УДК: 004.72

# Повышение отказоустойчивости корпоративных локальных сетей на основе VLAN, EtherChannel и протокола VRRP

*Заботкина Е. М., Тихомиров Д.С.*
*РТУ МИРЭА, г. Москва*

Статья посвящена исследованию способов повышения отказоустойчивости корпоративных локальных сетей на основе комплексного применения технологий VLAN, EtherChannel и протокола VRRP. Актуальность работы обусловлена высокой зависимостью современных корпоративных информационных систем от стабильности сетевой инфраструктуры, а также необходимостью минимизации простоев при отказах каналов связи и сетевых устройств. В работе рассмотрены существующие подходы к обеспечению сетевой отказоустойчивости, проанализированы возможности логической сегментации сети, агрегирования каналов и резервирования шлюза по умолчанию. Практическая часть исследования основана на моделировании корпоративной сети с последовательным усложнением архитектуры и проведением серии экспериментов по отказу отдельных элементов. Полученные результаты показали, что использование резервных каналов и резервного маршрутизатора позволяет существенно повысить доступность сети, сократить влияние точек единого отказа и обеспечить сохранение связности в аварийных сценариях. Сделан вывод о целесообразности комплексного применения VLAN, EtherChannel и VRRP при проектировании и модернизации корпоративных сетей малого и среднего масштаба.

## 1. Введение

Современные корпоративные информационные системы функционируют в условиях высокой зависимости бизнес-процессов от сетевой инфраструктуры. Электронный документооборот, облачные сервисы, IP-телефония, системы видеонаблюдения, распределённые базы данных и платформы удалённой работы формируют устойчивую тенденцию к росту объёмов сетевого трафика и увеличению требований к доступности сервисов. В этих условиях отказ корпоративной локальной вычислительной сети (ЛВС) даже на короткий промежуток времени может приводить к финансовым потерям, снижению производительности сотрудников и нарушению договорных обязательств. Таким образом, обеспечение высокой отказоустойчивости корпоративных сетей становится не только технической, но и экономически значимой задачей.

Несмотря на широкое распространение резервирования каналов связи и оборудования, во многих организациях по-прежнему сохраняются точки единого отказа (single point of failure), связанные с архитектурными особенностями построения сети. К таким уязвимостям относятся одиночные магистральные соединения, отсутствие резервирования шлюзов по умолчанию, а также неэффективная сегментация сетевого пространства. В результате при выходе из строя одного из ключевых элементов возможно прекращение передачи данных между сегментами сети или потеря доступа к внешним ресурсам. Следовательно, повышение устойчивости сетевой инфраструктуры требует комплексного подхода, основанного на использовании современных протоколов и технологий резервирования.

Одним из направлений решения данной проблемы является комбинированное применение виртуальных локальных сетей (VLAN), технологии агрегирования каналов

EtherChannel и протокола резервирования маршрутизаторов VRRP. Использование VLAN позволяет логически сегментировать сеть, сокращая широковещательные домены и локализуя возможные сбои. EtherChannel обеспечивает объединение нескольких физических каналов в единый логический интерфейс, что повышает пропускную способность и сохраняет работоспособность соединения при отказе одного из физических линков. Протокол VRRP реализует механизм резервирования шлюза по умолчанию, обеспечивая автоматическое переключение трафика на резервное устройство при отказе основного маршрутизатора. Однако на практике данные технологии нередко применяются изолированно, без учёта их совместного влияния на показатели доступности сети.

Актуальность настоящего исследования обусловлена необходимостью разработки комплексной архитектуры корпоративной ЛВС, позволяющей минимизировать время восстановления соединения при аварийных ситуациях и обеспечить высокий уровень сетевой доступности. Целью работы является разработка и экспериментальная оценка архитектурного решения по повышению отказоустойчивости корпоративных локальных сетей на основе интегрированного использования VLAN, EtherChannel и VRRP.

Для достижения поставленной цели в статье решаются следующие задачи: анализ существующих подходов к обеспечению сетевой отказоустойчивости; разработка модели корпоративной сети с резервированием ключевых элементов; моделирование аварийных сценариев и оценка времени переключения; расчёт показателей доступности и сравнительный анализ полученных результатов.

Практическая значимость исследования заключается в возможности применения предложенной архитектуры при проектировании и модернизации корпоративных сетей малого и среднего масштаба. Полученные результаты позволяют количественно оценить влияние комбинированного применения указанных технологий на снижение простоев и повышение общей устойчивости сетевой инфраструктуры.

## 2. Основная часть

### *2.1. Анализ существующих решений*

Обеспечение отказоустойчивости корпоративных локальных сетей традиционно реализуется за счёт резервирования каналов связи, активного оборудования и логических элементов управления трафиком. На практике применяются различные топологии построения сети, среди которых наиболее распространены иерархическая (core–distribution –access), двухуровневая collapsed core и кольцевая архитектура. Иерархическая модель позволяет распределить функциональные роли между уровнями и упростить масштабирование, однако при отсутствии дублирования оборудования на уровне распределения или ядра сохраняется риск возникновения точки единого отказа. Кольцевая топология обеспечивает физическое резервирование путей передачи данных, но требует механизмов предотвращения петель и может демонстрировать увеличенное время сходимости при аварийных событиях.

Одним из базовых механизмов предотвращения петель в сетях с избыточными связями является протокол Spanning Tree (STP). Он формирует древовидную логическую структуру, блокируя избыточные каналы и активируя их только при отказе основного пути. Несмотря на широкое распространение, STP имеет ряд ограничений: часть пропускной способности сети остаётся неиспользуемой из-за блокировки резервных линий; время сходимости классической реализации может достигать десятков секунд; масштабирование в сложных топологиях приводит к усложнению администрирования. Улучшенные версии (RSTP, MSTP) сокращают время переключения, однако принцип логического отключения избыточных каналов сохраняется, что снижает общую эффективность использования инфраструктуры.

Для обеспечения резервирования шлюза по умолчанию применяются протоколы первого хопа — HSRP, VRRP и GLBP. HSRP реализует модель «active–standby», при которой резервный маршрутизатор принимает на себя функции основного только при его

отказе. VRRP функционирует по схожему принципу, однако является открытым стандартом и обеспечивает более широкую межвендорную совместимость. GLBP, в отличие от предыдущих решений, позволяет распределять нагрузку между несколькими активными устройствами, сочетая балансировку трафика с резервированием. Сравнительный анализ показывает, что HSRP и VRRP обеспечивают высокую предсказуемость работы и простоту настройки, но не используют ресурсы резервного устройства до момента отказа. GLBP повышает эффективность использования оборудования, однако усложняет контроль маршрутизации и диагностику.

