ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.05

Математическое и программное обеспечение вычислительных компьютерных сетей, повышение их эффективности путём внедрения принципов и компонентов программно-определяемой сети (часть 1)

Ю.В. Стреналюк, доктор технических наук, профессор, профессор кафедры «Информационные технологии и управляющие системы», Государственное бюджетное образовательное учреждение высшего образования Московской области «Технологический университет», г. Королев, Московская область

И.Н. Леандров, магистрант кафедры «Информационные технологии и управляющие системы», Государственное бюджетное образовательное учреждение высшего образования Московской области «Технологический университет», г. Королев, Московская область

Описывается и анализируются возможности программно-конфигурируемой сети с целью внедрения компонентов ПКС в локально-вычислительную сеть, таким образом модернизировав её, а именно определяется, каким образом принцип работы ПКС изменит сеть, анализируются технологии ПКС для модернизации, а также обозначается роль специального протокола OpenFlow в работе сети ПКС. Исходя из результатов анализа ставится постановка задачи исследования.

***Ключевые слова**: компьютерные сети, программно-определяемые сети*

Mathematical and software support of computing computer networks, increasing their efficiency by implementing the principles and components of a software-defined network (part1)

Yu.V. Strenalyuk, Doctor of Technical Sciences, Professor, Professor of the Department "Information Technologies and Control Systems", State Budgetary Educational Institution of Higher Education of the Moscow Region "Technological University", Korolev, Moscow region

I.N. Leandrov, Master's student of the Department "Information Technologies and Control Systems", State Budgetary Educational Institution of Higher Education of the Moscow region "Technological University", Korolev, Moscow region

The possibilities of a software-configurable network are described and analyzed in order to introduce the components of the PC into the local area network, thus modernizing it, namely, it is determined how the principle of operation of the PC will change the network, the PC technologies for modernization are analyzed, and the role of the special OpenFlow protocol in the operation of the PC network is also indicated. Based on the results of the analysis, the formulation of the research task is set.

***Keywords**: computer networks, software-defined networks*

Введение

Значительные изменения в архитектуре и рост сложности информационных систем и комплексов, облачные платформы и сервисы хранения/обработки больших объемов данных, мобильные сети с изменяющейся топологией и пр. приводят к тому, что эффективность применения традиционных сетей снижается и назревает необходимость реализации сетевой инфраструктуры на базе программно-определяемых (конфигурируемых) сетей (ПОС) и хранилищ информации.

Архитектура программно-конфигурируемых (ПКС) сетей - (*Software Defined Networking/SDN*) представляет значительные преимущества для решения задач обеспечения информационной безопасности сетей передачи информации, тем не менее, определенный ряд проблем, происхождение которых определено непосредственно особенностями технологии, остается актуальным. Приложения управления сетью, используемые в ПКС, предоставляют широкий спектр возможностей по противодействию угрозам за счет поддержки сложных интеллектуальных алгоритмов как предотвращения попадания в сеть злонамеренных потоков, так и сведения к минимуму последствий вторжений. При этом требуемая степень вмешательства на аппаратном уровне остается минимальной.

Часть 1. Анализ технологий программно-конфигурируемой сети

1.1 Развитие программно-конфигурируемой сети как предпосылка улучшения эффективности сети

Современные методы управления вычислительной сетью не обладают достаточной гибкостью для обеспечения соответствующего развития системы межсетевого взаимодействия в больших сетевых комплексах со сложной топологией. Такие сетевые комплексы не допускают использование методов, в основе которых лежит ручное конфигурирование каждого компонента сети и требуют равномерного распределения нагрузки по всем элементам сети, а также гибкого и эффективного средства централизованного управления сетевой инфраструктурой. Для получения желаемого механизма управления в настоящее время представлена новая сетевая концепция. Такой концепцией является использование программно- конфигурируемых сетей.

В основе этой технологии лежит отделение управления сетевой инфраструктурой от передачи данных по сети. Это достигается использованием автоматизированных функций управления в программном обеспечении специального назначения, которое связывает компоненты сети с центром управления сетью, функционирующей на выделенном компьютере.

Таким образом, архитектуру программно-конфигурируемых сетей можно представить в виде трех уровней, см. рисунок 1:

– уровень инфраструктуры сети включает в себя комплекс сетевых устройств и линий связи;

– уровень управления;

– уровень приложений, в котором реализуются различные функции обработки сетевого трафика.

