NETGEAR®

# ProSAFE® 10 Gigabit Managed Switches

Data Sheet

M7100 series

Auto-iSCSI DETECTION OPTIMIZATION

The NETGEAR® 10 Gigabit M7100 series consists of a fully managed, low-latency, line-rate 10G Copper "Base-T" switch solution; 24 ports 10GBase-T (RJ45) that support Fast Ethernet, Gigabit Ethernet and 10 Gigabit speeds for server, storage and network progressive upgrade; 4 ports SFP+ that broaden 10 Gigabit connectivity for 1G/10G fiber uplinks and other DAC connections.

The M7100 series is ideal for all organizations considering reliable, affordable and simple 10 Gigabit Ethernet Top-of-Rack server access layer and high-density, high-performance 10GbE backbone architectures.

## Highlights

### Layer 2+ with static routing

- The M7100 series comes with Port-based/VLAN-based/Subnet-based "static routing" Layer 2+ versions
- L3 fixed routes to the next hop towards the destination network are added to the routing table
- L3 routing is wire-speed in the M7100 series hardware with up to 128 static routes (IPv4)

### 10 Gigabit transition with Base-T

- 10GBase-T, like other Base-T technologies, uses the standard RJ45 Ethernet jack
- It is backward compatible, auto-negotiating between higher and lower speeds – thereby not forcing an all at once network equipment upgrade
- Cat5/Cat5E are supported for Gigabit speeds; when Cat6 twisted pair copper cabling is a minimum requirement for 10 Gigabit up to 30 meters
- Cat6A or newer Cat7 cabling allow for up to 100 meter 10GBase-T connections

### Top-of-the-line performance and IPv6 ready

- Two redundant, hot-swap power supplies (one PSU comes with the switch; second optional PSU is ordered separately)
- Two removable fan trays provide front-to-back cooling airflow for best compatibility with data center hot aisle/cold aisle airflow patterns
- Multi-Chassis Link Aggregation (MLAG) allows for active-active redundant server connections across two switches, using LACP

### Top-of-rack availability

- Two redundant, hot-swap power supplies (one PSU comes with the switch; second optional PSU is ordered separately)
- Two removable fan trays provide front-to-back cooling airflow for best compatibility with data center hot aisle/cold aisle airflow patterns

### Industry standard management

- Industry standard command line interface (CLI)
- Fully functional NETGEAR web interface (GUI)

### Industry leading warranty

- NETGEAR M7100 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

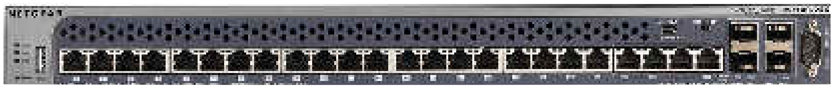
LIFETIME WARRANTY Hardware Warranty

LIFETIME WARRANTY Next Business Day

LIFETIME Tech Support

## Hardware at a Glance

| | FRONT | | | | REAR | | |
|---|---|---|---|---|---|---|---|
| Model name | 100/1000/ 10GBase-T RJ45 ports | 1000/10GBase-X Fiber SFP+ ports | Management console | Storage (image, config) | Modular PSUs (redundant, hot-swap) | Modular Fan Trays (front-to-back cooling, hot-swap) | Model number |
| M7100-24X | 24 | 4 (shared) | 1 x RS232 DB9,<br>1 x Mini-USB (selectable) | 1 x USB | 2<br>(Part-number: APS300W)<br>(1 power supply already installed) | 2<br>(Part-number: AFT200)<br>(2 fan trays already installed) | XSM7224 v1h1 |



M7100-24X is a 24 x 10Gbase-T version, Layer 2+

4 shared SFP+

M7100 series rear view

2 modular, redundant PSUs

- Each M7100 series ships with one installed modular PSU
- Additional PSU unit is available for hot swap HA (APS300W)

2 modular fan trays

- Each M7100 series ships with two installed fan trays
- Spare units are available for hot swap HA (AFT200)

