Data Sheet

Pluribus Netvisor Network Operating System

Comprehensive Network Operating System Optimized to Meet the Stringent Requirements for Distributed Enterprise and Service Provider Data Centers with Best-in-Class Layer 2/3 Switching, Routing, VXLAN Overlay and Advanced Network Services

Highlights

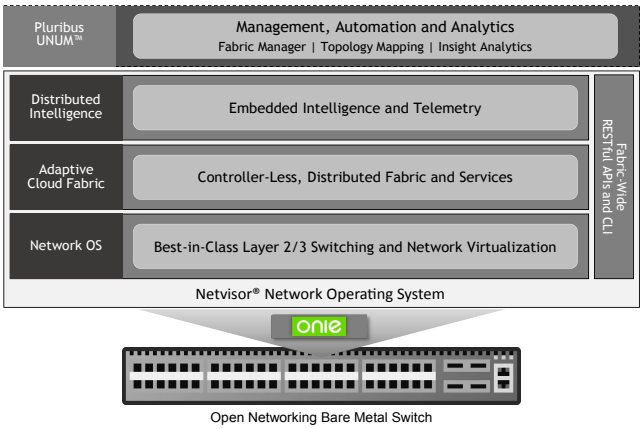
- Advanced Network Operating System that maximizes open networking switch performance
- Best-in-class layer 2 and layer 3 switching, routing and VXLAN overlay services
- Consistent Data Center OS supports Leaf and Spine placements
- Support for distributed campus aggregation and core deployments
- Simple, controller-less fabric architecture supports geographically distributed environments
- Fabric-wide API-driven, automation and policy management
- Secure traffic segmentation and strict multi-tenant services
- Integrated monitoring telemetry for pervasive network and application visibility
- Integration with VMware vCenter, NSX and vSAN

Product Overview

To empower the journey to the digital enterprise, the data center network needs to move from being static and hardware-bound, to a more dynamic, software-driven environment. Pluribus Networks has changed the way Software-Defined Networks (SDN) operate by radically simplifying the architectural, and operational model for the modern network.

The innovative Pluribus Netvisor® software is a data center-class Network Operating System (OS) that virtualizes open networking hardware to build a holistic, distributed network that is more intelligent, automated and resilient. Delivering exceptional operational flexibility, the Netvisor OS combines a best-in-class layer 2 and layer 3 networking foundation, the highly scalable distributed Adaptive Cloud Fabric™ architecture, and embedded network performance monitoring telemetry to empower the agile, and future-ready data center.

Netvisor OS delivers continuous availability for mission-critical environments and is optimized to meet the stringent requirements of enterprise and service provider data centers. The programmability of the Netvisor OS easily adapts to evolving standards and new technologies, and delivers comprehensive Ethernet features and advanced network services that maximize the performance of high-density, open networking switches.



The Netvisor Software-Defined Architecture

The Netvisor OS is standards-based, and eliminates the architectural complexities of SDN controllers, so it can seamlessly interoperate with existing networks, enabling the graceful migration to a software-defined data center architecture. The Netvisor OS simplifies data center operations by providing a single network OS to support all deployment points, such as the Leaf and Spine, for consistent operations with unmatched agility, and a significantly lower TCO.

Netvisor OS supports traditional CLI, RESTful APIs, and an OVSDB interface, enabling IT organizations to overcome IT skill gaps, and bridge the operational models of DevOps and NetOps. Tight integration with VMware vSphere® and NSX allows automated provisioning of network resources across the Adaptive Cloud Fabric architecture via VMware vCenter® to further streamline operations, and provide an ideal NSX underlay.

Runs on Open Networking Hardware

The Netvisor OS runs on many Open Compute Project (OCP), and Open Network Install Environment (ONIE) hardware compliant switches, including devices from Dell EMC, D-Link Systems, Edge-core, and the Pluribus Freedom™ series network switches. This flexibility allows organizations the choice of hardware to build scale-out networks with any combination of 10, 25, 40 or 100 Gigabit Ethernet interfaces. Consequently, an entire data center can be built with only a few physical switch models to improve operational consistency, lower costs, and simplify sparing.

Advanced Virtualized, Modular and Resilient Software Design

The Netvisor OS can be deployed as a single software image that supports all deployment points, including the Leaf, Spine and Campus aggregation, and can run on any mix of multiple vendor open networking switches.