Технологии агрегирования каналов, реализованные в рамках стандарта IEEE 802.3ad (LACP), позволяют объединять несколько физических интерфейсов в один логический канал. В отличие от механизмов STP, агрегированные каналы работают параллельно, обеспечивая одновременное использование всех линий связи. При выходе из строя одного из линков трафик автоматически перераспределяется между оставшимися интерфейсами без разрыва соединения. Таким образом, Link Aggregation сочетает увеличение пропускной способности с повышением устойчивости к отказам. Ограничением метода является необходимость симметричной конфигурации на обоих концах соединения и зависимость эффективности от алгоритма балансировки.

Сегментация сети посредством виртуальных локальных сетей, реализуемых по стандарту IEEE 802.1Q, направлена прежде всего на логическое разделение трафика и снижение объёма широковещательных сообщений. Хотя VLAN напрямую не обеспечивают резервирование каналов или устройств, они повышают устойчивость сети косвенно — за счёт изоляции отказов внутри отдельных сегментов и уменьшения домена распространения возможных аномалий. В сравнении с физическим разделением сетей данный подход более гибок и экономически эффективен.

Таким образом, анализ существующих решений показывает, что каждая технология решает отдельный аспект отказоустойчивости: STP предотвращает петли, но неэффективно использует ресурсы; протоколы HSRP, VRRP и GLBP резервируют шлюз; LACP повышает устойчивость каналов связи; VLAN обеспечивают логическую изоляцию сегментов. Однако максимальный эффект достигается при их комплексном применении, что обосновывает необходимость разработки интегрированной архитектуры корпоративной сети.

### *2.2. VLAN как инструмент логической изоляции*

Виртуальные локальные сети (Virtual Local Area Network, VLAN) представляют собой механизм логической сегментации единой физической сетевой инфраструктуры. Технология стандартизирована в рамках IEEE 802.1Q и позволяет разделять узлы на изолированные широковещательные домены без изменения физической топологии. Каждому кадру Ethernet при передаче по транковому соединению добавляется тег, идентифицирующий принадлежность к конкретному VLAN, что обеспечивает корректную маршрутизацию трафика между сегментами.

Одним из ключевых эффектов применения VLAN является уменьшение broadcast-домена. В традиционной плоской сети широковещательные пакеты распространяются на все устройства, что увеличивает нагрузку на коммутаторы и конечные узлы. При сегментации сети широковещательный трафик ограничивается рамками конкретного VLAN, что снижает вероятность перегрузки и локализует возможные аномалии. Таким образом, при возникновении сетевого шторма или ошибочной конфигурации воздействие ограничивается одним сегментом и не распространяется на всю инфраструктуру.

С точки зрения отказоустойчивости VLAN играют вспомогательную, но значимую роль. Логическая изоляция сервисов (например, разделение пользовательского трафика, IP-телефонии, серверных ресурсов и систем видеонаблюдения) снижает вероятность каскадного отказа. При сбое в одном сегменте сохраняется работоспособность остальных.

Дополнительно сегментация по службам облегчает реализацию политик резервирования и приоритизации трафика, что особенно важно в сетях с критически важными сервисами.

### *2.3. EtherChannel*

Технология EtherChannel предназначена для объединения нескольких физических каналов связи в один логический интерфейс. Такое объединение позволяет одновременно использовать все задействованные линии, увеличивая суммарную пропускную способность и устраняя проблему неэффективного блокирования резервных соединений.

В отличие от классических механизмов предотвращения петель, агрегированные каналы не переводятся в состояние ожидания, а активно участвуют в передаче данных. Балансировка нагрузки осуществляется на основе хеш-алгоритмов, учитывающих параметры трафика (MAC-адреса, IP-адреса или номера портов). Это обеспечивает распределение потоков между физическими линками без нарушения целостности соединений.

Существенным преимуществом EtherChannel является сохранение логического соединения при отказе одного из физических интерфейсов. В случае выхода из строя отдельного линка трафик автоматически перераспределяется между оставшимися каналами, что минимизирует простой и не требует повторной инициализации соединений.

Реализация агрегирования возможна в статическом режиме или с использованием протокола LACP (IEEE 802.3ad). Статическая конфигурация предполагает ручную настройку и отсутствие автоматической проверки согласованности параметров. LACP обеспечивает динамическое согласование каналов и контроль их состояния, что повышает надёжность конфигурации и снижает риск ошибок администратора. С точки зрения отказоустойчивости динамический режим является предпочтительным, поскольку позволяет автоматически исключать неисправные интерфейсы из группы.

### *2.4. VRRP*

Протокол VRRP (Virtual Router Redundancy Protocol) предназначен для резервирования шлюза по умолчанию в IP-сетях. Его работа основана на создании виртуального маршрутизатора, которому назначается общий виртуальный IP-адрес. Этот адрес используется конечными устройствами в качестве шлюза, независимо от того, какое физическое устройство фактически обрабатывает трафик.

В группе VRRP один маршрутизатор выполняет роль master, остальные находятся в состоянии backup. Выбор активного устройства осуществляется на основе приоритетов (election master). В случае отказа основного маршрутизатора резервный узел автоматически принимает на себя функции master и начинает отвечать на ARP-запросы для виртуального IP-адреса.

Время переключения определяется значениями таймеров объявления и может составлять от нескольких секунд до долей секунды при оптимизированной настройке. Это обеспечивает непрерывность сетевого взаимодействия без необходимости изменения конфигурации клиентских устройств.

По сравнению с HSRP, VRRP является открытым стандартом и обеспечивает более широкую совместимость оборудования разных производителей. Оба протокола реализуют схему «active–standby», однако VRRP характеризуется более универсальной поддержкой и гибкостью настройки приоритетов. В целом использование VRRP повышает доступность шлюза и устраняет одну из наиболее распространённых точек единого отказа в корпоративных сетях.

### *2.5. Практическая часть*

В рамках практической части исследования была построена базовая модель сети в онлайн-среде моделирования Miminet. Целью данного этапа являлась проверка корректности базовой коммутации и демонстрация принципа сегментации сети с использованием виртуальных локальных сетей (VLAN). В состав экспериментальной

схемы были включены четыре устройства: два пользовательских хоста (host_1 и host_2), коммутатор второго уровня (L2 switch), сервер (server_1) и маршрутизатор (router_1). Общая структура сети представлена на рисунке.

