



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at wvOASIS.gov. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at WVPurchasing.gov with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 2

[List View](#)

General Information


[Contact](#)[Default Values](#)[Discount](#)[Document Information](#)

Procurement Folder: 735458

SO Doc Code: CRFQ

Procurement Type: Central Purchase Order

SO Dept: 0603

Vendor ID: 

SO Doc ID: ADJ2000000033

Legal Name: INDICIUM TECHNOLOGIES INC

Published Date: 6/3/20

Alias/DBA:



Close Date: 6/16/20

Total Bid: \$44,100.00

Close Time: 13:30

Response Date: 

Status: Closed

Response Time: Solicitation Description:  

Total of Header A ttachments: 2

Total of All A ttachments: 2



Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

**State of West Virginia
 Solicitation Response**

Proc Folder : 735458

Solicitation Description : Ethernet Switches, Power Cords, Transceivers, & Cables MCAS

Proc Type : Central Purchase Order

Date issued	Solicitation Closes	Solicitation Response	Version
	2020-06-16 13:30:00	SR 0603 ESR06162000000007636	1

VENDOR
000000162797 INDICIUM TECHNOLOGIES INC

Solicitation Number: CRFQ 0603 ADJ2000000033

Total Bid : \$44,100.00 **Response Date:** 2020-06-16 **Response Time:** 13:25:44

Comments:

FOR INFORMATION CONTACT THE BUYER
 John W Estep
 (304) 558-7839
 john.w.estep@wv.gov

Signature on File	FEIN #	DATE
--------------------------	---------------	-------------

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Ethernet Switches, Power Cords, Transceivers, & Cables MCAS	1.00000	LS	\$44,100.000000	\$44,100.00

Comm Code	Manufacturer	Specification	Model #
43222612			

Extended Description :	Ethernet Switches, Power Cords, Transceivers, & Cables MCAS
-------------------------------	---

Comments: Fortinet Switches and Transceivers submitted for consideration.

FORTINET[®]

WVSOS

Fortinet Security Fabric

- Network Security
- Multi-Cloud Security
- Device, Access, and Application Security
- Open Ecosystem
- Security Operations

BROAD

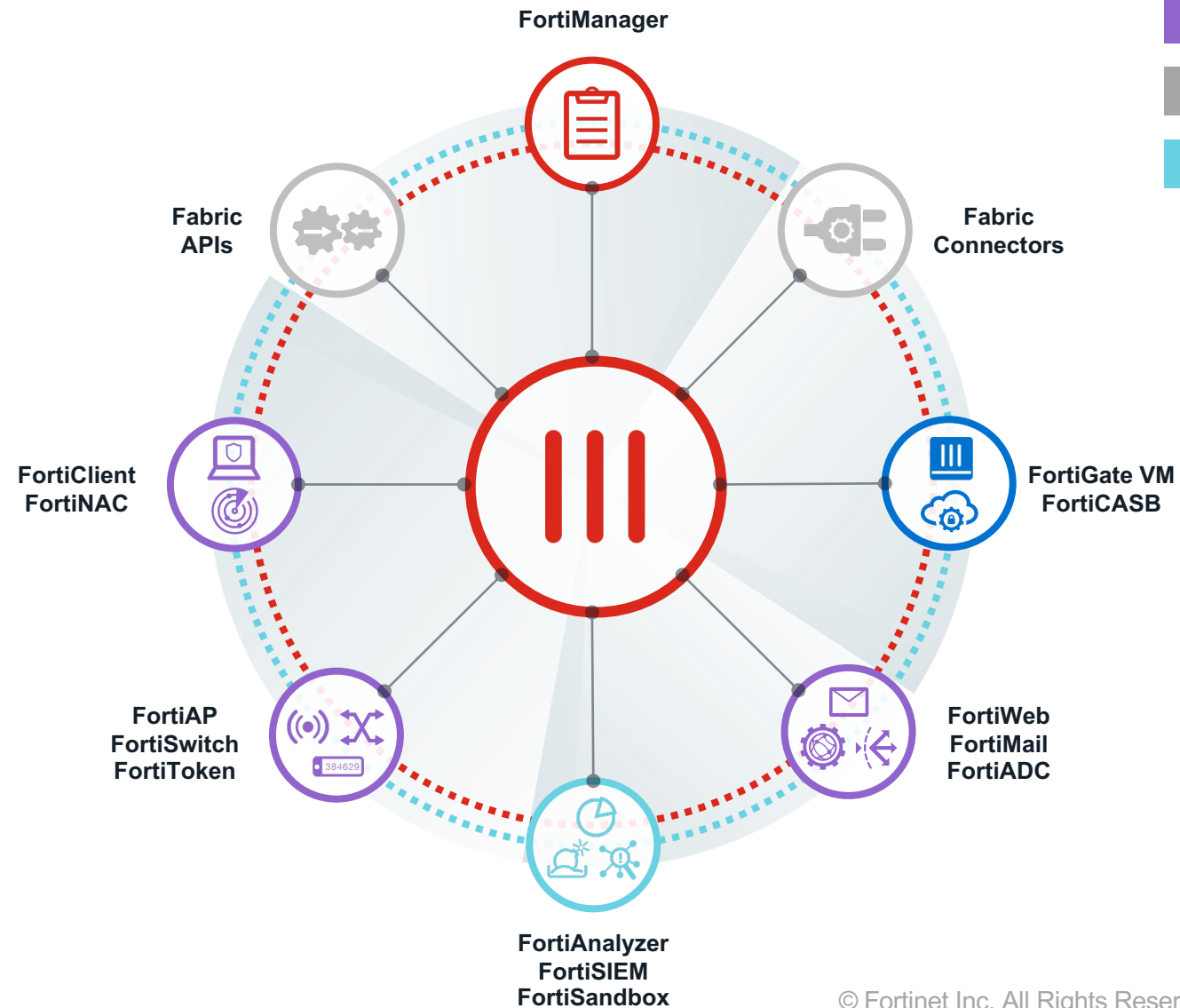
Visibility of the entire digital attack surface

