Highlights

- Designed for small sites, delivering full-featured network virtualization capabilities in a range of low-cost 1/10 Gigabit Ethernet platforms
- Deliver multiple services without managing multiple complex protocols, with the compact Edge device in your network
- Leverage network virtualization technology easily for small offices – and separate traffic to help meet regulatory or security requirements
- Provide rich multi-service functionality in multi-tenant environments – and help separate and protect each tenant's traffic
- Supports both conventional Routed IP and/or Fabric- based networking deployments

Virtual Services Platform 4000

Simplify your network end-to-end with the Fabric-enabled multiservice edge device

Simplify your network with the Extreme Virtual Services Platform (VSP) 4000. Designed to extend the reach of Extreme Fabric Connect technology to the branch and network edge, the VSP 4000 delivers fully featured network virtualization capabilities in a low-cost 1/10 Gigabit platform optimized for small locations. Offering full multiservice capabilities without deployment of multiple protocols, the VSP 4000 offers a simplified, streamlined way to build and manage networks.

For deployments in small offices where it is desirable to extend fabric technology across the wide area, the metro, or the campus edge or where you need separation of traffic for regulatory/security reasons or to support multiple entities, the VSP 4000 delivers rich multiservice and multi-tenant functionality in a cost-effective platform for small locations.

A New Way of Building Networks

Reflecting the complexity of most networks, a recent Extreme survey of IT managers found that 41% of all respondents need one month or more to implement a simple network change. This is not surprising when even moves, adds and changes, for example, often require cumbersome network-wide configuration that makes them difficult to implement. Fixing one thing can mean breaking something else when rigid design rules and a myriad of protocols are involved. What's needed is more speed, agility, and flexibility in configuring networks – especially when incorporating megatrends such as video, mobility, Cloud Computing, Big Data, and the rapid advancement of applications and end devices.

Switch Cluster: Improving Resiliency, Enhancing Availability

Extreme pioneered, more than a decade ago, the concept of the high-availability network with development of the Switch Cluster technology. Creating a single, unified, logical Core from two physically independent Switches – clustering them – ensures that no one single point-of-failure

can disrupt dual/multi-homed connectivity. This is the very essence of end-to-end always-on availability. Deploying Switch Cluster technology in the Core delivers high-availability for the Edge of the network, supporting the Campus Wiring Closet, Servers, Routers, or other networking devices in the Core/Data Center.

The Switch Cluster technology is built using the Split Multi-Link Trunking protocol that is unique to our products, yet is fully interoperable with third party Switches, Servers, Appliances, and Routers. This delivers a series of benefits that provide real value; while it may be possible to simulate certain individual elements, no competitive offering can rival the combined capabilities, particularly in terms of simplicity and efficiency.

Switch Cluster delivers an interoperable solution that extends beyond simply Switches. This means that high-availability is not limited to only the switching network (the Switches themselves and their direct links), but to the total network; importantly also extended to attached Servers, Appliances, and WAN Routers, etc. Competing offers are based on interactions purely within the Switch domain, and crucially do not extend to the application hosts themselves. Most rival offerings are based on variations of the Spanning Tree Protocol (STP); however, support for this is limited to Switches alone and is not commonly supported by other devices. By excluding Servers from the active resiliency technology, these solutions cannot extend high-availability to the applications. The Switch Cluster technology is independent of STP and extends to support any device that utilizes Link Aggregation, a technology that is both basic and ubiquitous. Devices that attach to the Switch Cluster create a virtual connection using multiple physical links, this provides resiliency together with additional capacity.

Delivering availability and facilitating in-service maintenance and optimized performance are well-known features of Switch Cluster technology. Enabling sub-second failover and recovery remains extremely important, perhaps never more important, however it is not necessarily a feature that remains unique. Enhancements to STP – namely rapid reconfiguration – can be aggressively configured to deliver similar levels of failover performance.

However, all flavors of STP remain tied to the concept of detecting and acting upon changes to the network topology. This makes a network extremely sensitive to the reliability and availability of particular devices (Root Bridges, etc.). Extreme's Switch Cluster technology is built around the concept of mirrored devices and virtualized capabilities.

Switch Cluster technology is so effective that the loss of an entire Switch – for planned maintenance or through failure – can be accommodated without any loss of overall application availability.

Traditional Networks	Fabric Connect
Complex: • Multiple protocols (STP, RIP, OSPF, BGP, PIM) • Network design rules • Cumbersome adds moves and changes • Network wide configuration (STP groups, VLANs, hop by hop)	• Simple: • Single protocol (IS-IS) Design flexibility (Independent from physical topology, services can be added wherever needed) • Quick adds, moves and changes • Single-command end point provisioning for new services and changes to services
Inefficient use of resources (blocked ports)	Efficient use of resources (no blocked ports, optimized shortest latent path from source to destination)
Slow recovery (generally seconds)	Sub second recovery

Switch Cluster technology can be implemented in the classic – physically connected – manner, but in an evolution of the technology, also with a 'Virtual IST'. This is an enhancement of the Inter-Switch Trunk functionality; it leverages a virtualized connection between the Cluster members, rather than via the traditional physical link. This delivers greater flexibility, optimizes utilization of high-value backbone connections, and forms the basis of further developments that will include scalability of a Cluster beyond two members, and the ability to mix-and-match device types within a Cluster.

Virtual IST (vIST) delivers a dependable scalability capability and de-risks purchasing decisions; the Core can provide both always-on high-availability and flexible pay-as-you-grow efficiencies.

Extreme's Switch Cluster technology delivers a level of network resiliency that also facilitates in-service maintenance. The deterministic nature of Switch Cluster empowers network operators to compartmentalize the network, making essential services even more resilient, and allowing for individual failures to be repaired in real-time, without service restoration work impacting on collateral components or applications.

Fabric Connect: Replacing Complexity with Capability

Traditionally, to provision new services or to change existing ones, engineers are required to touch every device in the service path, configuring every device to enable both the active and redundant links. The bigger the network the more complex and risky this becomes.

The Extreme Fabric Connect technology is based on an extended implementation of the Shortest Path Bridging (SPB) standards of IEEE 802.1aq and IETF RFC 6329, augmented with Extreme Networks enhancements that deliver Enterprise-specific optimization. It offers the ability to create a simplified network that can dynamically virtualize elements to empower efficient provisioning and utilization of resources. This can reduce the strain on the network and IT personnel.

Leveraging Fabric Connect technology to virtualize the network enables a profound change. Rather than the network appearing as a mass of individual devices, it becomes an opaque cloud, so that engineers only need to touch the single unique device that is providing service directly to the end-point. Fabric Connect technology automatically and instantly propagates all service attributes to every other node within the cloud, delivering end-to-end connectivity.

Creating a fault-tolerant, powerful, and self-aware end-to-end Fabric, this technology creates a solution where service provisioning occurs only at the perimeter. The advantage is immediate and pronounced; administrative effort is reduced, errors can be avoided, and time-to-service is vastly enhanced. The beauty of the underlying technology is that it masks devices, links, and protocols and delivers what is logically an extended Ethernet LAN that provides connectivity for multiple end-points. That's the simple concept, and it is achieved in an interesting and quite unique way. Fabric Connect leverages a dynamic link-state routing protocol called Intermediate System-to-Intermediate System (IS-IS) and uses standardized extensions to share topology, reachability, and device information between every node in the domain. With nodes holding their own self-determined view of the network, including the optimal path to any destination, a fully distributed and dynamically maintained solution is created Fabric Connect technology has the added advantage of separating and segmenting traffic to unique service constructs.