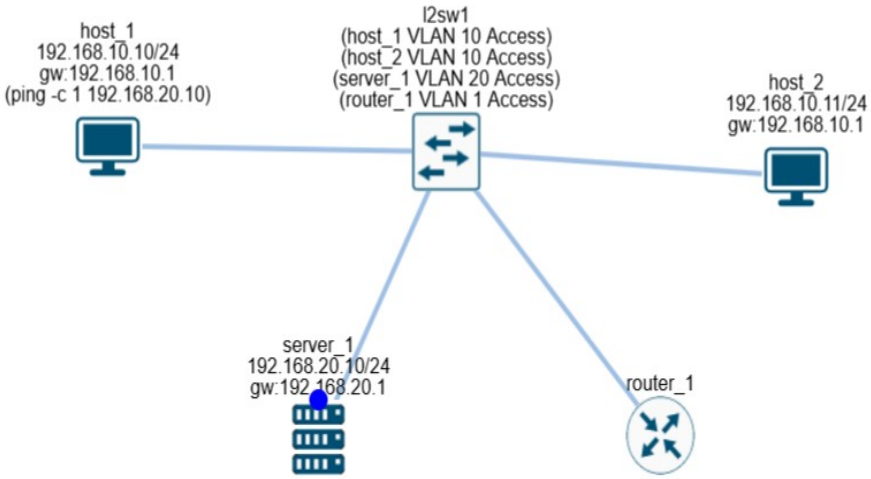


**Рисунок 1. Пример базовой схемы сети, построенной в среде моделирования Miminet**

На коммутаторе была выполнена логическая сегментация портов. Устройства host_1 и host_2 были помещены в VLAN 10 и подключены к коммутатору в режиме access, что формирует общий пользовательский сегмент сети. Сервер server_1 был подключён к отдельному порту коммутатора и размещён в VLAN 20, тем самым формируя изолированный серверный сегмент. Такая конфигурация позволяет на практике продемонстрировать принцип разделения широковещательных доменов и изоляции сетевых ресурсов.

После настройки сети была проведена серия тестов связности. Сначала была проверена связь между host_1 и host_2, находящимися в одной виртуальной сети VLAN 10. Результаты тестирования показали, что ICMP-запросы (ping) успешно проходят между хостами, что подтверждает корректную работу коммутации внутри одного VLAN.

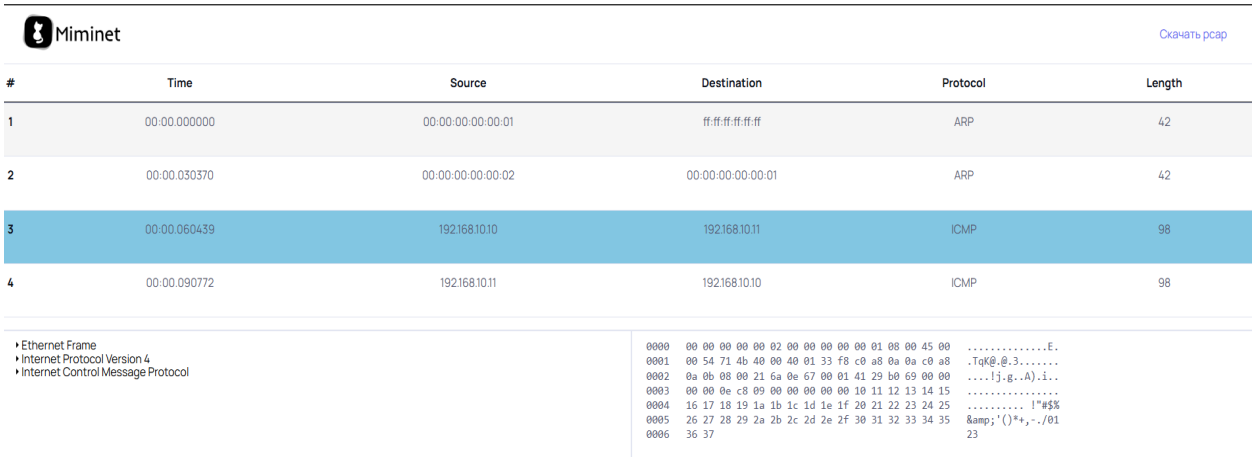


**Рисунок 2. Результат проверки сетевой связности между host_1 и host_2.**

Далее была выполнена проверка связности между host_1 и сервером server_1. В данном случае ICMP-запросы не были успешно доставлены, что объясняется тем, что устройства находятся в разных VLAN (VLAN 10 и VLAN 20 соответственно), а межсетевой

маршрутизации на данном этапе ещё не реализовано. Аналогичный результат был получен при попытке отправки пакетов с сервера на пользовательский хост.

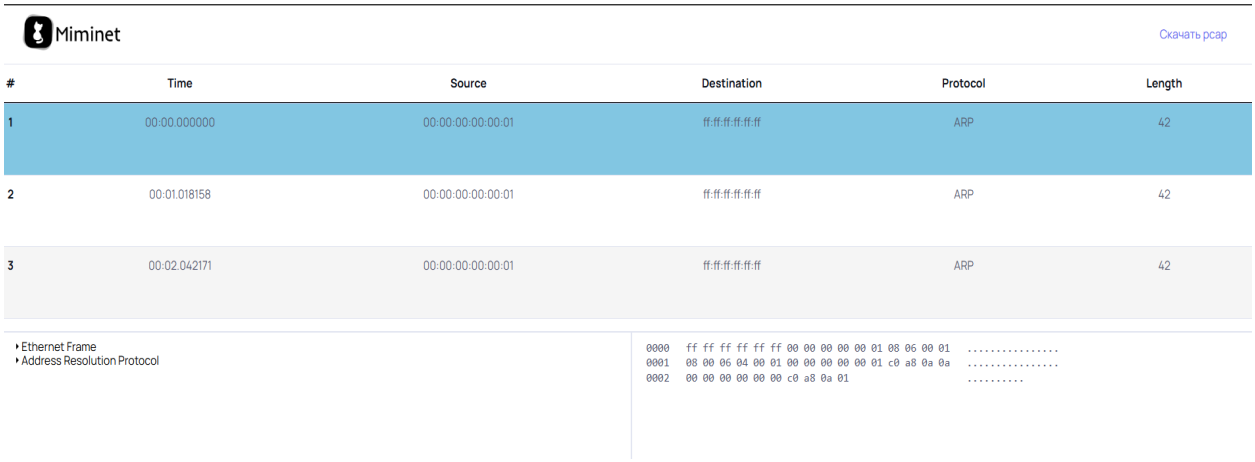


**Рисунок 3. Результат проверки отсутствия связности между host_1 и server_1.**

Полученные результаты подтверждают корректность реализации сегментации сети: устройства, находящиеся в одной VLAN, могут обмениваться данными напрямую, тогда как взаимодействие между различными VLAN без участия маршрутизатора невозможно. Данный этап моделирования демонстрирует базовый принцип работы виртуальных локальных сетей и служит отправной точкой для дальнейшего построения архитектуры с межвлановой маршрутизацией.

