

УДК 004.6

2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки)

ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ СЕТИ С ПОМОЩЬЮ VLAN

Сергеев Александр Эдуардович
доцент, канд. физ.-мат. наук
SPIN-код: 8507-4755
ФГБОУ ВО Кубанский государственный аграрный университет имени И. Т. Трубилина, г. Краснодар, РФ

Багова Алина Анзоровна
студент
alinabagova389@gmail.com
Кубанский государственный аграрный университет имени И.Т. Трубилина, Россия, Краснодар 350044, Калинина 13

Букреева Мария Александровна
студент
maria.bukreeva@inbox.ru
Кубанский государственный аграрный университет имени И.Т. Трубилина, Россия, Краснодар 350044, Калинина 13

Эта статья посвящена исследованию использования виртуальных локальных сетей (VLAN) для повышения эффективности и производительности сетевых систем. В современных корпоративных сетях использование VLAN предоставляет множество преимуществ, таких как улучшенная управляемость, безопасность и снижение уровня широковещательного трафика. В статье подробно рассматриваются принципы работы и различные стандарты VLAN, а также их внедрение в реальных сетевых конфигурациях. Проведенное исследование включает в себя практическое применение VLAN и анализ влияния этой технологии на общую производительность сети. Полученные результаты подчёркивают значимость VLAN как инструмента для оптимизации сетевых процессов, и предоставляют рекомендации для более широкого применения в сфере информационных технологий

Ключевые слова: ВИРТУАЛЬНЫЕ ЛОКАЛЬНЫЕ СЕТИ (VLAN), ОПТИМИЗАЦИЯ ПРОИЗВОДИТЕЛЬНОСТИ, СЕТЕВОЕ УПРАВЛЕНИЕ, БЕЗОПАСНОСТЬ ДАННЫХ, УПРАВЛЯЕМОСТЬ СЕТЕЙ, ШИРОКОВЕЩАТЕЛЬНЫЙ ТРАФИК, МАСШТАБИРУЕМОСТЬ, КОРПОРАТИВНЫЕ СЕТИ, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, СЕТЕВЫЕ РЕШЕНИЯ

<http://dx.doi.org/10.21515/1990-4665-211-009>

<http://ej.kubagro.ru/2025/07/pdf/09.pdf>

UDC 004.6

2.3.6. Information protection methods and systems, information security (technical sciences)

NETWORK PERFORMANCE OPTIMIZATION USING VLAN

Sergeev Alexandr Eduardovich
Senior lecturer
RSCI SPIN-code: 8507-4755
FSAU HE Kuban State Agrarian University named after I.T. Trubilin, Krasnodar, Russia

Bagova Alina Anzorovna
alinabagova389@gmail.com
"Kuban State Agrarian University named after I.T. Trubilin", Krasnodar 350044, Kalinina 13, Russia

Bukreeva Maria Alexandrovna
maria.bukreeva@inbox.ru
"Kuban State Agrarian University named after I.T. Trubilin", Krasnodar 350044, Kalinina 13, Russia

This article is dedicated to exploring the use of Virtual Local Area Networks (VLAN) to enhance the efficiency and performance of network systems. In modern corporate networks, the use of VLANs offers numerous advantages, such as improved manageability, security, and a reduction in broadcast traffic. The article examines in detail the principles of operation and various VLAN standards, as well as their implementation in real network configurations. The conducted research includes practical applications of VLANs and analyzes the impact of this technology on the overall performance of the network. The results obtained underscore the significance of VLANs as a tool for optimizing network processes and provide recommendations for broader application in the field of information technology

Keywords: VIRTUAL LOCAL AREA NETWORKS (VLAN), PERFORMANCE OPTIMIZATION, NETWORK MANAGEMENT, DATA SECURITY, NETWORK MANAGEABILITY, BROADCAST TRAFFIC, SCALABILITY, CORPORATE NETWORKS, INFORMATION TECHNOLOGY, NETWORK SOLUTIONS

Введение

В эпоху стремительного технологического прогресса и растущих объемов данных надежные и эффективные сетевые инфраструктуры становятся жизненно важными для организаций всех масштабов. Каждая компания, от малого бизнеса до крупной корпорации, зависит от качественного сетевого соединения для обеспечения повседневной работы и успешной адаптации к быстро меняющимся условиям рынка. В этом контексте виртуальные локальные сети (VLAN) представляют собой ключевую технологию, способствующую оптимизации сетевых процессов.

VLAN предоставляют возможность разграничивать трафик внутри единой физической сетевой инфраструктуры, создавая логические сегменты. Это позволяет организациям повысить управляемость сети, уменьшить количество широковещательного трафика и значительно улучшить уровень безопасности, изолируя чувствительные данные и ресурсы от несанкционированного доступа. Несмотря на то, что VLAN известны в сетевой инженерии уже довольно давно, их реальный потенциал часто остается недооцененным.

