МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»**

Кафедра Математического и компьютерного моделирования

Анализ и оптимизация лабораторной сетевой среды для исследования и тестирования технологий и методов работы сети передачи данных

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 2 курса 247 группы

направление 09.04.03 — Прикладная информатика

механико-математического факультета

Норкина Павла Владимировича

Научный руководитель
проф., д.э.н., профессор Л.В. Кальянов

Зав. кафедрой
зав. каф., д.ф.-м.н., доцент Ю.А. Блинков

Саратов 2023

Введение. Сети передачи данных сегодня служат основой для развертывания современных форм связи. В зависимости от своего назначения и сложности, более простой или более сложной реализации, сети становятся более сложными и могут гарантировать различный уровень качества обслуживания, предлагать большую степень избыточности или устойчивости к ошибкам. В этом случае надежность самой сети является решающим фактором для предоставления сервисов конечным пользователям. В этой работе описывается, проектируется и внедряется оптимизация для лабораторной сети с акцентом на изучение сетевых технологий.

Корпоративные сети передачи данных. Корпоративная сеть - это среда для реализации базовых сетевых служб передачи данных и других расширенных сервисов, характерных для корпоративной среды. Такая сеть, независимо от ее размера и сложности, должна гарантировать определенный уровень надежности, безопасности, доступности услуг и, наконец, возможности для ее эффективного управления. С ростом числа сервисов растут и требования к ее проектированию и управлению. Требование взаимной интеграции сервисов и их объединения через единый элемент управления доступом также характерно для среды предприятия. В большинстве случаев корпоративная сеть управляется одной организацией. Если необходимо реализовать сеть передачи данных между географически разделенными местами (например, главный офис и удаленный филиал), то для обеспечения взаимосвязи и безопасной передачи данных между этими сетями принято использовать, например, IP-туннели. Они могут соединять эти удаленные сети в одну большую, кажущуюся «локальной» сеть. Однако для целей данной работы ограничимся одной географически разделенной сетью, которая реализована в одном месте.

Разделение сетей передачи данных. В сетях передачи данных любого масштаба обычно сталкиваются с активными элементами, которые обеспечивают взаимосвязь взаимодействующих узлов как на физическом, так и на логическом уровне. К элементам, обеспечивающим физическое соединение, относятся в основном коммутаторы и точки доступа для беспроводных сетей. Эти элементы работают в большинстве своем с адресами канального уровня и поэтому коммутируют только единицы данных. Взаимосвязь ло-

гических сетей обеспечивается маршрутизаторами, интерфейсы которых в основном принадлежат этим взаимосвязанным сетям, между которыми пакеты направляются на сетевом уровне, в настоящее время в большей степени исключительно на уровне IP пакета протоколов TCP/IP.

Разделение физической топологии с помощью VLAN. Коммутаторы устраняют недостатки хабов путем развертывания процессов или схем, которые обеспечивают коммутацию на основе информации, содержащейся в заголовке коммутируемых кадров. Заголовок каждого кадра содержит, помимо прочего, адрес отправителя и адрес получателя, обеспечивая тем самым возможность адресации коммутируемых устройств между двумя связывающимися узлами. Коммутация кадров от одного отправителя к нескольким получателям также очень распространена в локальных сетях. Сегодня в локальных сетях, реализующих многоточечные каналы связи, часто сталкиваемся с блоками (кадрами) типа Ethernet II. В соответствии с рисунком 1, представлена структура этого кадра.

Рисунок 1 — Структура кадра Ethernet II

Сегментация на сетевом уровне. Логические адреса IP используются для адресации коммуникаций на интернет-уровне TCP/IP. Поскольку устройства не являются членами одного и того же домена L2 после сегментации канального уровня, необходима маршрутизация. Хотя коммутаторы L3, которые способны маршрутизировать кадры на основе данных, содержащихся в IP-пакете, сейчас устанавливаются в качестве стандарта для больших сетей, в небольших сетях необходимо использовать маршрутизаторы. Работа с блоками данных сетевого уровня предоставляет несколько возможностей для выборочной фильтрации трафи10 ка, трансляции логических адресов или реализации механизмов обеспечения качества обслуживания.

