ipinfusion™

OcNOS™ Data Sheet

OcNOS™

Product Overview

OcNOS™ is a networking solution built with traditional networking components along with components to transition to the new disruptive networking technologies. It has been designed to meet the one primary need of a networking solution when deployed at multiple locations, and that is reduced CapEx and OpEx.

Designed to take advantage of commodity hardware and therefore reduced CapEx, it maintains investor protection by maintaining the operational and interop requirements met as present with traditional networking gear.

OcNOS heavily borrows from the popular ZebraOS line of products, thus has a rich feature density and robustness built up over the years. OcNOS provides industry standard CLI, supports all standard MIBs and other standard operation and management tools.

Its integrated centralized management and provisioning layer allows for transaction based configuration and device feature modelling. The management layer exposes Netconf, REST APIs besides custom CLI generation capability. All this allows an OcNOS system to be configured, managed and controlled by Network Management System for scaled topologies and in more than one way.

OcNOS is a modular, multi-tasking network operating system, with tight integration capabilities on commodity hardware. This design allows for scaled and performance critical deployments. The niche coupling with merchant silicon utilizes key hardware capabilities for better performance and feature set.

Features and Benefits

Flexibility and Scalability

- **Common software for multiple deployments and hardware:** OcNOS is designed using several inbuilt abstraction layers. These abstraction layers, allow the software to run over multiple control plane CPU and forwarding chipset hardware. The system calls are also well abstracted allowing to switch across operating systems if required. It has been integrated with verified with multiple commodity hardware, which again allows transition easily.
- **Interoperation and ease of use:** OcNOS solution is build using standards based definitions, as well as has popular vendor specific extensions. The operation and management is provided using CLI and SNMP. This allows the OcNOS based network node to be easy to operate and interoperate with another vendor node.
- **Modular software design:** OcNOS software design is highly modular with multiple processes handing each individual key protocols. The processes are managed and contained by a process handler framework, which also monitors the processes, restarts and maintains event logging for them. OcNOS can be build and packaged with minimal software features, reducing CapEx and device footprint.
- **Support for disruptive networking technologies:** OcNOS supports technologies required for bandwidth scaling at data centers and interconnects. It has a centralized transaction based modelling layer which allows for multiple management interfaces, this in-turn allows for a central service level provisioning and chaining across multiple devices. It supports technologies required for SDN and NFV.

Availability

- **Protocol level redundancy:** OcNOS provides standards based redundancy protocols like VRRP, BFD, ring failure recovery protocols, MLAG, UDLD and graceful restart mechanisms. These provide a guaranteed network level redundancy.
- **Device level redundancy:** OcNOS supports service availability frameworks based master-slave hot standby syncing. This feature is supported for several key protocols allowing device level redundancy in the absence of peer level network support.
- **Easy upgrades:** The modularity of OcNOS allows for individual process/protocol level upgrades and restarts without disturbing the running system. OcNOS will support ISSU for stateless upgrades.
- **Process survivability:** OcNOS has an inbuilt process hearbeat monitoring and restart feature in a 1U or multi-chassis format. This leads to minimal downtime and unavailability at critical deployments.

Serviceability

- **Troubleshooting and diagnostics:** OcNOS supports event and process logging both local and remote, using standard mechanisms like syslog and traps. It also supports several system level diagnostics for health monitoring. These can provide useful data for troubleshooting and diagnostics.
- **Traffic Monitoring:** OcNOS can monitor traffic using standard port mirroring techniques. It can also do sample based traffic monitoring using sFlow protocol.
- **System Configuration and Management:** OcNOS provides well known mechanisms for device control like boot parameters, password recovery.

Manageability

- **Programmable and Flexible Management Layer:** OcNOS has an internal transaction based management layer with open programmable upper layer. This allows it be programmed using NetConf, SNMP, HTTP traditional or Custom CLI mechanism.
- **Simple Network Management Protocol (SNMP):** OcNOS complies with SNMPv1, v2c, and v3.

A comprehensive collection of MIBs is supported.

- **Configuration verification and rollback:** With OcNOS, the system operator can verify the consistency of a configuration and the availability of necessary hardware resources prior to committing the configuration. A device can thus be preconfigured and the verified configuration applied at a later time. Configurations also include checkpoints to allow operators to roll back to a known good configuration as needed.
- **Role-based access control (RBAC):** With RBAC, OcNOS enables administrators to limit access to switch operations by assigning roles to users. Administrators can customize access and restrict it to the users who require it. The authentication and authorization is supported using both RADIUS & TACACS+.

