**Протоколы и функции, обеспечивающие работу сети**

**Маршрутизация**

Маршрутизация осуществляется на сетевом уровне OSI, который отвечает за обеспечение связи между любыми хостами в сети. Маршрутизирующие устройства (например, Интернет-маршрутизаторы или межсетевые экраны) объединяют отдельные сети в общую составную сеть. В сложных составных сетях почти всегда существует несколько альтернативных маршрутов для передачи пакетов между конечными хостами. Задачу выбора маршрутов из нескольких возможных решают маршрутизирующие устройства. Правильно выбранная структура сети и настроенная в соответствии с ней маршрутизация гарантируют, что отправленный по сети пакет будет доставлен по назначению.

Что же такое "маршрутизация"?

***Маршрутизация (Routing)*** – процесс определения в коммуникационной сети (наилучшего) пути, по которому пакет может достигнуть адресата или, точнее – это набор правил, определяющих маршрут следования информации в сетях связи. Любые сетевые пакеты направляются в соответствии с набором правил – таблиц маршрутизации. Как правило, маршрутизация сводится к выбору интерфейса и следующего транзитного хоста при следовании пакета между сетями.

***Маршрут*** – это путь, который должен пройти пакет от отправителя до точки назначения через маршрутизирующие устройства.

Маршрутизирующее устройство выбирает маршрут на основании информации о текущей конфигурации сети и соответствующего критерия выбора маршрута. Обычно в качестве критерия выступает ***метрика***, которая отражает приоритет маршрута (наилучший маршрут). При определении наилучшего маршрута и назначения метрики рассматриваются следующие характеристики: время прохождения маршрута, которое в локальных сетях совпадает с длиной маршрута, измеряемой в количестве пройденных узлов маршрутизации; надежность и пропускная способность канала связи; время передачи пакета по каждой линии связи; нагрузка сетевого ресурса.

Маршрутизация может осуществляться статическим или динамическим способом.

Алгоритмы статической маршрутизации представляют таблицы, составленные сетевым администратором. Содержимое этих таблиц может быть изменено только сетевым администратором.

Итак, ***статическая маршрутизация***(Static routing) – это метод маршрутизации в сетях с коммутацией пакетов, при котором данные передаются по заданному пути. При конфигурировании таблиц маршрутизации должны быть указаны все взаимосвязи между логическими сетями, которые остаются неизменными.

Динамическая маршрутизация предполагает, что маршрутизирующее устройство может автоматически определять новые пути либо модифицировать информацию о существующих путях.

***Динамическая маршрутизация***(Dynamic routing) – это метод выбора маршрута в сетях с коммутацией каналов, учитывающий динамическое состояние выходных каналов хоста (локальная маршрутизация) или сети (глобальная маршрутизация). Алгоритмы динамической маршрутизации адаптируются к изменениям сетевой обстановки, анализируя поступающие сообщения об обновлении маршрутов и используя при этом протоколы маршрутизации такие, как RIP (Routing Information Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol).

Осуществление маршрутизации в межсетевых экранах D-Link рассмотрено в разделе "Создание и проверка правил маршрутизации" приложения D "Управление межсетевыми экранами через Web-интерфейс".

Маршрутизация осуществляется, используя IP-адресацию сетей и сетевых устройств. В версии IPv4 IP-адрес представляет собой 32-битное двоичное число, состоит из 4-х октетов и в десятичном виде записывается в виде четырех чисел, разделенных точками (например: 192.168.1.1). Существует также понятие "маска подсети". В десятичном представлении она имеет такой же вид, как и IP-адрес. Маска определяет, какая часть IP-адреса узла сети относится к адресу сети, а какая – к адресу самого узла в этой сети.

В версии IPv6 IP-адрес имеет 128-битное представление, состоит из 8 октетов, разделяющихся двоеточиями и записывается с использованием шестнадцатеричных чисел (например: *СА81:0:0:0:800:800С:121:1Б*).

**Протокол OSPF**

***OSPF*** (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Последняя версия протокола представлена в RFC 2328. OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol – IGP), распространяет информацию о доступных маршрутах между маршрутизирующими устройствами (маршрутизаторами) одной автономной системы.