INTEGRATED

Protection across all devices, networks, and applications

AUTOMATED

Operations and response driven by Machine Learning



FortiLink enables Secure Access

FortiLink protocols enable FortiGate to manage Fortinet's network access layer

Simplicity

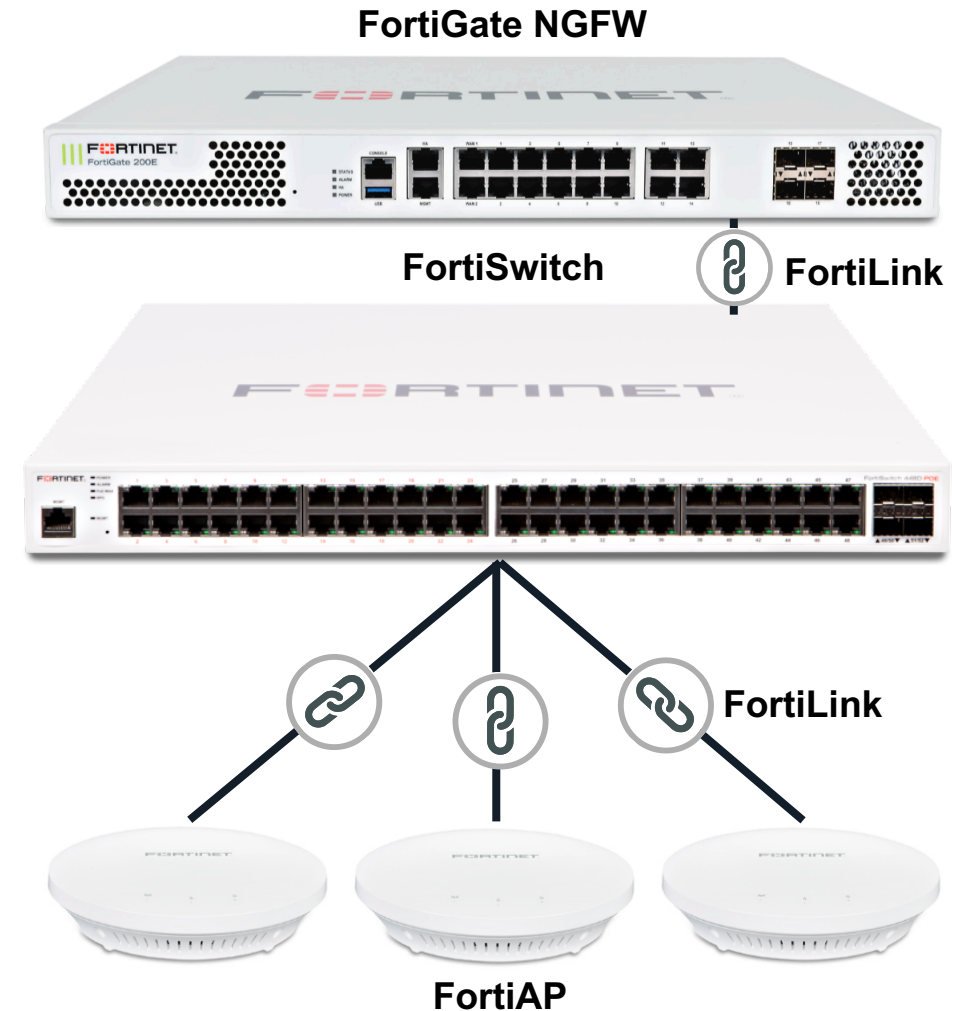
- Flexible architecture, scales as needs change
- Management visibility and analytics across wired, wireless, and security

Security

- Firewall and switch ports equally secure, SSIDs tied directly to firewall policies
- Global Security polices down to port and WLAN level

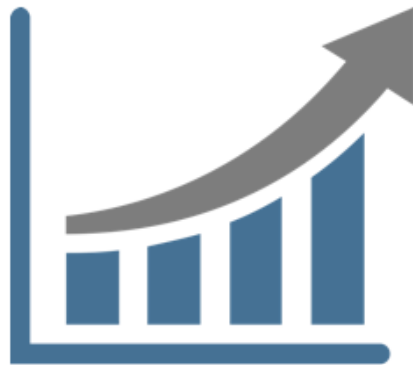
Lower Cost of Ownership

- Access Management included with SD-Branch. No licenses required



A Secure Simple Scalable model to address Ethernet access

Number of Devices



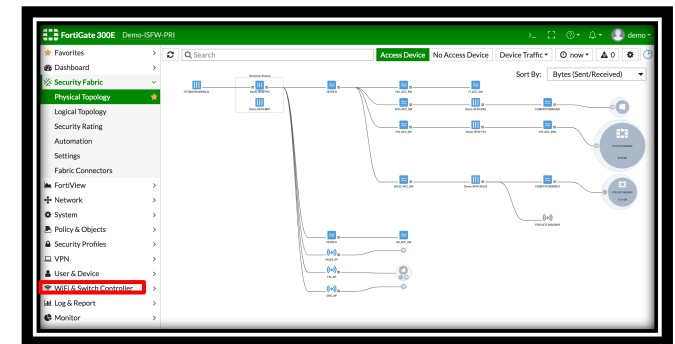
FortiSwitch Scales to support growth and higher bandwidth requirements

Security



Security Integrated into Ethernet Access through FortiLink

Management






















Single Interface to Manage Security, Access, and WAN.



