NETGEAR®

ProSAFE® LAN Access and Aggregation Chassis Switches

Data Sheet

M6100 series

The NETGEAR® LAN Access and Aggregation Chassis M6100 series delivers L2/L3/L4 and IPv4/IPv6 rich services for enterprise edge and SMB core deployments, as well as 1G/10G mixed infrastructures in server rooms. Innovative distributed fabric provides non-stop forwarding resiliency and world-class availability - including passive backplane, hitless failover, redundant fabric and redundant management - without having to pay the exorbitant acquisition and maintenance costs associated by other networking vendors in this class. NETGEAR Lan Access and Aggregation Chassis Switch solutions combine the latest advances in hardware and software engineering for higher flexibility, lower complexity and stronger investment protection, at a high-value price point.

Highlights

Word-class availability

- Dependable continuity of operations with non-stop switching, non-stop routing and hitless failover supported for both fabric and management
- N+1 redundancy for power supplies and loop-free, disruption-free multi-chassis link aggregation (MLAG)

High speed performance

- 1.4 Tbps total routing/switching capacity and up to 1,071 Mpps intra-blade throughput
- 480 Gbps distributed fabric inter-module with each slot providing 2 x 40G access to the passive backplane (80G half-duplex; 160G full-duplex)

Extra high-density

- Only 4U height (7 inches - 17.59cm) and 17.39 inches depth (44.16cm)
- Supports 144 RJ45 10/100/1000 ports, or 120 SFP 100/1000 ports, or 72 RJ45 10GBASE-T ports, or 48 SFP+ 1000/10GBASE-X ports, or a combination

Higher flexibility

- Distributed fabric removes the need for a dedicated supervisory module yet provides passive backplane, redundant fabric and redundant management
- Any I/O blade spares hardware and software distributed fabric on board, facilitating campus management, maintenance and upgrades

Lower complexity

- Entire feature set including datacenter (DCBX, PFC, ETS, FIP Snooping) and advanced IPv6 L3 routing (OSPF, PBR, BGP) is available without a license
- Innovative slot-1 supervisory and slot-2 backup supervisory design simplifies the entire chassis installation and ongoing maintenance tasks

Investment protection

- Multi-role versatile platform engineered for cost-effective Gigabit edge, flexible Gigabit/10 Gigabit distribution and scalable 10 Gigabit core applications
- Any Gigabit copper blade can be upgraded with PoE+ 30W or UPOE 60W daughter card and downgraded later if the application has changed

Industry standard management

- Industry standard command line interface (CLI), functional NETGEAR web interface (GUI), SNMP, sFlow and RSPAN
- Single-pane-of-glass NMS300 management platform with centralized firmware updates and mass-configuration support

Industry leading warranty

- NETGEAR M6100 series is covered under NETGEAR ProSafe Lifetime Hardware Warranty*
- 90 days of Technical Support via phone and email, Lifetime Technical Support through online chat and Lifetime Next Business Day hardware replacement

NETGEAR®

ProSAFE® LAN Access and Aggregation Chassis Switches

Data Sheet

M6100 series

Software at a Glance

	LAYER 3 PACKAGE											
Model Name	Management	IPv4/IPv6 ACL and QoS, DiffServ	IPv4/IPv6 Multicast Filtering	IPv4/IPv6 Policing and Convergence	Spanning Tree Green Ethernet	VLANs	Trunking Port Channel	IPv4/IPv6 Authentication Security	IPv4/IPv6 Static Routing	IPv4/IPv6 Dynamic Routing	Datacenter Features*	Model Number
M6100-3S	Out-of-band; Web GUI; HTTPs CLI; Telnet; SSH SNMP, MIBs RSPAN	Ingress/egress 1 Kbps shaping Time-based Single Rate Policing	IGMPv3 MLDv2 Snooping + Querier Control Packet Flooding	Auto-VoIP Auto-iSCSI Policy-based routing (PBR) LLDP-MED	STP, MTP, RSTP PV(R)STP* BPDU/STRG Root Guard EEE (802.3az)	Static, Dynamic, Voice, MAC GVRP/ GMRP QinQ, Private VLANs	Distrib-uted LAG across all I/O slots MLAG across two chassis switches	Successive Tiering (DOT1X; MAB; Captive Portal) DHCP Snooping IP Source Guard	Port, Subnet, VLAN routing, DHCP Relay; Multicast static routes; Stateful DHCPv6 Server	IPv4: RIP, VRRP IPv4/IPv6: OSPF, BGP*, Proxy ARP, PIM-SM PIM-DM, 6-to-4 tunnels	DCBX (802.1Qaz) Priority Flow Control (PFC) Enhanced Transmission Selection (ETS) FCoE FIP Snooping	XCM8903

* CLI only

Performance at a Glance

	TABLE SIZE										
Model Name	Passive Backplane	Fabric Speed	Routing/ Switching Capacity	Throughput	High Availability	Packet Buffer CPU Latency	MAC; ARP/ NDP VLANs ; DHCP	Application Route Scaling	Multicast IGMP Group Membership	IP Multicast Forwarding Entries	sFlow	Model number
M6100-3S	Each Slot provides 2 x 40G access to the backplane 80G half-duplex 160G full-duplex per slot	480 Gbps Inter-Module Distributed Fabric	1.4 Tbps Intra-Module Each Line-Card provides local line-rate capacity	357 Mpps Inter-Module 1,071 Mpps Intra-Module	Dual Supervisory Modules Fabric and Management Nonstop Forwarding Failover (NSF)	1G/10G Blades: 32Mb/72Mb Packet Buffer CPU 800 Mhz 1GB RAM 64MB Flash Latency 3.7µs 10G RJ45 1.5µs 10G SFP+	32K MAC 8K ARP/NDP ARP: 1.2kpps 4K VLANs DHCP: 4K leases in 256 pools	Static: 512 RIP: 512 OSPF and BGP: 12,000 routes	2K IPv4 2K IPv6	1.5K IPv4 512 IPv6	32 samplers 52 pollers 8 receivers	XCM8903

Each Line Card provides line-rate switching and routing capacity. Each Slot provides 2 x 40G channels (80G half-duplex /160G full-duplex) access to passive backplane.

Hardware at a Glance

		FRONT		REAR		SIZE		
Model name	Form-Factor	I/O Slots	PSU Bay	Fan Tray	External PSU Bay	Height	Depth	Model number
M6100-3S	Chassis	3 open line-card slots	4 power supply slots (N+1)	1 fan tray slot (front-to-back)	Connectors RPS/EPS	4U height 6.93 in (17.59 cm)	17.39 in (44.16 cm)	XCM8903
		Passive backplane; management and fabric 1+1 redundancy with hitless failover and non-stop forwarding. Supports a maximum of 144 RJ45 10/100/1000 ports or 120 SFP 100/1000 ports, 72 RJ45 10GBASE-T ports or 48 SFP+ 1000/10GBASE-X ports, or a combination.						

		LINE-CARDS								
Model name	Form-Factor	10/100/ 1000BASE-T RJ45 ports	100/1000X Fiber SFP ports	100/1000/ 10GBASE-T RJ45 ports	1000/10GBase-X Fiber SFP+ ports	POE+ or UPOE upgradeable	Out-of-band Management (Ethernet)	Management Console (Serial)	Storage (image, config, log files)	Model number
XCM8948	I/O Blade	48	-	-	-	Yes	1 x RJ45 Ethernet OOB 10/100/1000 (service port)	1 x RJ45 RS232 (straight-through wiring) 1 x Mini-USB	1 x USB	XCM8948
XCM8944	I/O Blade	40	-	2	2 (independent)	Yes				XCM8944
XCM8944F	I/O Blade	-	40	2	2 (independent)	-				XCM8944F
XCM8924X	I/O Blade	-	-	24	16 (shared with 10GBASE-T)	-				XCM8924X

		ACCESSORIES	
Model name	Form-Factor	Notes	Model number
XCM89P	Daughter Card	Add PoE+ 802.3at functionality to XCM8948 and XCM8944 blades (1 daughter card per blade required; up to 30W per 1G RJ45 port; backward compatible with PoE)	XCM89P
XCM89UP	Daughter Card	Add UPOE functionality to XCM8948 and XCM8944 blades (1 daughter card per blade required; up to 60W per 1G RJ45 port; backward compatible with PoE+/PoE)	XCM89UP
APS1000W	Power Supply	PSU 1,000W AC (up to four PSUs in M6100-3S chassis; up to four more PSUs in RPS4000v2 external power supply bay)	APS1000W
AFT603	Fan Tray	Fan Tray for M6100-3S chassis (front-to-back cooling principle; one fan tray per chassis required)	AFT603
RPS4000v2	External PSU Bay	Additional 1U power shelf (RPS/EPS unit with four open power supply slots)	RPS4000v2

NETGEAR®

ProSAFE® LAN Access and Aggregation Chassis Switches

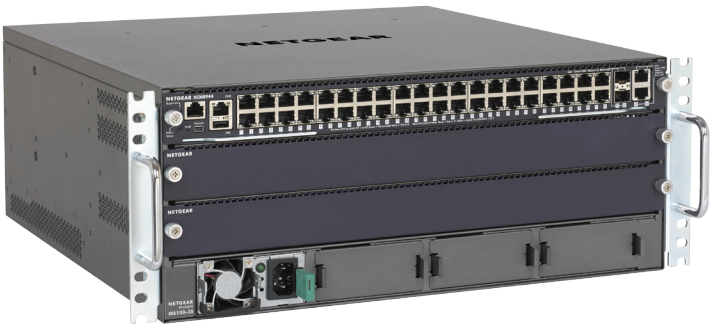
Data Sheet

M6100 series

Hardware at a Glance

	POWER OVER ETHERNET											
	110V AC in						220V/230V/240V AC in					
Examples of configuration	1 x XCM8944 1 x daughter card XCM89P / XCM89UP		1 x XCM8944 1 x XCM8948 2 x daughter cards XCM89P or XCM89UP		1 x XCM8944 2 x XCM8948 3 x daughter cards XCM89P or XCM89UP		1 x XCM8944 1 x daughter card XCM89P / XCM89UP		1 x XCM8944 1 x XCM8948 2 x daughter cards XCM89P or XCM89UP		1 x XCM8944 2 x XCM8948 3 x daughter cards XCM89P or XCM89UP	
(Watts)	PoE Budget N / N+1	**40 ports** PoE+ or UPOE	PoE Budget N / N+1	**88 ports** PoE+ or UPOE	PoE Budget N / N+1	**136 ports** PoE+ or UPOE	PoE Budget N / N+1	**40 ports** PoE+ or UPOE	PoE Budget N / N+1	**88 ports** PoE+ or UPOE	PoE Budget N / N+1	**136 ports** PoE+ or UPOE
4U height - 1 x PSU	570W/ -	14.2W per port	510W/ -	5.7W per port	450W/ -	3.3W per port	840W/ -	21W per port	780W/ -	8.8W per port	720W/ -	5.2W per port
4U height - 2 x PSU	1050W/570W	26.2W per port	990W/510W	11.2W per port	930W/450W	6.8W per port	1470W/840W	36.7W per port	1410W/780W	16W per port	1350W/720W	9.9W per port
4U height - 3 x PSU	1610W/1050W	40.2W per port	1550W/990W	17.6W per port	1490W/930W	10.9W per port	2240W/1470W	56W per port	2180W/1410W	24.7W per port	2120W/1350W	15.5W per port
4U height - 4 x PSU	2170W/1610W	54.2W per port	2110W/1550W	23.9W per port	2050W/1490W	15W per port	3010W/2240W	60W per port	2950W/2180W	33.5W per port	2890W/2120W	21.2W per port
5U height - 5 x PSU	2730W/2170W	60W per port	2670W/2110W	30.3W per port	2610W/2050W	19.1W per port	3780W/3010W	60W per port	3720W/2950W	42.2W per port	3660W/2890W	26.9W per port
5U height - 6 x PSU	3290W/2730W	60W per port	3230W/2670W	36.7W per port	3170W/2610W	23.3W per port	4550W/3780W	60W per port	4490W/3720W	51W per port	4430W/3660W	32.5W per port
5U height - 7 x PSU	3850W/3290W	60W per port	3790W/3230W	43W per port	3730W/3170W	27.4W per port	5320W/4550W	60W per port	5260W/4490W	59.7W per port	5200W/4430W	38.2W per port
5U height - 8 x PSU	4410W/3850W	60W per port	4350W/3790W	49.4W per port	4290W/3730W	31.5W per port	6090W/5320W	60W per port	6030W/5260W	60W per port	5970W/5200W	43.8W per port

Visit www.netgear.com/m6100 and download "M6100 basic configurator", or "M6100 expert configurator" files under Resources tab for tailored design and error-free SKU list.



For illustration only: Starter Kit is not pre-assembled.
Starter kit components ship in their individual packaging.
Shipping master carton arrives on a pallet.

Starter Kit

M6100-44G3-POE+ is M6100 series chassis Starter Kit

- 1 empty chassis M6100-3S (XCM8903)
- 1 blade 40x1G + 4x10G (XCM8944)
- 1 PoE+ daughter card (XCM89P)
- 1 power supply unit (APS1000W)
- 1 fan tray front to back (AFT603)
- 2 blank panels for open blade slots
- 3 power supply panels for empty PSU slots
- Rack-mount kit for 2-post racks and wiring cabinets
- Complimentary handles for rack-mount kit
- Complimentary sliding rails kit for 4-post racks and wiring cabinets

Ordering SKU number (worldwide):
XCM8903SK-10000S

NETGEAR®

ProSAFE® LAN Access and Aggregation Chassis Switches

Data Sheet

M6100 series

Product Brief

The M6100 switch series consists of Gigabit access layer and 10 Gigabit distribution layer switches in the NETGEAR modular chassis switch product line. The M6100 switch series offers high-quality, high-density chassis alternative to stackable switches in campus LAN and midsize organizations demanding networks. With more than 1.4 Tbps switching and routing capacity, passive backplane, management and fabric nonstop forwarding redundancy, the M6100 series delivers world-class resiliency and scalability. Ultimately, operating software and system management features take the complexity out of delivering L2/L3/L4 rich services for enterprise edge and SMB core deployments.

NETGEAR M6100 series key features:

- Proficient access layer in campus LAN networks, and competent distribution or core layer for midsize organizations networks
- Advanced Layer 2, Layer 3 and Layer 4 feature set - no license required - including PBR, BGP, DCBX, PFC, ETS and FCoE FIP
- Innovative distributed fabric, with nonstop forwarding and hitless failover redundancy between supervisory I/O modules
- Up to 144 (Gigabit) ports, or 72 (10 Gigabit) ports, or a combination of both in dense form factor models
- PoE+ (30 watts per port) and UPOE (60 watts per port) modular, flexible implementation
- Ultra-low latency and scalable table size with 32K MAC, 8K ARP/NDP, 4K VLANs, 12K routes

NETGEAR M6100 series PoE features:

- Any Gigabit copper blade can receive PoE+ or UPOE daughter cards for easy upgrade/downgrade and best investment protection
- Up to 3,000W PoE budget is provided by internal power supplies when 6,000W are available with additional 1U power shelf
- All set for rapid proliferation of PoE/PoE+ devices, such as IP telephony endpoints, 802.11n / 802.11ac access points and IP security cameras
- Future-proof 60W UPOE power delivered to next-gen VDI clients or physical security devices; UPOE is backward compatible with PoE/PoE+

NETGEAR M6100 series software features:

- Advanced classifier-based, time-based hardware implementation for L2 (MAC), L3 (IP) and L4 (UDP/TCP transport ports) security and prioritization
- Voice VLAN with SIP, H323 and SCCP protocols detection and LLDP-MED IP phones automatic QoS and VLAN configuration
- Efficient authentication tiering with successive DOT1X, MAB and Captive Portal methods for streamlined BYOD
- Best-in-class IPv4/IPv6 static and dynamic routing including Proxy ARP, OSPF, BGP, Policy-based routing and automatic 6-to-4 tunneling
- Enhanced IPv4/IPv6 multicast forwarding with IGMPv3/MLDv2 Querier and Control Packet Flooding protection
- High performance IPv4/IPv6 multicast routing with PIM timer accuracy and unhandled PIM (S,G,rpt) state machine events transitioning
- Advanced IPv4/IPv6 security implementation including malicious code detection, DHCP Snooping, IP Source Guard protection and DoS attacks mitigation
- Innovative multi-vendor Auto-iSCSI capabilities for easier virtualization optimization
- Datacenter-ready features include DCBX (802.1Qaz), Priority Flow Control (PFC), Enhanced Transmission Selection (ETS) and FCoE FIP Snooping

NETGEAR M6100 series resiliency and availability features:

- Passive backplane, distributed redundant fabric and redundant management provide hitless, nonstop forwarding failover protection for always-on availability
- Redundant N+1 power protection contributes to business continuity management
- Distributed Link Aggregation across all I/O blades allows for multi-resiliency and advanced load balancing capabilities
- Multi Chassis Link Aggregation (MLAG) between two M6100 switches overcomes limitations of Spanning Tree, increasing bandwidth while preserving redundancy
- Per VLAN Spanning Tree and Per VLAN Rapid Spanning Tree (PVSTP/PVRSTP) offer interoperability with PVST+ infrastructures

NETGEAR M6100 series management features:

- DHCP/BootP innovative auto-installation including firmware and configuration file upload automation
- Industry standard SNMP, RMON, MIB, LLDP, AAA, sFlow and RSPAN remote mirroring implementation]\
- Selectable service port for out-of-band Ethernet management (OOB)
- Selectable standard RS232 straight-through serial RJ45 and Mini-USB ports for local management console
- Standard USB port for local storage, logs, configuration or image files
- Dual firmware image and configuration file for updates with minimum service interruption
- Industry standard command line interface (CLI) for IT admins used to other vendors commands
- Fully functional Web console (GUI) for IT admins who prefer an easy to use graphical interface
- Single-pane-of-glass NMS300 management platform with mass-configuration support

NETGEAR M6100 series warranty and support:

- NETGEAR ProSAFE Lifetime Hardware Warranty*
- Included Lifetime Technical Support
- Included Lifetime Next Business Day Hardware Replacement

Modern access layer features highlights

High Density Layer 2/Layer 3/Layer 4 Chassis Switch Solution	
M6100 series chassis switch provides extra high-density in 4U height (7 inches - 17.59cm) and only 17.39 inches depth (44.16cm)	• M6100 series uses latest generation silicon low-power 40-nanometer technology • Up to 144 RJ45 10/100/1000 ports, or 120 SFP 100/1000 ports, or 72 RJ45 10GBASE-T ports, or 48 SFP+ 1000/10GBASE-X ports, or a combination • L2, L3 and L4 switching features (access control list, classification, filtering, IPv4/IPv6 routing, IPv6 transition services) are performed in hardware at interface line rate for voice, video, and data convergence
M6100 series Layer 3 software package provides advanced IPv4/IPv6 fault tolerant routing capabilities for interfaces, VLANs, subnets and multicast	
Top-of-the-line switching performance	
32K MAC address table, 4K concurrent VLANs and 12K Layer 3 route table size for the most demanding enterprise or campus networks	
Each line-card (I/O blade) provides line-rate local switching and routing capacity	
Each slot provides 2 x 40G channels (80G half-duplex/160G full duplex) access to passive backplane	
480 Gbps inter module distributed fabric for up to 1.4 Tbps total routing/switching capacity	
Up to 1,071 Mpps intra-blade throughput and 357 Mpps inter-blade throughput	
80 PLUS certified power supplies for energy high efficiency	
Increased packet buffering with up to 32 Mb (Gigabit blades) and 72 Mb (10 Gigabit blades) for most intensive applications	
Low latency at all network speeds, including 10 Gigabit copper and fiber interfaces	
Jumbo frames support of up to 12Kb accelerating storage performance for backup and cloud applications	
iSCSI Flow Acceleration and Automatic Protection/ QoS for virtualization and server room networks containing iSCSI initiators and iSCSI targets	• Detecting the establishment and termination of iSCSI sessions and connections by snooping packets used in the iSCSI protocol • Maintaining a database of currently active iSCSI sessions and connections to store data, including classifier rules for desired QoS treatment • Installing and removing classifier rule sets as needed for the iSCSI session traffic • Monitoring activity in the iSCSI sessions to allow for aging out session entries if the session termination packets are not received • Avoiding session interruptions during times of congestion that would otherwise cause iSCSI packets to be dropped
Tier 1 availability	
M6100 series is designed upon Distributed Fabric innovative concept, providing passive backplane, redundant fabric and redundant management	• Distributed fabric removes the need for a dedicated supervisory module yet simplifying inventory management, maintenance and upgrades • Equipped with high-end hardware and software distributed fabric on board, any I/O blade can efficiently handle supervisory role in slot 1 • When inserted in slot 2, any I/O blade can handle back-up supervisory role for both management and fabric (active/passive stand-by mode) • In case of a failure for the supervisory blade in slot 1 (removal), the back-up supervisor in slot 2 is instantly taking over as the new supervisor • Instant failover from slot 1 to slot 2 is hitless for non-stop forwarding world-class resiliency and availability • Back to normal production conditions, hitless failback requires a command in CLI (movemanagement <2> <1>) or in GUI, for more control
Any M6100 I/O blades support hot-plug and hot-swap and can be inserted in any slot of M6100 base chassis switch	
M6100-3S base chassis features a passive backplane for exceptional availability and 387 years MTBF when at 25°C ambient (90 years at 50°C ambient)	

Distributed Link Aggregation, also called Port Channeling or Port Trunking, offers powerful network redundancy and load balancing between I/O blades	• Servers and other network devices benefit from greater bandwidth capacity with active-active teaming (LACP—link aggregation control protocol) • From a system perspective, a LAG (Link Aggregation Group) is treated as a physical port by M6100 Chassis switch for even more simplicity
Multi Chasssis Link Aggregation (MLAG) offers Link Aggregation benefits across two M6100 Chassis switches (currently supported on Supervisory blade only)	• Servers and other network partner devices are oblivious to the fact that they are pairing with two M6100 Chassis switches to form a LAG • Instead, the two M6100 Chassis switches appear as a single device to the partner • All links can carry data traffic and in case of link or device failures, the traffic can continue to flow with minimal disruption
Rapid Spanning Tree (RSTP) and Multiple Spanning Tree (MSTP) allow for rapid transitionning of the ports to the Forwarding state and the suppression of Topology Change Notification	
NETGEAR PVSTP implementation (CLI only) follows the same rules than other vendor's Per VLAN STP for strict interoperability	• Including industry-standard PVST+ interoperability • PVSTP is similar to the MSTP protocol as defined by IEEE 802.1s, the main difference being PVSTP runs one instance per VLAN • In other words, each configured VLAN runs an independent instance of PVSTP • Each PVRSTP instance elects a root bridge independent of the other • Hence there are as many Root Bridges in the region as there are VLANs configured • Per VLAN RSTP has in built support for FastUplink and FastBackbone
IP address conflict detection performed by embedded DHCP servers prevents accidental IP address duplicates from perturbing the overall network stability	
IP Event Dampening reduces the effect of interface flaps on routing protocols: the routing protocols temporarily disable their processing (on the unstable interface) until the interface becomes stable, thereby greatly increasing the overall stability of the network	
Ease of deployment	
Automatic configuration with DHCP and BootP Auto Install eases large deployments with a scalable configuration files management capability, mapping IP addresses and host names and providing individual configuration files to multiple switches as soon as they are initialized on the network	
Both the Chassis Switch Serial Number and primary MAC address are reported by a simple "show hardware" command in CLI - facilitating discovery and remote configuration operations	
M6100 DHCP L2 Relay agents eliminate the need to have a DHCP server on each physical network or subnet	• DHCP Relay agents process DHCP messages and generate new DHCP messages • Supports DHCP Relay Option 82 circuit-id and remote-id for VLANs • DHCP Relay agents are typically IP routing-aware devices and can be referred to as Layer 3 relay agent
Automatic Voice over IP prioritization with Auto-VoIP simplifies most complex multi-vendor IP telephones deployments either based on protocols (SIP, H323 and SCCP) or on OUI bytes (default database and user-based OUIs) in the phone source MAC address; providing the best class of service to VoIP streams (both data and signaling) over other ordinary traffic by classifying traffic, and enabling correct egress queue configuration	
An associated Voice VLAN can be easily configured with Auto-VoIP for further traffic isolation	
When deployed IP phones are LLDP-MED compliant, the Voice VLAN will use LLDP-MED to pass on the VLAN ID, 802.1P priority and DSCP values to the IP phones, accelerating convergent deployments	
Versatile connectivity	
Up to 6,000 Watts PoE budget depending on number of power supplies and I/O blades combination	• M6100 configurators are available at www.netgear.com/m6100 under the Resources tab
XCM8948 (48 x 1G RJ45) and XCM8944 (40 x 1G RJ45; 2 x 10GBASE-T; 2 x SFP+) can be equipped with a PoE daughter card for PoE+ (30W) or UPOE (60W)	
These I/O blades can be upgraded with PoE at any point of time, and possibly downgraded if the application has changed	• XCM89P daughter card supports PoE (802.3af) and PoE+ (802.3at) • XCM89UP daughter card supports PoE (802.3af), PoE+ (802.3at) and UPOE (Universal Power over Ethernet)
IEEE 802.3at Power over Ethernet Plus (PoE+) provides up to 30W power per port using 2 pairs while offering backward compatilibity with 802.3af	• IEEE 802.3at Layer 2 LLDP method and 802.3at PoE+ 2-event classification method fully supported for compatibility with most PoE+ PD devices

UPOE (Universal Power over Ethernet) provides up to 60W per port using 4 pairs while offering backward compatibilty with 802.3af and 802.3at	• UPOE LLDP TLV, an 802.3 organizationally specific TLV, is fully supported for compatibility with UPOE next-generation PD devices • Additionally, a forced 4-pair high power static method is supported in CLI or Web GUI to enable the forced 4-pair configuration
Large 10 Gigabit choice for uplinks with SFP+ ports for fiber or short, low-latency copper DAC cables; 10GBase-T ports for legacy Cat6 RJ45 short connections (up to 50m) and Cat6A / Cat7 connections up to 100m	
Automatic MDIX and Auto-negotiation on all ports select the right transmission modes (half or full duplex) as well as data transmission for crossover or straight-through cables dynamically for the admin	
IPv6 full support with IPv6 host, dual stack (IPv4 and IPv6), multicasting (MLD for IPv6 filtering and PIM-SM / PIM-DM for IPv6 routing), ACLs and QoS, static routing and dynamic routing (OSPFv3) as well as Configured 6to4 and Automatic 6to4 tunneling for IPv6 traffic encapsulation into IPv4 packets	
Ease of management and granular control	
Distributed fabric technology simplifies network operations, bringing simplicity for maintenance, upgrades and spare inventory management	• When inserted in Slot 1, any I/O blade will handle the supervisory role • When inserted in Slot 2, any I/O blade will handle the back-up supervisory role
Dual firmware image and dual configuration file for transparent firmware updates / configuration changes with minimum service interruption	
Flexible Port-Channel/LAG (802.3ad - 802.1AX) implementation for maximum compatibility, fault tolerance and load sharing with any type of Ethernet channeling from other vendors switch, server or storage devices conforming to IEEE 802.3ad - including static (selectable hashing algorithms) - or to IEEE 802.1AX with dynamic LAGs or port-channel (highly tunable LACP Link Aggregation Control Protocol)	
Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD detect and avoid unidirectional links automatically, in order to prevent forwarding anomalies in a Layer 2 communication channel in which a bi-directional link stops passing traffic in one direction	
Port names feature allows for descriptive names on all interfaces and better clarity in real word admin daily tasks	
SDM (System Data Management, or switch database) templates allow for granular system resources distribution depending on IPv4 or IPv6 applications:	• ARP Entries (the maximum number of entries in the IPv4 Address Resolution Protocol ARP cache for routing interfaces) • IPv4 Unicast Routes (the maximum number of IPv4 unicast forwarding table entries) • IPv6 NDP Entries (the maximum number of IPv6 Neighbor Discovery Protocol NDP cache entries) • IPv6 Unicast Routes (the maximum number of IPv6 unicast forwarding table entries) • ECMP Next Hops (the maximum number of next hops that can be installed in the IPv4 and IPv6 unicast forwarding tables) • IPv4 Multicast Routes (the maximum number of IPv4 multicast forwarding table entries) • IPv6 Multicast Routes (the maximum number of IPv6 multicast forwarding table entries)
Loopback interfaces management for routing protocols administration	
Private VLANs and local Proxy ARP help reduce broadcast with added security	
Management VLAN ID is user selectable for best convenience	
Industry-standard VLAN management in the command line interface (CLI) for all common operations such as VLAN creation; VLAN names; VLAN "make static" for dynamically created VLAN by GRVP registration; VLAN trunking; VLAN participation as well as VLAN ID (PVID) and VLAN tagging for one interface, a group of interfaces or all interfaces at once	
System defaults automatically set per-port broadcast, multicast, and unicast storm control for typical, robust protection against DoS attacks and faulty clients which can, with BYOD, often create network and performance issues	
IP Telephony administration is simplified with consistent Voice VLAN capabilities per the industry standards and automatic functions associated	
Comprehensive set of "system utilities" and "Clear" commands help troubleshoot connectivity issues and restore various configurations to their factory defaults for maximum admin efficiency: traceroute (to discover the routes that packets actually take when traveling on a hop-by-hop basis and with a synchronous response when initiated from the CLI), clear dynamically learned MAC addresses, counters, IGMP snooping table entries from the Multicast forwarding database etc...	
All major centralized software distribution platforms are supported for central software upgrades and configuration files management (HTTP, TFTP), including in highly secured versions (HTTPS, SFTP, SCP)	
Simple Network Time Protocol (SNTP) can be used to synchronize network resources and for adaptation of NTP, and can provide synchronized network timestamp either in broadcast or unicast mode (SNTP client implemented over UDP - port 123)	
Embedded RMON (4 groups) and sFlow agents permit external network traffic analysis	

Engineered for convergence	
Audio (Voice over IP) and Video (multicasting) comprehensive switching, filtering, routing and prioritization	
Auto-VoIP, Voice VLAN and LLDP-MED support for IP phones QoS and VLAN configuration	
IGMP Snooping and Proxy for IPv4, MLD Snooping and Proxy for IPv6 and Querier mode facilitate fast receivers joins and leaves for multicast streams and ensure multicast traffic only reaches interested receivers everywhere in a Layer 2 or a Layer 3 network	
Multicast VLAN Registration (MVR) uses a dedicated Multicast VLAN to forward multicast streams and avoid duplication for clients in different VLANs	
Distance Vector Multicast Routing Protocol (DVMRP) is a dense mode multicast protocol also called Broadcast and Prune Multicasting protocol	• DVMRP uses a distributed routing algorithm to build per-source-group multicast trees • DVMRP assumes that all hosts are part of a multicast group until it is informed of multicast group changes • It dynamically generates per-source-group multicast trees using Reverse Path Multicasting • Trees are calculated and updated dynamically to track membership of individual groups
Multicast routing (PIM-SM and PIM-DM, both IPv4 and IPv6) ensure multicast streams can reach receivers in different L3 subnets	• Multicast static routes allowed in Reverse Path Forwarding (RPF) selection • Multicast dynamic routing (PIM associated with OSPF) including PIM multi-hop RP support for routing around damage advanced capabilities • Full support of PIM (S,G,Rpt) state machine events as described in RFC 4601 • Improved Multicast PIM timer accuracy with hardware abstraction layer (HAPI) polling hit status for multicast entries in real time (without caching)
PoE power management and schedule enablement	
Power redundancy for higher availability when mission critical convergent installation, including hot-swap main PSU replacement without interruption	
Advanced Layer 3 routing package	
Static Routes/ECMP Static Routes for IPv4 and IPv6	• Static and default routes are configurable with next IP address hops to any given destination • 512 static routes are configurable for IPv4 when 512 other static routes are configurable for IPv6 • Permitting additional routes creates several options for the network administrator • The admin can configure multiple next hops to a given destination, intending for the router to load share across the next hops • The admin distinguishes static routes by specifying a route preference value: a lower preference value is a more preferred static route • A less preferred static route is used if the more preferred static route is unusable (down link, or next hop cannot be resolved to a MAC address) • Preference option allows admin to control the preference of individual static routes relative to routes learned from other sources (such as OSPF) since a static route will be preferred over a dynamic route when routes from different sources have the same preference
Advanced Static Routing functions for administrative traffic control	• Static Reject Routes are configurable to control the traffic destined to a particular network so that it is not forwarded through the router • Such traffic is discarded and the ICMP destination unreachable message is sent back to the source • Static reject routes can be typically used to prevent routing loops • Default routes are configurable as a preference option
In order to facilitate VLAN creation and VLAN routing using Web GUI, a VLAN Routing Wizard offers the following automated capabilities:	• Create a VLAN and generate a unique name for VLAN • Add selected ports to the newly created VLAN and remove selected ports from the default VLAN • Create a LAG, add selected ports to a LAG, then add this LAG to the newly created VLAN • Enable tagging on selected ports if the port is in another VLAN • Disable tagging if a selected port does not exist in another VLAN • Exclude ports that are not selected from the VLAN • Enable routing on the VLAN using the IP address and subnet mask entered as logical routing interface