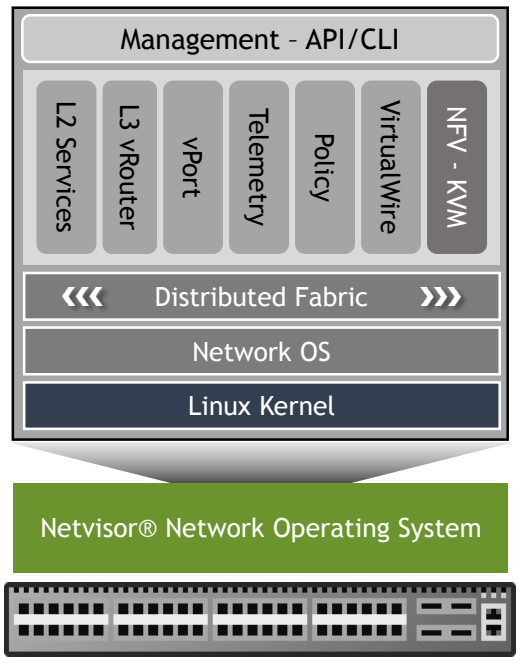
This enables constructing a multi-vendor network with a common OS that can flexibly support evolving physical interface and device requirements while maintaining a programmable, operationally consistent, and software-powered operating environment.

Modular, Resilient Software Design

The modular and containerized architecture of Netvisor OS allows new features, and patches to be quickly integrated into the software. The fully distributed control plane allows for a highly available L2/L3 underlay and VXLAN overlay infrastructure. In addition, switch clustering, vLAG (Netvisor Multi-chassis LAG), VRRP, ECMP, BFD, redundant VTEPs, and distributed Anycast gateway enable convergence and sub-second failover, for both the underlay and overlay network.

The Netvisor OS decouples network resources from the underlying hardware and segments the operating system and hardware resources into virtual network containers, similar to how a hypervisor virtualizes a bare metal server.

Consequently, virtualization of the network allows a single switch to instantiate multiple virtual networks that can be dynamically allocated to a single device, or span across an entire fabric to enable granular east/west and north/south network segmentation, strict multi-tenant services, and the integration of virtualized network services and functions into switching hardware.



Netvisor OS provides a modular, resilient software design with advanced layer 2 and layer 3 networking and services

Each virtual network container has its own software processes and dedicated network resources, including dedicated routing data and control planes, and an independent management environment. The virtualized network container is not hardware bound, so a virtualized network container can reside on any switch, or be duplicated on any switch, in any location across the fabric. Similar to how vMotion operates in VMware deployments, each virtualized network container is mobile, and can be moved on-demand and reallocated from one physical switch to another physical switch enabling unsurpassed operational agility.

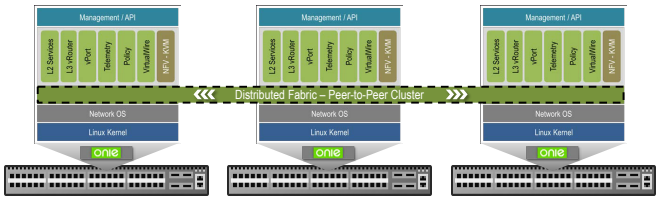
Control Plane Traffic Protection

Netvisor delivers exceptional high availability with its Control Plane Traffic Protection (CPTP) architecture. CPTP protects the CPU from excessive traffic volumes, and provides fine-grained control and QoS over different types of control plane classes using 64 independent queues. The auto-quarantine host-hog prevention mechanism identifies and automatically quarantines offending host traffic in hardware. The offending host activity is monitored and traffic is resumed automatically when the offending flow ceases.

Adaptive Cloud Fabric Architecture

Powered by the Netvisor OS, the Adaptive Cloud Fabric is a simple, dynamic and secure architecture for building a holistic distributed network that brings the elasticity benefits of cloud-scale and adaptability to the modern data center. The Adaptive Cloud Fabric operates without a controller, and delivers a more dynamic network that supports a wide-range of deployment scenarios and easily adapts to change to streamline operations, improve efficiency and lower costs. The Adaptive Cloud Fabric can be deployed across a single data center, targeted to specific racks, application server farms or used to stretch Hyper-Converged Infrastructure (HCI) deployments.