Функции DHCP. DHCP основан на RFC 1531 и считается преемником BOOTP. Связь DHCP основана на модели сервер-клиент, т.е. сервер отвечает на запросы клиентов о передаче параметров конфигурации сети. Наиболее распрос траненными параметрами являются параметры IP-адреса запрашивающего узла, маска сети, адрес шлюза по умолчанию этой сети и IP-адреса серверов разрешения имен DNS. Однако протокол DHCP предлагает и более продвинутые возможности, в частности, передачу сетевой информации узлу и наоборот. Эта информация передается через сообщения DHCP Options, которые представляют собой отдельные параметры, устанавливаемые с помощью протокола DHCP.

Функции DNS. DNS занимает важное место в современных локальных и публичных сетях. Ведение полной базы данных сетевых узлов в их естественном, т.е. числовом, виде сегодня практически невозможно. Однако связь в компьютерных сетях осуществляется исключительно посредством IP-адресов, то есть 32- или 128-битных числовых идентификаторов, и поэтому система DNS с точки зрения пользователя служит скорее инструментом, помогающим узлам сети присвоить легко запоминающееся имя. DNS - это прикладной протокол, который использует транспортные протоколы UDP 53 и TCP 53 на стороне сервера. Он использует модели связи клиент-сервер и сервер-сервер. Транспортный протокол UDP используется для «нормальной передачи» клиентских запросов, в основном из-за его быстрого времени отклика. Надежность передачи здесь обычно не требуется, возможная ошибка передачи DNS обычно компенсируется клиентом путем отправки нескольких запросов к нескольким DNS-серверам за очень короткое время. Напротив, связь, ориентированная на соединение, с использованием протокола TCP требуется при так называемой передаче зон, то есть передаче и синхронизации информационной базы между самими DNS-серверами, где, наоборот, надежность передачи желательнее скорости передачи.

Лабораторная сетевая среда. глава посвящена описанию текущей топологии и представленных в ней устройств. Также оцениваются преимущества и недостатки логической структуры сети и функционирующих в ней сервисов. Лабораторная сеть обеспечивает передачу блоков данных в отдельных сетях VLAN, специфичных для каждого рабочего места. Затем эти VLAN

передаются на коммутатор, соединяющий физические экспериментальные устройства. Экспериментальные VLAN с VID в диапазоне 330–360 передаются только с использованием тегированных кадров. Таким образом, экспериментальные сети представляют собой совершенно отдельную часть лабораторной сети, и их взаимосвязь обычно нежелательна. Эти сети могут содержать большое количество неправильно защищенных рабочих станций, неправильно настроенных сетевых устройств, а их взаимосвязь может нарушить работу лабораторной сети (например, неправильно настроенный STP).

В настоящее время в сети передачи данных используется один маршрутизатор и четыре коммутатора. Для простоты будем использовать символическую маркировку элементов сети и подключенных физических и виртуальных станций.

Пусть R1 формирует граничный маршрутизатор лабораторной подсети, выполняет трансляцию адресов сетевого уровня и выборочную трансляцию адресов транспортного уровня. На маршрутизаторе определена только одна локальная сеть, которая распространяется на первый коммутатор SW1 с использованием нетегированных кадров. На этом коммутаторе уже определены определенные виртуальные сети (VLAN), которые выборочно назначаются отдельным интерфейсам. Однако отделение так называемых обучающих VLAN от экспериментальных.

Новая архитектура сети передачи данных. Сеть передачи данных, описываемая в данной дипломной работе, должна служить основой для выполнения большого количества лабораторных заданий в тестирования, но в то же время должна обеспечивать доступ к остальной рабочей сети и сети Интернет, должна обеспечивать доступ к некоторым более продвинутым сервисам, обычно используемым в корпоративной среде, и в то же время гарантировать определенную степень надежности. Поскольку доступно несколько активных сетевых элементов и передовых серверных технологий, в работе также учитывается возможность включения этих элементов в окончательный проект.