DHCP Relay Agents relay DHCP requests from any routed interface, including VLANs, when DHCP server doesn't reside on the same IP network or subnet	• The agent relays requests from a subnet without a DHCP server to a server or next-hop agent on another subnet • Unlike a router which switches IP packets transparently, a DHCP relay agent processes DHCP messages and generates new DHCP messages • Supports DHCP Relay Option 82 circuit-id and remote-id for VLANs • Multiple Helper IPs feature allows to configure a DHCP relay agent with multiple DHCP server addresses per routing interface and to use different server addresses for client packets arriving on different interfaces on the relay agent server addresses for client packets arriving on different interfaces on the relay agent
Virtual Router Redundancy Protocol (VRRP) provides backup for any statically allocated next-hop router address going down, based on RFC 3768 (IPv4)	• VRRP is based on the concept of having more than one router recognize the same router IP address • VRRP increases the availability of the default path without requiring configuration of dynamic routing, or router discovery protocols on end stations • Multiple virtual routers can be defined on any single router interface • One of the routers is elected the master router and handles all traffic sent to the specified virtual router IP address • When the master router fails, one of the backup routers is elected in its place and starts handling traffic sent to the address
As an enhancement to RFC 3768, VRRP Interface can be configured as pingable to help troubleshoot network connectivity issues	• In that case, VRRP master responds to both fragmented and unfragmented ICMP echo requests packets destined to VRRP address(es) • VRRP master responds with VRRP address as the source IPv4 address and VRMAC as the source MAC address • A virtual router in backup state discards these ICMP echo requests
VRRP Route/Interface Tracking feature extends the capability of the Virtual Router Redundancy Protocol (VRRP)	• Allows tracking of specific route/interface IP states, within the router, that can alter the priority level of a virtual router for a VRRP group • It ensures the best VRRP router is master for the group
Router Discovery Protocol is an extension to ICMP and enables hosts to dynamically discover the IP address of routers on local IP subnets	• Based on RFC 1256 for IPv4 • Routers periodically send router discovery messages to announce their presence to locally-attached hosts • The router discovery message advertises one or more IP addresses on the router that hosts can use as their default gateway • Hosts can send a router solicitation message asking any router that receives the message to immediately send a router advertisement • Router discovery eliminates the need to manually configure a default gateway on each host • It enables hosts to switch to a different default gateway if one goes down
Loopback interfaces are available as dynamic, stable IP addresses for other devices on the network, and for routing protocols	
Tunnel interfaces are available for IPv4 and IPv6	• Each router interface (port, or VLAN interface) can have multiple associated tunnel interfaces • Support for Configured 6to4 (RFC 4213) and Automatic 6to4 tunneling (RFC 3056) for IPv6 traffic encapsulation into IPv4 packets • 6to4 tunnels are automatically formed for IPv4 tunnels carrying IPv6 traffic • M6100 can act as a 6to4 border router that connects a 6to4 site to a 6to4 domain
Support of Routing Information Protocol (RIPv2) as a distance vector protocol specified in RFC 2453 for IPv4	• Each route is characterized by the number of gateways, or hops, a packet must traverse to reach its intended destination • Categorized as an interior gateway protocol, RIP operates within the scope of an autonomous system
Route Redistribution feature enables the exchange of routing information among different routing protocols all operating within a router	• Configurable when different routing protocols use different ways of expressing the distance to a destination or different metrics and formats • For instance, when OSPF redistributes a route from RIP, and needs to know how to set each of the route's path attributes

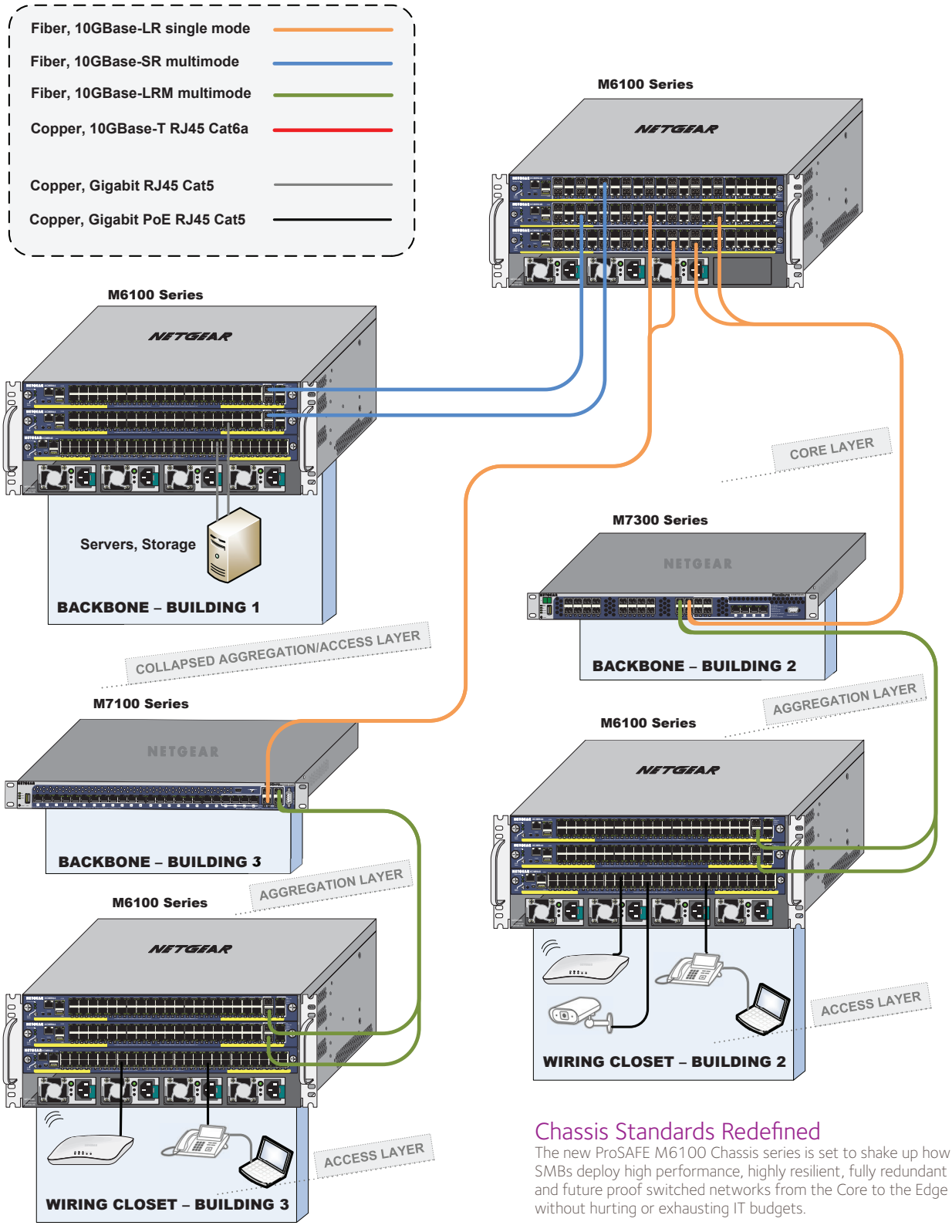
Open Shortest Path First (OSPF) link-state protocol for IPv4 and IPv6	• For IPv4 networks, OSPF version 2 is supported in accordance with RFC 2328, including compatibility mode for the RFC 1583 older specification • For IPv6 networks, OSPF version 3 is fully supported • OSPF can operate within a hierarchy, the largest entity within the hierarchy is the autonomous system (AS) • An AS is a collection of networks under a common administration sharing a common routing strategy (routing domain) • An AS can be divided into a number of areas or groups of contiguous networks and attached hosts • Two different types of OSPF routing occur as a result of area partitioning: Intra-area and Inter-area • Intra-area routing occurs if a source and destination are in the same area • Inter-area routing occurs when a source and destination are in different areas • An OSPF backbone distributes information between areas
Advanced OSPF implementation for large routing domains	• OSPF NSSA feature supports RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option • Forwarding of OSPF Opaque LSAs is enabled by default • Passive interface feature can disable sending OSPF routing updates on an interface • Static Area Range Costs feature allows to configure a fixed OSPF cost that is always advertised when an area range is active • OSPF Equal Cost Multipath (ECMP) feature allows to forward traffic through multiple paths, taking advantage of more bandwidth • ECMP routes can be learned dynamically, or configured statically with multiple static routes to same destination but with different next hops • OSPF Max Metric feature allows to to override the metric in summary type 3 and type 4 LSAs while in stub router mode • Automatic Exiting of Stub Router Mode feature allows to exit stub router mode, reoriginating the router LSA with proper metric values on transit links • Static Area Range Costs feature allows to configure a fixed OSPF cost that is always advertised when an area range is active
OSPF LSA Pacing feature improves the efficiency of LSA flooding, reducing or eliminating the packet drops caused by bursts in OSPF control packets	• LSA transmit pacing limits the rate of LS Update packets that OSPF can send • With LSA refresh groups, OSPF efficiently bundles LSAs into LS Update packets when periodically refreshing self-originated LSAs
OSPF Flood Blocking feature allows to disable LSA flooding on an interface with area or AS (domain-wide) scope	• In that case, OSPF does not advertise any LSAs with area or AS scope in its database description packets sent to neighbors
OSPF Transit-Only Network Hiding is supported based on RFC 6860 with transit-only network defined as a network connecting only routers	• Transit-only networks are usually configured with routable IP addresses which are advertised in LSAs but are not needed for data traffic • If router-to-router subnets are advertised, remote attacks can be launched against routers by sending packets to these transit-only networks • Hiding transit-only networks speeds up network convergence and reduces vulnerability to remote attacks • 'Hiding' implies that the prefixes are not installed in the routing tables on OSPFv2 and OSPFv3 routers
IP Multinetting allows to configure more than one IP address on a network interface (other vendors may call it IP Aliasing or Secondary Addressing)	
ICMP Throttling feature adds configuration options for the transmission of various types of ICMP messages	• ICMP Redirects can be used by a malicious sender to perform man-in-the-middle attacks, or divert packets to a malicious monitor, or to cause Denial of Service (DoS) by blackholing the packets • ICMP Echo Requests and other messages can be used to probe for vulnerable hosts or routers • Rate limiting ICMP error messages protects the local router and the network from sending a large number of messages that take CPU and bandwidth

Border Gateway Protocol version 4 (BGP4) is supported for typical routed data center topologies (IPv4 and IPv6) up to max L3 route table size (12K routes)	• BGP is an inter-Autonomous System (AS) routing protocol as described in RFC 4271 section-3 • The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems • This network reachability information includes information on the list of Autonomous Systems (ASes) that reachability information traverses
BGP Route Reflection feature as described in RFC 4456 allows to a router to reflect a route received from an internal peer to another internal peer	• Under conventional BGP rules, a router can only send an internal peer routes learned from an external peer or routes locally originated • Route reflection eliminates the need to configure a full mesh of iBGP peering sessions • The administrator can configure an internal BGP peer to be a route reflector client • Alternatively, the administrator can configure a peer template to make any inheriting peers route reflector clients • The client status of a peer can be configured independently for IPv4 and IPv6 a cluster may have multiple route reflectors • A cluster may have multiple route reflectors
The Policy Based Routing feature (PBR) overrides routing decision taken by the router and makes the packet to follow different actions based on a policy	• It provides freedom over packet routing/forwarding instead of leaving the control to standard routing protocols based on L3 • For instance, some organizations would like to dictate paths instead of following the paths shown by routing protocols • Network Managers/Administrators can set up policies such as: – My network will not carry traffic from the Engineering department – Traffic originating within my network with the following characteristics will take path A, while other traffic will take path B – When load sharing needs to be done for the incoming traffic across multiple paths based on packet entities in the incoming traffic
Enterprise security	
Traffic control MAC Filter and Port Security help restrict the traffic allowed into and out of specified ports or interfaces in the system in order to increase overall security and block MAC address flooding issues	
DHCP Snooping monitors DHCP traffic between DHCP clients and DHCP servers to filter harmful DHCP message and builds a bindings database of (MAC address, IP address, VLAN ID, port) tuples that are considered authorized in order to prevent DHCP server spoofing attacks	
IP source guard and Dynamic ARP Inspection use the DHCP snooping bindings database per port and per VLAN to drop incoming packets that do not match any binding and to enforce source IP / MAC addresses for malicious users traffic elimination	
Time-based Layer 2 / Layer 3-v4 / Layer 3-v6 / Layer 4 Access Control Lists (ACLs) can be binded to ports, Layer 2 interfaces, VLANs and LAGs (Link Aggregation Groups or Port channel) for fast unauthorized data prevention and right granularity	
For in-band switch management, management ACLs on CPU interface (Control Plane ACLs) are used to define the IP/MAC or protocol through which management access is allowed for increased HTTP/HTTPS or Telnet/SSH management security	
Out-of-band management is available via dedicated service port (1G RJ45 OOB) when in-band management can be prohibited via management ACLs	
Bridge protocol data unit (BPDU) Guard allows the network administrator to enforce the Spanning Tree (STP) domain borders and keep the active topology consistent and predictable – unauthorized devices or switches behind the edge ports that have BPDU enabled will not be able to influence the overall STP by creating loops	
Spanning Tree Root Guard (STRG) enforces the Layer 2 network topology by preventing rogue root bridges potential issues when for instance, unauthorized or unexpected new equipment in the network may accidentally become a root bridge for a given VLAN	
Dynamic 802.1x VLAN assignment mode, including Dynamic VLAN creation mode and Guest VLAN/ Unauthenticated VLAN are supported for rigorous user	• Up to 48 clients (802.1x) per port are supported, including the authentication of the users domain, in order to facilitate convergent deployment. For instance when IP phones connect PCs on their bridge, IP phones and PCs can authenticate on the same switch port but under different VLAN assignment policies (Voice VLAN versus other Production VLANs)

802.1x MAC Address Authentication Bypass (MAB) is a supplemental authentication mechanism that lets non-802.1x devices bypass the traditional 802.1x process altogether, letting them authenticate to the network using their client MAC address as an identifier	• A list of authorized MAC addresses of client NICs is maintained on the RADIUS server for MAB purpose • MAB can be configured on a per-port basis on the switch • MAB initiates after unsuccesful dot1x authentication process (configurable time out), when clients don't respond to any of EAPOL packets • When 802.1X unaware clients try to connect, the switch sends the MAC address of each client to the authentication server • The RADIUS server checks the MAC address of the client NIC against the list of authorized addresses • The RADIUS server returns the access policy and VLAN assignment to the switch for each client
With Successive Tiering, the Authentication Manager allows for authentication methods per port for a Tiered Authentication based on configured time-outs	• By default, configuration authentication methods are tried in this order: Dot1x, then MAB, then Captive Portal (web authentication) • With BYOD, such Tiered Authentication is powerful and simple to implement with strict policies • For instance, when a client is connecting, M6100 tries to authencate the user/client using the three methods above, the one after the other • The admin can restrict the configuration such that no other method is allowed to follow the captive portal method, for instance
Double VLANs (DVLAN - QinQ) pass traffic from one customer domain to another through the "metro core" in a multi-tenancy environment: customer VLAN IDs are preserved and a service provider VLAN ID is added to the traffic so the traffic can pass the metro core in a simple, secure manner	
Private VLANs (with Primary VLAN, Isolated VLAN, Community VLAN, Promiscuous port, Host port, Trunks) provide Layer 2 isolation between ports that share the same broadcast domain, allowing a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains accross switches in the same Layer 2 network	• Private VLANs are useful in DMZ when servers are not supposed to communicate with each other but need to communicate with a router • They remove the need for more complex port-based VLANs with respective IP interface/subnets and associated L3 routing • Another Private VLANs typical application are carrier-class deployments when users shouldn't see, snoop or attack other users' traffic
Secure Shell (SSH) and SNMPv3 (with or without MD5 or SHA authentication) ensure SNMP and Telnet sessions are secured	
TACACS+ and RADIUS enhanced administrator management provides strict "Login" and "Enable" authentication enforcement for the switch configuration, based on latest industry standards: exec authorization using TACACS+ or RADIUS; command authorization using TACACS+ and RADIUS Server; user exec accounting for HTTP and HTTPS using TACACS+ or RADIUS; and authentication based on user domain in addition to user ID and password	
Superior quality of service	
Advanced classifier-based hardware implementation for Layer 2 (MAC), Layer 3 (IP) and Layer 4 (UDP/TCP transport ports) prioritization	
7 queues for priorities and various QoS policies based on 802.1p (CoS) and DiffServ can be applied to interfaces and VLANs	
Advanced rate limiting down to 1 Kbps granularity and mininum-guaranteed bandwidth can be associated with time-based ACLs for best granularity	
Single Rate Policing feature enables support for Single Rate Policer as defined by RFC 2697	• Committed Information Rate (average allowable rate for the class) • Committed Burst Size (maximum amount of contiguous packets for the class) • Excessive Burst Size (additional burst size for the class with credits refill at a slower rate than committed burst size) • DiffServ feature applied to class maps
Automatic Voice over IP prioritization with protocol-based (SIP, H323 and SCCP) or OUI-based Auto-VoIP up to 144 simultaneous voice calls	
iSCSI Flow Acceleration and automatic protection/QoS with Auto-iSCSI	
Flow Control	
802.3x Flow Control implementation per IEEE 802.3 Annex 31 B specifications with Symmetric flow control, Asymmetric flow control or No flow control	• Asymmetric flow control allows the switch to respond to received PAUSE frames, but the ports cannot generate PAUSE frames • Symmetric flow control allows the switch to both respond to, and generate MAC control PAUSE frames
Allows traffic from one device to be throttled for a specified period of time	• A device that wishes to inhibit transmission of data frames from another device on the LAN transmits a PAUSE frame