This delivers 'stealth networking' solutions that help with compliance for business processes such as those that require special handling for credit card payments (PCI) or the protection of healthcare data (HIPAA).

Traffic Separation: Traditional Networks	Traffic Separation: Fabric Connect

MPLS-Based Separation
• Complex:
  • Multiple protocols (IGPs, BGP, MPLS)
  • Complex to configure (VRFs, IGP, iBGP, MPBGP, route targets, route distinguishers)
  • Complex to move, add and change tenants
• Slow recovery (generally in seconds)
VLAN-Based Separation
• No true traffic isolation
• Vulnerable to security breaches (VLAN jumping)
	Extreme Fabric Connect
	• Simple:
	  • Single protocol (IS-IS)
	  • Easy to configure (VRF to ISID)
	  • Easy to move, add and change tenants
	• Fast recovery (sub second)
	• True traffic isolation; meet regulatory requirements
	• More Secure (MAC-in-MAC) encapsulation helpsprevents VLAN jumping)

Network segmentation means that each service is uniquely encapsulated and carried independently of every other service. Leveraging a single unified protocol, with integrated IP Routing and IP Multicast capabilities, enables Fabric Connect to deliver the Industry's premier solution for simplified, scalable, and resilient IP Multicast-based applications. The Edge-only provisioning model also delivers significant advances in how the network interacts with virtual machine mobility. Layer 2 VLANs can be easily and seamlessly extended throughout the Core or Data Center whether that is a single site or multi-site. Traffic flows are automatically load-balanced and more protected across all available links.

Fabric Connect devices support a number of different User-Network-Interface (UNI) types to provide agile deployment capabilities:

- VLAN UNI (C-VLAN) – a node-specific VLAN ID maps to a L2 Virtual Service Network (VSN). All physical ports on that node associated with this VLAN are therefore associated with the service.
- Flex UNI has the following sub-types:
  - Switched UNI – a combination of VLAN ID and a Port maps to a L2 VSN. With this UNI type, VLAN IDs can be re-used on other ports and therefore mapped to different VSNs.
  - Transparent Port UNI – a physical port maps to a L2 VSN. All traffic through that port, 802.1Q tagged or untagged, ingress and egress is mapped to the VSN.

- E-Tree UNI – Private VLANs extend beyond one node to form a network-wide E-Tree service infrastructure. An E-Tree UNI is a L2 VSN where broadcast traffic flows from Hub sites to Spokes sites, from Spokes to Hubs, but not between Spoke sites. E-Tree Hubs can be formed with any VLAN UNI, while E-Tree Spokes must be configured as Private VLAN UNIs.
- L3 VSN UNI – a node-specific VRF maps to an L3 VSN, and the control plane exchanges the L3 routes with all nodes belonging to the same VSN. All VRFs in a network sharing the same L3 VSN, effectively forming an L3 VPN. L3 VSNs can be configured to simultaneously support both IP Unicast and IP Multicast.

Transitioning to an autonomic virtualized network delivers crucial advantages. It means that businesses no longer need to configure the Core of the network for every service change; service is only configured at the Edge of the network. This has dramatic impacts for the entire change paradigm.

Fabric Connect has garnered a well-earned reputation for simplifying how networks are built and improving how they are run. Independent research commissioned by Extreme reports that Fabric Connect deployments feature up to 91% less implementation time, up to 66% change less wait time,

and an 85% reduction in both configuration and troubleshooting times. Similarly, Fabric Connect delivers enhanced resiliency, with failover times more than 2,500x better, and outages caused by human error virtually eliminated.

Fabric Attach: The Missing Link for Service Automation

Service automation is the Holy Grail for IT. Creating solutions that enable business systems and processes to spin-up, move, or be decommissioned in real-time transitions IT from roadblock to facilitator. Extreme has developed technology to address automation of the critical “last yard”, where end- points devices meet the virtualized network.

The Extreme Fabric Connect technology delivers a number of key networking benefits. The independent Fabric Connect Customer Experience Research that Extreme commissioned demonstrates dramatic improvements in areas: implementation, configuration, and troubleshooting times, recovery, and error-induced outages are all improved.

Fabric Connect is able to deliver these benefits by leveraging the power on the underlying Shortest Path Bridging protocol.

This, amongst other characteristics, enables services to be defined only at the network edge, mitigating the traditional requirement for link-by-link, device-by-device configuration change. It is this legacy requirement that typically slows service deployment and introduces undesirable risk.

However, a challenge remains. That of delivering an automated attachment capability to an increasing large and diverse base of users and end-point devices, in what is a highly virtualized networking scenario. Any solution must be flexible, open, and complement the desire – in some cases, the mandatory requirement – to maximize the isolation of different traffic flows and minimize the unnecessary exposure of sensitive or mission-critical networks.

IP Multicast: Traditional IP	IP Multicast: Fabric Connect
Complex: • Multiple protocols (PIM over OSPF) • Complex to operate and troubleshoot (proprietary tools) • Network wide configuration (boot strap routers, rendezvous points)	Simple: • Single protocol (IS-IS) • Easy to operate and troubleshoot (IEEE 802.1 ag extensions) • Single command end point configuration
Recovery from failures seconds even minutes	Fast recovery (sub second)
Limited scale (100’s of streams)	Massive scaling (10’s of thousands of streams)

It is important, at this point, to be more specific about the challenge. The concept of implementing at least some level of automated attachment is not new. Vendors have independently developed MAC- and RADIUS-based solutions, and the industry has collaborated on open solutions such as the 802.1X Extensible Authentication Protocol. More recently, the 802.1AB Link Layer Discovery Protocol with media extensions assists with the deployment of VoIP/unified communication applications.

However, those approaches rely on the increasingly flawed assumption that the network edge has already been provisioned with access to all network segments (typically implemented as virtual LANs, VLANs). This may have made perfect sense when the network was essentially just a single “data” network, and when a single “voice” network was later added.

In response to this challenge, Extreme has developed Fabric Attach, a standards-based capability that facilitates the automatic attachment ("Auto-Attach" in standards verbiage) of end-point devices. Businesses can leverage Fabric Attach to dynamically deploy end-points, temporarily extending unique networking services to the edge as required. Auto-attached end-point devices connect to the appropriate network resources: this would typically be a Fabric Connect Virtual Service Network (VSN), or it could be a conventional VLAN. The Fabric Attach capability delivers the "Enabled Edge", a foundational tenet of the Extreme Fabric-based architecture.

Fabric Attach is designed to streamline the deployment of generic IT end-point devices, networking devices, compute resources, and business-centric Internet of Things (IoT) end-point devices. In its simplest form, Fabric Attach facilitates the assignment of these devices to the correct network segment, where necessary extending segment presence to the edge node only for the duration of active, valid sessions. Fabric Attach can also deliver enhanced service differentiation through the implementation of granular business-driven policy.

Fabric Attach works by creating a "gateway" automation function between conventional end-point devices and the network. Typically, the network will be a Fabric Connect private cloud, although the standardized nature of Fabric Attach means that it is equally relevant to conventional 802.1Q VLAN-based networks. The 802.1AB Link Layer Discovery Protocol is utilized to pass signalling between Fabric Attach components, meaning that it is highly flexible, extensible, and portable. Fabric Attach has been submitted to the IETF for consideration as a standard and in collaboration with Wind River, Extreme has contributed Fabric Attach to the Open vSwitch open source development project .

