ТЕХНИЧЕСКОЕ ОПИСАНИЕ

Enterasys K-Series™

Гибкий модульный коммутатор с функциями премиум-класса для применения на периферии или в ядре сети небольшого предприятия

Сокращение совокупной стоимости владения благодаря универсальной коммутации высокой плотности от периферии до ядра небольшой сети с гибкими вариантами подключения и энергопотребления

Максимальная эффективность и надежность поддержки новых ИТ-служб (таких как виртуальные настольные системы) благодаря расширенным возможностям предоставления сетевых ресурсов

Сокращение затрат и защита премиум-класса для критически важных сетей благодаря комплексным возможностям контроля и управления

Надежные функции определения местоположения, идентификации и общего управления, включая поддержку программ BYOD (использование личных устройств для работы), благодаря легким в развертывании средствам управления доступом и приоритетами

Обзор продукта

Enterasys K-Series™ – самое экономичное в отрасли решение для коммутации на основе потоков. Предоставляя исключительные уровни автоматизации, доступности и управления от границы сети до ядра небольшого предприятия, эти гибкие модульные коммутаторы существенно сокращают эксплуатационные расходы, предлагая при этом функции премиум-класса.

Решения K-Series построены на базе специализированных микросхем Enterasys CoreFlow2 ASIC. Эта краеугольная технология коммутации обеспечивает высокую доступность важных бизнес-приложений и возможность улучшить средства управления для выполнения соглашений об уровне обслуживания (SLA) в соответствии с потребностями бизнеса.

Разработанные для решения проблем, связанных с растущим спросом на доступ к новым приложениям и сервисам, устройства K-Series защищают бизнес-трафик и поддерживают меняющиеся потребности. Они поддерживают консьюмеризацию ИТ и программы BYOD, требующие более надежных средств определения местоположения, идентификации, контроля и общего управления. Коммутаторы K-Series прекрасно подходят для интеллектуального управления обменом данными между пользователем, устройством и приложением. Кроме того, они обеспечивают контроль и управление для устранения проблем подключения и определения местоположения устройств, а также гарантируют защиту корпоративных данных.

Коммутаторы Enterasys K-Series поставляются в следующих формфакторах:

• 6-слотовое шасси, вмещающее до 144 портов 10/100/1000 и 4 порта 10 Гбит;

• 10-слотовое шасси, вмещающее до 216 портов 10/100/1000 и 8 портов 10 Гбит.

K-Series поддерживает до 12 каналов 10 Гбит для подключения к магистральной сети, включая 4 порта на плате коммутационной матрицы и 8 портов в двух модулях ввода/вывода 10 Гбит.

K-Series принимает решения о пересылке и применяет политики безопасности и роли во время классификации/определения приоритетов трафика со скоростью физической пропускной способности канала. Все модули ввода/вывода предоставляют максимальные возможности качества обслуживания (QoS) для критически важных приложений (например, передача голоса или видео высокой четкости) даже во время большой загруженности сети, а также упреждающе предотвращают DoS-атаки и распространение вредоносного ПО.

В решениях K-Series реализована передовая архитектура коммутации на основе потоков для интеллектуального управления обменом данными между пользователем и приложением. Это значительно превосходит возможности коммутаторов, использующих для реализации управления доступом только сети VLAN, списки управления доступом и порты. Чтобы гарантировать каждому пользователю доступ к его критически важным приложениям (независимо от того, где он подключен к сети), применяются идентификация пользователя и назначение ролей. Правила политик K-Series объединены с глубоким анализом пакетов и могут интеллектуально определять угрозы безопасности и автоматически реагировать на них, повышая при этом надежность и качество работы.

Преимущества

Соответствие требованиям бизнеса

- Гарантированное получение каждым конечным пользователем информации, сервисов и приложений, необходимых для достижения целей бизнеса с помощью широких возможностей контроля и управления сетью.
- Сокращение затрат на энергопотребление и охлаждение благодаря экологичной и эффективной модульной системе электропитания, обеспечивающей оптимальное постепенное увеличение потребления энергии.
- Согласование удобства работы конечных пользователей и защиты сети с помощью эффективного предоставления важнейших сетевых сервисов с одновременной блокировкой подозрительного трафика.

Эффективность эксплуатации

- Шасси высокой плотности и малого формфактора, устанавливаемое в стандартную стойку, содержит до 216 портов 10/100/1000 с 8 каналами 10 Гбит для подключения к магистральной сети, что существенно сокращает место в стойке.
- Снижение эксплуатационных расходов и увеличение срока безотказной работы с помощью автоматизации управления и встроенных функций восстановления работоспособности.
- Автоматическое определение и поддержка новых устройств и сервисов с сокращением времени развертывания.

Безопасность

- Сокращение рисков и упрощение управления сетью со встроенной, а не внешней системой безопасности.
- Защита бизнес-трафика от атак злоумышленников и обеспечение конфиденциальности, целостности и доступности данных.
- Расширение функций управления доступом к сети и безопасностью до уровня существующих пограничных коммутаторов и беспроводных точек доступа, а также решение проблем, связанных с консьюмеризацией ИТ.

Поддержка и обслуживание

- Лидирующее в отрасли решение по степени удовлетворенности клиентов и показателям устранения неполадок на первоначальном этапе.