Traffic Routing, Forwarding, and Management

- **Ethernet switching:** The solution supports the complete feature set required to run it as pure Layer2 or Layer2-3 switch. This feature set includes IEEE 802.1D-2004, Rapid Spanning Tree Protocol(RSTP), Multiple Spanning Tree Protocol(MSTP) IEEE 802.1w & 802.1s, RPVST, QinQ, IEEE 802.3ad link aggregation, Multi-Chassis Link Aggregation, IEEE 802.1AB Link Layer Discovery Protocol (LLDP), PVLAN, UDLD, BPDU Guard, Loop guard, Switched VLAN Interface support, EVB & DCB support.
- **Datacenter features:** OcNOS supports multiple standards based multi-path Ethernet technologies for the datacenter. They are TRILL, SPB and Multi-chassis Link Aggregation Group. Apart from these it also supports Data Center Bridging (DCB), QCN, ETS and PFC for true unified Ethernet backplane. These technologies are well supported by the related integrated hardware, resulting in line rate performance. For Layer-3 based data center deployments, OcNOS has BGP, OSPF support with a very large ECMP fan out.
- **IP routing:** OcNOS supports a wide range of IPv4 and v6 services and routing protocols. Notable;
  - Open Shortest Path First (OSPF) Protocol Versions 2 (IPv4) and 3 (IPv6)
  - Intermediate System-to-Intermediate System (IS-IS) Protocol for IPv4 and IPv6
  - Border Gateway Protocol (BGP) for IPv4 and IPv6
  - Routing Information Protocol Version 2 (RIPv2)

The implementations of these protocols are fully compliant with the latest standards, providing modern enhancements and parameters such as 4-byte autonomous system numbers (ASNs), NSF graceful restart (NSF-GR) is supported by all unicast protocols. All protocols support all interface types, including Ethernet interfaces, switched virtual interfaces (SVIs) and subinterfaces, PortChannels, tunnel interfaces, and loopback interfaces. The great variety of routing protocols and functions is complemented by a broad collection of IP services, including the following:

  - VRF-lite and MPLS VPNs as described in RFCs 2547 and 4364
  - Dynamic Host Configuration Protocol (DHCP) Helper
  - Unicast Reverse Path Forwarding (uRPF) for IPv4 and IPv6
  - Hot-Standby Routing Protocol (HSRP) for IPv4 and IPv6
  - Virtual Router Redundancy Protocol (VRRP) for IPv4
  - Generic routing encapsulation (GRE) tunneling
  - Unicast graceful restart for IPv4 OSPF, LDP, RSVP
  - Unicast graceful restart for OSPFv3 in IPv6

- **IP Multicast:** OcNOS provides an a feature rich in multicast. The OcNOS implementation lays the foundation for the future development of a comprehensive portfolio of multicast- enabled network functions. In a way similar to its support for the unicast routing protocols, OcNOS includes state-of-the-art implementations of the following multicast protocols and functions:
  - Protocol-Independent Multicast Version 2 (PIMv2)
  - Source-Specific Multicast (SSM) for IPv4 and IPv6
  - PIM Sparse Mode (Any-Source Multicast [ASM] for IPv4 and IPv6)
  - Bidirectional PIM (Bidir PIM) for IPv4 and IPv6
  - Anycast Rendezvous Point (Anycast-RP)
  - RP-Discovery using bootstrap router (BSR): Auto-RP and static
  - Internet Group Management Protocol (IGMP) Versions 1, 2, and 3 router role
  - IGMPv2 host mode
  - IGMP snooping
  - Multicast Listener Discovery (MLD) Protocol Version 2 (for IPv6)
  - Multicast Source Discovery Protocol (MSDP) (for IPv4 only)
  - IGMP cache on non-disaster recovery for fast convergence
  - IGMP group-specific queries to router ports only
  - Debug filters for IGMP snooping
- **Quality of service (QoS):** OcNOS supports numerous QoS mechanisms, including classification, marking, queuing, policing, and scheduling. Both Hierarchial and Modular QoS CLI (MQC) are supported.
- **Multiprotocol Label Switching (MPLS):** OcNOS supports a comprehensive set of MPLS features including label switching, Layer 3 VPNs, MPLS Traffic Engineering with Fast Reroute (FRR), Multicast VPNs for IPv4, and IPv6 provider edge (6PE) and IPv6 VPN provider edge (6VPE).
- **Time synchronization:** Utilizing Precision Time Protocol (PTP): IEEE 1588, or PTP, is a time synchronization protocol for nodes distributed across a network. It provides greater accuracy than other time synchronization protocols, such as NTP, because of its hardware time-stamp feature.

