https://orcid.org/0000-0001-7673-5204
https://orcid.org/0000-0002-5080-1856

УДК 004.7

Е.В. ПОДРОЙКО[*], Ю.М. ЛИСЕЦКИЙ[*]

СЕТЕВЫЕ ТЕХНОЛОГИИ: ЭВОЛЮЦИЯ И ОСОБЕННОСТИ

[*]ДП «ЭС ЭНД ТИ УКРАИНА», г. Киев, Украина

Анотація. *Корпоративна мережа у сучасному розумінні є комплексною і традиційно має на увазі набір базових компонентів, що взаємодіють, серед яких Main Site – мережа головного офісу, Remote Site (Branch) – мережі віддаленого офісу, WAN – глобальна мережа, що об'єднує мережі офісів, LAN – локальна мережа, WAN Edge – точка підключення до WAN, Internet Edge – точка підключення до Internet, Data Center – корпоративний центр обробки даних. У деяких джерелах як компонент також розглядають Service Block – окрему частину мережі, яка містить специфічні мережеві службові сервіси. Кожен компонент корпоративної мережі вміщує власний набір технологій, кожна з яких, у свою чергу, має історію виникнення та розвитку. У статті наведено короткий огляд основних технологій, що сформували історію корпоративних мереж, а також їх еволюцію від набору розрізнених мережевих технологій до єдиної мультисервісної мережевої інфраструктури, що нерозривно пов'язана зі світовою глобальною мережею Internet, яка для більшості сучасних корпоративних мереж є одночасно і сервісом, і транспортним середовищем. Описано виникнення та розвиток мережі Internet, локальних та глобальних мереж, Wi-Fi-мереж та мереж, які визначаються програмно. Корпоративна мережа пройшла довгий еволюційний шлях від існування розрізнених технологій до сучасної уніфікованої інтелектуальної мережевої інфраструктури з високою безпекою та надійним керуванням. Завдяки стрімкому розвитку інформаційних технологій, корпоративні мережі динамічно трансформувались за різними напрямами: віртуалізація мережевих функцій (NFV – Network Functions Virtualization), використання SDN-рішень, автоматизація процесів керування, аналітика, безпека, використання хмарних сервісів. Унаслідок такої трансформації корпоративна мережа перетворилась в уніфіковану, гнучку та орієнтовану на роботу додатків високонадійну інфраструктуру з функціоналом, який легко налаштовувати та розширювати, єдиним центром управління, єдиними політиками безпеки, можливістю швидкого та детального аналізу процесів, які у ній відбуваються.*

Ключові слова: *мережеві технології, корпоративна мережа, еволюція, трансформація, інфраструктура, стандарт, протокол, рівні.*

Аннотация. *Корпоративная сеть в современном понимании является комплексной и традиционно подразумевает набор взаимодействующих базовых компонентов, среди которых Main Site – сеть головного офиса, Remote Site (Branch) – сети удаленного офиса, WAN – глобальная сеть, объединяющая сети офисов, LAN – локальная сеть, WAN Edge – точка подключения к WAN, Internet Edge – точка подключения к Internet, Data Center – корпоративный центр обработки данных. В некоторых источниках в качестве компонента также рассматривается Service Block – отдельная часть сети, содержащая специфические сетевые служебные сервисы. Каждый компонент корпоративной сети включает в себя собственный набор технологий, каждая из которых, в свою очередь, имеет историю возникновения и развития. В статье приведены краткий обзор основных технологий, сформировавших историю корпоративных сетей, а также их эволюция от набора разрозненных сетевых технологий до единой мультисервисной сетевой инфраструктуры, неразрывно связанной с мировой глобальной сетью Internet, являющейся для большинства современных корпоративных сетей одновременно и сервисом, и транспортной средой. Описано возникновение и развитие сети Internet, локальных и глобальных сетей, Wi-Fi-сетей и программно определяемых сетей. Корпоративная сеть прошла длинный эволюционный путь от сосуществования разрозненных технологий до современной унифицированной интеллектуальной сетевой инфраструктуры с высокой безопасностью и надежным управлением. Благодаря стремительному развитию информационных технологий, корпоративные сети динамично трансформировались по различным направлениям: виртуализация сетевых функций (NFV – Network Functions Virtualization), использование SDN-решений, автоматизация процессов управления, аналитика, безопасность, использование облачных сервисов. В результате такой трансформации корпоративная сеть превратилась в*

унифицированную гибкую и ориентированную на работу приложений высоконадежную инфраструктуру с легко перестраиваемым и расширяемым функционалом, единым центром управления, едиными политиками безопасности, возможностью быстрого и детального анализа происходящих в ней процессов.
Ключевые слова: *сетевые технологии, корпоративная сеть, эволюция, трансформация, инфраструктура, стандарт, протокол, уровни.*

Abstract. *Today corporate network is seen as a complex system and traditionally provides the set of interacting essential components, such as: Main Site – a network of head office; Remote Site (Branch) – networks of remote office, WAN – global network uniting networks of the offices; LAN – a local network; WAN Edge – a point of connection to WAN. Internet Edge – a point of connection to the Internet; Data Center – corporate centre of data processing. Some sources also regard Service Block as a component, which is a separate segment of the network with specific services. Every component of corporate network features contains individual set of technologies, each having its history of origination and development. The paper offers short review of basic technologies which form the history of development of corporate network, as well as their evolution from a set of separated network technologies to a unified multiservice network infrastructure. This unified infrastructure is inextricably linked with a global network of Internet which is both a service and a carrier for majority of modern corporate networks. The paper describes origination and development of Internet, local and global networks, Wi-Fi networks and software defined networks. Corporate network has been through a long evolution from co-existence of separated technologies to modern unified intellectual network infrastructure with high security and reliable management. Due to fast-moving development of information technologies the corporate networks have dynamically transformed in several directions: network functions virtualization (NFV – Network Functions Virtualization), utilization of SDN solutions; automation of management processes, analytics, security, cloud services. In the course of such a transformation the corporate network turned into unified, flexible, application oriented infrastructure with high reliability, easily modified and expanded functionality, single management center, unified security policies, fast and detailed analysis of internal network processes.*
Keywords: *network technologies, corporate network, evolution, transformation, infrastructure, standard, protocol, levels.*

DOI: 10.34121/1028-9763-2020-2-14-29

1. Введение

Определение «корпоративная сеть» в современном понимании является комплексным и традиционно подразумевает набор взаимодействующих базовых компонентов, среди которых Main Site – сеть головного офиса, Remote Site (Branch) – сети удаленного офиса, WAN – глобальная сеть, объединяющая сети офисов, LAN – локальная сеть, WAN Edge – точка подключения к WAN, Internet Edge – точка подключения к Internet, Data Center – корпоративный ЦОД. В некоторых источниках рассматривается также Service Block – отдельная часть сети, содержащая специфические сетевые служебные сервисы, такие, как, например, wireless-контроллеры, терминация ISATAP туннелей, Unified Communications services и т.д. (рис. 1).

