

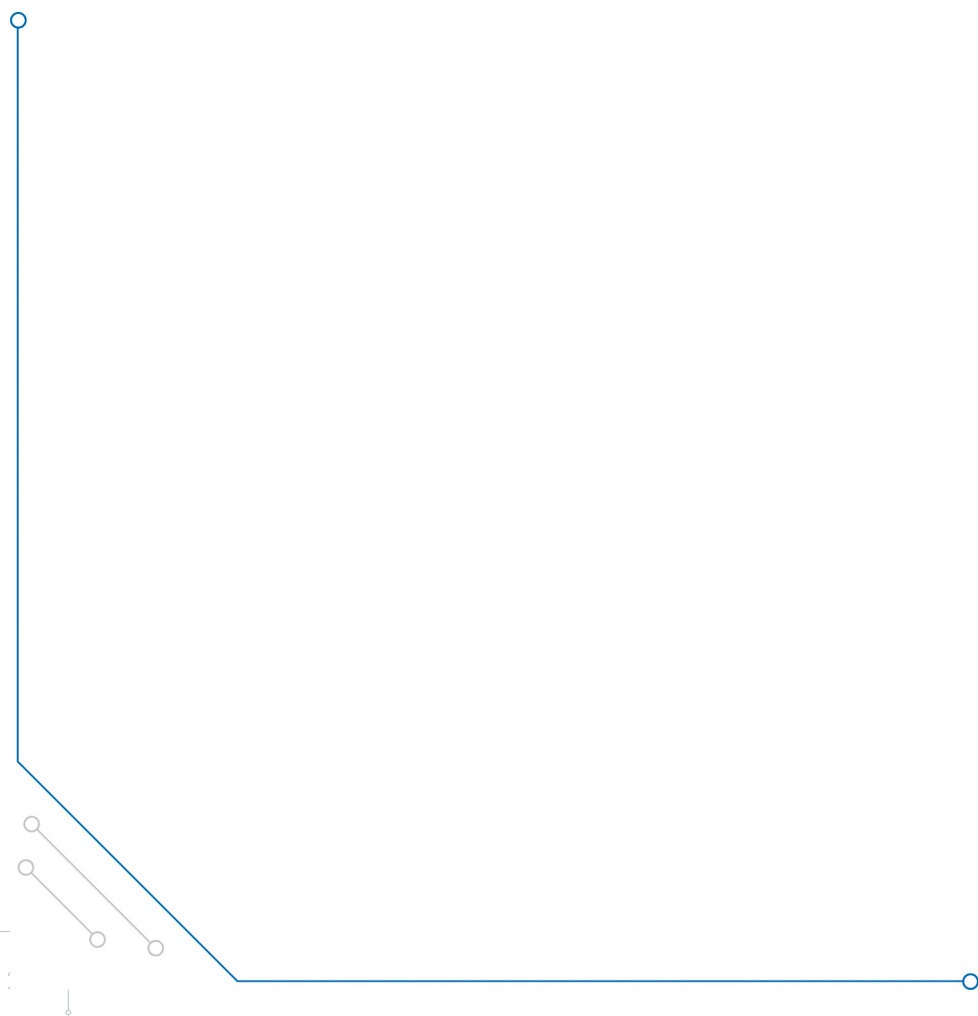
ДатаРy



СЕРИЯ КОММУТАТОРОВ
ДАТАРУ КА СХ9300

ОГЛАВЛЕНИЕ

| | |
|---|-----------|
| Серия коммутаторов линейки ДатаРу КА CX9300..... | <u>3</u> |
| Основные характеристики | <u>4</u> |
| Технические характеристики. Таблица..... | <u>10</u> |
| Поддерживаемые стандарты, протоколы и их реализации | <u>12</u> |



СЕРИЯ КОММУТАТОРОВ ЛИНЕЙКИ ДАТАРУ КА CX9300

Высокопроизводительные коммутаторы для Enterprise-сетей ЦОД



ДатаРу КА CX9300 — это серия коммутаторов нового поколения с уровнем производительности в 25,6 Тбит/с и высотой всего 1U. Коммутаторы оснащены 32 портами, поддерживающими пропускные способности в 100GbE, 200GbE и 400GbE*. ДатаРу КА CX9300 — это идеально гибкий по сфере применения продукт для организации экономически целесообразного решения с высокой коммутационной плотностью для 400 GbE-серверов, СХД, а также для интраконнекта коммутационных фабрик (intra-fabric connectivity). Коммутаторы этой серии помогут защитить вложения в критически важную сетевую инфраструктуру во время процесса архитектурной миграции серверных ферм предприятия с 10 GbE и 10/25 GbE на 100/400 GbE EVPN-VXLAN leaf- и/или spine-конфигурации, которые будут занимать меньшую площадь и иметь меньшее совокупное энергопотребление (углеродный след). Их масштабируемость/коммутационная плотность в 8 раз выше по сравнению с моделью ДатаРу КА CX8325–32С, которая масштабируется до показателя в 700 серверов 25GbE.

Решения линейки ДатаРу КА CX9300 могут использоваться как 100GbE-коммутаторы в роли leaf или как 100GbE/400GbE-коммутаторы в роли spine (128 портов 100GbE или 64 порта 200GbE с breakout-коммутацией). В случае деплоя в роли spine коммутатор ДатаРу КА CX9300 может быть подключен к коммутаторам, сконфигурированных в роли leaf, из линеек ДатаРу КА CX8325 или ДатаРу КА CX8360.

С выходом последнего релиза операционной системы AOS-CX модели из линеек CX9300 и CX8325 стали идеальным решением для ЦОД, облаков и СХД; они могут выполнять роль top-of-rack для серверов/СХД и поддерживают масштабируемую "leaf-spine" топологию сетевых фабрик. Эти инновационные обновления в операционной системе AOS-CX обеспечивают оптимизацию сети для СХД: они гарантируют низкое время задержки в сети и "lossless"-качество работы с гарантированными и надежными политиками «Качества обслуживания» (QoS), предоставляя именно те характеристики, которые необходимы для СХД.