Для нас нет ничего важнее наших клиентов

Существенной отличительной особенностью K-Series является возможность собирать данные NetFlow со скоростью физической линии, предоставляя пользователям и приложениям полную информацию об утилизации сетевых ресурсов. Решения K-Series вместе с устройствами S-Series являются единственными корпоративными средствами коммутации, поддерживающими многопользовательскую/многофакторную аутентификацию на каждом порту. Эти возможности абсолютно необходимы при использовании IP-телефонов, компьютеров, принтеров, копировальных устройств, камер видеонаблюдения, устройств считывания идентификационных карточек, а также подключенных к сети виртуальных машин.

Новые модульные коммутаторы предоставляют гибкие возможности подключения, функции премиум-класса и интегрированную систему безопасности, позволяющую быстро адаптировать сеть к меняющимся бизнес-требованиям.

Аппаратные функциональные возможности для обеспечения высокой доступности

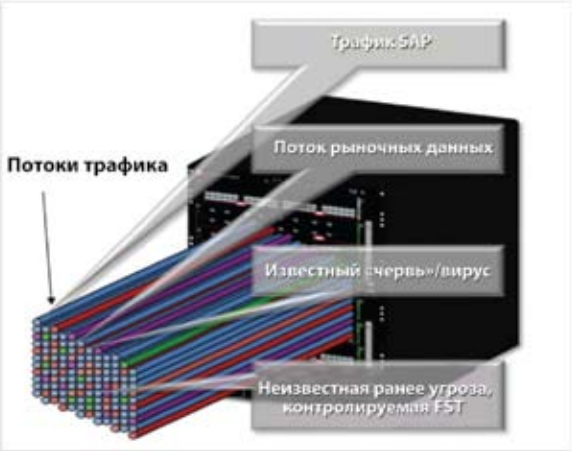
В устройствах K-Series предусмотрено множество стандартных функций для обеспечения высокой доступности. Эти аппаратные возможности обеспечения высокой доступности позволяют внедрять K-Series в критически важные среды, требующие круглосуточной ежедневной доступности.

Решения K-Series поддерживают следующие аппаратные возможности для обеспечения высокой доступности:

- пассивная объединительная плата шасси;
- вентиляторные отсеки с возможностью горячей замены и несколькими вентиляторами;
- источники питания с горячей заменой и распределением нагрузки;
- подключение нескольких входов переменного тока для резервирования электропитания;
- создание групп агрегирования нескольких каналов (LAG) путем объединения до 36 групп по 8 портов Ethernet.

Распределенная архитектура на основе потоков

Чтобы обеспечить для трафика детальный контроль и управление без вреда для производительности, в Enterasys K-Series использована архитектура на основе потоков. Она гарантирует, что при установлении специфического потока обмена данными между двумя оконечными устройствами первые пакеты в этом взаимодействии обрабатываются в коммутаторе с помощью механизмов многоуровневой классификации и модуля матрицы ввода/вывода. При этом определяются роли и применяемые политики, выполняется анализ пакетов и выбирается действие. После идентификации потока все последующие пакеты, связанные с этим потоком, автоматически передаются на Enterasys ASIC без дополнительной обработки.



В таком случае в Enterasys K-Series применяется детальное управление каждым потоком со скоростью, соответствующей полной пропускной способности линии.

Многопользовательская/многофакторная аутентификация и политика

С помощью аутентификации компании получают возможность управлять доступом к сети и обеспечивать мобильность пользователей и устройств. Она позволяет узнать, какие устройства/пользователи подключены к сети и в каком месте выполнено это подключение. Устройства Enterasys K-Series обладают уникальными, лучшими в отрасли передовыми в части методов средствами одновременной аутентификации. Модули K-Series могут одновременно поддерживать несколько различных технологий аутентификации, в том числе:

- аутентификацию по стандарту 802.1X;
- аутентификацию устройств в сети по MAC-адресу;
- аутентификацию через веб-интерфейс, также известную как PWA, при которой имя пользователя и пароль вводятся в окне браузера;
- CEP (конвергенция оконечных устройств); при этом методе идентифицируются и аутентифицируются VoIP-телефоны различных производителей. Эта возможность предоставляет большую гибкость компаниям, стремящимся внедрить в инфраструктуру механизмы управления доступом.

Важно отметить, что коммутаторы K-Series поддерживают многопользовательскую аутентификацию. Она позволяет подключать к одному и тому же физическому порту несколько устройств и пользователей, при этом они аутентифицируются по отдельности с помощью одного из методов (802.1X, MAC, PWA или CEP). Основным преимуществом многопользовательской аутентификации является авторизация нескольких человек с помощью динамических политик или назначения VLAN для каждого аутентифицированного пользователя. Использование динамической политики называется многопользовательской политикой.

Многопользовательская аутентификация и политика предоставляют клиентам значительные преимущества, распространяя сервисы безопасности на пользователей, подключенных на границе сети к неуправляемым устройствам, коммутаторам/маршрутизаторам других производителей, VPN-концентраторам или беспроводным точкам доступа LAN. Использование аутентификации обеспечивает управление безопасностью, приоритетами и пропускной способностью, защищая при этом инвестиции в сетевую инфраструктуру. Решения K-Series поддерживают до 8 пользователей на порт с лицензируемой возможностью до 256 пользователей на порт. Системные ресурсы (шасси) рассчитаны на 1152 пользователей в K6 и 1920 пользователей в K10.

