухточечных связей в дуплексном режиме.
  - ... Разные скорости передачи данных
 

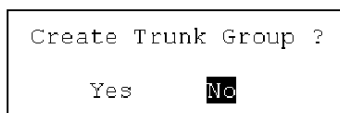
Все связи в транкинговой группе должны иметь одну и ту же скорость передачи данных (т.е. 10 Mb/s, 100 Mb/s, или 1000 Mb/s).
8. Пользователь не может удалить мастер-порт из транкинговой конфигурации, например, CH0 из транкинговой группы, состоящей из каналов 0, 1, 2 и 3. Первый порт (имеющий наименьший индексный номер) в транкинговой группе всегда считается мастер-портом. Чтобы убрать мастер-порт из транкинговой группы, вам необходимо удалить всю транкинговую группу.

### Процедура настройки:

- Шаг 1. Настройка начинается с View and Edit Configuration Parameters -> Communication Parameters -> View and Edit Trunk Group Setting. Нажать Enter, чтобы войти в подменю.



- Шаг 2. На приглашение Create Trunk Group? нажать Enter, или **Yes** для продолжения.



Если нет в наличии хост-портов для организации транкинга, или ранее созданы MC/S группы, вы получите сообщение об ошибке: "No available channel!".

- Step 3. Нажать Enter однократно, чтобы выбрать каждый канал. Перемещение к следующему каналу клавишами <-, >-. Нажать ESC по окончании выбора.

CHL	IPv4	IPv6
1 0	10.10.10.10	Disable
2 1	10.10.10.20	Disable
2	10.10.10.30	Disable
3	10.10.10.40	Disable

Некоторые каналы **НЕ МОГУТ БЫТЬ** выбраны:

1. Каналы, к которым уже подключены логические диски.
2. Каналы, уже включенные в транкинговые группы.
3. Каналы, уже включенные в MC/S группы.

- Шаг 4. Выбрать Yes и нажать Enter для подтверждения.

```

Trunk group member: CH 0, 1
                    IPv4: 10.10.10.10
                    IPv6: Disable

Create trunk group ?

Yes      No      Back
    
```

Шаг 5. Транкинговая конфигурация может выглядеть подобным образом. Вы можете отобразить до 4 хост-портов в транкинговую группу.

Member	Ch1	IPv4	IPv6
0, 1		10.10.10.10	Disable
2, 3		10.10.10.30	Disable

Шаг 6. Вы можете удалить канал из группы, или удалить полностью существующую группу с помощью следующих команд:

```

Remove exist trunk group member
Add new trunk group member
Delete current trunk group
    
```

Следует иметь в виду, что вы не можете удалить из группы каналы, к которым уже подключены логические диски.

Шаг 7. Установки начнут действовать после перезагрузки вашей iSCSI системы. Если порты вашего свича не настроены для транкинга, вы получите сообщение об ошибке.

Если вы объедините порты 0 и 1 в группу 1, а порты 2 и 3 в группу 2 в меню **View and Edit Channels**, вы сможете увидеть, что соответствующие каналы автоматически сконфигурированы в MC/S группы.

```

Tue Mar 31 12:00:15 2009          cache status: Clean
                                BAT: ++++
    
```

Q	Ch1	Mode	Grp	AID	BID	DefsyncClk	Defwid	S	Term	CursyncClk	Curwid
V	0	Host	0	0	1	Auto	iSCSI			1GHz	iSCSI
V	1	Host	0			Auto	iSCSI			1GHz	iSCSI
V	2	Host	2	0	1	Auto	iSCSI			1GHz	iSCSI
V	3	Host	2			Auto	iSCSI			1GHz	iSCSI
S	4	Drive				3.0 GHz	SAS	A		3.0 GHz	SAS
V	5	Drive				3.0 GHz	SAS	A			SAS
V	6	Drive				3.0 GHz	SAS	A			SAS
V	7(C)	RCCOM				3.0 GHz	SATA			3.0 GHz	SATA

```

Arrow Keys:Move Cursor   Enter:Select   Esc:Exit   Ctrl+L:Refresh Screen
    
```

### 3. Настройки сетевого интерфейса

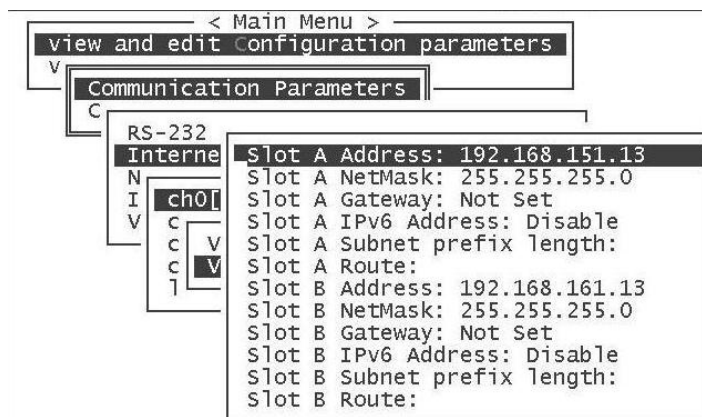
#### IP адреса iSCSI хост-портов

Получите у администратора вашей сети список действительных IP адресов. Присвойте соответствующие значения параметрам NetMask и Gateway, так чтобы подключить хост-порты к инициаторам на ваших серверах приложений.

Чтобы войти в подменю **Internet Protocol**, нажмите **[ENTER]** для подтверждения выбора и используйте стрелки для навигации.

**Шаг 1.** IP адреса iSCSI хост-порта можно найти следующим образом: "View and Edit Configuration Parameters" -> "Communication Parameters" -> "Internet Protocol (TCP/IP)".

В системе с избыточными контроллерами оба контроллера имеют 4 канала хоста, обозначенные как CH0, CH1, CH2 и CH3.



**Шаг 2.** Нажать **[ENTER]** на порту хоста, который вы хотите настроить.

Параметры порта отображаются в виде:

"Channel number [LAN] MAC address – IP address (IP acquisition method)"

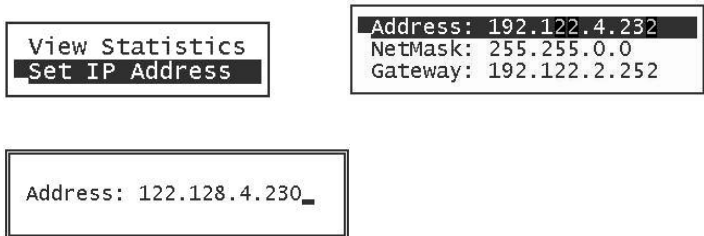
Адреса Slot A и Slot B относятся к хост-портам на разных RAID контроллерах.

**ПРИМЕЧАНИЕ 1:** "lan0" есть порт управления 10/100BaseT для доступа Telnet или SANWatch.

**ПРИМЕЧАНИЕ 2:** Соответствующие порты контроллера A и

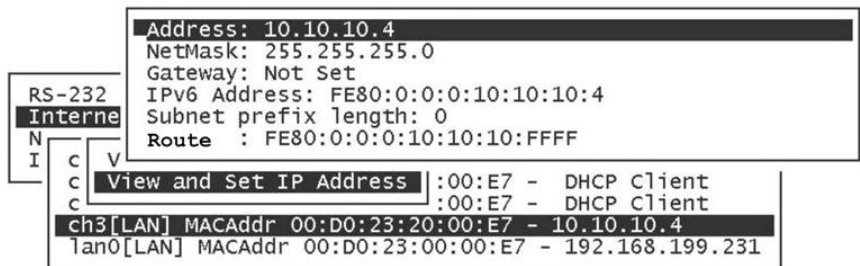
контроллера В должны быть в одной и той же подсети. В случае отказа контроллера хост должен иметь возможность доступа к исправному контроллеру по альтернативным путям.

Шаг 3. Нажать **[ENTER]** , чтобы выбрать "Set IP Address".



Шаг 4. Перегрузить контроллер после завершения всех настроек сети.

### Адреса в Internet Protocol Version 6 (IPv6)



Так как использование IPv6 предусматривает более автономную работу с автоматической адресацией, то в большинстве случаев происходит автоматическая настройка сети. Доступно автоматическое определение локальных имен как с локальным DNS сервером, так и без него.

Введите **"AUTO"** в поле **IPv6 address**, и адрес будет доступен после перезагрузки системы.

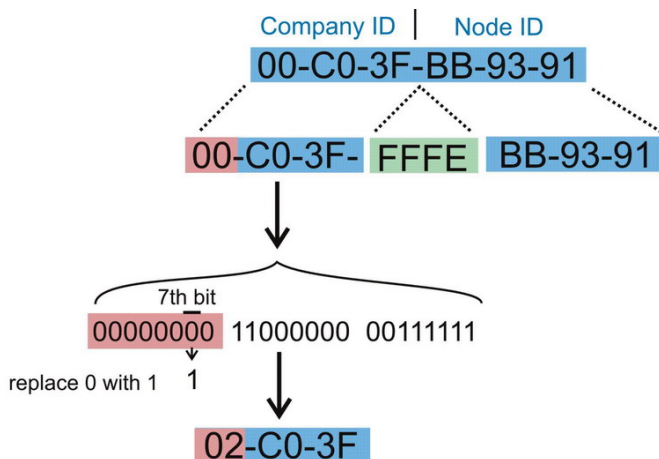
IPv6 адреса можно получить следующими способами:

- Локальные адреса автоматически задаются вводом **AUTO** в поле IPv6 адреса. При двухточечном соединении без роутера адреса генерируются с использованием адресов портов и начинаются с "fe80::" Локальные связи имеют адресацию в той же подсети.
- Если адреса назначаются автоматически, то поля **"Subnet prefix length"** и **"Route"** можно оставить пустыми.



- Если в сети имеется DHCPv6 сервер, то его IPv6 адрес будет запрошен автоматически.
- Если имеется IPv6 роутер, то вы можете ввести AUTO в поле Route и разрешить роутеру определить сетевые адреса.
- Вы можете также вручную ввести IPv6 адреса, генерируя их из 48-битных адресов Ethernet портов в формате EUI-64 добавлением до 64 шестнадцатиричных битов, после чего использовать комбинацию префикса fe08 и длины префикса для того, чтобы обозначить подсеть.

Пример показан ниже:: 1. Ввести FFFE между ID компании и ID узла как четвертый и пятый октеты (16 бит). 2. Установить для бита Universal/Local (U/L) (седьмой в первом октете), значение 0, или 1. "0" указывает на локальное администрирование, а "1" указывает на уникальный глобальный ID в интерфейсе IPv6 .



IPv6 interface ID = **2C0:3FFF:FEBB:9391**

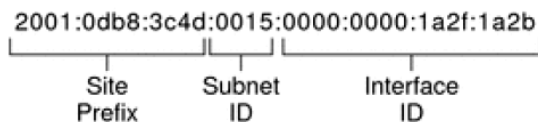
Системы Infortrend поддерживают различные IPv6 механизмы, включая Neighbor Unreachability Detection, stateful/stateless автонастройку адресов, ICMPv6, Aggregatable Global Unicast Address, Neighbor Discovery, и т.д.

## Поле длины префикса

Длина префикса является частью ручной установки. IPv6 сеть представляет собой группу смежных IPv6 адресов. Размер этого поля должен быть степенью 2. Длина префикса означает количество битов для первых 64 битов IPv6 адресов, которые одинаковы для всех хостов в данной сети и называются сетевым префиксом адреса.

Эти последовательные биты в IPv6 адресе записываются в таких же обозначениях, как ранее в IPv4 Classless Inter-Domain Routing (CIDR). В CIDR к ведущей последовательности битов добавляется размер этого блока битов (префикса) в десятичной нумерации, отделенный символом (/), т.е. 2001:0db8:1034::5678:90AB:CDEF:5432/48. (На экране встроенного ПО слэш не нужен. Номер префикса вводится в поле длины.)

Структура IPv6 адреса показана ниже:



Первые 48 битов содержат префикс устройства, следующие 16 битов содержат информацию о подсети. Префикс IPv6 адреса представляет собой комбинацию IPv6 рефикса (**адрес**) и **длины префикса**. Префикс имеет структуру "ipv6-prefix/prefix-length" и представляет собой блок адресного пространства (или сети). Переменная ipv6-prefix следует общим правилам IPv6 адресации (см. RFC 2373).

IPv6 сеть может быть определена первым адресом в сети и количеством битов префикса, как, например, 2001:0db8:1234::/48. С префиксом /48 сеть начинается с адреса 2001:0db8:1234:0000:0000:0000:0000:0000 и заканчивается адресом 2001:0db8:1234:ffff:ffff:ffff:ffff:ffff.

Индивидуальные адреса часто записываются в CIDR обозначениях, чтобы показать поведение сети, к которой они принадлежат. Например, адрес 2001:db8:a::123/128 указывает на простую интерфейсную связь для него, тогда как 2001:db8:a::123/32 может означать другое окружение.