Новая модель сети передачи данных создается в течение летнего семестра параллельно с лабораторией. По этой причине здесь используется совершенно отдельный коммутатор Cisco WS3750X-48P, настроенный на роль главного

коммутатора, образующего ядро сети. В нем, помимо прочего, имеется 48 интерфейсов 1000BASE-T, которые соединяют не только пограничный маршрутизатор, но и другие коммутаторы доступа. Установленная версия операционной системы Cisco IOS включает, среди прочего, пакет ipservices, который делает коммутатор пригодным для предоставления основных услуг на базе IP (коммутация L3, создание и применение ACL, агент DHCP Relay и т.д.).

Как уже упоминалось, используемый коммутатор Cisco WS-3750X обладает функцией коммутации L3 и будет использоваться в качестве основного коммутатора в новой конструкции. В сетях меньшего масштаба, таких как эта, это очень распространено для уровня распределения и ядра сети. Новая топология представлена в соответствии с рисунком 2.

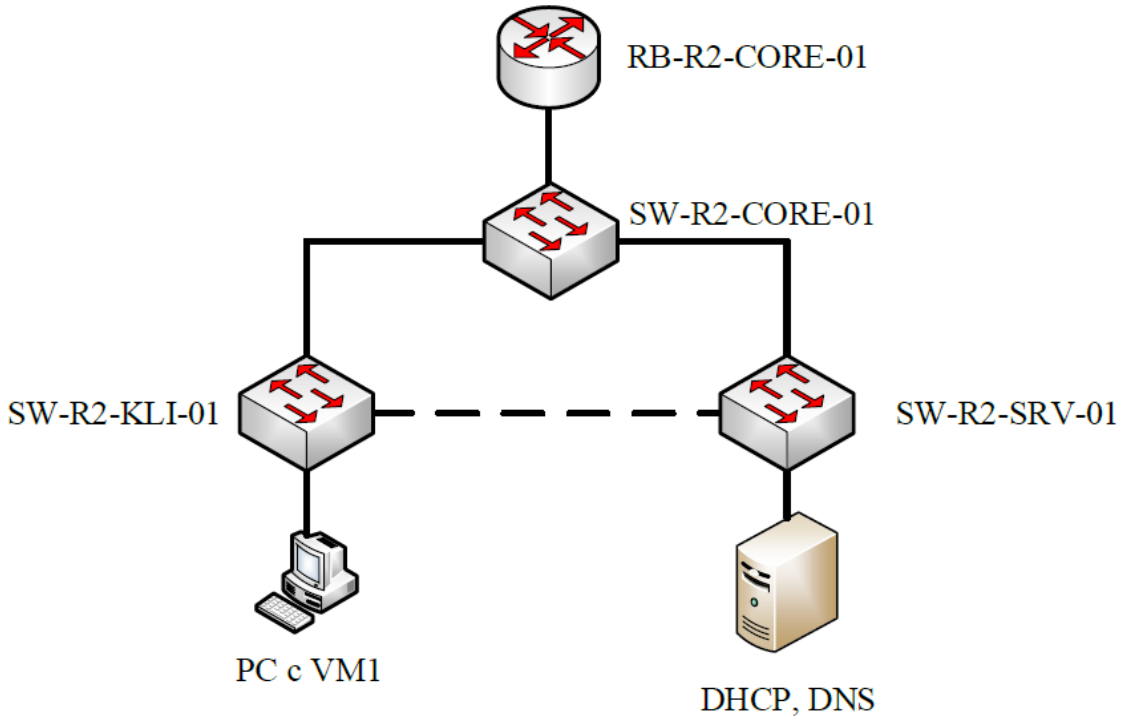

Рисунок 2 — Инфраструктура сети передачи данных без экспериментальных топологий

На диаграмме сети передачи данных показана реализация фрагмента пользователя и сервиса с использованием только двух коммутаторов. Затем они подключаются к «центральному» коммутатору L3, на интерфейсе которого IP-пакеты маршрутизируются между отдельными VLAN. Такая схема подразумевает требование доступности суб-каналов к коммутатору в яд-