## Software at a Glance

| | LAYER 2+ PACKAGE | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Model name | IPv4/IPv6 ACL and QoS | IPv4/IPv6 Multicast filtering | Auto-iSCSI Auto-VoIP | EEE (802.3az) Auto-EEE | VLANs | Convergence | IPv4 Unicast Static Routing | Model number |
| M7100-24X | L2, L3, L4, ingress, egress, 1 Kbps | IGMP and MLD Snooping, Querier mode, MVR | Yes | Yes | Static, Dynamic, Voice, MAC, Subnet, Protocol-based, QoQ, Private VLANs | LLDP-MED, RADIUS, 802.1X, timer | Yes<br>(Port-based, Subnet, VLANs) | XSM7224 v1h1 |

## Performance at a Glance

| | TABLE SIZE | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Model name | Packet buffer | CPU | ACLs | MAC address table ARP/NDP table VLANs DHCP server | Fabric | Latency | Static Routes | Multicast IGMP Group member-ship | sFlow | Model number |
| M7100-24X | 16 Mb | 800Mhz 256M RAM 128M Flash | 1K ingress<br>512 egress | 32K MAC<br>6K ARP/NDP<br>VLANs: 1K<br>DHCP: 16 pools<br>1,024 max leases | 480Gbps line-rate | 10GBase-T <3.7 µs<br>SFP+ <1.8 µs | 128 IPv4 | 2K | 32 samplers<br>52 pollers<br>8 receivers | XSM7224 v1h1 |

## Product Brief

The 10 Gigabit Aggregation M7100 series switches are NETGEAR affordable fully managed switches for 1G/10G server access layer in campus and enterprise networks, and for high-density, high-performance 10GbE backbone architectures. The M7100 series delivers pure line-rate performance for top-of-rack virtualization or convergence, without having to pay the exorbitant acquisition and maintenance costs associated by other networking vendors. NETGEAR 10 Gigabit Aggregation solutions combine latest advances in hardware and software engineering for higher availability, lower latency and stronger security, at a high-value price point. Like all NETGEAR products, the M7100 series delivers more functionality with less difficulty: Auto-iSCSI optimization, Private VLANs and Local Proxy ARP take the complexity out of delivering network services for virtualized servers and 10 Gigabit infrastructures.

### NETGEAR 10 Gigabit M7100 series key features:

- Line-rate 10G Copper “Base-T” switch solution with low latency
- 24 ports 10GBase-T (RJ45) supporting Fast Ethernet, Gigabit Ethernet and 10 Gigabit speeds for server and network progressive upgrade
- 4 ports SFP+ for 1G/10G fiber uplinks and other DAC connections
- IPv4 routing in Layer 2+ package (static routing) with IPv4/IPv6 ACLs and QoS
- Enterprise-class L2/L3 tables with 32K MAC, 6K ARP/NDP, 1K VLANs, 128 static L3 routes
- Two redundant, hot-swap power supplies (one PSU comes with the switch; second optional PSU is ordered separately)
- Two removable fan trays and front-to-back cooling airflow for best compatibility with data center hot aisle/cold aisle airflow patterns
- Auto-EEE Energy Efficient Ethernet associated with Power Back Off for 15% to 20% less consumption when short copper cables

### NETGEAR 10 Gigabit M7100 series software features:

- Innovative multi-vendor Auto-iSCSI capabilities for easier virtualization optimization, iSCSI flow acceleration and automatic protection/QoS
- Automatic multi-vendor Voice over IP prioritization based on SIP, H323 and SCCP protocol detection
- Voice VLAN and LLDP-MED  for automatic IP phones QoS and VLAN configuration
- IPv4/IPv6 Multicast filtering with IGMP and MLD snooping, Querier mode and MVR for simplified video deployments
- Advanced classifier-based hardware implementation for L2 (MAC), L3 (IP) and L4 (UDP/TCP transport ports) security and prioritization
- Unidirectional Link Detection Protocol (UDLD) prevents forwarding anomalies