OSPF предлагает решение следующих задач:

* увеличение скорости сходимости сети (т.е. одинаковое понимание текущей сетевой топологии всеми маршрутизаторами) по сравнению с протоколом RIP;
* поддержка сетевых масок переменной длины (VLSM, применяются в бессклассовой IP-адресации);
* достижимость сети;
* оптимальное использование пропускной способности сети;
* определение кратчайшего маршрута.

**Терминология протокола OSPF**

***Объявление о состоянии канала*** (Link-State Advertisement, LSA) – объявление описывает все каналы маршрутизатора, все интерфейсы и состояние каналов.

***Состояние канала*** (Link state) – состояние канала между двумя маршрутизаторами; обновления происходят при помощи пакетов LSA.

***Метрика*** (metric) – условный показатель "стоимости" пересылки данных по каналу;

***Автономная система*** (Autonomous System, AS) – группа устройств, обменивающаяся маршрутизирующей информацией в соответствии с единой политикой и протоколом маршрутизации.

***Зона***(area) – совокупность сетей и маршрутизаторов, имеющих один и тот же идентификатор зоны.

***Соседи*** (neighbours) – два маршрутизатора, имеющие интерфейсы в общей сети.

***Состояние соседства***(adjacency) – взаимосвязь между определенными соседними маршрутизаторами, установленная с целью обмена информацией маршрутизации.

***Hello-пакеты*** (Hello packets) – используются для обмена информации и поддержания соседских отношений.

***База данных соседей*** (Neighbours database) – список всех соседей.

***База данных состояния каналов*** (Link State Database, LSDB) – список всех записей о состоянии каналов. Встречается также термин топологическая база данных (topological database), употребляется как синоним базы данных состояния каналов.

***Идентификатор маршрутизатора*** (Router ID, RID) – уникальное 32-битовое число, которое уникально идентифицирует маршрутизатор в пределах одной автономной системы.

***Выделенный маршрутизатор*** (Designated Router, DR) – управляет процессом рассылки LSA в сети. Каждый маршрутизатор сети устанавливает отношения соседства с DR и отправляет ему информацию об изменениях в сети, а DR отвечает за то, чтобы данная информация была отправлена остальным маршрутизаторам сети. Недостатком в схеме работы с DR маршрутизатором является то, что при выходе его из строя должен быть выбран новый DR. Новые отношения соседства должны быть сформированы и, пока базы данных маршрутизаторов не синхронизируются с базой данных нового DR, сеть будет недоступна для пересылки пакетов. Для устранения этого недостатка выбирается BDR.

***Резервный выделенный маршрутизатор*** (Backup Designated Router, BDR). Каждый маршрутизатор сети устанавливает отношения соседства не только с DR, но и BDR. DR и BDR также устанавливают отношения соседства между собой. При выходе из строя DR, BDR становится выделенным маршрутизатором и выполняет все его функции. Так как маршрутизаторы сети устанавливают отношения соседства с BDR, то время недоступности сети минимизируется.

**Краткое описание работы протокола OSPF**

Маршрутизаторы обмениваются hello-пакетами через все интерфейсы, на которых активирован OSPF. Устройства, разделяющие общий канал передачи данных, становятся соседями после согласования определенных параметров, указанных в hello-пакетах.

Далее маршрутизаторы обмениваются hello-пакетами с устройствами других сетей для установления соседства. OSPF определяет несколько типов сетей и несколько типов маршрутизаторов. Пара маршрутизаторов, находящихся в состоянии соседства синхронизирует между собой базу данных состояния каналов.

Каждый маршрутизатор посылает объявление о состоянии канала своему соседу. Последний, получив объявление, записывает передаваемую в нем информацию в базу данных состояния каналов маршрутизатора и рассылает копию объявления всем другим своим соседям.

Рассылая объявления через зону, все маршрутизаторы строят идентичную базу данных состояния каналов маршрутизатора.