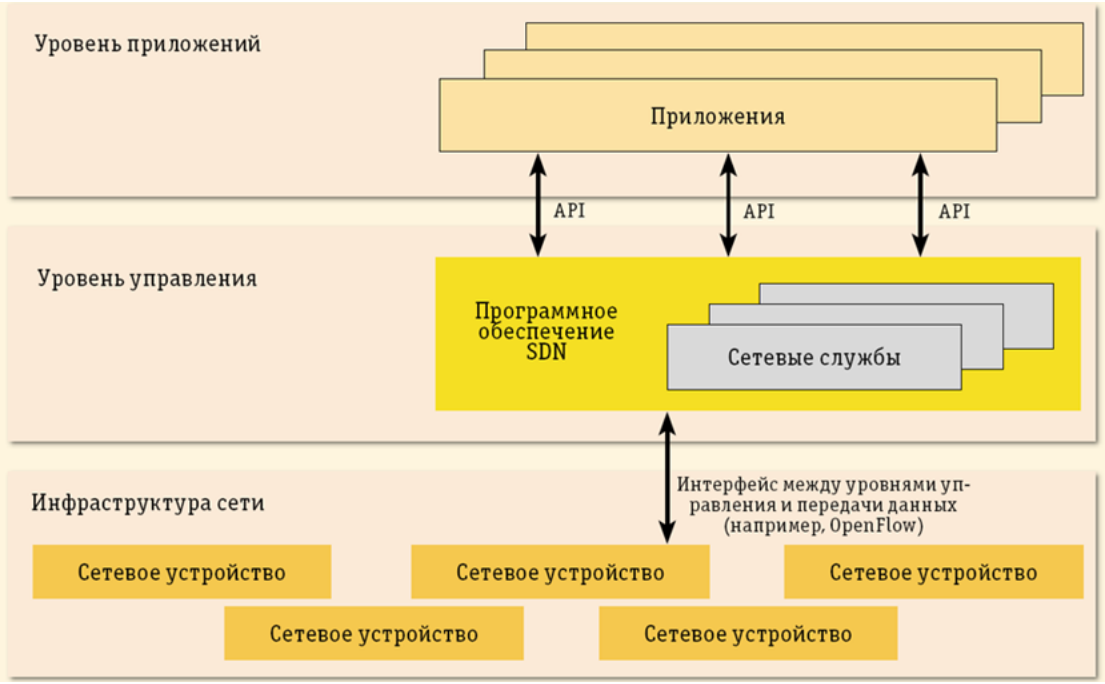

Рисунок 1 – Структура уровней ПКС

В нынешней модели при передаче кадров данных коммутатор *Ethernet* по данным таблицы коммутации посредством коммутационной матрицы обрабатывает и передает кадры данных на требуемый выходной порт, т.е. в нем одновременно работают плоскость управления и плоскость передачи данных, одна - на встроенном микроконтроллере, а вторая в таблице и коммутационной матрице.

Для технологии ПКС в коммутаторе реализован лишь уровень передачи данных на простом устройстве, принимающем поступивший кадр, считывании из него адреса и передаче кадра коммутационной матрице.

В противном случае коммутатор отправляет запрос на центральный контроллер управления ПКС и вносит необходимые изменения в таблицу коммутации, а коммутатор осуществляет обработку кадра. Поэтому контроллер управле-

ния имеет актуальную информацию о структуре и топологии сети, что дает возможность оптимизировать пересылку кадров и обеспечивать связи «порт-порт» на уровне *L2*, не прибегая к *IP*-маршрутизации. При этом в терминологии ПКС используется название - таблица потоков.

ПКС при управлении сетью позволяет достичь прироста эффективности по следующим причинам:

– в технологии ПКС реализовано дифференцирование задачи управления сетевой инфраструктурой и задачи передачи данных по сети. Процессы передачи данных по сети продолжают выполнять на коммутаторе, тогда как за управление берет на себя контроллер ПКС. Такие разделение позволяет повысить эффективность межсетевого взаимодействия, минимизировать нагрузку механизмов управления на пропускную способность сети. Производительность сети, построенной на технологии ПКС, резко возрастает в связи с отсутствием на сетевых устройствах ответственности за принятие решений: все ресурсы сетевых устройств направлены на ускорение перемещения трафика;

– представляется возможным создать гибкую централизованную систему управления сетью с возможность получения представления как о всей сети в целом, так и о каждом устройстве в отдельности. Система мониторинга за состоянием сети позволит оперативно предсказывать и выявлять проблемы в сети, задавать и перераспределять нагрузку на устройства без непосредственного контакта с устройством или ручной настройки его интерфейсов;

– технология предоставляет системному администратору гибкий механизм классификации процессов, происходящих в сети. Таким образом, различные типы трафика получают различные значения приоритета или правила для обработки. С использованием специального языка администратор определяет, какое действие нужно совершить с входящим пакетом: переслать пакет дальше, отказаться от пересылки пакета, изменить поле в заголовке пакета. Выбор того или иного действия зависит от многих параметров, таких как: наличие каких-то специфичных битов в содержимом сетевого пакета; приоритет обработки сетевых пакетов данной конфигурации; состояние сетевого оборудования, обрабатывающего данный пакет.