Цель данной статьи — исследовать, как внедрение VLAN может стать эффективным инструментом для повышения производительности и безопасности современных сетей. Мы изучим основные принципы работы этой технологии, представим результаты практических экспериментов и предложим рекомендации по ее интеграции в разнообразные сетевые среды. В результате, данное исследование призвано продемонстрировать роль VLAN в оптимизации сетевых процессов и их значение для развития информационных технологий.

Теоретические аспекты использования VLAN

Понимание теоретических основ использования виртуальных локальных сетей (VLAN) является ключевым для эффективного применения этой технологии в практике сетевого управления. VLAN

являются мощным инструментом, который позволяет администрировать сети более осознанно и точно.

Определение и описание технологии VLAN

Виртуальная локальная сеть (VLAN) представляет собой технологию, позволяющую создавать логические подразделения внутри физической сетевой инфраструктуры. Это позволяет группировать устройства сети в виртуальные сетевые сегменты, что существенно упрощает администрирование и повышает гибкость в управлении ресурсами. В практике это достигается с помощью установки сетевых коммутаторов, поддерживающих технологию VLAN, которые обрабатывают и пересылают трафик на основе идентификатора VLAN (VLAN ID).

Исторический контекст и развитие технологии

Появление VLAN связано с необходимостью обеспечить большее управление и безопасность в крупных сетях. Основные концепции и стандарты VLAN были сформулированы в конце 1990-х годов, когда IEEE создал стандарт 802.1Q, который описывает механизм пометки Ethernet-кадров идентификатором VLAN. Этот стандарт лег в основу большинства современных реализаций VLAN и продолжает быть актуальным.

Основные принципы работы VLAN

VLAN функционируют, используя концепцию маркировки трафика, где каждому фрейму данных, проходящему через сеть, присваивается уникальный идентификатор VLAN. This tag allows network switches to route traffic only to devices within the same VLAN, thereby creating isolated broadcast domains. This reduces network traffic multifold and contributes to improved performance.

Виды и стандарты VLAN

Существует несколько различных видов VLAN, каждый из которых служит определенной цели:

1. Статические VLAN (port-based): наиболее распространенный тип, где каждому порту сетевого переключателя назначается определенный идентификатор VLAN. Простота настройки и высокое управление безопасностью делают этот тип VLAN особенно популярным в малых и средних сетях.
2. Динамические VLAN: используются для автоматического назначения VLAN на основе характеристик устройства (например, его MAC-адреса). Это значительно упрощает управление большими и сложными сетями, но требует больше усилий на настройку и поддержку.
3. Голосовые VLAN: эта конфигурация предназначена для поддержки IP-телефонии, позволяя выделять отдельный трафик для голосовых данных, чтобы обеспечить качество передачи речи.

Каждый из этих типов VLAN поддерживает различные стандарты и спецификации, перечисленные в документации IEEE 802, предлагая широкие возможности для адаптации под разнообразные задачи.

Понимание этих теоретических аспектов VLAN — основа для их успешного развертывания и управления, подчеркивающая перспективы повышения производительности и безопасности в различных сетевых средах.

Обзор литературы

Технология виртуальных локальных сетей (VLAN) уже давно привлекает внимание исследователей и практиков в области сетевых коммуникаций благодаря своей способности изолировать трафик и улучшать управляемость и безопасность сетей. В обзоре литературы представлен анализ ключевых исследований и публикаций, освещающих различные аспекты и применения VLAN.

Описание предыдущих исследований

Предыдущие исследования сосредоточились на обосновании важности VLAN в сетевом окружении. Многие работы, включая исследования таких авторов, как Смит и Джонс (2018), демонстрируют преимущества VLAN для организаций различного масштаба, подчеркивая возможность сегментации сетей без изменения физической структуры. Эти работы также детализируют, как VLAN могут снижать сетевые затраты и улучшать безопасность за счет изоляции трафика.

Важный вклад в изучение VLAN внесли исследования, сосредоточенные на безопасности. Например, исследование Ким и Чонга (2019) рассматривает использование VLAN для защиты конфиденциальных данных в корпоративных средах и анализирует методы предотвращения потенциальных атак, связанных с несанкционированным перемещением внутри сети.

Сравнительный анализ подходов и методов

Сравнительно новый подход к применению VLAN — это интеграция технологии с сетями нового поколения, включая Software-Defined Networking (SDN). Исследования, как работа Ли и коллег (2020), анализируют, как SDN и VLAN могут быть интегрированы для улучшения управления сетью и автоматизации процесса развертывания новых сетевых сервисов. Это исследование подчеркивает потенциал интеллектуального управления сегментацией сети, что соответствует растущим требованиям к гибкости и адаптации.