ре сети, поэтому они образуют агрегированный канал, который обеспечит связь для фрагмента в случае отказа одной из пар, образующих логический канал. Уровень доступа как для пользовательского, так и для сервисного фрагмента состоит из двух соединенных между собой коммутаторов. Если один коммутатор используется для рабочих станций, а другой - только для серверных устройств, конфигурация обоих коммутаторов доступа значительно упрощается. Кроме того, можно применять другой уровень безопасности «глобально», то есть с областью действия, ко всем интерфейсам серверного коммутатора, чем в случае коммутатора, используемого для подключения рабочих станций, и серверов. Однако эта реализация предъявляет повышенные требования к доступности серверной инфраструктуры в сети передачи данных. Если сегмент сервера недоступен для рабочих станций, рабочие станции теряют доступ к службам домена DHCP, DNS и Active Directory. Недоступность этих служб не позволит всем пользователям рабочих станций работать, поскольку учетные записи пользователей в базе данных AD не могут быть аутентифицированы, если контроллер домена недоступен.

По этой причине серверная VLAN с VID 20 также передается на коммутатор клиентского доступа с помощью магистрального интерфейса. Интерфейс 41 выделен на этом коммутаторе для подключения ADC, вторичного DNS-сервера и вторичного DHCP-сервера. Это обеспечивает доступность основных сетевых услуг и возможность использования рабочих станций, даже если все устройства, включая сам коммутатор серверного сегмента будут отключены.

Подключение экспериментальных сетей. Описанная до сих пор топология не учитывает возможность подключения других устройств, в основном экспериментальных сетевых элементов, конфигурация которых обычно является предметом тестирования. Оригинальная конструкция обеспечивает доступность экспериментальных устройств с помощью коммутатора HP ProCurve 2650, на интерфейсе которого передаются тегированные кадры экспериментальных сетей VLAN между коммутаторами SW-R2-KLI-01, SWR2-SRV-01 и SW-R3-LAB-01. Из-за характера тестирования такая реализация очень неуместна. Используемый сервер виртуализации предлагает достаточное количество интерфейсов, которые можно подключать по мере необходи-

мости к коммутаторам доступа, чтобы обеспечить кратчайший сетевой путь между двумя напрямую взаимодействующими станциями.

К сожалению, на коммутаторе SW-R3-LAB-01 (модель HP ProCurve 2650) доступны только два интерфейса 1000BASET. По этой причине один интерфейс будет предназначен для передачи тегированных кадров между коммутатором SW-R2-KLI-01, соединяющим рабочие станции, а другой интерфейс - для прямого подключения сервера виртуализации. С помощью тегированных кадров кадры передаются между двумя коммутаторами, сопровождаемые соответствующим тегом в соответствии с принадлежностью станции к заданию тестирования. Соединение активных элементов и участвующих станций для связи в соответствии с потребностями лабораторных заданий показано, в соответствии с рисунком 3

