IOLAN SCR1618 Konsolenserver

perlesystems.de/products/iolan-scr1618-console-server.shtml

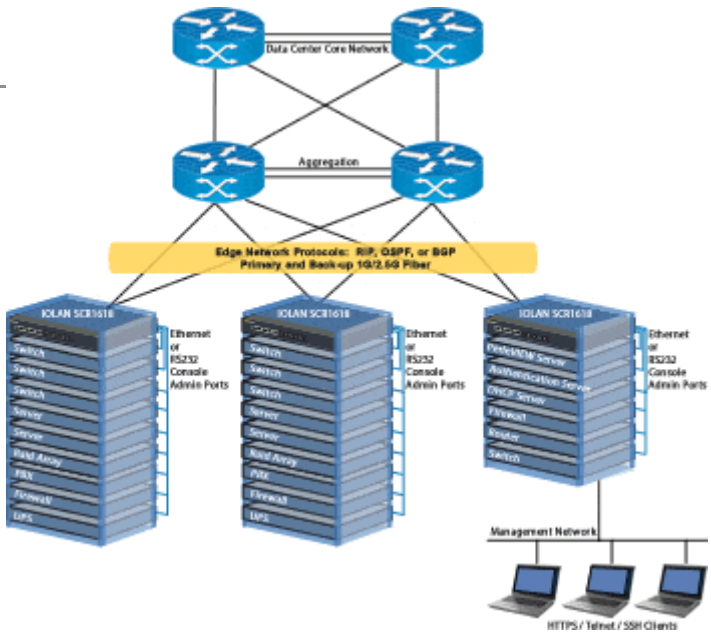
IOLAN SCR1618 Secure Console Server

In-Band- & Out-of-Band-IT-Infrastrukturmanagement

- 16 x RS232 RJ45 Konsolenmanagementports
- 16 x Ethernet RJ45 Konsolenmanagementports
- 2 x SFP Slots mit 1 G/2,5 G LWL oder 10/100/1000Base-T Support
- PerleVIEW Zentrale Management Software vereinfacht Konfiguration, Verwaltung, Überwachung und Fehlerbehebung.
- Cloud Hosting – Netzwerk Bereitstellung und Verwaltung über die Cloud
- Erweitertes Routing-Engine mit AAA-Sicherheit und SSH/SSL-Verschlüsselung erfüllt alle Compliance-Unternehmensrichtlinien

Der **IOLAN SCR1618 Konsolenserver** bietet Managern von Rechenzentren sichere Konsolenverwaltung aus der Ferne und für jedes Gerät mit einem **RS232- oder Ethernet-RJ45-Konsolenport**. Diese kostengünstige 1U-Rack-Lösung bewahrt die Protokollintegrität über Ethernet und bietet vollständige IPv4/IPv6-Routing-Funktionen mit Unterstützung für RIP-, OSPF- und BGP-Protokolle. Die **integrierte Firewall** und **Zwei-Faktor-Authentifizierung** erhöhen die Sicherheit, während die leistungsstarke Multi-Core-CPU blitzschnelles Routing und rasantes Switching gewährleistet. Mit **fortschrittlichem Failover** auf mehrere Netzwerke und **Zero Touch Provisioning (ZTP)** ist der IOLAN SCR ideal für die Durchführung eines sicheren Managements von Rechenzentren und das Out-of-Band-Management von IT-Assets weltweit.

Konsolenmanagement für IT-Assets



Der **IOLAN SCR1618 Konsolenserver** unterstützt **Ethernet- und RS232-RJ45-Konnektivität zu Konsolenports** von Geräten wie **Cisco, Juniper, HP, Routern, Switches, Firewalls, Servern, PBXs, Netzwerkspeichergeräten und Sicherheitsvorrichtungen** über ein IP-Netzwerk. Die RS232-RJ45-Ports können per Software so konfiguriert werden, dass sie mit 'straight-thru' oder 'rolled' Kabeln an Ihre Cisco-Geräte angeschlossen werden können. Darüber hinaus kann ein DCD-Pin für Geräte von Drittanbietern konfiguriert werden, die dieses zusätzliche Signal

benötigen. Dies bedeutet, dass der **Perle IOLAN SCR mehr serielle Geräte unterstützt als jeder andere Konsolenserver auf dem Markt**. Dies macht ihn zu einer idealen Out-of-Band-Managementlösung für IT-Geräte, die sich in Datenzentren oder an entfernten Standorten befinden.