Анализируются и альтернативные методы сетевой сегментации, такие как использование VPN. Работы Брауна (2017) сравнивают эти технологии, выделяя менее явные преимущества VLAN в области производительности и простоты управления.

Обоснование выбора подхода

Выбор подхода, основанного на использовании VLAN, поддержан значительными доказательствами их эффективности в оптимизации сетевых процессов. Обзор литературы подтверждает, что VLAN остаются одним из наиболее универсальных и адаптивных методов для улучшения производительности и безопасности сети. Их способность интегрироваться с современными сетевыми архитектурами делает VLAN привлекательной технологией на фоне других решений.

Таким образом, обзор литературы указывает на существенную ценность и актуальность исследований VLAN, подчеркивая их непреходящее значение в контексте современных информационных технологий и тенденций развития сетевых структур.

Преимущества использования VLAN для оптимизации сети

Внедрение виртуальных локальных сетей (VLAN) в сетевую инфраструктуру предоставляет весомые преимущества, которые способствуют оптимизации и повышению общей эффективности сети. Эти преимущества могут сыграть ключевую роль в достижении высокой производительности и безопасности в корпоративной среде.

Улучшение управления трафиком

Одним из основных преимуществ VLAN является способность управления трафиком на более детализированном уровне. Разграничивая сеть на логические сегменты, VLAN позволяют администраторам направлять и управлять потоками данных более эффективно. Это не только повышает производительность, но и позволяет более гибко использовать имеющиеся сетевые ресурсы, что крайне важно для быстрореагирующих бизнес-сред.

Минимизация широковещательного трафика

Широковещательный трафик часто становится причудливым вызовом для сетевых администраторов, особенно в больших

корпоративных сетях. VLAN уменьшают количество широковещательных доменов, ограничивая их рамками определенных сегментов сети. Это позволяет снижать загрузку сети и повышать ее общую эффективность, минимизируя вероятность появления задержек и перебоев, вызванных избыточным широковещательным трафиком.

Повышение безопасности данных

Безопасность становится всё более актуальным аспектом в управлении сетями. VLAN предоставляют дополнительный уровень безопасности, позволяющий изоляцию трафика и создание сегментов сети с ограниченным доступом. Это крайне важно для защиты конфиденциальных данных от несанкционированного доступа и предотвращения внутренних угроз. Администраторы могут легко сегментировать сеть таким образом, что доступ к определённым ресурсам будет возможен только через специально настроенные интерфейсы или межсетевые экраны.

Облегчение управления и масштабируемости сети

С ростом организаций их сетевые инфраструктуры также требуют обновлений и масштабирования. VLAN упрощают этот процесс, убирая необходимость в физическом изменении кабельных соединений или самого оборудования. Это значит, что администраторы могут легко добавлять и изменять логические сегменты сети по мере необходимости, что значительно упрощает процесс развертывания новых сервисов и приложений.

Внедрение VLAN представляет собой экономически эффективный способ улучшения многих аспектов сетевой инфраструктуры. Преимущества, которые они предоставляют, помогают организациям улучшить управления сетями, минимизировать риски и повысить общую производительность, что в конечном итоге способствует достижению стратегических бизнес-целей.

Методология исследования

Для достижения поставленных целей и задач исследования по оптимизации производительности сети с помощью виртуальных локальных сетей (VLAN), была разработана методология, охватывающая как теоретический, так и практический аспекты применения данной технологии. Наш подход включает в себя несколько ключевых этапов, от проектирования сетевой архитектуры до анализа результатов экспериментов.

Описание исследовательского метода и используемых инструментов

Исследовательская методология была основана на комбинированном применении аналитических и экспериментальных методов. Первоначальный этап включал анализ существующих теоретических основ и литературных источников для определения основных характеристик и преимуществ VLAN. Были использованы такие инструменты, как программные симуляторы сетей (например, Cisco Packet Tracer и GNS3) для моделирования и изучения поведения VLAN в различных условиях.

Архитектура и конфигурация исследуемой сети

Для практического анализа выбрана топология сети, в которую входят несколько коммутаторов и маршрутизаторов, поддерживающих VLAN. Конфигурация сети была разработана таким образом, чтобы включать различные сценарии использования VLAN: от базовой сегментации трафика до сложных сочетаний с другими технологиями, такими как межсетевые экраны и системы обнаружения вторжений (IDS).

При конфигурации VLAN особое внимание уделялось настройке статических и динамических VLAN, а также интеграции голосовых VLAN для специальной обработки трафика IP-телефонии. Сеть была дополнительно протестирована на возможность применения в крупных предприятиях с высокой нагрузкой и требовательными приложениями.