*Поддержка функционала 25GbE и 50GbE ("split-out") появится в будущем релизе ОС AOS-CX.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ ЛИНЕЙКИ AOS-CX — современная операционная система

Серия коммутаторов ДатаРу КА CX9300 управляется программируемой сетевой операционной системой AOS-CX. Основанная на базе данных современная операционная система автоматизирует и упрощает многие критически важные и сложные сетевые задачи. Встроенная база данных временных рядов ("time-series" БД) позволяет клиентам и разработчикам использовать программные сценарии для ретроспективного траблшутинга и анализа трендов прошлого. Это помогает прогнозировать и устранять проблемы, влияющие на показатели масштабируемости, безопасности и производительности.

Полный функционал сетевой операционной системы AOS-CX «зашит» в программные лицензии разного уровня — CX Foundation (базовый) и CX Advanced (расширенный). Каждый коммутатор серии ДатаРу CX поставляется с бесплатной активированной лицензией CX Foundation. В базовой лицензии CX Foundation есть все необходимые возможности для развертывания, подключения и траблшутинга в Enterprise-сети, включая:

- Network Analytics Engine (NAE).
- Динамическая сегментация.
- Стекирование коммутаторов.
- Высокая доступность ресурсов и отказоустойчивость.
- Quality of Service (QoS).
- Коммутация уровня L2.

- Сервисы и маршрутизация уровня L3.
- “IP Multicast”.
- Сетевая безопасность.

Сетевая операционная система AOS-CX построена на модульной Linux-архитектуре со “Stateful” базой данных, что обеспечивает следующие уникальные возможности:

- Легкий и понятный доступ ко всей информации о состоянии сети предоставляет уникальные возможности в плане аналитики и визуализации данных.
- Поддержка REST API и Python-скриптов обеспечивает точную и тонкую программируемую настройку сетевых задач.
- Микросервисная архитектура делает возможной полную интеграцию с любыми другими, уже запущенными в эксплуатацию, системами и сервисами.
- Постоянная синхронизация состояний обеспечивает непревзойденную отказоустойчивость и высокую доступность ресурсов.
- Все программные процессы коммуницируют с базой данных гораздо чаще, нежели друг с другом. Это гарантирует представление текущего состояния сети в режиме, близком к реальному времени, и позволяет производить независимое обновление отдельных программных модулей, чтобы обеспечить более высокий уровень доступности.

Network Analytics Engine (NAE) — средство продвинутого мониторинга и диагностики

AOS-CX включает средство расширенного мониторинга и диагностики Network Analytics Engine (NAE) для телеметрии и автоматизации на продвинутом уровне. Платформа NAE — это лучшая в индустрии система мониторинга и траблшутинга, обеспечивающая значительное улучшение работы сети. Она позволяет легко отслеживать и устранять проблемы, которые нарушают работоспособность сети, системы, приложений и снижают безопасность, с помощью скриптов Python и REST API. База Данных временных рядов (“Time Series Database”) сохраняет в себе конфигурации и служебные оперативные данные, которые позволяют быстро устранять неполадки в сети. Эти данные могут быть также использованы для аналитики трендов, идентификации аномалий и предсказания будущих необходимых требований, предъявляемых к емкости сети.

Оптимизация для Ethernet-сетей под СХД от HPE

ДатаПу КА CX9300 — это идеальное решение для центров обработки данных, облачных вычислений и систем хранения данных, которое может использоваться в роли Top-of-Rack для подключения к серверам и системам хранения данных и в архитектуре leaf-spine в масштабируемых сетевых фабриках.

В AOS-CX добавлены улучшения для оптимизации хранения данных, которые обеспечивают работу сети с малыми задержками и без потерь и характеристики подключения, необходимые для СХД.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ:

- Более 25,6 Тбит/с производительности матрицы коммутации с пакетной пропускной способностью до 5000 Мпак/с.
- Компактное 1U-решение, обеспечивающее высокую коммутационную плотность с поддержкой до 32 400GbE – интерфейсов.
- Высокий уровень доступности ресурсов с лидирующим в индустрии функционалом VSX-резервирования, а также поддержка функционала резервирования блоками питания и вентиляторными модулями.
- Использование в роли Spine, на уровне ядра/агрегации, а также в роли Top of Rack, Leaf или End of Row в ЦОД.
- Автоматизация и программируемая настройка AOS-CX с помощью REST API и Python-скриптов.
- Расширенный набор функций уровня L2/L3 с поддержкой BGP, OSPF, VRF-Lite и IPv6.
- Технология динамической виртуализации VXLAN с BGP-EVPN для глубокой сегментации в сетях ЦОД и кампуса.
- Интеллектуальный мониторинг, графическое представление структуры сети и устранение узких мест благодаря функциональным возможностям Network Analytics Engine (NAE).
- Оптимизация для сетей под СХД от HPE.

Функционал расширенной виртуальной коммутации Virtual Switching Extension (VSX)

Способность сетевой операционной системы AOS-CX поддерживать синхронизацию состояний с использованием “dual control planes” позволяет реализовать решение с высокой доступностью ресурсов, называемое Virtual Switching Extension (VSX). VSX обеспечивает высокую избыточность благодаря развертыванию двух шасси с межкоммутационным линком, где каждое шасси сохраняет независимое управление.

В VSX применяются лучшие на сегодняшний момент технологии обеспечения высокой доступности ресурсов, такие как функционал агрегации линков между несколькими шасси MC LAG (Multi-chassis Link Aggregation) и фреймворк виртуализации коммутаторов VSF (Virtual Switching Framework). Это позволяет реализовать распределенную архитектуру с высокой степенью доступности ресурсов даже во время апгрейда или событий на уровне “control plane”.