Динамическая классификация пакетов на основе потоков

Еще одной уникальной особенностью Enterasys K-Series, отличающей эти решения от конкурирующих коммутаторов, является возможность многоуровневой классификации пакетов на основе пользователя или QoS. Из-за широкого набора используемых в сетях приложений одной традиционной многоуровневой классификации пакетов уже недостаточно, чтобы гарантировать своевременную передачу критически важных приложений. В устройствах K-Series многоуровневая классификация пакетов на основе пользователей позволяет классифицировать трафик не только по типу пакетов, но и по роли пользователя в сети и назначенной ему политике. Благодаря такой классификации пакеты можно классифицировать на основе уникальных идентификаторов, например «все пользователи», «группы пользователей» или «индивидуальный пользователь». Это обеспечит более детальный подход к управлению сетью и сохранение ее конфиденциальности, целостности и доступности.

Мониторинг сети с помощью NetFlow высокой точности

В коммутаторах Enterasys K-Series доступны возможности управления производительностью сети и обеспечения ее безопасности с помощью стандарта NetFlow без замедления коммутации и маршрутизации или покупки дорогостоящих дочерних плат для каждого модуля. В отличие от обычных технологий периодической выборки Enterasys NetFlow отслеживает каждый пакет в каждом потоке.

Значение недискретизированного мониторинга NetFlow в режиме реального времени заключается в возможности точного контроля того, какой трафик проходит через сеть. Аномальные ситуации обнаруживаются NetFlow, и выполняется соответствующее действие. Кроме того, NetFlow можно использовать для планирования пропускной способности, позволяя администратору сети отслеживать потоки и объемы трафика, чтобы при необходимости изменить конфигурацию или выполнить модернизацию сети. Это экономит время и средства, т. к. администраторы знают, когда и где могут потребоваться изменения.

Мониторинг сетевого трафика: зеркалирование портов

Зеркалирование портов – это интегрированное средство диагностики для отслеживания производительности сети и обеспечения ее безопасности, особенно полезное при отражении проникновений в сеть и атак. Это экономичная альтернатива специальным ответвляющим устройствам и другим решениям, которые могут потребовать дополнительного оборудования, нарушить работу сети, повлиять на клиентские приложения или создать точки отказа в сети.

Зеркалирование портов хорошо поддается масштабированию и мониторингу. Его очень удобно использовать в сетях с недоста-точным количеством портов. Для зеркалирования можно настроить физические и виртуальные порты, порты узлов (VLAN-интерфейсы), а также порты для обнаружения вторжений. Благодаря этой функции становятся легкими и экономичными процессы анализа двунаправленного трафика и мониторинга подключения, например, коммутатора подразделения его высокоскоростным каналом к магистральному коммутатору.

Зеркалирование портов в K-Series можно настроить для входящего трафика, для исходящего трафика или для обоих видов трафика, суммарно до 4 зеркал портов, «один в один», «многие в один», «один в многие», зеркалирование в соответствии с политикой.

Краткие характеристики

Многоуровневая классификация пакетов: предоставляет пользователям доступ к критически важным приложениям с помощью анализа трафика и функций управления

- Уровни пользователя, порта и устройства (классификация пакетов с уровня 2 по 4)
- Привязка QoS к приоритетным очередям (802.1p и IP ToS/DSCP): доступно до 11 очередей на порт
- Различные механизмы организации очередей (SPQ, WFQ, WRR и гибридный)
- Детальные уровни QoS/ограничение скорости
- Привязка сетей VLAN к политикам

Службы коммутации/VLAN: обеспечение высокоэффективных процессов подключения, агрегации и служб быстрого восстановления

- Расширенное соответствие отраслевым стандартам (IEEE и IETF)
- Управление входящей и исходящей пропускной способностью на поток
- Поддержка служб VLAN
  - Агрегирование каналов (IEEE 802.3ad)
  - Множественные остовные деревья (IEEE 802.1s)
  - Быстрое изменение конфигурации остовного дерева (IEEE 802.1w)
- Мосты провайдеров (IEEE 802.1ad), готовность к поддержке Q-in-Q
- Подавление избыточного потокообразования
- Сервер DHCP

IP-маршрутизация: динамическая оптимизация трафика, ограничение широковещательной передачи и эффективная устойчивость сети

- Стандартные функции маршрутизации: статические маршруты, поддержка RIPv2, RIPng и многоадресной маршрутизации (DVMRP, IGMP версий 1/2/3), маршрутизация на основе политик, карты маршрутов и VRRP
- Лицензируемые протоколы маршрутизации: OSPF версий 2/3, VRF и PIM-SM

Безопасность (пользователь, сеть и управление)

- Защита на уровне пользователя
  - Аутентификация (802.1X, MAC, PWA+ и CEP), блокирование портов по MAC-адресу (статическое и динамическое)
  - Многопользовательская аутентификация/политики
- Защита на уровне сети
  - Списки управления доступом (ACL): стандартные и расширенные
  - Службы безопасности на основе политик (например, защита от спуфинга, доступа по неподдерживаемому протоколу, предотвращение проникновения, ограничение DoS-атак)
- Безопасность управления
  - Безопасный доступ к K-Series по протоколу SSH, SNMP версии 3

Управление, контроль и анализ: средства, оптимизированные для управления доступностью и работоспособностью сети

- Конфигурация
  - Поддержка отраслевого стандарта интерфейса командной строки и веб-управления
  - Множество образов микрокода с редактируемыми файлами конфигураций
- Анализ сети
  - SNMP версий 1/2/3, RMON (9 групп) и SMON (rfc2613) VLAN и статистика
  - Зеркалирование портов/VLAN («один к одному», «один ко многим», «многие ко многим»)
  - Недискретизированный NetFlow на каждом порту без влияния на эффективность коммутации и маршрутизации
- Автоматизированная настройка и изменение конфигурации
  - Установленный для замены модуль ввода/вывода автоматически наследует настройки предыдущего модуля.