The Adaptive Cloud Fabric is a peer-to-peer distributed architecture that clusters all member switches into a symmetrical, unified operating domain. The fabric uses an innovative distributed control plane that runs on top of any standard underlay network, allowing multiple fixed form factor switches to be managed as a single, virtualized large chassis switch. However, unlike a traditional chassis architecture, each member switch maintains its own individual control and data plane providing greater scale, with no single-point-of failure, resulting in higher levels of resiliency than a chassis can provide. Fabric automation distributes intelligence, integrates a broad range of advanced network services, and provides pervasive visibility for all traffic traversing the fabric. The dynamic, scale-out architecture delivers multi-terabit capacity with predictable performance and latency, and supports millions of concurrent connections.



The Adaptive Cloud Fabric architecture clusters member switches into a symmetrical, unified operating domain

Manageability, Programmability, and Automation

The Netvisor OS and Adaptive Cloud Fabric are built for complete programmability and agility enabling operational changes and new services to be rolled-out quickly. Any fabric member can act as the logical management point to define and provision fabric-wide policy and services across all fabric member switches with a single command via RESTful APIs, or Command Line Interface (CLI) with functional parity.

Automation tools, such as Ansible, or the Pluribus UNUM™ management platform are also available to provision an entire Leaf and Spine fabric. In addition, the Netvisor OS supports a wide array of Linux tools for scripting and automation, and supports traditional NetOps interfaces for SNMP, Syslog, sFlow and IPFIX. As a result, Netvisor OS workflow automation reduces configuration time by up to 90% over traditional box-by-box management, lowers the risk of configuration errors, and dramatically improves service velocity and operational agility.

All switch-to-switch communications, network-wide configuration, policies and state information are dynamically updated across the fabric. An advanced transactional model guarantees that device configuration is consistently maintained across every member network node. To minimize configuration errors, the Netvisor OS offers dynamic configuration roll-back capabilities that allows the network operator to instantaneously restore a previous configuration across the entire fabric to prevent unwanted disruptions.

Role-Based, Secure Management Access

The Netvisor OS has extensive security mechanisms to protect access to device and fabric automation through Authentication, Authorization, and Accounting (AAA) access controls. Administrative user authentication is supported through standards-based AAA mechanisms including TACACS+, Secure Shell (SSH) Version 2, and TLS 1.2. Granular permissions can be defined on a per-user, per-role, and per-tenant basis, limiting command-level access for all commands performed for all configuration levels.

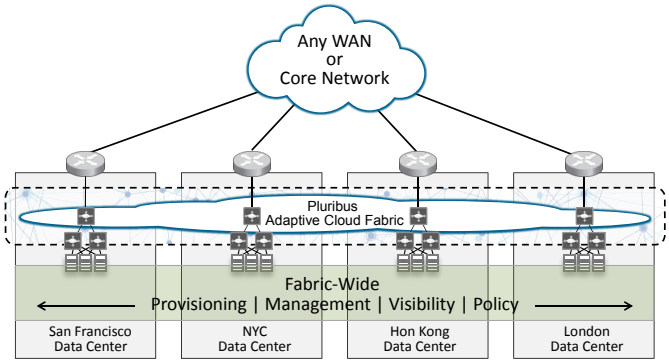
All CLI, SSH Shell and vtysh level commands, even invalid commands, are individually validated and logged. Detailed reports are available on a per-user basis providing a complete audit trail that documents all system administration activity. To assure system access during an AAA server outage, when the AAA server is reachable all local accounts are disabled, but if the AAA server is unreachable, local accounts can be enabled or disabled.

Multi-Vendor Interoperability

Because the Netvisor OS does not require a centralized controller or use proprietary protocols, the Adaptive Cloud Fabric can be seamlessly inserted into existing networks and fully interoperate with any standards-based networking equipment, protocols, or network topology. Consequently, Netvisor powered switches can be inserted into the Leaf or Spine layers with no Leaf/Spine lock-in, enabling graceful migrations to next generation architectures while preserving existing technology investments.

Distributed Architecture Enables Data Center Interconnect

The Adaptive Cloud Fabric can seamlessly interconnect dozens of geographically distributed data centers over any existing Layer 2 or Layer 3 core, underlay, WAN or dark fiber network without requiring reengineering or proprietary protocols. The Pluribus Networks Data Center Interconnect (DCI) solution leverages a sophisticated VXLAN-based Layer 2 extension and Virtual Link Extension (vLE) technologies to achieve transparent inter-site communication with dynamic end-point tracking over existing networks. The stretched fabric provides a single-point-of-management and delivers fabric-wide resiliency with sub-second failover for any failure scenario, to support mission-critical environments requiring stringent loss-less high availability.