Erweiterte Netzwerksicherheit, Authentifizierung und Datenverschlüsselung

Die **Zwei-Faktor-Authentifizierung (2FA)** stellt sicher, dass der Zugriff auf Geräte und Daten auf autorisierte Benutzer beschränkt ist, während die Verwaltung der Fernauthentifizierung (RADIUS, TACACS+ und LDAP) die Integration mit Systemen der Unternehmensklasse ermöglicht, um den Zugriff auf Geräte vor Ort zu kontrollieren.

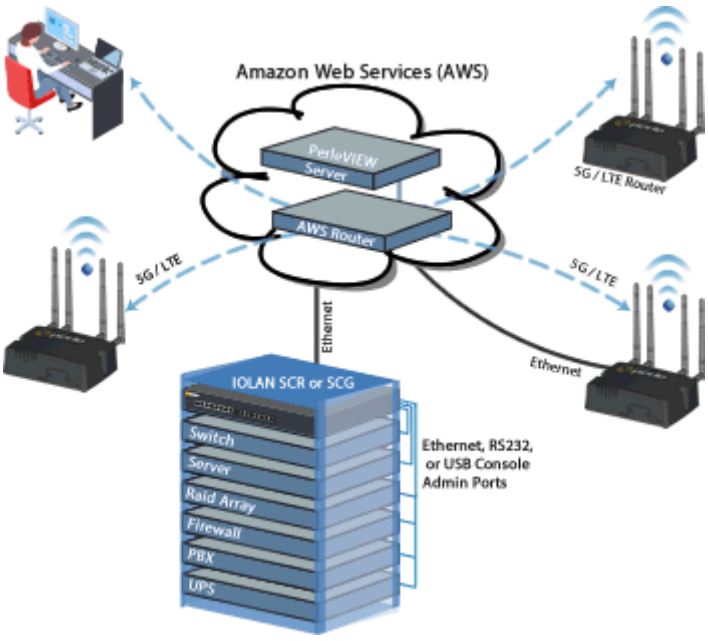
Die **integrierte Firewall** bietet intuitive Richtlinien zum Schutz vor unberechtigtem Zugriff innerhalb von Netzwerken. Die Firewall ermöglicht auch die Trennung der internen Netzwerke voneinander. Wenn Netzwerkressourcen einem externen Benutzer zur Verfügung stehen müssen, wie z. B. ein Web- oder FTP-Server, können diese Ressourcen in einem separaten Netzwerk hinter der Firewall in einer entmilitarisierten Zone (DMZ) platziert werden.

Netzwerkdatenübertragungen und der Zugriff auf Remote-Konsolen-Verwaltungsports an IT-Geräten werden durch **Standardverschlüsselungstools** wie Secure Shell (SSH) und Secure Sockets Layer (TLS/SSL) geschützt. Mithilfe von Verschlüsselungstechnologien kann ein IOLAN SCR-Konsolenserver sensible und vertrauliche Daten eines seriellen Geräts schützen, bevor sie über Intranet eines Unternehmens oder das öffentliche Internet verschickt werden. Alle großen Verschlüsselungsalgorithmen wie AES, 3DES, RC4, RC2 und CAST128 werden vollständig unterstützt, um die Kompatibilität mit anderen Verschlüsselungsgeräten zu gewährleisten.

Durch mehrere gleichzeitige VPN-Sitzungen, OpenVPN und IPSec VPN, wird eine robuste Authentifizierung und Verschlüsselung von IP-Paketen auf der Netzwerkschicht des OSI-Modells bereitgestellt Dies ist ideal für die Interoperation mehrerer Anbieter innerhalb eines Netzwerks und bietet Flexibilität sowie die Möglichkeit, die richtige Lösung für eine bestimmte Anwendung zu finden.

High Availability Access: Zugriff mit hoher Verfügbarkeit

Damit Netzadministratoren sie leichter verwalten und schnell auf Probleme reagieren können, müssen sie über eine einzige Portalansicht auf alle Konsolenanschlüsse zugreifen können. Die Cloud-basierte zentralisierte Verwaltungslösung von Perle vereint Ihre gesamte Netzwerk- und IT-Infrastruktur in einer einzigen App und bietet sicheren, zuverlässigen Zugriff und Transparenz während des normalen Betriebs sowie bei kritischen Netzwerkausfällen. Cloud-basiertes Zentralisiertes Management ist für jede Unternehmensanforderung skalierbar, reduziert menschliches Versagen und garantiert Wiederholbarkeit.