FortiSwitch

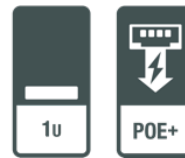
FortiSwitch Family

48 ports		 FSW-248E-FPOE	 FSW-448D-FPOE	 FSW-548D-FPOE		
		 FSW-248D/E-POE	 FSW-448D-POE			
		 FSW-248D	 FSW-448D	 FSW-548D	 FSW-1048E FSW-1048D	
32 ports					 FSW-3032E FSW-3032D	
24 ports		 FSW-124E-FPOE	 FSW-224D-FPOE	 FSW-424D-FPOE	 FSW-524D-FPOE	
		 FSW-124E-POE	 FSW-224E-POE	 FSW-424D-POE		
		 FSW-124E	 FSW-224E	 FSW-424D	 FSW-524D	
8 ports		 FSW-108E-FPOE				
		 FSW-108E-POE				
		 FSW-108E				
	100 Series	200 Series	400 Series	500 Series	1000/3000 Series	
	+ 2x GE SFP uplink (except FS-124E/-POE/-FPOE)	+ 4x GE SFP uplink	+ 2x10 GE SFP+ uplink	+ 4x 10 GE SFP+ and 2x 40 GE stacking	Data Center Switches	

FortiSwitch 400 Series



- ① 24x GE RJ45 POE/POE+ Ports
- ② 2x 10GE SFP slots



- ① 48x GE RJ45 POE/POE+ Ports
- ② 4x 10GE SFP slots



FS-424D-FPOE

FS-448D-FPOE

Switch Capacity	88 Gbps	176 Gbps
MAC Address Storage	16K	16K
Network Latency (64b)	<1 μ s	<1 μ s
VLANs Supported	4K	4K
Max LAG Size	up to 12 ports	up to 12 ports
PoE Power Budget	370 W	370 W
Power Supply	Single PS, Optional FRPS-740	Dual Redundant PS

F **ORTINET**®

6. FORTISWITCH SECURE SWITCHING

FortiSwitch Ethernet Access and Data Center Switches are a feature-rich yet cost-effective range of devices, supporting the needs of enterprise campus and branch offices, as well as data center environments.



The FortiSwitch Secure Access Switch series integrates directly into the FortiGate Connected UTM, with switch administration and access port security managed from the familiar FortiGate interface. Regardless of how users and devices connect to the network, you have complete visibility and control over your network security and access through this single pane of glass, perfectly suited to threat-conscious organizations of any size.

Virtualization and cloud computing have created dense high-bandwidth Ethernet networking requirements in the data center, pushing the limits of existing data center switching. FortiSwitch Data Center switches meet these challenges by providing a high performance 10 or 40 GbE capable switching platform, with a low Total Cost of Ownership. Ideal for Top of Rack server or firewall aggregation applications, as well as enterprise network core or distribution deployments, these switches are purpose-built to meet needs of today's bandwidth intensive environments.

Integrated Security	Pervasive Security through Fortinet Security Fabric Integration addressing the broadest threat surface.
Simplified Management	FortiGate integration creates one interface to manage security and access.
Scalable	Able to scale from desktop to datacenter across platforms allowing flexibility to grow as devices and traffic increase.

Highlights

Wide Range of Models – With 1 GbE, 10 GbE and 40 GbE models, as well as Power over Ethernet options, there is a FortiSwitch to suit any deployment scenario.

Power over Ethernet (PoE) – Simplifies the installation of PoE equipment in the network, eliminating the need for the installation of additional power sockets to support APs and VOIP handsets.

Flexible management – Various management capabilities are available including CLI, Web or directly from a connected FortiGate GUI.

Network Segmentation Support – You can configure a single physical switch to support the convergence of voice, data and wireless traffic, while still meeting compliance requirements.

40GbE Capability – Future proofed 40 GbE will meet the bandwidth requirements of even the most intensive data center and network core applications.

Port Level Network Access Security Features – Secure Access Switch Series devices enable true port level network access security with 802.1X technology, managed centrally from any FortiGate.

Offering Limited Lifetime Warranty (hardware replacement) - Refer to policy at Fortinet Warranty Policy: <http://www.fortinet.com/doc/legal/EULA.pdf>

Security Fabric – FortiSwitch devices are essential part of Fortinet's Security Fabric, offering visibility, user access control, and threat mitigation at the switch port level.

6.1 Secure Access Switches – Simple, Secure, Scalable Unified Access Layer Ethernet Switches

Outstanding network security, performance, and manageability

Single-pane-of-glass management through tight integration with the industry leading FortiGate using FortiLink

FortiSwitch Secure Access switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding security, performance and manageability for threat conscious small to mid-sized businesses, distributed enterprises and branch offices. Tightly integrated into the FortiGate® Network Security Platform, the FortiSwitch Secure Access switches can be managed directly from the familiar FortiGate interface. This single pane of glass management provides complete visibility and control of all users and devices on the network, regardless of how they connect.

When a device connects to a Secure Access Switch Ethernet port, it is first identified, and then the user is authenticated. Once authenticated, access to the network is granted based on pre-defined security policy from the FortiGate, ensuring secure network access across the enterprise, without impacting the user experience. If any attacks sent by the user is detected by FortiGate, the user can be quarantined on FortiSwitch to stop it from spreading malicious traffic to other hosts in the network.

Security Fabric Integration

Reduces complexity and decreases management cost with network security functions managed through a single console via FortiGate.

This integration allows all users to be authenticated against the same user database, regardless of whether they connect to the wired or wireless network, including temporary guest users.

In addition, same security policy can apply to a user or device regardless of how or where they connect to the network.

Models: FS-108D-POE, FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124D, FS-124D-POE, FS-224E, FS-224E-POE, FS-224D-FPOE, FS-248E, FS-248E-POE, FS-248E-FPOE, FS-424D, FS-424D-POE, FS-424D-FPOE, FS-448D, FS-448D-POE, FS-448D-FPOE, FS-524D, FS-524D-FPOE, FS-548D and FS-548D-FPOE.

Highlights

- Secure Access switches suitable for wire closet and desktop installations.
- Devices are identified and users authenticated prior to being granted access to the network.
- Security Fabric integration with actions taken on switch port level (user quarantine, Access VLAN, etc).
- Stackable up to 256 switches per FortiGate depending on model
- Centralized security management and reporting from FortiGate interface.
- Up to 48 ports in a compact 1 RU form factor.
- Power over Ethernet capable, including PoE+
- Ideal for converged network environments; enabling voice, data and wireless traffic to be delivered across a single network

Key Features & Benefits

Single Management Framework: Reduces complexity and decreases management cost with network security functions managed through a single console.

