

# **ZISA OP3608 8Ports GPON Cassette OLT**



High Performance 8ports GPON OLT, 8xGE or 2\*10G SFP+ uplink

#### **Product Overview**

OP3608 is a small capacity and enhancement mode cassette GPON OLT, meeting the requirements of *ITU-T G.984/G.988* and relative standards of *Telecom level GPON*, possessing super GPON access capacity, carrier-class reliability and the complete security function. It can satisfy long-distance optical fiber access requirement on account of its excellent management, maintenance and monitoring capability, abundant service features and flexible network mode.OP3608 can be used via CLI and SNMP network management system so as to provide users with the perfect solution.

OP3608 provides 8 downlink GPON port, 8 \*GE combo port or 2\* 10G SFP+ port. Single PON port can manage 128 ONUs, one pcs OP3608 max to 1024 ONUs. The height is only 1U for easy installation and space saving. OP3608 is suitable for Broadcast *three in one*, video surveillance network, enterprise LAN, Internet of Things, etc.FTTH network.

#### OP3608



- □ 1 RU19 inch
- □ 1+1 power redundancy
- 8\* fixed GPON port
- □ 8\*GE or 2\*10GE SFP+
- 1\* console port
- □ 2\* MGMT port



# Product Specification:

Item	OP3608
Switching Capacity	40Gbps
Forwarding Capacity(Ipv4/Ipv6)	104MPPS
Service Port	8*PONport, 8*GE SFP, or 2*10GE SFP+ port
Redundancy Design	Dual power supply Support AC input, double DC input and AC+DC input
Power Supply	AC: input 90~264V 47/63Hz; DC: input -36V~-72V;
Power Consumption	Typical: 48W; Maximum: 72W
Dimensions (Width x Depth x Height)	440mm×44mm×340mm
Weight (Full-Loaded)	≤3kg
Environmental Requirements	Working temperature: -5°C∼55°C Storage temperature: -40°C∼70°C Relative humidity: 10%∼90%, non-condensing

## **Product Features:**

Item		OP3608	
		ITU-TG.984.x standard	
		Maximum 20 Km PON transmission distance	
		Each PON port access 128 ONU and 1K T-CONT	
		Uplink and downlink triple churning encrypted function with 128Bits	
		Support of five types T-CONT bandwidth profile	
PON Features		ONU terminal legitimacy certification, report illegal ONU registration	
		Support of multiple ONU authentication mechanism: SN, Password, SN plus Password, Loid, LoidPassword.	
		Support of ranging and logical distance configuration	
		Support of upstream and downstream FEC enabling/disabling	
		DBA algorithm, the particle is 1Kbit/s	
		Standard OMCI management function	
		ONU batch software upgrade, fixed time upgrade, real time upgrade	
		PON port optical power detection	
L2 Features	MAC	MAC Black Hole	
		Port MAC Limit	
		64K MAC (packet exchange chip cache 2MB, external cache 720 MB )	
	VLAN	4K VLAN entries	
		Port-based/MAC-based/protocol/IP subnet-based	