Network Security

- **Network security features:**
  - Authentication, authorization, and accounting (AAA) and TACACS+
  - Secure Shell (SSH) Protocol Version 2
  - SNMPv3 support
  - Port security
  - IEEE 802.1x authentication and RADIUS support
  - Policies based on basic and extended ACL's

Software Features for OcNOS R0 release

The tables below list the software features in OCNOS available release. Note, the below mentioned features are only indicative and the detail feature list may vary.

System Level Features

Description
ONIE support
Hardware Diagnostics: Status/Utilization Monitor Memory, CPU, FAN, power supply, temperature, voltage
Display System information (model revision, motherboard assembly number and revsion number, chassis serial, SFP type and serial, Power supply type and serial, FAN status, type and speed, software version, software package)
System uptime
Fan/LED/System level control
SFP+ /SFP Bandwidth setting

Layer2 Features

Description
STP-IEEE 802.1D
IEEE 802.1w - RSTP
IEEE 802.1s - MSTP
Root Guard
VLAN-IEEE 802.1Q VLAN trunking
Routed VLAN interface
Port based VLAN
QinQ
VLAN translation
Static MAC address assignment
IEEE 802.3ad-LAG
IEEE 802.1ab-LLDP
LAG load sharing
MAC addresses
VLANs
CFM 802.1ag
Authentication 802.1X

Layer3 Features

Description
Static Routing
Routing policy
RIP
IPv6
BFD Echo Mode
BFD Packet Intervals and failure detection on physical interfaces
BFD for IPV4(single hop)
BFD over BGP(IPV4)
BFD over ISIS(v4 and V6)
BFD over OSPF
BFD on static route (IPV4)
BFD on static route (IPV6)
BFD for IPV6(global and link local addressing)
BFD on mutlihops
BGP 4
BGP 4 Multipath Support
BGP 4 Prefix Filter and In-bound Route Maps
BGP 4 Soft Config

Layer3 Features, continued

Description
BGP Named Community Lists
BGP Neighbor Policy
BGP Next Hop Propagation
BGP Per Neighbor Graceful Restart Configuration
BGP Per Neighbor SOO Configuration
BGP Prefix-Based Outbound Route Filtering
BGP Soft Reset
BGP Support for 4-byte ASN
BGP Support for BFD
BGP Support for Named Extended Community Lists
BGP Support for Next-Hop Address Tracking
BGP Support for Sequenced Entries in Extended Community Lists
BGP Support for the L2VPN Address Family
BGP - Remove/Replace Private AS Filter
BGP - iBGP NSR
BGP VPLS Auto Discovery Support on Route Reflector
BGP: Graceful Shutdown (GSHUT)
BGP: RT Constrained Route Distribution
BGPv4 MD5 Authentication
Open Shortest Path First Version 2
Open Shortest Path First Version 2 (OSPFv2) MIB – Supported RFC 4750
Applicability statement for OSPF
OSPF Opaque LSA option
OSPF-TE: Traffic Engineering (TE) Extensions
OSPFv2 Multiple Instance Support
Prioritized Treatment of Specific OSPFv2 Packets and Congestion Avoidance
Passive Interface Support for OSPFv2
OSPF Multi-Area Adjacency
OSPF Database Exchange Summary List Optimization
OSPF Not-So-Stubby-Area (NSSA) Option
Bidirectional Forwarding Detection Trigger
OSPF: Link-local Signaling
OSPF: Restart Signaling
IP FRR: OSPF-LFA
Open Shortest Path First Version 3 (OSPFv3) for IPv6 Support

Layer3 Features, continued

Description
OSPF Multi-Area Adjacency
OSPF Multi-Instance Extensions
OSPF Database Exchange Summary List Optimization
OSPF Not-So-Stubby-Area (NSSA) Option
Passive Interface Support in OSPFv3
Traffic Engineering Extensions to OSPF Version 3 OSPFv3 MIB
Bidirectional Forwarding Detection Trigger for OSPFv3
Support for Multiple Address Families
VRRP
Multiple Virtual Router Support
VRRP Router priority and Preemption
VRRP Advertisements
VRRP Object Tracking
VRRP Authentication
VRRP support over IPv6
VRRP MIB
VRRP on VLAN
VRRP Interface tracking