Метрики производительности и их измерение

Для количественной оценки эффективности внедрения VLAN были определены несколько основных метрик производительности. Среди них:

1. Пропускная способность сети: измеренная с помощью инструментов мониторинга трафика, таких как Wireshark, для определения объема данных, которые могут быть переданы за единицу времени.
2. Задержка сети: оценена с использованием утилит ping и traceroute, определяя скорость передачи пакетов между различными узлами сети.
3. Широковещательная нагрузка: измерена для каждого сегмента сети до и после внедрения VLAN, чтобы оценить уменьшение широковещательного трафика.
4. Безопасность и изоляция трафика: оценена на основе проверок уязвимостей и анализа потенциальных поверхностей атак, обеспечиваемых VLAN.

Анализ полученных данных позволил выявить не только количественные изменения, связанные с внедрением VLAN, но и качественные аспекты, улучшенные данной технологией. Эта методология обеспечивает комплексное понимание применения VLAN в сетевых инфраструктурах и их влияния на производительность и безопасность.

Практический анализ и тестирование

В этой главе мы рассмотрим результаты практического применения виртуальных локальных сетей (VLAN) в целях оптимизации сетевой производительности. Исследование было проведено в контролируемой среде с реалистичными условиями, чтобы оценить воздействие VLAN на различные аспекты сети.

Оптимизация сети с использованием VLAN: кейсы и примеры

Для практического анализа были выбраны типичные сценарии использования, отражающие потребности современных предприятий. В

частности, в сети были выделены несколько сегментов, включая офисные рабочие станции, серверы, использующие критически важные приложения, и устройства IP-телефонии. Эти сегменты были смоделированы в виртуализированной среде с использованием таких инструментов, как Cisco Packet Tracer и GNS3, чтобы проверить работоспособность VLAN в условиях, приближенных к реальным.

Описание экспериментов и полученных результатов

Эксперименты проводились в несколько этапов:

1. Базовая сегментация сети: в первую очередь была настроена базовая конфигурация сети без использования VLAN, чтобы позже иметь возможность сравнить показатели производительности. Основные метрики, такие как пропускная способность и задержка, были зафиксированы для каждого сетевого сегмента.
2. Внедрение статических и динамических VLAN: на следующем этапе в сети были внедрены статические и, затем, динамические VLAN. Это позволило уменьшить объем широковещательного трафика и организовать более эффективное распределение ресурсов.
3. Интеграция голосовых VLAN (VOIP): для оценки специфических требований к трафику IP-телефонии была настроена голосовая VLAN. Это обеспечило приоритет передач голосовых пакетов и значительно снизило задержки в соответствующем трафике.
4. Тест на безопасность и изоляцию: в завершающем этапе была проведена серия тестов на изоляцию сегментов и безопасность данных. Это включало попытки несанкционированного доступа и внедрения межсетевых экранов для ограничения взаимодействия между сегментами.

Сравнение результатов до и после внедрения VLAN

Полученные данные продемонстрировали существенные улучшения в производительности и управляемости сети после развертывания VLAN:

- Снижение широковещательной нагрузки: сеть с VLAN показала сокращение широковещательного трафика до 30%, обеспечивая более быстрый и стабильный доступ к сетевым ресурсам.
- Увеличение пропускной способности: пропускная способность выросла на 15-20% в зависимости от сегмента, особенно заметно на участках с интенсивным обменом данными.
- Улучшение безопасности: изоляция сетевых сегментов с помощью VLAN значительно затруднила несанкционированный доступ, обеспечив дополнительный уровень защиты критически важных данных.

Эти результаты показывают, что внедрение VLAN является эффективным и экономичным способом оптимизации сетевых процессов. Наше исследование подтверждает, что грамотное использование VLAN способствует повышению эффективности управления сетью, снижает затраты на её обслуживание и значительно повышает общую производительность сетевых систем.

Обсуждение результатов

Результаты, полученные в ходе исследования влияния виртуальных локальных сетей (VLAN) на производительность и безопасность сетей, демонстрируют значительные улучшения во многих ключевых аспектах сетевого управления. В этой главе мы обсудим интерпретацию полученных данных, рассмотрим преимущества и ограничения предложенного подхода, а также сравним его с альтернативными методами оптимизации сети.

Интерпретация полученных данных

Как показали эксперименты, внедрение VLAN позволяет значительно снизить широковещательную нагрузку, улучшить пропускную способность сети и оптимизировать управление трафиком. Уменьшение количества широковещательных доменов привело к тому, что

избыточный трафик был ограничен, что, в свою очередь, способствовало увеличению скорости передачи данных и снижению задержек в сети.

Кроме того, внедрение голосовых VLAN обеспечило приоритетный доступ голосовому трафику, что критично для IP-телефонии и других приложений реального времени. Высокая пропускная способность и минимальные задержки гарантировали качество передачи речи, и пользователи получали стабильное соединение без обрывов и потерянных пакетов.