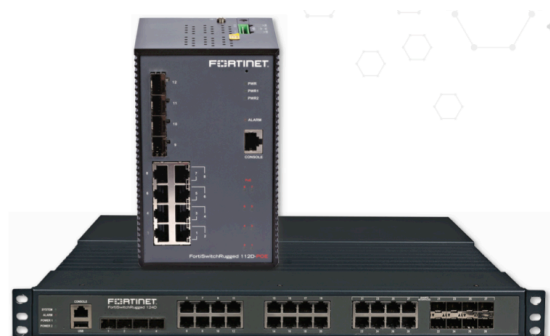
Single Policy Provisioning: The same security policy can apply to a user or device regardless of how or where they connect to the network. Enables access to certain network ports based on the role of a user within the organization, such as in shared conference rooms or engineering facilities.

Centralized Authentication: All users are authenticated against the same user database, regardless of whether they connect to the wired or wireless network, including temporary guest users.

Role-Based Ports: Enables access to certain network ports based on the role of a user within the organization, such as in shared conference rooms or engineering facilities.

6.1.1 FortiSwitch Rugged

FortiSwitch Rugged switches deliver all of the performance and security of the trusted FortiSwitch Secure, Simple, Scalable Ethernet solution, but with added reinforcement that makes them ideal for deployments in harsh outdoor environments.



Resilient, sturdy and capable of withstanding intense temperature fluctuations, FortiSwitch Rugged ensures the integrity and performance of mission-critical networks in even the most challenging of deployments.

Add Ruggedized FortiGate for Tough and Powerful Protection

Engineered to survive in hostile environments with an extreme temperature range, the combination of FortiGate Rugged network security appliances with the FortiSwitch Rugged provides a connected network security solution.

Simple Network Deployment

The Power over Ethernet (PoE) capability enables simple installation of cameras, sensors and wireless access points in the network, with power and data delivered over the same network cable.

There is no need to contract electricians to install power for your PoE devices, reducing your overall network TCO.

Highlights

- Mean time between failure greater than 25 years
- Fanless passive cooling
- DIN-rail or wall-mountable
- Power over Ethernet capable including PoE+
- Redundant power input terminals
- Controlled by FortiGate

Key Features and Benefits

Sturdy IP30 construction	Built to ingress protection 30 standards, the construction is designed to perform while enduring hostile conditions.
Passive cooling	With no fan and no moving parts, the mean time between failure is greater than 25 years.
Redundant power inputs	Maximizes network availability by eliminating the downtime associated with failure of a power input.
Power over Ethernet capability	Seamless integration of peripheral devices such as cameras, sensors and wireless access points into the network.

Models: FSR-112D-POE, FSR-124D

See datasheet environmental and compliance information.

6.2 Data Center Switches – High Performance Switching with Data Center Capabilities

Outstanding throughput, resiliency, and scalability

Single-pane-of-glass management through tight integration with FortiGate using FortiLink

FortiSwitch Data Center switches deliver a Secure, Simple, Scalable Ethernet solution with outstanding throughput, resiliency and scalability for organizations with high performance network requirements. They are ideal for Top of Rack server or firewall aggregation applications, as well as enterprise network core or edge deployments, where high performance 10 GE or 40 GE is required. Purpose-built to meet the needs of today's bandwidth intensive data centers and enterprise networks, FortiSwitch Data Center switches deliver high-performance with a low Total Cost of Ownership.

Security Fabric Integration

Reduces complexity and decreases management cost with network security functions managed through a single console via FortiGate.

This integration allows all users to be authenticated against the same user database, regardless of whether they connect to the wired or wireless network, including temporary guest users.

In addition, same security policy can apply to a user or device regardless of how or where they connect to the network.

High-performance and resilient managed data center switch

Designed in a compact 1 RU form factor, FortiSwitch Data Center switches are equipped with dual hot swappable power supplies to maximize network uptime. With 10 GE access ports and a high-throughput backplane, the FortiSwitch Data Center switches satisfy the Top of Rack server or firewall aggregation performance requirements of today's virtualization centric data centers. Advanced Link Aggregation with 802.3ad, Link Aggregation Control Protocol (LACP) and Multi-Chassis Link Aggregation Groups (MCLAG) provide increased uplink, server aggregation, or firewall aggregation throughput. Other advanced switch capabilities, such as large MAC address tables, jumbo frame support and port security, are standard features. The high-speed switching fabric is also well suited to enterprise network core or backbone network installations. FortiSwitch Data Center switches are a future-proof investment, providing the flexibility of deploying 1 GE, 10 GE or even 40 GE if required.

Models: FS-1024D, FS-1048D, FS-3032D

Highlights

- High capacity switch suitable for Top of Rack or enterprise network deployments.
- Stackable up to 256 switches per FortiGate depending on model
- Maximum availability through dual hot swappable power supplies.
- Simply management via web-based or command line interface.
- Switch security features protect vulnerable infrastructure without adding latency.

- 1 GE or 10 GE access ports, in a compact 1 RU form factor.
- 40 GE capability options.

Key Features and Benefits

10 GE Capability: Future-proofed 10 GE to satisfy the bandwidth requirements of intensive data center and network core applications.

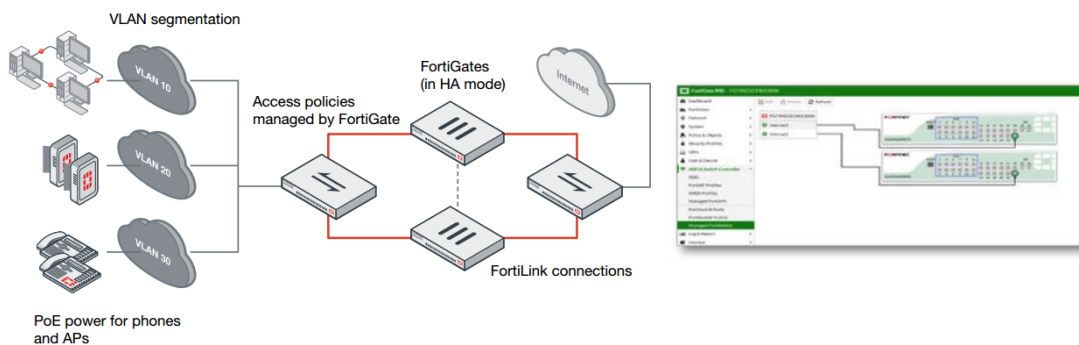
Dual Power Supply Units: Maximizes network availability by eliminating the downtime associated with single power supplies.