Multicast Features

Description
IGMPv1,v2,v3
IGMP Snooping,querier,proxy report suppression
PIM-SM
PIM-SSM
PIM-DM

Data Center Features

Description
IEEE 802.1Qbb - PFC
IEEE 802.1Qaz - ETS
DCBX

Security Features

Description
Secure interface login and password
RADIUS
Ingress and Egress Filters
Filter actions: Logging, system logging, reject, mirror, counters, forwarding lcass, permit, drop, police, mark
SSH v1,v2
Static ARP support
DHCP Snooping
Flow control: IEEE 802.3x & back-pressure

QoS Features

Description
L2 & L3 QoS
HQoS
Rate Limiting - 1/2/3 rate coloring, Policing, Marking
802.1p remarking
Classification based on interface, MAC address, Ethertype, 802.1p, VLAN
Trust IEEE 802.1p

Availability Features

Description
OSPF Graceful Restart
BGP Graceful Restart

MPLS/MPLS-TP Features

Description
MPLS Architecture
MPLS Label Stack Encoding
Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)
Multiprotocol Label Switching (MPLS) Forwarding Equivalence Class to Next Hop Label Forwarding Entry (FEC-To-NHLFE) Management Information Base (MIB)
Time to Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks
Label Distribution Protocol
LDP Applicability
Definitions of Managed Objects for Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
Support for LDP TCP-MD5
RSVP (support limited to RSVP-TE requirements)
Use of RSVP with IETF Integrated Services
RSVP Refresh Overhead Reduction Extensions
RSVP-TE: Extensions to RSVP for LSP Tunnels
Multi-Protocol Label Switching (MPLS) Support of Differentiated Services
Protocol Extensions for Support of Diff-Serv-aware MPLS Traffic Engineering
Fast Reroute Extensions to RSVP-TE for LSP Tunnels
RSVPv1 - Message Processing Rules
Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
RSVP-TE Scalability
Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels
Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)
Pseudowire Setup and Maintenance using the Label Distribution Protocol
Encapsulation Methods for Transport of Ethernet Over MPLS Networks
Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling
Virtual Private LAN Service (VPLS) Using BGP for signaling and auto-discovery
BGP MPLS IPv4 VPN
OAM for MPLS Networks
A Framework for MPLS OAM
BFD For MPLS LSPs
Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)
Pseudowire Virtual Circuit Connectivity Verification (VCCV)
MPLS TP frame work
MPLS Generic Associated Channel
Requirements of an MPLS Transport Profile

MPLS/MPLS-TP Features, continued

Description
Operations, Administration and Maintenance Framework for MPLS-based Transport Networks
MPLS On-demand Connectivity Verification and Route Tracing
Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile
MPLS-TP Identifiers
MPLS Fault Management Operations, Administration, and Maintenance (OAM)
MPLS Transport Profile Lock Instruct and Loopback Functions
MPLS Transport Profile (MPLS-TP) Linear Protection
MPLS TP identifiers following ITUT coneventions
MPLS TP OAM based on Y1731 (CCM, AIS, LCK, LM, 1DM, 2DM, LBM, LBR, TST)
MPS TP ITU-T based Linear Protection Switching
MPLS-TP Ring Protection Switching (MRPS)

Management Features

Description
Role based CLI management and access
CLI via console, telnet, SSH
SNMP v1/v2/v3
Traffic Mirroring(port/LAG/VLAN/Filter based)

Standards Supported

Standards Support
IEEE Standards
IEEE 802.1D
IEEE 802.1w
IEEE 802.1
IEEE 802.1Q
IEEE 802.1p
IEEE 802.1ad
IEEE 802.3ad
IEEE 802.1AB
IEEE 802.3x
IEEE 802.1Qbb
IEEE 802.1Qaz
IEEE 802.1Qau*
IEEE 802.1Qbg*

Supported RFCs
RFC 768 UDP
RFC 783 Trivial File Transfer Protocol (TFTP)
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet client and server
RFC 894 IP over Ethernet
RFC 1058 Routing Information Protocol
RFC 1112 IGMP v1
RFC 1142 OSI IS-IS Intra-domain Routing Protocol
RFC 1492 TACACS+
RFC 1519 Classless Interdomain Routing (CIDR)