Der IOLAN SCR verfügt über eingebaute Fehlertoleranzfunktionen, um einen sicheren und zuverlässigen Zugang zur Verwaltung wichtiger unternehmenskritischer Ausrüstung zu gewährleisten. Mit 18 Routing-/Switching-Ethernet-Schnittstellen bietet der IOLAN SCR mehrere redundante Netzwerkpfade, um sicherzustellen, dass der Zugriff auf das Konsolenmanagement auch während eines Netzwerkausfalls möglich ist. Die duale AC-Stromversorgung stellt sicher, dass das Konsolenmanagement auch dann verfügbar ist, wenn die primäre AC-Stromquelle ausfällt.

Der Schutz vor elektrostatischen Entladungen und Stromstößen wird durch robuste 15Kv ESD-Schutzschaltungen an jedem Konsolenanschluss gewährleistet.

Gewährleistung auf Lebenszeit

Alle Perle IOLAN SCR-Modelle werden durch den besten Service und Support in der Branche unterstützt, einschließlich der einzigartigen lebenslangen Garantie von Perle. Seit 1976 bietet Perle seinen Kunden Netzwerkprodukte, die ein Höchstmaß an Leistung, Flexibilität und Qualität bieten. Mit dem Perle IOLAN SCR ist die Bereitstellung und Aufrüstung neuer Dienste und Geräte bei gleichzeitiger Minimierung der Investitionsausgaben so einfach wie nie.

Softwarefunktionen - IOLAN SCR Secure Konsolenserver

Verwaltung und Konfiguration
Zero Touch Provisioning (ZTP): automatisiert die Bereitstellung sowohl der Konfigurations- als auch der Firmware-Dateien durch DHCP/Bootp-Optionen
PerleView Central Management: ein webbasiertes Serverkonfigurations-Tool, das die Einrichtung und Bereitstellung vereinfacht und Netzwerkmanagern Transparenz und Kontrolle über Netzwerkkonfigurationen an entfernten Standorten bietet.
Verwaltung und Überwachung: HTTP/HTTPS, CLI/Piping, Telnet, SNMPv1/v2/v3, RESTful API, TACACS+
Auf dem Gerät können mehrere Firmware-Versionen gespeichert werden. Dies ermöglicht dem Kunden den Wechsel zwischen älteren und neueren Firmware-Versionen, ohne dass ein Download erforderlich ist.
Auf dem Gerät können mehrere Konfigurationsdateien gespeichert werden, sodass der Kunde während der Test- oder Produktionseinführung problemlos zwischen älteren und neueren Konfigurationen hin- und herschalten kann.
Automatische Prüfung auf verfügbare Software-Updates über FTP, HTTP, HTTPS, SCP, SFTP und TFTP.
LLDP-Link Layer Discovery Protocol gemäß IEEE 802.1AB ist ein Neighbor Discovery Protocol (NDP), das für Netzwerkgeräte verwendet wird, um anderen Geräten im Netzwerk Informationen über sich selbst mitzuteilen. Dieses Protokoll wird über die Datenverbindungsschicht ausgeführt, wodurch zwei Systeme, die über unterschiedliche Protokolle der Netzwerkschicht ausgeführt werden, über TLVs (Type-Length-Value) voneinander erfahren können.

