Российские решения
для сетевой компоненты центров обработки данных

Дмитрий ПЛЕШАКОВ,
заместитель технического директора компании ИЦ ТЕЛЕКОМ-СЕРВИС, www.teleserv.ru

Центры обработки данных (ЦОД), являясь сердцем современной цифровой инфраструктуры, требуют надежной и высокопроизводительной сетевой составляющей. Это обусловлено необходимостью поддерживать огромные объемы трафика, обеспечивать высокую доступность сервисов и соответствовать строгим требованиям безопасности и отказоустойчивости. Особенно актуально развитие отечественных решений в условиях санкционного давления и роста потребности в импортозамещении ключевых элементов IT-инфраструктуры. Российские производители активно работают над созданием конкурентоспособных продуктов, соответствующих международным стандартам качества и функциональности. Рассмотрим ключевые аспекты российских решений для сетевых компонентов ЦОД – от требований к оборудованию до примеров реализации сетей различной сложности.

Требования к сетевому оборудованию для ЦОД

Производительность и надежность

Производительность сетевого оборудования определяется несколькими ключевыми показателями:

Скорость передачи данных. Высокая пропускная способность каналов связи необходима для эффективного функционирования приложений, использующих большие объемы данных. Современные серверные платформы поддерживают скорости от 10 Гбит/с до 400 Гбит/с и выше.

Масштабируемость. Способность масштабирования сетевой архитектуры позволяет гибко реагировать на рост нагрузки путем добавления новых узлов и расширения существующих соединений.

Отказоустойчивость. Обеспечение высокой доступности критически важно для бесперебойной работы бизнес-приложений. Для достижения этого используются резервирование устройств и путей передачи данных, технологии автоматического восстановления маршрутов и балансировки нагрузки.

Важнейшими аспектами надежности являются: высокий коэффициент готовности (обычно 99,99% и выше); поддержка горячего резервирования (standby), позволяющая избежать перерывов обслуживания даже при выходе из строя отдельных компонентов, а также использование эффективных механизмов мониторинга состояния сети и раннего предупреждения о возможных проблемах.

Поддерживаемые протоколы

Современное оборудование должно поддерживать широкий спектр стандартных сетевых протоколов и технологий, среди которых наиболее значимыми являются:

- Ethernet IEEE 802.3 различных версий (включая новейшие стандарты, такие как 802.3bs/802.3cd).
- Протоколы динамической маршрутизации (OSPF, BGP, ISIS и др.).
- Технологии виртуализации и сегментирования сетей (VLAN, VXLAN, EVPN).
- Безопасные протоколы шифрования (IPsec, TLS, SSH).
- Методы управления трафиком QoS (Quality of Service).

Данные протоколы обеспечивают совместимость российского оборудования с существующими международными стандартами и позволяют интегрироваться в глобальные облачные экосистемы и корпоративные ИТ-решения.

Примеры топологий построения сети ЦОД

Рассмотрим три наиболее распространенных подхода к проектированию сетевой инфраструктуры ЦОД:

Рис. 1. Модульный коммутатор уровня распределения QTECH QSW-8113

Оборудование Qtech Источник изображения https://www.qtech.ru/catalog/

1. Топология трехуровневой иерархии («Core-Aggregation-Access»)

Эта традиционная архитектура включает следующие уровни:

Уровень ядра (core layer): обеспечивает высокую производительность и связность между всеми узлами ЦОД. Здесь размещаются мощные коммутаторы агрегации с большим числом портов и поддержкой высоких скоростей передачи данных.

Уровень распределения (aggregation layer): объединяет ресурсы уровня доступа и передает данные на ядро. Используется для подключения локальных зон и распределения ресурсов.

Уровень доступа (access layer): соединяет конечные устройства (серверы, хранилища данных). В современных центрах обработки данных обычно организуется по принципу Top-of-Rack (когда в каждой стойке имеется коммутатор, к которому подключено оборудование, установленное в ней) или End-of-Row (когда коммутатор устанавливается в конце ряда стоек).