Standards Supported, continued

Supported RFCs
RFC 1587 OSPF not-so-stubby area (NSSA) Option
RFC 1812 Requirements for IP Version 4 routers
RFC 1997 BGP Communities Attribute
RFC 2030 SNTP, Simple Network Time Protocol
RFC 2138 RADIUS Authentication
RFC 2139 RADIUS Accounting
RFC 2154 OSPF (Password, MD-5)
RFC 2236 IGMP v2
RFC 2267 Network ingress filtering
RFC 2328 OSPF v2 (edge mode)
RFC 2338 VRRP
RFC 2362 PIM-SM (edge mode)
RFC 2370 OSPF Opaque link-state advertisement (LSA) Option
RFC 2385 Protection of BGP Sessions via the TCP Message Digest 5 (MD5) Signature Option
RFC 2439 BGP Route Flap Damping
RFC 2453 RIP v2
RFC 2474 Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers
RFC 2597 Assured Forwarding PHB (per-hop behavior) Group
RFC 2598 An Expedited Forwarding PHB
RFC 2697 A Single Rate Three Color Marker
RFC 2698 A Two Rate Three Color Marker
RFC 2796 BGP Route Reflection—An Alternative to Full Mesh IBGP
RFC 2918 Route Refresh Capability for BGP-4
RFC 3065 Autonomous System Confederations for BGP
RFC 3376 IGMP v3 (source-specific multicast include mode only)
RFC 3392 Capabilities Advertisement with BGP-4
RFC 3569 SSM
RFC 3623 Graceful OSPF Restart
RFC 4271 Border Gateway Protocol 4 (BGP-4)
RFC 4360 BGP Extended Communities Attribute
RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
RFC 4486 Subcodes for BGP Cease Notification Message
RFC 4724 Graceful Restart Mechanism for BGP
RFC 4812 OSPF Restart Signaling
RFC 4893 BGP Support for Four-octet AS Number Space
RFC 5668 4-Octet AS Specific BGP Extended Community
RFC 5880 Bidirectional Forwarding Detection (BFD)
Configuration Protocol (DHCP) server

Standards Supported, continued

MIBS
RFC 1155 SMI
RFC 1157 SNMPv1
RFC 1212, RFC 1213, RFC 1215 MIB-II, Ethernet-Like MIB and TRAPs
RFC 1850 OSPFv2 MIB
RFC 1901 Introduction to Community-based SNMPv2
RFC 2011 SNMPv2 for Internet protocol using SMIv2
RFC 2012 SNMPv2 for transmission control protocol using SMIv2
RFC 2013 SNMPv2 for user datagram protocol using SMIv2
RFC 2233, The Interfaces Group MIB Using SMIv2
RFC 2287 System Application Packages MIB
RFC 2570 Introduction to Version 3 of the Internet-standard Network Management Framework
RFC 2578 SNMP Structure of Management Information MIB
RFC 2579 SNMP Textual Conventions for SMIv2
RFC 2580 Conformance Statements for SMIv2
RFC 2665 Ethernet-like interface MIB
RFC 2787 VRRP MIB
RFC 2790 Host Resources MIB
RFC 2819 RMON MIB
RFC 2863 Interface Group MIB
RFC 2932 IPv4 Multicast MIB
RFC 3410 Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3413 Simple Network Management Protocol (SNMP)—
RFC 3416 Version 2 of the Protocol Operations for the SNMP
RFC 3418 Management Information Base (MIB) for the SNMP
RFC 4188 Definitions of Managed Objects for Bridges
RFC 4318 Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4363b Q-Bridge VLAN MIB

Please contact us to learn more about OcNOS

Phone: +1 877-MYZEBOS
Email: sales@ipinfusion.com
Web: www.ipinfusion.com

U.S. (Santa Clara), +1 408-400-1912
Japan (Tokyo), +81 03-5259-3771
Korea (Seoul) +82 (2) 3153-5224

India (Bangalore), +91 (80) 6728 7000
China (Shanghai), +86 186 1658-6466
EMEA (Stockholm), +46 8-566 300 42

About IP Infusion

IP Infusion is a leading provider of intelligent network software for enhanced Ethernet and IP services. Tier one and two OEMs rely on IP Infusion's ZebOS software and global professional services to bring products to market faster, and to differentiate them from competitors with less cost. Products built on IP Infusion technology are deployed in networks with five-9s reliability across five continents—as well as a growing number of enterprises—to improve network performance, decrease network infrastructure costs, and grow revenue. IP Infusion is headquartered in Santa Clara, Calif., and is a wholly owned and independently operated subsidiary of ACCESS CO., LTD., of Tokyo, Japan.