Die RESTful API verwendet HTTP-Anforderungen für den Zugriff auf und die Verwendung von IOLAN-Statistiken und Konfigurationsdaten. Jeder der CLI-Befehle kann über ein RESTFul API-Skript ausgeführt werden, das extern von einem Server gesteuert werden kann.
Der Connectivity Watchdog kann den IOLAN anweisen, andere Aktionen (z. B. einen Neustart) durchzuführen, wenn die Netzwerkverbindung zu einer vordefinierten IP-Adresse verloren geht. Dies ist für Situationen hilfreich, in denen es bei an entfernten, schwer zu wartenden Standorten eingesetzten IOLANs zu einem Verlust der Netzwerkkonnektivität kommt.
Automatische DNS-Aktualisierung: Verwendet DHCP Opt 81, um den IOLAN-Domänennamen für eine einfache Namensverwaltung festzulegen. Mithilfe der Unterstützung für dynamisches DNS können Internetnutzer über den Namen auf den Geräteserver zugreifen, ohne dessen IP-Adresse kennen zu müssen. Siehe Unterstützung zur automatischen DNS-Aktualisierung für Einzelheiten
Dynamisches DNS mit DYNDNS.org
Network Assist: Diese Windows-basierte Desktop-Anwendung hilft viel beschäftigten IT-Managern bei der Konfiguration und Überwachung des Status der eingesetzten Perle-Geräte.
Remote Access
Dial, direct serial: PPP, PAP/CHAP, SLIP
HTTP tunneling enables firewall-safe access to remote serial devices across the internet
Automatic DNS update: Utilize DHCP Opt 81 to set IOLAN domain name for easy name management and with Dynamic DNS support , users on the Internet can access the device server by name without having to know its IP address.
IPSEC VPN client/servers: Microsoft IPSEC VPN Client, Cisco routers with IPSEC VPN feature set, Perle IOLAN SDS, SDG, STS, STG, SCS, SCG, and SCR models
OpenVPN: Clients & Servers
Protokollierung, Berichterstattung und Warnmeldungen
E-Mail-Benachrichtigung
Syslog, Ereignistyp, Berichtstyp, Warnungen und Überwachung, Bericht des Trigger-Statusbildschirms, Datenverwendung, Diagnose, Anmeldebanner
Zugriff auf Konsolenmanagementports (seriell und Ethernet)
Serielle Protokolle: PPP, PAP/CHAP, SLIP
Direkte Verbindung über Telnet/SSH nach Port und IP-Adresse
Verwenden für den Zugriff mit HTTP oder sicherem HTTPS einen Internet-Browser
Java-freier Browserzugriff auf entfernte serielle Konsolenschnittstellen über Telnet und SSH

Ports kann eine bestimmte IP-Adresse zugewiesen werden
Multisession-Fähigkeit ermöglicht es mehreren Benutzern, gleichzeitig auf Ports zuzugreifen
Multisessions ermöglichen es mehreren Benutzern, gleichzeitig auf Ports zuzugreifen
Konsolenmanagementfunktionen
Sun/Oracle Solaris Break Safe
Anzeige des lokalen Portpuffers – 256 Kilobytes pro Port
Externe Portpufferung über NFS, verschlüsseltes NFS und Syslog
Benachrichtigung über Ereignisse
Windows Server / Azure – SAC unterstützt GUI-Zugriff auf textbasierte Special Administrative Console
Terminalserverfunktionen:
Telnet
SSH v1 und v2
Automatische Sitzungsanmeldung
LPD-, RCP-Drucker
MOTD - Message of the day
Seriell-Ethernet-Funktionen
Tunneln Sie serielle Rohdaten über Ethernet – klar oder verschlüsselt
Serielle Rohdaten über TCP/IPP
Serielle Rohdaten über UDP
Serielle Datenkontrolle von paketierten Daten
Gemeinsame Nutzung serieller Schnittstellen mit mehreren Hosts/Servern
Virtuelles Modem simuliert eine Modemverbindung – Zuweisung der IP-Adresse erfolgt über AT-Telefonnummer
Virtuelle Modemdaten können über die Ethernet-Verbindung mit oder ohne SSL-Verschlüsselung gesendet werden
TruePort COM/TTY redirector stellt feste TTY- oder COM-Ports für serielle Anwendungen zur Verfügung und ermöglicht die Kommunikation mit entfernten Geräten, die an Perle IOLANs angeschlossen sind, entweder im verschlüsselten oder im Klartext-Modus.

Die TrueSerial-Pakettechnologie bietet die authentischsten seriellen Verbindungen über Ethernet und gewährleistet die Integrität des seriellen Protokolls.
RFC 2217-Standard für den Transport von seriellen Daten und RS232-Steuersignalen
Anpassbare oder feste serielle Baud-Raten
Serielle Kapselung von Industrieprotokollen wie ModBus, DNP3 und IEC-870-5-101
Das ModBus-TCP-Gateway ermöglicht einen seriellen Modbus-ASCII/RTU-Geräteanschluss an ModBus-TCP
Die Datenprotokollierung speichert empfangene serielle Daten, wenn keine aktive TCP-Sitzung stattfindet, und leitet sie an den Netzwerk-Peer weiter, sobald die Sitzung wiederhergestellt ist – 32 Kilobytes zirkulär pro Port
Redundanz
Lastausgleich
VPN-Failover
Das Virtual Router Redundancy Protocol (VRRPv3) ermöglicht es einer Gerätegruppe, ein einzelnes virtuelles Gerät zu bilden, um eine Netzwerkredundanz bereitzustellen.
Die Primär-/Backup-Host-Funktion ermöglicht automatische Verbindungen zu alternativen Hosts
Routing-Protokolle
Der IOLAN kann für jedes der wichtigsten Routing-Protokolle konfiguriert werden, um eine einfache Integration in das Ethernet-Backbone des Rechenzentrums zu ermöglichen: RIP/RIPNg, OSPFv3, BGP-4, NAT, IPv4/IPv6, statisches Routing, IPv6-Kapselungen (GRE, 6in4), Port-Routing, STP, MSTP
Die Übersetzung von IPv6 in IPv4 wird für Umgebungen, in denen das Ethernet-Daten-Backbone unter IPv6 und das Portmanagement unter IPv4 betrieben wird, vollständig unterstützt.
Mit NAT für erhöhte Sicherheit kann der IOLAN eine einzelne IP-Adresse über alle oder mehrere seiner Ethernet-Ports abbilden.
IP-Anwendungen
DDNS, DNS-Proxy/Spoofing, Relais, Kunde, Opt. 82,
NTP & SNTP (Versionen 1, 2, 3, 4)
DHCP-/DHCPv6-Server/DHCP-Snooping und BOOTP
VLAN und VPN
VLAN, OpenVPN, VPN-Failover (16 gleichzeitige VPN-Tunnel)
IPSec VPN: NAT-Traversal, ESP-Authentifizierungsprotokoll