The focus for facilitating auto-attach is at the network edge, where end-point devices first connect and are most visible. This where a Fabric Attach Client (FA Client) agent would reside, being software code that can be implemented in a number of flexible ways. The FA Client could take the following forms:

- In an Extreme Ethernet Access Switch, detecting conventional end-points devices – generic PCs, IP Phones, Printers, IP Cameras, etc – and extending customized network service connectivity and attributes.
- In an ExtremeWireless LAN Access Point, facilitating simplified hands-free deployment, service delivery, and device connectivity.
- Leveraging a collaboration with Wind River: any Open vSwitch-based device system, including Xen, KVM, and VirtualBox Hypervisors, and the new Extreme Open Networking Adapter product line.
- Leveraging the IETF submission: any end-point or networking device operating a compliant implementation; this could include third party Switches or any Ethernet-enabled networking device.

Individual FA Clients may require specific networking services – particular VSN IDs, VLAN IDs, etc – or they can simply make a generic request, and rely upon centralized policy for assignment. For example, IP Phones will be assigned to the default "Voice VLAN", whereas IP Cameras – recognized by virtue of their hardware addressing – would be assigned to the "Video Security VLAN". Further, a Virtual Machine could request application-specific network assignment during the spin-up process. Fabric Attach compliments the existing techniques for device recognition, authorization, and authentication – i.e. MAC- and/or RADIUS-based, 802.1X, and 802.1AB – and leverages these to integrate with network provisioning and policy enforcement.

The FA Client communicates, using LLDP extensions, with a Fabric Attach Server (FA Server), either directly or via a Fabric Attach Proxy (FA Proxy). The FA Proxies are conventional Networking Switches, deployed as and when the topology requires, that pass auto-attach requests from FA Clients through to the FA Server. It is also feasible that a Switch acting as an FA Proxy will simultaneously be acting as an FA Client. This would be the case when the Switch is providing FA Client functionality for directly attached end-point devices (e.g. PCs and IP Phones), and also acting as a proxy for an attached FA Client (e.g. an Extreme Wireless LAN AP). The FA Proxy and FA Client agent functionalities easily coexist to provide for maximum deployment flexibility.

The FA Server is a Networking Switch, but is distinguished from the FA Proxy insofar as it is the boundary between the Fabric Connect private cloud and the conventional Ethernet Access network. The FA Server, being a Fabric Connect node, has full network and service awareness and can dynamically extend networking services – again, via the FA Proxy when dictated by topology – to the FA Client and any attached end-point devices.

Putting it another way, end-point devices are connected to the broader network by the FA Client obtaining service extensions from the FA Server; providing the mapping of conventional VLANs to Fabric Connect VSNs. VOSS 5.0 introduces the FA Server capability to the VSP 4000 Series product line; additionally, it is also now supported on the VSP 8000 Series and VSP 7200 Series products.

The Fabric Attach process dynamically and automatically extends networking services from the FA Server to both FA Clients and end-points devices hosted by FA Clients. It gives an "elastic" nature to the network, stretching services to the edge only as required and only for the required duration. As and when end-point devices closedown or disconnect, redundant networking services retract from the edge; this has the added benefit of reducing exposure and the attack profile.

And important value-added element to this solution is the Extreme Identity Engines policy server. Fabric Attach can deliver basic connectivity automation without Identity Engines, however the solution is significantly enhanced by Identity Engines delivering advanced authentication services for users and end-devices. Identity Engines enables more granular control of networking services, over-and-above VSN/VLAN assignment. Leveraging per-user and/or per-device authentication enables custom networking services to be dynamically created and applied on-demand.

There is also a variation on the typical deployment: here Fabric Attach is used in a purely conventional VLAN-based network, and no FA Server (i.e. Fabric Connect node/network) exists. In this scenario, the FA Proxy Switch operates in "standalone" mode, and addresses FA Client requests for VLAN IDs. Identity Engines can also be applied to this model, providing enhanced user and/or device authentication and policy control. This variant of Fabric Attach delivers an auto-attach capability even to those businesses that are yet to implement Fabric Connect.

Fabric Attach delivers substantial operational benefits. End-point devices can be deployed in real-time, without the need for IT intervention and manual configuration, with a centralized policy engine defining and policing device auto-attach in compliance with business policy. Replacing static network device configuration with dynamic programming reduces overall complexity in the network and has a corresponding benefit in reducing the risk of outage.

Fabric Extend: Taking Benefits to a Broader Audience

For many adopters, Fabric Connect has delivered an almost ideal networking solution. Ideal that is, except perhaps for the fact that Shortest Path Bridging, the standard upon which Fabric Connect has been developed, is designed around the concept of physical Ethernet. Being limited to Ethernet-based networking topologies means, for example, that businesses have been unable to extend services-based connectivity end-to-end, across their wide-area networks. Technically, this limitation is due to a dependence for the "establishment" of NNI links – network-to-network interface links – over which IS-IS adjacencies are formed and services defined and delivered. This means that the extent of Ethernet availability has defined an arbitrary boundary for the Fabric Connect network virtualization cloud.

This situation has represented something of a constraint for those businesses that want to fully integrate remote sites into their private cloud. There could be driven by a need to distribute support for IP Multicast-based applications throughout the entire company, or quickly roll-out IPv6 but the infrastructure is not fully ready. There are times when there's a requirement to offer an extended multi-tenant/segmentation capability, or perhaps the issue is as simple as wanting to surgically deploy Fabric Connect in a mixed-vendor environment. Whatever the specific requirement, there's lots of reason why Routed IP connectivity alone isn't a complete-enough solution and why businesses would benefit from being able to extend their Fabric Connect cloud.

Now, with Extreme's development of its Fabric Extend technology, businesses can fully integrate remote locations with the Fabric Connect cloud. Fabric Extend enables configure NNI interfaces to be logically defined, and through VXLAN encapsulation, seamlessly tunnel Shortest Path Bridging connectivity across IP-based topologies such as MPLS and Optical Ethernet. Fabric Extend is a versatile technology that can deliver VLAN and VRF extension, Layer 2 and Layer 3 Hub-and-Spoke networking, and site interconnect for dispersed Campus and Data Center locations.

Fabric Extend perpetuates Fabric Connect's well-earned reputation for simplifying the network. Continuing this theme, the Extreme Fabric Orchestrator management platform incorporates a new Tunnel Manager utility that automatically configures the bi-directional tunnels required to integrate new nodes into Fabric Extend domains.

Tunnel Manager delivers an intuitive, graphical capability to deploy both any-to-any and hub-and-spoke configurations; additionally, a command-line option remains if manual setup is preferred.

In terms of product support, Fabric Extend is available on three Ethernet Switch platforms: on the VSP 4000 Series when deployed in combination with the Extreme Open Networking Adaptor, and also natively on the VSP 8000 Series and VSP 7200 Series products. Extreme's new Fabric Extend technology provides a flexible and scalable solution to enable network-wide extension over private and provider IP infrastructures for the very significant benefits that Fabric Connect is delivering businesses today.