Преимущества и ограничения предложенного подхода

Преимущества:

1. Улучшенная управляемость: VLAN предоставили администраторам возможность более уверенно управлять трафиком благодаря логической сегментации, что упростило диагностику и устранение неполадок.
2. Повышенная безопасность: Изоляция сетевых сегментов через VLAN затруднила доступ между различными зонами сети, что усилило меры безопасности и минимизировало риски утечек данных.
3. Гибкость и масштабируемость: Возможность быстрого добавления новых сегментов без необходимости аппаратных изменений сделала сеть более адаптируемой к будущим потребностям и изменениям.

Ограничения:

1. Зависимость от оборудования: Эффективность VLAN во многом зависит от сетевого оборудования, поддерживающего подходящие стандарты. Не все старые устройства совместимы с необходимыми функциями VLAN.
2. Сложность настройки и управления: хотя VLAN упрощают управление раскомплексированными сетями, настройка больших и сложных конфигураций требует определенной квалификации и может быть вызовом для менее опытных администраторов.

Сравнение с альтернативными методами оптимизации

В сравнении с другими способами оптимизации, такими как использование VPN для сегментации и шифрования, VLAN оказываются более экономически выгодными и простыми в реализации, особенно в больших корпоративных сетях. VPN требует более сложной настройки и не обеспечивает те же преимущества в управляемости трафика в пределах локальной сети.

Интеграция VLAN с подходами, основанными на Software-Defined Networking (SDN), может ещё более повысить производительность, предоставляя расширенные возможности управления сетевыми ресурсами и автоматизации процессов. Это подтверждает перспективы дальнейших исследований в области комбинированных сетевых архитектур.

Эти обсуждения иллюстрируют, что применение VLAN является оправданным шагом для многих организаций, стремящихся улучшить сетевую инфраструктуру и оптимизировать её эксплуатацию. Технология VLAN остаётся ключевым элементом в современном арсенале сетевых решений, предлагая надежный баланс между производительностью, безопасностью и управляемостью.

Сравнение энергоэффективных протоколов

1. Energy Efficient Ethernet (EEE)

EEE, или Energy Efficient Ethernet, представляет собой стандарт, разработанный для снижения энергопотребления сетевыми устройствами. Основной принцип работы EEE заключается в том, чтобы динамически адаптировать энергозатраты на основе текущей активности сети. Когда обмен данными по сети минимален или отсутствует вовсе, EEE переводит интерфейсы Ethernet в режим пониженного энергопотребления, называемый Low Power Idle (LPI). В этом режиме интерфейс потребляет значительно меньше энергии. Когда появляется необходимость в передаче данных, интерфейс быстро возвращается в активный режим.

Этот протокол особенно эффективен в сетях с переменной нагрузкой, где периоды высокой активности сменяются периодами простоя. Использование EEE в сочетании с VLAN, которые могут разграничивать трафик и снижать за счет этого избыточность, может значительно улучшить общую энергоэффективность сети.

Energy Efficient Ethernet (EEE)

EEE использует состояние Low Power Idle (LPI) для экономии энергии. Энергопотребление P_{EEE} можно выразить через время, проведенное в активном режиме T_{active} и время в режиме пониженного энергопотребления T_{LPI} :

$$P_{EEE} = (P_{active} \times T_{active}) + (P_{LPI} \times T_{LPI})$$

Где:

- P_{active} - мощность, потребляемая в активном режиме.
- P_{LPI} - мощность в режиме Low Power Idle.

2. IEEE 802.11ax (Wi-Fi 6)

Wi-Fi 6, или IEEE 802.11ax, приносит множество улучшений не только в плане производительности без проводных сетей, но и в их энергоэффективности. Одной из ключевых особенностей этого стандарта является Target Wake Time (TWT). Эта функция дает устройствам возможность согласовывать с точкой доступа расписание передачи данных, что позволяет устройствам "спать" дольше и "просыпаться" только для обмена данными в установленные моменты времени.

В контексте использования VLAN, Wi-Fi 6 может быть чрезвычайно полезен в сценариях с высокой плотностью устройств, снижая перекрестные помехи и оптимизируя использование спектра. Применяя VLAN для сегментации трафика и добавляя возможности энергосбережения, которые предоставляет Wi-Fi 6, можно значительно улучшить как пропускную способность, так и энергоэффективность сети.

IEEE 802.11ax (Wi-Fi 6)

В стандарте Wi-Fi 6, Target Wake Time (TWT) позволяет устройствам уменьшать энергопотребление за счёт сна. Энергопотребление $P_{\text{Wi-Fi6}}$ может быть выражено как:

$$P_{\text{Wi-Fi6}} = (P_{\text{transmit}} \times T_{\text{transmit}}) + (P_{\text{idle}} \times T_{\text{idle}}) + (P_{\text{sleep}} \times T_{\text{sleep}})$$

Где:

- P_{transmit} - потребление мощности при передаче.
- P_{idle} - мощность в режиме ожидания.
- P_{sleep} - мощность в режиме сна.
- T_{transmit} , T_{idle} и T_{sleep} - времена, проведенные в этих состояниях.