Когда база данных построена, каждый маршрутизатор использует алгоритм нахождения кратчайшего пути для вычисления графа без образования петель (т.е. дерева кратчайшего пути), который будет описывать кратчайший маршрут к каждому известному пункту назначения, отображая в качестве корня самого себя. Самый короткий путь в дереве соответствует оптимальному маршруту к каждой сети назначения в автономной системе.

Каждый маршрутизатор строит таблицу маршрутизации из своего дерева кратчайшего пути и отправляет соседям не все записи таблицы, а только обновленные и измененные данные о маршрутах.

Учитывая, что в сетях с множественным доступом отношения соседства должны быть установлены между всеми маршрутизаторами, существует проблема рассылки огромного количества копий LSA. Для предотвращения этой проблемы в сетях выбираются выделенный (DR) и резервный выделенный (BDR) маршрутизаторы.

**Типы зон**

При разделении автономной системы на зоны, маршрутизаторам, принадлежащим к одной зоне, не известна информация о детальной топологии других зон.

Разделение на зоны позволяет:

* снизить нагрузку на ЦПУ маршрутизаторов за счет уменьшения количества перерасчетов по алгоритму SPF;
* уменьшить размер таблиц маршрутизации;
* уменьшить количество пакетов обновлений состояния канала.

Каждой зоне присваивается *идентификатор зоны* (Area ID) и может быть указан в десятичном формате или в формате записи IP-адреса. Однако идентификаторы зон не являются IP-адресами и могут совпадать с любым назначенным IP-адресом.

В любых OSPF-сетях обязательно должна быть определена магистральная зона (Backbone area), известная также как нулевая зона (Area 0) или зона 0.0.0.0, которая формирует ядро сети OSPF. Все остальные зоны должны быть соединены с ней при помощи маршрутизатора, через который обеспечивается межзональная маршрутизация. Если область не связана физически с магистралью, то необходимо добавить виртуальное соединение.

***Тупиковая зона*** (Stub area) не принимает информацию о внешних маршрутах для автономной системы, а объявляет о маршруте по умолчанию. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию.

***Транзитная зона*** (Transit area) передает информацию из зон, не связанных непосредственно с магистральной зоной.

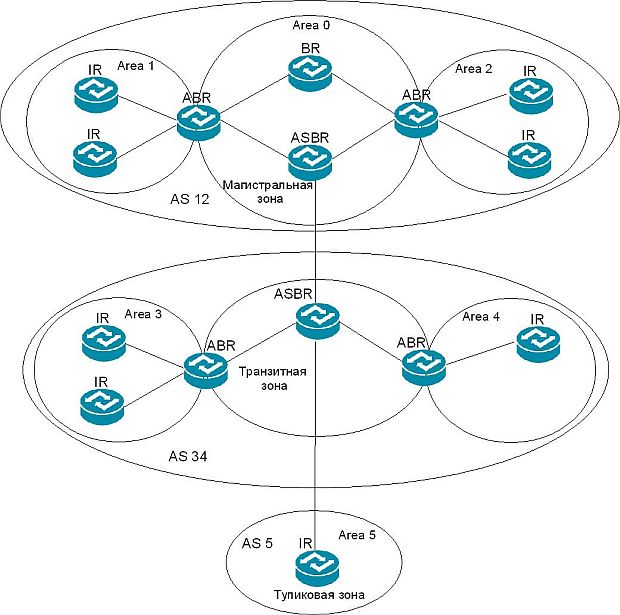
**Типы маршрутизаторов**

Все интерфейсы ***внутреннего маршрутизатора*** (Internal Router, IR) принадлежат одной зоне. У таких маршрутизаторов только одна база данных состояния каналов.

***Граничный маршрутизатор*** (Area Border Router, ABR) соединяет одну или больше зон с магистральной зоной и выполняет функции шлюза для межзонального трафика. У граничного маршрутизатора всегда хотя бы один интерфейс принадлежит магистральной зоне. Для каждой присоединенной зоны маршрутизатор поддерживает отдельную базу данных состояния каналов.