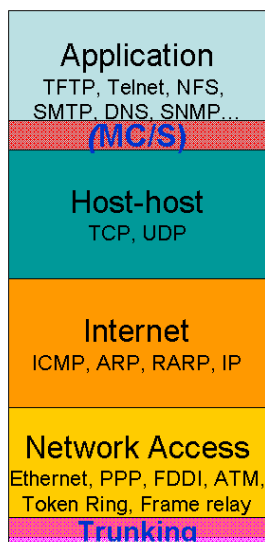
IPv6 Prefix	Описание
2001:410:0:1::45FF/128	Подсеть только с одним IPv6 адресом
2001:410:0:1::/64	Подсеть, содержащая $2^{64}$ узлов. Часто это длина префикса для подсети
2001:410:0::/48	Подсеть, содержащая $2^{16}$ узлов. Часто это длина префикса для места

## 4. Группирование (MC/S, Multiple Connections per Session)

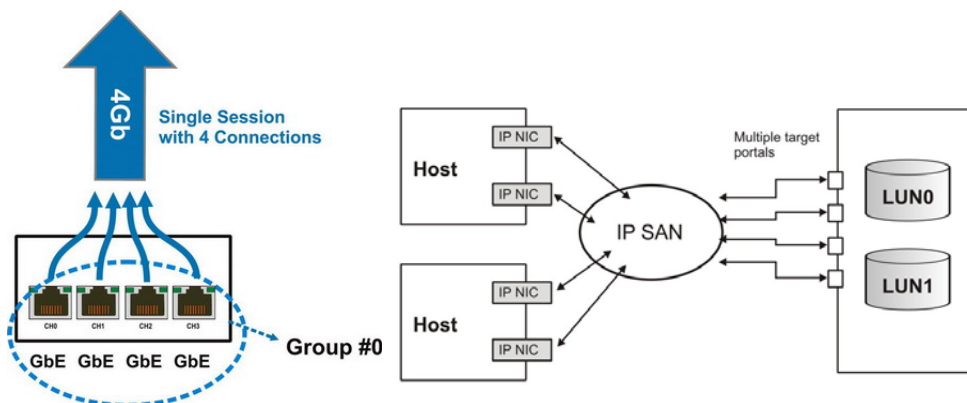
**ПРИМЕЧАНИЕ:** Если iSCSI порты сконфигурированы в транкинговые группы, то они автоматически объединяются в MC/S группы, и вы можете пропустить этот раздел.

Группирование отличается от транкинга. Транкинг связывает множественные физические интерфейсы, так что они рассматриваются как один и образуют TCP/IP стек. С другой стороны, MC/S позволяет порталам инициатора и приемника взаимодействовать скоординированно. MC/S обеспечивает интеллектуальную обработку ошибок, так что отказавшая связь может быть быстро восстановлена за счет других ненарушенных соединений в том же сеансе. MC/S является частью протокола iSCSI, который лежит под SCSI и над TCP/IP.

### Trunk vs. MCS vs. TCP/IP



Группирование (MC/S) объединяет множественные хост-порты в логическом сеансе "инициатор-приемник". MC/S может улучшить пропускную способность и эффективность передачи данных в ходе TCP сеанса. Кроме того, эта функция помогает вам подключать логический диск ко множественным ID хост-каналов на множественных хост-портах.



**ПРИМЕЧАНИЕ:** Если вы предпочитаете группирование с использованием карт HBA iSCSI TOE, ваши HBA должны тоже поддерживать MC/S.

**Конифигурации:**

Доступ к функции группирования через "View and Edit Channels." Нажмите Enter на Host Channel для отображения функций канала. Измените номер группы на выбранных каналах, чтобы объединить их в одну логическую группу.

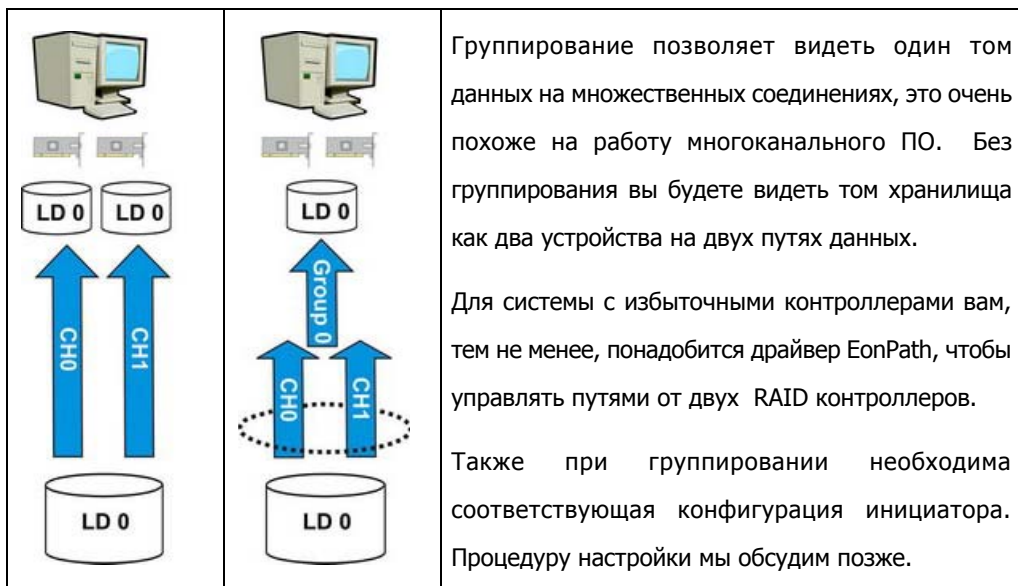
Q	Ch1	Mode	Grp	ID	DefSynClk	Defwid	s	Term	CurSynClk	Curwid
V	0	Host	0	0	Auto	iSCSI			100MHz	iSCSI
V	1	Host	0	0	Auto	iSCSI			100MHz	iSCSI
V	2	Host	1	0	Auto	iSCSI			100MHz	iSCSI
V	3	Host	3	0	Auto	iSCSI			100MHz	iSCSI
V					Auto	SATA				SATA
V					Auto	SATA				SATA
V	6	Drive			Auto	SATA				SATA
V	7	Drive			Auto	SATA			1.5 GHz	SATA

Q	Ch1	Mode	Grp	ID	DefSynClk	Defwid	s	Term	CurSynClk	Curwid
V	0	Host	0	0	Auto	iSCSI			100MHz	iSCSI
V	1	Host	1	0	Auto	iSCSI			100MHz	iSCSI
V	2	Host	2	1	Auto	iSCSI			100MHz	iSCSI
V	3	Host	3	1	Auto	iSCSI			100MHz	iSCSI
V					Auto	SATA				SATA
V					Auto	SATA				SATA
V	6	Drive			Auto	SATA				SATA
V	7	Drive			Auto	SATA			1.5 GHz	SATA

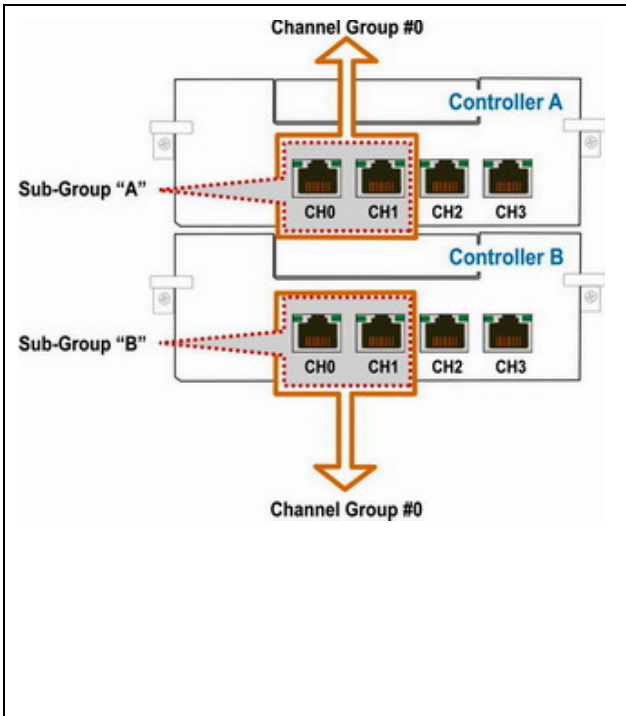
**ПРИМЕЧАНИЕ:** Изменение конфигурации групп требует перезагрузки системы.

После логического группирования логический диск, подключенный к группе каналов, будет виден как одно устройство на многих путях данных. Это очень напоминает использование многоканальных драйверов.



Без группы	В группе	
------------	----------	--

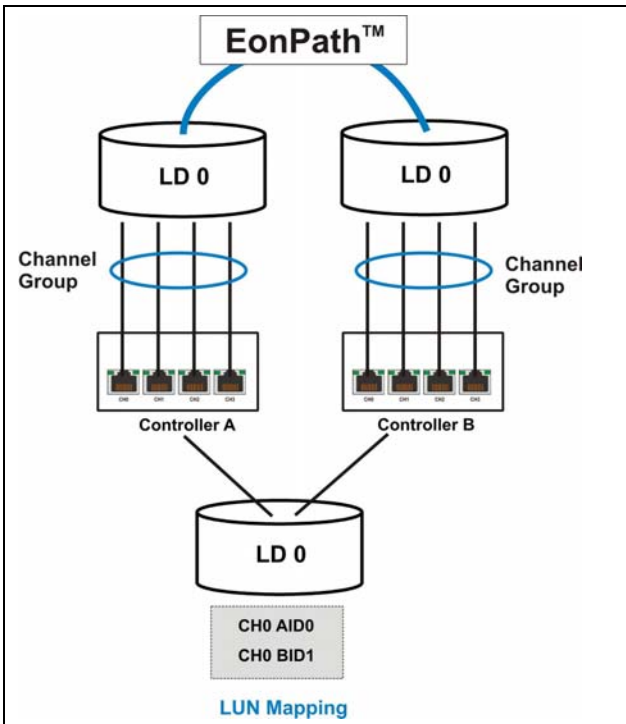
Хост-порты разных RAID контроллеров (система с избыточными контроллерами) НЕ ОБЪЕДИНЯЮТСЯ в группу. То-есть, в случае отказа одного контроллера IP адреса не будут переключены на контроллер, сохранивший работоспособность.



Q	Ch1	Mode	Grp	AID	BID	DefSynC1k	DefWid	S	Term	CurSynC1k	CurWid
V	0	Host	0	0	1	Auto	iSCSI			1GHZ	iSCSI
V	1	Host	0			Auto	iSCSI			1GHZ	iSCSI
V	2	Host	0			Auto	iSCSI			1GHZ	iSCSI
V	3	Host	0			Auto	iSCSI			1GHZ	iSCSI
V	4	Drive				3.0 GHZ	SAS	A		3.0 GHZ	SAS
V	5	Drive				3.0 GHZ	SAS	A			SAS
V	6	Drive				3.0 GHZ	SAS	A			SAS
V	7(C)	RCCOM				3.0 GHZ	SATA			3.0 GHZ	SATA

Встроенное ПО обеспечивает параллельную работу. На экране системы с избыточными контроллерами вы можете видеть настройки одного контроллера, однако они автоматически применяются и ко второму контроллеру. Если вы сконфигурируете "группы каналов", тем самым вы в действительности создадите такие же группы на параллельном контроллере (см. рисунок слева).

Один том, подключенный как AID и BID, появится как два устройства на канале A и на канале B. Затем вам понадобится многоканальный драйвер EonPath для управления отказоустойчивыми путями.



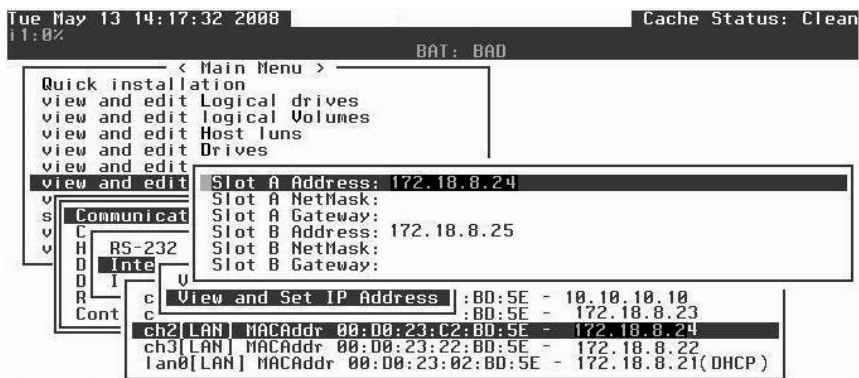
На рисунке слева вы видите 1 логический диск как два устройства на 8 линиях передачи данных (в двух группах каналов). Подключение к ID обоих контроллеров с помощью EonPath обеспечит непрерывный доступ к данным в случае отказа кабеля или контроллера.

**ПРИМЕЧАНИЕ:** Если каналы сгруппированы, то группа каналов ведет себя как один канал, и атрибуты отдельных каналов исчезают. Например, если 4 канала объединены в группу, то сохраняются только ID на первом канале.