The Adaptive Cloud Fabric can seamlessly interconnect distributed data centers over any existing WAN or Network

Distributed Fabric-Wide Intelligence

Netvisor Virtual Port (vPort) technology distributes intelligence and control to all connected end-points, VMs, containers and mobile devices across the global fabric. Each vPort is associated with an end-point MAC address and is auto-learned by all fabric member switches. The dynamic vPort database provides a persistent, distributed end-point directory and activity history for the entire fabric, and is the cornerstone of the intelligent forwarding and security capabilities of the Adaptive Cloud Fabric.

The vPort tracks the location, identity, policy and history for each end-point, and dynamically shares state status to all fabric member devices in real-time, eliminating network broadcasts. This assures that movements are legitimate, and replaces less-than-optimal "flood and learn" approaches with more efficient conversational forwarding. When mobile end-points or VMs move from one port to another, even across data centers, end-point re-registration updates automatically in the vPort database in near real-time.

VMware Integration Extends Automation

Netvisor OS integrates with VMware vCenter enabling one-touch provisioning of network, compute, and storage services from a single management interface. Leveraging the familiar vCenter console, a virtualization administrator can orchestrate and provision network resources in conjunction with ESXi hosts, and VMs. vSAN services are also automated, including implementing vSAN cluster configurations across the network fabric without the manual configuration of multicast.

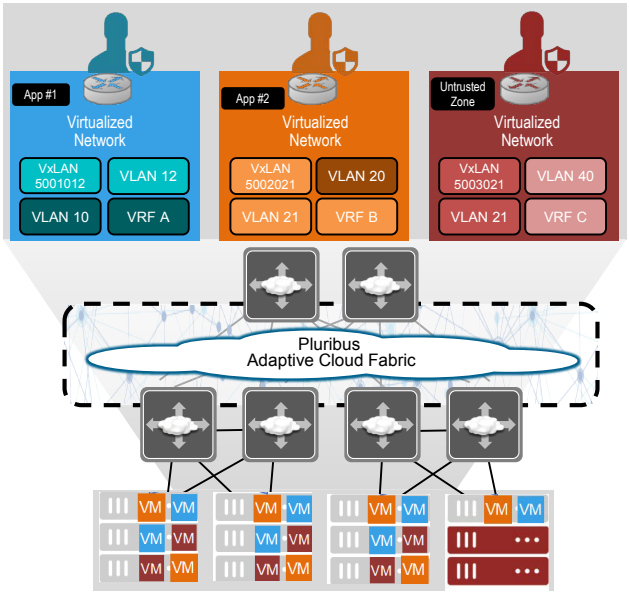
In addition, the Netvisor OS integrates with the VMware NSX Controller to automate the off-load of L2 VTEP Gateways directly on the switch, thus extending the reach of NSX virtual networks to bare metal network services and applications. This increases flexibility, simplifies deployments, and reduces human touch points, speeding time-to-deployment, and further minimizing the risk of configuration errors.

Secure Segmentation and Multi-Tenancy

The Netvisor OS enables the creation of independent, virtual networks, called vNETs. Different than a traditional VLAN, vNETs are virtualized network containers with separate resource management spaces and policies that are completely isolated from each other.

vNETs are designed to meet virtually any security requirement, and are ideal for north/south and east/west traffic segmentation or strict multi-tenant services. Each vNET functions like a separate physical switch, with its own control, data and management plane, and can be located on a single switch, or replicated on multiple physical switches located anywhere across the fabric.

There is no limit to the number vNETs that can be created, and because vNETs are not VLANs, network administrators can make use of all 4,000 VLAN IDs per tenant.



The Netvisor OS enables the creation of independent, virtualized network containers

Since the Adaptive Cloud Fabric operates as one unified entity, vNET segments can be distributed across a global fabric, enabling strict segmentation across a virtualized multi-site overlay. Network virtualization ensures that each segment or tenant maintains complete isolation from other segments or tenants, and the public underlay across a distributed fabric. In addition, each tenant is managed independently so each vNET can limit access to only a subset of the Netvisor OS resources or policies relating to members of a specific vNET.