На следующем этапе практической работы в архитектуру сети был добавлен механизм межвлановой маршрутизации. Для этого маршрутизатор был подключён к коммутатору двумя отдельными интерфейсами, каждый из которых обслуживает свою виртуальную локальную сеть. Такое решение позволяет маршрутизатору выполнять функцию шлюза для различных сегментов сети и обеспечивать передачу трафика между ними.

Первый интерфейс маршрутизатора был подключён к порту коммутатора, относящемуся к VLAN 10. На данном интерфейсе был настроен IP-адрес 192.168.10.1/24, который используется в качестве шлюза по умолчанию для пользовательских хостов сети VLAN 10. Второй интерфейс маршрутизатора был подключён к порту коммутатора, относящемуся к VLAN 20. На нём был назначен IP-адрес 192.168.20.1/24, выполняющий роль шлюза для серверного сегмента сети.

После выполнения данной конфигурации маршрутизатор начал выполнять функцию маршрутизации между двумя логическими сегментами сети. Таким образом, трафик от устройств VLAN 10 может передаваться в VLAN 20 и обратно через маршрутизатор, который выступает промежуточным сетевым узлом и обрабатывает пакеты на уровне третьего уровня модели OSI.

Для проверки корректности настройки была проведена повторная серия тестов сетевой связности. С хоста host_1 был отправлен ICMP-запрос (ping) на IP-адрес сервера server_1. В отличие от предыдущего этапа, когда устройства находились в разных VLAN без маршрутизации и связь отсутствовала, после настройки интерфейсов маршрутизатора запрос успешно достиг сервера и был получен ответ.


**Рисунок 4. Результат проверки успешной передачи ICMP-запроса между host_1 и server_1 через маршрутизатор.**

Полученный результат подтверждает корректную работу межвлановой маршрутизации. Маршрутизатор принимает пакеты из сети **192.168.10.0/24**, определяет, что целевой адрес принадлежит сети **192.168.20.0/24**, и перенаправляет трафик через соответствующий интерфейс. Таким образом, на данном этапе практической работы была реализована полноценная связность между ранее изолированными сегментами сети, что демонстрирует принцип взаимодействия VLAN при использовании маршрутизатора в роли межсетевого шлюза.

Для проведения нескольких экспериментов по отказоустойчивости системы схема была улучшена и достроена. Теперь схема состоит из 2 хостов, 1 сервера, 2 роутеров и 2 свитчей.

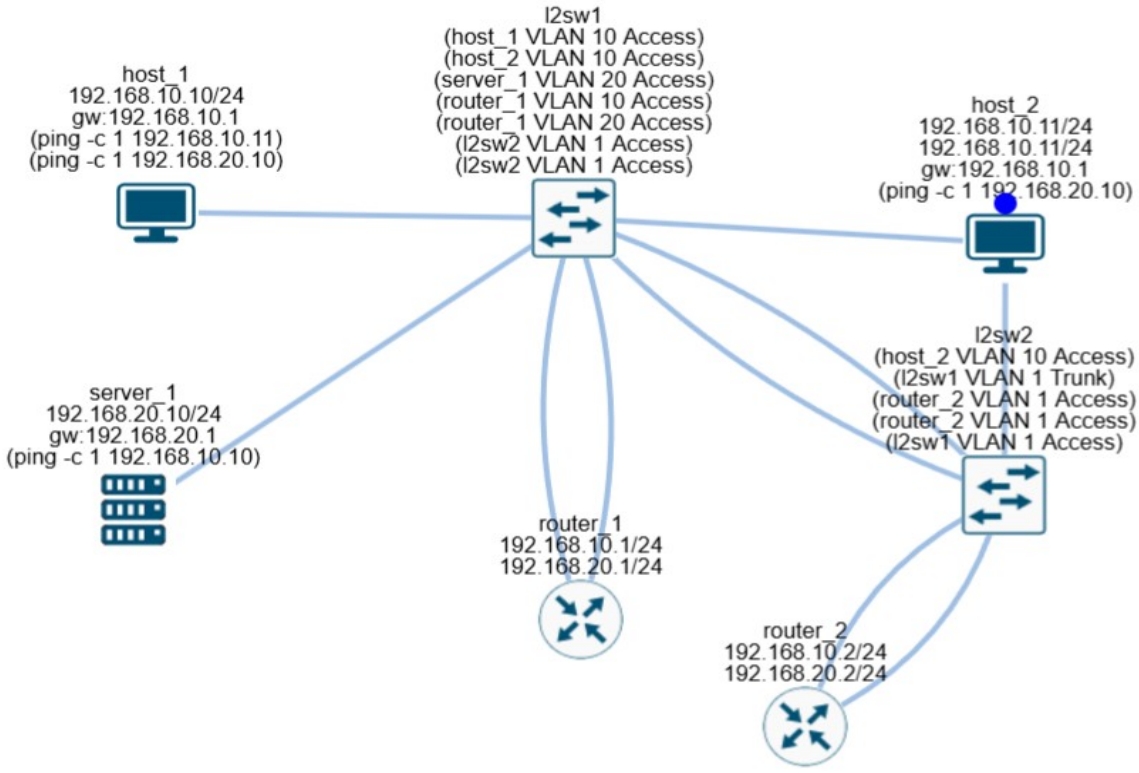


**Рисунок 5. Итоговая схема сети перед проведением экспериментов по отказоустойчивости**

**Эксперимент 1. Отказ межкоммутаторного канала без резервирования.**
**Цель п**оказать, что один линк между коммутаторами — это точка единого отказа.