FortiLink, Web and CLI Management: Configuration and visibility into the network is made simple via FortiLink, web-based interface or CLI.

6.3 Deployment Options

6.3.1 FortiLink Mode

The FortiSwitch Secure Access Switch series integrates directly into the FortiGate* Connected UTM, with switch administration and access port security managed from the familiar FortiGate interface. Regardless of how users and devices connect to the network, you have complete visibility and control over your network security and access through this single pane of glass, perfectly suited to threat conscious organizations of any size. (* selected models only)



FortiLink Advantages

Feature	Fortilink Advantage
Auto Discovery	FortiGate discovers FortiSwitch without need of additional configuration
Segment Network Centrally	With FortiGate it becomes simple to attach policies to ports

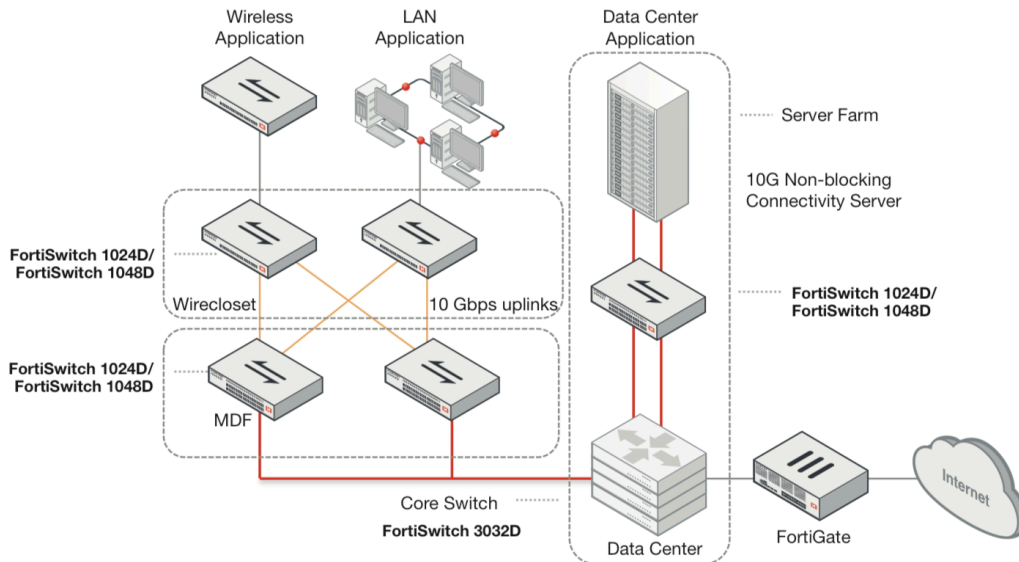
Upgrade Image	FortiGate upgrades FortiSwitchOS
Zero-touch provisioning	FortiGate automatically authorizes and configures FortiSwitch
Security Fabric Integration	Security applied to the switch port – FortiSwitch is simple extension to FortiGate
Wired and Wireless Central Control	FortiGate as central Switch+Wireless controller
POE Management	Control power budget centrally
Centralized Authentication	All users are authenticated against the same user database
Centralized Management	Use FortiManager to centrally manage FGts and corresponding managed FortiSwitch
Stack	Control up to 256 FortiSwitch from the same FGT GUI

Capabilities: FortiLink Mode

FORTISWITCH FORTILINK MODE (WITH FORTIGATE)	
Management and Configuration	
Auto Discovery of Multiple Switches	Yes
Number of Managed Switches per FortiGate	8 to 256 Depending on FortiGate Model (Please refer to admin-guide)
FortiLink Stacking (Auto Inter-Switch Links)	Yes
Software Upgrade of Switches	Yes
Centralized VLAN Configuration	Yes
Switch POE Control	Yes
Link Aggregation Configuration	Yes
Spanning Tree	Yes
LLDP/MED	Yes
IGMP Snooping	Yes (not supported on 108D-POE, 224D-POE, 1xxE-Series)
L3 Routing and Services	Yes (FortiGate)
Policy-Based Routing	Yes (FortiGate)
Virtual Domain	Yes (FortiGate)
Security and Visibility	
802.1x Authentication (Port-based, MAC-based, MAB)	Yes
Syslog Collection	Yes
DHCP Snooping	Yes
Device Detection	Yes
MAC Black/White Listing	Yes (FortiGate)
Policy Control of Users and Devices	Yes (FortiGate)
UTM Features	
Firewall	Yes (FortiGate)
IPC, AV, Application Control, Botnet	Yes (FortiGate)
High Availability	
Support FortiLink FortiGate in HA Cluster	Yes
LAG support for FortiLink Connection	Yes
Active-Active Split LAG from FortiGate to FortiSwitches for Advanced Redundancy	Yes (with FS-2xx, 4xx, 5xx)

6.3.2 Standalone Mode

Virtualization and cloud computing have created dense high-bandwidth Ethernet networking requirements in the data center, pushing the limits of existing data center switching. FortiSwitch Data Center switches meet these challenges by providing a high performance 10 or 40 GE capable switching platform, with a low Total Cost of Ownership. Ideal for Top of Rack server or firewall aggregation applications, as well as enterprise network core or distribution deployments, these switches are purpose-built to meet the needs of today's bandwidth intensive environments.