Support of VLAN add, remove, translate and transparent per ONU service   Support of VLAN add, remove, translate and transparent per ONU service     PVLAN to realize port isolation and saving public-vlan resources   GVRP     Spanning Tree   Str/RSTP/MSTP Remote loop detecting     Bi-directional bandwidth control Static link aggregation and LACP(Link Aggregation Control Port mirroring and traffic mirroring     Viser's Security   Anti-ARP-spoofing Anti-ARP-flooding IP Source Guard create IP+VLAN+MAC+Port binding Port Isolation     Viser's Security   Port colation     Anti-ARP-flooding IEEE 802.1x and AAA/Radius authentication     Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP     detection, worm and Msblaster worm attack SSHv2 Secure Shell SNMP v3 encrypted management Security IP login through Telnet Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and proce-out user with abnormal ARP traffic of each user and proce-out user with abnormal ARP traffic of each user and proce-out user with abnormal ARP traffic of each user and core-out user with abnormal ARP traffic of each user and ANA, NAN, 802, 10, 10, 10, 10			Support of QinQ based on port or service flow
Spanning Tree   GVRP     Spanning Tree   STP/RSTP/MSTP Remote loop detecting     Bi-directional bandwidth control   Static link aggregation and LACP(Link Aggregation Control Protocol)     Port   Bi-directional bandwidth control     Static link aggregation and LACP(Link Aggregation Control Protocol)   Port mirroring and traffic mirroring     User's   Security   Anti-ARP-spoofing Anti-ARP-flooding     IP Source Guard create IP+VLAN+MAC+Port binding Port Isolation   Port and MAC address filtering IEEE 802.1x and AAA/Radius authentication     Device   Security   Anti-OS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP     Oevice   Security   ShV2 Secure Shell     SNMP v3 encrypted management Security IP login through Telnet   Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP traffic of each user and bob bytes of the head of user-defined packet     Network Security   Standard and extended ACL     Time Range ACL Pion vasification and flow definition based on source/destination P(PV/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head Support of priority remark based on port or self-defined service flow Support of provi			Support of VLAN add, remove, translate and transparent per
Spanning Tree   STP/RSTP/MSTP Remote loop detecting     Bi-directional bandwidth control   Static link aggregation and LACP(Link Aggregation Control Prot mirroring and traffic mirroring     Port   Static link aggregation and LACP(Link Aggregation Control Prot mirroring and traffic mirroring     User's   Anti-ARP-spoofing Anti-ARP-spoofing     Viser's   Port counce Guard create IP+VLAN+MAC+Port binding Port Isolation     MAC address binding to the port and MAC address filtering IEEE 802.1x and AAA/Radius authentication     Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP detection, worm and Msblaster worm attack SSHv2 Secure Shell SNMP v3 encrypted management Security IP login through Telnet Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP traffic of each user and force-out user with abnormal ARP traffic of user and force-out user with abnormal ARP traffic of user and strack DHCP Option82 and PPPoE+ upload user's physical location Plaintex authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication     Service Features   Standard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination PICH/4I/Pv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head Support of rate-limit based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			
Spanning Tree   Remote loop detecting     Port   Bi-directional bandwidth control Static link aggregation and LACP(Link Aggregation Control Protocol) Pott mirroring and traffic mirroring     User's   Anti-ARP-spoofing Anti-ARP-flooding     User's   Security     Port Isolation   MAC address binding to the port and MAC address filtering IEEE 802.1x and AAA/Radius authentication     Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP detection, worm and Msblaster worm attack SSHv2 Secure Shell SNMP v3 encrypted management Security Piogin through Telnet Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP table-based binding IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based bioadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPOE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication     Service Features   AC			GVRP
Security   Remote loop detecting     Port   Bi-directional bandwidth control Static link aggregation and LACP(Link Aggregation Control Protocol)     Port   Static link aggregation and LACP(Link Aggregation Control Protocol)     Port mirroring and traffic mirroring   Anti-ARP-spoofing Anti-ARP-flooding     User's   Security     Port Isolation   MAC address binding to the port and MAC address filtering IEEE 802.1x and AAA/Radius authentication     Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP detection, worm and Msblaster worm attack     Security   Device Security     Features   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP table-based binding IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port URF to prevent IP address counterfeit and attack DHCP Option82 and PPPOE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication     Service Features   ACL   Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(Pv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head Support of rate-limit based on port or self-defined service flow and provide 802.1P, DSCP priority and R			STP/RSTP/MSTP
Port   Static link aggregation and LACP(Link Aggregation Control Protocol)     Port   Static link aggregation and LACP(Link Aggregation Control Protocol)     Port mirroring and traffic mirroring   Anti-ARP-spoofing Anti-ARP-spoofing     IJser's Security   IP Source Guard create IP+VLAN+MAC+Port binding Port Isolation     MAC address binding to the port and MAC address filtering IEEE 802.1x and AAA/Radius authentication     Device Security   Anti-ARP-flooding telest Security     Device Security   Device Security     Security   Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP detection, worm and Msblaster worm attack     Security   SSHv2 Secure Shell     Security   SNMP v3 encrypted management Security IP login through Telent     Hierarchical management and password protection of users     Security   User-based MAC and ARP traffic examination     Restrict ARP traffic of each user and force-out user with abnormal ARP traffic     Dynamic ARP table-based binding IP+VLAN+MAC+Port binding     L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet     Port-based broadcast/multicast suppression and auto-shutdown risk port     URPF to prevent IP address counterfeit and attack DHCP option82 and PPDet-upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5		Spanning free	Remote loop detecting
Poil   Protocol)   Protocol)     Port mirroring and traffic mirroring   Port mirroring and traffic mirroring     Anti-ARP-spoofing   Anti-ARP-flooding     IP Source Guard create IP+VLAN+MAC+Port binding   Port Isolation     MAC address binding to the port and MAC address filtering   IEEE 802.1x and AAA/Radius authentication     Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP   detection, worm and Msblaster worm attack     Security   Device   Security P login through Telnet     Features   User-based MAC and ARP traffic examination     Restrict ARP traffic of each user and force-out user with abnormal ARP traffic   Dynamic ARP table-based binding     IP+VLAN+MAC+Port binding   L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet     Port-based broadcast/multicast suppression and auto-shutdown risk port   URPF to prevent IP address counterfeit and attack     DHCP Option82 and PPPOE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MDS   Standard and extended ACL     Service   Features   Standard and extended ACL   Time Range ACL     Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc   packet filtration of L2~L7 deep to 80 bytes of IP packet hea			Bi-directional bandwidth control