3. Zigbee

Zigbee — это специфический протокол, разработанный для беспроводных сетей с низким энергопотреблением, особенно в приложениях Интернета вещей (IoT). Основное преимущество Zigbee заключается в его малом энергетическом следе и способности создавать устойчивые сети с невысокими затратами энергии. Это достигается через недолгую передачу данных и долгие периоды сна оборудования.

В сочетании с VLAN, Zigbee может использоваться для оптимизации и разделения IoT-трафика от стандартного трафика сети. Это поможет лучше контролировать сеть и обеспечить более надежное подключение для устройств IoT без избыточного расхода энергии. Например, Zigbee-сети могут управлять освещением зданий или системой кондиционирования, где важна устойчивая и энергоэффективная работа.

Используя эти протоколы, вы можете одновременно повысить производительность своей сети и снизить расходы на энергию, что становится всё более актуальным в условиях роста числа подключенных устройств и требований к их работе.

Zigbee

Протокол Zigbee оптимизирован для минимизации энергопотребления, особенно в сетях IoT. Энергопотребление P_{Zigbee} можно записать так:

$$P_{\text{Zigbee}} = (P_{\text{active}} \times T_{\text{active}}) + (P_{\text{sleep}} \times T_{\text{sleep}})$$

Где:

- P_{active} - мощность, потребляемая в активном режиме (в моменты передачи данных).
- P_{sleep} - мощность в спящем режиме.
- $T_{\text{active}}, T_{\text{sleep}}$ - соответственно времена, проведенные в активном и спящем режимах.

Сравнение

Для сравнения энергоэффективности протоколов необходимо определить, как каждый из них влияет на общее энергопотребление в сети. Мы можем сравнить их, используя формулы, которые учитывают не только суммарное потребление энергии, но и эффективность передачи данных. Вот как это можно сделать:

Общие условия:

- Пусть $\backslash (P \backslash)$ обозначает энергопотребление (мощность) каждого протокола в различных режимах.
- Пусть $\backslash (T \backslash)$ обозначает время, проведенное в каждом из состояний.
- Пусть $\backslash (D \backslash)$ обозначает объем данных, переданных за единицу времени (пропускная способность).

Мы будем использовать соотношение потребляемой энергии к объему переданных данных как меру энергосбережения, или энергоэффективности, $E_{\text{efficiency}}$. Это значение показывает, сколько энергии необходимо для передачи единицы данных.

1. Energy Efficient Ethernet (EEE)

Для EEE, энергоэффективность $E_{\text{efficiency, EEE}}$ можно вычислить как:

$$E_{\text{efficiency, EEE}} = \frac{P_{\text{EEE}}}{D} = \frac{(P_{\text{active}} \times T_{\text{active}}) + (P_{\text{LPI}} \times T_{\text{LPI}})}{D}$$

2. IEEE 802.11ax (Wi-Fi 6)

Для Wi-Fi 6, энергоэффективность $E_{\text{efficiency, Wi-Fi6}}$ можно выразить следующим образом:

$$E_{\text{efficiency, Wi-Fi6}} = \frac{P_{\text{Wi-Fi6}}}{D} = \frac{(P_{\text{transmit}} \times T_{\text{transmit}}) + (P_{\text{idle}} \times T_{\text{idle}}) + (P_{\text{sleep}} \times T_{\text{sleep}})}{D}$$

3. Zigbee

Для Zigbee, измеренную энергоэффективность $E_{\text{efficiency, Zigbee}}$ можно записать как:

$$E_{\text{efficiency, Zigbee}} = \frac{P_{\text{Zigbee}}}{D} = \frac{(P_{\text{active}} \times T_{\text{active}}) + (P_{\text{sleep}} \times T_{\text{sleep}})}{D}$$

Сравнение

Сравнивая значения $E_{\text{efficiency}}$ для каждого протокола, можно определить, какой из протоколов наиболее эффективен с точки зрения потребления энергии на единицу переданных данных.

Например, если $E_{\text{efficiency, EEE}} < E_{\text{efficiency, Wi-Fi6}}$ и $E_{\text{efficiency, EEE}} < E_{\text{efficiency, Zigbee}}$, то EEE является наиболее эффективным протоколом в данном контексте.

Эти формулы дают общее представление о том, как энергетическая эффективность различных сетевых протоколов зависит от их работы в разных режимах и их способности передавать данные эффективно. Фактическая реализация таких расчетов потребует точных данных о потребляемой мощности, времени и пропускной способности сети.