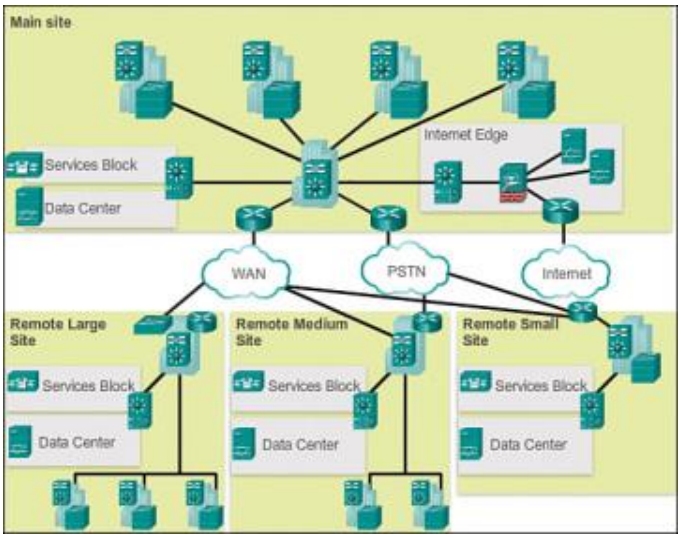

Рисунок 1 – Компоненты корпоративной сети

Каждый компонент корпоративной сети включает в себя собственный набор технологий, каждая из которых, в свою очередь, имеет историю возникновения и развития. Далее приведены

краткий обзор основных технологий, сформировавших историю корпоративных сетей, а также их эволюция от набора разрозненных технологий до единой мультисервисной сетевой инфраструктуры, неразрывно связанной с мировой глобальной сетью Internet, являющейся для большинства современных корпоративных сетей одновременно и сервисом, и транспортной средой.

Цель данной статьи – обзор эволюции и особенностей развития сетевых технологий, определивших историю развития корпоративных сетей, сформировавших понятие корпоративной сети, а также ставших основой современных информационно-технологических инфраструктур.

2. Возникновение и развитие INTERNET

Впервые идея обмена цифровыми данными между двумя компьютерами была реализована исследователем лаборатории Массачусетского технологического института Лари Робертсом (Lawrence Gilman Roberts, December 21, 1937 – December 26, 2018) [1]. Впоследствии идея развилась в проект, в рамках которого Агентством Министерства обороны США по перспективным исследованиям в 1969 г. была построена сеть передачи данных ARPANet (Advanced Research Projects Agency Network), которая стала основой для развития более совершенной сети NSFNet (National Science Foundation Network), а затем и глобальной сети Internet.

Первоначально в рамках данной сети были соединены исследовательские центры, занятые в разработке ARPANET. Сеть развивалась и становилась все более разветвленной. В январе 1983 года произошло поистине знаковое событие. Сеть ARPANet перешла на использование стека протоколов TCP/IP вместо предшествующего ему NCP. В 1985 году Национальным научным фондом США (NSF) была создана новая сеть NSFNet, также использовавшая TCP/IP и предназначенная для обмена научными данными, которая позднее начала использоваться и коммерческими структурами, получая лучшее финансирование. В итоге ARPANet и NSFNet начали стремительную трансформацию в современный Internet.

3. Возникновение и развитие локальных сетей

Параллельно с Internet развивались и локальные сети (Local Area Network – LAN) [2]. Начало истории локальных сетей передачи данных было положено в 1973 году инженером компании Xerox Робертом Меткалфом (Robert Melancton Metcalfe), создавшим проект экспериментальной сети, получившей название «Ethernet» и предназначавшейся для соединения нескольких персональных компьютеров (с графическим интерфейсом) Xerox Alto, серверов, а также лазерных принтеров.

Физическая скорость в данной сети составляла 2.94 Mbps. Данное техническое решение было развитием более раннего проекта Alto Aloha Network. Название «Ethernet» основывалось на слове «ether» (эфир), что намекало на одновременную передачу битовой информации в физической среде всем участникам сети.

Первую попытку стандартизировать Ethernet предпринял консорциум, включающий компании DEC, Intel, Xerox. Стандарт получил название DIX (первые буквы названий компаний). Последним стандартом DIX, увидевшим свет, был DIXv2.0 (The Ethernet, A Local Area Network: Data Link Layer and Physical Layer Specifications).

Технология стала общепризнанным стандартом в 1985 году в результате работы Института инженеров электротехники и электроники – IEEE (англ. Institute of Electrical and Electronics Engineers). Стандарт носит название IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. IEEE, в процессе создания стандарта дистанцировался от коммерческого названия «Ethernet», однако данное название прочно закрепилось в среде производителей.

Далее стандарт активно развивался путем переработок и внесения дополнений (supplements). Относительная простота, наряду с своевременными улучшениями, позволила технологии Ethernet (IEEE 802.3) проникнуть почти во все сферы применения сетей передачи данных от LAN до глобальных (Wide Area Network – WAN). Поэтому к настоящему времени современная часть дерева стандартов IEEE 802.3 (например, 1000BASE-T, 1000BASE-LX, 1000BASE-SX, 10G BASE-SR, 10G BASE-LR и др.) наряду с WI-FI (IEEE 802.11) легли в основу современных enterprise сетей.

Количество дополнений стандарта ярко иллюстрирует большой объем наработок, накопленный данной технологией в процессе активного развития (табл. 1). Стек протоколов TCP/IP дал возможность унифицировать передачу данных в сетях и легко подключать локальные сети к Internet.

Таблица 1 – Дополнения стандарта IEEE 802.3

Дополнения стандарта IEEE 802.3	Год создания	Описание
802.3a	1985	10BASE2 thin Ethernet
802.3c		10 Mbps repeater specifications, clause 9
802.3d	1987	FOIRL fiber link
802.3i	1990	10BASE-T twisted-pair
802.3j	1993	10BASE-F fiber optic
802.3u	1995	100BASE-T Fast Ethernet and Auto-Negotiation
802.3x	1997	Full-Duplex standard
802.3z	1998	1000BASE-X Gigabit Ethernet
802.3ab	1999	1000BASE-T Gigabit Ethernet over twisted-pair
802.3ac	1998	Frame size extension to 1522 bytes for VLAN tag
802.3ad	2000	Link aggregation for parallel links
802.3ae	2002	10-Gigabit Ethernet
802.3af	2003	Power over Ethernet - first standard release for this technology
802.3ah	2004	Ethernet for the First Mile
802.3ak	2004	10G-Base-CX4 10Gbps, Ethernet over twinaxial cables.
802.3an	2006	10G-Base-T 10Gbps over unshielded twisted pair, UTP.
802.3ap	2007	Backplane Ethernet, 1 & 10 Gbps over a PCB.
802.3aq	2006	1-G-Base-LRM 10 Gbps over multimode fibre.
802.3as	2005	Frame expansion
802.3at	2005	Power over Ethernet Plus - enhancements to 25.5W
802.3au	2006	Isolation requirements for Power over Ethernet
802.3av	2009	10 Gbps
802.3ax	2008	Link aggregation - see IEEE 802.1ax
802.3az	2010	Energy efficient Ethernet
802.3ba	2010	40Gbps & 100Gbps Ethernet
802.3bc	2009	Update of Ethernet Type, Length & Value, TLVs that were previously specified in 802.1AB to 802.3
802.3bd	2011	Priority based flow control
802.3bf	2011	Provision of accurate indication of transmission and reception initiation times of some packets to support IEEE P802.1AS

Современные стандарты Ethernet практически не похожи на свою родоначальную технологию. Средой передачи является так называемая витая пара или оптоволокно. Скорости передачи данных в этих средах намного выше. К тому же среда передачи давно не является разделяемой – каждый фрейм, сгенерированный хостом, не передается обязательно всем остальным хостам. Для этого в передаче данных участвует активное оборудование, способное запоминать принадлежность MAC-адресов, и после обучения на основе трафика сети коммутировать фреймы Ethernet только для хостов, соответствующих MAC-адресу получателя. Поскольку современные стандарты Ethernet предполагают два независимых канала передачи данных в противоположных направлениях, понятие «коллизий» и «доменов коллизий» потеряло свою актуальность. Прямой и обратный потоки трафика не испытывают взаимного влияния, что на уровне коммутаторов достигается с помощью специальной матрицы коммутации.

Однако Ethernet не утратил некоторых своих рудиментарных недостатков. Одним из них является BUM (Broadcast, Unknown unicast and Multicast) трафик, расточительно расходующий пропускную способность сети. Причина существования данного трафика кроется, во-первых, в особенности работы протокола ARP, призванного отображать интернет-адреса (IPv4 адреса) получателей в их адреса в рамках физической среды передачи (MAC-адреса), для чего первоначально необходимо опрашивать все хосты-участники подсети на предмет обладания искомым IP-адресом. Во-вторых, коммутатор, не имеющий в своей таблице коммутации MAC-адреса хоста – получателя, вынужден транслировать фрейм во все свои порты (всем получателям).

