ООО «НАГ»
+7 (343) 379-98-38
sales@nag.ru

Коммутационный модуль IBM BladeCenter 6 портов 10Гб SFP+

46M6071

Описание

Cisco IBM BladeCenter 46M6071 Коммутационный модуль 6 портов 10Гб SFP+. Коммутатор Cisco® Nexus 4001I разработан специально для высокоскоростного шасси BladeCenter H и HT. Имеет шесть внешних и четырнадцать внутренних портов 10Gb, выделенный порт управления 10/100/1000T и RS232. Поддержка разнообразных внешних подключений обеспечивается с помощью трансиверов Cisco SFP+. С помощью ключа активации, приобретаемого отдельно, поддерживает FCoE (Fibre Channel over Ethernet).

Технические характеристики

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	
Наименование	Cisco Nexus 4001I Switch Module (46M6071)
Порты подключения	14 внутренних портов 10Gb 6 внешних портов 10Gb SFP+ 1 внутренний порт 100Mb соединенный с консолью управления 1 внешний порт 10/100/1000Mb RJ45-RS232 консольный порт (кабель в комплекте)
Производительность	400-Gbps switching capacity Forwarding rate of 300 million packets per second (mpps) Low, predictable, and consistent latency of 1.5 microseconds regardless of packet size, traffic pattern, or enabled features on 10 Gigabit Ethernet interface Line-rate traffic throughput on all ports Configurable maximum transmission units (MTUs) of up to 9216 bytes (jumbo frames)
Поддержка MIB	SNMPv2-SMI CISCO-SMI SNMPv2-TM SNMPv2-TC IANA-ADDRESS-FAMILY-NUMBERS-MIB DIFFSERV-DSCP-TC NOTIFICATION-LOG-MIB CISCO-SYSLOG-EXT-MIB CISCO-PROCESS-MIB

	RMON-MIB
Поддерживаемые стандарты	IEEE 802.1D: Spanning Tree Protocol IEEE 802.1p: CoS Prioritization IEEE 802.1Q: VLAN Tagging IEEE 802.1s: Multiple VLAN Instances of Spanning Tree Protocol IEEE 802.1w: Rapid Reconfiguration of Spanning Tree Protocol IEEE 802.3: Ethernet IEEE 802.3ad: Link Aggregation Control Protocol (LACP) IEEE 802.3ae: 10 Gigabit Ethernet SFF 8431 SFP+ CX1 support RMON
Поддержка FCoE	Support for T11-compliant FCoE on all 10-Gigabit Ethernet interfaces FCoE Initialization Protocol (FIP): Converged Enhanced Ethernet Data Center Bridging Exchange (CEE-DCBX) protocol supports T11-compliant Gen-2 CNAs 802.1Q VLAN tagging for FCoE frames Priority-based flow control (IEEE 802.1Qbb) simplifies management of multiple traffic flows over a single network link and creates lossless behavior for Ethernet by allowing class-of-service (CoS)-based flow control Enhanced Transmission Selection (IEEE 802.1Qaz) enables consistent management of QoS at the network level by providing consistent scheduling of different traffic types (IP, storage, and so on) Data Center Bridging Exchange (DCBX) Protocol (IEEE 802.1AB) simplifies network deployment and reduces configuration errors by providing autonegotiation of IEEE 802.1 DCB features between the network interface card (NIC) and the switch and between switches
Поддержка VLAN	До 512VLAN
Безопастность	IEEE 802.1x allows dynamic, port-based security, providing server authentication. IEEE 802.1x with VLAN assignment allows dynamic VLAN assignment for a specific server, regardless of where the server is connected. IEEE 802.1x and port security are provided to authenticate the port and manage network access for all MAC addresses, including those of the server. IEEE 802.1x with an ACL assignment allows the use of specific identity-based security policies, regardless of where the server is connected. IEEE 802.1x with Guest VLAN allows servers without IEEE 802.1x clients limited network access on the guest VLAN. Cisco security VLAN ACLs (VACLs) on all VLANs prevent unauthorized data flows from being bridged within VLANs. Port-based ACLs (PACLs) allow security policies to be applied on individual switch ports. SSHv2, Kerberos, and SNMPv3 provide network security by encrypting administrator traffic during Telnet and SNMP sessions. SSH, Kerberos, and the cryptographic version of SNMPv3 require a special cryptographic software image because of U.S. export restrictions. Secure Sockets Layer (SSL) provides a secure means to use Web-based tools such as HTML-based device managers. Dynamic ARP Inspection (DAI) helps ensure user integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol. DHCP Snooping prevents malicious users from spoofing a DHCP server and sending out bogus addresses. This feature is used by other primary security features to prevent a number of other attacks such as ARP poisoning. IP Source Guard prevents a malicious user from spoofing or taking over another user's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN. Private VLANs restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a nonbroadcast multi-access-like segment. Private VLAN Edge provides security and isolation between switch ports, helping ensure that

ООО «НАГ»
+7 (343) 379-98-38
sales@nag.ru

	users cannot snoop on other users' traffic. Bidirectional data support on the Switched Port Analyzer (SPAN) port allows Cisco Secure Intrusion Prevention System (IPS 4200 Series Sensors) to take action when an intruder is detected. TACACS+ and RADIUS authentication enables centralized control of the switch and restricts unauthorized users from altering the configuration. MAC address notification allows administrators to be notified of servers added to or removed from the network. Port security secures the access to an access or trunk port based on the MAC address. After a specific time period, the Aging feature removes the MAC address from the switch to allow another server to connect to the same port. Multilevel security on console access prevents unauthorized users from altering the switch configuration. The user-selectable address-learning mode simplifies configuration and enhances security. BPDU Guard shuts down Spanning Tree Protocol PortFast-enabled interfaces when BPDUs are received, to avoid accidental topology loops. Spanning Tree Root Guard (STRG) prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes. IGMP filtering provides multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port. Dynamic VLAN assignment is supported through implementation of the VLAN Membership Policy Server (VMPS) client function to provide flexibility in assigning ports to VLANs. Dynamic VLAN enables the fast assignment of IP addresses. 1000 security access control entries are supported.
Энергопотребление	12V at 3.75A (45W) (maximum)
Индикаторы	Всего 10: -8 индикаторов активности -2 индикатора состояния модуля
Параметры среды	Operating temperature: 32° to 104° F (0 to 40°C) Storage temperature: -13° to 158°F (-25 to 70°C) Operating relative humidity: 10 to 85% noncondensing Storage relative humidity: 5 to 95% noncondensing
MTBF	Примерно 436,000 часов
Физические размеры	112 X 30 X 260 mm
Вес	1.1 кг