До группирования		После группирования	
Channel 0	ID 0	Channel 0	ID 0
Channel 1	ID 0	Channel 1	-
Channel 2	ID 0	Channel 2	-
Channel 3	ID 0	Channel 3	-

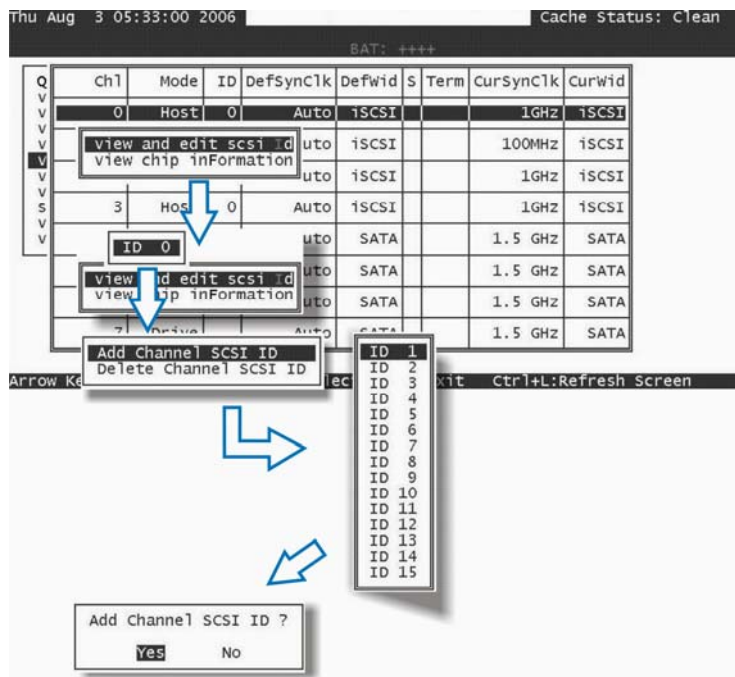
Q	Ch1	Mode	Grp	AID	BID	DefSynCk	DefWid
v	0	Host	0	0	1	Auto	iSCSI
v	1	Host	0	-	-	Auto	iSCSI
v	2	Host	0	-	-	Auto	iSCSI
v	3	Host	0	-	-	Auto	iSCSI
s	4	Drive				3.0 GHz	SAS
v	5	Drive				3.0 GHz	SAS
v	6	Drive				3.0 GHz	SAS
v	7(C)	RCCOM				3.0 GHz	SATA

**ПРИМЕЧАНИЕ:** Хотя информация об отдельных каналах недоступна, вы, тем не менее, должны позаботиться о TCP/IP подключениях. К примеру, вам следует проконсультироваться с вашим сетевым администратором и настроить статические IP адреса портов для iSCSI хост-портов. Информацию об отдельных хост-портах вы найдете по пунктам меню "View and Edit Configuration Parameters" -> "Communication Parameters" -> "Internet Protocol (TCP/IP)" -> "chx[LAN] MACAddr xxxxx."



## 5. Назначение ID хост-каналов

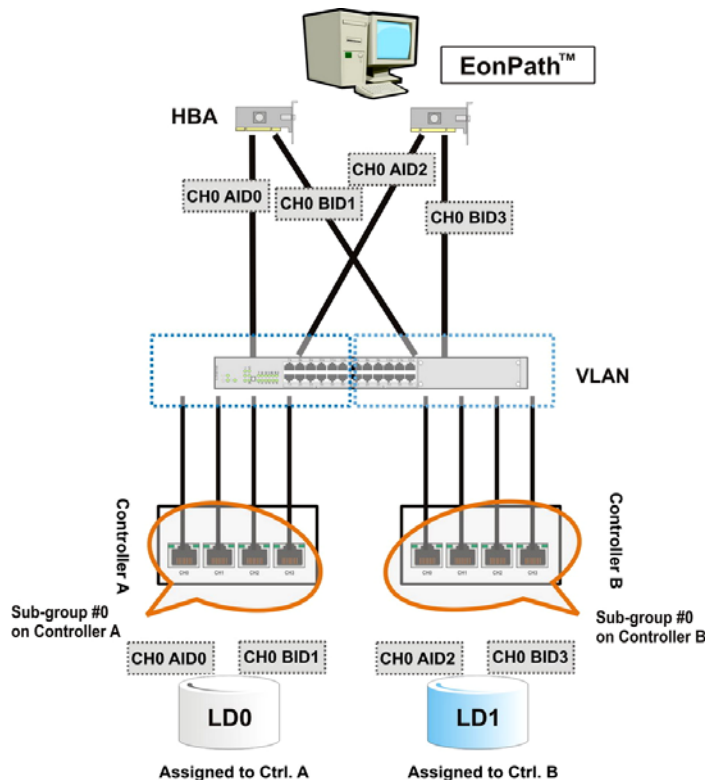
Система с избыточными контроллерами поставляется с двумя ID, AID0 и BID1, что недостаточно для настройки избыточных контроллеров. Следует назначить дополнительные ID в меню "View and Edit Channel". Добавление ID требует перезагрузки вашей системы хранения.



## 6. Назначение LUN томам данных

После того, как выполнены все настройки сети и RAID томов, установите и запустите инициаторы на вашем сервере приложений. Теперь вы можете включить сетевые устройства, хранилище, сервер и подключить тома данных к LUN хоста, после чего можно проверить правильность соединений и адресации в сети.





На рисунке выше показана базовая отказоустойчивая конфигурация, где обслуживание может продолжаться при одностороннем отказе кабеля или контроллера. Для простоты показан только 1 сервер и 4 хост-канала от него. К этой конфигурации можно присоединить другие логические диски, HBA и серверы.

### Создайте список инициаторов

```

< Main Menu >
Quick installation
view and edit Logical drives
view and edit logical Volumes
view and edit Host Luns
v
v
v
v
s
v
v
v
v
v
v
CHL 0 ID 0 (Slot A)
CHL 0 ID 1 (Slot B)
CHL 1 ID 0 (Slot A)
CHL 1 ID 1 (Slot B)
CHL 2 ID 0 (Slot A)
CHL 2 ID 1 (Slot B)
CHL 3 ID 0 (Slot A)
CHL 3 ID 1 (Slot B)
Edit iSCSI Initiator List
    
```

```

< Main Menu >
Quick installation
view and edit Logical drives
view and edit logical Volumes
view and edit Host Luns
v
v
v
v
s
v
v
v
v
v
v
CHL 0 ID 0 (Slot A)
CHL 0 ID 1 (Slot B)
CHL 1 ID 0 (Slot A)
CHL 1 ID 1 (Slot B)
CHL 2 ID 0 (Slot A)
CHL 2 ID 1 (Slot B)
CHL 3 ID 0 (Slot A)
CHL 3 ID 1 (Slot B)
View Information
Edit
Add iSCSI Initiator
Edit iSCSI Initiator
Delete iSCSI Initiator
Appserver1
    
```

После включения вашего сервера приложений вы должны увидеть



инициаторы на экране встроенного ПО. Используйте эти инициаторы для организации iSCSI соединений.

Вы можете выполнить следующие настройки в окне атрибутов инициаторов:

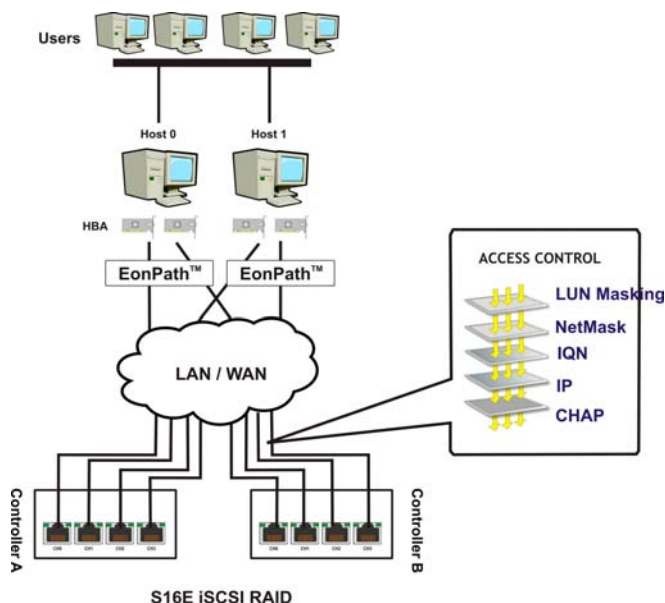
- 1. Введите имя инициатора.
- 2. 2-1. Вручную введите IQN инициатора, или
  - 2-2. Выберите инициатор из списка уже обнаруженных IQN.
- 3. Задайте одностороннюю или взаимную идентификацию CHAP (см. **7. Идентификация доступа по протоколу CHAP**).
- 4. Задайте IP адрес и установки NetMask (если необходимо). Иногда множественные порты инициатора на сервере приложений могут иметь одинаковые IQN.



Получив список инициаторов, встроенное ПО может начать процедуру настройки подключения LUN хоста и маскирования LUN. Продолжение настройки CHAP - в следующем разделе.

## 7. Идентификация доступа по протоколу CHAP

CHAP является одним из методов взаимной идентификации сетевых серверов и iSCSI хранилища.



CHAP - это **Challenge Handshake Authentication** protocol. По этому протоколу инициаторы на стороне хоста и системы хранения дистанционно идентифицируют друг друга с помощью зашифрованных паролей.

**Шаг 1.** Чтобы разрешить CHAP идентификацию, выберите "View and Edit Configuration Parameters" в главном меню, "Host-side Parameters," затем нажмите [ENTER] на "Login Authentication with CHAP", чтобы активировать приглашение к выбору режима CHAP.

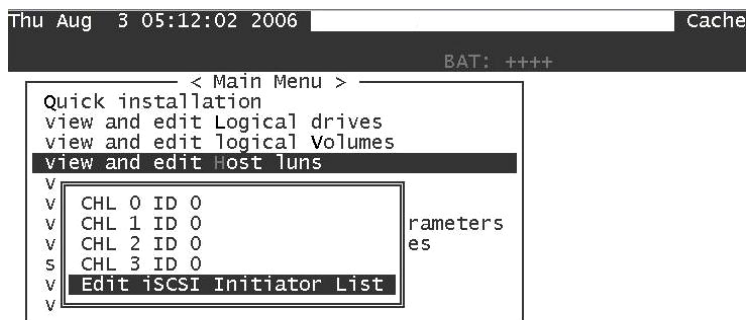
```

Thu Aug 3 05:39:26 2006                               Cache Status: Clean
                                                         BAT: ++++
< Main Menu >
Quic
view Maximum Queued I/O Count - 256
view LUNS per Host SCSI ID - 8
view Max Number of Concurrent Host-LUN Connection - Def(4)
view Number of Tags Reserved for each Host-LUN Connection - Def(32)
view Peripheral Device Type Parameters
view Cylinder - Variable / Head - Variable / Sector - Variable
view Login Authentication with CHAP - Disable
view Jumbo Frames - Disable
V
S
C
V
V
Host-side Parameters
Drive-side Parameters
Disk Array Parameters
Controller Parameters
Arrow Keys:Move Cursor  Enter:Select  Esc:Exit  Ctrl+L:Refresh Screen

```

**Шаг 2.** Поддерживается как односторонняя, так и двухсторонняя (взаимная) идентификация. При двухсторонней идентификации инициируется отдельное тройное квитирование между iSCSI инициатором и портами системы хранения.

Связанные с CHAP опции вы можете найти в списке iSCSI инициаторов на экране встроенного ПО в подменю "View and Edit Host LUNs".



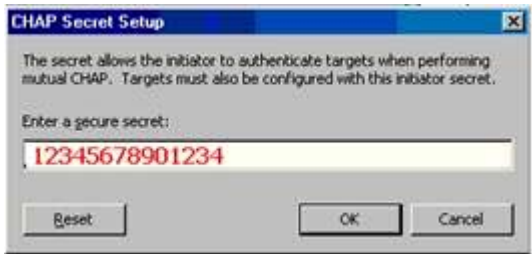
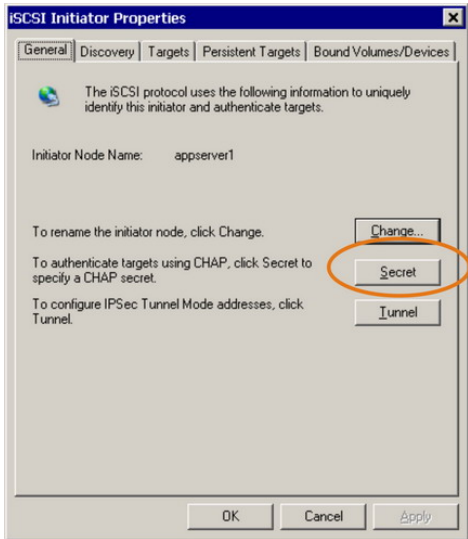
Arrow Keys:Move Cursor Enter:Select Esc:Exit Ctrl+L:Ref

Необходимо установить CHAP для каждого инициатора. Выберите и отредактируйте атрибуты инициаторов, как показано на следующем экране. Для CHAP идентификации используются User Name, User Password, Target Name и Target Password .