Все перечисленные недостатки проистекают от первоначально простого предназначения данного протокола и, безусловно, имеют большое значение в использовании Ethernet для WAN-сетей и сетей операторов связи.

Растущее количество пользователей, увеличение объемов трафика вместе с требованиями надежности повлияли на дизайн локальных сетей. Иерархический дизайн сети стал решением проблем масштабируемости, расширяемости и надежности сети. Согласно требованиям иерархического дизайна, сеть стала многоуровневой. Традиционно в сети выделяют три уровня: уровень доступа (Access) – оборудование для подключения пользователей сети; уровень распределения (Distribution) – оборудование для объединения устройств доступа, ответственное за наиболее интеллектуальный функционал сети, такой, как, например, VLAN-сегментация, L3-коммутация, фильтрация пакетов и т.д.; уровень ядра (Core) – оборудование, объединяющее устройства уровня распределения и ответственное за быструю коммутацию (обычно это L3 – коммутация) трафика. Иерархический дизайн локальной сети представлен на рис. 2.

В подобных топологиях активно используется резервирование устройств и линков между ними. Традиционно для предотвращения логических петель, при наличии избыточных L2-линков, и переключения маршрутов, при отказах L3-линков, используются соответственно spanning-tree в нескольких модификациях и IGP-протоколы маршрутизации, такие, как, например, OSPF, EIGRP. С развитием технологий кластеризации и стекирования оборудования появилась возможность заменить spanning-tree на EtherChannel, превратив резервирующие друг друга независимые линки в участников одного общего EtherChannel- линка (рис. 3).

Кластеризованные для резервирования физические устройства представляют собой одно логическое. А поскольку EtherChannel всегда представляет собой один логический линк между двумя устройствами, то образование логических колец между его физическими линками-участниками невозможно. Такой подход позволяет также легко балансировать трафик.

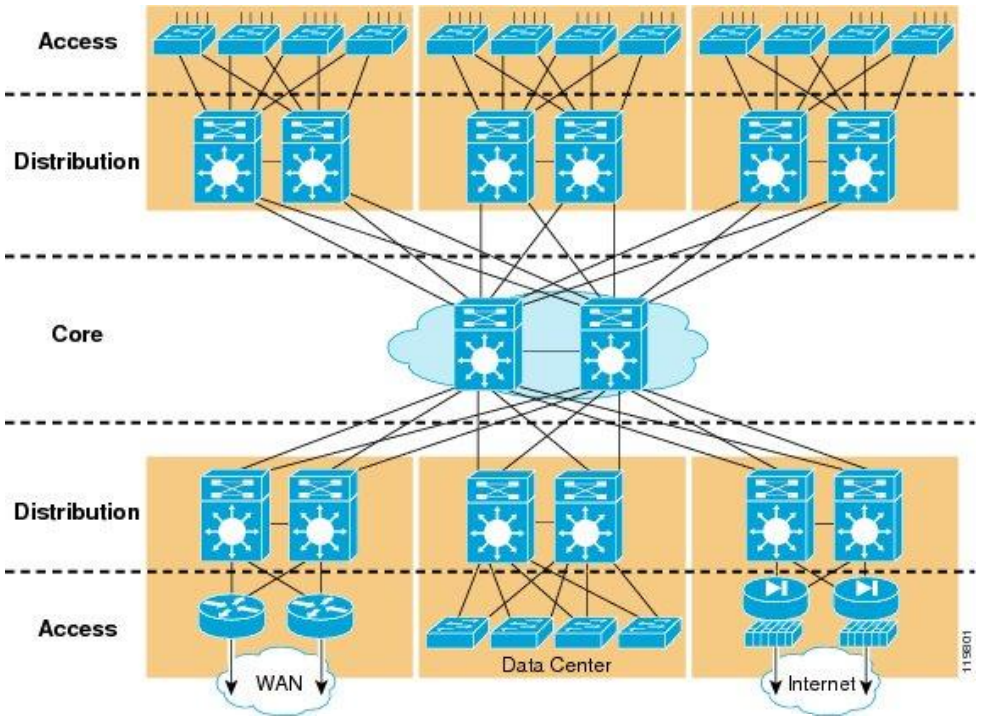

Рисунок 2 – Иерархический дизайн локальной сети

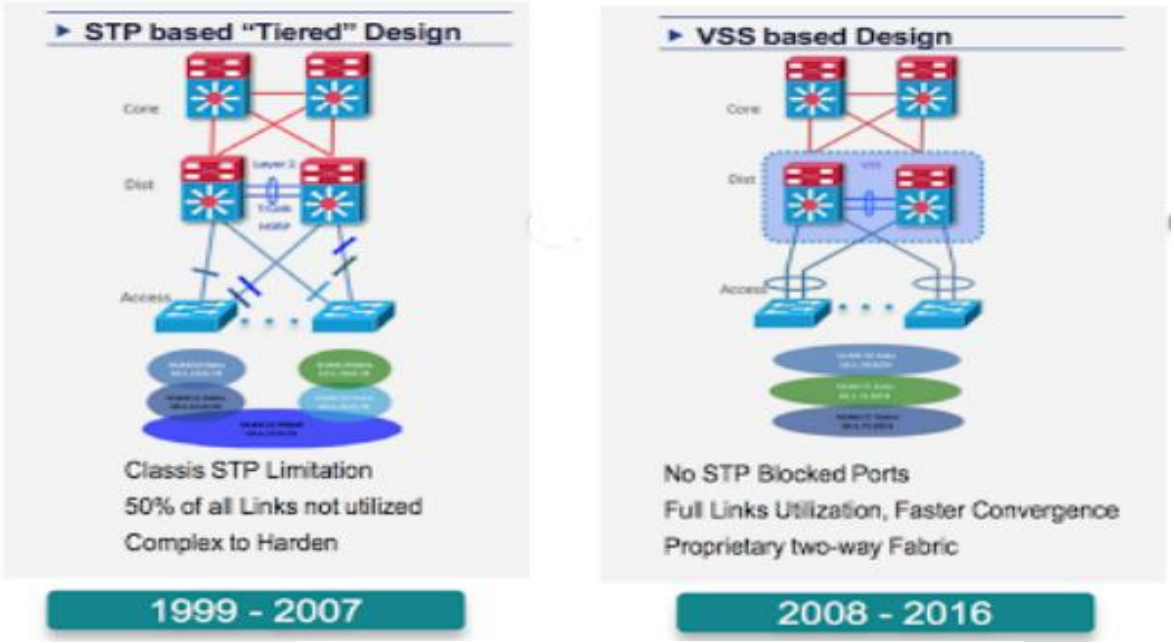

Рисунок 3 – Переход от Spanning-Tree к кластеризации и EtherChannel

4. Возникновение и развитие Wi-Fi-сетей

Технология WI-FI родилась как средство предоставления широкополосного доступа в Internet, использующее радиосигнал [3]. Маршрутизатор или бридж со специальным радиопередатчиком на борту принимает трафик из Internet или локальной сети, преобразовывая полученные данные в радиосигнал, который может быть принят и считан конечными устройствами, поддерживающими соответствующий формат. Обмен между передатчиком и конечным устройством происходит симметрично.

Официальным рождением WI-FI можно считать 1997 год, когда была создана рабочая группа IEEE 802.11, занимающаяся созданием стандартов беспроводных сетей

(WLANs –Wireless Local Area Networks) с последующей основной спецификацией, предусматривающей обмен данными между устройствами на скорости 1-2Mbps на частоте 2.4 GHz [4]. В 1999 году технология WI-FI начала проникать в сферу домашнего использования.