Поддерживаются следующие возможности:

- Синхронизация состояний в режиме реального времени благодаря AOS-CX.
- Гибкие, в плане дизайна и архитектуры сетей, свойства и характеристики оборудования, заложенные на этапе проектирования в виде реализации схемы резервирования “active-active” сетевой архитектуры на уровнях L2 и L3.

- Простота эксплуатации для упрощенного процесса настройки.
- Высокий уровень доступности ресурсов во время обновлений, включая поддержку VSX Live Upgrade с утечкой трафика LACP.

ВОЗМОЖНОСТИ КОММУТАТОРОВ ДАТАРУ СЕРИИ KA CX9300

ПРОИЗВОДИТЕЛЬНОСТЬ

Высокая производительность полностью распределенная архитектура

- Производительность матрицы коммутации до 25,6 Тбит/с для двунаправленной коммутации с пакетной пропускной способностью до 5000 Мпак/с. Вся коммутация и маршрутизация выполняются на уровне “wire-speed” (максимальной пропускной способности интерфейса), что позволяет удовлетворять высокие требования приложений к полосе пропускания сегодня и в будущем.

Масштабируемый дизайн системы

- Обеспечивает защиту инвестиций при внедрении новых технологий и более высокоскоростных соединений в будущем.

ВОЗМОЖНОСТИ ИНТЕРФЕЙСОВ

Несколько вариантов плотности портов

Компактные коммутаторы 1U с высокой плотностью портов и гибким менеджментом коридоров направления воздушных потоков доступны в следующих конфигурациях:

- 32 порта 100GbE, 200GbE или 400GbE. Порты 400 Гбит/с могут быть сконфигурированы как 4x100GbE, 2x200GbE или 1x400GbE.

Jumbo frames

- Поддержка Jumbo Frames позволяет сохранять бэкапы на высокой скорости и работать высокоскоростным системам восстановления данных. Максимальный поддерживаемый размер Jumbo Frame — 9К байт.

Функция “Loopback Detection”

- Поддерживается функционал тестирования на наличие внутреннего loopback для упрощения процессов технического обслуживания и повышения уровня доступности сети и ресурсов; функция “loopback detection” позволяет защитить сеть и коммутаторы в ней от некорректного подключения сетевых кабелей или неправильной конфигурации администратором. Данная функция может быть активирована на уровне физического порта или на уровне VLAN.

Защита от пакетных штормов

- Защита от неизвестных broadcast-, multicast- или unicast-штормов с задаваемыми пользователем пороговыми значениями.

ФУНКЦИИ И ФУНКЦИОНАЛ QUALITY OF SERVICE (QOS)

Очереди Strict priority (SP) и Deficit Weighted Round Robin (DWRR)

- Позволяет избежать перегрузок в сети, обеспечивая более эффективное использование сетевых ресурсов, благодаря congestion avoidance.

Data Center Bridging (DCB)

- Поддержка Lossless Ethernet позволяет предотвратить потерю пакетов из-за переполнения очереди.
- Поддержка протокола Priority Flow Control (PFC), 7 уровней приоритета на порт.
- Поддержка Enhanced Transmission Service (ETS).
- Поддержка DCB Exchange Protocol (LLDP DCBX по стандарту IEEE, предварительная версия 1.01).

Flow-Control Guard

- Предотвращает чрезмерные перегрузки в сети благодаря регулярному процессу удаления избыточного трафика и позволяет избежать длительные задержки передачи пакетов.

ECN с функцией “slope”

- Маркирует пакеты как ECN-CE (Congestion Experienced), что помогает TCP уменьшить размер окна приема по время перегрузки.

ПЕРЕДОВЫЕ ВОЗМОЖНОСТИ НАСТРОЙКИ ПУЛА БЕЗ ПОТЕРИ ДАННЫХ

Динамическая настройка пула

- Поддерживается настройка пула без необходимости перезагрузки коммутатора с передачей трафика без потерь.

ПОЛНАЯ СТАТИСТИКА БУФЕРИЗАЦИИ

Поддержка решений хранения данных

- iSCSI, Lossless iSCSI, RDMA over Converged Ethernet версии 2 (RoCE v1 и v2) и Non-Volatile Memory Express (NVMe over Fabrics).

ВЫСОКАЯ ДОСТУПНОСТЬ РЕСУРСОВ И РЕЗЕРВИРОВАНИЕ

Вентиляторы и блоки питания, обеспечивающие более равномерное распределение ресурсов и нагрузки

- Повышает общую производительность и доступность питания.

Модули блоков питания и вентиляторов с возможностью горячей замены (“Hot Swap”)

- Позволяет заменять модули, не влияя на работу других модулей и коммутаторов.

Разделение каналов передачи данных и управления

- Отделяет каналы управления от каналов работы сервисов, изолируя обработку сервисов; повышает безопасность и производительность.

Virtual Switching Extension (VSX)

- Функционал расширенной виртуальной коммутации Virtual Switching Extension (VSX) обеспечивает распределенную архитектуру с высокой избыточностью за счет развертывания двух коммутаторов, каждый из которых сохраняет независимое управление, но остается синхронизированным при обновлении или аварийном переключении. Поддерживается обновление «на лету» (в процессе эксплуатации).

Virtual Router Redundancy Protocol (VRRP)

- VRRP позволяет группе коммутаторов динамически создавать высокодоступное маршрутизируемое пространство.
- Также поддерживается возможность пропускать маршруты к/от основного VRF-маршрутизатора.

Bidirectional Forward Detection (BFD)

- Обеспечивает обнаружение неисправностей в сети за долю секунды и используется для быстрой перебала-сировки маршрутов в сетях.

Ethernet Ring Protection Switching (ERPS)

- Обеспечивает защиту и быстрое восстановление в сетях с топологией вида «звезда».

Unidirectional Link Detection (UDLD)

- Проверяет наличие соединения через линк и отключает порты на обеих сторонах линка в случае обнаружения однонаправленного трафика, что предотвращает закольцовывание в сетях с использованием STP.