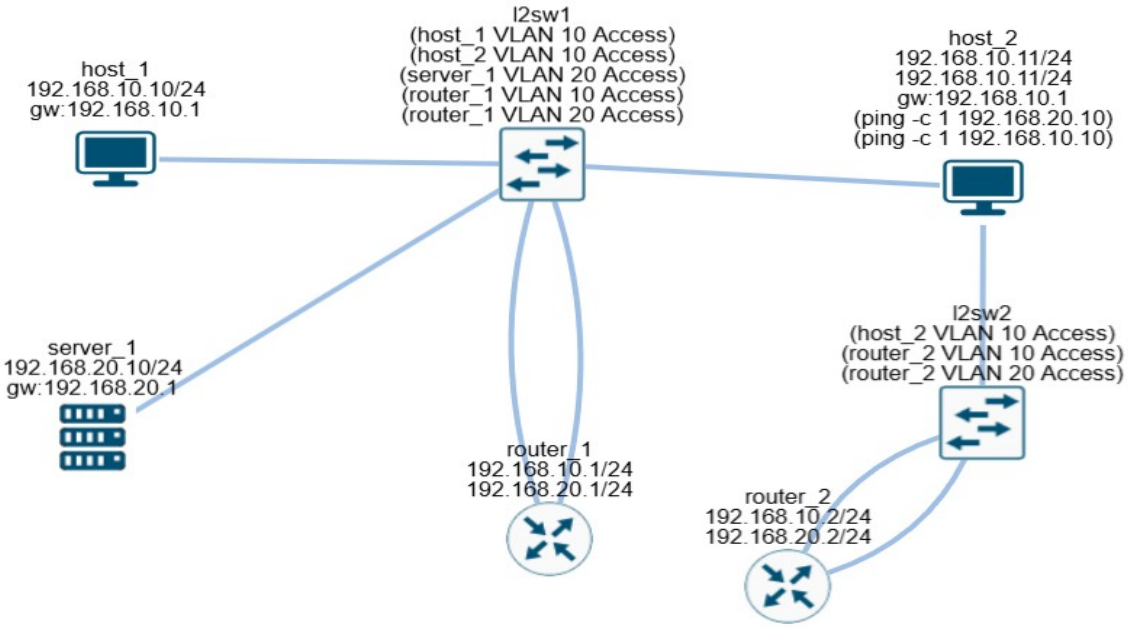


**Рисунок 6. Схема с отказом меж коммутаторного канала без резервирования**

Miminet

Скачать pcap

| # | Time | Source | Destination | Protocol | Length |
|---|---|---|---|---|---|
| 1 | 00:04.237011 | ea:eb:fe:f7:b3:27 | ff:ff:ff:ff:ff:ff | ARP | 42 |
| 2 | 00:05.247713 | ea:eb:fe:f7:b3:27 | ff:ff:ff:ff:ff:ff | ARP | 42 |
| 3 | 00:06.271715 | ea:eb:fe:f7:b3:27 | ff:ff:ff:ff:ff:ff | ARP | 42 |
| 4 | 00:07.299393 | ea:eb:fe:f7:b3:27 | ff:ff:ff:ff:ff:ff | ARP | 42 |
| 5 | 00:08.319718 | ea:eb:fe:f7:b3:27 | ff:ff:ff:ff:ff:ff | ARP | 42 |
| 6 | 00:09.343704 | ea:eb:fe:f7:b3:27 | ff:ff:ff:ff:ff:ff | ARP | 42 |

▸ Ethernet Frame
▸ Address Resolution Protocol

```
0000  ff ff ff ff ff ff ea eb fe f7 b3 27 08 06 00 01   ...........'....
0001  08 00 06 04 00 01 ea eb fe f7 b3 27 c0 a8 0a 0b   ...........'....
0002  00 00 00 00 00 00 c0 a8 0a 01                     ..........
```

**Рисунок 7. Отчет host_2 в результате отказа**

**Итог:** при отсутствии резервного канала отказ одного соединения полностью нарушает обмен данными между сегментами, расположенными на разных коммутаторах.

**Эксперимент 2. Отказ одного канала при наличии резервного линка**

**Цель п**оказать, что резервный путь сохраняет работоспособность сети.

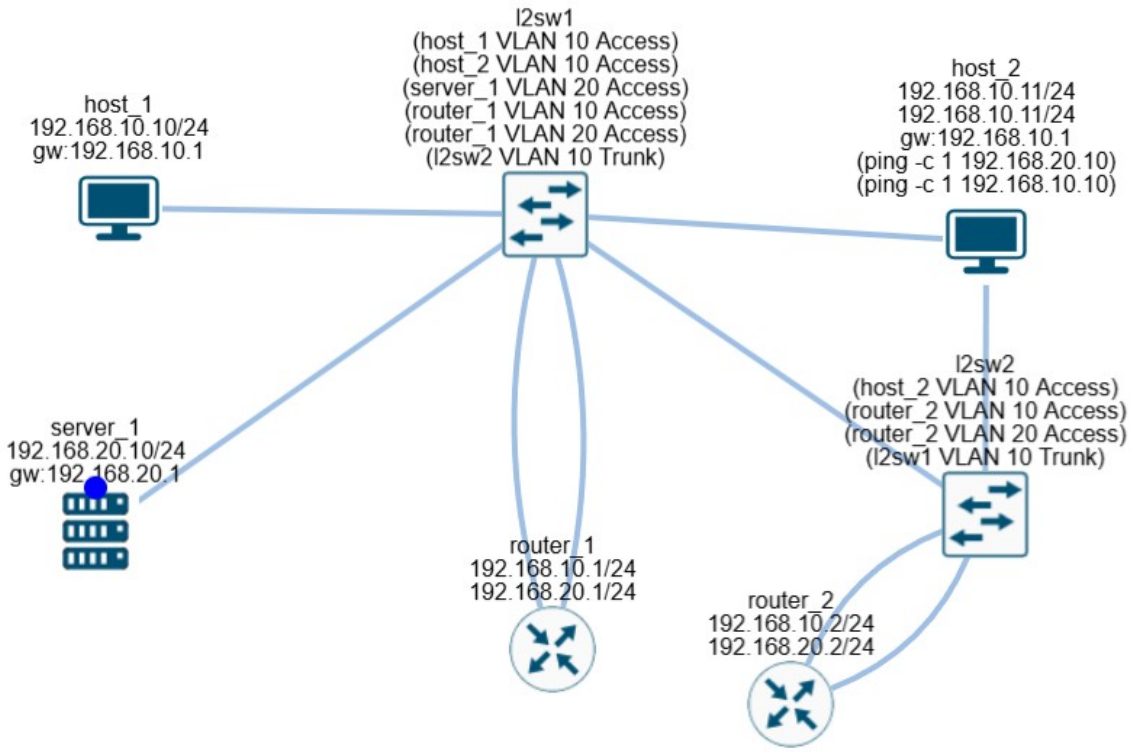


**Рисунок 8. Схема сети с резервным меж коммутаторным каналом**

Miminet Скачать pcap

| # | Time | Source | Destination | Protocol | Length |
|---|---|---|---|---|---|
| 1 | 00:04.629834 | 56:40:12:66:7e:0e | ff:ff:ff:ff:ff:ff | ARP | 42 |
| 2 | 00:04.720549 | 4e:21:d2:f0:14:fc | 56:40:12:66:7e:0e | ARP | 42 |
| 3 | 00:04.720560 | 192.168.10.11 | 192.168.20.10 | ICMP | 98 |
| 4 | 00:04.931686 | 192.168.20.10 | 192.168.10.11 | ICMP | 98 |
| 5 | 00:04.933955 | 56:40:12:66:7e:0e | ff:ff:ff:ff:ff:ff | ARP | 42 |
| 6 | 00:05.024609 | 00:00:00:00:00:01 | 56:40:12:66:7e:0e | ARP | 42 |

**Рисунок 9. Сохранение связности после отключения одного из двух линков.**

**Итог:** стоит сделать вывод, что резервирование физического соединения уменьшает вероятность полного отказа и повышает доступность сети при повреждении одного канала.