Преимущества такой структуры включают простоту эксплуатации и поддержки, хорошую расширяемость и возможность выбора оптимальных решений для каждого слоя.

Примеры российского оборудования для данной топологии:

- Модульный коммутатор ядра QTECH QSW-7610. Коммутаторы уровня ядра серии QSW-7600 разработаны специально для интегрированных сетей следующего поколения. Шасси имеет 8 слотов для сервисных модулей, 2 слота для модулей управления, 2 слота для модулей коммутаторной матрицы, имеет резервирование модулей управления, питания и вентиляции. Заявленная производителем производительность коммутационной матрицы составляет 12800 Гбит/с, пропускная способность – 9523,2 Мпак/с.
- Модульный коммутатор уровня распределения QTECH QSW-8113. Шасси имеет 6 слотов для сервисных модулей и 2 слота для модулей управления. Производительность коммутационной матрицы до 9600 Гбит/с, пропускная способность – 7142,4 Мпак/с.
- Коммутаторы Eltex MES5300-24, оснащенные 6 интерфейсами с поддержкой 40GBASE-R/100GBASE-R и 24 портами 1000BASE-X /10GBASE-R, предназначенные в качестве Top-of-Rack или End-of-Row-коммутаторов в современных центрах обработки данных.

Недостатками трехуровневой топологии («Core-Aggregation-Access») можно назвать:

- Сложность администрирования: из-за наличия нескольких уровней иерархии усложняется процесс настройки и управления сетью. Изменения в одном уровне могут повлиять на остальные части сети, что требует внимания архитектора сети и координации действий администраторов.
- Зависимость от центрального узла: если произойдет сбой на уровне ядра или агрегации, это приведет к значительным проблемам с доступностью сети. Центральные точки отказа повышают риски нарушения работоспособности сети.
- Проблемы с производительностью: по мере роста сети количество транзитных пакетов увеличивается, создавая дополнительную нагрузку на каналы связи. Если каналы перегружены, это снижает общую производительность сети.
- Повышенные задержки: пакеты проходят через несколько промежуточных слоев, что добавляет дополнительные задержки. Хотя современное оборудование способно минимизировать этот эффект, проблемы остаются заметными в больших сетях.

Таким образом, несмотря на свою популярность и распространенность, трехуровневая топология подходит не каждому проекту, особенно там, где важна максимальная производительность и минимальные издержки на обслуживание.

Рис. 2. Коммутатор ToR (Top-of the-Rack) Eltex MES5300-24

Оборудование Eltex: Источник изображения: https://eltex-co.ru/

2. Топология Clos (Spine-leaf architecture)

Clos-топология представляет собой сеть с двумя основными элементами:

Spine-коммутаторы (хребтовое звено): формируют высокоэффективную магистральную структуру с высоким уровнем пропускной способности и минимальными задержками.

Leaf-коммутаторы (листовые узлы): отвечают за подключение серверов и межсегментную связь внутри одного сегмента.

Такая структура позволяет обеспечить низкую латентность и высокий уровень масштабируемости. Ключевым преимуществом является простота проектирования и высокая скорость реакции на изменения конфигурации сети.

Пример отечественного оборудования для Clos-топологии:

- Коммутаторы Eltex MES5500-32 – это высокопроизводительные устройства, оснащенные 32 интерфейсами 40GBASE-R и 100GBASE-R, специально разработанные для использования в сетях ЦОД в качестве Spine-коммутаторов.
- Коммутаторы Eltex MES5410-48 – это высокопроизводительные устройства, имеющие 6 интерфейсов 40GBASE-R/100GBASE-R для подключения к spine коммутаторам и 48 портов 10GBASE-R, предназначенные для использования в качестве leaf-коммутаторов или в качестве Top-of-Rack или End-of-Row-коммутаторов в трехуровневой архитектуре.