IEEE 802.3ad LACP

- Поддерживает до 128 LAG'ов, до 16 линков/соединений на один LAG (32 для VSX-пары); а также определяемый пользователем алгоритм хэширования L1-L4.

УПРОЩЕННАЯ НАСТРОЙКА И УПРАВЛЕНИЕ СЕТЬЮ

Помимо Network Analytics Engine серия коммутаторов KA CX9300 предлагает следующие возможности: Встроенный программируемый интерфейс REST API с простым в использовании функционалом.

Стандартный в индустрии интерфейс командной строки (CLI) с иерархической структурой

- Уменьшает стоимость и время обучения администраторов сети, повышая продуктивность эксплуатации в мультивендорских сетях.

Безопасность управления

- Ограничивает доступ к критическим командам конфигурации; предлагает несколько уровней привилегированного доступа с защитой паролем; списки контроля доступа (ACL) обеспечивают доступ к протоколу SNMP; локальные и удаленные возможности Syslog позволяют регистрировать любой доступ.

- Private VLAN (PVLAN) обеспечивает изоляцию трафика между пользователями в одной сети VLAN. Порт коммутатора может взаимодействовать только с другими портами в той же группе и/или с uplink-портом, независимо от идентификатора VLAN или MAC-адреса назначения. Ограничение одноранговой коммуникации предотвращает различные вредоносные атаки и повышает безопасность сети.

IPSLA

- Отслеживает ухудшение качества различных сервисов в сети, включая голосовую связь.
- Мониторинг через NAE отслеживает историю и обеспечивает моментальный автоматический сбор дополнительной информации при обнаружении аномалий.

SNMP v2c/v3

- Обеспечивает возможность чтения и отправки SNMP-трэпов в базе промышленного стандарта MIB (Management Information Base) и ее частных расширениях.
- Поддержка TCN-трэпов в рамках STP, STP New Root и изменения описания интерфейса через SNMP (SNMP-Write-Set-Description on Interface).

sFlow® (RFC 3176)

- Обеспечивает масштабируемый мониторинг и учет сети на основе ASIC на максимальной скорости интерфейса без ущерба производительности сети; это позволяет сетевым операторам собирать разнообразную сложную сетевую статистику и информацию для планирования емкости и мониторинга сети в реальном времени.

Удаленный мониторинг (RMON)

- Использует стандартный протокол SNMP для мониторинга основных функций сети и поддерживает группы событий, тревожных сообщений, истории и статистики, а также группу расширений для частных тревожных сообщений.

Поддержка протоколов TFTP и SFTP

- Поддерживает различные механизмы апдейта конфигурации устройств; обычный протокол FTP (TFTP) позволяет организовать двунаправленную передачу данных по TCP/ IP-сети.
- Протокол SFTP (Secured File Transfer Protocol), в отличие от «обычного» TFTP, запускается «поверх» туннеля протокола SSH для обеспечения дополнительного уровня безопасности.

Утилиты Debug и Sampler

- Поддерживают команды “ping” и “traceroute” для протоколов IPv4 и IPv6.

Протокол NTP (Network Time Protocol)

- Синхронизирует и поддерживает обмен информацией между территориально распределенными серверами

и клиентами данного протокола; поддерживает синхронизацию между всеми устройствами, чья работа зависит от времени и его точности, и гарантирует наличие постоянного синхронного показания системных часов в них.

- Может служить NTP-сервером.

Протокол LLDP (Link Layer Discovery Protocol)

по стандарту IEEE 802.1AB

• Анонсирует и принимает служебную информацию от всех соседних устройств сети, что упрощает маппинг служебных управляющих сетевых приложений и сервисов.

LACP-fallback

• Позволяет автоматически переключаться на режим LACP, если основной режим работы недоступен.

Функция "Dual Flash Images"

• Обеспечивает хранение primary- и secondary-файлов образов операционной системы в энергонезависимой памяти для бэкапа и для безопасного обновления ОС.

Множество версий файлов конфигурации устройства

• Могут храниться в энергонезависимой памяти устройства.

СЕРВИСЫ, ПРОТОКОЛЫ И ФУНКЦИИ КОММУТАЦИИ УРОВНЯ L2 (LAYER 2 SWITCHING)

VLAN

• Поддержка до 4040 VLAN на базе портов или IEEE 802.1Q

Переназначение VLAN

• Данная функция ремапирует VLAN'ы в процессе передачи трафика в ядре сети.

Туннелирование данных протокола BPDU (Bridge Protocol Data Unit)

• Поддерживает прозрачное туннелирование данных STP BPDU, что позволяет проводить корректные вычисления древа через сети интернет-провайдеров/операторов связи, WAN или MAN.

Зеркалирование порта

• Позволяет продублировать трафик с одного порта (входящий и исходящий потоки трафика) на локальный или удаленный порт для мониторинга или захвата этого трафика; поддерживается до 4-х зеркалируемых групп, с неограниченным количеством портов на группу.

STP

• Поддерживает стандарты IEEE 802.1D STP, IEEE 802.1w (RSTP) Rapid Spanning Tree Protocol для ускорения конвергенции и IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

Rapid Per-VLAN Spanning Tree Plus (RPVST+)

• Позволяет каждому VLAN построить свое собственное древо протокола STP, чтобы повысить пропускную способность линка в сетевых окружениях с несколькими VLAN.

Internet Group Management Protocol (IGMP)

• Контролирует и управляет потоками пакетов мультикаст-рассылки на сетевом уровне L2.

Статический VXLAN

• Позволяет операторам вручную соединить две или больше конечные точки туннеля VXLAN (VTEP).

Динамический VXLAN с BGP-EVPN

• Глубокая сегментация для сетей ЦОД в топологии Spine/Leaf и кампусных сетей уровня L3 с централизованным шлюзом и симметричным интегрированным маршрутизатором и мостом (IRB) на основе распределенных шлюзов VXLAN туннелей.