Firewall-Funktionen
Ermöglicht das Einrichten von Firewalls, um ein- und ausgehende Pakete zu beschränken.
Integrierte zonenbasierte Richtlinien-Firewall für lokale Sicherheit und Verkehrsfilterung.
Zugriffskontrolllisten (Liste, Bereiche und Zeit)
Filter basierend auf MAC-Adresse, IP, Port, Protokoll, Benutzer
Die IEEE 802.1x-Authentifizierung und Port-Sicherheit können für jeden Ethernet-Port aktiviert werden, um die Sicherheit beim Port-Zugriff zu erhöhen.
Layer 2 MAC address filtering
Port-Weiterleitung
BGP-Gemeinschaften
Sicherheitsmerkmale
AAA-Sicherheit durch Fernauthentifizierung (Radius, TACACS+ und LDAP)
Filterung vertrauenswürdiger Hosts (IP-Filterung), die nur den in der Host-Tabelle konfigurierten Hosts den Zugriff auf den Router erlaubt.
Möglichkeit, Dienste (z. B. Telnet, TruePort, Syslog, SNMP, Modbus, HTTP) für zusätzliche Sicherheit zu deaktivieren.
Möglichkeit, Ping-Antworten zu deaktivieren.
SSH-Client/Server-Verbindungen (SSH 1 und SSH 2). Unterstützte Verschlüsselungen: Blowfish, 3DES, AES-CBC, AES-CTR, AES-GMC, CAST, Arcfour und ChaCha20-Poly1305. Möglichkeit zur individuellen Deaktivierung von Netzwerkdiensten, die von den SSH-Client-/Server-Verbindungen nicht genutzt werden.
SSL-/TLS-Client-/Server-Datenverschlüsselung (TLS v1.2)
SSL-Peer-Authentifizierung
SSL-Verschlüsselung: SSL-Verschlüsselung: AES-GCM, Schlüsselaustausch ECDH-ECDSA, HMAC SHA256, SHA384
Verschlüsselung: AES (256/192/128), 3DES, DES, Kugelfisch, CAST128, ARCFOUR(RC4), ARCTWO(RC2)
Hashing-Algorithmen: MD5, SHA-1, RIPEMD160, SHA1-96 und MD5-96
Schlüsselaustausch: RSA, EDH-RSA, EDH-DSS, ADH
VPN: OpenVPN & IPSec VPN (NAT Traversal, ESP authentication protocol)
Zertifikat-Unterstützung (X.509)

Liste der Zertifizierungsstellen
Lokale Datenbank
RIP-Authentifizierung (per Passwort oder MD5)
Die Zwei-Faktor-Authentifizierung (2FA) per E-Mail erhöht die Sicherheit des Verwaltungszugriffs
Zugriffskontrollmanagement
Entmilitarisierte Zone (DMZ)
Sicherer HTTP/HTTPS/FTP/Telnet-Authentifizierungs-Proxy
Unterstützung von SNMP v3-Authentifizierung und -Verschlüsselung
Filterung von IP-Adressen
Abschaltung unbenutzter Daemons
Active Directory über LDAP
Protokolle
IPv6, IPv4, TCP/IP, Reverse SSH, SSH, SSL, IPSec/IPv4, IPSec/IPv6, IPSec, RIPV2/MD5, ARP, RARP, UDP, UDP Multicast, ICMP, BOOTP, DHCP, TFTP, SFTP, SNTP, Telnet, raw, reverse-Telnet, LPD, RCP, DNS, Dynamic DNS, WINS, HTTP, HTTPS, SMTP, SNMPV3, PPP, PAP/CHAP, SLIP, CSLIP, RFC2217, MSCHAP