В аббревиатуре «WI-FI» заложено словосочетание Wireless Fidelity, что буквально переводится как «цифровая привязанность». Все реализации стандартов IEEE 802.11 тестируются организацией WI-FI Alliance – объединением крупнейших производителей беспроводных устройств. Успешное тестирование WI-FI Alliance является залогом успешной совместной работы устройств различных производителей.

WI-FI использует два частотных диапазона: 2.4 GHz (традиционно 802.11b) и 5 GHz (традиционно 802.11a). Многие годы стандарт 802.11b был первым по популярности стандартом среди WI-FI – пользователей в виду поддержки большим количеством устройств и в связи с меньшей стоимостью в сравнении с 802.11a. Стандарт 802.11b использует диапазон 2.4GHz. Поддерживаемая максимальная скорость передачи данных составляет 11Mbps, на практике – не более 6Mbps. Стандарт 802.11a использует диапазон 5GHz, что увеличивает вероятность потери сигнала из-за наличия препятствий в виде стен и других предметов. Обеспечиваемая максимальная скорость – 54Mbps, на практике – не более 25Mbps.

В 2003 году скорость и покрываемое расстояние WI-FI увеличилось благодаря появлению стандарта 802.11g. Данный стандарт работает в диапазоне 2.4GHz, обеспечивая максимальную пропускную способность 54 Mbps, на практике – 10-27 Mbps, и имеет обратную совместимость с 802.11b. В 2009 году мир увидела финальная версия стандарта 802.11n, сделавшая ощутимый скачок в производительности и надежности сигнала по сравнению с предыдущими технологиями благодаря применению способа кодирования MIMO (Multiple Input Multiple Output – множественные входы, множественные выходы) [5]. MIMO – это метод пространственного кодирования сигнала, при котором для передачи и приема используются группы антенн по две и более соответственно (рис. 4). Между передающими и приемными антеннами одного устройства минимизируется взаимное влияние.

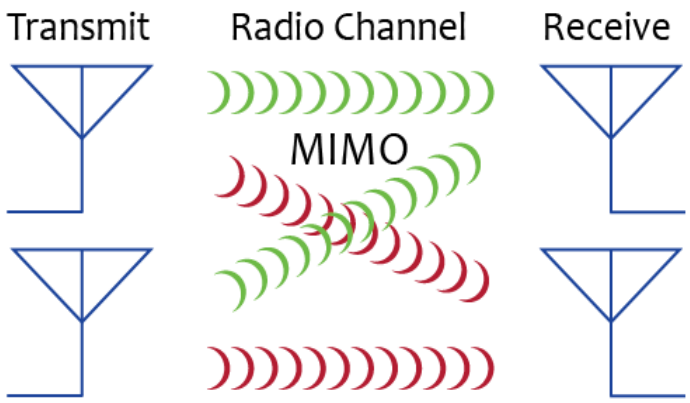

Рисунок 4 – Принцип Multiple Input Multiple Out

Первый патент на использование MIMO был зарегистрирован еще в 1984 году. Стандарт работает на частоте 2.4 – 2.5 и 5 ГГц и обратно, совместим с 802.11 a/b/g, а потому обозначается как 802.11 a/b/g/n. Максимальная скорость передачи данных у стандарта – 300Mbps. В 2011 году вышел новый стандарт 802.11ac, одной из основных задач которого был выход на рубеж пропускной способности 1Gbps (табл. 2).

Стандарт опирается лишь на частоту 5GHz, хотя в нем заявлена поддержка всех предыдущих стандартов. Теоретически финальная версия стандарта обеспечивает максимальную скорость в 6.9 Gbps. Стандарт развивался поэтапно, и по результатам каждого из них создавался отдельный релиз стандарта (802.11ac Wawe1, 802.11ac Wawe2) для скорейшего внедрения. Стандарт использует технологию MU-MIMO (Multi User MIMO), позволяющую одному пользователю подключать несколько клиентских устройств, давая возможность использовать несколько одновременных исходящих потоков, что открывает широкие возможности для IoT (Internet of Things), поддерживает высокую производитель-

ность, большую плотность клиентов, а также предусматривает экономное энергопотребление.

Таблица 2 – Параметры стандартов 802.11n и 802.11ac

	802.11n	802.11n IEEE Specification	802.11ac Wave 1 Today	802.11ac Wave2 WFA Certification Process Continues	802.11ac IEEE Specification
Band	2.4 GHz & 5 GHz	2.4 GHz & 5 GHz	5 GHz	**5 GHz**	5 GHz
MIMO	Single User (SU)	Single User (SU)	Single User (SU)	**Multi User (MU)**	Multi User (MU)
PHY Rate	450 Mbps	600 Mbps	1.3 Gbps	**2.34 Gbps - 3.47 Gbps**	6.9 Gbps
Channel Width	20 or 40 MHz	20 or 40 MHz	20, 40, 80 MHz	20, 40, 80, **80-80, 160** MHz	20, 40, 80, 80-80, 160 MHz
Modulation	64 QAM	64 QAM	256 QAM	256 QAM	256 QAM
Spatial Streams	3	4	3	3-**4**	8
MAC Throughout*	293 Mbps	390 Mbps	845 Mbps	1.52 Gbps- 2.26 Gbps	4.49 Gbps

* Assuming a 65% MAC efficiency with highest MCS

Еще одним принципиально новым шагом в стандарте 802.3.ac является наличие beamforming. Beamforming – это управляемое формирование сигнала, возможное за счет работы нескольких раздельных антенн, позволяющее автоматически в реальном времени менять диаграмму направленности точки доступа в зависимости от расположения клиентских устройств. Конечная цель данной функции – концентрировать мощность излучаемого сигнала в районе расположения клиентов, обеспечивая их качественным сигналом и экономя энергопотребление.

В 2012 году появился стандарт IEEE 802.11ad, который стал частью реализации MGWS (Multigigabit Wireless System) – концепции высокоскоростной сети, базирующейся на частотном диапазоне в области 60 GHz. WI-FI-решения, базирующиеся на частотах в области 60GHz, также получили условное название WiGig. Рассматриваемый диапазон 2.4GH и 5GHz. Этот диапазон (60GHz) накладывает большие ограничения на распространение радиосигнала. Сигнал не может обходить препятствия. Область уверенного приема сигнала ограничена радиусом менее 10 метров. Однако высокая несущая частота может обеспечивать высокую скорость передачи данных, что делает технологию перспективной для таких применений, как, например, передача несжатого видео высокой четкости. В виду небольшой мощности точек доступа (до 10dBm) и поглощения волн стенами помещения хорошо решается проблема засоренности эфира. Стандарт покрывает частотный диапазон 57 ÷ 71 GHz, делящийся на 6 каналов (табл. 3). Каждый канал занимает полосу 2160 MHz и обеспечивает пропускную способность 1760 MHz.

Технологии WiGig сталкиваются с проблемой пропускной способности коммутаторов доступа, которые предлагают, в основном, 1Gbps, что почти вдвое меньше пропускной способности, обеспечиваемой WiGig. Также необходимо отметить, что во многих странах мира диапазон используемых стандартом частот может быть значительно ограничен вследствие занятости определенных полос. Стандарт 802.3ad использует простые виды модуляции, такие, как BPSK и QPSK – двоичная и квадратурная модуляция соответственно.

Таблица 3 – Частотный диапазон 802.11ad

•				
Channel	Center (GHz)	Min. (GHz)	Max. (GHz)	BW (GHz)
1	58,32	57,24	59,40	2,16
2	60,48	59,40	61,56	
3	62,64	61,56	63,72	
4	64,80	63,72	65,88	
5	66,96	65,88	68,04	
6	69,12	68,04	70,20	

Технологии WiGig сталкиваются с проблемой пропускной способности коммутаторов доступа, которые предлагают, в основном, 1Gbps, что почти вдвое меньше пропускной способности, обеспечиваемой WiGig. Также необходимо отметить, что во многих странах мира диапазон используемых стандартом частот может быть значительно ограничен вследствие занятости определенных полос. Стандарт 802.3ad использует простые виды модуляции, такие, как BPSK и QPSK – двоичная и квадратурная модуляция соответственно.