VSP 4000 Models:

The VSP 4000 comes in six model variants:

- **VSP 4450GSX-PWR+** - 36 x 100/1000 Mbps SFP ports, 12-ports of 10/100/1000BASE-T with PoE+, and 2-ports of 1/10 Gigabit SFP+ which have been enabled with MACsec encryption.
- **VSP 4450GSX-DC** - 36 ports of 100/1000 Mbps SFP, 12 ports of 10/100/1000BASE-T, and two SFP+ MACsec capable uplink ports with optional DC redundant power.
- **VSP 4850GTS** - 48 ports of 10/100/1000 including two Combo SFP and two SFP+ uplink ports with optional redundant power.
- **VSP 4850GTS-PWR+** - 48 ports of 10/100/1000 with PoE+ including two Combo SFP and two SFP+ uplink ports with optional redundant power.
- **VSP 4850GTS-DC** - 48 ports of 10/100/1000 including two Combo SFP and two SFP+ uplink ports with optional DC redundant power.
- **VSP 4450GTX-HT-PWR+** - A high temperature variant of the VSP 4000 series that can be deployed in extreme temperature range of 0-70 degrees centigrade. 48 ports of 10/100/1000 with PoE+ including two Combo SFP and two SFP+ uplink ports with optional redundant power.

VSP 4000 Services Overview:

The VSP 4000 offers a wide range of network services that can be deployed simply and easily. The first release supports:

- Layer 2 Virtualized Services that extend VLANs across the Fabric (including across subnets and long distances).
- Layer 3 Virtualized Services that interconnect and extend VRFs across the Fabric.
- Native routing between Layer 2 and Layer 3 Virtualized Services for access to shared services.
- IP Shortcut Routing that enables direct Layer 3 connectivity between individual end-points without requiring deployment of additional IGPs.
- IP Multicast Shortcuts for scalable, efficient and resilient multicast distribution without the deployment of PIM-based protocols.
- IP Multicast Virtualization for the support of PIM-free multicast within a Layer 2 or Layer 3 Virtual Services Network.
- Support for IP Routing techniques including Static, RIP, OSPF, eBGP, BGP+, ECMP, VRRP, PIM-SM/SSM, and VRF. Additionally, supports Static, RIPng, OSPFv3, ECMP, and VRRP for IPv6 deployments.

VSP 4000 Deployment Scenarios:

Offering a multiplicity of services, VSP 4000 is well suited to a wide array of deployment scenarios including:

- Virtualized small/mid-sized enterprise
- Distributed enterprise

A deployment may require either or both of the following (which are discussed in detail further down in this document):

- End-to-end traffic separation for multi-tenancy or for security/regulatory compliance (i.e. PCI DSS).
- Integrated video surveillance, video distribution and digital signage support.

The VSP 4850 series is optimized for copper-based deployments while the VSP 4450 is optimized for heavy fiber-based deployments. An example is a riser of a building, where Gigabit connectivity is delivered to each of the floors.

Virtualized Small/Midsized Enterprise

The Extreme Fabric Connect strategy includes delivering the value of fabric based technology to any size company. Providing a small-to-midsize enterprise solution that is both feature-rich and cost-effective, the VSP 4000 can be deployed with VSP 8200 in the core to enable a simplified, agile, resilient network. Deployed together, this powerful combination of Fabric-enabled edge and small compact core options enables the main stream adoption of Fabric technology by making it cost-effective for the smaller enterprise.

Distributed Enterprise

For Extreme Fabric Connect technology to truly transform the network end-to-end, it must extend to remote locations. Enabling a single technology that can be used throughout the network, the VSP 4000 provides connectivity to remote sites across Service Provider Layer 2 Services (E-Line and E-Tree). VSP 4000s can also be deployed over a physical ring based infrastructure extending the reach of the Fabric Connect network across the metro.

End-to-End Traffic Separation to Support Multi-Tenancy

Within any type of enterprise environment, end-to-end traffic separation may be required to support multi-tenancy. Airports, universities, governments, healthcare and enterprises engaged in acquiring other entities, for example, sometimes want to segregate traffic while offering some shared services.

With its integrated VRF capabilities, Extreme Fabric Connect allows Layer 3 networks to be deployed easily across the fabric with simple end point provisioning. Acting as a low-cost multi-tenant demarcation service that supports and isolates traffic from multiple entities, the VSP 4000 makes a critical contribution to the environment.

End-to-End Traffic Separation for Security or Regulatory Reasons

For security or regulatory reasons enterprises may need to separate traffic end to end. Examples include protecting credit card transactions, medical equipment or surveillance cameras from other network traffic or, in any vertical, separating VoIP and managing it independently.

With its integrated VRF capabilities, Extreme Fabric Connect allows Layer 3 networks to be deployed easily across the fabric and kept isolated end to end.

This, in addition to Mac-in-Mac encapsulation at the edge, can deliver the multiple networks required and offer additional security offer additional security by helping to prevent breaches like VLAN jumping.

Integrated Video Surveillance, Video Distribution and Digital Signage

Verticals such as transportation, government and hospitality often rely on video surveillance technology to protect people and products and, while it is evolving toward multicast, video surveillance still relies largely on unicast traffic. VSP 4000 supports both types of surveillance networks - without requiring additional IGPs or PIM protocols. In addition, VSP 4850GTS-PWR+ and VSP 4450GSX-PWR+ devices, which also support IEEE 802.3at PoE+, can power new point tilt and zoom cameras.

Extreme Fabric Connect technology is built from the ground up to handle Multicast trees efficiently since Broadcast and Multicast forwarding are inherent functions within Ethernet. Enabling the network to instantiate point-to-point, point-to-multi-point and any-to-any connectivity services on demand, Extreme Fabric Connect offers a highly efficient, scalable, more resilient way to distribute multicast to support IPTV, digital signage or multicast enabled video surveillance networks.

Additionally, VOSS supports the Extreme Fabric Connect-PIM Gateway. This feature enables seamless bi-directional interoperability between Fabric Connect and a standards-based PIM Multicast Routing environment. While traditional PIM - Protocol Independent Multicast - is notoriously restrictive, complex, and unstable, it was, unfortunately, the only option if an organization needed to route IP Multicast traffic. Fabric Connect completely changes the Multicast paradigm, making this flexible to plan, simple to deploy, stable to operate. Now, organizations operating a legacy IP Multicast environment - either the PIM-SM or PIM-SSM - can implement Fabric Connect and enjoy seamlessly co-existence pending an eventual transition away from PIM. This feature is flexible, supports high-availability options, and enables organizations to deploy and retire technology at their own pace. The VSP 4000 Series supports the Interface functionality component of the Fabric Connect-PIM Gateway feature.

System Compatibility

From a software perspective, the VSP 4000 Series was introduced with the VOSS 4.1 unified software release; this is, therefore, the minimum level of software available to operate the Switch. The recent VOSS 7.0 release delivers the following major enhancements:

- Introduction of the Zero-Touch Fabric Connect capability
- Phase 1 of IPv6 IP Routing Virtualization
- Adding IPv6 Peering to BGPv6
- Introduction of an Energy Saver capability
- Integration with Extreme Management Center
- Expanded Transceiver availability and support

Zero-Touch Fabric Connect. The intent of the new "Zero-Touch Fabric" feature is to automate the addition of new Fabric Connect nodes into an existing domain, greatly simplifying scale-out in distributed and Cloud architectures.

How it works: Assuming a Fabric Connect domain is already in place – and this can be as a simple as a single "Seed Switch" – an automatically generated "Fabric Area Network" facilitates administrative communication between established and candidate Fabric Connect nodes. Zero-

Touch Fabric enables new nodes to automatically detect the IS-IS Area and request the domain-specific Nickname (think, conceptually, DHCP), establish bi-directional IS-IS communication using the default B-VID values, and self-configures a System ID and a Management IP Address.