### NETGEAR 10 Gigabit M7100 series link aggregation and channeling features:

- Flexible Port-Channel/LAG (802.3ad) implementation for maximum compatibility, fault tolerance and load sharing with any type of Ethernet channeling
- Including static (selectable hashingalgorithms) or dynamic LAGs (LACP)
- Multi Chassis Link Aggregation (MLAG) between two M7100 switches overcomes limitations of Spanning Tree, increasing bandwidth while preserving redundancy

### NETGEAR 10 Gigabit M7100 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 implementation
- Selectable serial RS232 DB9 and Mini-USB port for management console
- Standard USB port for local storage, 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

### NETGEAR 10 Gigabit M7100 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

| | |
|---|---|
| **Layer 3 hardware with L2+ software affordability** | |
| M7100 series models are built upon L3 hardware platform while Layer 2+ software package allows for better budget optimization | • M7100 series uses latest generation silicon low-power 65-nanometer technology<br>• M7100 series L2 and L3 switching features (access control list, classification, filtering, IPv4 routing) are performed in hardware at interface line rate for voice, video, and data convergence |
| M7100 series Layer 2+ software package provides straight forward IP static routing capabilities for physical interfaces, VLANs and subnets | • M7100-24X<br>• At the edge of campus networks or in the server room, static routes are often preferred for simplicity (L3 fixed routes to the next hop towards the destination network are manually added to the routing table), without any impact on performance because L3 routing is wire-speed in M7100 series hardware |
| **Top-of-the-line switching performance** | |
| 32K MAC address table, 1K concurrent VLANs and 128 static routes for demanding enterprise and campus network access/distribution layers | |
| 80 PLUS certified power supplies for energy high efficiency | |
| Green Ethernet with Energy Efficient Ethernet (EEE) defined by IEEE 802.3az Energy Efficient Ethernet Task Force | • Supports Auto-EEE mode<br>• Additionally, Power Back Off feature drops power consumption by 15% to 20% when short copper cables are detected |
| Increased packet buffering with up to 16 Mb dynamically shared accross all interfaces for most intensive virtualization applications | |
| Low latency at all network speeds, including 10 Gigabit Copper links | |
| 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 by: | • Detecting the establishment and termination of iSCSI sessions and connections by snooping packets used in the iSCSI protocol<br>• Maintaining a database of currently active iSCSI sessions and connections to store data about the participants; this allows the formulation of classifier rules giving the data packets for the session the desired QoS treatment<br>• Installing and removing classifier rule sets as needed for the iSCSI session traffic<br>• Monitoring activity in the iSCSI sessions to allow for aging out session entries if the session termination packets are not received<br>• Avoiding session interruptions during times of congestion that would otherwise cause iSCSI packets to be dropped |
| **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 Switch Serial Number and Switch primary MAC address are reported by a simple "show" command in the CLI - facilitating discovery and remote configuration operations | |
| 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** | |
| Large 10 Gigabit choice for access with 10GBase-T ports for legacy Cat6 RJ45 short connections (up to 300m) and Cat6A/Cat 7 connections up to 100m; and SFP+ ports for fiber optic uplinks or short, low-latency copper DAC cables | |
| 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 | |
| 100Mbps and 1000Mbps backward compatiblity on all 10GBase-T RJ45 ports | |
| 1000Mbps backward compatibility on all SFP+ fiber ports | |

## Modern access layer features highlights

| | |
|---|---|
| IPv6 support with multicasting (MLD for IPv6 filtering), ACLs and QoS | |
| **Tier 1 availability** | |
| Multi-Chassis Link Aggregation (MLAG) for distributed link aggregation across two independant switches | • A server with two Ethernet ports (or any Ethernet device such as an edge switch) can use virtual port channeling with LACP across two M7100 series<br>• Active-active teaming across two separate fabrics at Layer 2 without creating loops<br>• Load-balancing and automatic failover ensure greater bandwidth network layers and maximize redundancy |
| 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 | |
| PVSTP and PVRSTP implementation (CLI only) follows same rules than other vendors' Per VLAN STP/RSTP for strict interoperability | |
| IP address conflict detection performed by the embedded DHCP server prevents accidental IP address duplicates from perturbing the overall network stability | |
| Power redundancy for higher availability when mission critical, including hot-swap PSUs and Fans | |
| **Ease of management and control** | |
| Dual firmware image and dual configuration file for transparent firmware updates/configuration changes with minimum service interruption | |
| Flexible Port-Channel/LAG (802.3ad) 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 dynamic LAGs (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) and 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 GVRP 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 | |
| Simplified VLAN configuration with industry-standard Access Ports for 802.1Q unaware endpoints and Trunk Ports for switch-to-switch links with Native VLAN | |
| 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 | |