5. Возникновение и развитие глобальных сетей

В отличие от сетей LAN, призванных связывать набор офисного компьютерного оборудования, глобальные сети (WAN – Wide Area Network) создавались для связи географически разнесенных объектов. Учитывая большую протяженность необходимых каналов передачи данных, было логично использовать готовую инфраструктуру операторов связи.

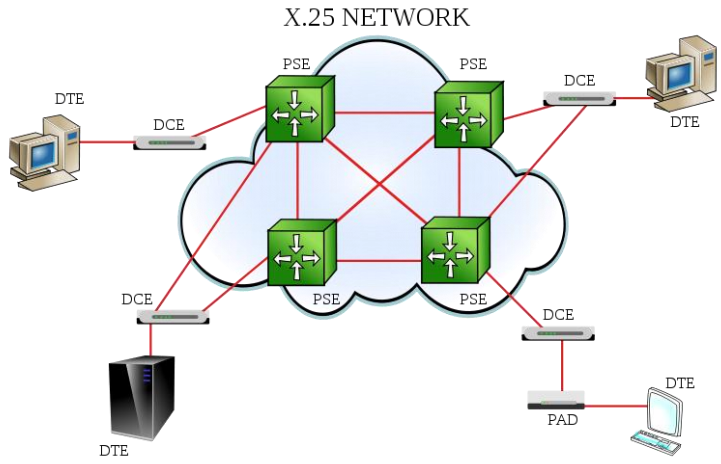

Рисунок 5 – Сеть X.25

История WAN-сетей началась со стандарта X.25, разработанного комитетом ITU-T [6]. Стандарт был реализован и получил популярность в 70-х–80-х годах прошлого столетия. X.25 – сеть на основе коммутации пакетов, располагающая своим собственным стеком протоколов и специальным коммутирующим оборудованием. Первым применением сетей X.25 было использование для связи удаленных терминалов с мейнфреймами (рис. 5).

Для объединения LAN в 80-е годы активно использовались цифровые выделенные «point-to-point» каналы. Это были каналы DS0 (56Kbps) или более дорогие T1/E1, T3/E3. Изначально данный тип каналов (E1) разрабатывался для передачи голоса (рис. 6).

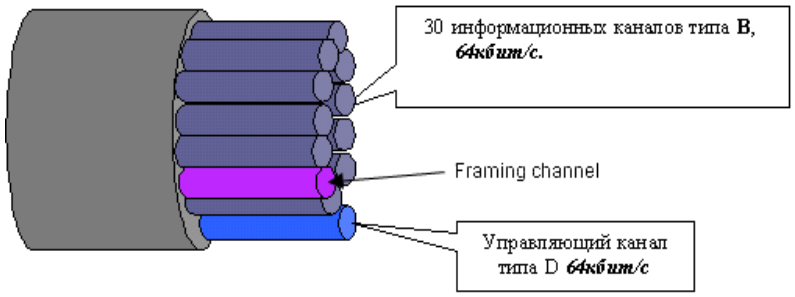

Рисунок 6 – Структура канала E1

Каналы коммутируются у операторов связи на постоянной основе, используя специальные коммутаторы потоков и мультиплексоры, объединяющие каналы малой пропускной способности в более крупные (цифровая иерархия). LAN сопрягаются с WAN посредством устройств-шлюзов (Gateway), являющихся IP-маршрутизаторами, имеющими на борту LAN и WAN-интерфейсы. Стек протоколов TCP/IP выступает унифицированным инструментом для передачи данных с помощью различных базовых технологий. Способ организации WAN на базе цифровых синхронных каналов, разработанных для передачи голоса из конца в конец, является дорогостоящим и негибким.

В начале 90-х стала активно внедряться технология Frame Relay. Технология также предполагает использование каналов DS0, T1/E1, T3/E3 между абонентским оборудованием (DTE – Data Terminal Equipment) и оборудованием оператора связи (DCE – Data Communication Equipment). Данные каналы не соединяют абонентское оборудование напрямую, а лишь являются транспортом для виртуальных каналов Frame Relay, которые, в свою очередь, непосредственно соединяют между собой абонентское оборудование (маршрутизаторы на площадках абонента) в соответствии с логической топологией (рис. 7). Коммутация происходит на специальных Frame Relay-коммутаторах на стороне оператора связи. Преимущество данной технологии состоит в возможности строить гибкие топологии для объединения локальных сетей абонента поверх существующих цифровых каналов без привлечения дополнительных выделенных линий point-to-point.

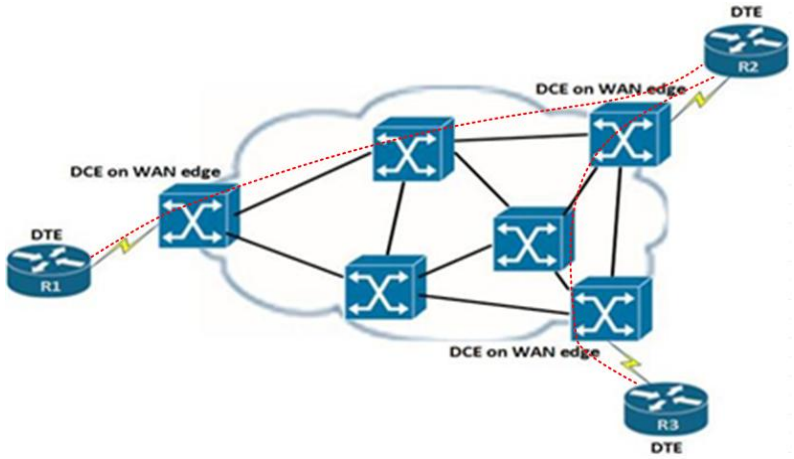

Рисунок 7 – Сеть Frame-Relay

Кроме того, единая инфраструктура используется для построения сетей множества независимых абонентов. Frame Relay позволила значительно уменьшить OpEx и CapEx для WAN-среды, чем завоевала заслуженную популярность у операторов связи. В течение пяти лет даже наиболее консервативные клиенты, такие как банки, перешли на использование Frame Relay.

В 90-е годы также развивалась довольно сложная технология ATM, однако в качестве WAN для корпоративных сетей она почти не использовалась.

Полноправным преемником Frame Relay стала технология MPLS (Multiprotocol Label Switching) [7]. MPLS обычно реализуется в рамках сети оператора связи (рис. 8).