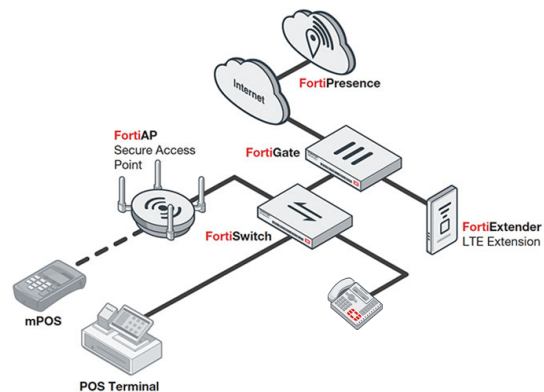


6.5 Solution Integration

Retail

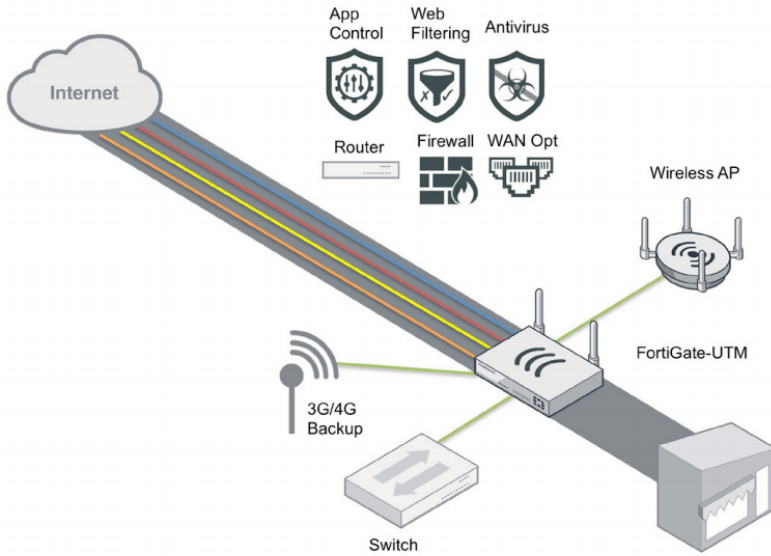
FortiSwitch integrates with Fortinet's complete solution for retail business. Benefits:

- Cost reduction
- Standardization
- Easy deployment in high scale
- Visibility
- Easily adapt to new retail tech



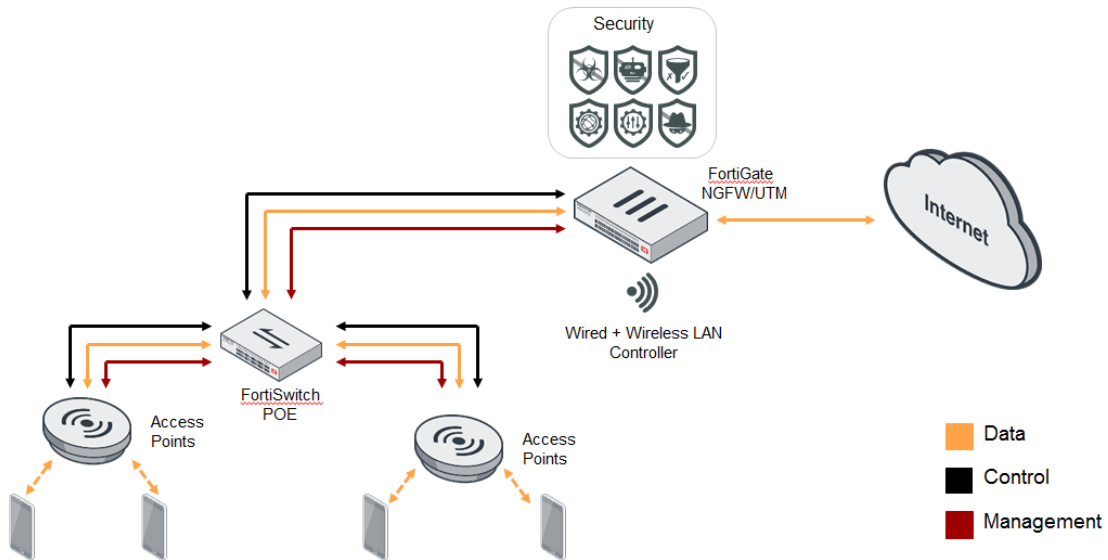
Connected UTM

FortiSwitch integrates with Connected UTM solution providing extended connectivity and POE for SMB deployments. With FortiLink, FortiSwitch becomes an extension to FortiGate and it's possible to easily enforce policies for all of the different wired and wireless devices, kiosks, systems, and terminals in the network from a "single pane of glass".



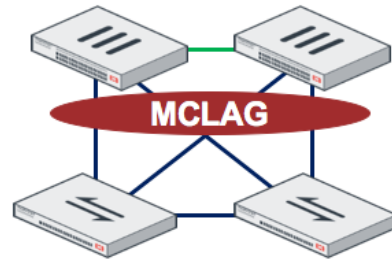
Secure Access Architecture

FortiSwitch integrates with Secure Access Architecture solution providing network infrastructure necessary to interconnect wired and wireless. It also provides POE to power wireless access points and other devices in the network. The complete network can be controlled via FortiGate in a “single pane of glass”.



FortiGate in HA

With the use of MCLAG, FortiGate HA pair can be connected in full mesh to FortiSwitch pair, providing complete link and switch level redundancy to the security solution.



Supported in FortiLink or Standalone mode.

7. FORTISWITCH COMMON REQUIREMENT SPECIFICATIONS AND ANSWERS

Use the following list to help answering RFP questions and, when possible, to tailor RFPs to Fortinet’s favor. For supported models, check feature matrix in release notes. For physical/environmental specifications, refer to datasheets. For any unsupported feature, consult your regional SME/CSE.

7.1. General system requirements

Requirement	FortiLink	Standalone	Response
MUST support simple management access i.e. without the need for local management clients (HTTPS preferred)	Yes	Yes	Fully Compliant: FortiSwitch has a CLI however this is for initial setup and includes some debugging commands for convenience. All configuration and management of the platform is web based using standard browsers.
MUST support SNMP for polling of system statistics	Yes	Yes	Fully Compliant: FortiSwitch supports SNMP v1, v2c and v3. FortiSwitch MIBs are available for download from the Fortinet Technical Support web site.
MUST support SNMP Traps for key system thresholds (specify)	Yes	Yes	Fully Compliant: FortiSwitch supports configurable SNMP TRAPS for key system thresholds.
MUST support SNMP MIB download from system GUI	Yes	Yes	Fully Compliant: FortiSwitch MIBs are available in the GUI.
MUST display a visual representation of authentication in the GUI	Yes	Yes	Fully Compliant: FortiSwitch includes a “Logout” button showing that user is logged in the system and offering the option to logout.
MUST log all authentication events:			