Таким образом, технология ПКС предоставляет возможность разбиения всей сетевой инфраструктуры на логические элементы: то есть определение возможных путей пересылки для того или иного сетевого потока.

1.2. Модернизация локально-вычислительной сети за счет принципа работы программно-конфигурируемой сети

Интеграция компонентов ПКС позволяет модернизировать ЛВС в существующей сетевой инфраструктуре. При этом не нужна замена существующей инфраструктуры, т.к. практически все преимущества ПКС-достигаются даже

при частичной замене ядра сети или уровня агрегации. ПКС-сеть интегрируются с *IP* сетями на уровнях *L2* и *L3*. При этом одно подключение включает физические интерфейсы с разных коммутаторов. Один ПКС сегмент может иметь несколько *L2* и/или *L3* подключений с IP сетями, реализованных с одних или разных ПКС коммутаторов, входящих в домен.

Таким образом можно предложить теоретическую схему модернизации локально-вычислительной сети с учетом интеграции компонентов программно-конфигурируемой сети.

В рамках традиционной архитектуры (рисунок 2) сетевые задачи распределены по устройствам, такие как:

– Балансировка нагрузки
– Сетевое экранирование
– Управление полосой и прочие.

Такой подход несмотря на свою практичность, делает обслуживание инфраструктуры трудозатратным, а гибкость настроек зачастую не позволяет оптимизировать трафик под различные условия.

Ввиду таких условий и приоретизации курса на виртуализацию сети схема модернизированной ЛВС примерно будет иметь такой вид (рисунок 3).

Таким образом можно подчеркнуть эффективность от внедрения компонентов следующими особенностями:

– централизованное управление сетью *OpenFlow*;
– свободно распределенная топология (*Location Free Networking*) – виртуальных машины и сетевые устройства в любой точке сети;
– снижение эксплуатационных расходов, связанных с конфигурированием и обслуживанием сети;
– существенное снижение сложности сети и ее конфигурирования.

Недостатки:

1. Малое количество проприетарных решений с учетом ПКС специфики, стоимость которых нередко сопоставима с проприетарными решениями
2. Отсутствие поддержки вендора, что является необходимым в работе крупных компаний
3. Сложность эксплуатации и установки доп. средств
4. Малое количество документации.

1.3. Анализ решений программно-конфигурируемой сети для модернизации локально-вычислительной сети

Сейчас по технологии ПКС видно активное участие крупных вендоров сетевых решений. Благодаря развитию предлагаемых ими решений происходит процесс стандартизации технологий ПКС, что подкрепляется множеством исследований в этой области и их приоретизациию.

Основные решения ПКС классифицируются в относительно архитектуры ПКС и образуют следующие группы:

- спецпроцессоры гибридного вида, использующие протоколы традиционной архитектуры и протоколы ПКС (коммутаторы, маршрутизаторы);
- программные средства для управления сетью (контроллеры типа *OpenDayLight*, на его базе разрабатываются и вендорные решения;
- программные средства, выполняющие разные прикладные задачи (дополняющие возможности по управлению сетью, мониторинг и контроль качества, информационную безопасность и пр.).
- **«коробочные» решения** – различные решения, включающее все необходимые составляющие.

Исходя из этого выделим характерные прикладные решения:

- открытые решения и протоколы в качестве основных.
- комплексные решения (с привлечением специализированных), поддерживающие необходимые протоколы и интерфейсы.

Для сетевых решений характерны следующие черты:

- уровень управления на сетевых устройствах;
- гибридный подход с логическим уровнем, взаимодействующим с сетевым оборудованием;
- включение фирменных составляющих.

Таблица 1 Решения ПКС

	Поддержка OpenFlow	Поддержка расширений, специфичных для производителя
Уровень инфраструктуры	ARM, Cisco, Centec Networks, Dell, HP, IBM, ADARA Networks, NEC, Active Broadband Networks, BigSwitch, Broadcom, Juniper networks///	Avaya, Arista, BigSwitch, Cisco, Oracle, Huawei, Extreme Networks
Уровень управления	На основе OpenDayLight: Avaya, Cisco, IBM, Ciena, Dell, HP, Extreme networks, Ericsson, Active Broadband Networks	На основе контроллеров: ADVA Optical Networking, Beacon, Cyan, NEC, Netsocket, Huawei, BigSwitch, Juniper
Уровень приложений	Radware, Cyan, Arista, Centec Netwoks, Aricent, Ciena, Amartus, Corsa Technologies	
Интегральные решения	Dell, Ericsson, MRV Communications	

Таким образом, для анализа технологии был выбран вариант разработки стенда на основе открытых решений, позволяющего оценить преимущества и недостатки программно-конфигурируемой сети.