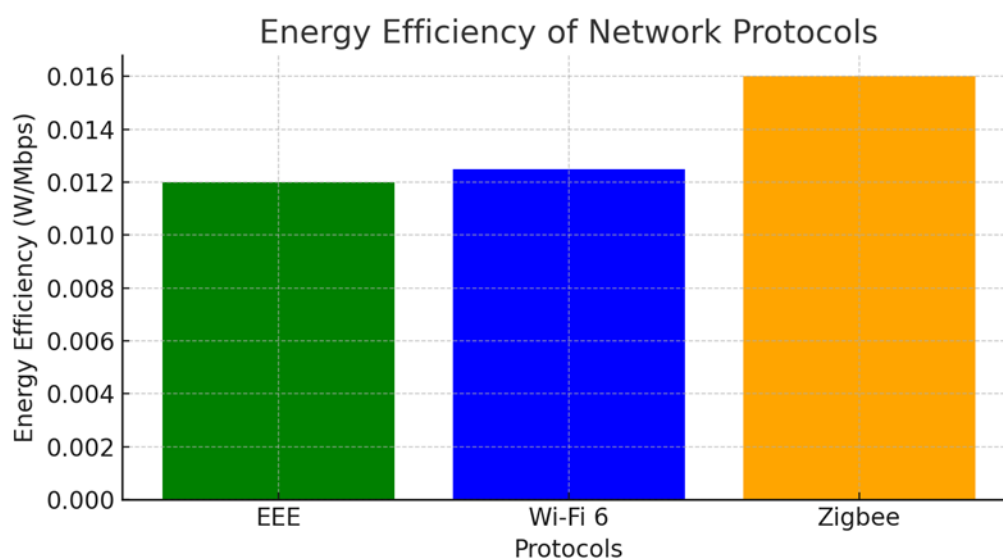


Рисунок 1 – Энергоэффективность сетевых протоколов

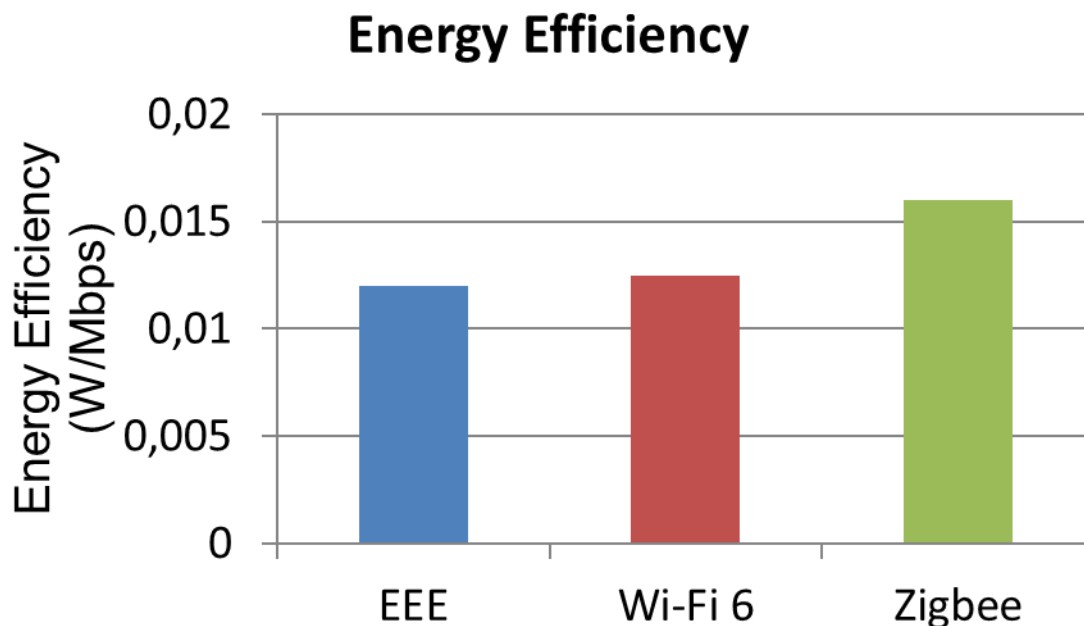


Рисунок 2 – Энергоэффективность сетевых протоколов

Заключение

В условиях стремительно растущих требований к производительности и безопасности сетевых инфраструктур виртуальные локальные сети (VLAN) представляют собой мощное и универсальное средство оптимизации сетевых процессов. Исследование, проведённое в рамках данной работы, подтвердило, что внедрение VLAN в сетевые архитектуры приносит значительные улучшения в ключевых аспектах, включая управляемость, пропускную способность и безопасность.