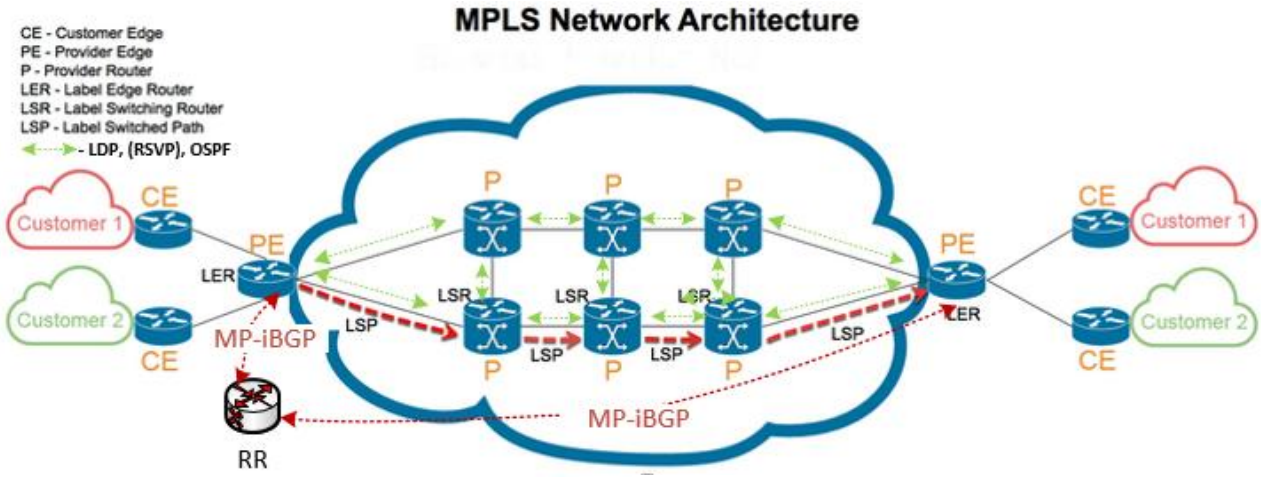

Рисунок 8 – Сеть MPLS

Технология предполагает маршрутизацию IP-пакетов только на границе сети провайдера. Внутри же сети происходит коммутация по меткам. Приходя извне на пограничный маршрутизатор, пакет попадает в FIB (Forwarding Information Base), где, согласно адресу назначения, пакет инкапсулируется в специальный MPLS-фрейм, в один из заголовков которого добавляется номер метки – значение, взятое из FIB при маршрутизации пакета. Далее MPLS-frame инкапсулируется во фрейм базового протокола передачи данных. Например, в Ethernet, где в заголовки фрейма добавляются MAC-адреса источника и назначения. Поскольку в рамках сетевой модели OSI заголовки MPLS добавляются между заголовками второго и третьего уровней, MPLS именуют протоколом уровня «2.5». Заголовки MAC назначения присваиваются в соответствии с адресом шлюза в FIB и adjacency-таблицей). Далее путь фрейма MPLS внутри MPLS – облака оператора связи – предопределен в соответствии с таблицами LFIB (Label Forwarding Information Base) промежуточных маршрутизаторов, где каждому возможному значению метки пришедшего фрейма соответствует новое значение метки, а также исходящий интерфейс. Цепочка меняющихся меток пакета на пути из одной крайней точки сети в другую называется LSP (Label Switched Path).

Метки могут образовывать так называемый «стек». Это значит, что MPLS-фреймы могут вкладываться друг в друга. На выходе из MPLS облака IP-пакет декапсулируется из фрейма MPLS и перенаправляется в исходящий интерфейс согласно LFIB. Информация об IP-маршрутах распространяется протоколами маршрутизации. Информация о метках может распространяться такими протоколами, как LDP, RSVP, BGP или даже OSPF. Обычно в MPLS-сети используются одновременно два протокола маршрутизации: IGP (обычно IS-IS или OSPF) для обмена инфраструктурными маршрутами (обычно /32 адреса лупбеков маршрутизаторов) и MP-BGP на границе сети для обмена клиентскими IPv4, 6PE, VPNv4, 6VPE маршрутами. Технология изначально создавалась как способ снизить нагрузку на внутренние маршрутизаторы сети оператора путем замены маршрутизации IP-пакетов коммутацией по меткам. Кроме того, технология MPLS на сегодня предлагает возможность организации независимых L2/L3 VPN поверх единой MPLS-сети (MPLS-облака). А протокол RSVP в сочетании с одним из Link-State протоколов таких, как OSPF или IS-IS, предлагает также возможность инжиниринга трафика, позволяющего выгодно нагружать физические каналы внутри операторской сети. Таким образом, MPLS – высокопроизводительная гибкая технология с удобными средствами виртуализации, позволяющая легко развертывать независимые высокоскоростные WAN-сети с заявленными SLA и QoS для множества клиентов поверх провайдерской инфраструктуры. Серьезным недостатком MPLS является ее сложность, обусловленная работой тандема нескольких протоколов сиг-

нализации (control-plane), таких, как OSPF, LDP (и/или) RSVP, MP-BGP, необходимых для сложных процедур построения LSP и маршрутизации, что повышает требования к квалификации обслуживающих инженеров. К тому же, из-за распределенности control-plane сложно привести сеть к единой точке управления. Облако MPLS ограничивается оборудованием оператора связи. В качестве технологий конечного доступа обычно выступают Ethernet, GEPON, DSL, а также Wireless-технологии. На текущий момент MPLS является стандартом де-факто в операторских сетях несмотря на «солидный возраст». Однако в качестве средства предоставления WAN в корпоративных сетях данная технология сегодня сдает позиции в виду своей дороговизны, незащищенности и привязки WAN к одному (возможно, двум) оператору связи.

Наряду с WAN-технологиями, опирающимися на инфраструктуру оператора связи, ближе к концу 90-х стали набирать популярность оверлейные VPN, позволяющие связывать участки корпоративной сети непосредственно через Internet. Основной идеей данного класса технологий является различного вида туннелирование, предполагающее инкапсуляцию IP-пакетов либо L2-фреймов корпоративного трафика в тело IP-пакетов (либо дейтаграмм транспортного уровня) Internet-трафика. При этом возможно использование специальных туннелирующих протоколов, несущих дополнительные промежуточные заголовки и, возможно, способных шифровать туннелируемый трафик. Наиболее распространенной VPN-технологией стала технология IPSec, поддерживающая туннелирование трафика, его шифрование, проверку сохранения неизменности трафика в пути, а также взаимную аутентификацию сторон, устанавливающих шифрованное соединение (рис. 9).

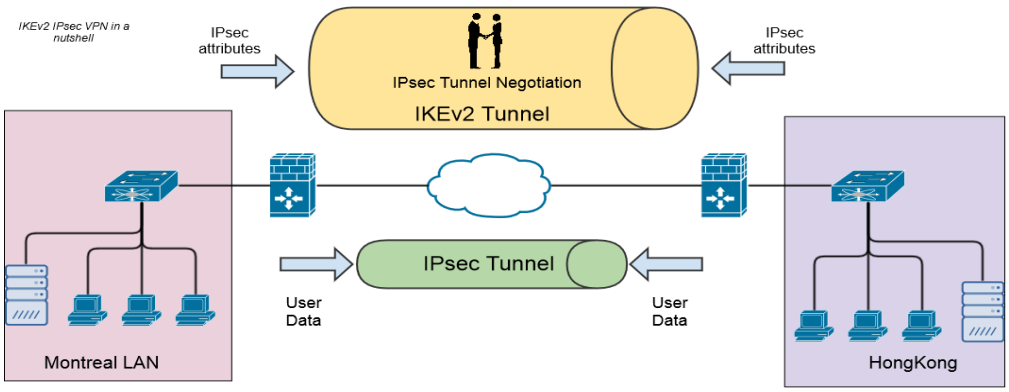

Рисунок 9 – Технология IPSec

Основой IPSec являются протоколы инкапсуляции ESP и AH, а также ISAKMP, протокол управления контекстами безопасности (Security Assotiation) и ключами. Для увеличения гибкости шифрованных туннелей совместно с IPSec часто используется разработанный в свое время компанией Cisco Systems протокол GRE (Generic Routing Encapsulation) как промежуточный слой между инкапсулированным полезным трафиком и IPSec. Оверлейные VPN позволяют напрямую через Internet связывать туннелями пограничные маршрутизаторы локальных сетей компании, не тратясь на дополнительные услуги Internet-провайдера.

Еще одним определяющим преимуществом оверлейных VPN (и IPSec в частности) являются встроенные функции безопасности. Однако простота реализации порождает существенный недостаток в виде невозможности установить SLA для туннеля в связи с недостаточным уровнем надежности Internet как транспортной среды. Вторым препятствием для организации IPSec туннелей, в отличие от MPLS VPN, могут послужить накладные расходы на шифрование на фоне низкой скорости доступа в Internet.