IPv6 IP Routing Virtualization (Phase 1). With this release, the existing IPv6 IP Routing capability is further enhanced through virtualization; that is, IPv6 is not limited to one instance, within the Global Routing Table. Now, the Switch supports 128 IPv6 Routing instances, supporting features such as ECMP, Alternative Route, Route Redistribution, Inter-VSN Routing, DHCP Relay, ICMP Ping & Traceroute, and VRRPv3 for IPv6. Additionally, VRF instances support unification of both IPv4 and IPv6, and L3 Virtual Service Networks.

Extreme Management Center

The network is the lifeblood of your business: it powers transformational applications and energizes your most vital asset, your people; integrating wired and wireless infrastructures, it delivers continuity and mobility; its dependability is intrinsically coupled with organizational success. Extreme Management Center gives you actionable insights, granular visibility, and automated control over users, devices, and applications.

Leveraging the dexterity that only a genuine single-pane-of-glass platform can enable, Extreme Management Center empowers you to deliver a superior quality of experience to all of your stakeholders. It works across your entire infrastructure, wired and wireless, from the access edge to the private cloud, giving you a true 360-degree view of your network, devices, applications, and users. Extreme Management Center is the integrated toolset that enables your business to go to the next level.

This powerful appliance-based solution offers the following functionality:

- **Single Pane-of-Glass** – A fully integrated suite of tools working together to provide a comprehensive, unified view of the network, streamlining workflows and reducing operational costs.
- **Discovery and Visualization** – Providing rich network and device discovery and visualization capabilities. Includes the ability to discover network-attached devices, including servers, storage servers, switches, routers, phones, virtual machines and their hosts, plus Extreme Aura applications.
- **Fault and Diagnostics** – Leverages information collected from the network to determine the most likely cause of network outages, and correlates events to determine affected devices and services.
- **Configuration and Orchestration** – Facilitates even the most complex of network configurations through simplified, intuitive wizards and easy-to-use templates. Configuration templates are created once, stored, and then conveniently applied in order to accelerate time-to-service and reduce the risk of human error.
- **Virtualization Management** – Provides insight into the complete lifecycle of virtual machines – activation, migration, and retirement – including the automatic provisioning of those companion networking services needed to parallel VM migrations.
- **Performance Management** – Delivers tools to monitor, analyze and report application behaviors and their bandwidth utilization trends.
  Collected data gives valuable insight into traffic patterns, application behaviors, and top talkers. Performance management tools enable capacity planning and change monitoring.
- I**ntegrated SDN Capabilities** – Crucially, Fabric Orchestrator is built with a clear eye towards the future. The platform provides an integration point for Open Daylight-based SDN Controller plugins, third party tools and controllers accessible through north-bound REST interfaces, and OpenStack ML2 drivers that enable network orchestration in conjunction with storage and compute resources.

Lifetime Warranty

Extreme includes comprehensive warranty services for its portfolio of stackable switches, including Fabric Connect edge devices. Complimentary next-business-day shipment of failed units is provided for the full life of the product in addition to next-business-day shipping to replace failed hardware worldwide. Extreme also offers complimentary basic technical support:

Level 1 for the supported lifecycle of the product and up to Level 3 for the first 90 days after purchase including support for the shipped software version with an optional Software Release Service.

Based on the industry norm for hardware, 'Lifetime' is defined as the production lifecycle phase plus 5 years post-discontinuation. And, for customers desiring protection over and above warranty provisions, Extreme offers a full suite of support services.

Summary

Deployed in conjunction with other Extreme Fabric Connect solutions, the VSP 4000 can increase profitability and productivity, streamline business operations, lower costs and help your business gain a competitive edge. Offering a simple, more elegant approach to deployment of all L2/3 services, Extreme is a leader in Fabric-enabled networking.

VSP 4450GSX-PWR+	
Switch Details	• 12-ports of 10/100/1000 Gigabit Ethernet RJ45 with PoE+ ports • 36 ports of 100/1000 Mbps SFP ports • 2 ports of 1/10 Gigabit SFP+ ports • System CPU operates at 1.2GHz • Switch configured with 2GB of 800 DDR3 DRAM • RJ-45 Console port and a USB 2.0 port • Ships with 1 set of 44mm/19" rack mount brackets
Dimensions	1U 4.4cm (H), 44cm [19" rack mount compatible] (W), 43.6cm (D)
Weight	17.2lbs (7.80 kg) with 1 PSU installed. A PSU weighs 3.1 lbs (1.40 kg)
Power and Thermal	• Supplied with 1 x 1000W AC field replaceable power supply unit • Supports addition of second field replaceable AC power supply for redundancy • Power consumption without PoE is 95W typical and 140W max so thermal is 324 BTU/hr typical and 477.70 BTU/hr max

VSP 4450GSX-DC	
Switch Details	• 12 ports of 10/100/1000 Gigabit Ethernet RJ45 ports • 36 ports of 100/1000 Mbps SFP ports • 2 ports of 1/10 Gigabit SFP+ ports • System CPU operates at 1.2GHz • Switch configured with 2GB of DRAM • RJ-45 Console port and a USB 2.0 port • Ships with 1 set of 44mm/19" rack mount brackets
Dimensions	1U 4.4cm (H), 44cm [19" rack mount compatible] (W), 43.6cm (D)
Weight	17.2lbs (7.80 kg) with 1 PSU installed. A PSU weighs 3.1 lbs (1.40 kg)
Power and Thermal	• Supplied with 1 x 300 watt Field Replaceable DC power supply • Supports addition of second Field Replaceable DC power supply for redundancy • Thermal Rating 323 BTU/hr

VSP 4850GTS	
Switch Details	• 48 10/100/1000 Gigabit Ethernet RJ45 ports • 2 Combo SFP ports • Plus 2 x 1/10 Gigabit SFP+ ports • System CPU operates at 533 MHz • Switch is configured with 1GB RAM • RJ-45 Console port provides industry standard serial port connectivity • Ships with 1 set of 44mm/19" rack mount brackets
Dimensions	4.4cm – 1RU (H), 44.0cm (W), 43.68cm (D)
Weight	11.48 Kg
Power and Thermal	• Supplied with 1 x 300 watt Field Replaceable AC power supply • Supports addition of second Field Replaceable AC power supply for redundancy • Thermal Rating 323 BTU/hr

VSP 4850GTS-PWR+	
Switch Details	• 48 10/100/1000 Gigabit Ethernet RJ45 ports • 48 ports support IEEE 802.3at PoE+ ports • 2 Combo SFP ports • Plus 2 x 1/10 Gigabit SFP+ ports • System CPU operates at 533 MHz • Switch is configured with 1GB RAM • RJ-45 Console port provides industry standard serial port connectivity • Ships with 1 set of 44mm/19" rack mount brackets
Dimensions	4.4cm – 1RU (H), 44.0cm (W), 43.68cm (D)
Weight	11.98 Kg
Power and Thermal	Supplied with 1 x 1000 watt Field Replaceable AC power supply Supports addition of second Field Replaceable AC power supply for redundancy or additional PoE Thermal Rating 383 BTU/hr
Maximum PoE Budget	• 855 watts when operating on one 1000w power supply • 1855 watts when operating on two 1000w power supply

VSP 4450GTX-HT-PWR+	
Switch Details	• 48 ports of 10/100/1000 Gigabit Ethernet with PoE+ RJ45 ports • 2 Combo ports of 1G SFP ports • 2 ports of 1/10 Gigabit SFP+ ports • System CPU operates at 1.2 GHz • Switch is configured with 2GB SDRAM • RJ-45 Console port provides industry standard serial port connectivity • Ships with 1 set of 44mm/19" rack mount brackets. • Operating temperature range 0-70C
Dimensions	8.8cm – 2RU (H), 44.0cm (W), 36.8cm (D)
Weight	With 1 PSU; total 23.1 lbs = 10.48 kg, PSU – 3.1 lbs = 1.4 kg
Power and Thermal	• Supplied with 1 x 1000 watt Field Replaceable AC power supply • Supports addition of second Field Replaceable AC power supply for redundancy • Thermal Rating: Power consumption without PoE is 100W typical and 145W max. Thermal is 341.2 BTU/hr typical and 494.8 BTU/hr max.