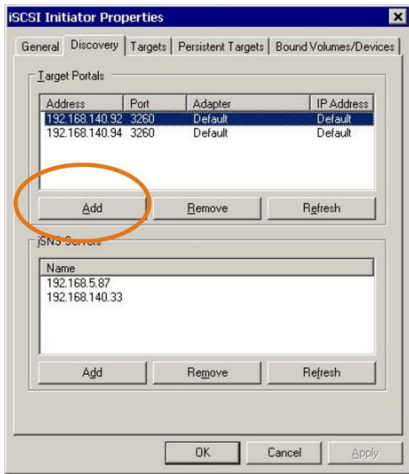
User Password (односторонний режим) должен иметь по крайней мере 12 байтов, а Target Password (двухсторонний режим) должен содержать не менее 14 байтов.



- Шаг 3.** Введите одинаковые пароли (секретный ввод) на экране конфигурации выше и на экране инициаторов ниже.
- Шаг 4.** Вернитесь к экрану Microsoft software initiator и введите пароль для двухсторонней CHAP идентификации в таблице **General**, щелкнув кнопку **Secret** (тот же, что вы ввели при конфигурировании для **Target Password**).

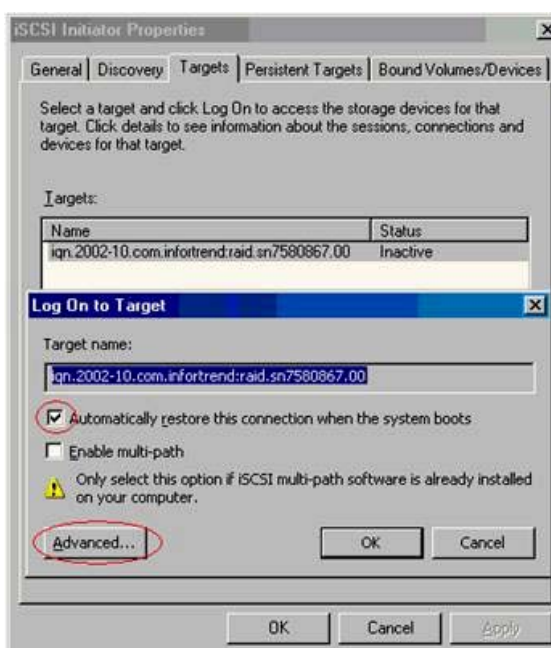


Шаг 5. Щелкните **Add** в таблице Discovery, щелкните кнопку и введите IP адреса iSCSI портов вашей системы хранения. Вы должны повторять процедуру **Add** до тех пор, пока все порты не будут добавлены, следовательно, CHAP **User Name** и **Secret** должны быть введены несколько раз.

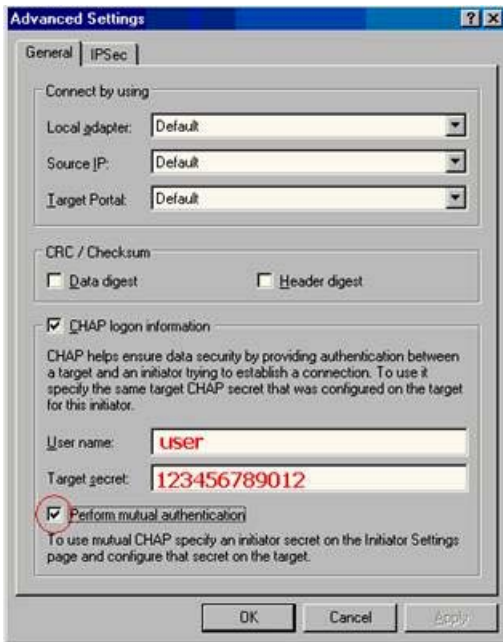




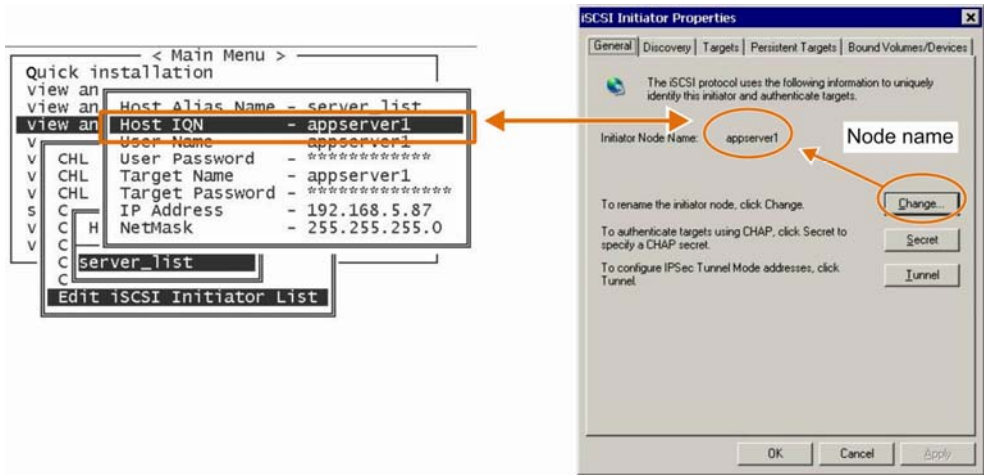
- Шаг 6. Щелкните **Log on** в таблице **Targets**, чтобы активировать соединение с iSCSI хост-портом. Щелкните кнопку **Advanced** после выбора клетки **Automatically Restore this connection...**



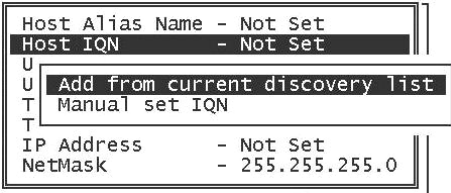
- Шаг 7. Вводит **User name** и **Target secret** для односторонней идентификации CHAP. Щелкните клетку **Perform Mutual Authentication**, если вы предпочитаете использовать взаимную идентификацию.



**ПРИМЕЧАНИЕ:** Убедитесь в праильности IQN, проверив экраны инициатора и конфигурации. Если вы видите активный статус на экране Discovery инициатора, значит, соединение прошло успешно.



Вы можете использовать функцию **"Add from current discovery list"**, чтобы проверить, не изменилось ли имя узла инициатора. Если IQN изменено, это изменение будет отражено в списке инициаторов.

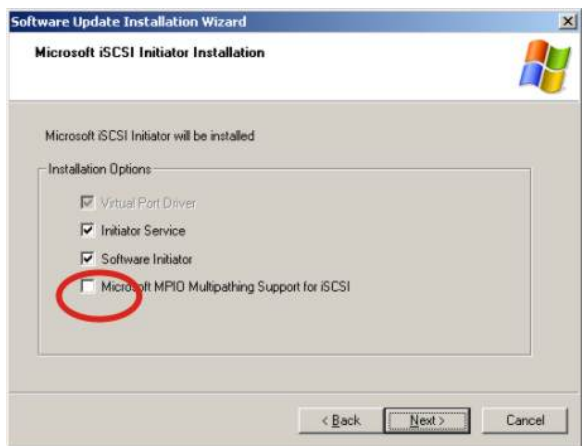


Microsoft iSCSI инициатор использует IQN по умолчанию как **User name** для настройки CHAP. Вместо него можно назначить другое имя **User Name**.

## 8. Настройка инициатора (на примере Microsoft Software Initiator)

### ВАЖНО!

Если вы намереваетесь использовать инициатор Microsoft и многоканальный драйвер Infotrend EonPath, отключите опцию MPIO, как показано ниже, при установке инициатора. Они могут оказаться несовместимыми.



При настройке iSCSI хранилища с избыточными контроллерами особое внимание следует уделять настройке инициаторов на стороне хоста. Ниже приводится процедура с использованием iSCSI инициаторов Microsoft.

Прежде всего, вы должны получить список IP хост-портов из меню "View and Edit Channels". В этом примере есть 8 IP хост-портов.

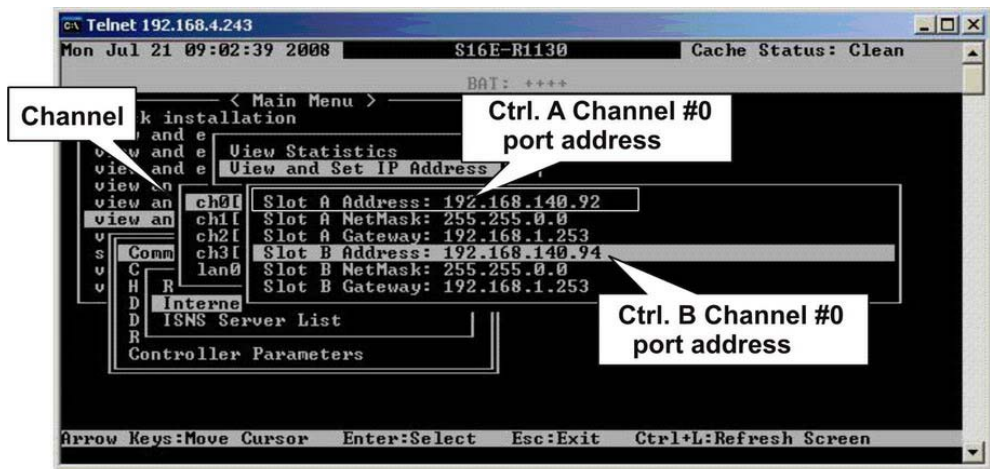
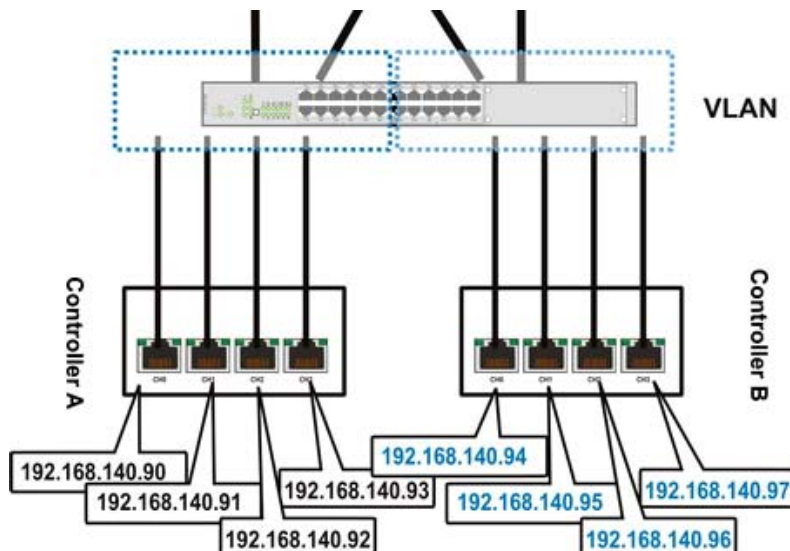


Схема соединений будет выглядеть следующим образом:





### Имя IQN:

Есть несколько мест, где вы можете видеть **IQN** (iSCSI Qualified Name) логического диска в сети. Имена IQN нужны, когда вы делаете настройки для iSCSI сеанса, или используете iSCSI TOE HBA.

1. Вы можете выполнить сканирование устройств хранения и увидеть IQN имя с помощью утилиты инициатора HBA, или программ инициатора, работающих на хосте, т.е. инициатора Microsoft iSCSI.
2. Вы можете использовать LCD кнопочную панель, чтобы найти серийный номер системы в **"Main Menu" → "System Information" - > "Serial Number"**

IQN хранилища Infotrend состоит из серийного номера системы и еще 3 цифр. IQN всегда выглядит приблизительно следующим образом:

`Iqn.2002-10.com.infotrend:raid.snXXXXXX.XXX`

6 цифр, следующих за "sn" - это **серийный номер** системы.

Последние 3 цифры показывают переменные в следующем порядке:

**"channel number" - "host ID" - "LD ownership"**

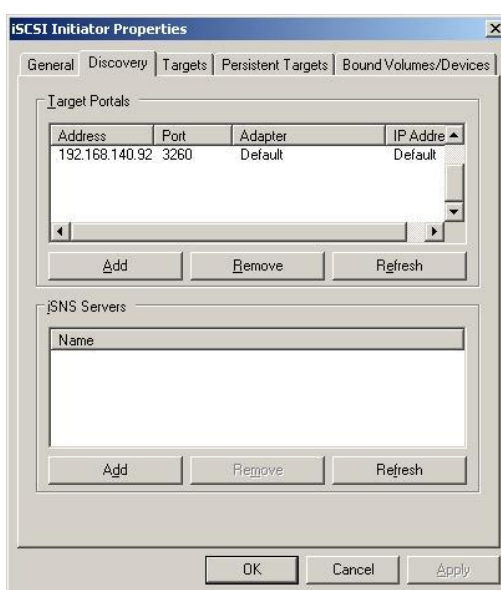
Цифра 1 в позиции "LD ownership" указывает на контроллер A, а цифра 2 - на контроллер B. Контроллер A, по определению, является доминирующим Primary контроллером. IQN соответствует подключению вашего логического диска к ID/LUN хоста. Например, если вы подключите ваш логический диск к каналу 0 и AID1, то последние три цифры будут 011.