***Граничный маршрутизатор автономной системы*** (AS Boundary Router, ASBR) обменивается информацией с маршрутизаторами других автономных систем. ASBR может находиться в любом месте автономной системы и быть внутренним, граничным или магистральным маршрутизатором.

***Магистральный маршрутизатор*** (Backbone Router, BR) используется в магистральной зоне.

[](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_1.jpg)

[увеличить изображение](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_1.jpg)  
**Рис. 4.1.**Сеть OSPF

OSPF поддерживает следующие методы аутентификации:

* **0** (в межсетевых экранах NetDefend: No Authentification) – для обмена информацией не требуется аутентификация OSPF;
* **1** (в межсетевых экранах NetDefend: Passphrase) – для аутентификации OSPF требуется простой пароль;
* **2** (в межсетевых экранах NetDefend: MD5 Digest) – MD5-аутентификация содержит идентификатор ключа (key ID) и 128-битный ключ. Определенный ключ используется для создания 128-бит MD5-хэша. Но назначение аутентификации не означает, что OSPF-пакеты шифруются. В случае необходимости передачи шифрованного OSPF-трафика, его направляют через VPN-туннель (например, IPSec

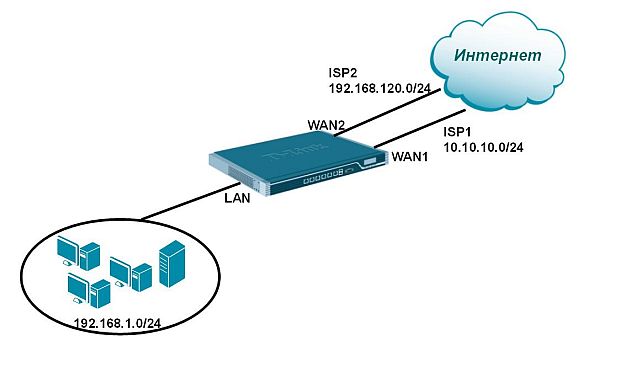
**Резервирование маршрутов (Route Failover)**

При подключении корпоративной сети ко второму провайдеру рано или поздно возникает вопрос обеспечения рационального использования двух Интернет-каналов и возможность автоматического резервирования, чтобы работоспособность сети быстро восстанавливалась при возникновении проблем на одном из каналов.

Основные задачи, которые можно решить при использовании резервирования каналов в сеть Интернет:

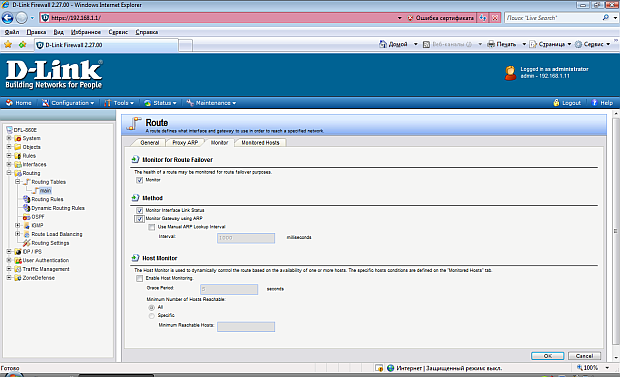
* перенаправление трафика при обрыве одного из каналов;
* направление чувствительного к задержкам трафика в более "быстрый" канал, в то время как остальной трафик, не критичный к скорости доставки пакетов, заворачивать в "медленный", но более дешёвый канал;
* переключение на более дорогой канал только на время проблем с дешёвым каналом.

Для таких ситуаций в межсетевых экранах D-Link серии NetDefend предусмотрена возможность переключения маршрутов при отказе (Route Failover): в случае отказа одного из маршрутов трафик автоматически начинает передаваться по другому, резервному маршруту. Система NetDefendOS выявляет неудачные маршруты, используя при этом функцию мониторинга маршрутов *Route Monitoring*, и перенаправляет трафик на резервный маршрут.

