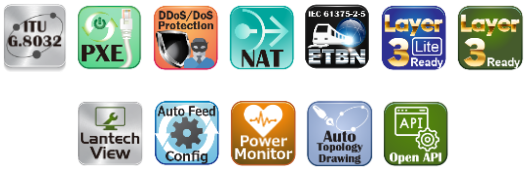
Lantech OS3/OS4 Switches

Complete Layer 2 management switch with optional software package of IEC 62443, L3 Lite, L3, NAT, and IEC 61375-2-5 ETBN



OVERVIEW

Lantech OS3/OS4 switch is powerful with complete Layer 2 management features and optional upgradable for future expansion, such as Layer 3 Lite, Layer 3, IEC61375-2-5 (ETBN), R-NAT (OS4), hardware NAT (OS4), automation protocols etc.

Support Open API document for Restful API for better switch performance; Auto-provisioning for firmware/configuration update

The switch supports Restful API that uses JSON format to access and use data for GET, PUT, POST and DELETE types to avoid traditional SNMP management occupying CPU utilization. It also supports auto-provisioning for switch to auto-check the latest software image and configuration through TFTP server.

Auto feed configuration for swapped new switches for Seamless Network Maintenance

Lantech OS3/4 switch supports auto-feed configuration features that revolutionize network switch setup and management. It ensures that new and replacement switches automatically receive the correct configuration without manual intervention.

The Optional Certified Cybersecurity IEC 62443-4-2** Helps Maintain the Safety and Reliability of Critical Infrastructure and Ensures Operational Continuity

Lantech OS3 platform is designed with the optional IEC 62443-4-2 SL2 standard of cybersecurity to prevent threats from network attacks. It includes vulnerability checking, encrypted files, public key management, strong password enforcement, account management, and penetration and stress testing, totaling more than 90 security measures. The optional certified IEC 62443-4-2** defines component-level security requirements, meets a set of security requirements with FR.1 Identification and authentication control, FR.2 Use Control, FR.3 System Integrity, FR.4 Data confidentiality, FR.5 Restricted data flow, FR.6 Timely response to events, and FR.7 Resource availability, to effectively mitigate network threats at the hardware and software level.

DDoS Security to Protect Switch and Server

OS5 platform is designed with a high standard of security methods to prevent network threads, such as prevention of DDoS attacks, 802.1X security authentication, Dynamic ARP Inspection, IP Source Guard and Port Security. The MAC-based port authentication is an alternative approach to 802.1x for authenticating hosts connected to a port. By authenticating based on the host's source MAC address, the host is not required to run a user for the 802.1x protocol. The RADIUS server that performs the authentication will inform the switch if this MAC can be registered in the MAC-table.

802.1X security by MAC address

MAC-based port authentication is an alternative approach to 802.1x for authenticating hosts connected to a port. By authenticating based on the host's source MAC address, the host is not required to run a user for the 802.1x protocol. The RADIUS server that performs the authentication will inform the switch if this MAC can be registered in the MAC address table of the switch.

DHCP option 82 & Port based, Mac based DHCP, Option 7/61/66, DHCP Snooping, IPv6 DHCP basic server, L3L**/L3** DHCP relay

DHCP server can assign dedicated IP address by MAC or by port (Port based for single switch), it also can assign IP address by port for multiple switches with single DHCP option82 server. DHCP Snooping is supported. Support DHCP Option 61 allows DHCP servers to assign consistent IP addresses or apply specific policies based on the client identity. DHCP option66 server can offer IP address of TFTP server to DHCP client for VOIP application while DHCP option7 can offer IP address of logging server. Basic Ipv6 DHCP service can be supported. (DHCP option 61 is L3L or L3 license required) Optional L3L/L3 DHCP Relay acts as an intermediary agent that enables DHCP communication between clients and servers located on different subnets or VLANs.

User friendly GUI, Auto topology drawing

The user-friendly UI, innovative auto topology drawing and topology demo makes OS3/OS4 Ethernet switches much easier to get hands-on. The complete CLI enables professional engineer to configure setting by command line.

Enhanced G.8032 ring, 8 MSTI MSTP; MRP ring

Lantech OS3/OS4 Ethernet switches features enhanced G.8032 ring which can be self-healed in less than 20ms for single ring topology protection covering multicast packets. They support various ring topologies that covers enhanced ring and basic ring by easy setup than others. OS3 also supports standard G.8032 ring to install with the other vendor's switch under G.8032 ring protection. OS3/OS4 support MSTP that allows RSTP over VLAN for redundant links with 8 MSTI. MRP (Media Redundancy Protocol) can be supported for industrial automation networks.