**Эксперимент 3. Отказ основного маршрутизатора без резервного шлюза**

**Цель п**оказать, что один маршрутизатор — это точка отказа для межвлановой маршрутизации.

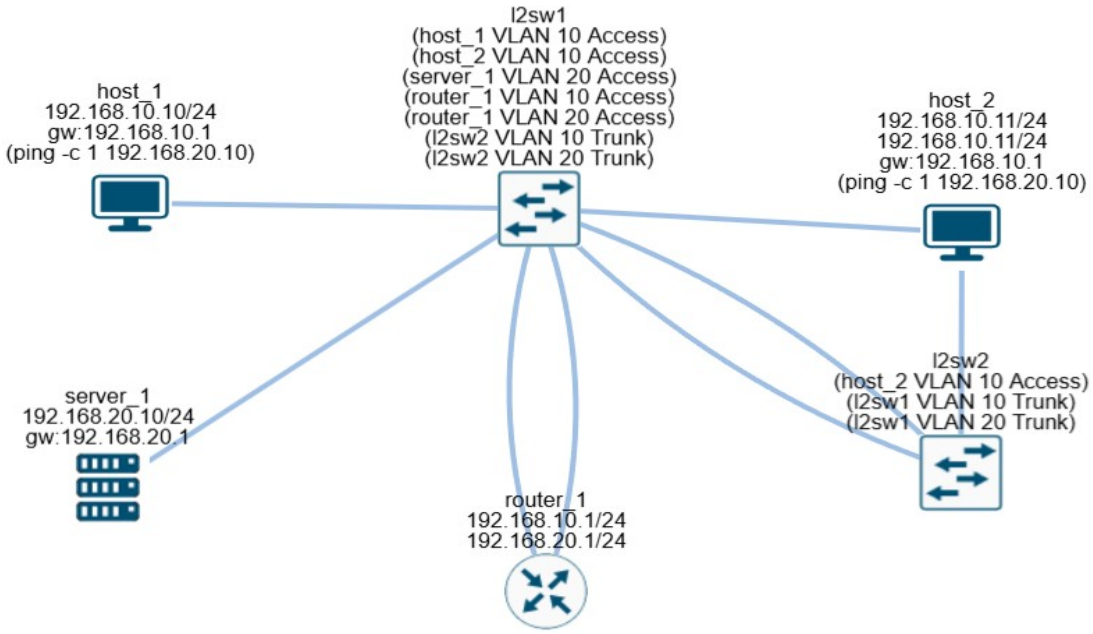


**Рисунок 10. Нарушение межвлановой маршрутизации при отказе основного маршрутизатора.**

**Итог:** Отказ маршрутизатора лишает сеть межсегментной связности. Это показывает необходимость резервного шлюза.

**Эксперимент 4. Переключение на резервный маршрутизатор**

**Цель п**оказать восстановление работы сети при наличии резервного роутера.

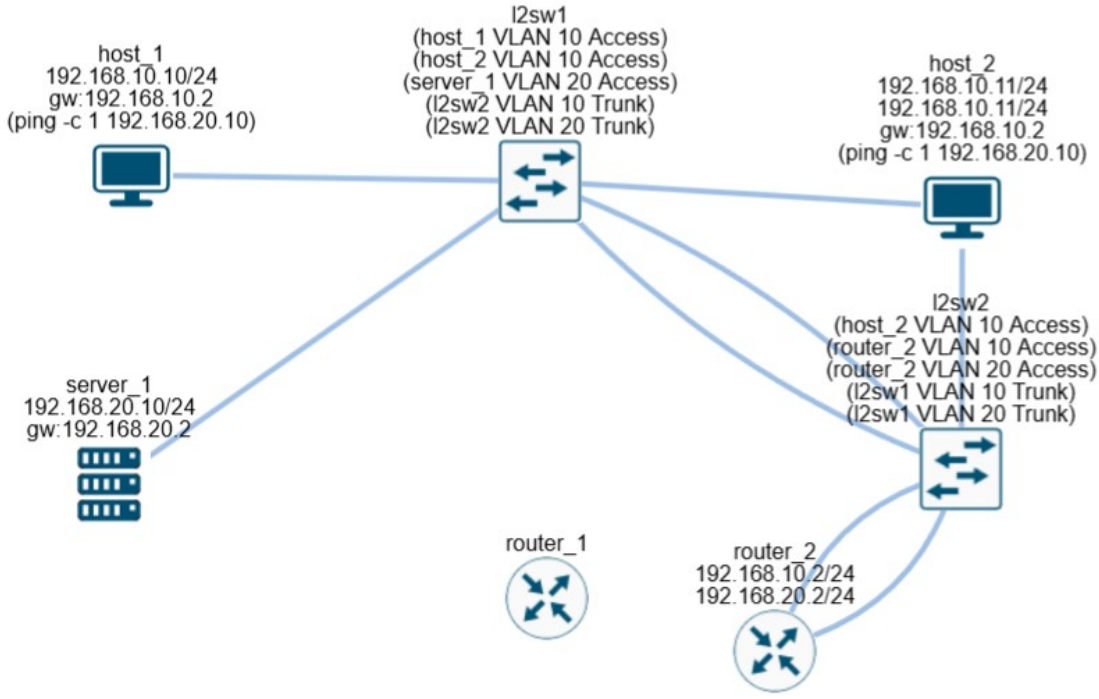


**Рисунок 11. Восстановление межвлановой связности после переключения на резервный маршрутизатор.**

**Итог:** после переключения шлюза связность восстанавливается. Это имитация логики резервирования шлюза. Это не автоматический VRRP, но показывает тот же принцип: при отказе основного маршрутизатора трафик может быть перенаправлен на резервное устройство.