## Modern access layer features highlights

<table>
<tr><td colspan="2">Remote mirroring (RSPAN) can transport packets captured on an interface on a source switch across the network to a destination on a possibly different destination switch</td></tr>
<tr><td colspan="2"><b>Engineered for convergence</b></td></tr>
<tr><td colspan="2">Audio (Voice over IP) and Video (multicasting) comprehensive switching, filtering, routing and prioritization</td></tr>
<tr><td colspan="2">Auto-VoIP, Voice VLAN and LLDP-MED support for IP phones QoS and VLAN configuration</td></tr>
<tr><td colspan="2">IGMP Snooping for IPv4, MLD Snooping for IPv6 and Querier mode facilitate fast receivers joins and leaves for multicast streams and ensure multicast traffic only reaches interested receivers without the need of a Multicast router</td></tr>
<tr><td colspan="2">Multicast VLAN Registration (MVR) uses a dedicated Multicast VLAN to forward multicast streams and avoid duplication for clients in different VLANs</td></tr>
<tr><td colspan="2">Schedule enablement</td></tr>
<tr><td colspan="2"><b>Enterprise security</b></td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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 topology by creating loops</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td>Dynamic 802.1x VLAN assignment mode, including Dynamic VLAN creation mode and Guest VLAN/ Unauthenticated VLAN are supported for rigorous user and equipment RADIUS policy server enforcement</td><td>• Up to 48 clients (802.1x) per port are supported, including the authentication of the users domain, in order to facilitate convergent deployments: 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 data VLANs</td></tr>
<tr><td>802.1x MAC Address Authentication Bypass (MAB) is a:</td><td>• A list of authorized MAC addresses of client NICs is maintained on the RADIUS server for MAB purpose<br>• MAB can be configured on a per-port basis on the switch<br>• MAB initiates only after the dot1x authentication process times out, and only when clients don't respond to any of the EAPOL packets sent by the switch<br>• When 802.1X unaware clients try to connect, the switch sends the MAC address of each client to the authentication server<br>• The RADIUS server checks the MAC address of the client NIC against the list of authorized addresses<br>• The RADIUS server returns the access policy and VLAN assignment to the switch for each client</td></tr>
<tr><td>With Successive Tiering, the Authentication Manager allows for authentication methods per port for a Tiered Authentication based on configured time-outs</td><td>• By default, configuration authentication methods are tried in this order: Dot1x, then MAB, then CaptivPortal (web authentication)<br>• With BYOD, such Tiered Authentication is powerful and simple to implement with strict policies<br>• For instance, when a client is connecting, M7100 tries to authencate the user/client using the three methods above, the one after the other<br>• The admin can restrict the configuration such that no other method is allowed to follow the captive portal method, for instance</td></tr>
<tr><td colspan="2">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 so the traffic can pass the metro core in a simple, secure manner</td></tr>
</table>

