



Серия маршрутизаторов H3C MSR830

Маршрутизаторы для филиалов

Дата выпуска: февраль 2021 г.



Обзор продукта

Устройства серии MSR830 могут применяться в качестве шлюзов для сетей малых и средних предприятий, обеспечивая функционирование различных сервисов – VPN, NAT и IPSec. Совместно с другими продуктами H3C маршрутизаторы MSR830 позволяют создавать комплексные решения для сетей заказчиков, работающих в сфере государственного управления, энергетики, финансов, налогообложения, общественной безопасности, железнодорожных перевозок и образования.

Серия MSR830 представлена следующими моделями: MSR830-6EI-GL, MSR830-10EI-GL, MSR830-6HI-GL и MSR830-10HI-GL.



Маршрутизатор H3C MSR830-6EI-GL



Маршрутизатор H3C MSR830-10EI-GL



Маршрутизатор H3C MSR830-6HI-GL



Маршрутизатор H3C MSR830-10HI-GL

Функциональные возможности и преимущества

Применение новейших технологий

- Маршрутизатор работает под управлением ведущей на рынке сетевой операционной системы Comware, которая обеспечивает механизм интеллектуального управления планированием сервисов и поддерживает свободное связывание различных сервисных модулей, а также динамическую загрузку процессов и исправлений.
- Вычисления выполняются высокопроизводительным многоядерным процессором (CPU), который позволяет значительно расширить возможности параллельной мультисервисной обработки.

Расширенный функционал безопасности

- Безопасность сервисов
 - Предусмотрены возможности фильтрации пакетов (в том числе с контролем состояния соединений), MAC-адресов, IP-адресов и номеров портов, а также фильтрация по интервалам времени.
 - Анализ трафика в реальном времени.
- Безопасность сети
 - Маршрутизатор поддерживает широкое разнообразие комплексных технологий VPN, таких как IPSec, L2TP, GRE, MPLS VPN и их различные сочетания.
 - Обеспечивается безопасность и защита маршрутизации за счет использования таких средств, как протоколы динамической маршрутизации OSPF/RIP/IS-IS/BGP, шифрование OSPFv3/RIPng/IS-ISv6/BGP на базе IPSec, а также разнообразные функции контроля маршрутизации на основе политик.
- Безопасный доступ с конечных устройств
 - Механизм унифицированной проверки подлинности конечных узлов с привязкой доступа, предусматривающий возможность аутентификации с проверкой по EAD, аутентификации по протоколу 802.1X, аутентификации по MAC-адресу конечного узла, аутентификации через веб-портал, статической привязки доступа конечного узла и автоматического изучения и привязки MAC-адреса.
 - Предотвращение ARP атак с помощью таких средств, как задание фиксированного MAC-адреса источника, защита от ARP атак, подавление источника ARP запросов, обнаружение ARP пакетов, проверка и защита согласованности MAC-адреса источника, ограничение скорости передачи данных ARP и механизм активного подтверждения приема ARP запросов.
- Безопасное управление оборудованием
 - Механизм контроля доступа на основе ролей позволяет распределять ресурсы в соответствии с ролями пользователей, обеспечивая возможность сопоставления пользователей и ролей.
 - Ограничение трафика плоскости управления, контроль и фильтрация трафика в зависимости от типа протокола, очереди, известного и специального протокола.
 - Средства удаленного безопасного управления, такие как удаленное управление по протоколам SNMPv3, SSH и HTTPS.
 - Возможности контроля и аудита управления доступом, в том числе централизованная аутентификация на сервере AAA, полномочия на использование командной строки и получение в реальном времени отчета о записях операций.

Детализированный контроль

- Устройство предусматривает детализированную идентификацию и контроль, что дает возможность фильтровать трафик сервисов прикладного уровня и ограничивать их скорость, а также обеспечивать необходимую пропускную способность и собирать подробную статистику, используемую для оптимизации сети.
- Благодаря использованию асимметричных каналов, распределения трафика и технологии динамической маршрутизации с поддержкой нескольких топологий маршрутизатор способен выполнять распределение нагрузки.
- Поддерживается гибкое разделение пропускной способности маршрутизатора в зависимости от типа сервиса, пользователя, группы, канала и пропускной способности на одного пользователя.

Интеллектуальное управление сетью

- Поддержка разных методов сетевого управления – с использованием командной строки и протокола SNMP.
- Возможность использования Zero-configuration для первоначального определения устройства и автоматизации базовой конфигурации, а также возможность автоматического конфигурирования через порт USB.
- Встроенная в Software функция EAA позволяет осуществлять мониторинг внутренних событий и состояния компонентов программного и аппаратного обеспечения системы. При обнаружении какой-либо неисправности эта функция собирает информацию о ней и предпринимает попытку автоматически исправить ошибку, а также отправляет на указанный адрес электронной почты все необходимые для диагностики сведения.