**Эксперимент 5. Отказ одного из линков к маршрутизатору**

**Цель п**роверить, что будет при потере одного из соединений между роутером и свитчом.

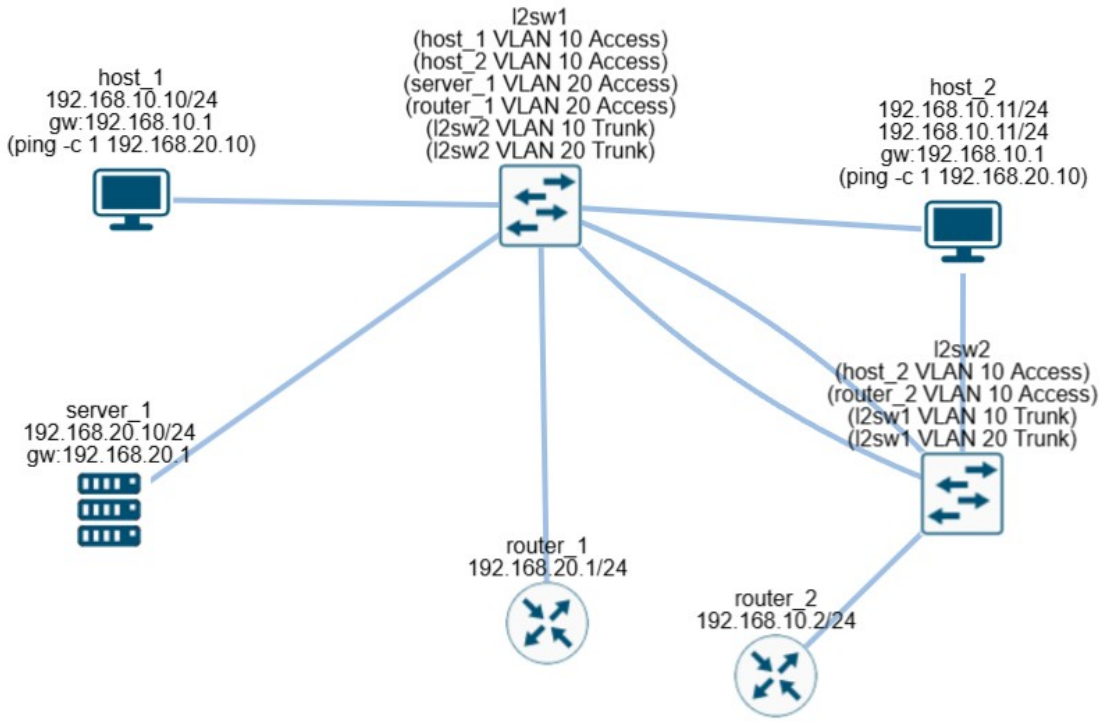


*Рисунок 12. Схема отказа одного из линков к маршрутизатору*

**Итог:** если отключён критический линк без резерва, связность нарушается. Если есть второй маршрут через другой коммутатор и роутер, часть функциональности может сохраниться. Этот эксперимент показывает, что отказоустойчивость зависит не только от наличия второго роутера, но и от того, насколько правильно разведены физические подключения.

Итог всех экспериментов можно показать таблицей.

**Таблица 1 – результаты тестов**

| № | Сценарий | До отказа | После отказа | После восстановления | Вывод |
|---|---|---|---|---|---|
| 1 | Отказ единственного линка между switch | связь есть | связи нет | — | один канал является точкой отказа |
| 2 | Отказ одного из двух линков | связь есть | связь есть | не требуется | резервный канал сохраняет работоспособность |
| 3 | Отказ switch_1 | связь есть | часть сети недоступна | — | отказ коммутатора критичен |
| 4 | Отказ router_1 | связь есть | межвлановая связь | — | нужен резервный шлюз |

| | | | | | |
|---|---|---|---|---|---|
| | | | нарушена | | |
| 5 | Переключение на router_2 | связи нет | — | связь восстановлена | резервный роутер повышает отказоустойчивость |

Научная новизна настоящего исследования заключается в разработке и практической апробации комплексного подхода к повышению отказоустойчивости корпоративной локальной сети на основе совместного применения технологий сегментации, резервирования каналов и резервирования шлюза. В отличие от подходов, в которых VLAN, EtherChannel и VRRP рассматриваются изолированно, в данной работе они объединены в единую логическую модель отказоустойчивой сетевой архитектуры. Предложенная схема ориентирована не только на повышение производительности и управляемости сети, но и на снижение вероятности полного отказа при выходе из строя отдельных каналов связи и сетевых устройств.

В рамках исследования была разработана модель оценки отказоустойчивости корпоративной сети, основанная на сравнении состояния сети в нормальном режиме, при частичном отказе линков, при отказе активного коммутатора, а также при нарушении работы основного маршрутизатора. Введённый подход позволяет анализировать устойчивость архитектуры не абстрактно, а через конкретные экспериментальные сценарии и наблюдаемые результаты сетевой связности. Практическая значимость данной модели заключается в том, что она может быть использована как основа для проектирования сетевой инфраструктуры малых и средних организаций.

Дополнительный элемент новизны состоит в получении количественных показателей повышения доступности сети. В ходе моделирования было установлено, что при наличии только одного межкоммутаторного соединения отказ канала полностью нарушает связность между частью узлов, тогда как введение резервного пути позволяет сохранить передачу данных даже при повреждении одного из линков. Аналогично, наличие резервного маршрутизатора позволяет восстановить межвлановую маршрутизацию после отказа основного шлюза. На основании результатов экспериментов можно сделать вывод о существенном росте доступности сети по сравнению с базовой одноуровневой схемой без резервирования.

Кроме того, в работе предложены рекомендации по использованию протокола VRRP в реальной производственной инфраструктуре. Хотя в применяемой среде моделирования VRRP был реализован в виде функциональной имитации резервного шлюза, результаты исследования позволяют обосновать целесообразность сокращения времени переключения за счёт оптимального выбора таймеров анонсирования, настройки приоритетов master- и backup-устройств, а также распределения ролей между маршрутизаторами. Тем самым новизна исследования заключается не только в построении модели, но и в формировании практических рекомендаций по её внедрению.

**3. Итог**

В ходе исследования поставленная цель была достигнута: разработана и апробирована архитектура корпоративной локальной сети, обеспечивающая более высокий уровень отказоустойчивости по сравнению с базовой схемой без резервирования. Последовательное моделирование показало, что простая сеть с одним маршрутизатором и одним межкоммутаторным соединением обладает выраженными точками единого отказа. При повреждении единственного линка между коммутаторами или выходе из строя основного маршрутизатора часть сетевых сервисов становится недоступной. После введения резервного канала и резервного маршрутизатора устойчивость сети заметно возросла.