• EVPN и VXLAN поддерживают следующие возможности: настройка маппинга маршрутов для входящего и исходящего трафика, сопоставление L3VNI с определенными правилами маршрутизации, настройка локального приоритета, установка следующей точки для трафика (ip next-hop), добавление префиксов "as-path", сопоставление ip/ipv6-адресов с определенными правилами маршрутизации.

- Поддержка VXLAN DC multi-fabric DCI.

Multicast

- Поддержка PIM Multicast Boundary (v4).
- «Мягкое» завершение работы VSX для IGMP/MLD.
- Поддержка Multicast NSF.

Мультикаст-рассылка IPv4 через VXLAN/EVPN оверлей

• Поддерживает перехват ("snooping") PIM-SM/IGMP в VXLAN оверлее.

Поддержка IPv6 через VXLAN/EVPN оверлей

• Поддерживает передачу IPv6 трафика через VXLAN оверлей.

Распределенный Anycast-шлюз VXLAN-сети

• Механизм адресации, который позволяет использовать одни и те же IP-адреса шлюза на всех leaf-коммутаторах сети VXLAN.

• Поддержка активного перенаправления данных между виртуальными коммутаторами (VSX Active Forwarding) с использованием VXLAN.

VXLAN ARP/ND Suppression

• Позволяет минимизировать флуд ARP- и ND-трафика внутри отдельных VXLAN-сегментов, оптимизируя работу VXLAN-сети.

СЕРВИСЫ, ПРОТОКОЛЫ И ФУНКЦИИ КОММУТАЦИИ УРОВНЯ L3 (LAYER 3 SWITCHING) Address Resolution Protocol (ARP)

- Определяет MAC-адреса других IP-хостов в пределах одной подсети; поддерживается статический ARP.
- Gratuitous ARP позволяет обнаружить дублирование IP-адресов.
- Proxy ARP позволяет обеспечить нормальную работу протокола ARP между подсетями или в тех случаях, когда подсети разделены сетью уровня L2.

IP Directed Broadcast

- Поддерживает направленную рассылку ("directed broadcast") в настроенных подсетях сети.

Dynamic Host Configuration Protocol (DHCP)

- Сервисы DHCP используются в клиентских сетях для упрощения управления сетью.
- DHCP Relay позволяет транслировать работу протокола DHCP внутрь подсетей.

DHCP-сервер

- Поддержка DHCP сервисов (для IPv4 и IPv6) в клиентских сетях.
- Поддержка совместной работы DHCP-relay и сервера.
- Поддержка совместной работы DHCP-relay и DHCP-сервера как для IPv4, так и для IPv6.

Domain Name System (DNS)

- Создает распределенную базу данных, которая транслирует доменные имена и IP-адреса, что существенно упрощает дизайн сети; поддерживается режим клиента и режим сервера.
- Также поддерживается функционал mDNS-шлюза.

Generic Routing Encapsulation (GRE)

- Позволяет туннелировать трафик на уровне между сетями уровня L3.

МАРШРУТИЗАЦИЯ УРОВНЯ L3 (LAYER 3 ROUTING)

Статическая IPv4-маршрутизация

- Обеспечивает возможность вручную «прописать маршруты», использующие протокол IPv4.

Open shortest path first (OSPF)

- Обеспечивает быструю конвергенцию; используется "link-state" маршрутизация протокола IGP (Interior Gateway Protocol), который поддерживает EIGRP, NSSA и MD5-методы аутентификации, что гарантирует повышенный уровень безопасности и позволяет мягко перезапускать систему ("graceful restart") для более быстрого восстановления функционирования после сбоя или ошибок в сети.
- Расширенный функционал включает настраиваемое расстояние OSPF для type-5 LSA и настраиваемую метрику по умолчанию ("Default-Metric") для OSPF default-information guide.

Перераспределение IP-адресов loopback-интерфейса в OSPF

- Поддерживает перераспределение IPv4- и IPv6-адресов loopback-интерфейса в OSPFv2/v3.

Border Gateway Protocol 4 (BGP-4)

- Обеспечивает реализацию протокола EGP (Exterior Gateway Protocol) с использованием векторов маршрутизации; применяется TCP для большего уровня надежности в реализации процесса объявления новых маршрутов; протокол снижает требования к полосе пропускания благодаря использованию инкрементного обновления; поддерживается расширенный функционал применения политик для большей гибкости; масштабируется до уровня очень больших сетей.

Динамическое подключение BGP

- Упрощает настройку BGP для сценариев ZTP (автоматической конфигурации оборудования).

Routing Information Protocol version 2 (RIPv2)

- Легкий в настройке протокол маршрутизации для небольших сетей, основанный на протоколе UDP (User Datagram Protocol).

Routing Information Protocol Next Generation (RIPng)

- Расширение протокола RIPv2 для поддержки сетей протокола IPv6.

Multiprotocol BGP (MP-BGP) с семейством адресов IPv6

- Обеспечивает возможность совместного использования IPv6-маршрутов с помощью функционала BGP и подключений к BGP-пирам с помощью IPv6.

Policy Based Routing (PBR)

- Позволяет использовать классификатор для выбора трафика, который может быть перенаправлен, на основе политики, установленной сетевым администратором.

Туннели 6in4

- Поддержка туннелирования трафика IPv6 в сети IPv4.

Повышение производительности в сетях протокола IP

- Поддерживается набор инструментов для повышения производительности в сетях протокола IPv4, включая направленные рассылки ("directed broadcasts"), настройку параметров TCP, поддержку пакетов ошибок ICMP и широкие возможности отображения информации.

Статическая IPv6 маршрутизация

- Обеспечивает возможность вручную «прописать маршруты», использующие протокол IPv6.

Dual IP Stack

- Поддержка двух отдельных стеков протоколов IPv4 и IPv6 в одной сети помогает осуществить плавный переход с сети с поддержкой только IPv4 на сеть с поддерж-

кой только IPv6.