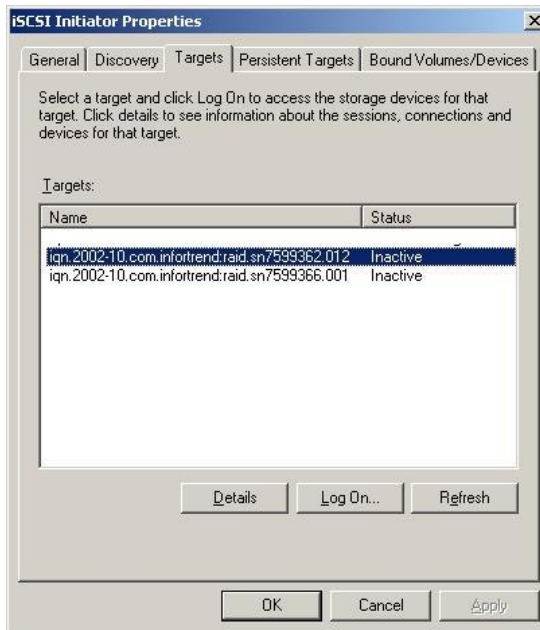
**ПРИМЕЧАНИЕ:** iSCSI системы EonStor со встроенным ПО rev. 3.64 и ниже, покажут только 2 цифры; номер канала и ID номер.

## Пример настройки

**Шаг 1.** Прежде всего откройте интерфейс инициатора и вручную добавьте адрес порта приемника, т.е. 192.168.140.90. Щелкните кнопку **Add**, чтобы добавить IP адрес порта приемника. (Это можно было также сделать во время настройки CHAP).



**Шаг 2.** Выберите IQN номер из списка в таблице **Targets**. Теперь вы можете идентифицировать iSCSI приемники 3-мя последними цифрами их IQN имен. Вы можете идентифицировать тома хранилища, видимые по различным линиям передачи данных.



**Шаг 3.** Щелкнуть **Log On...** Появится окно **Log On to Target**.  
Щелкните кнопку **Advanced** на нем.

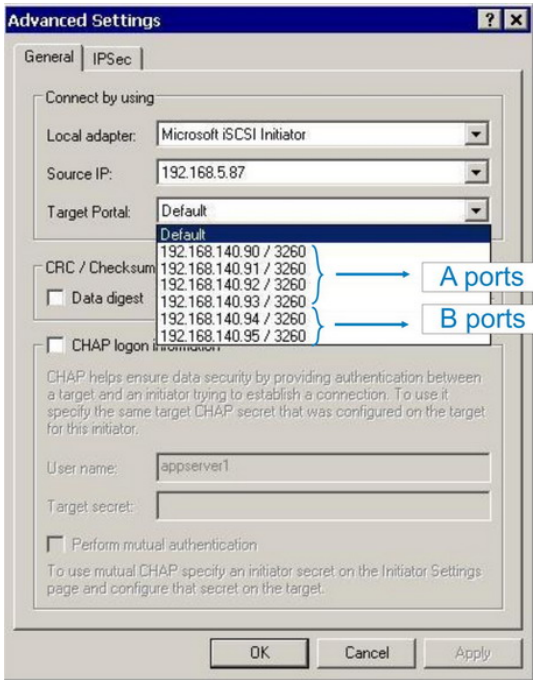


**Шаг 4.** Выберите подходящие опции для 1). **Local adapter**, 2). **Source IP** и 3). **Target Portal** из соответствующих выпадающих списков. Щелкните **OK**, чтобы закрыть окно.

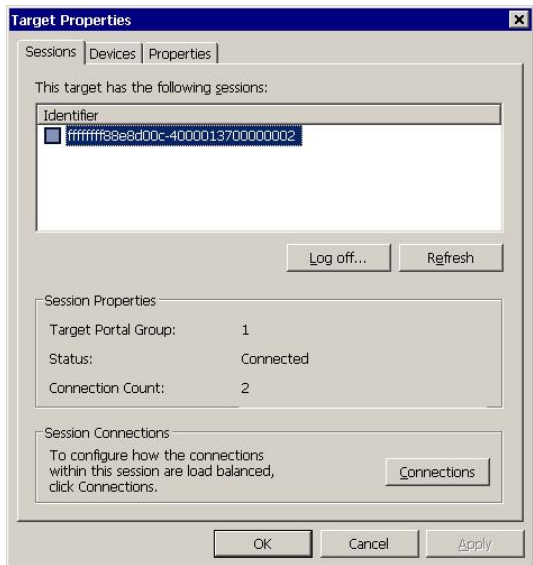
Выбирая портал приемника из выпадающего списка, убедитесь, что вы правильно связываете приемник с порталом приемника. Например, приемник (логический диск), управляемый контроллером А, должен быть связан с порталом приемника, которым является порт контроллера А.

`iqn.2002-10.com.infotrend:raid.snXXXXXX.XX1` -> A port target portal

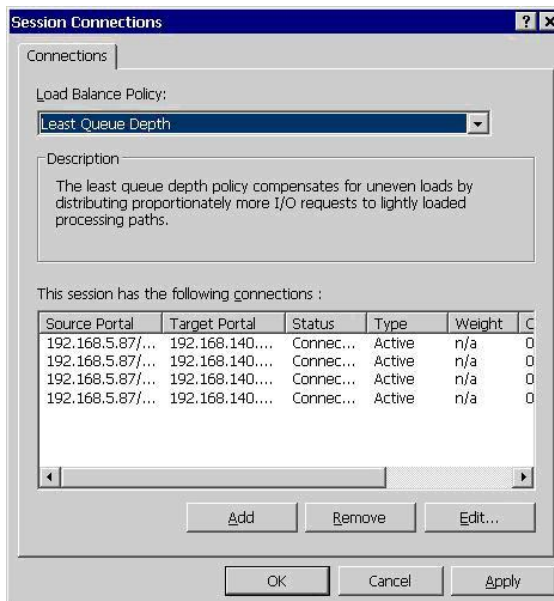
`iqn.2002-10.com.infotrend:raid.snXXXXXX.XX2` -> B port target portal



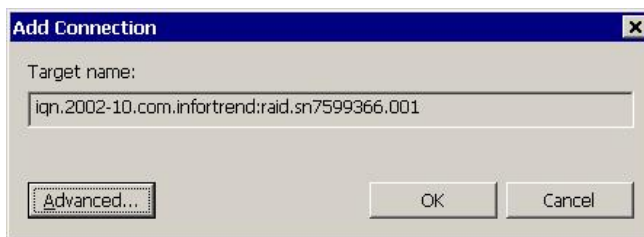
**Шаг 5.** Возвратитесь к окну **Targets**. Щелкните кнопку **Details**, чтобы добавить еще порты для этого iSCSI приемника. Появится окно **Target Properties**. Щелкните кнопку **Connections**.



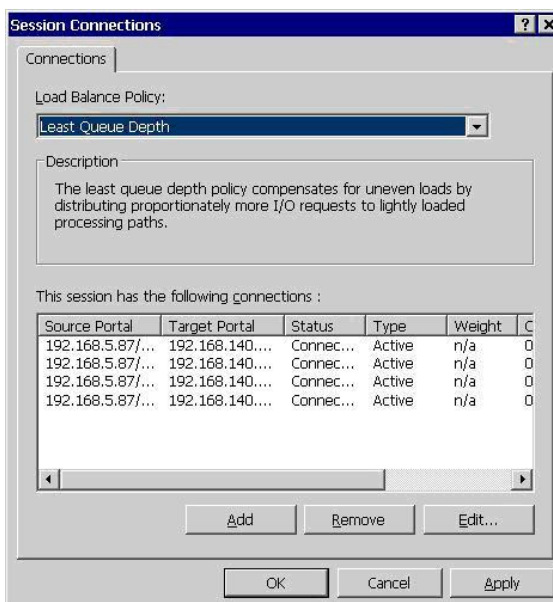
**Шаг 6.** Выберите **Least Queue Depth** в качестве режима балансировки нагрузки из выпадающего списка в окне **Session Connections**, затем используйте кнопку **Add**, расположенную ниже, чтобы включить другие порталы приемника (порталы порта A) в iSCSI сеанс.



**Шаг 7.** Щелкните кнопку **Advanced** в окне **Add Connection**.



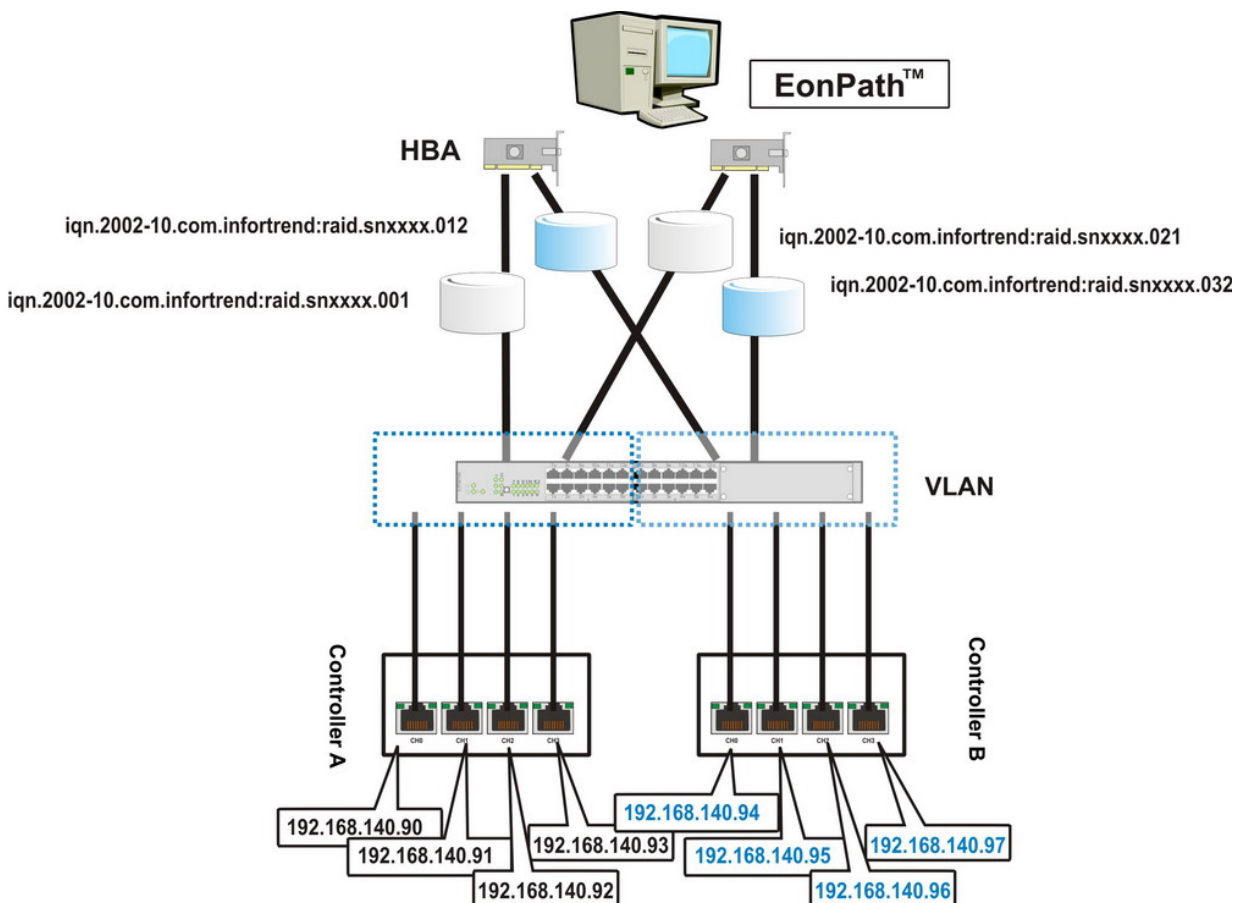
**Шаг 8.** Опять появится окно **Session Connections**. Выберите режим балансировки нагрузки и порт приемника, используя кнопку **Add**. Щелкните **OK** на следующих экранах, чтобы завершить процедуру настройки.



**Шаг 10.** Теперь вы закончили настройку связей приемника (логического диска) с порталами

приемника на контроллере А. Вы можете повторить эту процедуру, чтобы связать другой приемник, логический диск, с порталами приемника на контроллере В. Например, вы можете начать с добавления 192.168.140.94 (порт контроллера В) в окне **Discovery**. Другие порталы контроллера В, 192.168.140.95, ... 96, ...97, автоматически появятся в выпадающем списке.

**Шаг 11.** Когда вы закончите настройку, логические диски появятся как множественные дисковые устройства в окне управления Windows Disk Drive. Установите многоканальный драйвер EonPath, так чтобы хост смог распознать их как устройства, доступные через отказоустойчивые пути.