Топология Clos получила широкое распространение благодаря своей простоте, низкой латентности и хорошей масштабируемости. Тем не менее, у неё имеются некоторые недостатки, которые стоит учитывать при выборе сетевой архитектуры:

Повышенная чувствительность к нагрузкам – вся нагрузка равномерно распределяется между spine-коммутаторами и leaf-коммутаторами. Если возникает неравномерная нагрузка или сбои в работе некоторых узлов, сеть может испытывать деградацию производительности вплоть до полной потери соединения.

Рис. 3. SDN-коммутатор DEPO Switch 4360FK

Оборудование DEPO: Источник изображения: https://www.depo.ru/catalog/kommutatory/

Необходимость избыточных связей – число необходимых физических связей между spine и leaf значительно больше, чем в традиционных трёхуровневых схемах. Например, каждый листовой узел (leaf switch) должен иметь соединение с каждым спиновым узлом (spine switch). Это ведёт к повышению расходов на кабели и дополнительное пространство для разводки.

Потребность в специальных механизмах управления – для поддержания оптимальной производительности и правильного распределения трафика требуется использование сложных методов балансировки нагрузки и мониторинга сети. Это усложняет настройку и администрирование сети, требуя квалифицированного персонала и дополнительного программного обеспечения.

Дополнительные требования к оборудованию – Topology Clos предъявляет повышенные требования к производительности и ресурсам spine-коммутаторов. Они должны обладать большой пропускной способностью и поддерживать большое количество соединений одновременно. Это влияет на выбор оборудования и удорожает инфраструктуру.

Таким образом, топология Clos идеально подходит для высоконагруженных сетей с большими объемами данных и высокими требованиями к производительности. Но при малом масштабе сети или отсутствии грамотного управления преимуществами топологии воспользоваться сложно, а расходы на реализацию могут превысить выгоду. Поэтому важно внимательно оценивать перспективы роста и характер нагрузок перед принятием решения о переходе на такую архитектуру.

3. Топология Fabric-подход (например, SDN/Fabric)

Fabric (или Software Defined Network, SDN) предполагает создание единой управляемой среды, где управление сетью осуществляется централизованно. Основные элементы сети подключены к единому управляющему контроллеру, что упрощает конфигурирование и мониторинг всей системы.

Преимуществом данного подхода является снижение стоимости владения, повышение эффективности использования ресурсов и автоматизация процессов.

Ярким примером отечественной разработки является первое в России полностью импортонезависимое решение для организации программно-определяемых сетей – Basis SDN, недавно выпущенное компанией «Базис», российским разработчиком экосистемы для управления динамической ИТ-инфраструктурой.

Кроме того, следует отметить коммутаторы DEPO Switch 4360FK, специально разработанные для создания программно-конфигурируемых сетей SDN в центрах обработки данных. Коммутатор оснащен 36 портами 40/56 Гбит/с QSFP, каждый из которых с помощью специальных переходников и/или кабелей может трансформироваться в порт 10 Гбит/с. Устройство оснащено процессором 1047UE, имеет 4 Гб оперативной памяти и 16 Гб флэш-памяти, а также обеспечивает коммутационную емкость в 4,032 Тбит/с.

При всех преимуществах SDN-концепции, ее применение в центрах обработки данных также связано с определёнными рисками и недостатками:

Зависимость от управляющего компонента – основная особенность SDN заключается

в отделении плоскости управления (контроллера) от плоскости данных (коммутации и маршрутизации). Однако эта схема создает потенциальные точки отказа:

- управляющий компонент становится центральным элементом сети, и его выход из строя может привести к остановке работы всей сети или значительной части её функций;
- контроллер SDN обрабатывает значительное число запросов и команд. При увеличении масштаба сети нагрузка на контроллер возрастает, что может замедлить работу сети или вызвать нестабильность.

