go communications

Tel: +44 (0)1279 408 777
Email: sales@gocomsys.com
Website: www.gocomsys.com

Refurbished CISCO PWR-2921-51-AC Datasheet

CISCO > **ROUTERS**

Cisco 4000 Series Integrated Services Routers

How Cisco SM-X EtherSwitch Service Module Addresses Customer Needs

Scalability with High-Performance IP Routing for the LAN (IP Base and IP Services)

Isolation of LAN traffic and route between VLANs on the Cisco SM-X EtherSwitch Service Module	Cisco Express Forwarding hardware routing architecture delivers extremely high-performance IP routing and promotes scalability. The modules offer inter-VLAN IP routing with full local Layer 3 switching between two or more VLANs. Traffic can be forwarded between service modules over the MGF without affecting the router CPU.

Security Features of Cisco SM-X EtherSwitch Service Module

Feature

Feature	Benefit
Dynamic ARP Inspection (DAI)	DAI helps ensure user integrity by preventing malicious users from exploiting the insecure nature of the Address Resolution Protocol (ARP).
DHCP Snooping	This feature prevents malicious users from spoofing a Dynamic Host Configuration Protocol (DHCP) server and sending out bogus addresses. Other primary security features use DHCP Snooping to prevent numerous other attacks such as ARP poisoning.
IP Source Guard	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	Private VLANs restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a nonbroadcast multiaccess-like segment. Private VLAN Edge provides security and isolation between switch ports, helping ensure that users cannot snoop on other users' traffic. These features are available in the IP Base and IP Services license levels.
Unicast Reverse Path Forwarding (URPF)	This feature helps mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. This feature is available in the IP Base and IP Services license levels only.
IEEE 802.1x	IEEE 802.1x allows dynamic, port-based security, providing user authentication. IEEE 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user regardless of where the user is connected. IEEE 802.1x with voice VLAN permits an IP phone to access the voice VLAN irrespective of the authorized or unauthorized state of the port. IEEE 802.1x and port security are provided to authenticate the port and manage network access for all MAC addresses, including that of the client. IEEE 802.1x with an ACL assignment allows for specific identity-based security policies regardless of where the user is connected. IEEE 802.1x with guest VLAN allows guests without 802.1x clients to have limited network access on the guest VLAN. Web authentication for non-802.1x clients allows non-802.1x clients to use an SSL-based browser for authentication.
Cisco TrustSec security	Cisco TrustSec classification and policy enforcement functions are embedded in the Cisco Enhanced EtherSwitch Service Modules. Cisco TrustSec security simplifies the provisioning and management of secure access to network services and applications by classifying traffic based on the contextual identity of the endpoint versus its IP address. It enables more flexible access controls for dynamic networking environments. Cisco TrustSec security defines policies using logical policy groupings, so secure access is consistently maintained even as resources are moved in mobile and virtualized networks. De-coupling access entitlements from IP addresses allows common access policies to be applied to wired, wireless, and VPN access consistently.
MACsec	Exceptional security with integrated hardware support for MACsec is defined in IEEE 802.1AE. MACsec provides MAC layer encryption over wired networks using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the

	keys required for encryption when configured. MKA and MACsec are implemented following successful authentication using the 802.1x Extensible Authentication Protocol (EAP) framework. In Cisco Enhanced EtherSwitch Service Modules, both the user and down-link ports (links between the switch and endpoint devices such as a PC or IP phone) as well as the network and up-link ports can be secured using MACsec. With MACsec you can encrypt switch-to-switch links such as access to distribution, or encrypt dark fiber links within a building or between buildings.
Multidomain authentication	Multidomain authentication allows an IP phone and a PC to authenticate on the same switch port while placing them on the appropriate voice and data VLAN.
MAC Authentication Bypass (MAB)	MAB for voice allows third-party IP phones without an 802.1x supplicant to get authenticated using the MAC address. This feature is available in the IP Base and IP Services license levels only.
Advanced ACLs	Cisco security VLAN ACLs on all VLANs prevent unauthorized data flows from being bridged within VLANs. This feature is available in the IP Base and IP Services license levels only. Cisco standard and extended IP Security router ACLs define security policies on routed interfaces for control- and data-plane traffic. IPv6 ACLs can be applied to filter IPv6 traffic. This feature is available in the IP Base and IP Services license levels only. Port-based ACLs for Layer 2 interfaces allow security policies to be applied on individual switch ports.
Administrative traffic protection	Secure Shell (SSH) Protocol, Kerberos, and Simple Network Management Protocol Version 3 (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. Some of these features are available in the IP Base and IP Services license levels only.
Switched Port Analyzer (SPAN)	Bidirectional data support on the SPAN port allows the Cisco Intrusion Detection System (IDS) to take action when an intruder is detected.
Centralized authentication	TACACS+ and RADIUS authentication facilitates centralized control of the switch and restricts unauthorized users from altering the configuration.
MAC address authentication	MAC address notification allows administrators to be notified of users added to or removed from the network.
Port security	Port security secures the access to an access or trunk port based on MAC address.
Console security	Multilevel security on console access prevents unauthorized users from altering the switch configuration.
Bridge Protocol Data Unit (BPDU) Guard	BPDU guard shuts down Spanning Tree PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
Spanning-Tree Root Guard	This feature prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
Internet Group Management Protocol (IGMP) Filtering	IGMP filtering provides multicast authentication by filtering out nonsubscribers and limits the number of concurrent multicast streams available per port.
Dynamic VLAN Assignment	Dynamic VLAN assignment is supported through implementation of VLAN Membership Policy Server client capability to provide flexibility in assigning ports to VLANs. Dynamic VLAN facilitates the fast assignment of IP addresses.

The next steps...

ORDER NOW

VIEW ONLINE

Tel: +44 (0)1279 408 777

Email: sales@gocomsys.com

Website: www.gocomsys.com