Enhanced Storm control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces and the detection is more precise and reaction is more efficient.

Protocol based VLAN; Subnet based VLAN; QinQ, QoS and GVRP

It supports the QinQ, QoS and GVRP for large VLAN segmentation. The protocol-based VLAN processes traffic based on protocol. It filters IP traffic from nearby end-stations using a particular protocol such as IP, IPX, ARP or other Ethernet-types in a Hex value. Subnet based VLANs group traffics into logical VLANs based on the source IP address and IP subnet. The above features can help to build VLAN in the network mixed with managed and un-managed switch as to define packets to which VLAN group based on protocol or subnet.

IGMPv3, GMRP, router port, MLD Snooping, static multicast forwarding and multicast Ring protection

The unique multicast protection under enhanced G.8032 ring can offer immediate self-recovery instead of waiting for IGMP table timeout. It also supports IGMPv3, GMRP, router port, MLD snooping and static multicast forwarding binding by ports for video surveillance application.

Support NTP, SNTP server with built-in RTC clock source (RTC is subject to model variant)

The support of NTP/SNTP is able to synchronize system clock in Internet. Lantech OS3/OS4 switch supports NTP server & server/client mode. The switch also built-in a real-time clock (RTC) for measurement the passage of time with a NTP server. (RTC is subject to model variant)

Enhanced environmental monitoring for switch inside information

The enhanced environmental monitoring can detect switch overall temperature, total power load, actual input voltage and current. It can send the SNMP traps alert when abnormal. (Subject to model variant)

Snapshot switch information for trouble-shooting analysis

With the distinctive Snapshot feature to gather switch data including port statistics, system running information, configuration and event log at the point of time or by scheduling to address switch issues and analyze the root cause in a timely manner.

Optional Layer3 Lite / Layer3 / automation protocols to be upgradable

Lantech OS3/OS4 platform is optional upgradable to L3 Lite or L3 for future expansion. The optional L3L/L3 supports enhanced routing functionality, including RIP v1/v2(L3), OSPF v1/v2, DVMRP (L3), PIM, VRRPv2, VRRP aware PIM, hardware NAT, Static NAT, PAT, Port forwarding, etc. It provides better network performance for large scale applications. (NAT is only available on OS4-L3/L3L platform) Optioanl automation protocols such as PROFINET, Modbus to be upgradeable.

Optional TTDP, TRDP (MD Reply) and R-NAT protocol for train application (EN50155 models)

Lantech OS3/OS4 platform complies with IEC 61375-3-4 (ECN) standard. The support of Ethernet Consist Network allows interconnection between end devices located in single consist of train and interoperability with IEC61375-2-5 (ETBN). The optional TTDP (Train Topology Discovery Protocol) can assign IP and Gateway IP automatically when train network topology is changed due to the adjustment of train cars. Exclusive DHCP and VLAN over TTDP can help bind device with certain IP assignment and segment VLAN in ECN network. The optional R-NAT (Railway-Network Address Translation) is under TTDP that simplifies the management of network address translation between ETB and ECN. It supports TTDP** (Train Topology Discovery Protocol) according to IEC 61375-2-5, and TRDP** (Train Real-time Data Protocol) MD Reply.

Dual NTP Server Synchronization

The switch supports dual-source NTP synchronization to ensure continuous clock accuracy. By configuring Primary and Secondary NTP servers, the switch enables automated failover if the main source fails. This redundancy prevents clock drift, maintaining precise time-stamped logs across the network infrastructure.

10G Copper Cable Monitoring function

The 10G Copper Health Diagnostic tool proactively monitors 10G copper port SNR Margin data from chipset across all cable pairs to ensure optimal 10Gbps performance. Integrated into the Web UI , it enables administrators to proactively identify signal degradation caused by electromagnetic interference, faulty connectors, or excessive cable runs that may trigger automatic speed reductions , provide the rapid troubleshooting and ensuring optimal network reliability.