Integrated Monitoring Telemetry

The Netvisor OS provides embedded monitoring telemetry across every switch port to enable pervasive visibility of application and service flows without dedicated network probes. The telemetry monitors every TCP connection, including traffic within a VXLAN tunnel, across the entire fabric at the speed of the network measuring east/west and north/south traffic flows, and virtualized workloads to expose important network and application performance characteristics.

This actionable insight provides a real-time view into end-to-end latency, duration, total bytes transferred, and the state of TCP connections, to track the dynamic behavior of network traffic. Performance metrics can be viewed via CLI, API or through the Pluribus Insight Analytics™ platform to quickly pinpoint performance issues, accelerate troubleshooting, improve operational intelligence, identify security risks and speed remediation activities.

Network Intelligence Powers Intent-Based Networking

The integrated telemetry and distributed intelligence of the Netvisor OS tracks network and end-point service state across the Adaptive Cloud Fabric to understand how the users and services are consuming the infrastructure, and conversely how the infrastructure is supporting the users and services. Continued system enhancements will advance the depth of state-based intelligence across the fabric to dynamically compare actual versus desired state and automate corrective actions such as security or traffic policy changes, reroute traffic, and link to other systems to implement dynamic changes to the infrastructure, redefining real-time service assurance.

Netvisor OS Licensing

Pluribus Netvisor software is licensed on a per switch basis, and is available as a perpetual or subscription license. Several license-based feature options are available to meet different deployment requirements.

Netvisor OS Licensing Options

- **Netvisor Enterprise** (ONVL) — includes Layer 2 and Layer 3 switching and routing functionality with all standard networking protocols and high availability features
- **Netvisor Fabric** (ONVL) — adds VXLAN, Telemetry, Adaptive Cloud Fabric, Data Center Interconnect and security and segmentation capabilities

Optional Licensed Capabilities

- **vNET License** — supports multi-tenant and network/traffic segmentation requirements. Licensed one per fabric based upon the number of segments needed. vNET capabilities requires at least one switch capable of supporting vNET Manager be a member of the Adaptive Cloud Fabric architecture or the deployment of Virtual Netvisor (vNV) on a virtual server.
- **VirtualWire™** feature license — adds Layer 1 matrix and L2-4 network packet broker functionality that can co-exist with standard network interfaces. Licensed per switch.

Warranty and Support

Pluribus Networks offers a wide range of advanced services spanning the entire network lifecycle to protect investments and help accelerate success when deploying and optimizing the Netvisor operating system and next generation network architectures. Multiple extended support options are available, including 24x7 on-demand global support, on-site support, advanced hardware replacements, and professional implementation services. Maintenance options includes direct access to a team of expert network engineers with deep networking experience, and our self-service, on-line Customer Portal. For more information about Pluribus support options, visit http://www.pluribusnetworks.com/support or contact a Pluribus Networks authorized reseller.

Netvisor OS Features and Specifications

Pluribus Netvisor Operating System (ONVL) version 2.6.1.

Functionality varies based upon underlying open networking hardware capabilities

Layer 2

Enterprise Edition

- 802.3z Gigabit Ethernet
- 802.3ab 1000BASE-T
- 802.3ae 10 Gigabit Ethernet
- 802.3ba 40 Gigabit Ethernet
- 802.3ba 100 Gigabit Ethernet
- 802.1D Spanning Tree
- 802.1w Per VLAN Rapid Spanning Tree Protocol (RPVSTP) and RSTP PortFast
- 802.1s Multiple Spanning Tree Protocol (MSTP)
- 802.3ad Link Aggregation (LACP)
- Link Aggregation Group (LAG)
- Multi-Chassis LAG (vLAG)
- STP Cluster Awareness
- Port Fast, BPDU Guard, BPDU Filter, Root Guard
- 802.1q VLANs, VLAN Trunks
- 802.1ab Link Layer Discovery Protocol (LLDP)
- Storm control for Multicast and Broadcast
- 802.1/Qbb — Priority-based Flow Control
- IGMP v2/v3 snooping
- MLD snooping v1/v2
- Jumbo frames (9216 Bytes)
- Private VLAN Edge (for Cisco Interop)

Fabric Edition adds

- Automatic Port channeling
- Fabric ARP Optimization
- Fabric Guard

Layer 3

Enterprise Edition

- Routing Protocols: OSPFv2, BGPv4, and RIP
- Equal-cost multi-path routing (ECMP)
- Policy Based Routing (PBR)
- VRRP with active-active forwarding
- Bidirectional Forwarding Detection (BFD) for RIP static routes, OSPF and BGP (IPv4 and IPv6)
- Static routes
- Loopback interface
- DHCP relay
- PIM-SM / PIM-SSM (release 2.7)
- Route Maps