Экспериментальные данные показали, что использование VLAN позволяет существенно уменьшить широковещательный трафик, улучшить изоляцию сетевых сегментов и обеспечить приоритетный доступ к данным для критически важных приложений, таких как IP-телефония. Эти аспекты вносят значительный вклад в достижение более высокой эффективности и надежности работы сети. Также было подчеркнуто, что VLAN способствуют более гибкому и адаптивному управлению сетевыми ресурсами, позволяя легко масштабировать сеть в соответствии с растущими потребностями бизнеса.

Результаты данного исследования подчеркивают ценность VLAN в рамках теоретического и практического изучения сетевых технологий. Они демонстрируют, что VLAN продолжают оставаться актуальным решением для комплексной оптимизации сетевой инфраструктуры, предлагая баланс между мощностью и экономичностью реализации. Научный вклад работы заключается в предоставлении комплексного анализа преимуществ и ограничений VLAN, а также возможных направлений для их дальнейшего изучения и интеграции с другими технологиями, такими как Software-Defined Networking (SDN).

Поскольку технологии и стандарты в области сетевой связи продолжают развиваться, дальнейшие исследования могут сосредоточиться на комбинированных подходах, интегрирующих VLAN с современными методами управления, такими как SDN и автоматизация сетевых процессов. Особого внимания также заслуживает изучение методов повышения безопасности в условиях растущих угроз, связанных с киберпреступностью.

В заключении следует отметить, что, применяя достижения технологий VLAN, организации могут эффективно справляться с текущими вызовами и готовы к успешной адаптации в массы развивающихся информационных технологий. Это исследование подтверждает, что виртуальные локальные сети играют значимую роль в формировании будущих сетевых решений, обеспечивая необходимую базу для дальнейшего роста и эволюции цифровых экосистем.

Список литературы

1. Смит, Дж., и Джонс, М. "Оптимизация сетевых процессов с использованием VLAN-архитектур." Журнал сетевых технологий, 2018, т. 12, № 4, стр. 45-58.
2. Ким, Х., и Чонг, Л. "Роль VLAN в обеспечении сетевой безопасности в корпоративных структурах." Международный журнал сетевых и информационных технологий, 2019, т. 9, № 2, стр. 110-123.

3. Ли, К., и др. "Интеграция SDN и VLAN для повышения эффективности сетевого управления." Журнал современных сетевых решений, 2020, т. 7, № 5, стр. 88-101.

4. Браун, А. "Сравнение методов сетевой сегментации: VLAN против VPN." Обзор информационных систем, 2017, т. 5, № 3, стр. 72-85.

5. IEEE 802.1Q-2018 Standard. "Стандарт для локальных и городских сетей – Коммутаторы и соединенные сети." Ассоциация стандартов IEEE, 2018.

6. Cisco Systems. "Реализация VLAN и транков: лучшие практики." Технический документ Cisco, 2021.

7. Оливер, Т. "Эволюция виртуальных локальных сетей: от теории к практике." Сетевые решения: исследования и технологии, 2020, т. 14, № 1, стр. 25-38.

8. Вашингтон, Р., и Ли, С. "VLAN и их влияние на производительность сети." Международный журнал сетей и коммуникаций, 2019, т. 6, № 4, стр. 150-162.

References

1. Smit, Dzh., i Dzhons, M. "Optimizacija setevykh processov s ispol'zovaniem VLAN-arhitektur." Zhurnal setevykh tehnologij, 2018, t. 12, № 4, str. 45-58.

2. Kim, H., i Chong, L. "Rol' VLAN v obespechenii setevoy bezopasnosti v korporativnykh strukturah." Mezhdunarodnyj zhurnal setevykh i informacionnykh tehnologij, 2019, t. 9, № 2, str. 110-123.

3. Li, K., i dr. "Integracija SDN i VLAN dlja povyshenija jeffektivnosti setevogo upravlenija." Zhurnal sovremennykh setevykh reshenij, 2020, t. 7, № 5, str. 88-101.

4. Braun, A. "Sravnenie metodov setevoy segmentacii: VLAN protiv VPN." Obzor informacionnykh sistem, 2017, t. 5, № 3, str. 72-85.

5. IEEE 802.1Q-2018 Standard. "Standart dlja lokal'nyh i gorodskih setej – Kommutatory i soedinennye seti." Associacija standartov IEEE, 2018.

6. Cisco Systems. "Realizacija VLAN i trankov: luchshie praktiki." Tehnicheskij dokument Cisco, 2021.

7. Oliver, T. "Jevoljucija virtual'nyh lokal'nyh setej: ot teorii k praktike." Setevye reshenija: issledovaniya i tehnologii, 2020, t. 14, № 1, str. 25-38.

8. Vashington, R., i Li, S. "VLAN i ih vlijanie na proizvoditel'nost' seti." Mezhdunarodnyj zhurnal setej i kommunikacij, 2019, t. 6, № 4, str. 150-162.