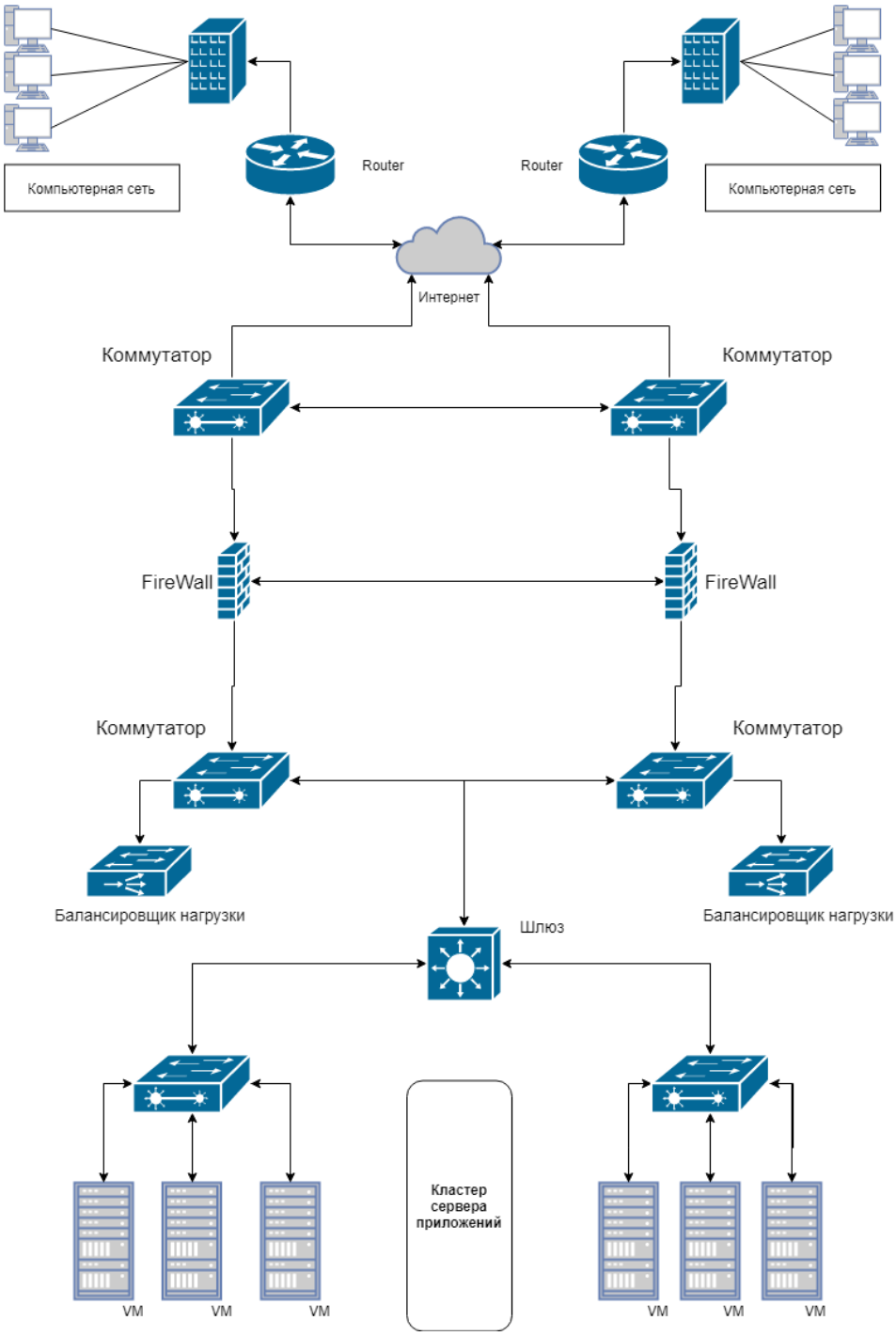

Рисунок 2 – Пример традиционной архитектуры

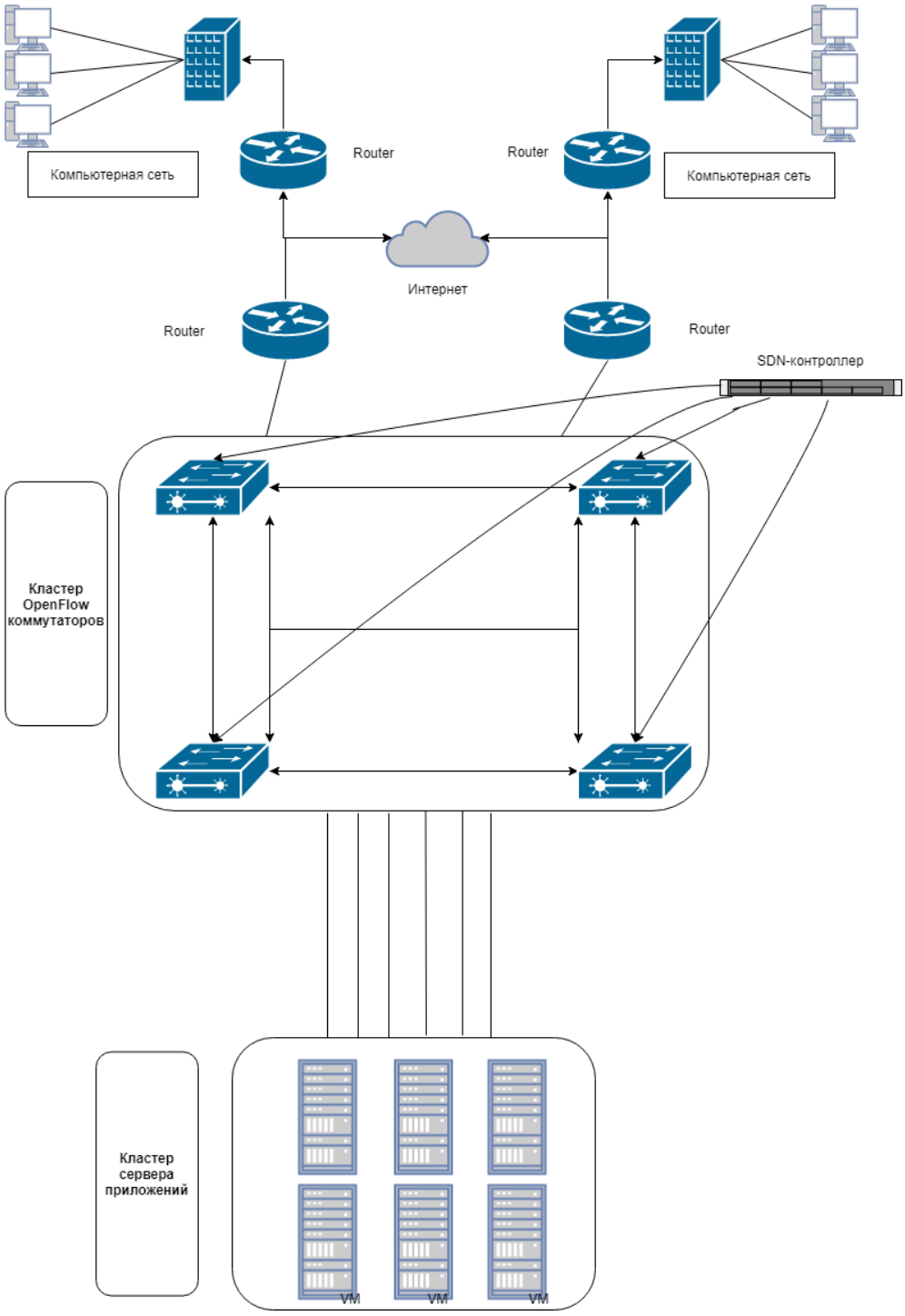

Рисунок 3 –Схема модернизированной ЛВС (теоретическая)

1.4. Характеристика и модернизация модели локально-вычислительной сети

Для реализации проведения оценки эффективности сети на экспериментальном стенде предлагается создания небольшой модели локально-вычислительной сети.

Традиционная модель локально-вычислительной сети представлена на рисунке 4.

Модель, изображенная на схеме, представляет собой сеть из 4 групп хостов, подключенных к *VLAN*, кроме серверов. От коммутаторов проходит *Ethernet* кабель на 100 Mbps.

Коммутаторы по гигабитной *Ethernet* линии подключены к маршрутизатору, тем самым позволяя сетям «общаться» между собой. Также имеется за пределом маршрутизатора имеется *FireWall* и шлюз, необходимый для фильтрации трафика.

Кластер серверов представляет собой набор серверов, таких *FTP*, сервер приложений, *Web*-сервисы и т.д. Они также могут служить генератором трафика и производить определенную нагрузку на сетевую инфраструктуру.

Для моделирования исходных данных, полагаем, что основным видом трафика в ЛВС организации является документооборот, мультимедийная информация, обслуживание множества внешне и внутренне входящих пакетов для работы серверов.