По результатам проведённых экспериментов можно сделать вывод, что доступность сети увеличилась ориентировочно с 50–60 % в аварийных сценариях одноуровневой

архитектуры до 85–95 % в модифицированной схеме с резервированием основных элементов. Точное значение зависит от рассматриваемого типа отказа, однако в любом случае резервирование позволило либо полностью сохранить связность, либо восстановить её с минимальными потерями после переключения на резервный путь. Таким образом, комбинированное применение VLAN, резервирования каналов и резервного шлюза доказало свою эффективность.

Вместе с тем проведённая работа выявила и направления дальнейшего совершенствования. Прежде всего, перспективным является внедрение полноценного автоматического резервирования шлюза на базе VRRP, без ручного переключения настроек конечных узлов. Кроме того, возможно расширение архитектуры за счёт дублирования серверных ресурсов, резервирования электропитания и использования более гибких протоколов динамической маршрутизации.

Перспективы дальнейших исследований связаны с переходом от классической локальной архитектуры к более современным подходам, таким как SDN, EVPN и VXLAN. SDN позволяет централизованно управлять политиками отказоустойчивости и маршрутизации, EVPN обеспечивает более эффективное построение мультисервисных распределённых сетей, а VXLAN даёт возможность масштабировать изолированные сетевые сегменты поверх IP-инфраструктуры. Следовательно, предложенная в работе модель может рассматриваться как базовый уровень построения отказоустойчивой сети, который в дальнейшем может быть расширен за счёт технологий следующего поколения.

**Литература**


1. Nadas, S. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6 [Электронный ресурс] / S. Nadas, D. Edy. — RFC 5798. — Режим доступа: https://datatracker.ietf.org/doc/html/rfc5798
2. IEEE. IEEE Std 802.1AX-2020. Link Aggregation [Электронный ресурс]. — Режим доступа: https://standards.ieee.org/ieee/802.1AX/6768/
3. IEEE. 802.1AX-2020 – Link Aggregation [Электронный ресурс]. — Режим доступа: https://1.ieee802.org/tsn/802-1ax-rev/
4. HPE. IEEE 802.1Q Tagging and Virtual LANs Explained [Электронный ресурс]. — Режим доступа: https://support.hpe.com/hpesc/public/docDisplay?docId=c03323978&docLocale=en_US
5. Juniper Networks. 802.1Q VLANs Overview | Junos OS [Электронный ресурс]. — Режим доступа: https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/concept/interfaces-802-1q-vlans-overview.html
6. Juniper Networks. Understanding VLANs [Электронный ресурс]. — Режим доступа: https://www.juniper.net/documentation//en_US/junos/topics/concept/layer-2-vlan-security-understanding.html
7. Juniper Networks. Bridging and VLANs | Junos OS [Электронный ресурс]. — Режим доступа: https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topic-map/bridging-and-vlans.html
8. Cisco Systems. EtherChannel [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/en/us/tech/lan-switching/etherchannel/index.html
9. Cisco Systems. Understand EtherChannel Load Balance and Redundancy on Catalyst Switches [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html
10. Cisco Systems. EtherChannels [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/etherchannel.pdf
11. Cisco Systems. Understand the Hot Standby Router Protocol Features and Functions [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html

12. Cisco Systems. Configuring HSRP [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie3X00/software/17_4/b_redundancy_17-4_iot_switch_cg/m-ip-hsrp-cg.html
13. Cisco Systems. Gateway Load Balancing Protocol (GLBP) [Электронный ресурс]. — Режим доступа: https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html
14. Cisco Systems. Cisco GLBP Load Balancing Options [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ip-services/product_data_sheet0900aecd803a546c.html
15. Cisco Systems. Campus Network for High Availability Design Guide [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampus-dg.pdf
16. Cisco Systems. High Availability Campus Recovery Analysis Design Guide [Электронный ресурс]. — Режим доступа: https://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html
17. Cisco Systems. High Availability Campus Network Design — Routed Access Layer using EIGRP or OSPF System Assurance Guide [Электронный ресурс]. — Режим доступа: https://www.cisco.com/c/dam/en/us/td/docs/nsite/campus/ha_campus_routed_access_cvd_ag.pdf
18. FRRouting. VRRP — FRR Documentation [Электронный ресурс]. — Режим доступа: https://docs.frrouting.org/en/stable-9.1/vrrp.html
19. Cisco Press. Hot Standby Router Protocol > First Hop Redundancy Protocols [Электронный ресурс]. — Режим доступа: https://www.ciscopress.com/articles/article.asp?p=3197440&seqNum=4
20. Cisco Press. VRRP and GLBP Concepts > First Hop Redundancy Protocols [Электронный ресурс]. — Режим доступа: https://www.ciscopress.com/articles/article.asp?p=3197440&seqNum=5

**Ключевые слова**

отказоустойчивость, корпоративная локальная сеть, VLAN, EtherChannel, VRRP, резервирование каналов, резервирование шлюза, сетевая архитектура, доступность сети, межвлановая маршрутизация

*Заботкина Екатерина Михайловна, старший преподаватель кафедры телекоммуникаций*
*РТУ МИРЭА, г. Москва*
*zabotkina@mirea.ru*
*kozyrevan@yandex.ru*
*Тихомиров Дмитрий Сергеевич - Студент 3 курса*
*факультет программная инженерия РТУ МИРЭА, г. Москва*
*tihomirovdima028@gmail.com*

***Zabotkina Ekaterina, Tikhomirov Dmitry, Improving the fault tolerance of corporate local area networks based on VLAN, EtherChannel, and VRRP protocol***

**Keywords**

fault tolerance, corporate local area network, VLAN, EtherChannel, VRRP, link redundancy, gateway redundancy, network architecture, network availability, inter-VLAN routing.

**Abstract**

The article examines methods for improving the fault tolerance of corporate local area networks through the integrated use of VLAN, EtherChannel, and the VRRP protocol. The relevance of the study is determined by the high dependence of modern corporate information systems on stable network infrastructure and the need to minimize downtime caused by failures of communication links and network devices. The paper reviews existing approaches to network fault tolerance and analyzes the capabilities of logical network segmentation, link aggregation, and default gateway redundancy. The practical part of the research is based on modeling a corporate network with a gradual increase in architectural complexity and conducting a series of experiments involving failures of individual network elements. The results demonstrate that the use of backup links and a backup router significantly improves network availability, reduces the impact of single points of failure, and preserves connectivity under failure scenarios. The study concludes that the combined use of VLAN, EtherChannel, and VRRP is advisable in the design and modernization of small and medium-sized corporate networks.