OSPFv3

- Поддержка OSPF для IPv6-маршрутизации.

Equal-Cost Multipath (ECMP)

- Поддерживает работу с несколькими маршрутами с одинаковыми метриками в маршрутизируемом окружении для увеличения количества резервируемых линков и увеличения пропускной способности.

Generic Routing Encapsulation (GRE)

- Позволяет туннелировать трафик на уровне между сетями уровня L3.

БЕЗОПАСНОСТЬ. БЕЗОТКАЗНОСТЬ. ДОВЕРЕННОСТЬ. НАДЕЖНОСТЬ. КОНТРОЛЬ ЦЕЛОСТНОСТИ

Соответствие требованиям ТАА

- Коммутатор КА CX8325 с AOS-CX, соответствующий требованиям ТАА, использует криптографический алгоритм FIPS 140–2 для защиты «чувствительных» данных.

Возможности Access Control List (ACL)

- Поддержка списков ACL как для протокола IPv4, так и для протокола IPv6. Возможность создания групп объектов, представляющих наборы устройств, таких как IP-адреса. Например, таким образом могут быть сгруппированы устройства управления ИТ.
- ACL также могут защищать сервисы Control Plane, такие как SSH, SNMP, NTP или веб-серверы.

Enrollment over Secure Transport (EST)

- Поддерживает создание подключений, защищенных сертификатом, упрощающее управление корпоративной инфраструктурой открытых ключей (PKI – Public Key Infrastructure).

Remote Authentication Dial-In User Service (RADIUS)

- Упрощает администрирование безопасного доступа за счет использования сервера аутентификации по паролю.

Terminal Access Controller Access-Control System (TACACS+)

- Представляет средство аутентификации, использующее протокол TCP с поддержкой шифрования для всего запроса на аутентификацию, что обеспечивает дополнительный уровень безопасности.

RadSec

- Обеспечивает безопасную и надежную передачу данных для аутентификации и учета на RADIUS-сервере через незащищенные сети, такие как интернет.

Management Access Security

- AOS-CX поддерживает аутентификацию административной

тора как “onbox” (непосредственно на самом оборудовании), так и “offbox” (на стороннем оборудовании). RADIUS или TACACS+ могут использоваться для обеспечения зашифрованной аутентификации пользователей.

- В дополнение, TACACS+ может также предоставлять сервисы авторизации для пользователей.

Secure Shell (SSHv2)

- Использует внешние серверы для безопасного входа на удаленное устройство; благодаря аутентификации и шифрованию защищает от подмены IP-адреса и перехвата пароля, передаваемого открытым текстом (“plaintext password”); повышает безопасность передачи данных Secure FTP (SFTP).

ПОДДЕРЖКА IP-MULTICAST'A

Internet Group Management Protocol (IGMP)

- Позволяет устанавливать членство в группах мультикаст-рассылки в сетях IPv4; поддерживает IGMP версий v1, v2 и v3.

Multicast Listener Discovery (MLD)

- Анонсирует потребителям мультикаст-рассылки IPv6-трафик; поддерживает MLD версий v1 и v2.

Multicast Service Delivery Protocol (MSDP) for Anycast RP

- Внутридоменная функция, обеспечивающая функционал резервирования и распределения нагрузки на сеть.

MSDP Mesh Groups

- Позволяет избежать флуда SA-сообщений на другие устройства mesh-группы.

PIM-Dense Mode

- Рассылает мультикаст-трафик во все уголки сети (push-модель). Метод предназначен для доставки данных получателям без запроса данных получателями. Может быть эффективным в определенных деплоях, в которых в каждой подсети сети есть активные получатели. Ветви без «нисходящих» (downstream) приемников отсекаются от древа пересылки.

FastLeave (FL) и Forced-FastLeave (FFL)

- Механизмы FL и FFL для IGMP/MLD ускоряют процесс блокировки ненужного мультикаст-трафика на порт коммутатора, который подключен к конечным узлам для IGMP. Это помогает устранить нагрузку на CPU, связанную с созданием сообщения IGMP/MLD Group-Specific Query.

Protocol Independent Multicast (PIM)

- Механизм PIM для IPv4 и IPv6 поддерживает сценарии multicast-вещания “one-to-many” и “many-to-many”, такие как IPTV через сети IPv4 и IPv6. Поддерживается режим PIM Sparse Mode (PIM-SM, IPv4, IPv6), Source-Specific Multicast (SSM) и Dense Mode (DM).