VSP 4850GTS-DC	
Switch Details	• 48 10/100/1000 Gigabit Ethernet RJ45 ports • 2 Combo SFP ports • Plus 2 x 1/10 Gigabit SFP+ ports • System CPU operates at 533 MHz • Switch is configured with 1GB RAM • RJ-45 Console port provides industry standard serial port connectivity • Ships with 1 set of 44mm/19" rack mount brackets
Dimensions	4.4cm – 1RU (H), 44.0cm (W), 43.68cm (D)
Weight	11.48 Kg
Power and Thermal	• Supplied with 1 x 300 watt Field Replaceable DC power supply • Supports addition of second Field Replaceable DC power supply for redundancy • Thermal Rating 323 BTU/hr

Specifications

General

- Frame length: 64 to 1518 Bytes (802.1Q Untagged), 64 to 1522 bytes (802.1Q Tagged)
- Jumbo Frame support: up to 9.6 KBytes
- Switching Fabric Capacity: 184 Gbps
- Packet Forwarding Throughput (64-byte packets): 102 Mpps
- Latency (64-byte packets): 9 microseconds
- RSTP, MSTP
- VRRP Backup Master
- IPv4 and IPv6 Routing
- Policy Based Routing
- Ingress and Egress Port ACLs
- Ingress VLAN ACLs
- Enterprise Device Manager GUI, on-box & off-box
- Configuration & Orchestration Manager
- Virtualization Performance & Fault Manager
- Virtualization Provisioning Service
- System Logging
- Mirroring: 1:1 / 1:M / M:1 / M:M
- Key Health Indicators
- Flight Recorder
- Auto MDIX
- MACsec (VSP 4450GSX-PWR+ only)
- TACACS+
- SLAMon agent

Layer 2

- MAC Address: 32,000
- Port-based VLANs: 4,059
- Private VLANs/E-Tree: 1,000
- MSTP Instances: 12
- MLT/LACP Groups: 50
- MLT Links per Group: 8
- LACP Links per Group: 8 Active
- Extreme VLACP Instances: 50
- Extreme SLPP Instances: 128

Layer 3 IPv4 Routing Services

- ARP Entries: 6,000
- Static ARP Entries: up to 2,000 per VRF/Switch
- IP Interfaces: 256
- CLIP Interfaces: 64
- IP Routes: up to 15,744
- IP Static Routes: 1,000 per VRF, 1,000 per Switch
- RIP Interfaces: 24
- RIP Routes: up to 15,744
- OSPF Interfaces: 100
- OSPF Routes: up to 15,744
- OSPF Areas: 12 per VRF, 64 per Switch
- BGP Peers: 12
- BGP Routes: up to 15,744
- ECMP Groups: 500
- ECMP Paths per Group: 4
- VRRP Interfaces: 64 or 24 with fast timers
- RSMLT Interfaces: 252
- IPv4 UDP Forwarding Entries: 128
- IPv4 DHCP Relay Forwarding Entries: 128
- IP Route Policies: 500 per VRF, 5,000 System-wide
- VRF Instances: up to 128

Layer 3 IPv6 Routing Services

- Neighbors: 4,000
- Static Neighbors: 128
- IP Interfaces: 256
- CLIP Interfaces: 64
- IP Configured Tunnels: 254
- IP Routes: up to 7,488
- IP Static Routes: 1,000
- RIPng Interfaces: 24
- RIPng Routes: up to 7,488
- OSPFv3 Interfaces: up to 100
- OSPFv3 Routes: up to 7,488
- OSPFv3 Areas: 64 per switch
- BGPv6 Peers: 12
- ECMP Groups: 500
- ECMP Paths per Group: 4
- VRRP Interfaces: 64 or 24 with fast timers

- RSMLT Interfaces: 252
- VRF Instances: up to 128

Multicast

- IGMP Interfaces: 4,059
- PIM Active Interfaces: 128
- PIM-SSM Static Channels: 512
- IP Multicast Streams: 1,000
- Fabric Connect-PIM Gateway Controllers per Region: 5
- Fabric Connect-PIM Gateway Nodes per Region: 64
- Fabric Connect-PIM Gateway Interfaces per BEB Node: 64
- Fabric Connect-PIM Gateway Source Announcements: 6,000

Fabric Connect

- 802.1aq/RFC 6329 Shortest Path Bridging with Extreme extensions
- MAC Address: 16,000
- NNI Interfaces/Adjacencies: up to 255
- BCB/BEB Nodes per Region: 2,000
- BEB Nodes per VSN: 2,000
- L2 Virtual Service Networks: 1,000
- L3 Virtual Service Networks: up to 128
- IP Shortcut Routes: IPv4 up to 15,744, and IPv6 up to 7,488
- L2 Multicast Virtual Service Networks: 1,000
- L3 Multicast Virtual Service Networks: 128

QoS and Filtering

- IPv4 ACE: 1530 Ingress and 254 Egress
- IPv6 ACE: 256 Ingress
- •QoS priority queues: 8

Operations and Managemment

- Mirrored Ports: 49
- sFlow: up to 100 samples per second
- Fabric RSPAN: 1,000 VLAN IDs

Environmental Specifications

- Operating temperature: 0°C to 50°C (32°F to 122°F)
- Storage temperature: -40°C to 85°C (-13°F to 158°F)
- Operating humidity: 0 to 95% maximum relative humidity, non-condensing
- Storage humidity: 10 to 90% maximum relative humidity, non-condensing Operating altitude: 0 to 3,048m (0 to 10,000ft) maximum
- Storage altitude: 0 to 12,192m (0 to 40,000ft) maximum
- Acoustic Noise:
  - Less than 50dbA at 35°C
  - Less than 57dbA at 50°C
- VSP 4000 Safety Agency Approvals
- Global basis for certification: IEC 60950 current edition with all CB member deviations
- CB Scheme Certification with Member Deviations
- EN60950 Europe Safety (CE)
- UL60950 United States of America Safety
- CSA22.2, #60950 Canada Safety
- NOM Mexico Safety
- S-mark Argentine Safety
- Anatel Brazilian Safety
- Electromagnetic Emissions & Immunity
- CISPR22 International EMC Emissions
- CIRPR24 International EMC Immunity
- EN55022:2006 European EMC Emissions (CE)
- EN55024 European EMC Immunity (CE)
- EN61000
- Additional European EMC Specifications (CE)
- FCC Part 15 US EMC Emissions
- ICES-003 Canadian EMC Emissions
- VCCI Japan EMC Emissions
- AN/NZS 3548 Australia/New Zealand EMC Emissions
- CNS13438 Taiwan EMC Emissions
- MIC Korean EMC Certification
- Anatel Brazilian EMC Certification

MTBF Values

- 214,542 to 311,104 hours (24.49 to 35.31 years)

Warranty

- Lifetime Next Business Day advanced hardware replacement
- Lifetime Basic Technical Support
- 90-Day Advanced Technical Support
- Optional Software Release Service also available: GW5300ASG / GW6300ASG