Функциональные возможности

Примеры дополнительных функций и возможностей, поддерживаемых устройствами Enterasys K-Series:

- NetFlow: контроль в режиме реального времени, профилирование приложений и планирование пропускной способности.
- LLDP-MED: протокол обнаружения канального уровня для мультимедийных оконечных устройств улучшает развертывания VoIP.
- Подавление избыточного потокообразования (Flow Setup Throttling): эффективное предупреждение DoS-атак и защита от них.
- Таблица узлов и псевдонимов: автоматически отслеживает местонахождение пользователя и устройства и улучшает производительность управления сетью и локализацию ошибок.
- Система защиты портов: поддержка доступности сети благодаря хорошей работе протокола и оконечного устройства.
- Технология Flex-Edge: расширенное управление пропускной способностью и распределение ресурсов для устройств доступа и граничных устройств, требовательных к ресурсам.

Подавление избыточного потокообразования (FST) – упреждающая функция, разработанная для уменьшения угроз, не распознаваемых текущими средствами, а также DoS-атак еще до того, как они смогут нарушить работу системы. FST борется с ранее неизвестными угрозами и DoS-атаками, ограничивая число новых и установленных потоков, которые могут быть запрограммированы для любого отдельного порта коммутатора. Это достигается путем мониторинга показателей появления новых потоков и/или контроля максимально разрешенного количества потоков.

В работе сети определение точного местоположения устройства или места подключения пользователя отнимает много времени. Это особенно важно при реагировании на нарушения безопасности. Модули Enterasys K-Series автоматически отслеживают местоположение пользователя/устройства в сети с помощью анализа трафика, проходящего через коммутатор. Затем полученные данные используются для заполнения таблицы узлов/адресов, в том числе такими сведениями, как MAC-адрес конечного устройства и информация об адресе уровня 3 (IP-адрес, IPX-адрес и т. д.). Эти сведения могут использоваться средствами управления Enterasys NMS Suite для быстрого определения коммутатора и номера порта для любого IP-адреса и выполнения необходимого действия в случае нарушения безопасности. Эти функции использования узла и имени уникальны, они позволяют сократить время точного определения места появления проблемы с нескольких часов до минут.

Организациям, желающим развернуть решения для унифицированных коммуникаций, коммутаторы Enterasys K-Series предлагают автоматизацию на основе политик с поддержкой различных стандартизированных методов обнаружения, включая LLDP-MED, SIP и H.323. Это позволит автоматически определять сервисы унифицированных коммуникаций для IP-телефонов всех основных производителей и предоставлять им необходимые ресурсы. Кроме того, коммутаторы K-Series обеспечивают динамическую мобильность IP-клиентов. При перемещении IP-телефона и подключении его в другом месте корпоративной сети настройки службы VoIP, безопасности и приоритета трафика перемещаются вместе с ним. Не требуется ничего перемещать, добавлять или изменять вручную.

K-Series также поддерживает комплекс функций по защите портов, например SPANguard и MACLock, которые позволяют определять неавторизованные мосты и ограничивать доступ по MAC-адресам для определенных портов. К другим средствам защиты портов относятся блокирование неустойчивых каналов, подавление широковещательной передачи и устранение петель остовного дерева, защищающее от неправильных конфигураций и сбоев протокола.

Технология Flex-Edge Enterasys K-Series позволяет классифицировать трафик для всех портов доступа с гарантированным обеспечением приоритета для трафика управления, а также трафика с высоким приоритетом в соответствии с политиками Enterasys. Кроме выделения ресурсов для важного сетевого трафика, приоритетная пропускная способность может быть назначена на уровне отдельных портов или аутентифицированных пользователей. Технология Flex-Edge прекрасно подходит для развертывания в коммутационных шкафах и точках распределения, которые часто страдают от пиковых нагрузок, приводящих к потерям пакетов. Благодаря этой технологии компаниям больше не нужно опасаться мгновенных перегрузок, приводящих к изменению топологии и неуправляемому отбрасыванию пакетов.

Стандарты и протоколы

Службы коммутации/VLAN
- Протокол GVRP
- 802.3u – Fast Ethernet
- 802.3ab – Gigabit Ethernet (по медному кабелю)
- 802.3ab – Gigabit Ethernet (по оптоволоконному кабелю)
- IEEE 802.3ae 10 Gigabit Ethernet (по оптоволоконному кабелю)
- 802.1Q – сети VLAN
- IEEE 802.1D – мосты уровня MAC
- IEEE 802.1ad – мосты провайдеров
- 802.1w – быстрое повторное схождение остовного дерева
- 802.1s – множественные остовные деревья
- 802.3ad – агрегация каналов
- 802.3ae – Gigabit Ethernet
- Управление потоком 802.3x
- Многоадресный IP (поддержка IGMP версий 1/2/3, разгрузка очередей VLAN)
- Пакеты большого размера с поддержкой обнаружения MTU для Gigabit
- Определение неустойчивости канала
- Динамический исходящий трафик (автоматизированная настройка портов VLAN)
- 802.S1ab – LLDP-MED