Optional LantechView** for Lantech devices maintenance

LantechView can automatically discover Lantech devices on the network, providing seamless configuration management. It supports both single-device operation and batch import/export of configurations across multiple IP subnets and VLAN areas, enhancing network efficiency and management.
Additionally, LantechView also features firmware management capabilities, allowing batch verification and simultaneous upgrades to the latest firmware versions, ensuring consistency across all devices.
To learn more about Lantech LantechView software solutions, please refer to **Lantech LantechView Software Datasheet**

L2 SPECIFICATIONS

Manageability / Network

Management	SNMP v1 v2c, v3/ Web/ Telnet/ CLI
User friendly UI	● Topology View (Auto topology drawing/topology demo) ● Complete CLI for professional setting
SNMP MIB	● MIBII ● MIB ● CD MIB ● Bridge MIB ● IF MIB ● RMON MIB ● Private MIB
SNMP Trap	Up to 5 trap stations; trap types including: ● Device cold start ● Authorization failure ● Port link up/link down ● DI/DO open/close ● Typology change (ITU ring) ● Power failure ● Environmental abnormal
Firmware Update	Supports TFTP firmware update, TFTP backup and restore; HTTP firmware upgrade; USB firmware update
Configuration import and export	Supports editable configuration file for system quick installation; Support factory reset ping to restore all settings back to factory default
DHCP	Provide DHCP Client/ DHCP Server/DHCP Option 82/Port based DHCP; DHCP Snooping, DHCP Option 66; DHCP Option 7/66/PXE; basic IPv6 DHCP server; IPv6 port based DHCP; L3L**/L3** DHCP relay
Mac based DHCP Server	Assign IP address by Mac in DHCP network
DNS	Provide DNS client feature and can set Primary and Secondary DNS server
System Log	Supports System log record and remote system log server
PXE	Offer IP address of TFTP server
LLDP	Supports LLDP to allow switch to advise its identification and capability on the LAN
CDP	Cisco Discovery Protocol for topology mapping
Remote Admin	Supports 25 IP addresses that have permission to access the switch management and to prevent unauthorized intruder

Redundancy / Protection

ITU G.8032	● Support ITU G.8032 for Ring protection in less than 20ms for self-heal recovery (single ring enhanced mode) ● Support basic single ring & enhanced ring ● OS3 also support standard G.8032 ring ● Enhanced G.8032 ring configuration with ease ● Cover multicast & data packets protection
Spanning Tree	Supports IEEE802.1d Spanning Tree and IEEE802.1w Rapid Spanning Tree, IEEE802.1s Multiple Spanning Tree 8 MSTI; Supports BPDU guard/Root guard/Aggregation port
Protection	● Miss-wiring avoidance ● Node failure protection ● Loop protection

PoE (PoE models)

PoE Management	PoE Detection to check if PD hangs then restart the PD
Per Port PoE Status	On/ Off, voltage, current, watts, temperature

Security

IEC62443-4-2 Cybersecurity ready** (OS3 only)	● Cybersecurity ● Vulnerability checking ● Identification and authentication ● Resource availability
Prevention of DDoS/DoS attack	● Suspicious Packets DoS/DDoS Attacks ● Network DoS/DDoS Attacks
Network Security	Support 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder. 802.1X access control for port based and MAC based authentication/static MAC-Port binding Ingress/Egress ACL L2/L3 SSL/SSH v2 for Management HTTPS for secure access to the web interface
Login Security	Supports IEEE802.1X authentication RADIUS/TACACS+ for Authentication

Switching

VLAN	Port Based VLAN IEEE 802.1Q Tag VLAN (256 entries)/ VLAN ID (Up to 4K, VLAN ID can be assigned from 1 to 4096) GVRP, QinQ, QoS (Max 32 entries; Max 7 entries when QoS by VLAN) Protocol based VLAN Ipv4 Subnet based VLAN

IGMP	Support IGMP snooping v1, v2, v3; Supports IGMP static route; 1024 multicast groups; IGMP router port; IGMP query; GMRP
MLD Snooping	Support Ipv6 Multicast stream
Static multicast forwarding	Static multicast forwarding forward reversed IGMP flow with multicast packets binding with ports for IP surveillance application
QoS	
Quality of Service	The quality of service determined by port, Tag and Ipv4 Type of service, Ipv4 Differentiated Services Code Points – DSCP
Class of Service	Support IEEE802.1p class of service, per port provides 8 priority queues
Bandwidth Control	Support ingress packet filter and egress* packet limit. The egress rate control supports all of packet type. Ingress filter packet type combination rules are Broadcast/Multicast/Flooded Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all types of packet. The packet filter rate can be set an accurate value through the pull-down menu for the ingress packet filter and the egress packet limit.
Port Trunk with LACP	LACP Port Trunk: 8 Trunk groups
Port	
Port Mirror	Support 3 mirroring types: “RX, TX and Both packet”
Enhanced Storm Control	prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces
System	
Enhanced Environmental Monitoring	System status for actual input voltage, current, total power load and ambient temperature to be shown in GUI and sent alerting if any abnormal status
Dual Image Firmware	Support dual image firmware function
Time Management	
NTP/NTS	Supports NTP/NTS to synchronize system clock in Internet Supports NTP server & server/client mode NTP server support Primary and Backup in client mode Support NTP Time Re-correct without battery Built-in RTC clock can be clock source for NTP server (RTC is subject to model variant)
Diagnostic	Support Ping, ARP table and DDM information
Train Protocol (EN50155 models)	
ECN	Complies with IEC 61375-3-4 (ECN) standard.
Others	
Rescue mode	Offer repairing ability to repair operating system if booting image of switch is damaged.