UDLD Support	
UDLD implementation detects unidirectional links physical ports (UDLD must be enabled on both sides of the link in order to detect an unidirectional link	• UDLD protocol operates by exchanging packets containing information about neighboring devices • The purpose is to detect and avoid unidirectional link forwarding anomalies in a Layer 2 communication channel
Both "normal-mode" and "aggressive-mode" are supported for perfect compatibility with other vendors implementations, including port "D-Disable triggering cases in both modes	
Datacenter Features (CLI only)	
The Priority Flow Control (PFC) is standardized by the IEEE 802.1Qbb specification and enables flow control per traffic class on IEEE 802 full-duplex links	• By pausing congested priorities independently, highly loss sensitive protocols can share the same link with traffic that has different loss tolerances • The priorities are differentiated by the priority field of the 802.1Q VLAN header • PFC uses a new control packet defined in 802.1Qbb and therefore disables 802.3x standard flow control on PFC configured interfaces
The Data Center Bridging Exchange Protocol (DCBX) is used by DCB devices to exchange configuration information with directly connected peers	• The protocol is also used to detect misconfiguration of the peer DCB devices and optionally, for configuration of peer DCB devices • DCBX is deployed in support of lossless operation for FCoE or ISCSI traffic when all network elements in FCoE topologies are DCBX enabled • M6100 automatically detects if a peer is operating with either of the two DCBX versions (the CEE DCBX and the IEEE standard DCBX) by default • DCBX protocol supports the propagation of received configuration information for the following features: – Enhanced Transmission Selection (ETS) – Priority-based Flow Control (PFC) – Application Priorities
Enhanced Transmission Selection (ETS) provides an operational model for priority processing and bandwidth allocation for the switch in a DCB environment	• Using priority-based processing and bandwidth allocations, different Traffic Class Groups (TCGs) within different types of traffic such as LAN, SAN and Management can be configured to provide bandwidth allocation or best effort transmit characteristics • CoS information is exchanged with peer DCBX devices using ETS TLVs • As part of the transmitted ETS TLVs, by default, DCBX advertises the following parameters on per port basis: – Mapping between ingress ports 802.1p priority to Traffic Class Group (TCG) – Bandwidth percentage (weight percentage) of each Traffic Class Group – Scheduling algorithm for each Traffic Class Group • ETS TLVs are accepted from auto-upstream devices and propagated to auto-downstream devices • ETS may be configured on a port in manual mode and M6100 switch may become the source for ETS configuration in the network
The FCoE Initialization Protocol (FIP) is used to perform the functions of FC_BB_E device discovery, initialization and maintenance	• FIP uses a separate EtherType from FCoE to enable the distinction of discovery, initialization, and maintenance traffic from other FCoE traffic • FIP frames are standard Ethernet size (1518 Byte 802.1q frame) whereas FCoE frames are a maximum of 2240 bytes
The FIP snooping capability is a frame inspection method used by FIP Snooping Bridges to monitor FIP frames and apply policies based upon the L2 header information in those frames, following the recommendations in Annex C of FC_BB_5 Rev 2.00 and supporting these features:	• Auto-configuration of Ethernet ACLs based on information in the Ethernet headers of FIP frames • Emulation of FC point-to-point links within the DCB Ethernet network • Enhanced FCoE security/robustness by preventing FCoE MAC spoofing
The FIP Snooping Bridge solution in M6100 supports the interior port role, the perimeter port role and the FCF-facing port role and is intended for use at the edge or the interior of the switched network	• Perimeter or Edge port (connected directly to ENode) • FCF facing port (that receives traffic from FCFs targeted to the Enodes)

Target Application



Chassis Standards Redefined

The new ProSAFE M6100 Chassis series is set to shake up how SMBs deploy high performance, highly resilient, fully redundant and future proof switched networks from the Core to the Edge - without hurting or exhausting IT budgets.

Get started today with NETGEAR M6100 series

Offering the densest Gigabit and 10G port solution in a 4U footprint, the M6100 is a fully distributed fabric, passive backplane solution with full management and power redundancy - as standard. UPOE capability extends its potential and delivers true investment protection to leverage today and tomorrow's evolving powered devices.

An ideal platform for virtualized, convergence and surveillance environment

- Designed for use at the center of a small to mid-sized organization, or as an aggregated or access solution in a larger campus or mid-sized enterprise branch network, the application scenarios for the M6100 are both wide and diverse. For those who require a resilient Gigabit connectivity option to the desktop or 10G for virtualized server and storage needs through to large IP camera surveillance environments, the M6100 provides the markets fastest backplane speeds with hitless failover to deliver enterprise grade service levels excellence for SMBs.

All the hallmarks of a chassis with associated benefits but at fixed stackable price points

- Integrated supervisor blades - NO need for separate or spare supervisor blades. Slot 1 is the primary supervisor with slot 2 the default back-up supervisor
- PoE/PoE+/UPOE flexibility - NO separate PoE blades required. Simply add PoE daughter cards to any Gigabit blade to introduce PoE as and when required
- 480Gbps inter-module backplane performance – NO performance compromise. With up to 10 x performance of fixed stackable solutions with similar port counts, value performance ratios are unrivalled
- Distributed fabric, passive backplane – NO single point of failure with management and power backup and distributed link aggregation across multiple chassis arrangements
- L2/L3/L4 routing as standard – NO additional licensing costs or annual maintenance contracts to inflate prices and jeopardise sales

Class leading support services as standard

- All M6100 Chassis series products come with Lifetime Warranty, Lifetime Next Business Day and Lifetime Technical online support included - at no extra cost.

Components

M6100-3S (XCM8903)
3-Slot 4U Base Chassis

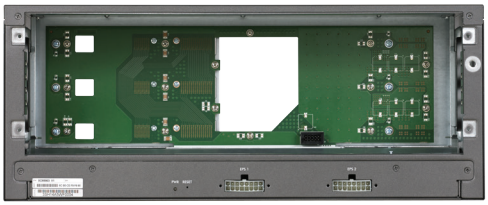
Ordering information

- Not orderable as a separate SKU
- Base chassis comes with M6100 starter kits
- Warranty: Lifetime

- 3 open line-card slots
- 4 power supply slots (8 slots with additional 1U power shelf with RPS4000v2)
- Strict passive backplane requirements
- 4U height (6.93 in; 17.59 cm) and 17.39 in depth (44.16 cm)

FRONT: Base chassis with blade and PSU blank pannels

FRONT: Base chassis without blank panels



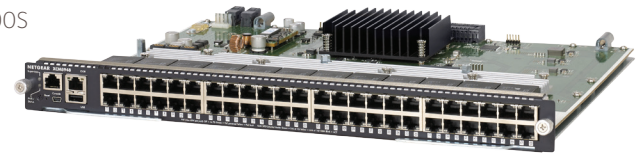
BACK: Base chassis without fan tray

XCM8948
I/O Blade

Ordering information

- Worldwide: XCM8948-10000S
- Warranty: Lifetime

- 48-port 10/100/1000BASE-T RJ45
- PoE, PoE+ and UPOE available as an option with XCM89P or XCM89UP daughter card

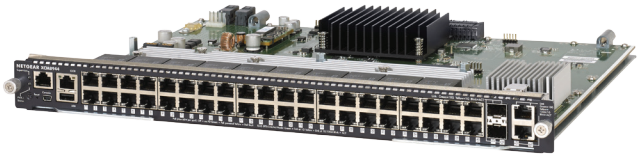


XCM8944
I/O Blade

Ordering information

- Worldwide: XCM8944-10000S
- Warranty: Lifetime

- 40-port 10/100/1000BASE-T RJ45
- 2-port 100/1000/10GBASE-T RJ45 (independent)
- 2-port 1000BASE-X/10GBASE-X SFP+ (independent)
- PoE, PoE+ and UPOE available as an option with XCM89P or XCM89UP daughter card



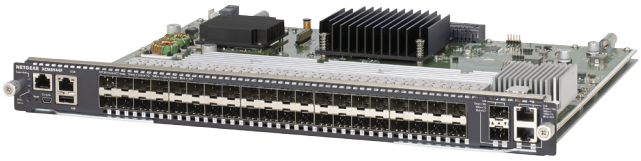
Components

XCM8944F
I/O Blade

- 40-port 100BASE-X/1000BASE-X SFP
- 2-port 100/1000/10GBASE-T RJ45 (independent)
- 2-port 1000BASE-X/10GBASE-X SFP+ (independent)

Ordering information

- Worldwide: XCM8944F-10000S
- Warranty: Lifetime



XCM8924X
I/O Blade

- 24-port 100/1000/10GBASE-T RJ45
- 16-port 1000BASE-X/10GBASE-X SFP+ (shared with 16 first 10GBASE-T ports)

Ordering information

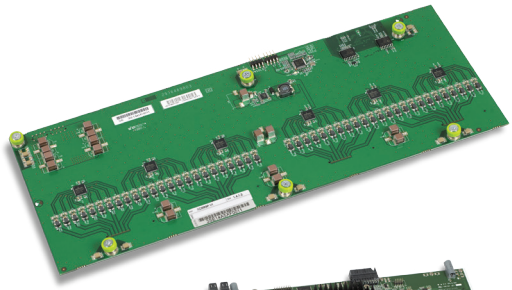
- Worldwide: XCM8924X-10000S
- Warranty: Lifetime

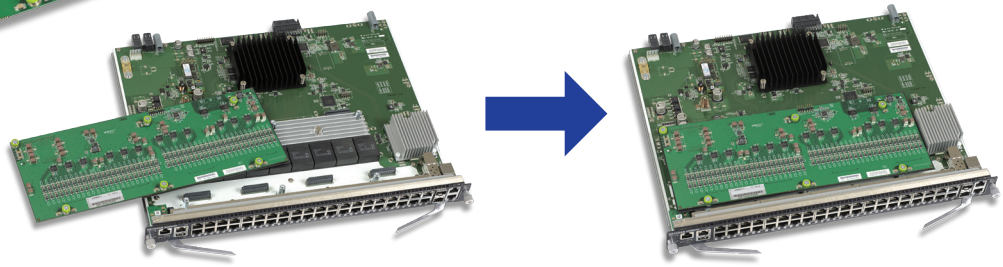
XCM89P
Daughter Card

- Adds PoE (802.3af) and PoE+ (802.3at) functionality to XCM8948 or XCM8944 blade
- One daughter card per blade

Ordering information

- Worldwide: XCM89P-10000S
- Warranty: Lifetime



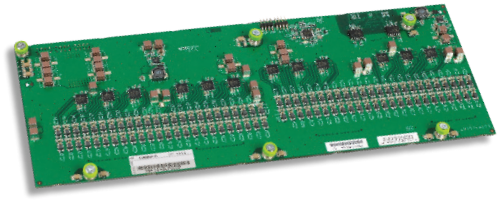


Components

XCM89UP
Daughter Card

Ordering information

- Worldwide: XCM89UP-10000S
- Warranty: Lifetime

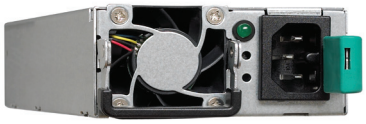


- Adds PoE (802.3af), PoE+ (802.3at) and UPOE functionality to XCM8948 or XCM8944 blade
- One daughter card per blade

APS1000W
Power Supply Unit

Ordering information

- Americas, Europe: APS1000W-100NES
- Asia Pacific: APS1000W-100AJS
- Warranty: 5 years



- C15 connector
- Capacity:
  - 110V-240V AC power input
  - Up to 640W output power at 110V AC
  - Up to 910W output power at 220V AC
- C15 connector

AFT603
Fan Tray

Ordering information

- Worldwide: AFT603-10000S
- Warranty: 5 years

- Front-to-back cooling principle

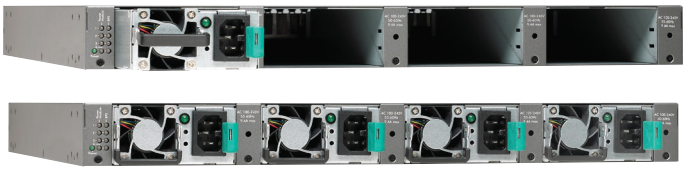
Components

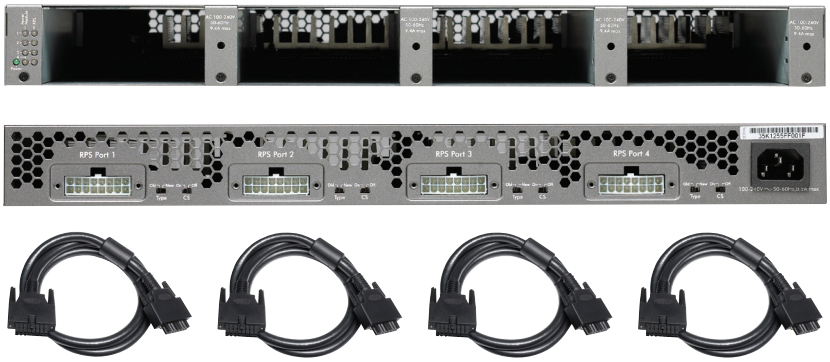
RPS4000v2
Additional 1U Power Shelf

Ordering information

- Americas, Europe: RPS4000-200NES
- Asia Pacific: RPS4000-200AJS
- Warranty: 5 years

- EPS mode: provide 4 additional PSU slots to M6100-3S chassis
  - M6100-3S power management system can use the four additional APS1000W PSUs transparently





Front view

- RPS4000 is 1RU unit with four (4) empty slots
- Power modules (APS1000W) are sold separately
- APS1000W requirement depends on RPS, EPS, PoE application

Rear view

- Four (4) embedded RPS connectors
- Switch selectors for RPS/EPS power modes
- Switch selectors for power modules two-by-two bridging

Included:

- Four (4) RPS cables - 60cm each (~2 ft)
- Rack mount kit
- Power cord

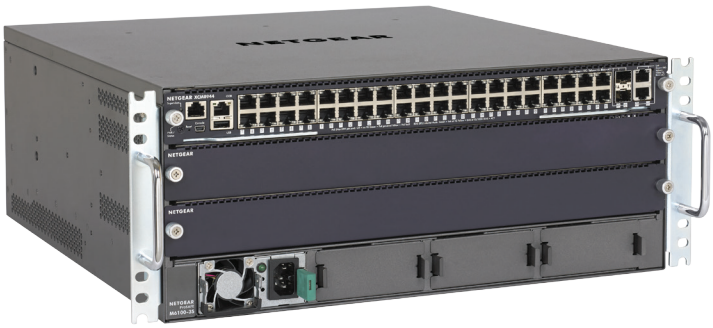
M6100-44G3-POE+ (XCM8903SK)
Starter Kit

Ordering information

- Worldwide: XCM8903SK-10000S

Starter kit components ship in their individual packaging:

- M6100-3S Base chassis (XCM8903)
- 1 blade 40x1G + 4x10G (XCM8944)
- 1 PoE+ daughter card (XCM89P)
- 1 power supply unit (APS1000W)
- 1 fan tray front to back (AFT603)
- 2 blank panels for open blade slots
- 3 blank panels for empty PSU slots
- Handles for rack-mount kit
- Rack-mount kit for 2-post racks
- Sliding rails kit for 4-post racks



Components

GBIC SFP and SFP+ Optics for M6100 series

Ordering information • Worldwide: see table below • Warranty: 5 years	Multimode Fiber (MMF)		Single mode Fiber (SMF)
	OM1 or OM2 62.5/125µm	OM3 or OM4 50/125µm	9/125µm
10 Gigabit SFP+  • Fits into XCM8944, XCM8944F SFP+ interfaces • Fits into XCM2924X SFP+ interfaces	**AXM763** 10GBase-LRM long reach multimode 802.3aq - LC duplex connector up to 220m (722 ft) **AXM763-10000S (1 unit)**	**AXM763** 10GBase-LRM long reach multimode 802.3aq - LC duplex connector up to 260m (853 ft) **AXM763-10000S (1 unit)** **AXM761** 10GBase-SR short reach multimode LC duplex connector OM3: up to 300m (984 ft) OM4: up to 550m (1,804 ft) **AXM761-10000S (1 unit)** **AXM761P10-10000S** **(pack of 10 units)**	**AXM762** 10GBase-LR long reach single mode LC duplex connector up to 10km (6.2 miles) **AXM762-10000S (1 unit)** **AXM762P10-10000S** **(pack of 10 units)**
Gigabit SFP  • Fits into XCM8944F SFP interfaces • Fits into XCM8944, XCM8944F SFP+ interfaces • Fits into XCM2924X SFP+ interfaces	**AGM731F** 1000Base-SX short range multimode LC duplex connector up to 275m (902 ft) **AGM731F (1 unit)**	**AGM731F** 1000Base-SX short range multi-mode LC duplex connector OM3: up to 550m (1,804 ft) OM4: up to 1,000m (3,280 ft) **AGM731F (1 unit)**	**AGM732F** 1000Base-LX long range single mode LC duplex connector up to 10km (6.2 miles)) **AGM732F (1 unit)**
Fast Ethernet SFP  • Fits into XCM8944F SFP interfaces	**AFM735** 100Base-FX IEEE 802.3 LC duplex connector up to 2km (1.24 miles) **AFM735-10000S (1 unit)**	**AFM735** 100Base-FX IEEE 802.3 LC duplex connector up to 2km (1.24 miles) **AFM735-10000S (1 unit)**	

AGM734
1000Base-T Gigabit RJ45 SFP

Ordering information
- Worldwide: AGM734-10000S
- Warranty: 5 years

- 1 port Gigabit RJ45 for XCM8944F blade (SFP ports)
- Supports only 1000Mbps full-duplex mode
- Up to 100m (328 ft) with Cat5 RJ45 or better
- Conveniently adds copper connectivity to XCM8944F fiber blade

Components

Direct Attach Cables for M6100 series

Ordering information • Worldwide: see table below • Warranty: 5 years	SFP+ to SFP+	
	1 meter (3.3 ft)	3 meters (9.8 ft)
10 Gigabit DAC  • Fits into XCM8944, XCM8944F SFP+ interfaces • Fits into XCM2924X SFP+ interfaces	**AXC761** 10GSFP+ Cu (passive) SFP+ connectors on both end **AXC761-10000S (1 unit)**	**AXC763** 10GSFP+ Cu (passive) SFP+ connectors on both end **AXC763-10000S (1 unit)**