При одновременном доступе общего количества около 100 хостов к серверам хранения данных, веб-сервисам и т.п. трафик будет примерно равен 60-80 Мбит/с, что позволяет говорить о значительном запасе пропускной способности сети при использовании архитектуры 1000BASE-T в магистральных сегментах ЛВС.

Главной проблемой данной топологии будет являться задержка при обработке и отправке данных, так как на коммутаторах в традиционной сети содержатся уровни управления, которые и создают задержку в сети, в то время как в ПКС уровень управления берет на себя контроллер.

Для более детального описания модели традиционной сети были выбраны популярные и «незамысловатые» модели коммутаторов и маршрутизатора.

Коммутатор D-Link DGS-1510-28X обладает статической маршрутизацией и обеспечивает надежное соединение и позволяет просто масштабировать существующую сеть. Коммутаторы этой серии оснащены 16, 24 или 48 портами 10/100/1000 Мбит/с, а также 2 - 4 портами 10G SFP+, используемыми для стекирования или uplink-соединения (рисунок 5).

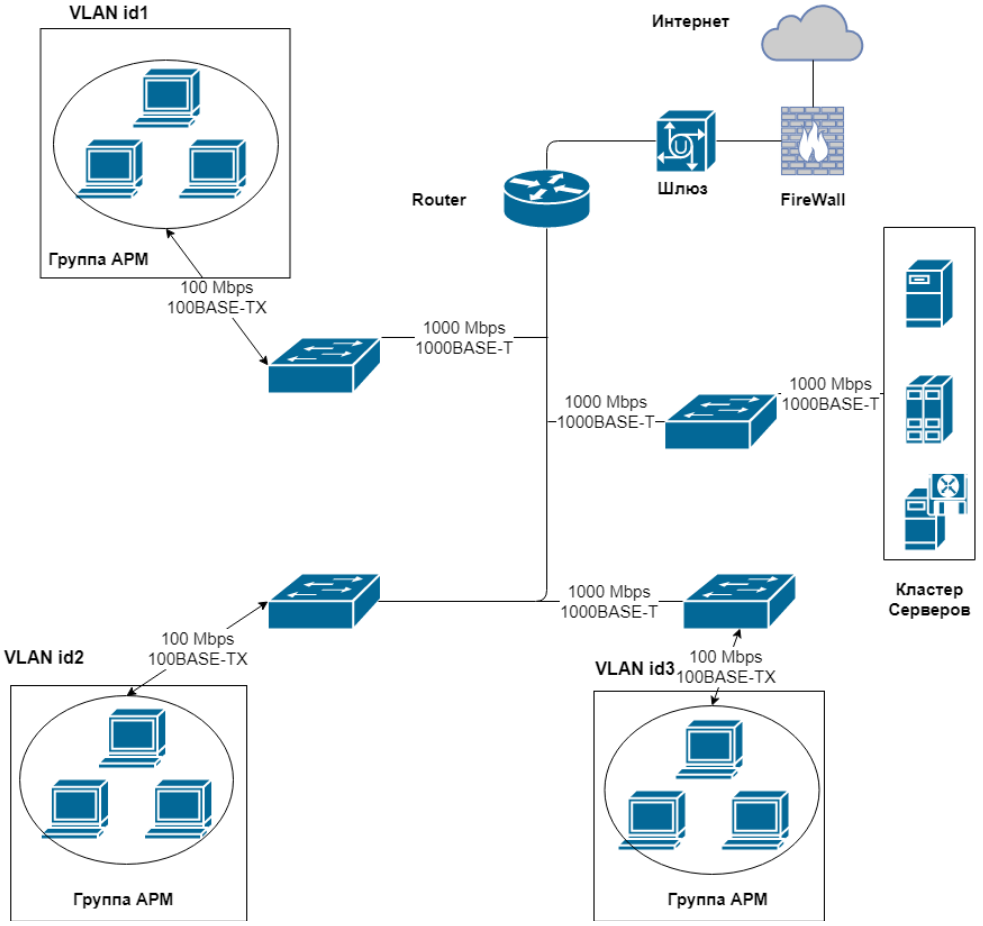

Рисунок 4 – Рассматриваемая модель традиционной сети

Рисунок 5 – L2 Коммутатор D-Link DGS-1510-28X – 20587 руб

Таблица 2 Характеристики коммутатора D-Link DGS-1510-28X

Возможность установки в стойку	есть
Количество LAN-портов	24
Базовая скорость передачи данных	1 Гбит/с
Тип управления коммутатора	уровень 2
Особенности	поддержка работы в стеке
Сетевые стандарты	IEEE 802.1q (VLAN), IEEE 802.3ad (Link Aggregation Control Protocol), IEEE 802.1p (Priority tags), IEEE 802.1d (Spanning Tree), Jumbo Frame, автоопределение MDI/MDIX, IEEE 802.1s (Multiple Spanning Tree)
Количество uplink/стек/SFP-портов и модулей	4
Максимальная скорость uplink/SFP-портов	10 Гбит/с