*Future release
**Optional
***Annual license

Upgradable Package

L3L & L3 SPECIFICATIONS

Unicast Routing	
RIP v1/v2 (L3 only)	Support RIP Redistribute ● Static routes ● Route-map ● Metric Support Enhanced Redistributing Routing Protocols ● Between routing protocols (RIP, OSPF, EIGRP, BGP). ● Directly connected routes can be redistributed into a routing protocol. ● Support OSPF and RIP running simultaneously in the same system (but need to be in different interfaces) Support Equal-cost multi-path routing (ECMP) for RIP
OSPF	Support OSPF Area ● Standard Area ● Stub Area ● Stub no-summary Area Support Equal-cost multi-path routing (ECMP)
Static Route	Up to 32
Multicast Routing	
DVMRP (L3 only)	Distance Vector Multicast Routing Protocol (DVMRP) is a routing protocol used to share information between routers to facilitate the transportation of IP multicast packets among networks.
PIM (Protocol Independent Multicast)	PIM-SM (Sparse Mode) PIM-BSR (Bootstrap) PIM-DM (Dense Mode) PIM-SSM (Source-Specific Multicast Mode)
Static	Static multicast routing
Routing	
VRRPv2(RFC3768)	For Routing Redundancy Combine Max. 2 gateways as single virtual gateway VRRP aware PIM
VLAN	
Inter-VLAN routing	Support dynamic routing and static routing
Router-on-a stick	Route traffic between different VLAN groups via VLAN trunking port.

NAT** (OS4-L3/L3L only)	
Hardware NAT	Max 384 clients
Static NAT	Max 128 connections; 1 to 1
PAT (port address translation)	Max 256 connections; 1 to many; many to 1; Port forwarding
Train (EN50155 models)	
TTDP**/TRDP**	TTDP (Train Topology Discovery Protocol) complies with IEC 61375-2-5 (ETBN) standard TRDP MD Reply
DHCP for TTDP**	Support Option 61/82
R-NAT** (OS4-L3/L3L only)	Support Railway-Network Address Translation
Others	
IP based port	Support