[](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_9.jpg)

[увеличить изображение](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_9.jpg)  
**Рис. 4.9.**Резервирование каналов

Выполнение данной задачи с использованием межсетевых экранов NetDefend заключается в активировании опции *Monitor for Route Failover*:

[](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_10.png)

[увеличить изображение](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_10.png)  
**Рис. 4.10.**Использование функции мониторинга маршрутов (Route Monitoring) при резервировании каналов в межсетевых экранах NetDefend

В сценарии с основным (предпочтительным) и резервным маршрутами в основной маршрут добавляется *Route Monitoring*. В резервном маршруте данная опция не указывается, если не требуется переключения при отказе (failover). Когда Route Monitoring для маршрута включен, нужно выбрать один из следующих методов контроля:

* **Monitor Interface Link Status** – cистемой NetDefendOS контролируется состояние подключения интерфейса, определенного для маршрута. Маршрут считается активным, пока существует физическое подключение интерфейса. Этот метод обеспечивает самый быстрый анализ маршрута, так как сразу обнаруживаются любые изменения состояния соединений.
* **Monitor Gateway using ARP** – при мониторинге шлюза как следующего сегмента (или как еще называют – next-hop) маршрута его доступность определяется при помощи ARP-запросов. До тех пор, пока шлюз отвечает на эти запросы, маршрут функционирует нормально.

Следует заметить, что функцию Route Monitoring нельзя применять для автоматически созданных маршрутов, так как им присвоен специальный статус, и обращение к ним происходит по-другому. К таким маршрутам относятся маршруты, автоматически создаваемые для физических интерфейсов при запуске системы NetDefendOS. Если же данным маршрутам требуется активировать Route Monitoring, то их необходимо сначала удалить, а затем добавить вручную, как новые маршруты.

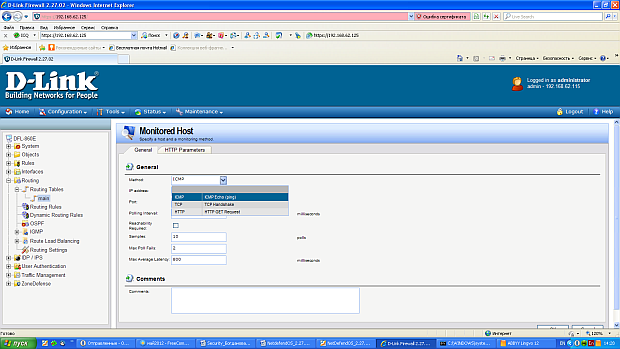
При определении маршрута необходимо установить метрику (metric) маршрута. Метрика – это целое положительное число, которое указывает на приоритет маршрута. При наличии двух маршрутов для одного и того же адреса назначения система NetDefendOS выберет маршрут с минимальным значением метрики.

ВНИМАНИЕ: приоритет основного подключения должен быть выше (т.е. значение метрики – меньше), чем у резервного подключения.

Дополнительная функция системы NetDefendOS *Host Monitoring* ([рис. 4.10](https://www.intuit.ru/studies/courses/16655/1300/lecture/25507?page=4#image.4.10)) обеспечивает гибкий и легко конфигурируемый способ контроля целостности маршрута. Данный метод позволяет межсетевому экрану посылать запрос одному или нескольким внешним узлам о доступности конкретного маршрута.

Довольно часто встречаются ситуации, когда канал работоспособен и шлюз доступен, но соединений нет, т.к. проблема возникла дальше, за шлюзом. Чтобы произошло переключение с маршрута первого выбора на резервный, предусмотрен механизм ICMP- /TCP- /HTTP-мониторинга, позволяющий осуществлять контроль за работоспособностью определенных хостов ([рис. 4.11](https://www.intuit.ru/studies/courses/16655/1300/lecture/25507?page=4#image.4.11)), которым назначена функция *Host Monitoring*. Межсетевые экраны NetDefend позволяют выбрать для конкретного маршрута один из методов мониторинга:

* **ICMP** – ICMP-запрос "ping". Для данного метода должен быть определен IP-адрес.
* **TCP** – TCP-соединение для хоста устанавливается и разъединяется. Для данного метода должен быть определен IP-адрес и порт.
* **HTTP** – запросы HTTP-сервера с использованием URL. Должны быть определены URL-адрес (во вкладке HTTP Parameters) и строковая переменная типа string, которая содержит начало или полный текст корректного ответа Web-сервера. Даже если такая величина не определена, любой ответ сервера будет считаться корректным.