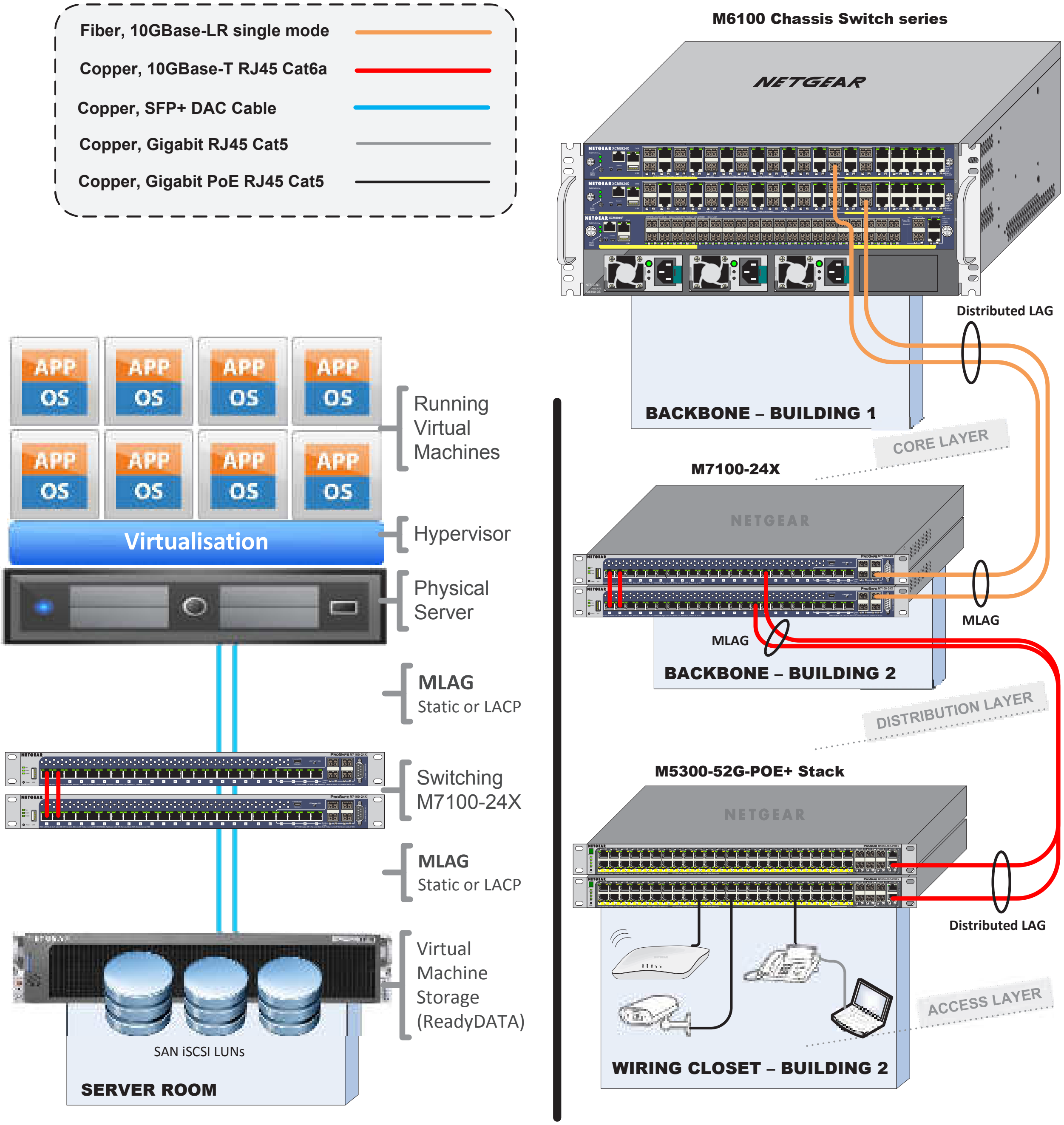
## Modern access layer features highlights

| | |
|---|---|
| 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<br>• 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 secure | |
| 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 | |
| 8 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 ACLs for best granularity | |
| Automatic Voice over IP prioritization with Auto-VoIP | |
| 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<br>• 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<br>• The purpose is to detect and avoid unidirectional link forwarding anomalies in a Layer 2 communication channel in which a bi-directional link stops passing traffic in one direction |
| Both "normal-mode" and "aggressive-mode" are supported for perfect compatibility with other vendors implementations, including port "D-Disable" triggering cases in both modes | |

## Target Application

### Why 10 Gigabit Ethernet for edge distribution of mid-sized networks?

- The IEEE standard for 10 Gigabit Ethernet (10GbE), IEEE Standard 802 3ae - 2002, was ratified ten years ago. Almost immediately, large enterprises started confidently deploying 10GbE in their corporate backbones, data centers, and server farms to support high-bandwidth, mission- critical applications.
- Over the years, improvements in 10GbE technology, price, and performance have extended its reach beyond enterprise data centers to mid-sized networks. Increasing bandwidth requirements and the growth of enterprise applications are also driving broader deployments of 10 Gigabit Ethernet.