Locally	Yes	Yes	Fully Compliant: All authentication attempts are logged to the local file system under Event logs with the sub-type “admin” with details of the authenticating system, username, disposition (success, failed) and details of any failure. Local logs can be stored up to maximum file size specified by the administrator, at which point the file overwritten or logging stops.
Via syslog	Yes	Yes	Fully Compliant: Logs can be automatically replicated out to multiple external SYSLOG in their entirety or selectively based on the SYSLOG level and facility. Logs are automatically exported to FortiGate in FortiLink mode.
MUST be simple to install, manage and upgrade	Yes	Yes	Fully Compliant: FortiSwitch is delivered in a fully self-contained appliance format consisting of a hardened OS and all preconfigured applications. FortiSwitch requires simple initial CLI configuration. Following installation, all configuration is performed via a simple web based GUI. All upgrades to the OS and application are performed via the upload of a firmware package available from the Fortinet Support Web Site. The file is simply downloaded to the desktop and uploaded to the appliance.
MUST support backup of the full system configuration via the GUI	Yes , as part of FortiGate config	Yes	Fully Compliant: Configuration can be backed up via the GUI.
MUST support a local user database	Yes , from FortiGate No need to login to the FSW	Yes	Fully Compliant: FortiSwitch allows configuration of multiple administrator accounts and corresponding access profiles to restrict permissions per configuration sub-system.
MUST support remote authentication users (LDAP, RADIUS and/or TACACS+)	No	Yes	Fully Compliant: FortiSwitch allows the configuration to remote authenticate users’ logins. For full details on parameters please refer to the FortiSwitchOS admin guide.
MUST have built-in tcpdump-like tool and log collecting functionality	Yes	Yes	Fully Compliant: Packet Capture and diagnose features in CLI offer similar packet capture capabilities like tcpdump.

MUST support REST API for configuration and monitoring	Yes	Yes	Fully Compliant: Based on JSON API.
MUST support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback.	Yes	Yes	Fully Compliant: Configuration backup/restore and alternate boot partition
MUST support dual power supply	Yes	Yes	Available on: FS-424D, FS-448D, FS-448D-FPOE, FS-5xx, FS-10xxD, FS-3032D
MUST support external RPS	Yes	Yes	Available on: FS-124D-POE, FS-224D-FPOE, FS-248D-FPOE, FS-424D-POE, FS-424D-FPOE, FS-448D-POE, FS-224E-POE, FS-248E-POE, FS-248E-FPOE
MUST support breakout cables (40G to 4x10G)	No	Yes	FS-5xx and FS-3xxx models
MUST offer hardware lifetime warranty	Yes	Yes	
MUST support auto-ranging power supply with input voltages between 100 and 240V AC	Yes	Yes	
MUST support 802.3ah (100BASE-X single/multimode fiber only)	Yes	Yes	Supported on 108D-POE/112D-POE/224D-POE
MUST support 802.3az for energy efficient Ethernet	No	No	

7.2. Layer 2 Requirements

Requirement	FortiLink	Standalone	Response
MUST support jumbo frames	Yes	Yes	Max frame size = 9216
MUST support link auto-negotiation	Yes	Yes	Fully Compliant: 10G ports work also at 10/100/1000 speeds
MUST support manual link negotiation	Yes, CLI	Yes	Fully Compliant
MUST support Spanning Tree Protocol	Yes	Yes	Fully Compliant: MSTP (802.1s) native, and backwards compatible with RTSP (802.1w) and STP (802.1d)
MUST support Edge Port / Port Fast	Yes	Yes	
MUST support STP Root Guard	Yes	Yes	
MUST support BPDU Guard	Yes	Yes	
MUST support IEEE 802.1p Mapping to priority queue	Yes	Yes	

MUST support IEEE 802.1q VLAN tagging	Yes	Yes	
MUST support 4096 VLANs	Yes	Yes	
MUST support Private VLAN	Yes	Yes	Except on FS-108D-POE and FS-224D-POE In FortiLink mode, Access VLAN
MUST support IEEE 802.3ad Link Aggregation with LACP	Yes	Yes	Fully Compliant: maximum number of link members depends on model
MUST support load balancing algorithms with Link Aggregation	Yes	Yes	Fully Compliant: dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac
MUST support MCLAG (MultiChassis Link Aggregation)	Yes	Yes	FOS 5.6.0 FSWOS 3.6.0 Not supported on FS-1xx models
MUST support Automatic Negotiation of Trunking Protocol, to help minimize the configuration & errors	Yes	No	Supported if managed by FGT, all ISLs are automatically provisioned
MUST support MVR (Multicast VLAN Registration)	No	No	
MUST support load balancing algorithms with Link Aggregation	Yes	Yes	Fully Compliant: dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac
MUST support virtual wire	Yes, CLI only	Yes	
MUST support full line rate without traffic oversubscription	Yes	Yes	Available on all models: non-blocking, store-n-forward architecture
MUST support low latency mode (cut-through)	No	Yes	Available on models: FS-10xxD and FS-3032D
MUST support Ethernet protection mechanisms (IEEE 802.3ah or ITU-G.8031/8032)	No	No	Check with CSE/PM for potential feasibility
MUST support Shortest Path Bridging (SPB IEEE 802.1aq)	No	No	Check with CSE/PM for potential feasibility
MUST support Unidirectional Link Detection (UDLD)	No	No	Cisco proprietary Use stp-loop-protection instead Or single member LAG with LACP Or Ethernet OAM (802.3ah) (roadmap)
MUST support DCB (802.1Qbb and 802.1Qaz)	No	No	