Высокая доступность

- Независимый аппаратный модуль обработки, предназначенный для мониторинга и управления программируемыми компонентами, поддерживает автоматическую загрузку и обновление в режиме онлайн, что повышает надежность продукта.
- Технология обнаружения и отслеживания неисправных каналов связи на базе протокола Bidirectional Forwarding Detection (BFD) позволяет за несколько миллисекунд выявить неработоспособность канала при статической маршрутизации, динамической маршрутизации RIP/OSPF/BGP/ISIS, VRRP или резервировании интерфейсов.
- Использование функционала Network Quality Analyzer (NQA) для анализа и отслеживания качества сети при статической маршрутизации, резервировании маршрутизаторов с помощью VRRP или резервировании интерфейсов.
- Возможность резервирования с использованием нескольких устройств и распределения нагрузки (VRRP/VRRPE).

Возможности подключения к облачным инфраструктурам

- Устройство поддерживает использование технологии VXLAN для организации сетевых подключений второго уровня в центрах обработки данных. Создание подключений второго уровня на базе VXLAN не требует изменения существующей структуры сети; достаточно просто развернуть граничные устройства с поддержкой соответствующего функционала. Это позволяет сократить затраты на эксплуатацию сети, а в сочетании с технологиями IPsec повысить безопасность трафика, передаваемого через общедоступную сеть.

Технические характеристики

Аппаратные характеристики

Характеристика	MSR830-6EI-GL	MSR830-10EI-GL	MSR830-6HI-GL	MSR830-10HI-GL
Процессор	800 МГц	800 МГц	1,3 ГГц	1,3 ГГц
Производительность пересылки в рабочем режиме (IMIX)	200 Мбит/с	200 Мбит/с	800 Мбит/с	800 Мбит/с
Память	1 Гбайт	1 Гбайт	1 Гбайт	1 Гбайт
Флэш-память (по умолчанию/максимум)	256 Мбайт	256 Мбайт	256 Мбайт/32 Гбайт	256 Мбайт/32 Гбайт
Внешняя флэш-память	н/п	н/п	Карта Micro SD	Карта Micro SD
Порты USB	н/п	1	1	1
Порты CON	1	1	1	1

Характеристика	MSR830-6EI-GL	MSR830-10EI-GL	MSR830-6HI-GL	MSR830-10HI-GL
Порты WAN	2 порта GE для витой пары	4 порта GE для витой пары	1 порт GE для витой пары 1 совмещенный порт GE	3 порта GE для витой пары 1 совмещенный порт GE
Порты LAN	4 порта GE (с возможностью настройки в качестве интерфейсов WAN)	6 портов GE (с возможностью настройки в качестве интерфейсов WAN)	4 порта GE (с возможностью настройки в качестве интерфейсов WAN)	6 портов GE (с возможностью настройки в качестве интерфейсов WAN)
Консольный порт	1	1	1	1
Максимальная потребляемая мощность	22 Вт	22 Вт	22 Вт	22 Вт
Номинальное напряжение	100 до 240 В перем. тока, 50/60 Гц			
Габариты (В × Ш × Г)	44 × 440 × 225 мм (1,73 × 17,32 × 8,86 дюйма)			
Вес	2,45 кг (5,40 фунта)			
Рабочая температура	0°C до 45°C (32°F до 113°F)			
Рабочая влажность	Относительная влажность 5% до 95%, без конденсации			
Электромагнитная совместимость	FCC Часть 15 (CFR 47) КЛАСС А			
	ICES-003 КЛАСС А			
	VCCI-3 КЛАСС А			
	VCCI-4 КЛАСС А			
	CISPR 22 КЛАСС А			
	EN 55022 КЛАСС А			
	AS/NZS CISPR22 КЛАСС А			
	CISPR 24			
	EN 55024			
	EN 61000-3-2			
	EN 61000-3-3			
	EN 61000-6-1			
	ETSI EN 300 386			
	EN 301 489-1			
EN 301 489-17				
Безопасность	UL 60950-1			
	CAN/CSA-C22.2 No.60950-1			
	IEC 60950-1			
	EN 60950-1/A11			
	AS/NZS 60950			
	EN 60825-1			
	EN 60825-2			
	FDA 21 CFR Подраздел J			
	GB 4943			