Fabric Edition adds

- Multiple virtual routers per switch (supported on selected switches)
- Distributed Anycast Gateway (release 2.7)
- Distributed subnets (release 2.7)
- Distributed VRF (release 2.7)

Fabric and Network Virtualization

(requires Fabric Edition license)

- Single VTEP for high availability cluster
- VXLAN VTEP with high availability
- Dynamic VXLAN tunnel creation
- VXLAN routing
- VXLAN bridging
- VXLAN egress load balancing
- ARP optimization
- Virtual Link Extension (VLE or transparent point-to-point Ethernet links over VXLAN)
- Link state tracking across the fabric for VLE
- vNET Manager on capable hardware platforms (requires vNET license)
- vNET Manager (vNV) as a VM on ESXi host (requires vNET license)
- vNET Manager high availability (requires vNET license)

Security

(Enterprise and Fabric Edition)

- IPv4 Ingress/Egress ACL (vFlow)
- IPv6 Ingress/Egress ACL (vFlow)
- ACL logging, counters
- Distributed ACL (Fabric Edition)
- Advanced Control Plane Policing (64 per protocol queues)
- Control plane DDOS detection and auto-quarantine of offending hosts
- DHCP Snooping
- AAA authorization and accounting of all commands
- Full AAA switch control (shell, vtysh, CLI)
- Password protected management access, with role-based controls
- TACACS+ AAA
- BGPv4 MD5
- MAC Security
- SNMPv3 SHA (Authentication)

QoS and Policy

(Enterprise and Fabric Edition)

- 802.1p Class of Service (CoS)
- Differentiated Services Code Point (DSCP)
- DSCP to CoS mapping
- CoS to DSCP mapping
- Strict priority queueing
- QoS interface trust (COS/DSCP)
- Egress per port rate limiting
- Per-port, per-CoS minimum egress bandwidth guarantee
- Per-port, per-CoS maximum egress bandwidth limit
- Weighted Round Robin (WRR) Scheduling
- ACL (vFlow) policing/rate limiting
- Priority-based Flow Control (PFC)

Monitoring and Visibility

Enterprise Edition

- Port Mirroring
- RSPAN
- ERSPAN
- RFC 3176 sFlow
- Traceroute

Fabric Edition adds

- Fabric-wide embedded network and application traffic telemetry
- nvFlow for TCP connection visibility
- nvFlow for VXLAN
- nvFlow for Virtual Link Extension (VLE)
- Flowtrace (trace synthetic flows across the fabric)
- IPFIX export for nvFlow
- Integrated packet capture/analysis with TCPDump (supported on selected switches)

VirtualWire Feature Set

(requires VirtualWire feature license)

- One:Many TAP/mirror aggregation
- Many:Many TAP/mirror aggregation
- Many:One TAP/mirror aggregation
- Bypass switch for inline tool deployment
- Bypass switch heartbeat packet to detect inline tool failure
- Layer 2/3/4 traffic filtering
- Layer 1 cut-through mode
- Error pass-through

Management, Automation and Extensibility

Enterprise Edition

- CLI
- RESTful API (with CLI parity)
- Pluribus UNUM for one-touch management and automation (see Pluribus UNUM datasheet)
- Ansible automation
- Zero-Touch Replacement for nodes in an HA cluster
- Syslog
- SNMP v1, v2, v3
- SHA for SNMP authentication
- SSHv2
- TLS 1.2
- IPv6 for management
- Configuration roll-back and roll-forward
- Native KVM support (supported on selected switches)

Fabric Edition Adds

- Open vSwitch Database Management Protocol (OVSDB)
- Fabric control plane over in-band or out-of-band management network
- Geographically distributed fabric over Layer 3 networks
- Management of switch groups within a fabric

Netvisor OS Features and Specifications (continued)

VMware Integration with vCenter, vSAN and NSX

(requires Fabric Edition license)

- VMware vSphere support with vSphere object discovery and association with vPorts (VM, Port Groups, vSwitches, VMKernel)
- ESXi host facing port VLAN configuration with vCenter
- Uplink and cluster port VLAN configuration with vCenter
- Auto-vLAG configuration with vCenter
- VLAN Creation/Pruning across the fabric with vCenter
- Multicast automatic configuration for VSAN support (release 2.7)
- NSX integration for L2 VTEP Gateway