Security   Anti-ARP-sporting Anti-ARP-flooding IP Source Guard create IP+VLAN+MAC+Port binding Port Isolation MAC address binding to the port and MAC address filtering IEEE 802.1x and AAA/Radius authentication     Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP detection, worm and Msblaster worm attack SSHv2 Secure Shell SNMP v3 encrypted management Security IP login through Telnet Hierarchical management and password protection of users     Vertex   User-based MAC and ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP table-based binding IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication     Service Features   ACL   Standard and extended ACL Time Range ACL Flow classification MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head     Service Features   Support of priotiv remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark		Port	
Security   Anti-ARP-flooding     IP Source Guard create IP+VLAN+MAC+Port binding Port Isolation   MAC address binding to the port and MAC address filtering IEEE 802.1x and AAA/Radius authentication     Device Security   Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP detection, worm and Msblaster worm attack SSHv2 Secure Shell SNMP v3 encrypted management Security IP login through Telnet Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP table-based binding IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication     Service Features   ACL   Standard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IP4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head     Support of rate-limit based on port or self-defined service flow support of rate-limit based on port or self-defined service flow service flow and provide 802.1P, DSCP priority and Remark			Port mirroring and traffic mirroring
Security   IP Source Guard create IP+VLAN+MAC+Port binding Port Isolation     MAC address binding to the port and MAC address filtering IEEE 802.1x and AAA/Radius authentication     Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP detection, worm and Msblaster worm attack SSHv2 Secure Shell SNMP v3 encrypted management Security IP login through Telnet Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP traffic abnormal and password protection of users     Network Security   L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port     URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication     Service Features   ACL   Standard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination M2C address, VLAN, 802.1p, ToS, DiffServ, source/destination M2C address, VLAN, 802.1p, ToS, DiffServ, source/destination PI(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			Anti-ARP-spoofing
Security   Port Isolation     MAC address binding to the port and MAC address filtering IEEE 802.1x and AAA/Radius authentication   Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP     Device Security   Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP   detection, worm and Msblaster worm attack     SSHv2 Secure Shell   SSHv2 Secure Shell   SSHv2 Secure Shell     Security IF login through Teinet   Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination     Restrict ARP traffic of each user and force-out user with abnormal ARP traffic   Dynamic ARP table-based binding     Dynamic ARP table-based binding   L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet     Port-based broadcast/multicast suppression and auto-shutdown risk port   URPF to prevent IP address counterfeit and attack     DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5   Standard and extended ACL     Time Range ACL   Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPV4/IPV6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head     Support of rate-limit based on port or self-defined service flow service flow and provide 802.1P, DSCP priority and Remark <td></td> <td></td> <td>Anti-ARP-flooding</td>			Anti-ARP-flooding
Security   MAC address binding to the port and MAC address filtering IEEE 802.1x and AAA/Radius authentication     Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP detection, worm and Msblaster worm attack SSHv2 Secure Shell SNMP v3 encrypted management Security IP login through Telnet Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP table-based binding IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication     Service Features   ACL   Standard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head     Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark		User's	IP Source Guard create IP+VLAN+MAC+Port binding
Security   IEEE 802.1x and AAA/Radius authentication     Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP detection, worm and Msblaster worm attack   SSHv2 Secure Shell     Security   SSHv2 Secure Shell   SNMP v3 encrypted management     Security IP login through Telnet   Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination     Restrict ARP traffic   Dynamic ARP traffic     Dynamic ARP traffic   Dynatoatestraffic     Dynatic ARP traffic   Dynothitatestraffic		Security	Port Isolation
Security   Anti-DOS attack(such as ARP, Synflood, Smurf, ICMP attack), ARP detection, worm and Msblaster worm attack SSHv2 Secure Shell SNMP v3 encrypted management Security IP login through Telnet Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP table-based binding IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication     Service Features   ACL   Standard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination MAC address, VLAN, 802. 1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			MAC address binding to the port and MAC address filtering
Security   attack), ARP     detection, worm and Msblaster worm attack   SSHv2 Secure Shell     SNMP v3 encrypted management   Security IP login through Telnet     Hierarchical management and password protection of users   Security IP login through Telnet     Features   User-based MAC and ARP traffic examination     Restrict ARP traffic of each user and force-out user with abnormal ARP traffic   Dynamic ARP table-based binding     IP+VLAN+MAC+Port binding   L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet     Port-based broadcast/multicast suppression and auto-shutdown risk port   URPF to prevent IP address counterfeit and attack     DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5   cryptograph authentication     Service   ACL   Standard and extended ACL   Time Range ACL     Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc   packet filtration of L2~L7 deep to 80 bytes of IP packet head     QoS   Support of rate-limit based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			IEEE 802.1x and AAA/Radius authentication
Device Security   SSHv2 Secure Shell     Security   SSHv2 Secure Shell     Security IP login through Telnet Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic     Network Security   User-based IAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic     Upnamic ARP table-based binding IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port     URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication     Standard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head     Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			