MikroTik RB4011iGS+RM (рисунок 6, таблица 3) - это роутер без *Wi-Fi* на 10 гигабитных сетевых портов и 1 SFP+ порт для подключения оптики (поддерживаются SFP модули 25G и 10G). Роутер имеет аппаратное шифрование *IPsec*. Внутри устройства установлен мощный четырехядерный процессор с частотой 1.4 ГГц. Маршрутизатор подходит для использования в сетях с количеством абонентов до 200 человек, а также для построения скоростных *VPN* каналов.

Рисунок 6 – Маршрутизатор mikrotik-rb4011igs-rm - 50 тыс.руб

Таблица 3 Характеристики маршрутизатора MikroTik

Возможность установки в стойку	есть
Количество LAN-портов	10
Базовая скорость передачи данных	1 Гбит/с
Количество WAN-портов	1
Функции VPN	IPSec
Особенности	поддержка PoE
Количество uplink/стек/SFP-портов и модулей	1
Максимальная скорость uplink/SFP-портов	10 Гбит/сек
Процессор	4-х ядерный AL21400 с частотой 1.4 ГГц; чип коммутации: RTL8367SB; датчик напряжения; датчик температуры платы; операционная система: RouterOS; MTBF: 200'000 часов, входное напряжение

Преимущества и недостатки модели традиционной сети – в Таблице 4.

Таблица 4 Преимущества и недостатки модели традиционной сети

Преимущества	Недостатки
• Надежная эксплуатация сети. VLAN позволяет конфигурировать и изменять сегменты сети • Высокая надежность сети, которая обусловлена опытом решения известных проблем • Удобное развертывание политик и конфигураций трафика • Применение проприетарных межсетевых экранов	• Низкая способность балансировка нагрузки • Рост задержки обработки пакетов • Большая вероятность джиттера во время использования VoIP технологий обусловлена загруженностью сети и большим временем разброса прохождения IP-пакета вследствие коллизий обработки коммутаторами • Отсутствие программируемости сети • Низкая масштабируемость сети

Для решения подобных проблем предлагается модернизировать сеть внедрив элементы ПКС (рисунок 7).

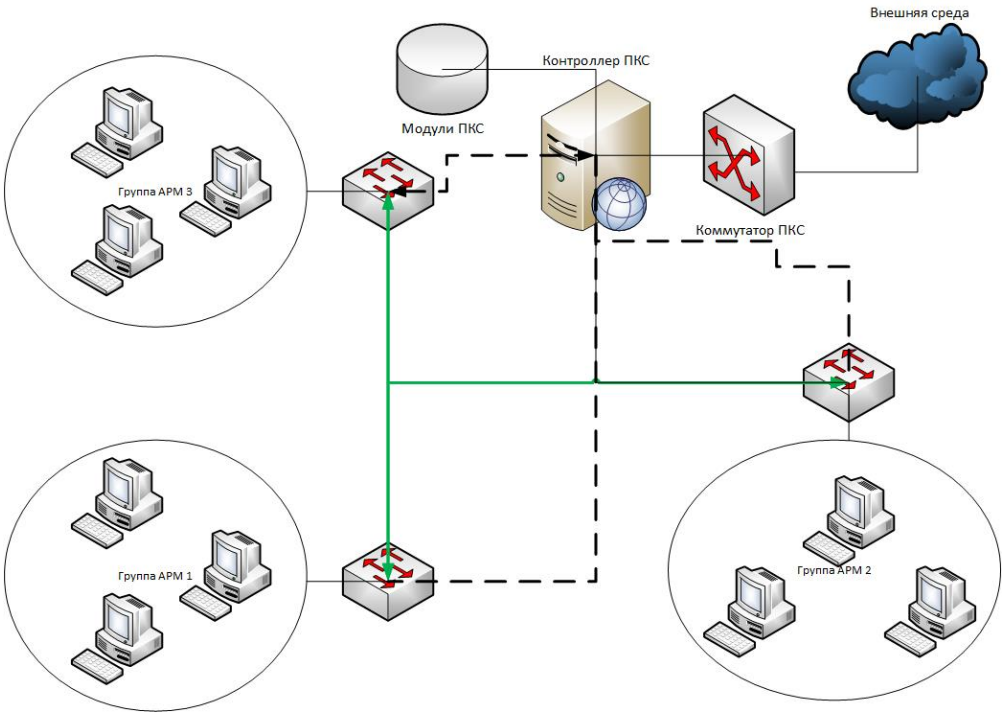

Рисунок 7 – Фрагмент топологии рассматриваемой модели модернизированной ЛВС

Сразу можно выделить следующие отличия, сравнивая две модели:

1) Коммутаторы соединены между собой и подключены к контроллеру ПКС

2) Отсутствие *FireWall*

3) Отсутствие маршрутизатора, его роль способен выполнять контроллер ПКС

Данные отличия существенно вносят изменения обработки данных в сетевой инфраструктуре. Реализация многих функций, которые осуществляются у традиционных сетей через различные решения могут осуществляться на уровне приложения, реализуемого на контроллере ПКС.