Country of Origin

- Peoples Republic of China

Standard Compliance

802.1 Bridging (Networking) and Network Management

- 802.1D MAC Bridges (a.k.a. Spanning Tree Protocol)
- 802.1p Traffic Class Expediting and Dynamic Multicast Filtering
- 802.1t 802.1D Maintenance
- 802.1w Rapid Reconfiguration of Spanning Tree (RSTP)
- 802.1Q Virtual Local Area Networking (VLAN)
- 802.1Qbp Equal-Cost Multi-Path (Shortest Path Bridging)
- 802.1Qcj Automatic Attachment to Provider Backbone Bridging (PBB) Services (Partial Support)
- 802.1s Multiple Spanning Trees (MSTP)
- 802.1v VLAN Classification by Protocol & Port
- 802.1ag Connectivity Fault Management
- 802.1ah Provider Backbone Bridges
- 802.1aq Shortest Path Bridging (SPB) MAC-in-MAC
- 802.1X Port-based Network Access Control
- 802.1AB-2005 Station & Media Access Control Connectivity Discovery; aka LLDP (partial support)
- 802.1AE Media Access Control Security
- 802.1AX Link Aggregation

802.3 Ethernet

- 802.3-1983 CSMA/CD Ethernet (ISO/IEC 8802-3)
- 802.3i-1990 10Mb/s Operation, 10BASE-T Copper
- 802.3u-1995 100Mb/s Operation, 100BASE-T Copper, with Auto-Negotiation
- 802.3x-1997 Full Duplex Operation, including Flow Control
- 802.3z-1998 1000Mb/s Operation, implemented as 1000BASE-X
- 802.3ab-1999 1000Mb/s Operation, 1000BASE-T Copper
- 802.3ae-2002 10Gb/s Operation, implemented as 10GBASE-SFP+
- 802.3an-2006 10Gb/s Operation, 10GBASE-T Copper
- 802.3ba-2010 40Gb/s and 100Gb/s Operation
- 802.3bm-2015 40Gb/s and 100Gb/s Operation, implemented as 40GBASE-QSFP+ & 100GBASE-QSFP28

IETF

- 768 UDP
- 783 TFTP
- 791 IP
- 792 ICMP
- 793 TCP
- 826 ARP
- 854 Telnet
- 894 Transmission of IP Datagrams over Ethernet Networks
- 896 Congestion Control in IP/TCP internetworks
- 906 Bootstrap Loading using TFTP
- 950 Internet Standard Subnetting Procedure
- 951 BOOTP: Relay Agent-only
- 959 FTP
- 1027 Using ARP to Implement Transparent Subnet Gateways
- 1058 RIP
- 1112 Host Extensions for IP Multicasting
- 1122 Requirements for Internet Hosts - Communication Layers
- 1155 Structure and Identification of Management Information for TCP/IP-based Internets
- 1156 MIB for Network Management of TCP/IP
- 1157 SNMP
- 1212 Concise MIB Definitions
- 1213 MIB for Network Management of TCP/ IP-based Internets: MIB-II
- 1215 Convention for Defining Traps for use with the SNMP
- 1256 ICMP Router Discovery
- 1258 BSD Rlogin
- 1271 Remote Network Monitoring MIB
- 1305 NTPv3
- 1321 MD5 Message-Digest Algorithm
- 1340 Assigned Numbers
- 1350 TFTPv2
- 1398 Ethernet MIB
- 1442 SMIv2 of SNMPv2
- 1450 SNMPv2 MIB
- 1519 CIDR
- 1541 DHCP
- 1542 Clarifications & Extensions for BOOTP
- 1573 Evolution of the Interfaces Group of MIB-II
- 1587 OSPF NSSA Option

IETF Cont.

- 1591 DNS Client
- 1650 Definitions of Managed Objects for the Ethernet-like Interface Types
- 1657 Definitions of Managed Objects for BGP-4 using SMIv2
- 1723 RIPv2 Carrying Additional Information
- 1812 Router Requirements
- 1850 OSPFv2 MIB
- 1866 HTMLv2
- 1907 SNMPv2 MIB
- 1930 Guidelines for creation, selection, and registration of an AS
- 1981 Path MTU Discovery for IPv6
- 2021 Remote Network Monitoring MIBv2 using SMIv2
- 2068 HTTP
- 2080 RIPng for IPv6
- 2131 DHCP
- 2138 RADIUS Authentication
- 2139 RADIUS Accounting
- 2236 IGMPv2 Snooping
- 2284 PPP Extensible Authentication Protocol
- 2328 OSPFv2
- 2362 PIM-SM
- 2404 HMAC-SHA-1-96 within ESP and AH1
- 2407 Internet IP Security Domain of Interpretation for ISAKMP1
- 2408 Internet Security Association and Key Management Protocol
- 2428 FTP Extensions for IPv6 and NAT
- 2452 TCP IPv6 MIB
- 2453 RIPv2
- 2454 UDP IPv6 MIB
- 2460 IPv6 Basic Specification
- 2463 ICMPv6
- 2464 Transmission of IPv6 Packets over Ethernet Networks
- 2466 MIB for IPv6: ICMPv6 Group
- 2474 Differentiated Services Field Definitions in IPv4 & IPv6 Headers
- 2475 Architecture for Differentiated Service
- 2541 DNS Security Operational Considerations
- 2545 BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- 2548 Microsoft Vendor-specific RADIUS Attributs
- 2572 Message Processing and Dispatching for SNMP
- 2573 SNMP Applications
- 2574 User-based Security Model for SNMPv3
- 2575 View-based Access Control Model for SNMP
- 2576 Coexistence between v1/v2/v3 of the Internet-standard Network Management Framework
- 2578 SMIv2
- 2579 Textual Conventions for SMIv2
- 2580 Conformance Statements for SMIv2
- 2597 Assured Forwarding PHB Group
- 2598 Expedited Forwarding PHB OA&M RFCs
- 2616 HTTPv1.1
- 2710 MLD for IPv6
- 2716 PPP EAP TLS Authentication Protocol
- 2787 Definitions of Managed Objects for VRRP
- 2818 HTTP over TLS
- 2819 Remote Network Monitoring MIB
- 2863 Interfaces Group MIB
- 2865 RADIUS
- 2869 RADIUS Extensions (partial support)
- 2874 DNS Extensions for IPv6
- 2925 Definitions of Managed Objects for Remote Ping, Traceroute, & Lookup Operations
- 2933 GMP MIB
- 2934 PIM MIB for IPv4
- 2992 ECMP Algorithm
- 3046 DHCP Relay Agent Information
- Option 82
- 3162 RADIUS and IPv6
- 3246 Expedited Forwarding PHB
- 3315 DHCPv6
- 3339 Date & Time on The Internet: Timestamps
- 3376 IGMPv3
- 3411 Architecture for Describing SNMP Management Frameworks
- 3412 Message Processing and Dispatching for SNMP
- 3413 SNMP Applications

IETF Cont.