Стандартные функции IP-маршрутизации
- Статическая маршрутизация
- Стандартные списки ACL
- Протокол открытого поиска кратчайшего пути (OSPF) с поддержкой нескольких путей
- Пассивные интерфейсы OSPF
- Поддержка маршрутизации IPv6
- Расширенные списки ACL
- Маршрутизация на основе политики
- RFC 147 – определение сокета
- RFC 768 – UDP
- RFC 781 – спецификация функции отметки времени (IP)
- RFC 783 – TFTP
- RFC 791 – IP-протокол
- RFC 792 – ICMP
- RFC 793 – TCP
- RFC 826 – ARP
- RFC 854 – Telnet
- RFC 894 – передача IP через сети Ethernet
- RFC 919 – широковещательная передача интернет-датаграмм
- RFC 922 – широковещательная передача IP-датаграмм через подсети
- RFC 925 – разрешение адресов нескольких LAN
- RFC 950 – стандартный интернет-процесс определения подсетей
- RFC 951 – BOOTP
- RFC 959 – протокол передачи файлов (FTP)
- RFC 1027 – Proxy ARP
- RFC 1112 – IGMP
- RFC 1122 – требования к IP-хостам – уровни взаимодействияl

Стандарты и протоколы (продолжение)

- RFC 1123, требования к IP-хостам – прикладные и служебные протоколы
- RFC 1191 – определение MTU пути
- RFC 1323 – расширения TCP для повышения производительности
- RFC 1349 – тип сервиса в стеке протоколов IP
- RFC 1388 RIPv2 – передача дополнительной информации
- RFC 1492 – TACAS+
- RFC 1517 – внедрение CIDR
- RFC 1518 – архитектура CIDR
- RFC 1519 – CIDR
- RFC 1542 – BOOTP: пояснения и расширения
- RFC 1583/RFC 2328 – OSPFv2
- RFC 1587 – OSPFv2 NSSA
- RFC 1624 –контрольная сумма IP с помощью постепенного обновления
- RFC 1722 – заявление о применимости RIPv2
- RFC 1723 – передача дополнительной информации RIPv2
- RFC 1745 – взаимодействие с OSPF
- RFC 1746 – взаимодействие с OSPF
- RFC 1765 – переполнение базы данных OSPF
- DVMRPv3-10
- RFC 1812 – общие протоколы маршрутизации
- RFC 1886 – DNS-расширения, поддерживающие IPv6
- RFC 1981 – обнаружение MTU пути для IPv6
- RFC 2001 – медленный запуск TCP
- RFC 2018 – выборочное подтверждение TCP
- RFC 2030 – SNTP
- RFC 2080 – RIPv6
- RFC 2082 – аутентификация в RIP-II с помощью MD5
- RFC 2113 – возможность извещения маршрутизатора IP
- RFC 2117 – спецификация протокола PIM-SM
- RFC 2131 – ретрансляция сервера DHCP
- RFC 2132 – параметры DHCP и расширения производителей для BOOTP
- RFC 2138 – аутентификация RADIUS
- RFC 2154 – OSPF с цифровыми подписями
- RFC 2236 – IGMPv2
- RFC 2328 – OSPFv2
- RFC 2329 – отчет по стандартизации OSPF
- RFC 2338 – VRRP
- RFC 2361 – независимая от протокола многоадресная рассылка в разреженном режиме (PIM SM)
- RFC 2362 – спецификация протокола PIM-SM
- RFC 2370 – возможность Opaque LSA для OSPF
- RFC 2373 – сжатие нотации адресов
- RFC 2374 – объединяемый формат адреса глобальной одноадресной передачи IPv6
- RFC 2375 – назначение адресов многоадресной рассылки протокола IPv6
- RFC 2401 – архитектура безопасности для протокола IP
- RFC 2404– использование HMAC-SHA-1-96 в рамках ESP и AH
- RFC 2406 – протокол защиты полезной нагрузки IP-пакетов (ESP)
- RFC 2407 – область применения протокола управления ключами для IP
- RFC 2408 – управление ключами и аутентификаторами защищенных соединений
- RFC 2428 – расширения FTP для IPv6 и NAT
- RFC 2453 – RIPv2
- RFC 2460 – спецификация IPv6
- RFC 2461 – обнаружение соседних узлов для IPv6
- RFC 2462 – автоконфигурирование адресов без учета информации о состоянии в IPv6
- RFC 2463 – ICMPv6
- RFC 2464 – передача пакетов IPv6 по сети Ethernet
- RFC 2474 – определение поля дифференцированного обслуживания (DS) в заголовках IPv4/v6
- RFC 2475 – архитектура дифференцированных сервисов
- RFC 2710 – MLDv1
- RFC 2711 – опция уведомлений маршрутизатора IPv6
- RFC 2827 – фильтрация входящего трафика сети
- RFC 2865 – аутентификация RADIUS; сбор сведений в RADIUS
- RFC 2894 – перенумерация маршрутизатора
- RFC 3041 – частные расширения для IPv6 SLAAC
- RFC 3101–опция NSSA для OSPF
- RFC 3137 – объявление транзитного маршрутизатора OSPF
- RFC 3376 – IGMPv3
- RFC 3411 – архитектура описания моделей управления SNMP
- RFC 3412 – обработка и диспетчеризация сообщений в SNMP
- RFC 3413 – приложения SNMP
- RFC 3446 – адресация любому устройству в точке встречи с помощью PIM и MSDP
- RFC 3484 – выбор адреса по умолчанию для IPv6
- RFC 3493 – расширение базового интерфейса сокетов для IPv6
- RFC 3509 – альтернативные реализации граничных маршрутизаторов зоны OSPF
- RFC 3513 – архитектура адресации IPv6
- RFC 3590 – обнаружение приемника многоадресной рассылки (MLD)
- RFC 3595 – текстовые обозначения для идентификаторов потока IPv6
- RFC 3596 – расширения DNS для поддержки IPv6
- RFC 3623 – корректный перезапуск протокола OSPF
- RFC 3704 – фильтрация входящего трафика сети
- RFC 3768 – VRRP
- RFC 3810 – MLDv2
- RFC 3879 – исключение локальных адресов сайта
- RFC 3956 – внедрение адреса RP в многоадресную рассылку IPv6
- RFC 4007 – архитектура адресов видимости IPv6
- RFC 4167 – отчет о корректном перезапуске OSPF
- RFC 4193 – уникальные локальные адреса одноадресной передачи IPv6
- RFC 4222 – приоритетная обработка пакетов OSPFv2
- RFC 4291 – архитектура адресации IPv6
- RFC 4301 – архитектура безопасности для IP
- RFC 4302 – аутентификационный заголовок IP
- RFC 4303 – протокол защиты полезной нагрузки IP-пакетов (ESP)
- RFC 4305 – требования к реализациям криптографических алгоритмов для ESP и AH
- RFC 4443 – ICMPv6 для IPv6
- RFC 4541 – отслеживание IGMP
- RFC 4552 – аутентификация/ конфиденциальность для OSPFv3
- RFC 4601 PIM-SM
- RFC 4602 – предложенный стандартный анализ запросов PIM-SM IETF
- RFC 4604 – IGMPv3 и MLDv2
- RFC 4607 – многоадресная рассылка для IP, определяемая источником
- RFC 4608 – PIM-SSM в списке 232/8
- RFC 4610 – адресация любому устройству в точке встречи с помощью PIM
- RFC 4835 – требования к реализациям криптографических алгоритмов для ESP и AH
- RFC 4861 – обнаружение соседних узлов для IPv6
- RFC 4878 – функции OAM в интерфейсах, соизмеримых с Ethernet
- RFC 4884 – расширенный протокол ICMP для поддержки сообщений из нескольких частей
- RFC 4940 – критерии IANA для OSPF
- RFC 5059 – BSR для PIM
- RFC 5095 – неодобрение заголовков маршрутизации типа 0 в IPv6
- RFC 5186 – взаимодействие протокола маршрутизации IGMPv3/MLDv2/MCAST
- RFC 5187 – корректный перезапуск протокола OSPFv3
- RFC 5250 – опция Opaque LSA для OSPF
- RFC 5340 – OSPF для IPv6
- RFC 5798 – VRRP версии 3
- RFC 6164 – использование 127-разрядных префиксов маршрутизации IPv6