Данная сеть будет обладать всеми упомянутыми преимуществами, а также:

- эффективная маршрутизация;
- программируемость сети;
- повышение надежности функционирования сети;
- уменьшение капитальных затрат.

Также архитектура программно-конфигурируемых сетей предоставляет широкие возможности по внедрению новых методов обеспечения информационной безопасности в свою архитектуру. Совокупность механизма унифицированного доступа к сетевой топологии и повышенной программируемости компонентов позволяет, к примеру, обеспечить сбор данных с систем обнаружения и предотвращения вторжений с их дальнейшей обработкой и внесением изменений в конфигурацию. Именно это свойство ПКС делает данную сетевую архитектуру значительно более привлекательной с точки зрения построения средств обеспечения защищенности, нежели традиционные подходы.

1.4. Роль протокола OpenFlow в модернизированной локально-вычислительной сети

В основе архитектуры ПКС лежит открытый протокол *OpenFlow*, обеспечивающий управление сетевой архитектурой. Преимущество этого протокола - он не принадлежит конкретному производителю сетевого оборудования, и, значит, применим для широкого спектра устройств различных производителей.

Протокол *OpenFlow* позволяет задавать конфигурацию сетевых устройств с централизованного аппарата управления сетью – контроллера ПКС, основные функции которого добавление и удаление записей из таблицы сетевых потоков в динамическом режиме и анализ состояния всей сети.

Это дает возможность системному администратору оценку состояния сети в данный момент с использованием сетевой ОС.

Задачи системы управления сетью

сбор сведений о компонентах сети,

сбор статистики взаимодействий внутри сети,

настройка сетевого оборудования.

Администратор сети имеет возможность задавать правила передачи данных в сети.

Выводы по части 1

На основе концепции ПКС и принципов работы данной сети был сделан вывод, что внедрение ПКС позволяет увеличить безопасность и надежность сетей, а также воспользоваться улучшенными возможностями по упрощению, визуализации и виртуализации, недоступными для имеющихся решений.

На основе анализа решений ПКС был выбран вариант реализации на основе открытых решений, а теоретические схемы традиционной сети и ПКС позволили выделить преимущества и недостатки обоих вариантов.

Для реализации проведения оценки эффективности сети на экспериментальном стенде была создана небольшая модель локально-вычислительной сети и дана краткая характеристика, которая была модернизирована путем внедрения

программно-конфигурируемых элементов. Ввиду этого были выделены следующие особенности:

- Коммутаторы соединены между собой и подключены к контроллеру ПКС
- Отсутствие *FireWall*
- Отсутствие маршрутизатора, его роль способен выполнять контроллер ПКС.

Данные отличия существенно вносят изменения обработки данных в сетевой инфраструктуре. Реализация многих функций, которые осуществляются у традиционных сетей через различные решения могут осуществляться на уровне приложения, реализуемого на контроллере ПКС.

Литература

1. Ушаков Ю.А., Ушакова М.В., Шухман М. В.. Основы программно-конфигурируемых сетей: учебное пособие . Самара: ПГУТИ, 2015. – 111с.
2. Полежаев П.Н., Адрова Л.С. Разработка архитектуры системы защиты информации в корпоративных программно-конфигурируемых сетях // Труды Международной научно-технической конференции, Том 1 «Перспективные информационные технологии», 2015.
3. Адрова Л.С., Полежаев П.Н. Разработка системы управления корпоративными сетями на основе технологии программно-конфигурируемых сетей, // Международная научно-техническая конференция «Перспективные информационные технологии», 2014.
4. Бахарева Н.Ф., Полежаев П.Н., Шухман А.Е., Ушаков Ю.А. Управление корпоративными программно-конфигурируемыми сетями // Вестник Оренбургского государственного университета № 13, 2015.
5. Захаров А. А., Попов Е. Ф., Фучко М. М.. Аспекты информационной безопасности архитектуры ПКС // Вестник СибГУТИ. № 1 83, 2016.
6. Смелянский Р.Л. Технологии ПКС и NFV: Новые возможности для телекоммуникаций // Вестник связи. – 2014. - №1.