Technical Specifications

Model Name	Description	Model number
M6100-3S	M6100 series 3-Slot Base Chassis	XCM8903
XCM8948	I/O Blade 48 x 1G (RJ45)	XCM8948
XCM8944	I/O Blade 40 x 1G (RJ45), 2 x SFP+, 2 x 10GBASE-T	XCM8944
XCM8944F	I/O Blade 40 x 1G (SFP), 2 x SFP+, 2 x 10GBASE-T	XCM8944F
XCM8924X	I/O Blade 24 x 10GBASE-T, 16 x SFP+ (shared)	XCM8924X
XCM89P	Daughter Card PoE+ XCM8944/XCM8948	XCM89P
XCM89UP	Daughter Card PoE+/UPOE XCM8944/XCM8948	XCM89UP
APS1000W	PSU 1,000W AC	APS1000W
AFT603	Fan Tray with front-to-back cooling principle	AFT603
RPS4000v2	Additional 1U Power Shelf	RPS4000v2

PHYSICAL INTERFACES				
Front	Auto-sensing RJ45 10/100/1000BASE-T	Auto-sensing SFP ports 100/1000BASE-X	Auto-sensing RJ45 100/1000/ 10GBASE-T	Auto-sensing SFP+ ports 1000/10GBASE-X
XCM8948 blade	48	-	-	-
XCM8944 blade	40	-	2	2 (independent)
XCM8944F blade	-	40	2	2 (independent)
XCM8924X blade	-	-	24	16 (shared)

Front (Management)	Console ports	Service port (Out-of-band Ethernet)	Storage port
All blades	Serial RS232 RJ45 (straight-through wiring); Mini-USB	1 x RJ45 10/100/1000BASE-T	1 x USB

Front (Line-Cards Slots)	I/O Slots
M6100-3S Base Chassis	3

Front (PSUs)	Standalone	With additional 1U power shelf RPS4000v2
M6100-3S Base Chassis	4 x PSU slots	8 x PSU slots

Back	Fans	EPS Connectors
M6100-3S Base Chassis	1 x Fan Tray slot (fan controllers located on Fan Tray)	2 (for one RPS4000v2)

Total Port Count	Gigabit	10 Gigabit
XCM8948 blade	48 ports total	-
XCM8944 blade	40 ports total	4 ports total
XCM8944F blade	40 ports total	4 ports total
XCM8924X blade	-	24 ports total

POWER OVER ETHERNET					
PSE Capacity	PoE+ ports	UPOE ports	Max PoE budget		
XCM8948 blade equipped with XCM89P daughter card	48	-	1,440 W		Use M6100 configurators www.netgear.com/m6100 under Resources tab
XCM8948 blade equipped with XCM89UP daughter card		48	2,880W		
XCM8944 blade equipped with XCM89P daughter card	40	-	1,200 W		
XCM8944 blade equipped with XCM89UP daughter card		40	2,400 W		
PoE Budget is remaining difference between Power Supplies delivered Wattage, and Blades consumption:	PSU delivered Wattage @ 110V		PSU deliveredWattage @220V		Blades consumption
	N	N+1	N	N+1	
1 x PSU (APS1000W)	640 W	-	910 W	-	XCM8948: 60W
2 x PSU (APS1000W)	1,120 W	640 W	1,540 W	910 W	XCM8944: 70W
3 x PSU (APS1000W)	1,680 W	1,120 W	2,310 W	1,540 W	XCM8944F: 150W
4 x PSU (APS1000W)	2,240 W	1,680 W	3,080 W	2,310 W	XCM8924X: 200W
5 x PSU (APS1000W)	2,800 W	2,240 W	3,850 W	3,080 W	Use M6100 configurators www.netgear.com/m6100 under Resources tab
6 x PSU (APS1000W)	3,360 W	2,800 W	4,620 W	3,850 W	
7 x PSU (APS1000W)	3,920 W	3,360 W	5,390 W	4,620 W	
8 x PSU (APS1000W)	4,480 W	3,920 W	6,160 W	5,390 W	
Features Support	Blades equipped with XCM89P daughter card		Blades equipped with XCM89UP daughter card		
IEEE 802.3af (up to 15.4W per port)	Yes		Yes		
IEEE 802.3at (up to 30W per port)	Yes		Yes		
IEEE 802.3at Layer 2 (LLDP) method	Yes		Yes		
IEEE 802.3at 2-event classification	Yes		Yes		
UPOE interoperability with LLDP 802.3 organizationally specific TLV	-		Yes		
UPOE interoperability with forced 4-pair static method	-		Yes		
PoE timer/schedule (week, days, hours)	Yes		Yes		

PROCESSOR/MEMORY		
Processor (CPU) - all blades	Integrated 5000 DMIPS Dual-Core CPU in switching silicon	
System memory (RAM) - all blades	1 GB	
Code storage (flash) - all blades	64 MB	Dual firmware image, dual configuration file
Packet Buffer Memory		
XCM8948, XCM8944, XCM8944F blades	32 Mb	Dynamically shared across only used ports
XCM8924X blade	72 Mb	

M6100-3S CHASSIS	
Backplane	Passive Backplane with redundant fabric and redundant management
Fabric	480Gbps Distributed Fabric (I/O Blades are equipped with dedicated hardware and software distributed fabric)
Resiliency	Control Plane + Management Plane Non-Stop Forwarding (NSF) and Hitless Failover
Supervisory Modules	Any I/O blade can handle the Supervisory Module and the Backup Supervisory Module roles
Supervisory Slot	Slot 1
Backup Supervisory Slot (secondary)	Slot 2 (continuous stand-by within the distributed fabric)
Failover Supervisory --> Backup Supervisory	Hitless, automatic failover

Fail back	Hitless fail back after CLI or GUI trigerring command				
PERFORMANCE SUMMARY					
Switching fabric					
M6100-3S chassis	480 Gbps		Each slot provides 2 x 40G channels (80G half-duplex/160G full-duplex) access to passive backplane		
Type	Distributed fabric				
Switching / Routing capacity					
M6100-3S Chassis	1.4 Tbps		Each Line-Card provides local line-rate capacity		
Throughput					
M6100-3S Chassis (intra-blade)	1,071 Mpps				
M6100-3S Chassis (inter-blade)	357 Mpps				
Latency	64-byte frames	512-byte frames	1024-byte frames	1518-byte frames	12288-byte frames
XCM8948 (10Mbps, Copper)	46.235µs	47.44µs	47.374µs	47.341µs	46.904µs
XCM8944 (10Mbps, Copper)	46.433µs	47.513µs	47.545µs	47.481µs	47.43µs
XCM8948 (100Mbps, Copper)	7.209µs	8.365µs	8.328µs	8.317µs	8.318µs
XCM8944 (100Mbps, Copper)	7.22µs	8.339µs	8.321µs	8.287µs	8.273µs
XCM8944F (100Mbps, Fiber)	5.66µs	5.7µs	5.77µs	5.71µs	5.61µs
XCM8924X (100Mbps, Copper)	8.523µs	8.625µs	8.65µs	8.629µs	8.594µs
XCM8948 (1Gbps, Copper)	3.395µs	4.549µs	4.857µs	4.499µs	4.552µs
XCM8944 (1Gbps, Copper)	3.411µs	4.526µs	4.82µs	4.485µs	4.557µs
XCM8944F (1Gbps, Copper)	2.708µs	2.814µs	2.838µs	2.776µs	2.806µs
XCM8924X (1Gbps, Copper)	2.56µs	2.573µs	2.587µs	2.567µs	2.545µs
XCM8944 (1Gbps, Fiber SFP)	2.368µs	2.474µs	2.538µs	2.466µs	2.436µs
XCM8944F (1Gbps, Fiber SFP)	3.061µs	4.163µs	4.459µs	4.119µs	4.195µs
XCM8924X (1Gbps, Fiber SFP)	2.682µs	2.691µs	2.7µs	2.686µs	2.656µs
XCM8944 (10Gbps, Copper 10GBASE-T)	3.87µs	3.99µs	4.042µs	3.966µs	3.97µs
XCM8944F (10Gbps, Copper 10GBASE-T)	3.92µs	4.04µs	4.062µs	4.016µs	4.04µs
XCM8924X (10Gbps, Copper 10GBASE-T)	3.34µs	3.34µs	3.362µs	3.336µs	3.33µs
XCM8944 (10Gbps, Fiber SFP+)	1.58µs	1.325µs	0.987µs	0.491µs	0.48µs
XCM8944F (10Gbps, Fiber SFP+)	1.63µs	1.555µs	1.412µs	1.136µs	1.14µs
XCM8924X (10Gbps, Fiber SFP+)	1.452µs	1.271µs	1.061µs	0.842µs	0.8µs
Green Ethernet					
Energy Efficient Ethernet (EEE)	IEEE 802.3az Energy Efficient Ethernet Task Force compliance				
Other Metrics					
Forwarding mode	Store-and-forward		Deactivated by default		
Addressing	48-bit MAC address				
Address database size	32,000 MAC addresses				
Number of VLANs	4,096 VLANs (802.1Q) simultaneously				
Number of multicast groups filtered (IGMP)	4K total (2,048 IPv4 and 2,048 IPv6)				
Number of Link Aggregation Groups (LAGs - 802.3ad)	64 LAGs with up to 8 ports per group				
Number of hardware queues for QoS	7 queues				
Number of routes IPv4, Unicast IPv4, Multicast IPv6, Unicast IPv6, Multicast	12,288 IPv4 Unicast Routes in IPv4 Routing Default SDM Template 2,048 IPv4 Multicast Routes in Dual IPv4 and IPv6 SDM Template 4,096 IPv6 Unicast Routes in Dual IPv4 and IPv6 SDM Template 512 IPv6 Multicast Routes in Dual IPv4 and IPv6 SDM Template		SDM (System Data Management, or switch database) templates allow for granular system resources distribution depending on IPv4 or IPv6 applications		

Number of static routes IPv4 IPv6	 512 512	
Number of IP interfaces (port or VLAN)	128	
Jumbo frame support	up to 12K packet size	
Acoustic noise (ANSI-S10.12)	@ 25°C ambient (77°F)	
M6100-3S Base Chassis	53 dB	Fan speed control
Heat Dissipation (BTU)		
M6100-3S Base Chassis	17 Btu/hr	
XCM8948 blade	205 Btu/hr	10,020 Btu/hr with XCM89UP output at 2880W
XCM8944 blade	239 Btu/hr	8,423 Btu/hr with XCM89UP output at 2400W
XCM8944F blade	512 Btu/hr	
XCM8924X blade	682 Btu/hr	
Mean Time Between Failures (MTBF)	@ 25°C ambient (77°F)	@ 50°C ambient (131°F)
M6100-3S Base Chassis	3,393,051 hours (~387.3 years)	791,646 hours (~90.4 years)
XCM8948 blade	862,954 hours (~98.5 years)	306,203 hours (~35 years)
XCM8944 blade	837,030 hours (~95.6 years)	302,649 hours (~34.5 years)
XCM8944F blade	694,849 hours (~79.3 years)	258,531 hours (~29.5 years)
XCM8924X blade	418,002 hours (~47.7 years)	144,699 hours (~16.5 years)
XCM89P daughter card (PoE+)	8,253,931 hours (~942.2 years)	3,905,780 hours (~445.9 years)
XCM89UP daughter card (UPOE)	4,943,696 hours (~564.3 years)	2,430,081 hours (~277,4 years)
APS1000W power supply unit	1,272,908 hours (~145.3 years)	469,094 hours (~53.5 years)
AFT603 fan tray	450,696 hours (~51.4 years)	80,820 hours (~9.2 years)
L2 SERVICES - VLANS		
IEEE 802.1Q VLAN Tagging	Yes	Up to 4,093 VLANs - 802.1Q Tagging
Protocol Based VLANs IP subnet ARP IPX	Yes Yes Yes Yes	
Subnet based VLANs	Yes	
MAC based VLANs	Yes	
Voice VLAN	Yes	Based on phones OUI bytes (internal database, or user-maintained) or protocols (SIP, H323 and SCCP)
Private Edge VLAN	Yes	
Private VLAN	Yes	
IEEE 802.1x Guest VLAN RADIUS based VLAN assignment via .1x RADIUS based Filter ID assignment via .1x MAC-based .1x Unauthenticated VLAN	Yes Yes Yes Yes Yes Yes	IP phones and PCs can authenticate on the same port but under different VLAN assignment policies
Double VLAN Tagging (QoQ) Enabling dvlan-tunnel makes interface Global ethertype (TPID) Interface ethertype (TPID) Customer ID using PVID	Yes Yes Yes Yes Yes	
GARP with GVRP/GMRP	Yes	Automatic registration for membership in VLANs or in multicast groups

Multiple Registration Protocol (MRP)	Yes	Can replace GARP functionality
Multicast VLAN Registration Protocol (MVRP)	Yes	Can replace GVRP functionality
MVR (Multicast VLAN registration)	Yes	
L2 SERVICES - AVAILABILITY		
IEEE 802.3ad - LAGs LACP Static LAGs Local Preference per LAG	Yes Yes Yes Yes	Up to 64 LAGs and up to 8 physical ports per LAG
LAG Hashing	Yes	
LAG Member Port Flaps Tracking	Yes	
LAG Local Preference	Yes	Known unicast traffic egresses only out of local blade LAG interfarce members
Multi Chassis Link Aggregation (MLAG)	Yes	Supported on Supervisory blade only
Storm Control	Yes	
IEEE 802.3x (Full Duplex and flow control) Per port Flow Control	Yes Yes	Asymmetric and Symmetric Flow Control
UDLD Support (Unidirectional Link Detection) Normal-Mode Aggressive-Mode	Yes Yes Yes	
IEEE 802.1D Spanning Tree Protocol	Yes	
IEEE 802.1w Rapid Spanning Tree	Yes	
IEEE 802.1s Multiple Spanning Tree	Yes	
Per VLAN STP (PVSTP) with FastUplink and FastBackbone	Yes (CLI only)	PVST+ interoperability
Per VLAN Rapid STP (PVRSTP)	Yes (CLI only)	RPVST+ interoperability
STP Loop Guard	Yes	
STP Root Guard	Yes	
BPDU Guard	Yes	
STP BPDU Filtering	Yes	
STP BPDU Flooding	Yes	
L2 SERVICES - MULTICAST FILTERING		
IGMPv2 Snooping Support	Yes	
IGMPv3 Snooping Support	Yes	
MLDv1 Snooping Support	Yes	
MLDv2 Snooping Support	Yes	
Expedited Leave function	Yes	
Static L2 Multicast Filtering	Yes	
IGMP Snooping Enable IGMP Snooping per VLAN Snooping Querier	 Yes Yes	
MGMD Snooping Control Packet Flooding Flooding to mRouter Ports Remove Flood-All-Unregistered Option	 Yes Yes Yes	
Multicast VLAN registration (MVR)	Yes	
L3 SERVICES - MULTICAST ROUTING		
IGMP Proxy	Yes	
MLD Proxy	Yes	

Multicast streams routing between subnets, VLANs	Yes	
Multicast static routes (IPv4, IPv6)	Yes	
DVMRP (Distance Vector Multicast Routing Protocol)	Yes	
Neighbor discovery	Yes	
PIM-DM (Multicast Routing - dense mode)	Yes	
PIM-DM (IPv6)	Yes	
PIM-SM (Multicast Routing - sparse mode)	Yes	
PIM-SM (IPv6)	Yes	
PIM multi-hop RP support	Yes	
PIM Timer Accuracy	Yes	
PIM-SM Unhandled Events	Yes	
IPMC replication (hardware support)	Yes	
L3 SERVICES - DHCP		
DHCP IPv4 / DHCP IPv6 Client	Yes	
DHCP IPv4 / DHCP IPv6 Server (Stateless, Stateful)	Yes	
DHCP Snooping IPv4 / IPv6	Yes	
BootP Relay IPv4 / IPv6	Yes	
DHCP Relay IPv4 / IPv6	Yes	
DHCP Relay Option 82 circuit-id and remote-id for VLANs	Yes	
Multiple Helper IPs	Yes	
Auto Install (DHCP options 66, 67, 150 and 55, 125)	Yes	
L3 SERVICES - ROUTING		
Static Routing / ECMP Static Routing Multiple next hops to a given destination Load sharing, Redundancy Default routes Static Reject routes	IPv4/IPv6 Yes Yes Yes Yes	
Port Based Routing	Yes	
VLAN Routing 802.3ad (LAG) for router ports	Yes Yes	
VRRP Pingable VRRP interface VRRP Route/Interface Tracking	IPv4 Yes Yes	
Loopback Interfaces	Yes	
Tunnel interfaces Configured 6to4 tunnels Automatic 6to4 tunnels 6to4 Border Router	IPv4 / IPv6 Yes Yes Yes	
RIP RIPv1/RIPv2	IPv4 Yes	
Route Redistribution	Yes	Enables the exchange of routing information among different routing protocols operating within a router