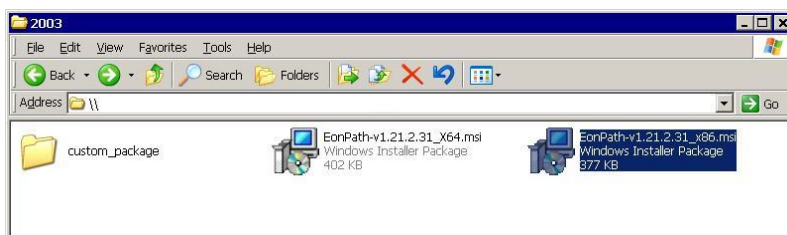


**ПРИМЕЧАНИЕ:** Ваша iSCSI конфигурация может содержать множественные серверы и много логических дисков. Максимальное число TCP сеансов - 64, если вы имеете 1GB кэш-памяти в RAID контроллере, и 32 сеанса, если вы используете кэш-память 512 MB.

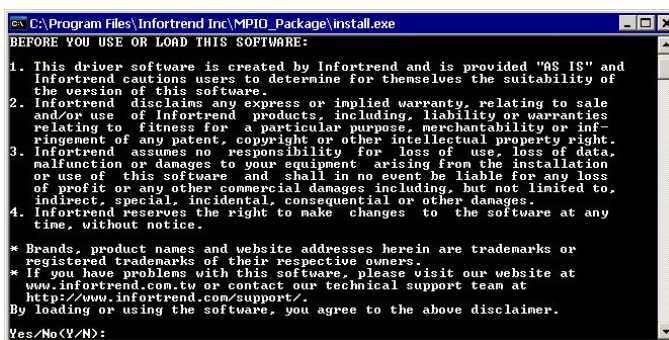
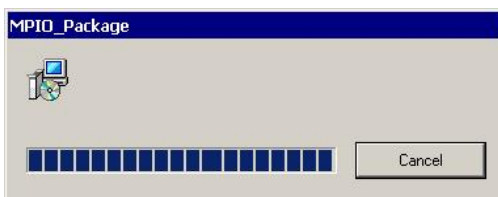
## 9. Установка драйвера EonPath

### Установите драйвер на сервер приложений (на примере Windows)

**Шаг 1.** Выберите и запустите двойным щелчком драйвер EonPath, соответствующий вашей ОС. EonPath поставляется на CD вместе с вашим продуктом, новые версии можно получить через службу технической поддержки.

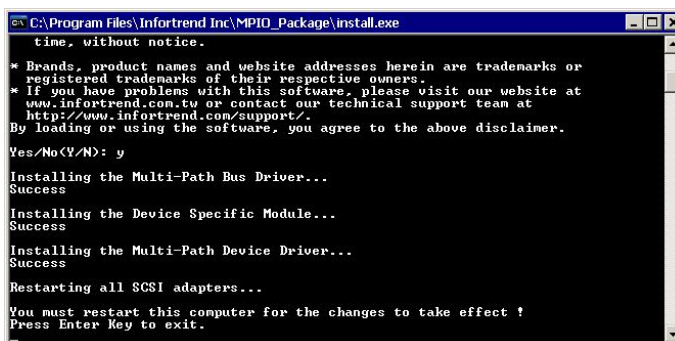


**Шаг 2.** Должен появиться индикатор загрузки и приглашение DOS.



**Шаг 3.** Нажмите **Y** для подтверждения прочтения соглашения.

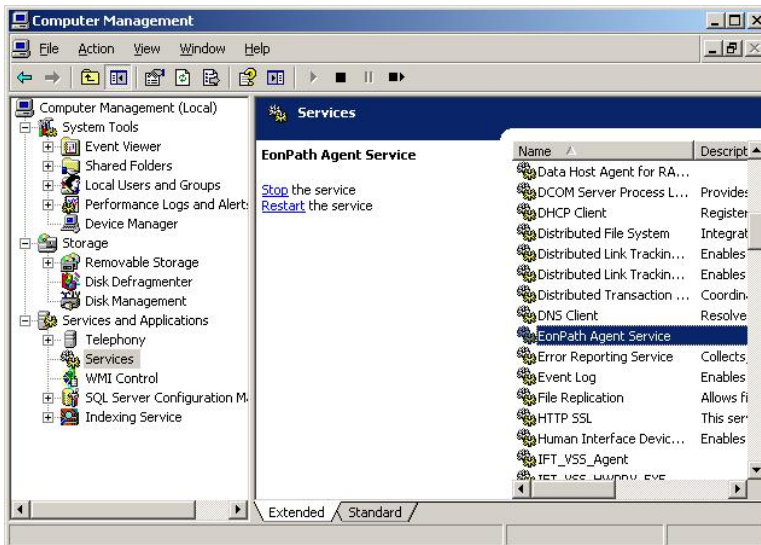
**Шаг 4.** После завершения установки нажмите Enter.



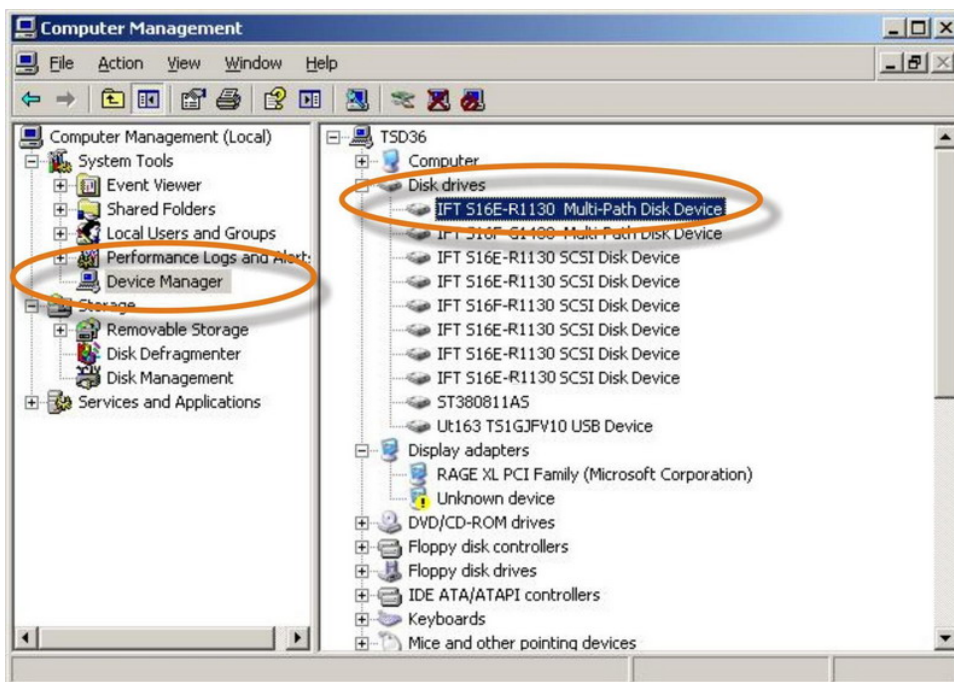
**Шаг 5.** Перегрузите ваш сервер, чтобы новая конфигурация вошла в силу.



**Шаг 6.** Вы можете проверить функционирование EonPath с помощью утилиты **Computer Management**, щелкнув правой кнопкой на иконке My Computer. Выберите **Manage**, затем **Services** из дерева меню.



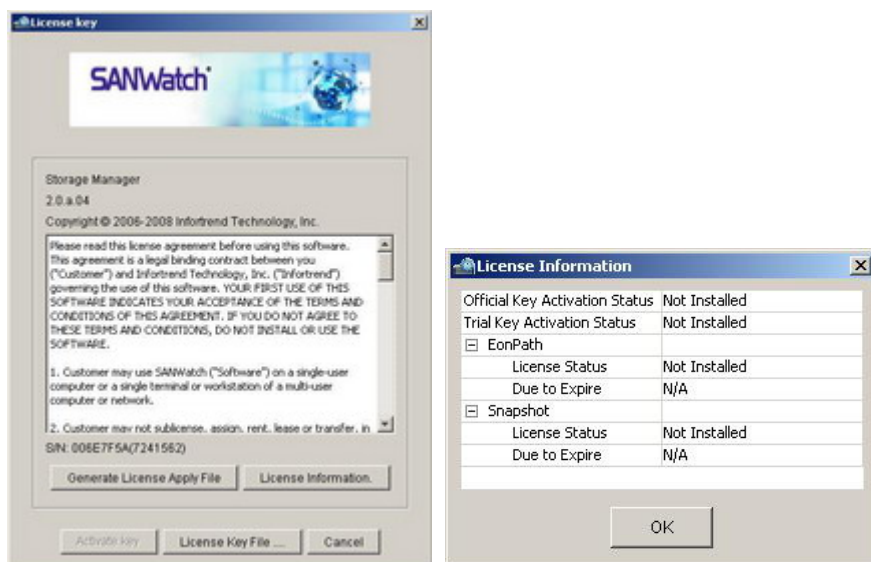
**Шаг 7.** Так как драйвер EonPath уже работает, вы можете видеть многоканальное устройство в **Device Manager -> Disk Drives**.



**Шаг 8.** После того, как вы увидели Multi-Path Disk Device, вы можете начать работу с томами данных на iSCSI системе хранения с избыточными контроллерами.

## ПРИМЕЧАНИЕ:

Установка может быть неудачной, если вы используете более ранние версии встроенного ПО, где лицензия EonPath не активирована. Почти все модели EonStor с ASIC400 поставляются с активированной лицензией. Вы можете проверить наличие ключей лицензии через меню программ SANWatch.



Если вы не обнаружите ключей лицензии EonPath, обратитесь в службу технической поддержки.

## 10. Настройка iSNS (дополнительно)

### Обзор iSNS

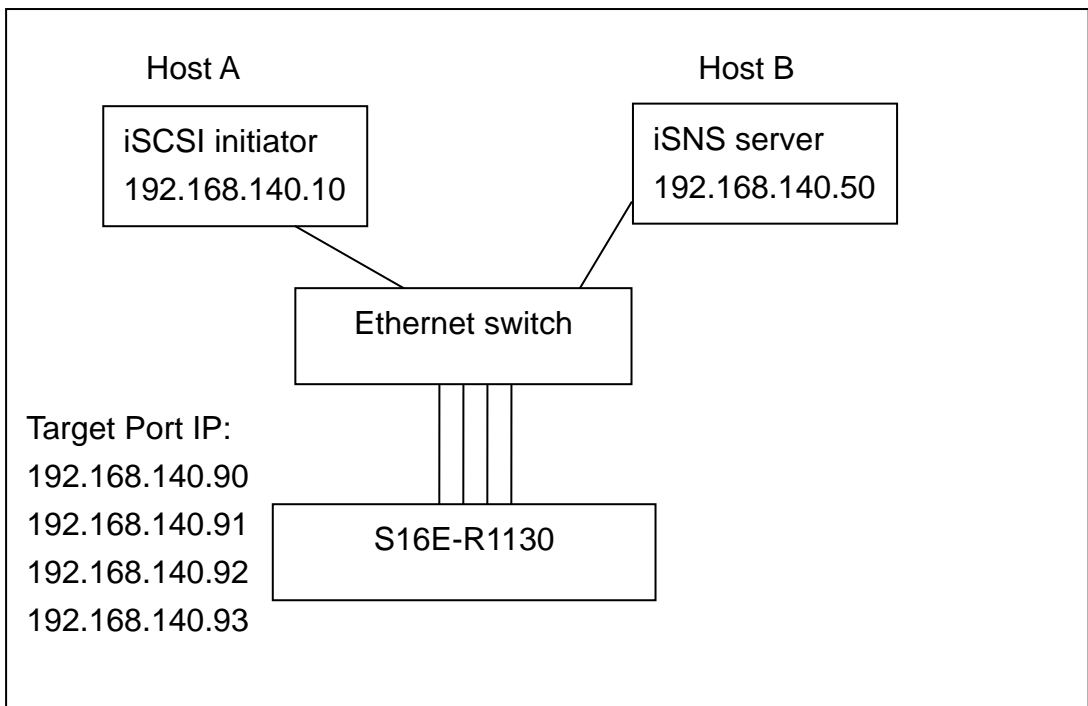
iSNS (Internet Storage Name Service) - это обычное средство для обнаружения, назначения имен и управления ресурсами для всех IP протоколов хранилищ данных. Реализация iSNS, принятая Infotrend, отвечает стандарту RFC 4171. iSNS обнаруживает iSCSI инициаторы и приемники в домене и собирает связанную с ними информацию. Windows iSNS server включен в Windows 2000 service pack 4 и Windows Server 2003.

- Функции iSNS могут быть заложены в IP свич, коммутатор, роутер, или сконцентрированы в iSNS сервере.
- Инициаторы должны запрашивать iSNS, чтобы идентифицировать потенциальные приемники.