Hardware-Spezifikationen - IOLAN SCR Secure Konsolenserver

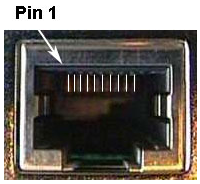
Interface Ports	
Back of Product	
Integrated Device Management Ports (Serial)	16 x RS232 RJ45 Data Bits: Configurable for 5,6,7 or 8-bit protocol support Paity: Odd, Even, Mark, Space, None Flow Control: Hardware, Software, Both, None Serial Protection: 15Kv Electrostatic Discharge Protection (ESD)
Integrated Device Management Ports (Ethernet)	16 x 10/100/1000 Base-T Copper Software selectable 10/100/1000 Ethernet, Auto Software selectable Half/Full/Auto duplex Ethernet isolation 1.5KV magnetic Up to 100m / 328ft

Network	2 x SFP Slots supporting 1G/2.5G Fiber or 10/100/1000Base-T IEEE 802.3 for 10Base-TX IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3ab for 1000Base-T IEEE 802.3x for Flow Control
Local Console Port	1 x RS232 RJ45
LEDs	Power 1 & 2, System, WAN / IP Health, Ethernet Port Activity & Speed
Reset	Reset Button used for restart, factory default and safe mode
Power	
Power Input	Dual AC power supplies
Nominal Input Voltage	110/230v AC
Input Voltage Range	100-240v AC
AC Input Frequency	47-63Hz
Current Consumption @ 100v (Amps)	.2A
Current Consumption @ 240v (Amps)	.15A
Typical Power Consumption (Watts)	16.8 Watts
Power Line Protection	Fast transients: 1 KV (EN61000-4-4 Criteria B) Surge: 2KV (EN61000-4-5 common mode), 1KV (EN61000-4-5 differential and common modes)
Environmental Specifications	
Operating Temperature	0°C to 55°C, 32°F to 131°F
Storage Temperature	-40°C to 85°C, -40°F to 185°F
Humidity	5 to 95% (non condensing) for both storage and operation.
Operating Altitude	Up to 3,048 meters (10,000 ft)
Ingress Protection Rating	IP30
Heat Output (BTU/HR)	122

MTBF (Hours)	190,295 Calculation model based on MIL-HDBK-217-FN2 @ 30 °C
Case	SECC Zinc plated sheet metal (1 mm)
Mounting	1U - 19" rack, front and rear mounting hardware included
Product Weight and Dimensions	
Product Weight	3.54 kg / 7.08 lbs
Dimensions	1U Rack form factor - 26.4 x 43.4 x 4.4 (cm), 10.38 x 17.1 x 1.75 (in)
Packaging	
Shipping Dimensions	59 x 36 x 9 (cm) / 23.23 x 14.17 x 3.54 (in)
Shipping Weight	4.26 kg / 9.40 lbs
Regulatory Approvals	
Emissions	FCC 47 Part 15 Subpart B Class A ICES-003 (Canada) EN55011 (CISPR11) EN55032 (CISPR32) EN61000-3-2 Limits for Harmonic Current Emissions EN61000-3-3 Limits of Voltage Fluctuations and Flicker
Immunity	EN55024 EN61000-4-2 (ESD): Contact EN 61000-4-3 (RS): EN 61000-4-4 (EFT) EN61000-4-5 (Surge) EN 61000-4-6 (CS) EN 61000-4-8 (PFMF) EN 61000-4-11
Safety	UL/EN/IEC 62368-1 (previously 60950-1) CAN/CSA C22.2 No. 62368-1 CE Mark
Other	Reach, RoHS and WEEE Compliant CCATS - G168387 ECCN - 5A992 HTSUS Number: 8517.62.0020 Perle Limited Lifetime warranty

IOLAN RJ45 Serial Connector Pinout - Straight-through cable to connect to Cisco Console port

RJ45 Socket	Pinout	Direction	EIA-232



1	in	CTS
2	in	DSR
3	in	RxD
4		GND
5		GND
6	out	TxD
7	out	DTR
8	out	RTS

Optional cable adapters available