OSPF	IPv4/IPv6	
OSPFv2 RFC 2328 including older RFC 1583 support	Yes	
OSPFv3	Yes	
OSPF Not-So-Stubby Area (NSSA) Option	Yes	
Forwarding of OSPF Opaque LSAs	Yes	
Passive interface feature	Yes	
Static Area Range Costs feature	Yes	
OSPF Equal Cost Multipath (ECMP)	Yes	
Dynamically learned ECMP routes	Yes	
Statically learned ECMP routes	Yes	
OSPF Max Metric feature	Yes	
Automatic Exiting of Stub Router Mode feature	Yes	
Static Area Range Costs feature	Yes	
OSPF LCA Pacing feature	Yes	
OSPF Flood Blocking feature	Yes	
OSPF Transit-Only Network Hiding	Yes	
IP Multinetting	Yes	
ICMP throttling	Yes	
Router Discovery Protocol	Yes	
DNS Client	IPv4/IPv6	
Border Gateway Protocol version 4 (BGP)	IPv4/IPv6	CLI only
Support of typical routed cata center topologies	Yes	
BGP Route Reflection	Yes	
Private AS Numbers Removal	Yes	
IP Helper	Yes	
Max IP Helper entries	512	
IP Event Dampening	IPv4/IPv6	
Proxy ARP	IPv4/IPv6	
ICMP	IPv4/IPv6	
ICMP redirect detection in hardware	Yes	
Policy Based Routing (PBR)	IPv4/IPv6	
Based on the size of the packet	Yes	
Based on the Protocol of the payload (Protocol ID field)	Yes	
Based on Source MAC address	Yes	
Based on Source or Destination IP address	Yes	
Based on VLAN tag	Yes	
Based on Priority(802.1P priority)	Yes	
NETWORK MONITORING AND DISCOVERY SERVICES		
ISDP (Industry Standard Discovery Protocol)	Yes	inter-operates with devices running CDP
802.1ab LLDP	Yes	
802.1ab LLDP - MED	Yes	
SNMP	V1, V2, V3	
RMON 1,2,3,9	Yes	
sFlow	Yes	
SECURITY		
Network Storm Protection, DoS		
Broadcast, Unicast, Multicast DoS Protection	Yes	
Denial of Service Protection (control plane)	Yes	Switch CPU protection
Denial of Service Protection (data plane)	Yes	Switch Traffic protection

DoS Attacks Protection	SIPDIP SMACDMAC FIRSTFRAG TCPFRAG TCPFLAG TCPPORT	UDPPORT TCPFLAGSEQ TCPOFFSET TCPSYN TCPSYNFIN TCPFINURGPSH	L4PORT ICMP ICMPV4 ICMPV6 ICMPFRAG PINGFLOOD	SYNACK
CPU Rate Limiting	Yes		Applied to IPv4 and IPv6 multicast packets with unknown L3 addresses when IP routing/multicast enabled	
ICMP throttling	Yes		Restrict ICMP, PING traffic for ICMP-based DoS attacks	
Management				
Management ACL (MACAL) Max Rules	Yes 64		Protects management CPU access through the LAN	
Out of band Management	Yes		In-band management can be shut down entirely when out-of-band management network	
Radius accounting	Yes		RFC 2565 and RFC 2866	
TACACS+	Yes			
Malicious Code Detection	Yes		Software image files and Configuration files with digital signatures	
Network Traffic				
Access Control Lists (ACLs)	L2 / L3 / L4		MAC, IPv4, IPv6, TCP, UDP	
Time-based ACLs	Yes			
Protocol-based ACLs	Yes			
ACL over VLANs	Yes			
Dynamic ACLs	Yes			
IEEE 802.1x Radius Port Access Authentication	Yes		Up to 48 clients (802.1x) per port are supported, including the authentication of the users domain	
802.1x MAC Address Authentication Bypass (MAB)	Yes		Supplemental authentication mechanism for non-802.1x devices, based on their MAC address only	
Network Authentication Successive Tiering	Yes		Dot1x-> MAP -> Captive Portal successive authentication methods based on configured time-outs	
Port Security	Yes			
IP Source Guard	Yes		IPv4 / IPv6	
DHCP Snooping	Yes			
Dynamic ARP Inspection	Yes			
MAC Filtering	Yes			
Port MAC Locking	Yes			
Private Edge VLAN	Yes		A protected port doesn't forward any traffic (unicast, multicast, or broadcast) to any other protected port - same switch	
Private VLANs	Yes		Scales Private Edge VLANs by providing Layer 2 isolation between ports across switches in same Layer 2 network	
DATACENTER FEATURES				
Priority Flow Control (PFC) Standardized by IEEE 802.1Qbb	Yes (CLI only)		Enables Flow Control per traffic class on IEEE 802 full-duplex links	
Data Center Bridging Exchange Protocol (DCBX)	Yes (CLI only)		Support of lossless operation for FCoE or ISCSI traffic when all network elements are DCBX enabled	
Enhanced Transmission Selection (ETS)	Yes (CLI only)		Priority-based processing and bandwidth allocations, different Traffic Class Groups (TCGs) for LAN, SAN	

FCoE Initialization Protocol (FIP)	Yes (CLI only)	Used to perform the functions of FC_BB_E device discovery, initialization and maintenance
FIP Snooping Auto-configuration of Ethernet ACLs for FIP frames Emulation of FC point-to-point links within DCB network Enhanced FCoE security preventing FCoE MAC spoofing	Yes (CLI only) Yes Yes Yes	Frame inspection by FIP Snooping Bridges to monitor FIP frames and apply policies based upon L2 header
FIP Snooping Bridge Solution Interior Port Role directly connected to ENode Perimeter Port Role directly connected to ENode FCF Facing Port Role receiving traffic from FCFs to ENodes	Yes (CLI only) Yes Yes Yes	Intended for use at the edge or the interior of the DCB Ethernet switched network
QUALITY OF SERVICE (QOS) - SUMMARY		
Access Lists L2 MAC, L3 IP and L4 Port ACLs Ingress Egress 802.3ad (LAG) for ACL assignment Binding ACLs to VLANs ACL Logging Support for IPv6 fields	 Yes Yes Yes Yes Yes Yes Yes	
DiffServ QoS Edge Node applicability Interior Node applicability 802.3ad (LAG) for service interface Support for IPv6 fields Ingress/Egress	Yes Yes Yes Yes Yes Yes	
IEEE 802.1p COS 802.3ad (LAG) for COS configuration WRED (Weighted Deficit Round Robin) Strict Priority queue technology	Yes Yes Yes Yes	
Single Rate Policing Committed Information Rate Committed Burst Size Excessive Burst Size DiffServ feature applied to class maps	Yes (CLI only) Yes Yes Yes Yes	
Auto-VoIP	Yes, based on protocols (SIP, H323 and SCCP) or on OUI bytes (default database and user-based OUIs) in the phone source MAC address	
iSCSI Flow Acceleration Dot1p Marking IP DSCP Marking	Yes Yes Yes	
QOS - ACL FEATURE SUPPORT		
ACL Support (general, includes IP ACLs) MAC ACL Support IP Rule Match Fields: Destination IP Destination IPv6 IP Destination L4 Port Every Packet IP DSCP IP Precedence IP TOS	Yes Yes Inbound/Outbound Inbound/Outbound Inbound/Outbound Inbound/Outbound Inbound/Outbound Inbound/Outbound Inbound/Outbound	

Protocol	Inbound/Outbound
Source IP (for Mask support see below)	Inbound/Outbound
Source IPv6 IP	Inbound/Outbound
L3 IPv6 Flow Label	Inbound
Source L4 Port	Inbound/Outbound
TCP Flag	Inbound/Outbound
Supports Masking	Inbound/Outbound
MAC Rule Match Fields	
COS	Inbound/Outbound
Destination MAC	Inbound/Outbound
Destination MAC Mask	Inbound/Outbound
Ethertype	Inbound/Outbound
Source MAC	Inbound/Outbound
Source MAC Mask	Inbound/Outbound
VLAN ID	Inbound/Outbound
Rules attributes	Inbound/Outbound
Assign Queue	Inbound/Outbound
Logging -- deny rules	Inbound/Outbound
Mirror (to supported interface types only)	Inbound/Outbound
Redirect (to supported interface types only)	Inbound/Outbound
Rate Limiting -- permit rules	Yes
Interface	
Inbound direction	Yes
Outbound direction	Yes
Supports LAG interfaces	Yes
Supports Control-plane interface	Yes
Multiple ACLs per interface, dir	Yes
Mixed-type ACLs per interface, dir	Yes
Mixed L2/IPv4 ACLs per interface, inbound	Yes
Mixed IPv4/IPv6 ACLs per interface, inbound	Yes
Mixed IPv4/IPv6 ACLs per interface, outbound	Yes
QOS - DIFFSERV FEATURE SUPPORT	
DiffServ Supported	Yes
Class Type	
All	Yes
Class Match Criteria	
COS	Inbound/Outbound
COS2 (Secondary COS)	Inbound
Destination IP (for Mask support see below)	Inbound/Outbound
Destination IPv6 IP	Inbound/Outbound
Destination L4 Port	Inbound/Outbound
Destination MAC (for Mask support see below)	Inbound/Outbound
Ethertype	Inbound/Outbound
Every Packet	Inbound/Outbound
IP DSCP	Inbound/Outbound
IP Precedence	Inbound/Outbound
IP TOS (for Mask support see below)	Inbound/Outbound
Protocol	Inbound/Outbound
Reference Class	Inbound/Outbound
Source IP (for Mask support see below)	Inbound/Outbound
Source IPv6 IP	Inbound/Outbound
L3 IPv6 Flow Label	Inbound
Source L4 Port	Inbound/Outbound
Source MAC (for Mask support see below)	Inbound/Outbound
VLAN ID (Source VID)	Inbound/Outbound
VLAN ID2 (Secondary VLAN) (Source VID)	Inbound/Outbound
Supports Masking	Inbound/Outbound

Policy	
Out Class Unrestricted	Yes
Policy Attributes -- Inbound	
Assign Queue	Yes
Drop	Yes
Mark COS	Yes
Mark COS-AS-COS2	Yes
Mark COS2 (Secondary COS)	Yes
Mark IP DSCP	Yes
Mark IP Precedence	Yes
Mirror (to supported interface types only)	Yes
Police Simple	Yes
Police Single-Rate	Yes
Police Two-Rate	Yes
Police Color Aware Mode	Yes
Redirect (to supported interface types only)	Yes
Policy Attributes -- Outbound	Yes
Drop	Yes
Mark COS	Yes
Mark IP DSCP	Yes
Mark IP Precedence	Yes
Mirror (to supported interface types only)	Yes
Police Simple	Yes
Police Single-Rate	Yes
Police Two-Rate	Yes
Police Color Aware Mode	Yes
Redirect (to supported interface types only)	Yes
Service Interface	
Inbound Slot.Port configurable	Yes
Inbound 'All' Ports configurable	Yes
Outbound Slot.Port configurable	Yes
Outbound 'All' Ports configurable	Yes
Supports LAG interfaces	Yes
Mixed L2/IPv4 match criteria, inbound	Yes
Mixed IPv4/IPv6 match criteria, inbound	Yes
Mixed IPv4/IPv6 match criteria, outbound	Yes
PHB Support	
EF	Yes
AF4x	Yes
AF3x	Yes
AF2x	Yes
AF1x	Yes
CS	Yes
Statistics -- Policy Instance	
Offered	packets
Discarded	packets
QOS - COS FEATURE SUPPORT	
COS Support	Yes
Supports LAG interfaces	Yes
COS Mapping Config	Yes
Configurable per-interface	Yes
IP DSCP Mapping	

COS Queue Config	
Queue Parms configurable per-interface	Yes
Drop Parms configurable per-interface	Yes
Interface Traffic Shaping (for whole egress interface)	Yes
Minimum Bandwidth	Yes
Weighted Deficit Round Robin (WDRR) Support	Yes
Maximum Queue Weight	127
WRED Support	Yes
FUNCTIONAL SUMMARY - IETF RFC STANDARDS AND IEEE NETWORK PROTOCOLS	
Core Management	
RFC 854 — Telnet	RFC 3414 — User-Based Security Model
RFC 855 — Telnet option specifications	RFC 3415 — View-based Access Control Model
RFC 1155 — SMI v1	RFC 3416 — Version 2 of SNMP Protocol Operations
RFC 1157 — SNMP	RFC 3417 — Transport Mappings
RFC 1212 — Concise MIB definitions	RFC 3418 — Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 1867 — HTML/2.0 forms with file upload extensions	Configurable Management VLAN
RFC 1901 — Community-based SNMP v2	SSL 3.0 and TLS 1.0 – RFC 2246 — The TLS protocol, version 1.0 – RFC 2346 — AES cipher suites for Transport layer security – RFC 2818 — HTTP over TLS
RFC 1908 — Coexistence between SNMP v1 and SNMP v2	
RFC 2068 — HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03	
RFC 2271 — SNMP framework MIB	
RFC 2295 — Transparent content negotiation	SSH 1.5 and 2.0 – RFC 4253 — SSH transport layer protocol – RFC 4252 — SSH authentication protocol – RFC 4254 — SSH connection protocol – RFC 4251 — SSH protocol architecture – RFC 4716 — SECSH public key file format – RFC 4419 — Diffie-Hellman group exchange for the SSH transport layer protocol
RFC 2296 — Remote variant selection; RSVA/1.0 state management cookies — draft-ietf-http-state-mgmt-05	
RFC 2576 — Coexistence between SNMP v1, v2, and v3	
RFC 2578 — SMI v2	
RFC 2579 — Textual conventions for SMI v2	
RFC 2580 — Conformance statements for SMI v2	
RFC 3410 — Introduction and Applicability Statements for Internet Standard Management Framework	
RFC 3411 — An Architecture for Describing SNMP Management Frameworks	HTML 4.0 specification, December 1997
RFC 3412 — Message Processing & Dispatching	Java Script™ 1.3
RFC 3413 — SNMP Applications	
Advanced Management	
Industry-standard CLI with the following features: – Scripting capability – Command completion – Context-sensitive help	Optional user password encryption Multisession Telnet server Auto Image Upgrade
Core Switching	
IEEE 802.1AB — Link level discovery protocol	IEEE 802.3ac — VLAN tagging
IEEE 802.1D — Spanning tree	IEEE 802.3ad — Link aggregation
IEEE 802.1p — Ethernet priority with user provisioning and mapping	IEEE 802.3ae — 10 GbE
IEEE 802.1Q — Virtual LANs w/ port-based VLANs	IEEE 802.3af — Power over Ethernet
IEEE 802.1S — Multiple spanning tree compatibility	IEEE 802.3at — Power over Ethernet Plus
IEEE 802.1v — Protocol-based VLANs	IEEE 802.3x — Flow control

IEEE 802.1W — Rapid spanning tree	ANSI/TIA-1057 — LLDP-MED
iEEE 802.1AB — LLDP	GARP — Generic Attribute Registration Protocol: clause 12, 802.1D-2004
IEEE 802.1X — Port-based authentication	GMRP — Dynamic L2 multicast registration: clause 10, 802.1D-2004
IEEE 802.3 — 10Base-T	GVRP — Dynamic VLAN registration: clause 11.2, 802.1Q-2003
IEEE 802.3u — 100Base-T	RFC 4541 — IGMP snooping and MLD snooping
IEEE 802.3ab — 1000Base-T	RFC 5171 — UniDirectional Link Detection (UDLD) Protocol
Additional Layer 2 Functionality	
Broadcast storm recovery	IGMP and MLD snooping querier
Double VLAN/VMAN tagging	Port MAC locking
DHCP Snooping	MAC-based VLANs
Dynamic ARP inspection	IP source guard
Independent VLAN Learning (IVL) support	IP subnet-based VLANs
IPv6 classification APIs	Voice VLANs
Jumbo Ethernet frames	Protected ports
Port mirroring	IGMP snooping
Static MAC filtering	Green Ethernet power savings mode
System Facilities	
Event and error logging facility	RFC 2030 — Simple Network Time Protocol (SNTP) V4 for IPv4, IPv6, and OSI
Runtime and configuration download capability	RFC 2131 — DHCP Client/Server
PING utility	RFC 2132 — DHCP options and BOOTP vendor extensions
XMODEM	RFC 2865 — RADIUS client
RFC 768 — UDP	RFC 2866 — RADIUS accounting
RFC 783 — TFTP	RFC 2868 — RADIUS attributes for tunnel protocol support
RFC 791 — IP	RFC 2869 — RADIUS extensions
RFC 792 — ICMP	RFC 28869bis — RADIUS support for Extensible Authentication Protocol (EAP)
RFC 793 — TCP	RFC 3164 — The BSD syslog protocol
RFC 826 — ARP	RFC 3580 — 802.1X RADIUS usage guidelines
RFC 951 — BOOTP	Power Source Equipment (PSE) IEEE 802.af Powered Ethernet (DTE Power via MDI) standard
RFC 1321 — Message digest algorithm	IEEE Draft P802.1AS/D6.7 — IEEE 802.1AS Time Synchronization Protocol
RFC 1534 — Interoperability between BOOTP and DHCP	
Core Routing	
RFC 826 — Ethernet ARP	RFC 2328 — OSPFv2
RFC 894 — Transmission of IP datagrams over Ethernet networks	RFC 2385—Protection of BGP Sessions via the TCP MD5 Signature Option
RFC 896 — Congestion control in IP/TCP networks	RFC 2453 — RIP v2
RFC 1027 — Using ARP to implement transparent subnet gateways (Proxy ARP)	RFC 3021 — Using 31-Bit Prefixes on Point-to-Point Links
RFC 1256 — ICMP router discovery messages	RFC 3046 — DHCP/BOOTP relay
RFC 1321 — Message digest algorithm	RFC 3101 — The OSPF "Not So Stubby Area" (NSSA) option
RFC 1519 — CIDR	RFC 3768 — Virtual Router Redundancy Protocol (VRRP)
RFC 1765 — OSPF database overflow	RFC 3623—Graceful OSPF Restart
RFC 1812 — Requirements for IPv4 routers	Route redistribution across RIP, BGP, and OSPF
RFC 2082 — RIP-2 MD5 authentication	VLAN routing
RFC 2131 — DHCP relay	