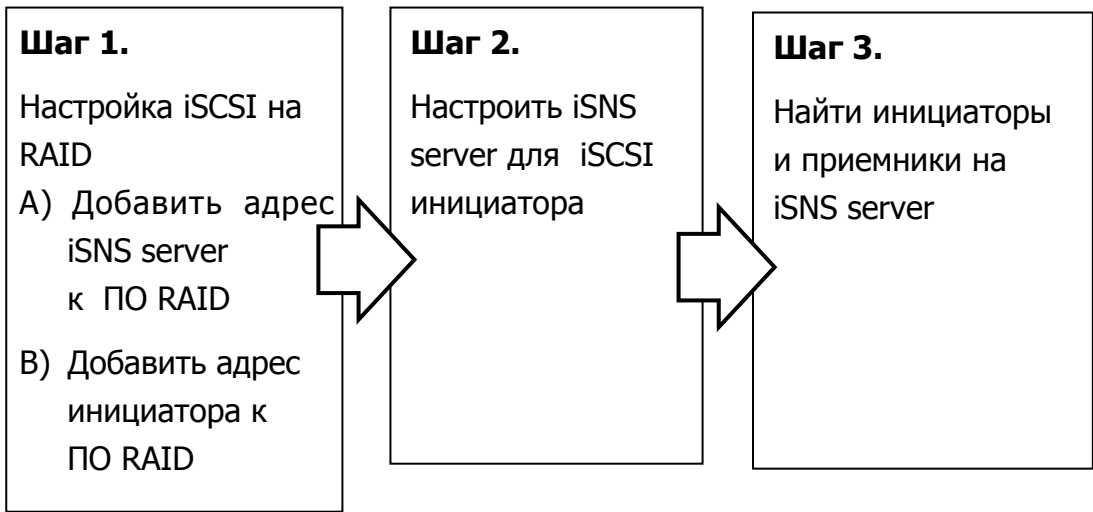


- Пример реализации iSNS - Microsoft's iSNS Server 3.0, который можно загрузить с сайта Microsoft:  
<http://www.microsoft.com/downloads/details.aspx?familyid=0dbc4af5-9410-4080-a545-f90b45650e20&displaylang=en>  
 iSNS сервер дает возможность обмена данными в домене, состоящем из инициаторов и приемников, в соответствии с установками пользователя.

**Пример iSNS конфигурации**

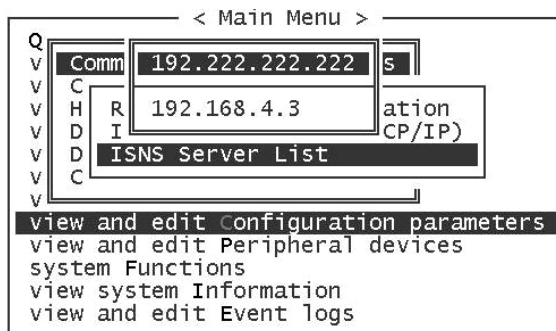


**Диаграмма настройки**

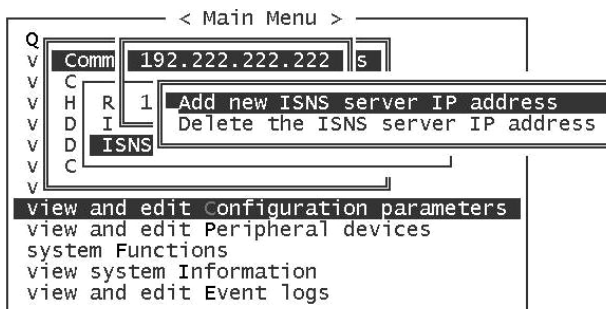


Опции iSNS service можно найти через "View and Edit Configuration Parameters" -> "Communication Parameters." Нажмите Enter на открывшемся или пустом поле, чтобы ввести резидентный IP адрес iSNS service.

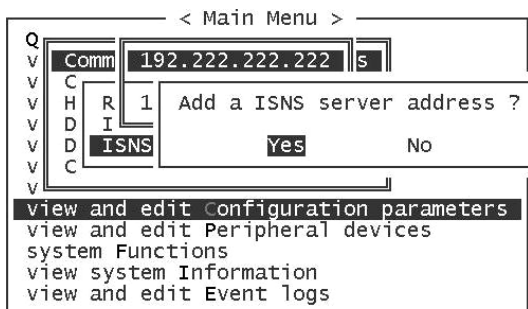
**Шаг 1.** Выделить список опций **iSNS Server List** в окне Communication Parameters. Нажать Enter на экране списка IP адресов.



**Шаг 2.** Выбрать **Add new iSNS server IP Address**.



**Шаг 3.** Выбрать Yes, затем ввести адрес iSNS server.



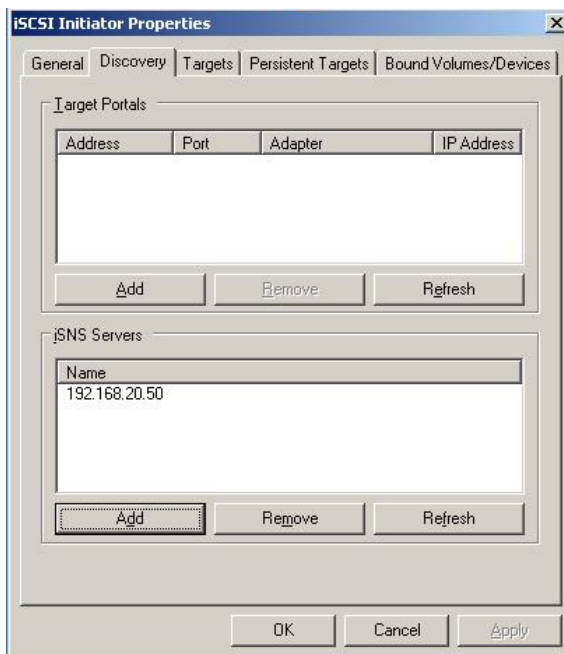
**Шаг 4.** После задания адреса iSNS server требуется перезагрузка системы.

Вы можете сделать это позже, после настройки остальных параметров iSCSI.

Изучите, пожалуйста, остальные разделы этой главы, чтобы выполнить настройки инициатора и связанные с этим настройки CHAP:

Процедура описана на примере Microsoft's iSCSI initiator.

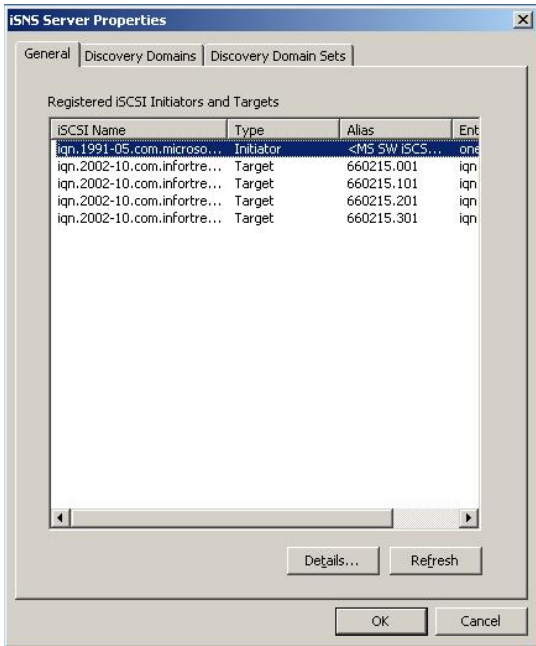
**Шаг 1.** Открыть iSCSI initiator, выделить поле iSNS server, щелкнув таблицу **Discovery**.



**Шаг 2.** Щелкнуть кнопку **Add**, чтобы ввести адрес. После того, как добавлен адрес iSNS server, вы можете проверить хост В (где установлен iSNS server). Если вы ранее сконфигурировали логические диски и подключили их к ID хоста, то LD-приемники появятся на экране настройки iSNS server.

Следует учесть, что iSNS server может потребовать несколько минут для обнаружения устройств в сети после начальной установки.

**Шаг 3.** Если приемники и инициаторы не появятся, попробуйте нажать кнопку **Refresh**.



**ПРИМЕЧАНИЕ:** Для установки и управления iSNS требуются права администратора. Неправильно установленный iSNS может, тем не менее, работать, однако функция сканирования и обнаружения устройств будет недоступна.

## 11. Настройка SLP (дополнительно)

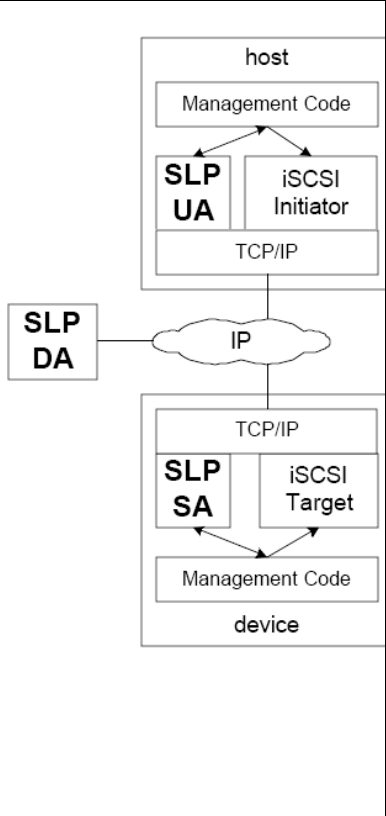
SLP (Service Location Protocol) поддерживается, начиная с rev. 3.63 встроенного ПО.

SLP полезен в случае:

- Если инициатор не имеет информации о приемнике.
- Если инициаторы могут слать групповые запросы обнаружения напрямую приемникам, либо отправлять их серверам.

■ Словарь SLP

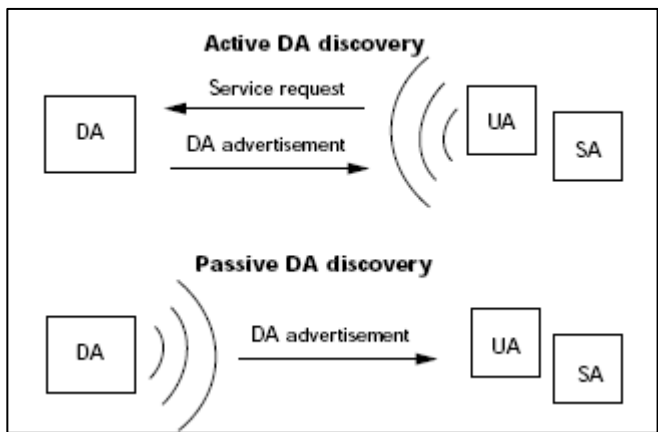
- Service Agent (SA)
  - **Advertises services**
  - **Services have attributes**
- User Agent (UA)
  - **Finds services**
  - **Zero configuration**



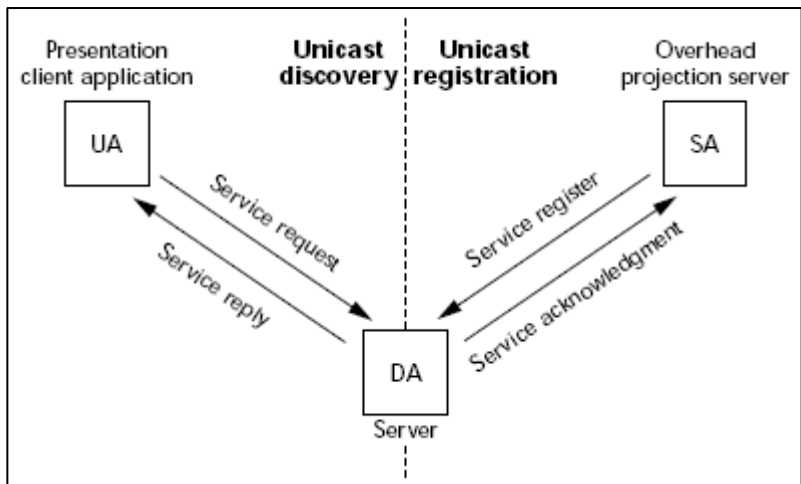
- Directory Agent (DA)
  - **Optional**
  - **Propagate service adverts**
- SLP Protocol
  - **UDP (default) or TCP**
  - **Minimize multicast**

Как это работает?