7.3. Management requirements

Requirement	FortiLink	Standalone	Response
MUST support zero-touch provisioning	Yes	No	Auto-discovery of switches
MUST support stacking	Yes	No	FortiGate is the stack controller, with single pane of glass.
MUST support stacking topology auto-discovery	Yes	No	
MUST support firmware update from a central point	Yes	No	
MUST support end device identification	Yes	No	
MUST support integration with Fortinet Security Fabric	Yes	No	
MUST support complete view of all switching solution from a single pane of glass	Yes	No	
MUST support 802.1x MAC-based authentication	Yes	Yes	
MUST support MAC Authentication Bypass (MAB)	Yes	Yes	
MUST support Time-Domain Reflectometry (TDR) Support	No	Yes	Except FS-108D-POE, FS-224D-POE
MUST support telnet/SSH	Yes	Yes	
MUST support SNMP	Yes	Yes	
MUST support firmware download via TFTP/FTP/GUI	Yes	Yes	
MUST support RMON I and II standards	No	No	
MUST support Centralized VLAN Management. VLANs created on the Core Switches should be propagated automatically	Yes	No	
MUST support MAC address notification	No	No	
MUST support Bridge MIB (RFC-1493)	Yes	Yes	
MUST support POE MIB (RFC 3621)	No	No	

7.4. Authentication Requirements

Requirement	FortiLink	Standalone	Response
MUST support LLDP	Yes	Yes	

MUST support LLDP-MED	Yes	Yes	MED-TLVs: inventory and network policy
MUST support MAC based VLAN assignment (802.1v)	Yes, CLI only	Yes	
MUST support IP based VLAN assignment (802.1v)	Yes, CLI only	Yes	
MUST support protocol based VLAN assignment (802.1v)	Yes, CLI only	Yes	
MUST support 802.1x port-based authentication	Yes	Yes	
MUST support 802.1x authentication via certificate EAP-TLS and EAP-TTLS	Yes	Yes	
MUST support 802.1x guest VLAN assignment	Yes	Yes	
MUST support 802.1x authentication fail VLAN for unauthenticated users	Yes	Yes	
MUST support 802.1x MAC-based authentication	Yes	Yes	
MUST support MAC Authentication Bypass (MAB)	Yes	Yes	
MUST support captive portal	Yes	No	
MUST support LDAP	No	Yes	
MUST support RADIUS	Yes	Yes	
MUST support RADIUS Accounting	Yes, CLI only	Yes	
MUST support RADIUS Change of Authorization (CoA)	No	Yes	
MUST support TACACS+	No	Yes	

7.5. POE Requirements

Requirement	FortiLink	Standalone	Response
MUST display total POE power consumption	Yes	Yes	
MUST display per port POE power consumption	Yes	Yes	
MUST support POE port enable/disable	Yes	Yes	
MUST support POE port reset	Yes	Yes	
MUST support IEEE 802.3af	Yes	Yes	

MUST support IEEE 802.3at (POE+)	Yes	Yes	All "-POE" and "-FPOE" models except FS-108D-POE and FS-224D-POE
---	------------	------------	--

7.6. Layer 3 Requirements

Requirement	FortiLink	Standalone	Response
MUST support static routing	Yes, via FortiGate	Yes	
MUST support line rate L3 forwarding	Yes, via FortiGate	Yes	Refer to release notes for supported models
MUST support RIPv2	Yes, via FortiGate	Yes	Requires Advanced license. Not supported on FS-1xx models.
MUST support OSPFv2	Yes, via FortiGate	Yes	Requires Advanced license. Not supported on FS-1xx models.
MUST support BGP	Yes, via FortiGate	Roadmap	
MUST support VRRP	Yes, via FortiGate	Yes	Requires Advanced license. Not supported on FS-1xx models.
MUST support IGMP	Yes, via FortiGate	Roadmap	
MUST support PIM	Yes, via FortiGate	Roadmap	
MUST support ECMP	Yes, via FortiGate	Yes	
MUST support BFD	No	Yes	
MUST support GRE	No	No	
MUST support L2TP	No	No	
MUST support MPLS, MPLS-TP	No	No	
MUST support ISIS	No	Roadmap	

7.7. Security

Requirement	FortiLink	Standalone	Response
MUST support Storm Control	Yes, CLI only	Yes	
MUST support LoopGuard	Yes	Yes	
MUST support IGMP snooping	Yes	Yes	
MUST support IGMP querier	Yes	Yes	
MUST support DHCP snooping	Yes	Yes*	
MUST support DHCP relay	Yes, via FortiGate	Yes	Includes option 82

MUST support DHCP server	Yes, via FortiGate	No	
MUST support Port mirroring	Yes, CLI only	Yes	
MUST support sFlow	Yes, CLI only	Yes	
MUST support ACL	Yes, CLI only	Yes	
MUST support ACL classifier	Yes, CLI only	Yes	Fully Compliant: src-mac, dst-mac, ether-type, src-prefix, dst-prefix, service-id, vlan-id
MUST support ACL drop action	Yes, CLI only	Yes	
MUST support ACL policer action	Yes, CLI only	Yes	
MUST support ACL counter action	Yes, CLI only	Yes	
MUST support ACL mirror action	Yes, CLI only	Yes	
MUST support ACL redirect action	Yes, CLI only	Yes	
MUST support security checks	Yes, CLI only	Yes	<p>sip-eq-dip - TCP packet with Source IP equal to Destination IP.</p> <p>tcp_flag - DoS attack checking for TCP flags.</p> <p>tcp-port-eq TCP packet with Source and destination TCP port equal</p> <p>tcp-flag-FUP - TCP packet with FIN, URG and PSH flags set, and sequence number is zero.</p> <p>tcp-flag-SF - TCP packet with SYN and FIN flag set.</p> <p>v4-first-frag - DoS attack checking for IPv4 first fragment.</p> <p>udp-port-eq - IP packet with source and destination UDP port equal.</p> <p>tcp-hdr-partial - TCP packet with partial header.</p> <p>macsa-eq-macda - Packet with source MAC equal to Destination MAC.</p>
MUST support port MAC limit	Yes, CLI only	Yes	
MUST support MAC-IP binding	Yes	Yes	Map a MAC address to an IP address to avoid untrusted hosts
MUST support static MAC	Yes	Yes	Map a MAC address to a port to avoid flooding
MUST support Dynamic ARP Inspection	Yes, CLI only	Yes	

MUST support Sticky Mac	Yes, CLI only	Yes	
--------------------------------	----------------------	------------	--