Security   Solve Secure Stein     Security   SNMP v3 encrypted management Security IP login through Telnet Hierarchical management and password protection of users     Features   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP table-based binding IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication     Service Features   ACL   Standard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head     Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			detection, worm and Msblaster worm attack
Security SNMP v3 encrypted management   Security IP login through Telnet Hierarchical management and password protection of users   Features User-based MAC and ARP traffic examination   Restrict ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP table-based binding   IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet   Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack   DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication   Service ACL Standard and extended ACL Time Range ACL   Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head   Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			SSHv2 Secure Shell
Security Features   Hierarchical management and password protection of users     Vertice   User-based MAC and ARP traffic examination Restrict ARP traffic of each user and force-out user with abnormal ARP traffic     Dynamic ARP table-based binding IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet     Port-based broadcast/multicast suppression and auto-shutdown risk port     URPF to prevent IP address counterfeit and attack     DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication     Service Features   ACL   Standard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head     Support of rate-limit based on port or self-defined service flow service flow and provide 802.1P, DSCP priority and Remark		Security	SNMP v3 encrypted management
Features User-based MAC and ARP traffic examination   Restrict ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP table-based binding   IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet   Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack   DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication   Service ACL Standard and extended ACL   Time Range ACL Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc   packet filtration of L2~L7 deep to 80 bytes of IP packet head Support of rate-limit based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			Security IP login through Telnet
Service ACL User-based MAC and ARP traffic examination   Restrict ARP traffic of each user and force-out user with abnormal ARP traffic Dynamic ARP table-based binding   IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet   Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack   DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 Standard and extended ACL   Service Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head   Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark Support of priority remark based on port or self-defined service flow	Security		Hierarchical management and password protection of users
Network Securityabnormal ARP traffic Dynamic ARP table-based binding IP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authenticationService FeaturesACLStandard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet headQoSSupport of rate-limit based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark	Features		User-based MAC and ARP traffic examination
Network SecurityIP+VLAN+MAC+Port binding L2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authenticationService FeaturesACLStandard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet headQoSSupport of rate-limit based on port or self-defined service flow service flow and provide 802.1P, DSCP priority and Remark			
Network SecurityL2 to L7 ACL flow filtration mechanism on the 80 bytes of the head of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authenticationService FeaturesACLStandard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet headQoSSupport of rate-limit based on port or self-defined service flow support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			Dynamic ARP table-based binding
Network Securityhead of user-defined packet Port-based broadcast/multicast suppression and auto-shutdown risk port URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authenticationService FeaturesACLStandard and extended ACL Time Range ACL Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet headSupport of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			IP+VLAN+MAC+Port binding
Service ACL Fortbased bioadcast suppression and auto-shutdown risk port   URPF to prevent IP address counterfeit and attack DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5   cryptograph authentication Standard and extended ACL   Time Range ACL Flow classification and flow definition based on source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc   Features QoS			
Building DHCP Option82 and PPPoE+ upload user's physical location Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5 cryptograph authentication   Service Standard and extended ACL   Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc   Features Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark		Security	
Plaintext authentication of OSPF, RIPv2 and BGPv4 packets and MD5   cryptograph authentication   Standard and extended ACL   Time Range ACL   Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc   Packet filtration of L2~L7 deep to 80 bytes of IP packet head   Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			URPF to prevent IP address counterfeit and attack
Service ACL Standard and extended ACL   Service Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc   Features packet filtration of L2~L7 deep to 80 bytes of IP packet head   Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow			Plaintext authentication of OSPF, RIPv2 and BGPv4 packets
Service ACL Time Range ACL   Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head   Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow			cryptograph authentication
ACL Flow classification and flow definition based on source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head   Service Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark		ACL	Standard and extended ACL
ACL source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP port number, protocol type, etc packet filtration of L2~L7 deep to 80 bytes of IP packet head   Support of rate-limit based on port or self-defined service flow Support of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			Time Range ACL
Features   packet filtration of L2~L7 deep to 80 bytes of IP packet head     Support of rate-limit based on port or self-defined service flow   Support of priority remark based on port or self-defined service flow     QoS   Support of priority remark based on port or self-defined			source/destination MAC address, VLAN, 802.1p, ToS, DiffServ, source/destination IP(IPv4/IPv6) address, TCP/UDP
QoSSupport of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark			packet filtration of L2 $\sim$ L7 deep to 80 bytes of IP packet head
QoSSupport of priority remark based on port or self-defined service flow and provide 802.1P, DSCP priority and Remark		QoS	Support of rate-limit based on port or self-defined service flow
			Support of priority remark based on port or self-defined
service flow, support of 8 priority queues, scheduler algorithm is SP, WRR, or SP plus WRR.			service flow, support of 8 priority queues, scheduler algorithm