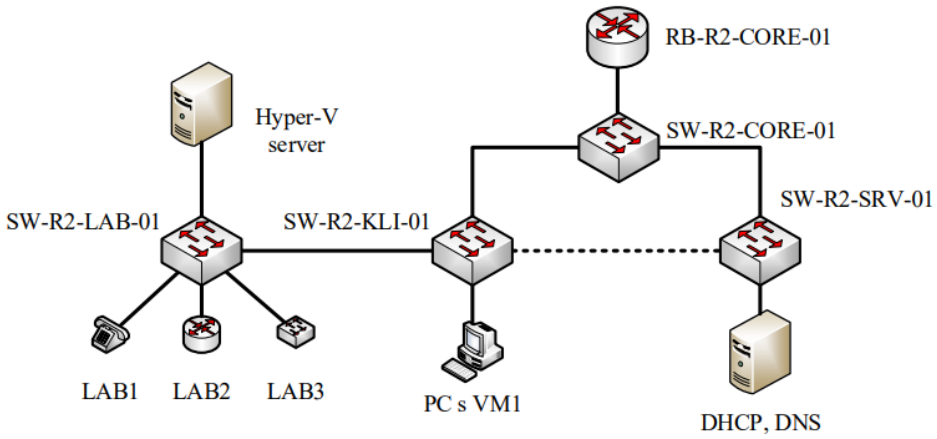

Рисунок 3 — Связь между компонентами лабораторного задания тестирования

Серверная инфраструктура. Основным элементом новой инфраструктуры серверного сегмента является коммутатор Zyxel XGS1910, который обеспечивает сетевой доступ ко всем физическим и виртуальным серверам. Это коммутатор, назначение которого намеренно зарезервировано только для подключения серверных устройств, взаимодействующих в недавно созданной виртуальной локальной сети с VID 20. Такая реализация выбрана с учетом повышенных требований к передаче данных между серверами (например, резервное копирование на общее хранилище, использование общего хранилища

кластером виртуализации). В определенной таким образом серверной подсети работают, в частности, следующие серверы:

- Два узла кластера виртуализации.
- Физический контроллер домена, DHCP и первичный DNS-сервер.
- Общее хранилище.
- Неиспользуемый сервер.

Поскольку службы и серверные системы Microsoft Windows Server в значительной степени были развернуты в старой версии 2008 R2, обновление (переход) на более свежую версию Windows Server происходит с переходом к новой концепции. Основная цель - более эффективное распределение серверных служб между доступными серверами и обеспечение устойчивости к отказам серверов, предоставляющих основные услуги, характерные для корпоративных сетей. По этой причине используется два сервера для формирования кластера виртуализации, который включает в себя резервный контроллер домена и выделенную станцию для управления сетевой инфраструктурой. Два узла кластера виртуализации обеспечивают High Availability для виртуального сервера, который способен запускать службы AD, DNS и DHCP. Все виртуальные станции для выполнения тестовыъ заданий обеспечиваются только одним узлом, и эти виртуальные машины не резервируются HA.

Хранилище данных. В лаборатории имеется запоминающее устройство с подключением к сети передачи данных. Это LenovoEMC™PX6-300d. Данное устройство имеет шесть внутренних отсеков для жестких дисков с интерфейсом SATA 6 Гбит/с и разъемы USB3.0 для подключения внешних устройств. Жесткие диски могут быть настроены для использования в дисковых массивах RAID 0, 1 и 5. Устройство также оснащено двумя сетевыми интерфейсами, которые поддерживают максимальную скорость до 1 Гбит/с и могут быть объединены в логический канал. Для лучшего доступа к устройству и его легкой идентификации в доменной структуре устройству присваивается имя SC5-32-NAS01 с IP-адресом 10.10.20.3 из диапазона 10.10.20.0/24. Кроме того, устройство хранения включено в доменную структуру Active Directory.

Инфраструктура виртуализации. Для сохранения привычек и легкой интеграции в существующую среду инфраструктура лаборатории будет расширена за счет совершенно нового узла кластера виртуализации, реализован-

ного с помощью Hyper-V. В качестве операционной системы хоста выбрана ОС Microsoft Windows Server 2016 Datacenter. Одним из критериев выбора здесь является требование простого управления платформой виртуализации и бесшовной интеграции в существующую среду, которая использует доменные службы Active Directory от Microsoft.

Обновление операционной системы серверов виртуализации приносит значительные преимущества, наиболее важными из которых являются новые режимы динамической памяти ВМ, новые сетевые службы ВМ (QoS, размещение общих дисков) и, наконец, возможность управления виртуальной машиной из Windows Powershell.

Работа AD, DNS и DHCP с высокой доступностью. С переходом на новую концепцию сети передачи данных и разделением ролей, установленных на доступных серверах, исчезла и роль альтернативного контроллера домена, который неоптимально функционировал на сервере виртуализации (не в ВМ). Поскольку в рамках защиты доменной структуры рекомендуется запускать как минимум два синхронизированных контроллера домена с функцией глобального каталога, устанавливается новая виртуальная машина SC5-32-DC03v с работающим датацентром MS Windows Server 2016. система. Далее виртуальная машина помещается в расположение смонтированного тома CSV и добавляется в качестве роли кластера.