*Future release
**Optional

SERIES COMPARISON

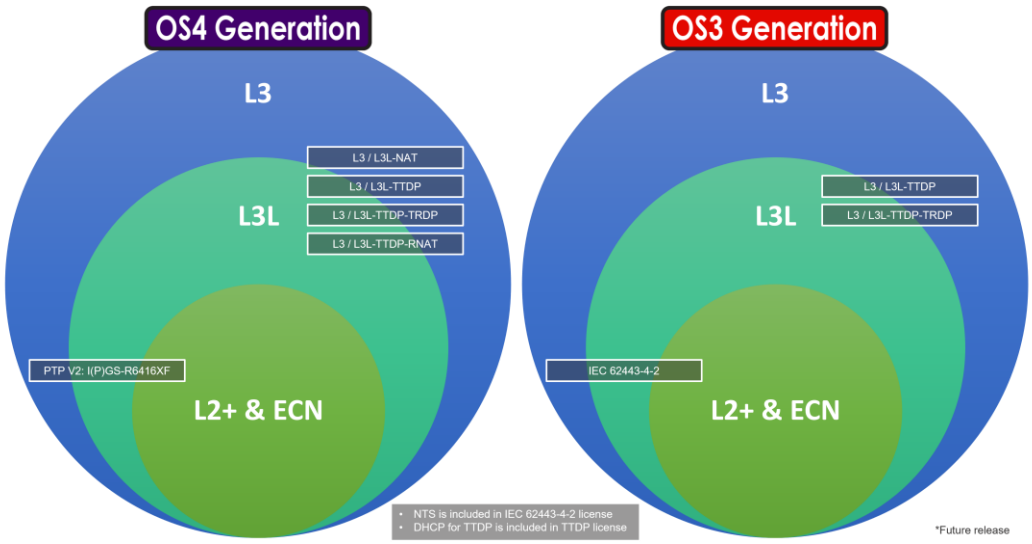
*Future release	OS5			OS4 / OS3			OS2PRO	OS2	OS1
**Optional	L3	L3 Lite	L2+	L3	L3 Lite	L2+			
Static Route	•	•		•	•		•		
Inter VLAN Routing	•	•		•	•		•		
L3 DHCP Relay	•	•		•	•		•		
Unicast Routing: RIP v1/v2	•			•			•		
Unicast Routing: OSPF v1/v2	•	•		•	•		•		
IPv6 Routing: RIPng / OSPFv3	•**								
Static Multicast Routing	•	•		•	•				
Multicast Routing: DVMRP (IPv4)	•			•					
Multicast Routing: PIM (DM) (IPv4)	•	•		•	•				
Multicast Routing: PIM (SSM) (IPv4)	•	•		•	•				
Multicast Routing: PIM (SM) (IPv4)	•	•		•	•				
Multicast Routing: PIM (BSR) (IPv4)	•	•		•	•				
IPv6 Multicast Routing: PIMv6	•**								
VRRPv2	•	•		•	•		•		
VRRP aware PIM	•	•		•	•				
VRRPv3 (IPv6)	•*								
Hardware NAT: Static NAT/ PAT	•**	•**		OS4 only**	OS4 only**		Software NAT		
MACsec	•**	•**	•**						
IEC 62443-4-2	•**	•**	•**	OS3 only**	OS3 only**	OS3 only**	•**		
Prevention of DDoS/DoS attack	•	•	•	•	•	•	•		
IP based port	•	•		•	•		•		
Rescue Mode				•	•	•			
ACL	Ingress/Egress	Ingress/Egress	Ingress/Egress	Ingress/Egress	Ingress/Egress	Ingress/Egress	Ingress Only	Ingress Only	Ingress/Egress
Port Security	•	•	•	•	•	•			
IPSource Guard	•	•	•	•	•	•			
Dynamic ARP Inspection	•	•	•	•	•	•			
Remote admin (limitation of accessing interface)	•	•	•	•	•	•	•	•	•
Remote admin Access Restriction Rules (25)	•	•	•	•	•	•	•		IP Security
Login Security (TACACS+)	•	•	•	•	•	•	•	•	•**
Login Security (RADIUS)	•	•	•	•	•	•	•	•	port authentication only
SSH	•	•	•	•	•	•	•	•	•
SSL Certificate Management	•	•	•	•	•	•	•	•	•
Perpetual / Fast PoE	•	•	•						
PTP	•**	•**	•**	I(P)GS-R6416XF**	I(P)GS-R6416XF**	I(P)GS-R6416XF**	gPTP**		
NTP/NTS (Network Time Security)	•**	•**	•**	•	•	•	•**		
PXE application	•	•	•	•	•	•			
TTDP (IEC 61375-2-5)	•**	•**		•**	•**				
R-NAT (built-in IEC 61375-2-5)	•**	•**		OS4 only**	OS4 only**				
DHCP for TTDP	•**	•**		•**	•**				
TRDP (IEC 61375-2-3)	•**	•**		•**	•**				
QoS under 61375-3-4	•	•	•	•	•	•		•	•