Класс обслуживания

- Очередность с учетом строгого приоритета
- Очереди взвешенного обслуживания с формированием трафика
- 11 очередей на порт
- Подсчет пакетов или пропускная способность на основе ограничителей скорости (пороговые значения между 64 Кбит/с и 4 Гбит/с)
- Маркирование/перемаркирование IP ToS/ DSCP
- 802.1D – привязка очередей приоритетных для передачи

Стандарты и протоколы (продолжение)

Защита сети и управление политиками
- 802.1X – аутентификация на основе порта
- Аутентификация на основе веб-интерфейса
- Аутентификация по MAC-адресу
- Обнаружение конвергентного оконечного устройства с динамической привязкой политик (Siemens HFA, Cisco VoIP, H.323 и SIP)
- Одновременно несколько типов аутентификации на порт
- Несколько аутентифицированных пользователей на каждом порту с уникальными политиками для каждого пользователя/конечной системы (независимо от связи с VLAN)
- RFC 3580 IEEE 802.1 – рекомендации по использованию RADIUS с привязкой VLAN к политике
- Предотвращение проникновения «червей» (подавление избыточного потокообразования)
- Подавление широковещательной передачи
- Защита от ARP-шторма
- Блокировка MAC-адресов для портов
- Span Guard (защита работы протокола остовных деревьев)
- Определение отклонений в работе/средство сбора данных потока (недискретизированный Netflow)
- Инициирование членства в статических группах рассылки
- Управление политиками для группы, отправителя и получателя многоадресной передачи

Управление, контроль и анализ
- SNMP версий 1/2c/3
- Веб-интерфейс управления
- Стандартный для отрасли интерфейс командной строки
- Поддержка нескольких образов ПО с возможностью отката к предыдущей версии
- Поддержка нескольких файлов конфигурации
- Редактируемый текстовый файл конфигурации
- ППЗУ удаленной загрузки через COM-порт и загрузка образа через ZMODEM
- Сервер и клиент Telnet
- Сервер и клиент SSHv2
- Протокол обнаружения Cabletron
- Протокол обнаружения Cisco версий 1/2
- Системный журнал
- Клиент FTP
- Протокол SNTP
- NetFlow версий 5 и 9
- RFC 2865 – RADIUS
- RFC 2866 – сбор данных в RADIUS
- TACACS+ для управления доступом
- VLAN управления
- 4 сеанса зеркалирования «многие к одному порту», «один ко многим портам», VLAN