[](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_11.png)

[увеличить изображение](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_11.png)  
**Рис. 4.11.**Назначение параметров при мониторинге хоста для резервирования маршрутов

**Балансировка нагрузки сети**

В терминологии компьютерных сетей ***балансировка (выравнивание) нагрузки***– распределение процесса выполнения заданий между несколькими серверами сети с целью оптимизации использования ресурсов и сокращения времени вычисления.

Типы серверов, которые должны быть сбалансированы:

* серверные кластеры;
* межсетевые экраны;
* серверы инспектирования содержания (такие как AntiVirus- или AntiSpam- серверы).

Обычно системы балансировки загрузки серверов используют возможности уровня L4 (UDP/TCP). При этом контролируется доступность сервера по IP-адресу и номеру порта и принимается решение: какому из доступных серверов следует переслать запрос. Наиболее часто для выбора сервера используется карусельный алгоритм (round-robin). В этом варианте предполагается, что все запросы создают одинаковую загрузку и длительность исполнения. В более продвинутых вариантах алгоритма используется уровень занятости сервера и число активных соединений.

Раньше возможности балансировки нагрузки встраивались в саму прикладную программу или операционную систему. Современные системы балансировки нагрузки должны удовлетворять следующим требованиям:

* обеспечивать управление трафиком, чтобы гарантировать доступность приложения и распределение нагрузки в условиях фермы серверов (группа серверов, соединенных сетью передачи данных и работающих как единое целое);
* ускорять выполнение приложений в несколько раз;
* гарантировать защиту приложений, сохранность данных и обеспечение мониторинга трафика.

Здесь важно учитывать, что доступность IP-адреса и порта еще не гарантирует доступа к приложению.

В последнее время для решения задачи балансировки нагрузки все чаще используется прикладной уровень. При этом в процессе принятия решения учитывается тип клиента, запрашиваемый URL, информация из cookie, возможности конкретного сервера и тип прикладной программы, что позволяет оптимизировать использование ресурсов системы.

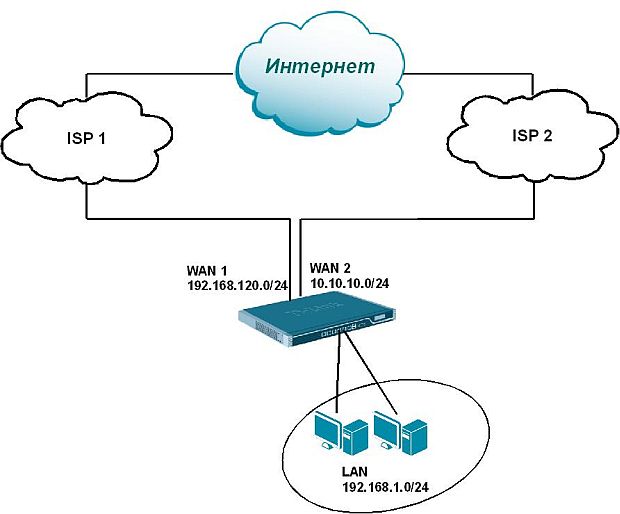
Довольно существенные преимущества может предоставить система GSLB (Global Server Load Balancing), которая способна решать задачу балансировки для произвольно расположенных ферм серверов с учетом их удаленности от клиента. Эта система может поддерживать несколько разных алгоритмов распределения нагрузки и обеспечивать оптимальное обслуживание клиентов, разбросанных по всему миру. Для администраторов система дает возможность формирования гибкой политики управления ресурсами.

Одним из способов ускорения обслуживания является кэширование. В случае хорошо сконфигурированного кэша доля запросов, удовлетворяемых кэшем, может достигать 40%. При этом ускорение обслуживания может быть улучшено в 30 раз.

Еще одним методом ускорения обслуживания может служить архивация данных, так как в этом варианте понижается уровень перегрузки каналов сети.