*Future release	OS5			OS4 / OS3			OS2PRO	OS2	OS1
**Optional	L3	L3 Lite	L2+	L3	L3 Lite	L2+			
OOB (Out of Band) Service	By model	By model	By model						
OPEN API document format for Restful API	•	•	•	•	•	•	•		
SNMP V1 / V2c / V3	•	•	•	•	•	•	•	•	•
SNMP V3 USM / VACM / TSM	•	•	•						
SNMP Trap	•	•	•	•	•	•	•	•	•
CDP	•	•	•	•	•	•	•	•	•
Firmware upgrading	WEB/SFTP/FTP	WEB/SFTP/FTP	WEB/SFTP/FTP	WEB/TFTP/FTP	WEB/TFTP/FTP	WEB/TFTP/FTP	WEB/TFTP/FTP	WEB/TFTP/FTP	WEB/TFTP/FTP
Configuration file import/export	WEB/SFTP/FTP	WEB/SFTP/FTP	WEB/SFTP/FTP	WEB/TFTP/FTP	WEB/TFTP/FTP	WEB/TFTP/FTP	WEB/TFTP/FTP	WEB/TFTP/FTP	WEB/TFTP/FTP
Auto-Provisioning	•	•	•	•*	•*				•
Snapshot	•	•	•	•	•	•	•		
Auto-Feed	•	•	•	•	•	•	•		
Dual Image				•	•	•			
Environment Monitoring	•	•	•	•	•	•	•	•**	•**
Digital Input/ Output	•	•	•	•	•	•	•	•	•
Triggered by event of environment	•	•	•	•	•	•	•	•**	•**
Triggered by event of SFP DDM	•	•	•	•	•	•	•	•	•
Ping	•	•	•	•	•	•	•	•	•
ARP	•	•	•	•	•	•	•	•	•
Topology View	•	•	•	•	•	•	•	•	•
RSPAN	•	•	•						
Port Mirroring	•	•	•	•	•	•	•		
VLAN based QoS	•	•	•	•	•	•	•	•	•
MSTP	•	•	•	•	•	•	•	•	•
MRP	•	•	•	•	•	•			•
Loop Protection	•	•	•	•	•	•	•	•	•
BPDU Guard	•	•	•	•	•	•	•		•
Dual Homing	•	•	•	•	•	•	•	•	•
Proprietary redundant protocol	ITU-Ring Standard mode	ITU-Ring Standard mode	ITU-Ring Standard mode	ITU-Ring Enhance mode (OS3 supports Standard mode)	ITU-Ring Enhance mode (OS3 supports Standard mode)	ITU-Ring Enhance mode (OS3 supports Standard mode)	ITU-Ring Enhance mode	ITU-Ring Enhance mode	ITU-Ring Enhance mode Auto Multiple VLAN Multiple Train
Protocol Based VLAN	•	•	•	•	•	•			
Subnet Based VLAN	•	•	•	•	•	•			
QinQ VLAN	•	•	•	•	•	•			•
GVRP	•	•	•	•	•	•	•	•	•
IGMP router port	•	•	•	•	•	•	•	•	•
MLD Snooping	•	•	•	•	•	•	•		
GMRP	•	•	•	•	•	•	•	•	•
DHCP by VLAN	•	•		•	•		•		
MAC based DHCP	•	•	•	•	•	•	•	•	•
Option82 DHCP Relay	•	•	•	•	•	•	•	•	•
Option 7/61/66	Option 7/66	Option 7/66	Option 7/66	Option 7/61	Option 7/61	Option 7/66	Option 7/61	Option 66 only	Option 66 only
DHCP Snooping	•	•	•	•	•	•	•	•	•
IPv6 DHCP Server	•	•	•	•	•	•			

*Future release	L3	L3 Lite	L2+	L3	L3 Lite	L2+			
**Optional	OS5			OS4 / OS3			OS2PRO	OS2	OS1

ORDERING INFORMATION

- **OS3 – L3L…….. P/N: 9000-114**
  OS3 software platform upgrade to Layer 3 Lite platform
- **OS3 – L3L –RAIL …….. P/N: 9000-115**
  OS3 software platform with IEC-61375-2-5 ETBN (Ethernet Train Backbone Networks) function w/TTDP & TRDP MD reply (under L3L)
- **OS3 – L3…….. P/N: 9000-116**
  OS3 software platform with Layer 3 functions incl. L3L
- **OS3 – L3 – RAIL …….. P/N: 9000-117**
  OS3 software platform with IEC-61375-2-5 ETBN (Ethernet Train Backbone Networks) function w/TTDP & TRDP MD reply (under L3)
- **OS3 – IEC62443-4-2…….. P/N: 9000-11**
  OS3 software platform IEC-62443-4-2 Cybersecurity features
- **OS4 – L3L…….. P/N: 9000-110**
  OS4 software platform upgrade to Layer 3 Lite platform
- **OS4 – L3L – RAIL ……P/N: 9000-113**
  OS4 software platform with IEC-61375-2-5 ETBN (Ethernet Train Backbone Networks) function w/ R-NAT, TTDP & TRDP MD reply (under L3L)
- **OS4 – L3…….. P/N: 9000-112**
  OS4 software platform with Layer 3 functions incl. L3L
- **OS4 – L3 – RAIL ……P/N: 9000-118**
  OS4 software platform with IEC-61375-2-5 ETBN (Ethernet Train Backbone Networks) function w/R-NAT, TTDP & TRDP MD reply (under L3)



Lantech Communications Global Inc.
www.lantechcom.tw
info@lantechcom.tw