Сложность внедрения и настройки – хотя SDN обещает упростить настройку и управление сетью, на практике интеграция SDN может оказаться сложной задачей:

- переход на SDN часто требует обновления существующего оборудования и специализированных настроек. Некоторые традиционные устройства могут не поддерживать SDN-функционал или требовать доработок;
- настройка правил маршрутизации и политики безопасности может стать сложнее из-за разделения функций между физическим оборудованием и управляющим компонентом.

Проблемы безопасности – SDN вводит новые возможности атак и уязвимости:

- управление всей сетью сосредоточено в одном месте, что делает контроллер привлекательной целью для злоумышленников. Взлом контроллера может позволить хакерам управлять всей сетью;
- появляются угрозы, специфичные именно для SDN, такие как атаки на механизмы трансляции таблиц потоков (Flow Table Poisoning) или атаки типа «отказ в обслуживании» (DoS/DDoS) против контроллеров.

Технология SDN открывает много возможностей для оптимизации и упрощения управления сетью, но её успешное внедрение требует серьёзных вложений, высокого уровня подготовки сотрудников и понимания потенциальных рисков. Перед выбором SDN-решений рекомендуется провести детальное тестирование и оценку конкретных потребностей вашей организации.

Оборудование для сетевой компоненты ЦОД

Среди производителей, предлагающих надежные отечественные решения для сетевой инфраструктуры ЦОД, выделяются:

- **«Элтекс»** – компания производит коммутационное и маршрутизирующее оборудование различного класса, от базовых моделей (MS11xx, MS22xx) для нужд небольшого офиса и до мощных устройств уровня ядра. Все продукты сертифицированы и соответствуют российским стандартам информационной безопасности.
- **Qtech** – специализируется на выпуске мощных маршрутизаторов и шлюзов, используемых в телекоммуникационных сетях операторов связи и крупных предприятиях. Продукция отличается высокими характеристиками отказоустойчивости и надежностью, соответствующей международным стандартам.
- **Компания «Сила»** – российский производитель высококачественного ИТ-оборудования. Модельный ряд сетевого оборудования «Сила» включает в себя коммутационное оборудование уровня ядра и агрегации (серия СКЗ-300), ЦОД (серия СКЗ-400 и СКЗ-600).

Все перечисленные решения ориентированы на достижение максимальной эффективности и соответствия актуальным нормативным актам РФ, таким как ГОСТ Р 54417–2011 и другие регулирующие документы.

Перспективы развития и современные тенденции

Российский рынок сетевого оборудования продолжает демонстрировать устойчивый рост благодаря активной поддержке государства и частных инвесторов. Основными направлениями развития становятся:

- Увеличение объема инвестиций в разработку перспективных технологий и интеграционные проекты.
- Создание совместных исследовательских лабораторий для повышения компетенций разработчиков и специалистов отрасли.
- Активное внедрение принципов Open Compute Project (OCP) и использование открытого программного обеспечения для снижения рисков блокировки западных поставщиков.

Приоритетные области исследований включают оптимизацию энергопотребления, улучшение тепловых характеристик, увеличение плотности размещения аппаратных средств и обеспечение высокой степени автоматизации процессов управления сетевыми ресурсами.

Кроме того, наблюдается тренд на переход к гибридным инфраструктурам, сочетающим физические и виртуализированные ресурсы, что позволит повысить эффективность использования вычислительных мощностей и снизить затраты на эксплуатацию ЦОД.

Заключение

Отечественная индустрия демонстрирует уверенный прогресс в разработке и внедрении передовых решений для сетевой составляющей ЦОД. Уже сегодня российский рынок предлагает богатый выбор высокотехнологичных решений, удовлетворяющих запросам большинства пользователей и эффективно конкурирующих с зарубежными аналогами.

Дальнейшее развитие индустрии потребует привлечения высококвалифицированных кадров, совершенствования регуляторной базы и усиления сотрудничества между государством, бизнесом и научными учреждениями. Только объединяя усилия всех заинтересованных сторон, Россия сможет создать полноценную альтернативу западному рынку сетевого оборудования и занять достойное место в мировой технологической гонке. ■