Управление балансировкой нагрузки можно совместить с функцией прикладного межсетевого экрана (70% успешных вторжений использует уязвимости приложений) и с использованием SSL по VPN-туннелю. SSL – Secure Sockets Layer – криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером.

Для достижения максимальной пропускной способности и отказоустойчивости межсетевые экраны позволяют распределить или сбалансировать нагрузку, используя все имеющиеся каналы Интернета (серверов) одновременно. Например, можно избежать такой ситуации, когда передаваемые по сети пакеты идут через одного провайдера, в то время как выход в Интернет через другого провайдера простаивает без дела. Или распределить сервисы и направить трафик через все имеющиеся Интернет-каналы. Возможна настройка балансировки нагрузки, если соединения с провайдерами осуществляются с разными типами подключения (Static IP, PPPoE, PPTP/L2TP), а также – для балансировки трафика, проходящего через VPN-туннели, установленные на разных физических интерфейсах.

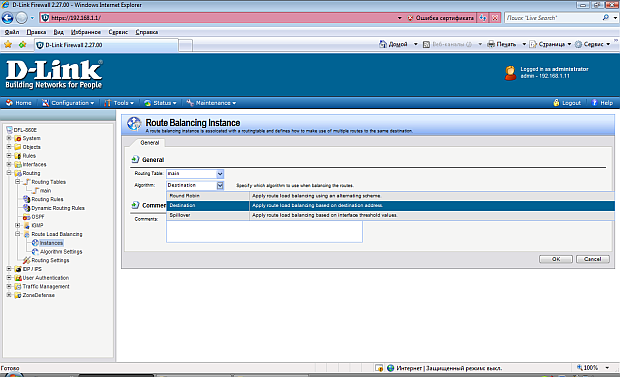
[](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_12.jpg)

[увеличить изображение](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_12.jpg)  
**Рис. 4.12.**Балансировка нагрузки по нескольким маршрутам

В межсетевых экранах D-Link серии NetDefend предусмотрена функция, предназначенная для балансировки сетевой нагрузки по разным маршрутам – *Route Load Balancing (RLB)*, возможности которой обеспечивают:

* балансировку трафика между интерфейсами на основе политик;
* балансировку нагрузки трафика при одновременном множественном доступе в Интернет, пользуясь услугами двух и более провайдеров;
* балансировку трафика, проходящего через VPN-туннели, установленные на разных физических интерфейсах.

Функция балансировки нагрузки в межсетевых экранах NetDefend активируется на основе таблицы маршрутизации путем создания объекта RLB *Instance*, в котором определены два параметра: таблица маршрутизации и RLB-алгоритм. С таблицей маршрутизации может быть связан только один объект Instance.

[](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_13.png)

[увеличить изображение](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_13.png)  
**Рис. 4.13.**Выбор алгоритма распределения нагрузки в межсетевых экранах NetDefend

Есть возможность выбрать один из алгоритмов распределения нагрузки между Интернет-интерфейсами:

* Алгоритм **Round Robin** распределяет нагрузку между интерфейсами WAN1 и WAN2 последовательно (поочередно). Каждый раз, когда возникает новая исходящая сессия с интерфейса LAN, выбирается интерфейс WAN1 или WAN2 для отправки пакетов. В дальнейшем, пакеты данной сессии будут использовать ранее определенный WAN-интерфейс. TCP-сессия открывается и закрывается на одном и том же WAN-интерфейсе.
* Алгоритм **Destination** позволит избежать проблем с некоторыми протоколами при использовании балансировки, например FTP. Данный алгоритм работает аналогично алгоритму Round Robin, за исключением того, что все данные к удаленному хосту идут через тот интерфейс, через который соединение было установлено.
* Значение **Spillover** определяет предельное значение нагрузки для основного WAN-порта (**Routing → Route Load Balancing > Algoritm Setings**) . При достижении этой нагрузки за указанный период начнет использоваться второй WAN-порт (для новых сессий). Как только загрузка основного канала упадет, новые сессии будут открываться на нем.