Quality of Service - DiffServ	
RFC 2474 — Definition of the differentiated services field (DS Field) in IPv4/IPv6 headers	RFC 2697 — A Single Rate Three Color Marker
RFC 2475 — An architecture for differentiated services	RFC 3246 — An expedited forwarding PHB (Per-Hop Behavior)
RFC 2597 — Assured forwarding PHB group	RFC 3260 — New terminology and clarifications for DiffServ
Quality of Service - Access Control Lists (ACLs)	
Permit/deny actions for inbound or outbound IP traffic classification based on: – Type of service (ToS) or differentiated services (DS) DSCP field – Source IP address – Destination IP address – TCP/UDP source port – TCP/UDP destination port – IPv6 flow label – IP protocol number	Permit/deny actions for inbound or outbound Layer 2 traffic classification based on: – Source MAC address – Destination MAC address – EtherType – VLAN identifier value or range (outer and/or inner VLAN tag) – 802.1p user priority (outer and/or inner VLAN tag) Optional rule attributes: – Assign matching traffic flow to a specific queue – Redirect or mirror (flow-based mirroring) matching traffic flow to a specific port – Generate trap log entries containing rule hit counts
Quality of Service - Access Control Lists (ACLs)	
Direct user configuration of the following: – IP DSCP to traffic class mapping – IP precedence to traffic class mapping – Interface trust mode: 802.1p, IP Precedence, IP DSCP, or untrusted – Interface traffic shaping rate – Minimum and maximum bandwidth per queue – Strict priority versus weighted (WRR/WDRR/WFQ) scheduling per queue – Tail drop versus Weighted Random Early Detection (WRED) queue depth management	Auto VoIP
Core Multicast	
RFC 1112 — Host extensions for IP multicasting	RFC3973 — PIM-DM
RFC 2236 — IGMP v2	RFC4601 — PIM-SM
RFC 2710 — MLDv1	Draft-ietf-idmr-dvmrp-v3-10 — DVMRP
RFC 2365 — Administratively scoped boundaries	Draft-ietf-magma-igmp-proxy-06.txt — IGMP/MLD-based multicast forwarding (IGMP/MLD proxying)
RFC 3376 — IGMPv3	Draft-ietf-magma-igmpv3-and-routing-05.txt — IGMPv3 and multicast routing protocol interaction
RFC3810 — MLDv2	Static RP configuration
Core BGP4	
RFC 1997 — BGP Communities Attribute	RFC 4271 — A Border Gateway Protocol 4 (BGP-4)
RFC 2385 — Protection of BGP Sessions via the TCP MD5 Signature Option	RFC 4486 — Subcodes for BGP Cease Notification Message
RFC 2545—BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	RFC 4760 — Multiprotocol Extensions for BGP-4
RFC 2918 — Route Refresh Capability for BGP-4	RFC 5492 — Capabilities Advertisement with BGP-4
Core IPv6 Routing	
RFC 1981 — Path MTU for IPv6	RFC 3513 — Addressing architecture for IPv6
RFC 2373 — IPv6 addressing	RFC 3542 — Advanced sockets API for IPv6
RFC 2460 — IPv6 protocol specification	RFC 3587 — IPv6 global unicast address format
RFC 2461 — Neighbor discovery	RFC 3736 — Stateless DHCPv6
RFC 2462 — Stateless autoconfiguration	RFC 4213 — Basic transition mechanisms for IPv6
RFC 2464 — IPv6 over Ethernet	RFC 4291 — Addressing architecture for IPv6
RFC 2711 — IPv6 router alert	RFC 4443 — Internet Control Message Protocol (ICMPv6) for the IPv6 Specification

RFC 3056—Connection of IPv6 Domains via IPv4 Clouds	RFC 5340—OSPF for IPv6
RFC 3315 —Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	RFC 5187 —OSPFv3 Graceful Restart
RFC 3484 — Default address selection for IPv6	RFC 6164 — Using 127-Bit IPv6 Prefixes on Inter-Router Links
RFC 3493 — Basic socket interface for IPv6	RFC 6583 — Operational Neighbor Discovery Problems
Data Center	
IEEE 802.1Qaz Draft 2.4 - DCBX (Data Center Bridging Protocol)	IEEE 802.1Qau Draft 2.4 - QCN (Quantized Congestion Notification)
DCB Capability Exchange Protocol Specification Rev 1.0 - DCBX	IEEE 802.1Qaz Draft 2.4 - ETS (Enhanced Transmission Selection)
DCB Capability Exchange Protocol Base Specification Rev 1.06 - DCBX	FC_BB_5 Rev 2.00, Annex C.3, C.4.3, D3, Section 7.9 - FIP Snooping
SUPPORTED MIBS	
Base Package MIBs MIBs can be dowloaded here: http://www.downloads.netgear.com/docs/m6100/enu/230-11407-01/index.htm	
ANSI/TIA-1057 — LLDP-EXT-MED-MIB	RFC 2674 — Q-BRIDGE-MIB
DIFFSERV DSCP TC (Draft — no RFC)	RFC 2677 — IANA Address Family Numbers MIB
DNS-RESOLVER-MIB (IETF DNS Working Group)	RFC 2819 — RMON MIB
DNS-SERVER-MIB (IETF DNS Working Group)	RFC 2925 — DISMAN-PING-MIB and DISMAN-TRACEROUTE-MIB
GreenEthernet Private MIB	RFC 3273 — RMON MIB for High Capacity Networks
IANA-ADDRESS-FAMILY-NUMBERS-MIB (IANA (3/2002)	RFC 3411 — SNMP Management Frameworks MIB
IEEE 802.1AB-2004 — LLDP MIB	RFC 3411 — SNMP-FRAMEWORK-MIB
IEEE 802.1AB-2005 — LLDP-EXT-DOT3-MIB	RFC 3412 — SNMP-MPD-MIB
POWER ETHERNET MIB (Draft — no RFC)	RFC 3413 — SNMP-NOTIFICATION-MIB
RFC 1155 — SMI-MIB	RFC 3413 — SNMP-PROXY-MIB (initial revision published as RFC 2273)
RFC 1450 — SNMPV2-MIB	RFC 3413 — SNMP-TARGET-MIB (initial revision published as RFC 2273)
RFC 2273 — SNMP Notification MIB, SNMP Target MIB	RFC 3414 — User-based Security Model for SNMPv3 MIB
RFC 2392 — IANA RTPROTO-MIB	RFC 3415 — View-based Access Control Model for SNMP MIB
RFC 2572 — SNMP Message Processing and Dispatching MIB	RFC 3417 — SNMPV2-TM
RFC 2574 — User-based Security Model for SNMPv3 MIB	RFC 3418 — SNMPv2 MIB
RFC 2575 — View-based Access Control Model for SNMP MIB	RFC 3434 — RMON MIB Extensions for High Capacity Alarms
RFC 2576 — SNMP Community MIB	RFC 3584 — SNMP Community MIB
RFC 2578 — SNMPV2-SMI	RFC 3621 — POWER-ETHERNET-MIB
RFC 2579 — SNMPV2-TC	SNMP-RESEARCH-MIB— SNMP research MIB definitions
RFC 2580— SNMPV2-CONF	SR-AGENT-INFO-MIB— SNMP research MIB definitions
RFC 2613 — SMON-MIB	USM-TARGET-TAG-MIB — SNMP research MIB definitions
Switching Package MIBs	
RFC 1213 — MIB-II	RFC 2011 — SNMPv2 Management Information Base
ANSI/TIA 1057 — LLDP-MED MIB	RFC 2213 — Integrated Services MIB
FASTPATH Enterprise MIBs supporting switching features	RFC 2233 — IF-MIB
FASTPATH-MMRP-MIB — MMRP private MIB for IEEE 802.1Q devices	RFC 2233 — The Interfaces Group MIB using SMI v2
FASTPATH-MSRP-MIB — MSRP private MIB for IEEE 802.1Q devices	RFC 2674 — VLAN and Ethernet Priority MIB (P-Bridge MIB)
FASTPATH-MVRP-MIB — MVRP private MIB for IEEE 802.1Q devices	RFC 2737 — Entity MIB (Version 2)
IANAifType-MIB — IANAifType Textual Convention	RFC 2819 — RMON Groups 1,2,3, & 9

IEEE 802.1AB — LLDP MIB	RFC 2863 — Interfaces Group MIB	
IEEE 802.3AD MIB (IEEE8021-AD-MIB)	RFC 3291 — INET Address MIB	
IEEE Draft P802.1AS/D7.0 (IEEE8021-AS-MIB)	RFC 3291 — Textual Conventions for Internet Network Addresses	
IEEE LAG-MIB — Link Aggregation module for managing IEEE 802.3ad	RFC 3621 — Power Ethernet MIB	
LLDP-EXT-DOT3-MIB (part of IEEE Std 802.1AB)	RFC 3635 — Etherlike MIB	
LLDP-MIB (part of IEEE Std 802.1AB)	RFC 3636 — IEEE 802.3 Medium Attachment Units (MAUs) MIB	
Private MIB for 802.1Qat, 802.1Qav Configuration	RFC 4022 — Management Information Base for the Transmission Control Protocol (TCP)	
RFC 1493 — Bridge MIB	RFC 4113 — Management Information Base for the User Datagram Protocol (UDP)	
RFC 1643 — Definitions of managed objects for the Ethernet-like interface types	RFC 4444 — IS-IS MIB	
Routing Package MIBs		
FASTPATH Enterprise MIBs supporting routing features	RFC 2096 — IP Forwarding Table MIB	
IANA-Address-Family-Numbers-MIB	RFC 2668 — IEEE 802.3 Medium Attachment Units (MAUs) MIB	
RFC 1724 — RIP v2 MIB Extension	RFC 2787 — VRRP MIB	
RFC 1850 — OSPF MIB		
IPv6 Management MIBs		
RFC 3419 — TRANSPORT-ADDRESS-MIB	IPv6-MIB (draft)	
IPv6-ICMP-MIB (draft)		
IPv6 Routing MIBs		
RFC 2465 — IPv6 MIB	RFC 2465 — IPv6 MIB	
QoS Package MIB		
RFC 3289 — DIFFSERV-MIB & DIFFSERV-DCSP-TC MIBs	Private MIBs for full configuration of DiffServ, ACL, and CoS functionality	
Security MIB		
RFC 2618 — RADIUS Authentication Client MIB	IEEE8021-PAE-MIB — The Port Access Entity module for managing IEEE 802.1X	
RFC 2620 — RADIUS Accounting MIB	IEEE 802.1X MIB (IEEE 8021-PAE-MIB 2004 Revision)	
Multicast Package MIBs		
RFC 2932 — IPv4 Multicast Routing MIB (for DVMRPv4 and PIMDMv4)	draft-ietf-idmr-dvmrp-mib-11.txt — DVMRP MIB	
RFC 5060 — PIM-SM and PIM-DM MIB for IPv4 and IPv6	draft-ietf-magma-mgmd-mib-05.txt — Multicast Group Membership Discovery MIB (both IGMP and MLD)	
RFC 5240 — BSR Protocol MIB	FASTPATH Enterprise MIBs supporting multicast features	
BGP Package MIB		
RFC 1GP-4 MIB	FASTPATH-BGP-MIB — Private MIB for FASTPATH Border Gateway Protocol Flex package	
Data Center Package MIBs		
IEEE8021-CN-MIB - Congestion Management MIB	FASTPATH-FIPSNOOPING-MIB - FIP Snooping management MIB	
IEEE8021-TC-MIB - Textual conventions MIB for IEEE 802.1		
MANAGEMENT		
Password management	Yes	
Configurable Management VLAN	Yes	
Out-of-band Management	Yes	In-band management can be shut down using Management ACLs when separate management network
Auto Install (BOOTP and DHCP options 66, 67, 150 and 55, 125)	Yes	Scalable deployment process (firmware, config)
Admin access control via Radius and TACACS+	Yes	Policies, Enable
Industry standard CLI (IS-CLI)	Yes	Command Line interface

CLI commands logged to a Syslog server	Yes	
Web-based graphical user interface (GUI)	Yes	Fully functional GUI (exceptions are noted below:)
Features without Web GUI support		
PV(R)STP	CLI only	
Authorization List	CLI only	
Control Plane ACL	CLI only	
DCBX	CLI only	
Priority Flow Control	CLI only	
ETS	CLI only	
FIP Snooping	CLI only	
UDLD	CLI only	
Policy Based Routing	CLI only	
LLPF	CLI only	
BGP	CLI only	
QoS Policy for Single Rate	CLI only	
DHCPv6 Snooping	CLI only	
IPv6 DHCP Relay	CLI only	
eMail Alerting	CLI only	
MMRP	CLI only	
Telnet	Yes	
IPv6 management	Yes	
Dual Software (firmware) image	Yes	Allows non disruptive firmware upgrade process
Dual Configuration file	Yes	Text-based (CLI commands) configuration file
IS-CLI Scripting	Yes	
Port descriptions	Yes	
SNTP client over UDP port 123	Yes	Provides synchronized network timestamp either in broadcast or unicast mode
XMODEM	Yes	
SNMP v1/v2	Yes	
SNMP v3 with multiple IP addresses	Yes	
RMON 1,2,3,9	Yes	
Max History entries	3 * (number of ports in the chassis + LAG + 10)	
Max buckets per History entry	10	
Max Alarm entries	3 * (number of ports in the chassis + LAG + 10)	
Max Event entries	3 * (number of ports in the chassis + LAG + 10)	
Max Log entries per Event entry	10	
Port Mirroring	Yes	
Number of monitor sessions	1 (multiple sessions are configurable)	
Tx/Rx	Yes	
Many to One Port Mirroring	Yes	
LAG supported as source ports	Yes	
Max source ports in a session	Total switch port count	
Remote Port Mirroring (RSPAN)	Yes When a particular session is enabled, any traffic entering or leaving the source ports of that session is copied (mirrored) onto a Remote Switched Port Analyzer (RSPAN) VLAN	
Flow based mirroring	Yes	
Cable Test utility	Yes	CLI, Web GUI
Outbound Telnet	Yes	
SSH	v1/v2	Secure Shell
SSH Session Configuration	Yes	
SSL/HTTPS and TLS v1.0 for web-based access	Yes	
File transfers (uploads, downloads)	TFTP/HTTP	

Secured protocols for file transfers	SCP/SFTP/HTTPS	
HTTP Max Sessions	16	
SSL/HTTPS Max Sessions	16	
HTTP Download (firmware)	Yes	
Email Alerting	Yes (CLI only)	
Syslog (RFC 3164)	Yes	
Persistent log supported	Yes	
USER ADMIN MANAGEMENT		
User ID configuration Max number of configured users Support multiple READWRITE Users Max number of IAS users (internal user database)	Yes 6 Yes 100	
Authentication login lists	Yes	
Authentication Enable lists	Yes	
Authentication HTTP lists	Yes	
Authentication HTTPS lists	Yes	
Authentication Dot1x lists	Yes	
Accounting Exec lists	Yes	
Accounting Commands lists	Yes	
Login History	50	
M6100 SERIES - AVAILABLILITY MEASUREMENTS		
LAG		
LACP Convergence Time (typical/max)	1 sec/2 sec	
LACP Timeout	90 sec	
RSTP		
Convergence Time (typical/max)	4 sec/6 sec	
MLAG (VPC)		
IKey Parameters Role election duration (typical/max) Keepalive Timeout	 14 sec/16 sec 5 sec	 Configurable range is 5-12 sec
Link Flap duration during Role Change (typical/max)	5 sec/5 sec	
Link Down upon reset (typical/max)	16 sec/20 sec	
Traffic Impact - Device failure scenarios Reset Primary Device (typical/max) Power-Off Primary Device (typical/max) Disable VPC on Primary Device (typical/max) Reset Secondary Device Power-Off Secondary Device Disable VPC on Secondary Device	 25 sec/28 sec 15 sec/18 sec 25 sec/28 sec Standard LAG timings apply Standard LAG timings apply Standard LAG timings apply	
Traffic Impact - Link failure scenarios Peer-Link down (typical/max) All member ports in a given VPC going down on Primary All member ports in a given VPC going down on Secondary	 7 sec/10 sec 12 sec/302 sec 12 sec/302 sec	
M6100 SERIES - PLATFORM CONSTANTS		
Maximum number of remote Telnet connections	5	
Maximum number of remote SSH connections	5	
Number of MAC Addresses	32K	