Поддержка IETF и IEEE MIB
- RFC 1213 – MIB-II
- RFC 1389 – расширение MIB для RIPv2
- RFC 1493 – BRIDGE-MIB
- RFC 1659 – RS-232-MIB
- RFC 1724 – расширение MIB для RIPv2
- RFC 1850 – MIB OSPFv2
- RFC 2012 – TCP-MIB
- RFC 2013 – UDP-MIB
- RFC 2096 – MIB для таблицы переадресации IP
- RFC 2233 – MIB группы интерфейсов, использующих SMIv2
- RFC 2578 – SNMPv2-SMI
- RFC 2579 – SNMPv2-TC
- RFC 2613 – SMON-MIB
- RFC 2674 – P/Q-BRIDGE-MIB
- RFC 2787 – MIB VRRP
- RFC 2819 – MIB RMON
- RFC 2863 – IF-MIB
- RFC 2864 – IF-INVERTED-STACK-MIB
- RFC 2922 – PTOPO-MIB
- RFC 2934 – MIB PIM для IPv4
- RFC 3273 – HC-RMON-MIB
- RFC 3291 – INET-ADDRESS-MIB
- RFC 3411 – архитектура описания моделей управления SNMP
- RFC 3412 – обработка и диспетчеризация сообщений в SNMP
- RFC 3412 – SNMP-MPD-MIB
- RFC 3413 – приложения SNMP
- RFC 3413 – SNMP-NOTIFICATIONS-MIB
- RFC 3413 – SNMP-PROXY-MIB
- RFC 3413 – SNMP-TARGET-MIB
- RFC 3414 – SNMP-USER-BASED-SM-MIB
- RFC 3415 – SNMP-VIEW-BASED-ACM-MIB
- RFC 3417 – SNMPv2-TM
- RFC 3418 – MIB SNMPv2
- RFC 3584 – SNMP-COMMUNITY-MIB
- RFC 3621 – POWER-ETHERNET-MIB
- RFC 3635 – ETHERLIKE-MIB
- RFC 4133 – ENTITY MIB
- RFC 4188 – MIB мостов
- RFC 4268 – ENTITY-STATE-MIB
- RFC 4268 – ENTITY-STATE-TC-MIB
- RFC 4292 – MIB для переадресации IP
- RFC 4293 – MIB для протокола IP
- RFC 4560 – DISMAN-PING-MIB
- RFC 4560 – DISMAN-TRACEROUTE-MIB
- RFC 4560 – DISMAN-NSLOOKUP-MIB
- RFC 4750 – MIB OSPFv2
- RFC 4836 – MAU-MIB
- RFC 4836 – IANA-MAU-MIB
- RFC 4884 – расширенный протокол ICMP для поддержки сообщений из нескольких частей
- RFC 5060 – MIB PIM
- RFC 5240 – MIB для самонастройки маршрутизатора, назначенного для PIM
- RFC 5519 – MGMD-STD-MIB
- RFC 5643 – MIB OSPFv3
- DVMRP-MIB
- IANA-ADDRESS-FAMILY-NUMBERS-MIB
- IEEE8021-PAE-MIB
- IEEE8023-LAG-MIB
- LLDP-EXT-DOT1-MIB
- LLDP-EXT-DOT3-MIB
- LLDP-EXT-MED-MIB
- LLDP-MIB
- RSTP-MIB
- U-BRIDGE-MIB
- USM-TARGET-TAG-MIB

Enterasys Network Management Suite

NMS Console
- NMS Policy Manager
- NMS Inventory Manager
- NMS Automated Security Manager
- NMS NAC Manager

Спецификация

	C5G124-24	C5G124-24P2
Производительность/мощность		
Пропускная способность коммутационной матрицы	280 Гбит/с	440 Гбит/с
Общая пропускная способность коммутатора	190 млн. пакетов в секунду (при использовании 64-байтовых пакетов)	299 млн. пакетов в секунду (при использовании 64-байтовых пакетов)
Общая пропускная способность маршрутизатора	190 млн. пакетов в секунду (при использовании 64-байтовых пакетов)	299 млн. пакетов в секунду (при использовании 64-байтовых пакетов)
Размер таблицы адресов	32 000 MAC-адресов	32 000 MAC-адресов
Поддерживаемые сети VLAN	4 096	4 096
Очереди передачи	11	11
Правила классификации	8 196/шасси	8 196/шасси
Физические характеристики		
Размеры корпуса (В x Ш x Г)	В: 22,15 см (8,719 дюйма) Ш: 44,7 см (17,6 дюйма) Г: 35,546 см (14 дюймов) 5U	В: 31,02 см (12,219 дюйма) Ш: 44,7 см (17,6 дюйма) Г: 35,546 см (14 дюйма) 7U
Память хоста и флэш-память	1 ГБ DRAM 32 МБ флэш-память	1 ГБ DRAM 32 МБ флэш-память
Условия эксплуатации		
Рабочая температура	От 5 до 40 °C (от 41 до 104 °F)	От 5 до 40 °C (от 41 до 104 °F)
Температура хранения	От -30 до 73 °C (от -22 до 164 °F)	От -30 до 73 °C (от -22 до 164 °F)
Рабочая влажность	5–90 % (относительная влажность, без конденсации)	5–90 % (относительная влажность, без конденсации)
Требования к электропитанию	• 100–125 В переменного тока, 12 А, или 200–250 В переменного тока, 7,6 А; 50–60 Гц (макс. на каждый источник питания)	• 100–125 В переменного тока, 12 А, или 200–250 В переменного тока, 7,6 А; 50–60 Гц (макс. на каждый источник питания)
Характеристики PoE		
Система энергопотребления	• Автоматизированное или ручное распределение питания по портам PoE • Вкл./выкл. каждого порта, уровень мощности, безопасность по приоритетам, защита от перегрузки и короткого замыкания • Мониторинг системы питания • Мощность PoE: 400 Вт на каждый источник питания (100–125 В переменного тока), 2400 Вт макс., 800 Вт на каждый источник питания (200–250 В переменного тока), 4800 Вт макс.	• Автоматизированное или ручное распределение питания по портам PoE • Вкл./выкл. каждого порта, уровень мощности, безопасность по приоритетам, защита от перегрузки и короткого замыкания • Мониторинг системы питания • Мощность PoE: 400 Вт на каждый источник питания (100–125 В переменного тока), 2400 Вт макс., 800 Вт на каждый источник питания (200–250 В переменного тока), 4800 Вт макс.
Соответствие стандартам	• IEEE 802.3af • IEEE 802.3at	• IEEE 802.3af • IEEE 802.3at
Стандарты и технические нормативы		
Безопасность	UL 60950-1, FDA 21 CFR 1040.10 и 1040.11, CAN/CSA C22.2 № 60950-1, EN 60950-1, EN 60825-1, EN 60825-2, IEC 60950-1, 2006/95/EC (Директива о низком напряжении)	UL 60950-1, FDA 21 CFR 1040.10 и 1040.11, CAN/CSA C22.2 № 60950-1, EN 60950-1, EN 60825-1, EN 60825-2, IEC 60950-1, 2006/95/EC (Директива о низком напряжении)
Электромагнитная совместимость	FCC 47 CFR (ч. 15, класс A), ICES-003 (класс A), EN 55022 (класс A), EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZ CISPR-22 (класс A). VCCI V-3. CNS 13438 (BSMI), 2004/108/EC (Директива по ЭМС)	FCC 47 CFR (ч. 15, класс A), ICES-003 (класс A), EN 55022 (класс A), EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZ CISPR-22 (класс A). VCCI V-3. CNS 13438 (BSMI), 2004/108/EC (Директива по ЭМС)
Климатическое исполнение	2002/95/EC (директива RoHS), 2002/96/EC (директива WEEE), Приказ Министерства информации № 39 (правила RoHS, КНР)	2002/95/EC (директива RoHS), 2002/96/EC (директива WEEE), Приказ Министерства информации № 39 (правила RoHS, КНР)