Supported RFCs

(Enterprise and Fabric Edition)

- RFC 7C8:D26 User Datagram Protocol (UDP)
- RFC 791 IP
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 Telnet
- RFC 959 FTP
- RFC 1305 Network Time Protocol (NTP) Version 3
- RFC 1519 Classless Interdomain Routing (CIDR)
- RFC 1591 Domain Name System (DNS) Client
- RFC 1724 RIPv2 MIB Extension
- RFC 1812 IPv4 Routers
- RFC 2236 Internet Group Management Protocol
- RFC 2328 OSPF Version 2
- RFC 2453 RIP Version 2
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2519 A Framework for Inter-Domain Route Aggregation
- RFC 3101 OSPF Not-So-Stubby-Area (NSSA) Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3376 Internet Group Management Protocol
- RFC 3509 Alternative Implementations of OSPF Area Border Routers
- RFC 4271 BGPv4
- RFC 4443 Internet Control Message Protocol (ICMPv6) for IPv6 specification
- RFC 4456 BGP Route Reflection
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4861 Neighbor Discovery for IP Version 6 (IPv6)
- RFC 4893 BGP Support for Four-Octet AS Number Space
- RFC 7011 IP Flow Information Export (IPFIX)

SNMP MIBs

(Enterprise and Fabric Edition)

- RFC 3635 EtherLike-MIB
- RFC 3418 SNMPv2-MIB
- RFC 2863 IF-MIB
- RFC 2096 IP-FORWARD-MIB
- RFC 4363 Q-BRIDGE-MIB
- RFC 4188 BRIDGE-MIB
- RFC 4273 BGP4-MIB
- RFC 4750 OSPF-MIB
- RFC 2787 VRRPv2MIB

Ordering Information

Software only, requires compatible switch hardware. License does not include maintenance, order desired maintenance separately.

Enterprise Edition Perpetual License (licensed per switch device)

- ONVL-10G-ENT-LIC — Pluribus Open Netvisor Linux Enterprise Edition for 10 GbE switches
- ONVL-40G-ENT-LIC — Pluribus Open Netvisor Linux Enterprise Edition for 40 GbE switches
- ONVL-100G-ENT-LIC — Pluribus Open Netvisor Linux Enterprise Edition for 100 GbE switches

Fabric Edition Perpetual License (licensed per switch device includes all enterprise edition functionality)

- ONVL-10G-PLEX-LIC — Pluribus Open Netvisor Linux Fabric Edition for 10 GbE switches
- ONVL-40G-PLEX-LIC — Pluribus Open Netvisor Linux Fabric Edition for 40 GbE switches
- ONVL-100G-PLEX-LIC - Pluribus Open Netvisor Linux Fabric Edition for 100 GbE switches

vNET Segmentation License (licensed per fabric)

- VNV-4-VNET — vNET license for network segmentation and multi-tenant operation

VirtualWire License Add-on (licensed per device)

VirtualWire feature set adds network packet broker and LAB automation capabilities. Licensed on a per switch bases and may be licensed with or without fabric and vNET licenses.

- ONVL-10G-VW-LIC - VirtualWire service license for 10G switch
- ONVL-40G-VW-LIC - VirtualWire service license for 40G switch
- ONVL-100G-VW-LIC - VirtualWire service license for 100G switch

Copyright © 2017 Pluribus Networks, Inc. All Rights Reserved. Netvisor is a registered trademark, and The Pluribus Networks logo, Pluribus Networks, Freedom, Adaptive Cloud Fabric, and VirtualWire are trademarks of Pluribus Networks, Inc. All other brands and product names are registered and unregistered trademarks of their respective owners. Pluribus Networks reserve the right to make changes to its technical information and specifications at any time, without notice. This informational document may describe features that may not be currently available or may be part of a future release, or may require separate licensed software to function as described. This document describes functionality that is dependent on the underlying open networking hardware device. Functionality will vary by physical device, and not all capabilities described herein will work on every device. Netvisor version 2.6.1 —October, 2017

Pluribus NETWORKS

Pluribus Networks, Inc.
2455 Faber Place, Suite 100
Palo Alto, CA 94303

1-855-438-8638
+1 650-289-4717
www.pluribusnetworks.com