Number of VLANs	4K	
VLAN ID Range	1 - 4093	
Number of 802.1p Traffic Classes	7 classes	
IEEE 802.1x Number of .1x clients per port	 48	
Number of LAGs	64 LAGs with up to 8 ports per group	
Maximum multiple spanning tree instances	31	
MAC based VLANS Number supported	Yes 256	
Number of network buffers	246	
Number of log messages buffered	200	
Static filter entries Unicast MAC and source port Multicast MAC and source port Multicast MAC and destination port (only)	 20 20 1,024	
Subnet based VLANs Number supported	Yes 128	
Protocol Based VLANs Max number of groups Max protocols	Yes 128 16	
Maximum Multicast MAC Addresses entries	2K	
Jumbo Frame Support Max Size Supported	Yes 12k	
Number of IP Source Guard stations	250	
Number of DHCP snooping bindings	32K	
Number of DHCPv6 snooping bindings	32K	
Number of DHCP snooping static entries	1024	
LLDP-MED number of remote nodes LLDP Remote Management address buffers LLDP Unknown TLV address buffers LLDP Organizationally Defined Large TLV buffers LLDP Organizationally Defined Small TLV buffers	2 x Total switch port count 100 100 12 x Total switch port count / 100 Total switch port count	
Port MAC Locking Dynamic addresses per port Static addresses per port	Yes 4096 48	
sFlow Number of samplers Number of pollers Number of receivers	 Total switch port count Total switch port count 8	
Radius Max Authentication servers Max Accounting servers	 32 32	
Number of Routes (v4/v6) IPv4 only SDM build IPv4/IPv6 SDM build IPv4 routes IPv6 routes RIP application route scaling OSPF application route scaling BGP application route scaling BGP application peer scaling	 12,288 8,160 4,096 512 12,000 12,000 128	SDM (System Data Management, or switch database)
Number of routing interfaces (including port/vlan)	128	

Number of static routes (v4/v6)	512/512	
Routing Heap size IPv4 only SDM build IPv4/IPv6 SDM build	 26M 32M	 SDM (System Data Management, or switch database)
OSPF OSPFv2 max neighbors OSPFv3 max neighbors OSPFv3 max neighbors per interface	 400 400 100	
Tunnels Number of configured v6-over-v4 tunnels Number of automatic (6to4) tunnels Number of 6to4 next hops	 8 1 16	
DHCP Server Max number of pools Total max leases	 256 4K	
DNS Client Concurrent requests Name server entries Seach list entries Static host entries Cache entries Domain search list entries	 16 8 6 64 128 32	
DHCPv6 Server Max number of pools DNS domain names within a pool DNS server addresses within a pool Delegated prefix definitions within a pool	 256 5 8 10	
Number of Host Entries (ARP/NDP) IPv4 only SDM build IPv4/IPv6 SDM build (v4/v6) Static v4 ARP Entries	 8,192 6,144 / 2,560 128	 SDM (System Data Management, or switch database)
Number of ECMP Next Hops per Route	16	
Total ECMP nexthops in Hardware	4096	
IGMPv3 / MLDv2 Snooping Limits IGMPv3/MLDv2 HW entries when IP Multicast present IGMPv3/MLDv2 HW entries when Routing w/o IP Multicast IGMPv3/MLDv2 HW entries when Switching only	 512 2,048 4,096	
IP Multicast Number of IPv4/IPv6 Multicast Forwarding Entries IGMP Group Memberships per system DVMRP Neighbors PIM-DM Neighbors PIM-SM Neighbors PIM-SM Static RP Entries PIM-SM Candidate RP Group Range Entries PIM-SM SSM Range Entries IGMP Sources processed per group per message	 1,536 (IPv4) and 512 (IPv6) 2K (IPv4) and 2K (IPv6) 256 256 256 5 20 5 73	
ACL Limits Maximum Number of ACLs (any type) Maximum Number Configurable Rules per List Maximum ACL Rules per Interface and Direction Maximum ACL Rules per Interface and Direction (IPv6) Maximum ACL Rules (system-wide) Maximum ACL Logging Rules (system-wide)	 100 1,023 1,023 893 ingress / 509 egress 16K 128	

COS Device Characteristics		
Configurable Queues per Port	7 queues	
Configurable Drop Precedence Levels	3	
DiffServ Device Limits		
Number of Queues	7	
Requires TLV to contain all policy instances combined	Yes	
Max Rules per Class	13	
Max Instances per Policy	28	
Max Attributes per Instance	3	
Max Service Interfaces	208	
Max Table Entries		
Class Table	32	
Class Rule Table	416	
Policy Table	64	
Policy Instance Table	1,792	
Policy Attribute Table	5,376	
Max Nested Class Chain Rule Count	26	
AutoVoIP number of voice calls	144	
iSCSI Flow Acceleration		
Max Monitored TCP Ports/IP Addresses	16	
Max Sessions	192	
Max Connections	192	
LEDS		
Per port	Speed, Link, Activity	
Per I/O blade	Supervisor, Status	
Power Supply (APS1000W)	Status	
M6100 Base Chassis - Rear	Power	
PHYSICAL SPECIFICATIONS		
Dimensions		
M6100-3S Base Chassis	Width: 17.01 inches (43.2 cm); Height: 4U - 6.93 inches (17.59 cm); Depth: 17.39 inches (44.16 cm)	
I/O Blades (all models)	Width: 16.87 inches (42.86 cm); Height: 1.59 inches (4.05 cm); Depth: 12.74 inches (32.35 cm)	
PoE Daughter Cards (all models)	Width: 13.12 inches (33.32 cm); Height: 0.65 inches (1.66 cm); Depth: 5.05 inches (12.82 cm)	
AFT603 Fan Tray	Width: 15.87 inches (40.3 cm); Height: 4.94 inches (12.56 cm); Depth: 3.35 inches (8.5 cm)	
APS1000W Power Supply unit	Width: 3.40 inches (8.64 cm); Height: 1.55 inches (3.93 cm); Depth: 8.17 inches (20.75 cm)	
Weight		
M6100-3S Base Chassis (empty)	27.34 lb (12.4 kg)	
M6100-3S Chassis (fully loaded)	69.67 lbs (31.6 kg)	Worst case example with 3 x XCM8924X and 4 x APS1000W
XCM8948 I/O Blade	7.12 lb (3.23 kg)	
XCM8944 I/O Blade	7.41 lb (3.36 kg)	
XCM8944F I/O Blade	7.45 lb (3.38 kg)	
XCM8924X I/O Blade	9.57 lb (4.34 kg)	
XCM89P PoE+ Daughter Card	0.49 lb (0.22 kg)	
XCM89UP UPOE Daughter Card	0.53 lb (0.24 kg)	
AFT603 Fan Tray	3.92 lb (1.78 kg)	
APS1000W Power Supply unit	2.27 lb (1.03 kg)	
POWER CONSUMPTION		
Worst case, all ports used, line-rate traffic		
M6100-3S Chassis	5W max	Use M6100 Expert configurator www.netgear.com/m6100 under Resources tab
XCM8948 I/O Blade without PoE daughter card	60W max	
XCM8948 I/O Blade with XCM89UP output at 2,880W	2,935W max	
XCM8944 I/O Blade without PoE daughter card	70W max	
XCM8944 I/O Blade without XCM89UP output at 2,400W	2,496W max	
XCM8944F I/O Blade	150W max	
XCM8924X I/O Blade	200W max	

ENVIRONMENTAL SPECIFICATIONS		
Operating: Temperature Humidity Altitude	 32° to 122°F (0° to 50°C) 90% maximum relative humidity, non-condensing 10,000 ft (3,000 m) maximum	
Storage: Temperature Humidity Altitude	 – 4° to 158°F (–20° to 70°C) 95% maximum relative humidity, non-condensing 10,000 ft (3,000 m) maximum	
ELECTROMAGNETIC EMISSIONS AND IMMUNITY		
Certifications	CE mark, commercial FCC Part 15 Class A VCCI Class A Class A EN 55022 (CISPR 22) Class A Class A C-Tick EN 50082-1 EN 55024	
SAFETY		
Certifications	CE mark, commercial CSA certified (CSA 22.2 #950) UL listed (UL 1950)/cUL IEC 950/EN 60950	
PACKAGE CONTENT		
M6100-44G3-POE+ Starter Kit (XCM8903SK-10000S)		
M6100-3S Base Chassis	M6100-3S Chassis Switch (XCM8903) 2-post rack mount kit 1 pair of 4-post sliding rails 2 blank panels for empty I/O slots 3 power supply panels for empty PSU slots Installation guide Resource CD (technical documentation, manuals) C14 to C15 power cord (for PDUs and UPS) Australian power cord (AC plug --> C15) Japanese power cord (AC plug --> C15)	The Starter Kit Bundle consists of a Master Carton shipping on a pallet: all components inside the Master Carton ship in their individual packaging.
APS1000W Power Supply unit	APS1000W PSU North American power cord (AC plug --> C15) UK power cord (AC plug --> C15) Euro schuko power cord (AC plug --> C15)	
AFT603 Fan Tray	AFT603 Fan Tray	
XCM8944 I/O Blade	XCM8944 Blade (40x1G + 4x10G) RJ45 straight-through wiring serial console cable to DB9 Mini-USB console cable Installation guide Resource CD (technical documentation, manuals)	
XCM89P PoE+ Daughter Card	XCM89P PoE+ Daughter Card Installation guide	
I/O Blades		
XCM8948 I/O Blade	XCM8948 Blade (48x1G) RJ45 straight-through wiring serial console cable to DB9 Mini-USB console cable Installation guide Resource CD (technical documentation, manuals)	

XCM8944 I/O Blade	XCM8944 Blade (40x1G + 4x10G) RJ45 straight-through wiring serial console cable to DB9 Mini-USB console cable Installation guide Resource CD (technical documentation, manuals)	
XCM8944F I/O Blade	XCM8944F Blade (40xSFP + 4x10G) RJ45 straight-through wiring serial console cable to DB9 Mini-USB console cable Installation guide Resource CD (technical documentation, manuals)	
XCM8924X I/O Blade	XCM8924X Blade (24x10G) RJ45 straight-through wiring serial console cable to DB9 Mini-USB console cable Installation guide Resource CD (technical documentation, manuals)	
Accessories		
XCM89P PoE+ Daughter Card	XCM89P PoE+ Daughter Card Installation guide	
XCM89UP UPOE Daughter Card	XCM89UP UPOE Daughter Card Installation guide	
APS1000W Power Supply unit	APS1000W PSU (-100NES version) North American power cord (AC plug --> C15) (-100NES version) UK power cord (AC plug --> C15) (-100NES version) Euro schuko power cord (AC plug --> C15) (-100AJS version) Australian power cord (AC plug --> C15) (-100AJS version) Japanese power cord (AC plug --> C15)	
AFT603 Fan Tray	AFT603 Fan Tray	
RPS4000v2 Additional 1U Power Shelf	RPS4000v2 External RPS EPS 4-Slot PSU Bay (-200NES version) North American power cord (-200NES version) UK power cord (-200NES version) Euro schuko power cord (-200AJS version) Australian power cord (-200AJS version) Japanese power cord Installation Guide Resource CD (technical documentation, manuals)	
OPTIONAL MODULES AND ACCESSORIES		
M6100-3S Base Chassis		**Ordering SKU:**
XCM8903SK	M6100-44G3-POE+ Starter Kit Bundle	XCM8903SK-10000S
XCM8948	I/O Blade 48 x 1G (RJ45)	XCM8948-10000S
XCM8944	I/O Blade 40 x 1G (RJ45), 2 x SFP+, 2 x 10GBASE-T	XCM8944-10000S
XCM8944F	I/O Blade 40 x 1G (SFP), 2 x SFP+, 2 x 10GBASE-T	XCM8944F-10000S
XCM8924X	I/O Blade 24 x 10GBASE-T, 16 x SFP+ (shared)	XCM8924X-10000S
XCM89P	Daughter Card PoE+ XCM8944/XCM8948	XCM89P-10000S
XCM89UP	Daughter Card PoE+/UPOE XCM8944/XCM8948	XCM89UP-10000S
AFT603	PSU 1,000W AC	AFT603-10000S
APS1000W	Fan Tray with front-to-back cooling principle	APS1000W-100NES/AJS
RPS4000v2	Additional 1U Power Shelf	RPS4000-200NES/AJS
XCM8948 I/O Blade		
XCM89P	Daughter Card PoE+ XCM8944/XCM8948	XCM89P-10000S
XCM89UP	Daughter Card PoE+/UPOE XCM8944/XCM8948	XCM89UP-10000S

XCM8944 I/O Blade XCM89P XCM89UP AGM731F AGM732F AXC761 AXC763 AXM761 AXM761 (Pack of 10 units) AXM762 AXM762 (Pack of 10 units) AXM763	Daughter Card PoE+ XCM8944/XCM8948 Daughter Card PoE+/UPOE XCM8944/XCM8948 1000Base-SX SFP GBIC (Multimode) 1000Base-LX SFP GBIC (Single mode) 10GSFP+ Cu (passive) SFP+ to SFP+ Direct Attach Cable 1m 10GSFP+ Cu (passive) SFP+ to SFP+ Direct Attach Cable 3m 10GBase-SR SFP+ GBIC (OM3/OM4 Multimode) 10GBase-SR SFP+ GBIC (OM3/OM4 Multimode) 10GBase-LR SFP+ GBIC (Single mode) 10GBase-LR SFP+ GBIC (Single mode) 10GBase-LRM SFP+ GBIC (Long Reach Multimode for OM1/OM2, also compatible with OM3/OM4)	XCM89P-10000S XCM89UP-10000S AGM731F AGM732F AXC761-10000S AXC763 -10000S AXM761-10000S AXM761P10-10000S AXM762-10000S AXM762P10-10000S AXM763-10000S
XCM8944F I/O Blade AFM735 AGM731F AGM732F AXC761 AXC763 AXM761 AXM761 (Pack of 10 units) AXM762 AXM762 (Pack of 10 units) AXM763	100Base-FX SFP GBIC (Multimode) 1000Base-SX SFP GBIC (Multimode) 1000Base-LX SFP GBIC (Single mode) 10GSFP+ Cu (passive) SFP+ to SFP+ Direct Attach Cable 1m 10GSFP+ Cu (passive) SFP+ to SFP+ Direct Attach Cable 3m 10GBase-SR SFP+ GBIC (OM3/OM4 Multimode) 10GBase-SR SFP+ GBIC (OM3/OM4 Multimode) 10GBase-LR SFP+ GBIC (Single mode) 10GBase-LR SFP+ GBIC (Single mode) 10GBase-LRM SFP+ GBIC (Long Reach Multimode for OM1/OM2, also compatible with OM3/OM4)	AFM735-10000S AGM731F AGM732F AXC761-10000S AXC763 -10000S AXM761-10000S AXM761P10-10000S AXM762-10000S AXM762P10-10000S AXM763-10000S
XCM8924X I/O Blade AGM731F AGM732F AGM734 AXC761 AXC763 AXM761 AXM761 (Pack of 10 units) AXM762 AXM762 (Pack of 10 units) AXM763	1000Base-SX SFP GBIC (Multimode) 1000Base-LX SFP GBIC (Single mode) 1000Base-T RJ45 SFP GBIC 10GSFP+ Cu (passive) SFP+ to SFP+ Direct Attach Cable 1m 10GSFP+ Cu (passive) SFP+ to SFP+ Direct Attach Cable 3m 10GBase-SR SFP+ GBIC (OM3/OM4 Multimode) 10GBase-SR SFP+ GBIC (OM3/OM4 Multimode) 10GBase-LR SFP+ GBIC (Single mode) 10GBase-LR SFP+ GBIC (Single mode) 10GBase-LRM SFP+ GBIC (Long Reach Multimode for OM1/OM2, also compatible with OM3/OM4)	AGM731F AGM732F AGM734-10000S AXC761-10000S AXC763 -10000S AXM761-10000S AXM761P10-10000S AXM762-10000S AXM762P10-10000S AXM763-10000S
WARRANTY AND SUPPORT		
ProSafe Lifetime Hardware Warranty*	Included, lifetime	
90 days of Technical Support via phone and email*	Included, 90 days after purchase	
Lifetime Technical Support through online chat*	Included, lifetime	
Lifetime Next Business Day hardware replacement*	Included, lifetime	
PROSUPPORT SERVICE PACKS		
Installation contracts		
PSB0304-10000S	Remote Installation Setup and Configuration Service Contract	
PSP1104-10000S	Onsite Installation Setup and Configuration Service Contract	
Supplemental support contracts		
PMP3134-10000S	OnSite NBD Replacement 3-year CAT 4	
PMB0334-10000S	OnCall 24x7 3-year CAT 4	
PMB0354-10000S	OnCall 24x7 5-year CAT 4	

ORDERING INFORMATION	
M6100-44G3-POE+ Starter Kit Bundle Worldwide	XCM8903SK-10000S
XCM8948 I/O Blade Worldwide	XCM8948-10000S
XCM8944 I/O Blade Worldwide	XCM8944-10000S
XCM8944F I/O Blade Worldwide	XCM8944F-10000S
XCM8924X I/O Blade Worldwide	XCM8924X-10000S
XCM89P PoE+ Daughter Card Worldwide	XCM89P-10000S
XCM89UP UPOE Daughter Card Worldwide	XCM89UP-10000S
AAPS1000W Power Supply unit Americas, Europe Asia Pacific	 APS1000W-100NES APS1000W-100AJS
AFT603 Fan Tray Worldwide	 AFT603-10000S
RPS4000v2 Additional 1U Power Shelf Americas, Europe Asia Pacific	 RPS4000-200NES RPS4000-200AJS

* This product comes with a limited warranty that is valid only if purchased from a NETGEAR authorized reseller and modifications to product may void the warranty; covers hardware, fans and internal power supplies - not software or external power supplies See http://www.netgear.com/about/warranty/ for details. Lifetime technical support includes basic phone support for 90 days from purchase date and lifetime online chat support when purchased from a NETGEAR authorized reseller.