Когда оверлейные VPN стали использоваться достаточно широко, а пропускная способность внешних каналов достигла приемлемых значений, дешевые VPN-каналы в некоторых случаях стали рассматриваться наряду с WAN, и сами, в конце концов, сыграли эту роль. Классический IPSec VPN, тем не менее, не обладал необходимым функционалом, чтобы по праву занять нишу WAN, и разработчики сетевых технологий принялись создавать новое, базирующееся на IPSec, WAN-решение с соответствующим набором функций. В частности, компания Cisco создала решение, носящее название iWAN (Cisco Intelligent WAN). Решение iWAN предлагает четыре основных преимущества на фоне классических WAN-решений: инвариантность по отношению к транспорту; интеллектуальный контроль трафика; оптимизацию приложений; безопасность соединений.

Независимость от физического транспорта базируется на принципе оверлейной сети. В качестве оверлейной технологии используется DMVPN, представляющая собой протокол mGRE, работающий поверх IPSec. DMVPN предоставляет довольно гибкие возможности в построении оверлейных топологий, учитывая резервирование внешних физических каналов (рис. 10).

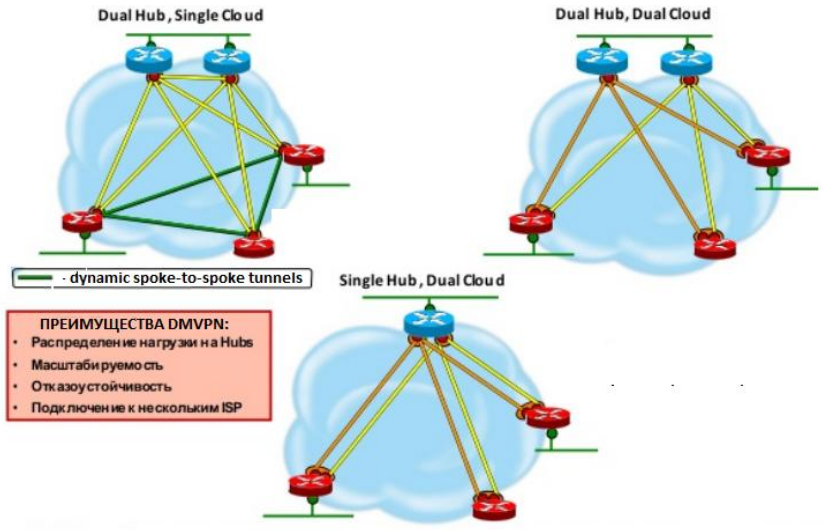

Рисунок 10 – Используемые топологии DMVPN

Протокол DMVPN создает оверлейную NBMA (None-Broadcast Multiple Access) среду (hub-and-spoke или full-mesh, достроенную автоматически поверх hub-and-spoke), в которой адресами хостов служат IP-адреса туннельных интерфейсов маршрутизаторов, а адресами канального уровня – IP-адреса внешних интерфейсов маршрутизаторов, к которым привязаны соответствующие туннельные интерфейсы(NBMA-адреса). Для разрешения туннельных адресов в NBMA-адреса служит протокол NHRP, функционирующий с помощью NHRP-сервера, являющегося одновременно хабом в топологии DMVPN.

Интеллектуальный контроль трафика предполагает дополнительные критерии выбора маршрута, необходимые для эффективной доставки приложений, балансировки нагрузки, увеличения доступности. В числе таких дополнительных критериев используются bandwidth, delay, jitter, loss и т.д. В составе iWAN интеллектуальный контроль трафика базируется на технологии PfR (Performance Routing), которая предполагает предварительный активный либо пассивный замер параметров производительности, проверку доступности каналов наряду с классификацией трафика и последующим применением политик маршрутизации. Протокол PfRv3 предполагает централизованное управление трафиком. На каждом сайте установлен Border Controller (Hub-BR, Branch-BR), в область ответственности которых входит локальное управление трафиком в пределах сайта. В его роли выступает один из пограничных маршрутизаторов. MC (Master Controller) располагается на HUB-сайте и задает политики управления трафиком для всей сети, взаимодействуя с Border Controllers каждого сайта. Стоит отметить, что PfRv3 не может функционировать самостоятельно и всегда работает совместно с протоколом маршрутизации таким, как, например, EIGRP или iBGP. Данные протоколы Cisco рекомендует как варианты использования в хорошо масштабируемых сетях на базе iWAN (рис. 11).

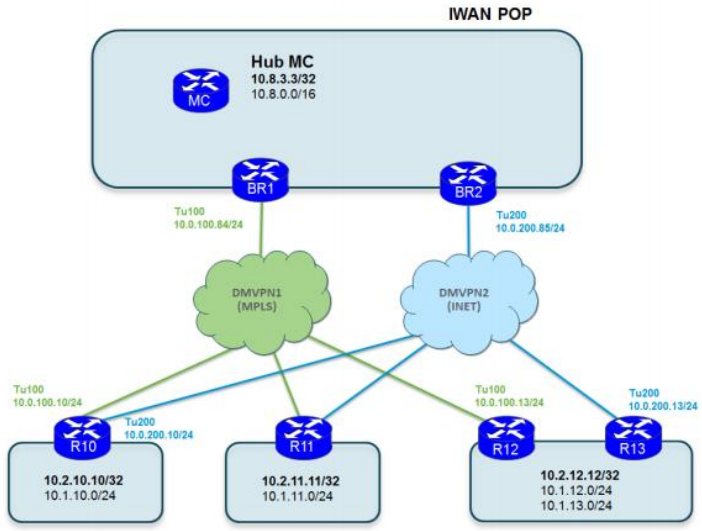

Рисунок 11 – Типовая топология iWAN

Оптимизация приложений включает в себя оптимизацию TCP-соединений, оптимизацию данных (кеширование), компрессию, оптимизацию прикладных протоколов.

6. Возникновение и развитие программно определяемых сетей

В последние годы множество технических решений, из которых складывается история компьютерных сетей, перестают удовлетворять масштабу и динамике бизнеса. Причиной тому стали несколько факторов:

• увеличение объемов трафика и преобладание в нем мультимедийной составляющей;

• необходимость в обслуживании мобильных пользователей (BYOD);

• обработка больших данных (Big Data);

• облачные сервисы и виртуализация.

Классические сети с их традиционными инструментами управления и автоматизации оказались слишком не приспособленными к динамике изменений конфигурации и масштабирования, а также к требованиям виртуализации. Потеряла былую эффективность концепция распределенного управления, при которой вся интеллектуальная составляющая работы сети была распределена по сетевому оборудованию. Рыночный запрос на новую технологию породил концепцию SDN (Software-defined Networking), что переводится как «программно определяемая сеть» [8].

Как известно, работу любого классического сетевого устройства можно рассматривать на трех уровнях (рис. 12):

1. Уровень управления устройством (Management Plane) – это встроенные командная строка, web-сервер, API, протоколы управления. Данный уровень отвечает за изменение конфигурации каждого устройства и формализует взаимодействие оператора с сетью.

2. Уровень управления трафиком (Control Plane) – часть функционала устройства, позволяющая ему контролировать состояние сети, реагировать на изменения ее состояния и предоставлять устройству информацию о том, как перенаправлять трафик в данный момент времени. Данный уровень представляет собой набор протоколов взаимодействия с соседними устройствами сети для обмена маршрутной информацией, построения топологии сети, построения путей для трафика, информирования о неисправности соседнего устройства или линка. Например, протоколы OSPF, IS-IS, EIGRP, BGP, LDP, RSVP, BFD.

3. Уровень передачи данных (Data Plane) – часть функционала устройства, ответственная непосредственно за передачу данных.