Система мониторинга и резервное коипрование. Последняя часть работы связана с проектированием и реализацией системы мониторинга в сети передачи данных лаборатории. Кроме того, имеются варианты резервного копирования конфигураций сетевых элементов, немедленная доступность которых позволит администратору отслеживать изменения и даст более четкую ориентацию в их настройках. Вместе с возможностью наблюдения за текущим состоянием оборудования лаборатории это является очень полезным источником информации, и не только в случае решения ошибочных ситуаций.

Zabbix выбран в данной работе в основном из-за простоты администрирования и использования системы. Целью развертывания системы мониторинга является возможность мониторинга основной оперативной информации (доступность, использование, применение физических ресурсов), инвентаризации и, возможно, предоставление основных методик для локализации

возможных проблем. Система Zabbix предлагает несколько способов мониторинга и сбора данных с целевого устройства. Первым широко распространенным является сбор и передача данных с помощью протокола SNMP. Этот метод особенно подходит для активных сетевых элементов (коммутаторов и маршрутизаторов). Информация о сетевом элементе передается через так называемый SNMP-агент, который генерирует SNMP-сообщения и отправляет их на заранее настроенный адрес элемента мониторинга.

Резервное копирование конфигураций сетевых элементов. Большинство операционных систем, развернутых сегодня на сетевых элементах, также реализуют методы резервного копирования и передачи файлов конфигурации с помощью TFTP, FTP и т.д. Резервное копирование и передача конфигураций с помощью установленного клиента TFTP по-прежнему является предпочтительным выбором, даже с учетом уступающих функций безопасности TFTP, в основном из-за его простоты. Сетевые элементы, которые предлагают графический интерфейс, обычно предлагают возможность загрузки или восстановления конфигурации с помощью HTTP-передачи. Однако недостатком сохранения конфигураций из среды веб-браузера является меньшая возможность автоматизации этой задачи.

Рассмотрим последовательность задач, которая приводит к успешной загрузке файла конфигурации на сервер TFTP из резервной копии элемента. Терминальный доступ почти всегда требует аутентификации. Эта аутентификация может быть выполнена, например, путем ввода пароля для используемой учетной записи или аутентификации с помощью пары закрытый/открытый ключ. Для простоты и ясности используется метод аутентификации с помощью пароля. После входа в устройство требуется переход в привилегированный режим. Затем пользователь получает право читать текущие конфигурации (часто называемые running-config или startup-config). Затем они могут быть загружены с помощью упомянутого выше TFTP-клиента. Когда процесс резервного копирования завершен, администратор выходит из системы и разрывает соединение. Для автоматизации этого процесса на устройствах Cisco IOS используется следующая последовательность команд.

Заключение. Дипломная работа посвящена разработке и описанию реализации совершенно новой сети передачи данных, которая реализуется в

одной из лабораторий организации. В этой сети упор сделан на надежность и эффективное использование сети передачи данных для нужд преподавания предметов с упором на изучение передовых сетевых технологий. Работа начинается с теоретического анализа практик, которые обычно используются сегодня при создании сетей передачи данных, и оцениваются возможности их внедрения и реализации в сети передачи данных лаборатории.

При проектировании новой сети передачи данных идет опора в первую очередь на знания пользователя, а затем на знания администратора существующей инфраструктуры. Этот анализ кратко обсуждается в главе **??**. При проектировании идет концентрация в основном на недостатки исходной инфраструктуры, к которым относится снижение безопасности, структуру сети передачи данных и ее недостаточную связность. Эти выводы заставляют заново оценить возможности управления такой сетью, надзора за самими элементами и оценки эффективности использования оборудования лаборатории.

Результаты исследования показывают, что оптимизация лабораторной сетевой среды имеет значительное значение для успешного проведения исследований и тестирования в области сетей передачи данных. В работе были выявлены узкие места, проблемы и недостатки существующей сетевой инфраструктуры, а также предложены и реализованы оптимальные решения для улучшения производительности и надежности. Были проведены эксперименты, которые позволили оценить эффективность предложенных изменений и их влияние на процессы исследования и тестирования сетевых технологий.