Информация для заказа

Номер изделия	Описание
Корпус K6	
K6-Chassis	6-слотовое шасси и вентиляторный отсек K-Series
K6-FAN	Запасной вентиляторный отсек K6
K6-MID-KIT	Комплект для монтажа в стойку K6
Корпус K10	
K10-Chassis	10-слотовое шасси и вентиляторный отсек K-Series
K10-FAN	Запасной вентиляторный отсек K10
K10-MID-KIT	Комплект для монтажа в стойку K10

Информация для заказа

Номер изделия	Описание
Источники питания и дополнительные принадлежности	
K-AC-PS-1400W	Источник питания для коммутаторов K-Series, 15 A, входное напряжение 100–240 В переменного тока (600 Вт – система, PoE – 400/800 Вт)
K-POE-4BAY	Внешняя полка питания для коммутаторов K-Series на 4 отсека
K-POE-4BAY-RAIL	Монтажный комплект для K-POE-4BAY
K-POE-CBL-2M	Кабель PoE для шасси K (2 м)
Модули ввода/вывода для матрицы	
KK2008-0204-F2	Модуль управления/матрицы K10 с 4 портами 10GB SFP+
KK2008-0204-F1	Модуль управления/матрицы K6 с 4 портами 10GB SFP+
Модули ввода/вывода	
KT2006-0224	Модуль ввода/вывода K-Series с 24 портами 10/100/1000 802.3at PoE
KG2001-0224	Модуль ввода-вывода K-Series с 24 портами 1Gb SFP
KK2008-0204	Модуль ввода-вывода K-Series с 4 портами 10Gb SFP+
Лицензии	
K-EOS-L3	Расширенная лицензия на маршрутизацию (OSPF, VRF, PIM-SM)
K-EOS-PPC	Лицензия для коммутаторов K-Series на увеличение количества пользователей, получающих доступ к порту

Трансиверы

Трансиверы Enterasys предоставляют варианты соединения для Ethernet через двужильный медный или оптоволоконный кабель со скоростью передачи данных от 100 Мбит/с до 10 Гбит/с. Все трансиверы соответствуют высочайшим требованиям качества, имеют продолжительный срок службы и способствуют быстрой окупаемости инвестиций. Подробные спецификации, сведения о совместимости и информацию для заказа см. по адресу http://www.enterasys.com/products/transceivers-ds.pdf.

Обслуживание и поддержка

Компания Enterasys Networks предоставляет комплекс предложений: от профессиональных услуг по разработке, развертыванию и оптимизации клиентских сетей, а также персонализированному техническому обучению, до индивидуальных услуг. Для получения дополнительной информации об обслуживании и поддержке свяжитесь со своим менеджером Enterasys по работе с клиентами.

Гарантия

Будучи компанией, ориентированной на покупателя, Enterasys предоставляет высококачественные продукты и решения. На случай возникновения сбоя из-за дефекта мы разработали комплексную гарантийную программу, которая защитит ваши интересы и предоставит возможность отремонтировать устройство или восстановить данные в кратчайшие сроки.

Коммутаторы K-Series поставляются с гарантией Enterasys от производственного брака на весь срок службы. С полным текстом гарантийных условий можно ознакомиться на странице www.enterasys.com/support/warranty.aspx.

Обратная связь

Для получения дополнительной информации свяжитесь с Enterasys Networks по телефону +7(495)937-8320 или посетите веб-сайт enterasys.com.

Лидерство мысли
Запатентованные инновации

05/12

enterasys® Secure Networks™

Delivering on our promises. On-time. On-budget.