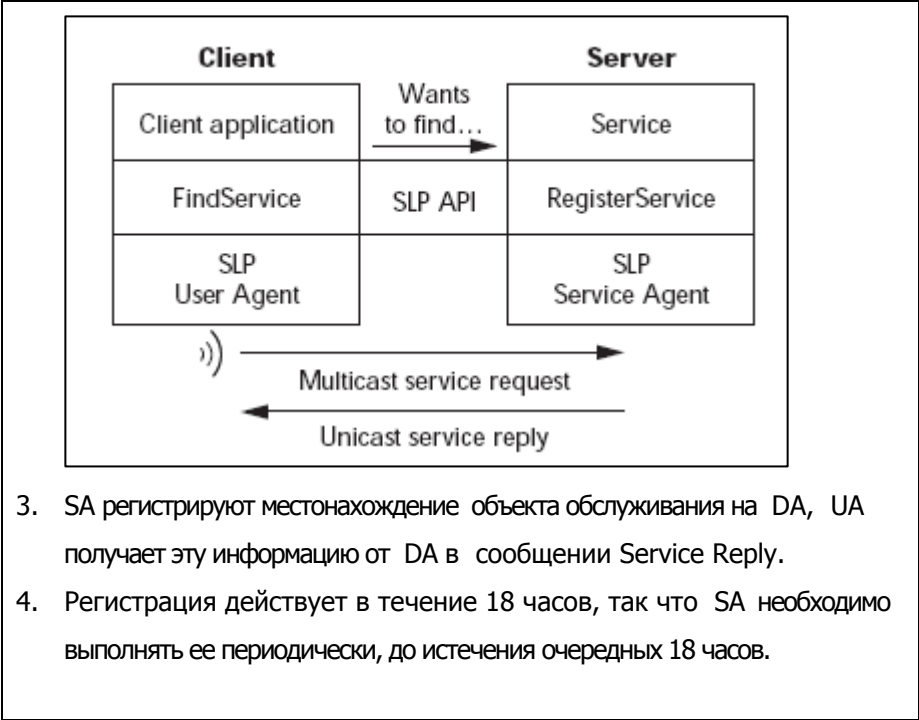
1. Вначале UA и SA определяют, имеются ли какие-либо DA в сети.



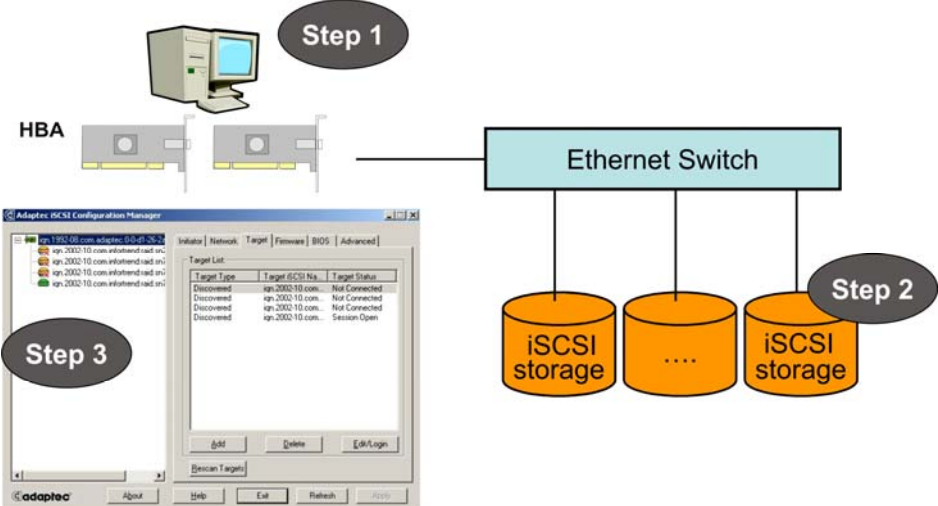
2. DA имеется, тогда он собирает всю информацию, выдаваемую SA, и UA посылают запросы к DA.



В случае отсутствия DA UA по очереди рассылают тот же запрос, который в противном случае отправляется только к DA. SA принимают эти групповые запросы и отвечают UA, если запрос на обслуживание относится к ним).



3. SA регистрируют местонахождение объекта обслуживания на DA, UA получает эту информацию от DA в сообщении Service Reply.
4. Регистрация действует в течение 18 часов, так что SA необходимо выполнять ее периодически, до истечения очередных 18 часов.

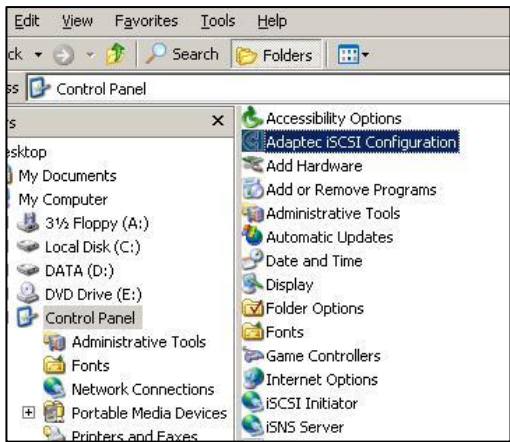


- Шаг 1. Установить Install iSCSI HBA, которые поддерживают SLP, например, Adaptec TOE.
- Шаг 2. Выполнить настройки iSCSI на хранилище.
  - 2-1. Подключить логические диски к хосту.
  - 2-2. Применить LUN Masking, если имеются требования по безопасности.
  - 2-3. Добавить инициаторы к вашему списку, хранящемуся во встроенном ПО.

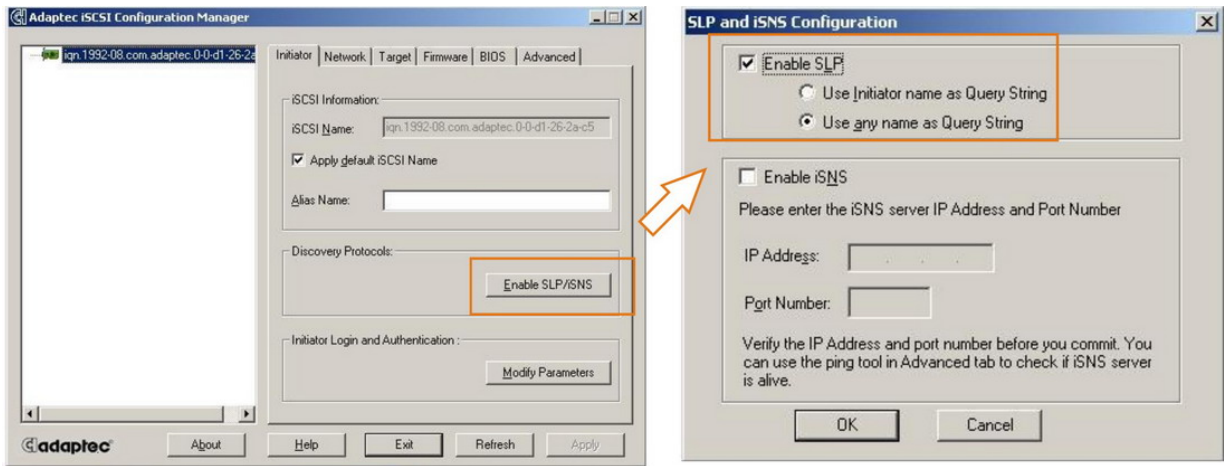


Шаг 3. Настройте iSCSI HBA на хосте.

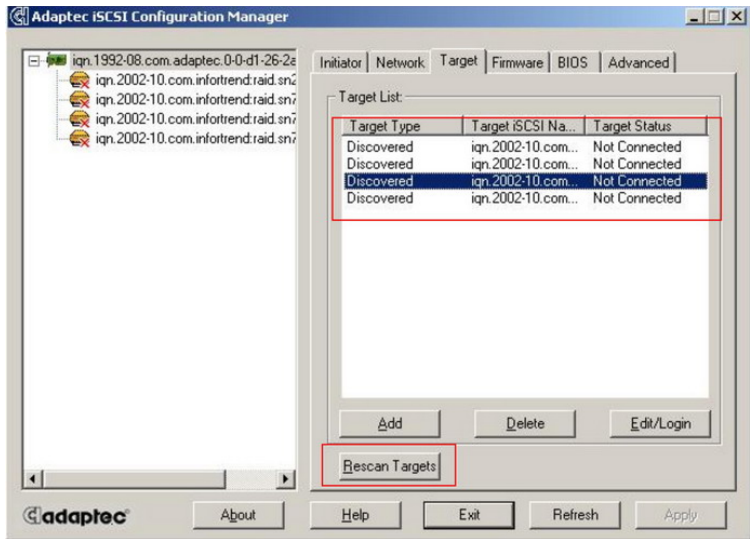
3-1. После успешной установки программы настройки HBA должны быть доступны ОС.



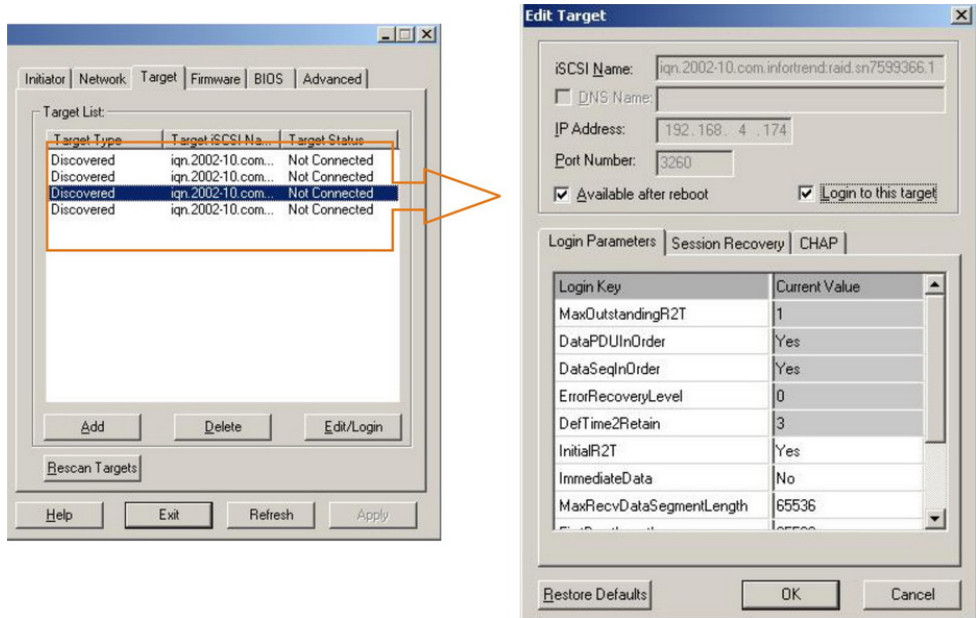
3-2. Разрешите SLP



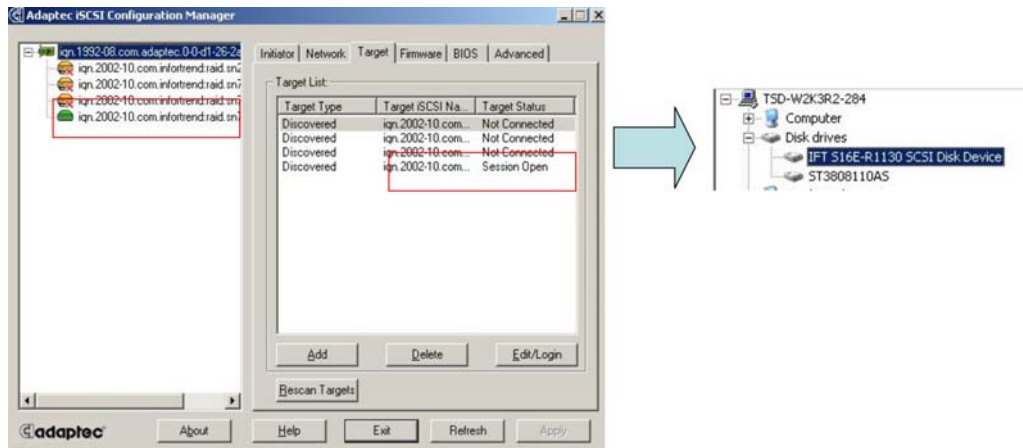
3-3. Через некоторое время iSCSI приемники должны появиться в таблице Target, в противном случае следует воспользоваться кнопкой Rescan Targets.



3-4. Активируйте доступ к приеникам (logging in) и примените идентификацию CHAP, если хотите.



3-5. Проверьте состояние iSCSI сеанса и завершите процедуру инициализации диска.





## 12. Jumbo Frame

```

      < Main Menu >
Quick
view Maximum Queued I/O Count - 256 (Default)
view LUNs per Host SCSI ID - 8 (Default)
view Max Number of Concurrent Host-LUN Connection - 4 (Default)
view Number of Tags Reserved for each Host-LUN Connection - 32 (Default)
view Peripheral Device Type Parameters
view Cylinder - Variable / Head - Variable / Sector - Variable
view Login Authentication with CHAP - Disable
view Jumbo Frames - Enable
V
S
V
V
C
Host-side Parameters
Drive-side Parameters
Disk Array Parameters
Controller Parameters
  
```

Arrow Keys:Move Cursor    Enter:Select    Esc:Exit    Ctrl+L:Refresh Screen

Jumbo Frames расширяет Ethernet пакеты, так что хост обрабатывает меньшее количество пакетов. Большинство современных адаптеров Gigabit Ethernet поддерживают режим jumbo frames, что позволяет хосту увеличить MTU (Maximum Transfer Unit) для передаваемых пакетов. По умолчанию это 9014 байтов.



### ВНИМАНИЕ!

Функция Jumbo Frame требует, чтобы все оконечные устройства в iSCSI сети тоже поддерживали функцию Jumbo Frame, и чтобы она была активирована. Обратите также внимание на настройку MTU для Jumbo Frame в этих устройствах.