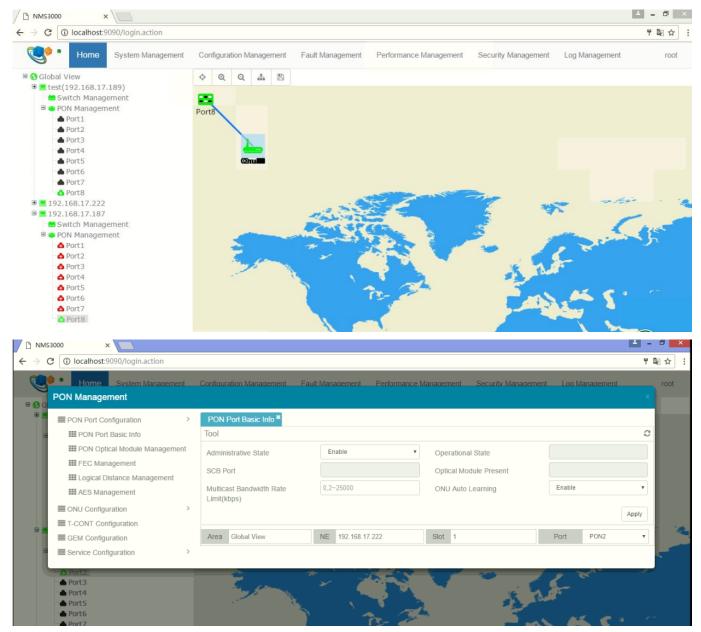


	IPv4	ARP Proxy DHCP Relay DHCP Server Static Routing RIPv1/v2 OSPFv2 BGPv4 Equivalent Routing Routing Strategy
	IPv6	ICMPv6 ICMPv6Redirection DHCPv6 ACLv6 OSPFv3 RIPng BGP4+ Configured Tunnels ISATAP 6to4Tunnels Dual stack of IPv6 and IPv4
	Multicast	IGMPv1/v2/v3 IGMPv1/v2/v3 Snooping IGMP Filter MVR and cross VLAN multicast copy IGMP Fast leave IGMP Proxy PIM-SM/PIM-DM/PIM-SSM PIM-SMv6, PIM-DMv6, PIM-SSMv6 MLDv2/MLDv2 Snooping
	Loop	EAPS and GERP (recover-time <50ms)
	Protection	Loopback-detection
Reliability	Link Protection	Flex link (recover-time <50ms) RSTP/MSTP (recover-time <1s) LACP (recover-time <10ms) BFD
	Device Protection	VRRP host backup 1+1 power hot backup
Maintenance	Network Maintenance	Port real-time, utilization and transmit/receive statistic based on Telnet RFC3176 sFlow analysis LLDP GPON OMCI RFC 3164 BSD syslog Protocol Ping and Traceroute
	Device Management	CLI, Console port, Telnet and WEB SNMPv1/v2/v3 RMON (Remote Monitoring)1,2,3,9 groups MIB



	NTP	
	NGBNView network management	

#### **OLT NMS software Detail**



#### **Purchase Information:**

Product name	Product description
OP3608	8*PON, 8*GE SFP or 2*10GE SFP+, support double AC/DC power supply
OP3616	16*PON, 8*GE SFP or 2*10GE SFP+, support double AC/DC power supply
360PWRAC	power module for360PWRAC
360PWRDC	power modulefor 360PWRDC



# Contact us

## ZISA Corporation Limited

Mail to :sales@zisacom.com.cn

URL: http://www.zisacom.com

Specifications are subject to change without notice.

Copyright © ZISA Corp. All rights reserved.