- 3414 USM for SNMPv3
- 3415 VACM for SNMP
- 3416 Protocol Operations v2 for SNMP
- 3417 Transport Mappings for SNMP
- 3418 MIB for SNMP
- 3484 Default Address Selection for IPv6
- 3513 IPv6 Addressing Architecture
- 3569 Overview of SSM
- 3579 RADIUS Support for EAP
- 3587 IPv6 Global Unicast Address Format
- 3596 DNS Extensions to support IPv6
- 3748 Extensible Authentication Protocol
- 3768 VRRP; plus draft-ietf-vrrp-ipv6-spec-08
- 3810 MLDv2 for IPv6: Host Mode-only
- 3879 Deprecating Site Local Addresses
- 4007 IPv6 Scoped Address Architecture
- 4022 TCP MIB
- 4087 IP Tunnel MIB
- 4113 UDP MIB
- 4133 Entity MIB Version 3 (partial support)
- 4193 Unique Local IPv6 Unicast Addresses
- 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
- 4250 SSH Assigned Numbers
- 4251 SSH Protocol Architecture
- 4252 SSH Authentication Protocol
- 4253 SSH Transport Layer Protocol
- 4254 SSH Connection Protocol
- 4255 DNS to Securely Publish SSH Key Fingerprints
- 4256 Generic Message Exchange Authentication for SSH
- 4291 IPv6 Addressing Architecture
- 4292 IP Forwarding Table MIB
- 4293 IP MIB
- 4301 Security Architecture for IP[1]
- 4302 IP Authentication Header[1]
- 4303 IP Encapsulating Security Payload[1]
- 4308 Cryptographic Suites for IPsec
- 4363 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions (partial support)
- 4443 ICMP for IPv6
- 4429 Optimistic DAD for IPv6 (partial support)
- 4541 Considerations for IGMP & MLD Snooping Switches
- 4552 Authentication/Confidentiality for OSPFv3
- 4601 PIM-SM: Revised Protocol Specification
- 4607 Source-Specific Multicast for IP
- 4675 RADIUS Attributes for Virtual LAN and Priority Support (partial support)
- 4835 Cryptographic Algorithm Implementation Requirements for ESP & AH[1]
- 4861 Neighbor Discovery for IPv6
- 4862 IPv6 Stateless Address Auto- Configuration
- 5095 Deprecation of Type 0 Routing Headers in IPv6
- 5176 Dynamic Authorization Extensions to RADIUS
- 5187 OSPFv3 Graceful Restart (Helper-mode)
- 5308 Routing IPv6 with IS-IS
- 5340 OSPF for IPv6
- 5424 The Syslog Protocol
- 5798 VRRPv3 for IPv4 & IPv6
- 5905 NTPv4: Protocol and Algorithms Specification
- 5997 Use of Status-Server Packets in RADIUS
- 6105 IPv6 Router Advertisement Guard
- 6329 IS-IS Extensions supporting Shortest Path Bridging
- 6933 Entity MIBv4 (partial support)
- 7358 VXLAN: A Framework for Overlaying Virtualized L2 Networks over L3 Networks (partial support)
- 7610 DHCPv6 Shield: Protecting against Rogue DHCPv6 Servers
- Internet-Draft IP/IPVPN services with IEEE 802.1aq SPB networks (draft-unbehagen-spb-ip-ipvpn-00)
- Internet-Draft SPB Deployment Considerations (draft-lapuh-spb-deployment-03)

MTBF

(Base Unit with Single Power Supply)

- VSP 4450GSX-PWR+ - up to 293,000 hours (33.44 years)
- VSP 4450GSX-DC - up to 308,000 hours (35.15 years)
- VSP 4450GTX-HT-PWR+ - up to 224,500 hours (25.62 years)
- VSP 4850GTS - up to 311,104 hours (35.51 years)
- VSP 4850GTS-PWR+ - up to 214,542 hours (24.49 years)
- VSP 4850GTS-DC - up to 311,104 hours (35.51 years)

[1] Implemented to deliver IPsec capability for Control Plane traffic only.

Ordering Information

Part Number*	Description
EC4400?05-E6	VSP 4450GSX-PWR+ 50-port Ethernet Switch, supporting 36 x 1000BASE-SFP ports, 12 x 10/100/1000BASE-T ports with PoE+, and 2 x 10GBASE-SFP+ Uplink ports. Includes single 1000W AC Power Supply, Country-specific Power Cord, and Base Software License.
EC4400004-E6	VSP 4450GSX-DC 50-port Ethernet Switch, supporting 36 x 1000BASE-SFP ports, 12 x 10/100/1000BASE-T ports, and 2 x 10GBASE-SFP+ Uplink ports. Includes single 300W DC Power Supply, DC Connector, and Base Software License.
EC4400?03-E6	VSP 4450GTX-HT-PWR+ 50-port High-Temperature Ethernet Switch, supporting 48 x 10/100/1000BASE-T ports with PoE+, including 2 x 1000BASE-SFP Combo ports, and 2 x 10GBASE-SFP+ Uplink ports. Includes single 1000W AC Power Supply, Country-specific Power Cord, and Base Software License.
EC4800?78-E6	VSP 4850GTS 50-port Ethernet Switch, supporting 48 x 10/100/1000BASE-T ports, including 2 x 1000BASE-SFP Combo ports, and 2 x 10GBASE-SFP+ Uplink ports. Includes single 300W AC Power Supply, Country-specific Power Cord, and Base Software License.
EC4800?88-E6	VSP 4850GTS-PWR+ 50-port Ethernet Switch, supporting 48 x 10/100/1000BASE-T ports with PoE+, including 2 x 1000BASE-SFP Combo ports, and 2 x 10GBASE-SFP+ Uplink ports. Includes single 1000W AC Power Supply, Country-specific Power Cord, and Base Software License.
EC4800078-E6	VSP 4850GTS-DC 50-port Ethernet Switch, supporting 48 x 10/100/1000BASE-T ports, including 2 x 1000BASE-SFP Combo ports, and 2 x 10GBASE-SFP+ Uplink ports. Includes single 300W DC Power Supply, DC Connector, and Base Software License.

Redundant Power Supplies

Part Number*	Description
AL1905?08-E5	300W AC Power Supply for VSP 4850GTS. Power Cord ordered separately.
AL1905?21-E6	1,000W AC Power Supply for VSP 4450GSX-PWR+ and VSP 4850GTS-PWR+. Power Cord ordered separately.
EC4005?03-E6HT	1,000W High-Temperature AC Power Supply for VSP 4450GTX-HT-PWR+, Medium Grey in color. Power Cord ordered separately.
AL1905005-E5	300W DC Power Supply for VSP 4450GSX-DC and VSP 4850GTS-DC[2]. Includes DC Connector.

*Note: Where applicable, the seventh character (?) of the switch order number must be replaced with the proper letter to indicate desired product nationalization. See table for details:
"A" No power cord included
"B" Includes European "Schuko" power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden
"C" Includes power cord commonly used in the United Kingdom and Ireland
"D" Includes power cord commonly used in Japan
"E" Includes North American power cord
"F" Includes Australian power cord, also commonly

[2] This PSU does not support PoE and is designed for the non-PWR+ VSP 4000 models

Licenses

Base Software License, included with hardware purchase, enables most features with the exception of those specifically noted an enabled by the Premier Software License.

Premier Software License, an optional accessory, enables the following functionality: Layer 3 Virtual Service Networks, Distributed Virtual Routing, greater than 24 Virtual Routing and Forwarding instances, and - where local regulations permit - MACsec.

Part Number	Description
338835	VSP 4000 Series Premier Software License: enables L3 VSNs, DvR Leaf, >24 VRFs, and MACsec.
338836	VSP 4000 Series Premier Software License: enables L3 VSNs, DvR Leaf, and >24 VRFs.

Extreme®
Connect Beyond the Network

http://www.extremenetworks.com/contact / Phone +1-408-579-2800