DR-KA-R9A29A



DR-KA-R9A30A



Технические характеристики

Таблица

| | | |
|-----------------------------------|--|---|
| Параметры/Модель | ДатаПу КА CX9300-32D - 32 порта 100/200/400G QSFP-DD; 2 порта 10G SFP+; "Front-to-Back" 6 вентиляторов; 2 блока питания AC Коммутатор, арт. (DR-KA-R9A29A) | ДатаПу КА CX9300-32D - 32 порта 100/200/400G QSFP-DD; 2 порта 10G SFP+; "Back-to-Front" 6 вентиляторов; 2 блока питания AC Коммутатор, арт. (DR-KA-R9A30A) |
| Описание | ДатаПу КА CX9300-32D — это коммутатор нового поколения с уровнем производительности в 25,6 Тбит/с и высотой всего 1U. Он оснащен 32 портами, поддерживающими пропускные способности в 100GbE, 200GbE и 400GbE. Это идеально гибкий по сфере применения продукт для организации экономически целесообразного решения с высокой коммутационной плотностью для серверов, СХД, а также для интраконнекта коммутационных фабрик. Коммутатор поможет защитить вложения в критически важную сетевую инфраструктуру во время процесса архитектурной миграции серверных ферм предприятия с 10 GbE и 25 GbE на 100/400 GbE EVPN-VXLAN spine-конфигурации, которые будут занимать меньшую площадь и иметь меньшее совокупное энергопотребление (углеродный след). | |
| Блоки питания | 2 быстросъемных (field-replaceable) блока питания с поддержкой функции резервирования и «замены на горячую» (hot-swappable) | |
| Вентиляторы | 6 быстросъемных (field-replaceable) вентиляторов с поддержкой функции резервирования и «замены на горячую» (hot-swappable) | |
| | Физические характеристики | |
| Габаритные размеры | 43,84 см x 59 см x 4,35 см (17,26" x 23,23" x 1,71") | |
| Масса | 11,85 кг (26,12 фунтов) | |
| | Спецификации аппаратного обеспечения вычислительных мощностей | |
| ЦПУ | x86 | |
| Объем оперативной и flash-памяти | 128 ГБ m.2 SSD, 4 ГБ mSATA, 16МБ SPI Flash, 16 ГБ x2 SODIMM | |
| Объем пакетного буфера | 132 МБ | |
| | Производительность* | |
| Коммутационная способность | 25,6 Тбит/с | |
| Емкость хостов протокола IPv4 | 163 840 | |
| Емкость хостов протокола IPv6 | 81 920 | |
| Количество unicast-маршрутов IPv4 | 65 536 (1 269 760 в одном направлении для "Spine") | |
| Количество unicast-маршрутов IPv6 | 32 768 (624 640 в одном направлении для "Spine") | |
| Емкость таблицы MAC-адресов | 81 920 (32 768 в одном направлении для "Spine") | |

* Некоторые из данных показателей масштабируемости предполагают использование общих таблиц.

| | | |
|--|--|---|
| Параметры/Модель | ДатаРу КА CX9300-32D - 32 порта 100/200/400G QSFP-DD; 2 порта 10G SFP+; "Front-to-Back" 6 вентиляторов; 2 блока питания AC Коммутатор, арт. (DR-КА-R9A29A) | ДатаРу КА CX9300-32D -32 порта 100/200/400G QSFP-DD; 2 порта 10G SFP+; "Back-to-Front" 6 вентиляторов; 2 блока питания AC Коммутатор, арт. (DR-КА-R9A30A) |
| Количество IGMP-групп | 8192 | |
| Количество MLD-групп | 8192 | |
| Количество multicast-маршрутов IPv4 | 8192 | |
| Количество multicast-маршрутов IPv6 | 4096 | |
| | Требования к окружающей среде, электропитанию, хранению и транспортировке устройств | |
| Максимально допустимый диапазон рабочих температур | от 0°C до 45°C на уровне моря, уменьшение на 1°C на каждые 0,3 км до 3 км | от 0°C до 35°C на уровне моря, уменьшение на 1°C на каждые 0,3 км до 3 км |
| Максимально допустимые условия для устройств в нерабочем состоянии | от -40°C до 70°C до высоты 4,6 км | |
| Максимально допустимый диапазон рабочей относительной влажности воздуха | от 15% до 95% при 45°C без выпадения конденсата | от 15% до 95% при 35°C без выпадения конденсата |
| Максимально допустимый диапазон относительной влажности воздуха в нерабочем состоянии / при хранении | от 15% до 90% при 70°C без выпадения конденсата | |
| Максимально допустимая рабочая высота над уровнем моря | до 3 км | |
| Максимально допустимая высота над уровнем моря в нерабочем состоянии | до 4,6 км | |
| Основное направление воздушного потока | от передней панели к задней ("Front-to-Back") | от задней панели к передней ("Back-to-Front") |
| Уровень шума ¹ | LWad = 8,1 Бел LpAm (Bystander) = 61 дБ | LWad = 8,3 Бел LpAm (Bystander) = 62 дБ |
| | Параметры электропитания | |
| Частота | 50-60 Гц | |
| Напряжение переменного тока | 100-127 / 220-240 В 200-240В требуется для конфигурации с 8-32 портами | |
| Сила тока | 12 А / 8 А | |
| Потребляемая мощность (230В AC) | при 100% трафике: 675 Вт; в режиме ожидания: 210 Вт | при 100% трафике: 688 Вт; в режиме ожидания: 221 Вт |
| | Интерфейсы управления | |
| | SNMP REST RJ-45 serial Консольный порт Micro USB RJ-45 OOBM-порт | |

¹ Представлены значения заявленного уровня звуковой мощности по шкале A (LWAd) и среднего уровня звукового давления по шкале A для наблюдателей (LpAm).

| | | |
|---|--|---|
| Параметры/Модель | ДатаРу КА CX9300-32D - 32 порта 100/200/400G QSFP-DD; 2 порта 10G SFP+; "Front-to-Back" 6 вентиляторов; 2 блока питания AC Коммутатор, арт. (DR-КА-R9A29A) | ДатаРу КА CX9300-32D -32 порта 100/200/400G QSFP-DD; 2 порта 10G SFP+; "Back-to-Front" 6 вентиляторов; 2 блока питания AC Коммутатор, арт. (DR-КА-R9A30A) |
| Варианты размещения, установки, монтажа | | |
| | Предусмотрена установка в 19-дюймовую, соответствующую стандартам EIA телекоммуникационную стойку или шкаф; предусмотрена возможность установки только на горизонтальную поверхность; комплект для монтажа в стойку с 2 опорами входит в комплект коммутатора, дополнительный комплект для монтажа в стойку с 4 опорами можно приобрести отдельно – DR-КА-JL483C | |