Как правило, работа на данном уровне представляет собой анализ заголовков пакетов, изменение данных заголовков при необходимости, а также перенаправление данных пакетов. Данный функционал традиционно обеспечивался узкоспециализированными микросхемами ASIC (Application Specific Integrated Circuit) или актуальными на сегодня сетевыми процессорами (Network Processor) – гибко программируемыми устройствами для производительной обработки пакетов.

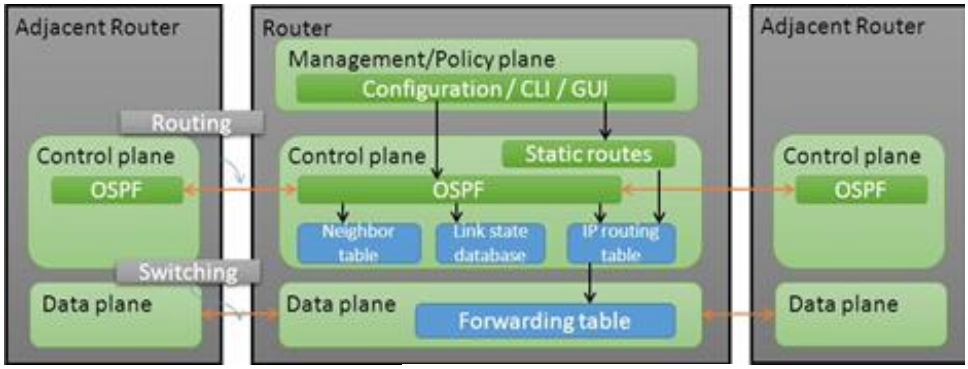

Рисунок 12 – Уровни сетевых устройств

Согласно одному из определений, программно определяемая сеть (SDN) – это сеть, в которой уровень управления отделен от уровня передачи данных и реализован программно [9]. Таким образом, вся логика управления сетью, в соответствии с концепцией SDN, должна быть изъята из сетевых устройств и реализована на отдельном сервере – SDN-контроллере. Сетевые же устройства должны ограничиться функционалом Data Plane и специальным программным интерфейсом, позволяющим SDN-контроллеру управлять работой их Data Plane. Функционал, связанный с конфигурированием и визуализацией, также выносится на отдельный уровень (Application Layer) и может быть реализован за пределами SDN-контроллера (рис. 13).

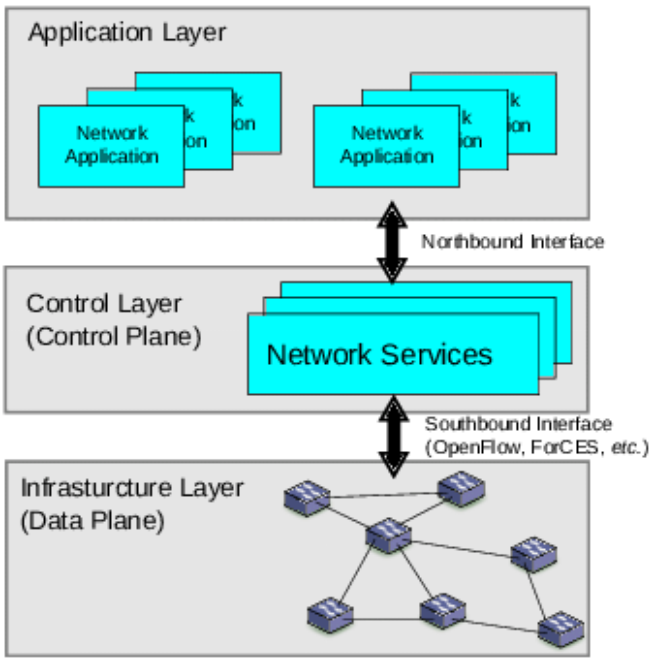

Рисунок 13 – Уровни SDN-сети

Взаимодействие SDN-контроллера с сетевыми устройствами происходит через его интерфейс, традиционно носящий название «Southbound Interface» (южный интерфейс). С различными приложениями контроллер взаимодействует через так называемый Northbound Interface (северный интерфейс).

В результате описанных выше нововведений заказчик получает функционально простое и дешевое сетевое оборудование, на рынке растет число вендоров, отсутствие необходимости разбираться в особенностях работы конкретного оборудования облегчает программирование сетевого функционала, привязанного к контроллеру. Наиболее распространенным протоколом взаимодействия сетевых устройств с контроллером (Southbound Interface) является протокол OpenFlow. Кроме OpenFlow, используются также протоколы NETCONF, OVSDB.

Взаимодействие контроллера с приложениями (Northbound Interface) осуществляется с помощью RESTful API. REST (REpresentational State Transfer – передача состояния представления) – это архитектурный стиль взаимодействия компонентов распределенного приложения в сети (не протокол обмена данными). Данному стилю могут соответствовать и HTTP-запросы. В теле таких HTTP-запросов могут использоваться такие форматы представления данных, как JSON либо XML. К веб-сервису, соответствующему REST, приме-

няется термин «RESTfull». RESTfull API позволяют разработчикам создавать приложения для управления сетью без необходимости изучения работы конкретных сетевых устройств.

Изменение вектора развития сетевых технологий вынуждает всех игроков ИТ-рынка обратить пристальное внимание на технологию SDN, которая является привлекательной для заказчиков. Именно поэтому организация Open Network Foundation (ONF) объединила множество производителей SDN на базе протокола OpenFlow, что, безусловно, укрепило его позиции и перспективы.

7. Выводы

Корпоративная сеть прошла длинный эволюционный путь от сосуществования разрозненных технологий до современной унифицированной интеллектуальной сетевой инфраструктуры с высокой безопасностью и надежным управлением. Благодаря стремительному развитию информационных технологий, корпоративные сети динамично трансформировались по различным направлениям: виртуализация сетевых функций (NFV – Network Functions Virtualization); использование SDN-решений; автоматизация процессов управления; аналитика; безопасность; использование облачных сервисов.

В результате такой трансформации корпоративная сеть превратилась в унифицированную гибкую и ориентированную на работу приложений высоконадежную инфраструктуру с легко перестраиваемым и расширяемым функционалом, единым центром управления, едиными политиками безопасности, возможностью быстрого и детального анализа происходящих в ней процессов, а также с низкими оперативными затратами.

СПИСОК ИСТОЧНИКОВ

1. История появления Интернета. URL: http://retrobazar.com/journal/interesting/988_istorija-pojavlenija-interneta.html.
2. Дизайн современной корпоративной LAN сети. URL: https://www.cisco.com/c/dam/m/ru_ru/training-events/2019/cisco-connect/pdf/sda_distributed_campus.pdf.
3. The history of WIFI. URL: https://purple.ai/blogs/history-wifi/.
4. Wireless LAN at 60 GHz. IEEE 802.11ad Explained. URL: https://web.archive.org/web/20140823221003/http://cp.literature.agilent.com/litweb/pdf/5990-9697EN.pdf.
5. Лисецкий Ю., Бобров С. WiMAX – высокоэффективная беспроводная «последняя миля». *Моделювання та інформаційні технології*. Спеціальний випуск: зб. наук. пр. Київ: Національна академія наук України, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2007. С. 21–29.
6. What Is a Wide Area Network (WAN)? URL: https://www.lifewire.com/wide-area-network-816383.
7. de Ghein L. MPLS Fundamentals Multiprotocol Label Switching (MPLS). URL: https://searchnetworking.techtarget.com/definition/Multiprotocol-Label-Switching-MPLS.
8. Introduction to Software Defined Networks (SDN). URL: https://www.researchgate.net/publication/311479628_Introduction_to_Software_Defined_Networks_SDN.
9. Overview of RFC7426: SDN Layers and Architecture Terminology. URL: https://sdn.ieee.org/newsletter/september-2017/overview-of-rfc7426-sdn-layers-and-architecture-terminology.

Стаття надійшла до редакції 28.02.2020