Характеристики программного обеспечения

Характеристика	Описание
Коммутация второго уровня	Ethernet, Ethernet II, сети VLAN (VLAN на основе портов, гостевые VLAN), 802.3x, 802.1p, 802.1Q, 802.1X, STP (802.1D), RSTP (802.1w), MSTP (802.1s), PPP, PPPoE клиент, PPPoE сервер и DDR
IP-сервисы	Одноадресная/многоадресная рассылка, TCP, UDP, IP option, IP unnumbered, маршрутизация на основе политик, NetStream и sFlow
IP-приложения	Ping, Tracert, ICMP, сервер DHCP, ретранслятор DHCP, клиент DHCP, клиент DNS, DNS прокси, DDNS, NTP и SNTP
Маршрутизация IPv4	Статическая маршрутизация
	Динамическая маршрутизация: RIPv1/v2, OSPFv2, BGP, IS-IS
	Итерационное построение маршрута
	Маршрутизация с использованием политик
	Множественные маршруты с равной стоимостью (ECMP)
IPv6	Маршрутизация многоадресной рассылки: IGMPv1/v2/v3, PIM-DM, PIM-SM, MBGP, MSDP
	IPv6 ND, IPv6 PMTU, IPv6 FIB, IPv6 ACL, NAT-PT, 6PE и DS-LITE
	Туннелирование IPv6: настройка туннелей вручную и автоматически, туннели GRE, IPv6 в IPv4, ISATAP
	Статическая маршрутизация
	Динамическая маршрутизация: RIPng, OSPFv3, IS-ISv6, BGP4+
QoS	Многоадресная рассылка IPv6: MLDv1/v2, PIM-DM, PIM-SM
	LR, Port-Based Mirroring, режим Port Trust Mode и port priority
	CAR
	Очереди FIFO, WFQ, CBQ
	GTS
Безопасность	Классификация трафика
	PPPoE клиент и сервер, портал, 802.1X
	Локальная аутентификация, RBAC, RADIUS, TACACS+
	Базовый функционал межсетевое экрана, ASPF, списки контроля доступа (ACL), фильтры, ограничение на количество подключений
	IKE, IPsec
MPLS	L2TP, NAT/NAPT, PKI, RSA, SSH v1.5/2.0, URPF, mGRE, GRE
	Предотвращение ARP атак
	SSL VPN, ADVPN, GDVPN
	AES, DES, 3DES, MD5, SHA1
	LDP, статические LSP
Высокая доступность	L3VPN: MPLS VPN между автономными системами (Inter-AS) (варианты 1/2/3), вложенные MPLS VPN, иерархия PE (HoPE), CE с двойной адресацией, MCE и многофункциональный хост
	L2VPN: Martini, Kompella, CCC PW и статические PW
	MPLS TE, RSVP TE
Высокая доступность	VRRP, VRRPv3
	Балансировка нагрузки и резервирование с учетом пропускной способности
	Балансировка нагрузки и резервирование на основе IP-адресов
	NQA в сочетании с маршрутизацией, VRRP или резервированием интерфейсов

Характеристика	Описание
Управление и обслуживание	SNMP v1/v2c/v3, MIB, SYSLOG, RMON
	Удаленное управление с помощью ViMS, загрузка с накопителя USB
	Интерфейс командной строки (CLI), файловая система, поддержка двух образов ПО
	DHCP, FTP, HTTP, ICMP, общедоступный UDP, частный UDP, общедоступный TCP, частный TCP, SNMP
	Подключение в систему через консольный порт, по протоколам Telnet (VTY), SSH и FTP

Информация для заказа

Модель	Описание
RT-MSR830-6EI-GL	6-портовый маршрутизатор Gigabit Ethernet H3C MSR830 (2 порта GE WAN, 4 порта GE LAN/WAN)
RT-MSR830-10EI-GL	10-портовый маршрутизатор Gigabit Ethernet H3C MSR830 (4 порта GE WAN, 6 портов GE LAN/WAN)
RT-MSR830-6HI-GL	6-портовый маршрутизатор Gigabit Ethernet H3C MSR830 (2 порта GE WAN (1 совмещенный), 4 порта GE LAN/WAN)
RT-MSR830-10HI-GL	10-портовый маршрутизатор Gigabit Ethernet H3C MSR830 (4 порта GE WAN (1 совмещенный), 6 портов GE LAN/WAN)



The Leader in Digital Solutions

New H3C Technologies Co., Limited

Штаб-квартира в Пекине
Пекин, район Чаоян, южная улица Гуаншунь,
LSH Центр 8, Башня 1
Индекс: 100102

Штаб-квартира в Ханчжоу
Чжэцзян, Ханчжоу, район Биньцзян, улица Чанхэ № 466
Китай
Индекс: 310052
Тел.: +86-571-86760000

Copyright ©2021 New H3C Technologies Co., Limited
С сохранением всех прав

Заявление об ограничении ответственности. H3C старается обеспечить точность информации в этом документе, однако мы не можем гарантировать, что данные сведения не содержат каких-либо технических ошибок или опечаток. Вследствие этого H3C не принимает на себя ответственность за какие-либо неточности в этом документе.

H3C оставляет за собой право вносить изменения в содержимое данного документа без предварительного уведомления

<http://www.h3c.com>