Поддерживаемые стандарты, протоколы и их реализации

- IEEE 802.1AB-2009
- IEEE 802.1ak-2007
- IEEE 802.1t-2001
- Link Aggregation по стандарту IEEE 802.1AX-2008
- Механизм ускорения трафика определенного класса и динамической фильтрации мультикаста по стандарту IEEE 802.1p
- Реализация VLAN по стандарту IEEE 802.1Q
- Multiple Spanning Trees по стандарту IEEE 802.1s
- Быстрая перестройка Spanning Tree по стандарту IEEE 802.1w
- LACP (Link Aggregation Control Protocol) по стандарту IEEE 802.3ad
- Flow Control по стандарту IEEE 802.3x
- Gigabit Ethernet по стандарту IEEE 802.3z
- 25-Gigabit Ethernet по стандарту IEEE 802.3by
- 40-Gigabit Ethernet по стандарту IEEE 802.3ba
- 50-Gigabit Ethernet по стандарту IEEE 802.3cd
- 100-Gigabit Ethernet по стандарту IEEE 802.3ba и 802.3cd
- 200- и 400-Gigabit Ethernet по стандарту IEEE 802.3bs
- Протокол UDP по стандарту RFC 768
- Протокол IP по стандарту RFC 791
- Протокол ICMP по стандарту RFC 792
- Протокол TCP по стандарту RFC 793
- Протокол ARP по стандарту RFC 826
- Стратегия окон и подтверждений в протоколе TCP согласно RFC 813
- Алгоритмы пересборки IP-дейтаграмм согласно RFC 815
- Максимальный размер сегмента для протокола TCP и связанные с этой тематикой статьи согласно RFC 879
- Управление "Congestion" в межсетевом взаимодействии по протоколу IP/TCP согласно RFC 896
- Подсети Интернет согласно RFC 917
- Вещание Интернет дейтаграмм согласно RFC 919
- Вещание Интернет дейтаграмм в присутствии подсетей (IP_BROAD) согласно RFC 922
- Multi-LAN Address Resolution согласно RFC 925
- Конвенция, определяющая типы SNMP, согласно RFC 1215
- ICMP-сообщения для обнаружения маршрутизаторов согласно RFC 1256
- Traceroute с помощью функционала опций протокола IP согласно RFC 1393

- Структура системы доменных имен и делегирование согласно RFC 1591
- Определение управляемых объектов протокола BGP-4 с помощью SMIv2 согласно RFC 1657
- Применение протокола Border Gateway Protocol в сети Интернет согласно RFC 1772
- Path MTU Discovery для протокола IPv6 согласно RFC 1981
- Атрибут BGP-сообщества согласно RFC 1997
- Применение атрибутов BGP-сообщества в "Multi-home" маршрутизации согласно RFC 1998
- Защита BGP-сессий с помощью опции подписи "TCP MD5" согласно RFC 2385
- Архитектура безопасности IP согласно RFC 2401
- Заголовок аутентификации в IP согласно RFC 2402
- Защищенная инкапсуляция полезной нагрузки протокола IP (IP Encapsulating Security Payload) согласно RFC 2406
- Спецификация протокола IPv6 согласно RFC 2460
- Использование мультипротокольных расширений протокола BGP-4 для внутридоменной маршрутизации в IPv6 согласно RFC 2545
- Multicast Listener Discovery (MLD) для протокола IPv6 согласно RFC 2710
- Определение управляемых объектов для протокола VRRP согласно RFC 2787
- Обновление маршрутов протокола BGP-4 согласно RFC 2918
- Protocol Independent Multicast MIB для IPv4 согласно RFC 2934
- OSPF Stub Router Advertisement согласно RFC 3137
- sFlow от InMon Corporation: метод мониторинга трафика в коммутируемых и маршрутизируемых сетях, согласно RFC 3176
- Выбор адреса по умолчанию для протокола IPv6 согласно RFC 3484
- Альтернативные имплементации граничных маршрутизаторов OSPF согласно RFC 3509
- «Мягкий перезапуск» OSPF согласно RFC 3623
- Multicast Listener Discovery Версии 2 (MLDv2) для протокола IPv6 согласно RFC 3810
- Базовые механизмы передачи для маршрутизаторов и хостов протокола IPv6, согласно RFC 4213
- Поддержка протокола Secure Shell (SSH) согласно RFC 4251

- Протокол BGP-4 согласно RFC 4271
- Определение управляемых объектов для протокола BGP-4 согласно RFC 4273
- Адресная архитектура IPv6 согласно RFC 4291
- IP Forwarding Table MIB согласно RFC 4292
- Management Information Base для IP согласно RFC 4293
- Атрибут расширения сообществ протокола BGP согласно RFC 4360
- Сабкоды для сообщений BGP Cease Notification согласно RFC 4486
- Аутентификация / Конфиденциальность для протокола OSPFv3 согласно RFC 4552
- Механизм «мягкого перезапуска» для протокола BGP согласно RFC 4724
- Мультипротокольные расширения для BGP-4 согласно RFC 4760
- IANA Considerations для протокола OSPF согласно RFC 4940
- Поддержка отказа от заголовков типа 0 в пакетах маршрутизации в сетях IPv6 согласно RFC 5095
- «Мягкий перезапуск» OSPFv3 согласно RFC 5187
- Поддержка атрибутов субтипа IPv6 Address Specific BGP Extended Community согласно RFC 5701
- Stub Router Advertisement в протоколе OSPF согласно RFC 6987
- Протокол управления базой данных Open vSwitch согласно RFC 7047
- Сравнение туннельных механизмов IPv6-over-IPv4 согласно RFC 7059
- Обновление маршрутов “Route Refresh Capability” для протокола BGP-4 согласно RFC 7313
- Path MTU Discovery для IPv6 согласно RFC 8201

DataRu — российский вендор технологических решений и сервисов. Компания производит серверное и сетевое оборудование, системы хранения данных, решения для высоконагруженных СУБД и бизнес-критичных приложений.

Компания DataRu предоставляет услуги в области консалтинга по продуктам для обработки Big Data, ERP-решениям и другим бизнес-приложениям, занимается сервисной поддержкой цифрового рабочего пространства и аутсорсингом печати, предоставляет услуги облачных сервисов.

+7 495 120 48 08

info@dataru.ru

Москва, Павелецкая площадь, 2, стр. 1

www.dataru.ru

ЭКСПЕРТИЗА·ТЕХНОЛОГИИ·ВОЗМОЖНОСТИ