**Использование метрик маршрута с алгоритмом Round Robin**

Метрика каждого маршрута по умолчанию равна нулю. При использовании взаимосвязанных алгоритмов *Round Robin* и *Destination* можно устанавливать разные значения метрик, позволяющие создать приоритет выбора маршрутов. Маршруты с минимальным значением метрики будут выбираться чаще, чем маршруты с более высоким значением.

Если в сценарии с двумя Интернет-провайдерами (часто встречается выражение "ISP-провайдер", т.е. Internet Service Provider) требуется, чтобы большая часть трафика проходила через одно из ISP-подключений, то следует активировать RLB и назначить меньшее значение метрики для маршрута основного ISP-подключения (например, 90) относительно второго (например, 100).

Если задача заключается в равномерной балансировке трафика между двумя Интернет-провайдерами, то значение метрик для обоих маршрутов следует назначать одинаковое.

**Использование метрик маршрута с алгоритмом Spillover**

При использовании алгоритма *Spillover* для каждого маршрута обязательно должна быть определена метрика. В этом случае система NetDefendOS всегда выбирает маршрут с самым низким значением метрики. *Алгоритм не предназначен для работы с одинаковыми метрическими значениями маршрутов, поэтому администратору следует устанавливать различные значения метрик для всех маршрутов, к которым применяется алгоритм Spillover*.

Значение метрики определяет порядок, в соответствии с которым трафик перенаправляется на другой маршрут после того, как для выбранного маршрута превышено допустимое значение передаваемого трафика.

Можно создать несколько альтернативных маршрутов с различными метрическими значениями, для каждого из которых определена пороговая величина настроек алгоритма – *Spillover Setting* – для каждого интерфейса. Сначала выбирается маршрут с минимальной метрикой; после того как превышен допустимый порог настроек алгоритма, будет выбран следующий маршрут.

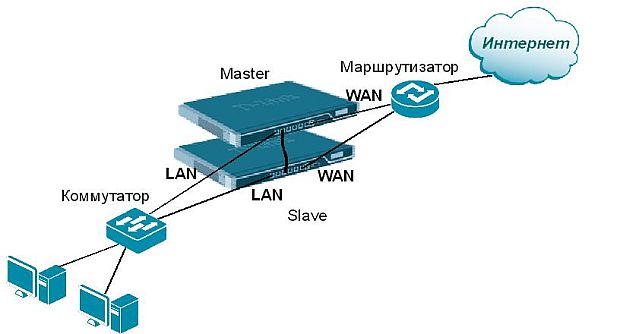
Если на всех альтернативных маршрутах достигнуты пороговые значения Spillover Setting, то маршрут не меняется.

**ВНИМАНИЕ**: значение метрики на интерфейсах (маршрутах), которые используются в балансировке, должно быть установлено выше, чем для остальных интерфейсов (маршрутов). Чем ниже значение метрики на интерфейсе (маршруте), тем чаще этот интерфейс (маршрут) будет использован для установки соединения, относительно интерфейса (маршрута) с большим значением метрики. Доля использования интерфейсов (маршрутов) будет пропорциональна разнице между значениями метрик на этих интерфейсах (маршрутах).

**Балансировка нагрузки сети и НА-кластеризация (резервирование устройств) межсетевых экранов NetDefend**

Высокий уровень сетевой отказоустойчивости достигается за счет использования двух межсетевых экранов NetDefend: основного устройства (master) и резервного устройства (slave). Основной и резервный межсетевые экраны взаимосвязаны и составляют логический HA-кластер.

Межсетевые экраны NetDefend *не поддерживают* балансировку нагрузки в **НА-кластеризации** устройств, т.е. распределение нагрузки между ними *не обеспечивается*, так как одно устройство всегда является активным (active), в то время как другое находится в режиме ожидания (passive).

[](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_14.jpg)

[увеличить изображение](https://www.intuit.ru/EDI/25_02_18_1/1519510898-10343/tutorial/1346/objects/4/files/4_14.jpg)  
**Рис. 4.14.**НА-кластеризация межсетевых экранов NetDefend