## Target Application

# Three reasons to get started today with NETGEAR M7100 series

### 10 Gigabit Ethernet and the server edge: better efficiency

Mid-sized organizations are optimizing their data centers and server rooms by consolidating servers to free up space, power, and management overhead. The first step usually involves consolidating applications onto fewer servers than the old single-application-per-server paradigm. Often, the next step is server virtualization.

Server virtualization supports several applications and operating systems on a single sever by defining multiple virtual machines (VMs) on the server. Each virtual machine operates like a stand-alone, physical machine, yet shares the physical server processing power, ensuring no processing power is wasted. IT departments can reduce server inventory, better utilize servers, and manage resources more efficiently.

Server virtualization relies heavily on networking and storage. Virtual machines grow and require larger amounts of storage than one physical server can provide. Network attached storage (NAS) or storage area networks (SANs) provide additional, dedicated storage for virtual machines. Connectivity between servers and storage must be fast to avoid bottlenecks. 10GbE provides the fastest interconnectivity for virtualized environments.

### 10 Gigabit Ethernet SAN versus Fibre Channel: simpler and more cost-effective

There are three types of storage in a network: Direct-attached storage (DAS), NAS, and SAN. Each has its advantages, but SAN is emerging as the most flexible and scalable solution for data centers and high-density computing applications. The main drawback to SAN has been the expense and specially trained staff necessary for installing and maintaining the Fibre Channel (FC) interconnect fabric. Nonetheless, SANs with Fibre Channel have become well established in large enterprises.

A new standard, the Internet Small Computer System Interface (iSCSI), is making 10 Gigabit Ethernet an attractive, alternative interconnect fabric for SAN applications. iSCSI is an extension of the SCSI protocol used for block transfers in most storage devices and Fibre Channel. The Internet extension defines protocols for extending block transfers over IP, allowing standard Ethernet infrastructure to be used as a SAN fabric. Basic iSCSI is supported in most operating systems today. The latest iSCSI capabilities allow 10 Gigabit Ethernet to compare very favorably to Fibre Channel as a SAN interconnect fabric:

- Reduced equipment and management costs: 10GbE networking components are less expensive than highly specialized Fibre Channel components and do not require a specialized skill set for installation and management
- Enhanced server management: iSCSI remote boot eliminates booting each server from its own direct-attached disk. Instead, servers can boot from an operating system image on the SAN. This is particularly advantageous for using diskless servers in rack-mount or blade server applications
- Improved disaster recovery: all information on a local SAN — including boot information, operating system images, applications, and data — can be duplicated on a remote SAN for quick and complete disaster recovery
- Excellent performance: even transactional virtual machines, such as databases, can run over 10 Gigabit Ethernet and iSCSI SAN, without compromising performance

### 10 Gigabit Ethernet and the aggregation layer: reduce bottlenecks

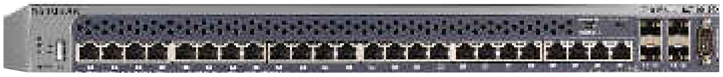
Until recently, network design best practices recommended equipping the edge with Fast Ethernet (100Base-T), and using Gigabit uplinks to either the core (for two-tiered network architectures) or aggregation layer (for three-tiered networks). Today, traffic at the edge of the network has increased dramatically. Bandwidth-intensive applications have multiplied, and Gigabit Ethernet to the desktop has become more popular as its price has decreased. Broader adoption of Gigabit Ethernet to the desktop has increased the oversubscription ratios of the rest of the network. The result: a bottleneck between large amounts of Gigabit traffic at the edge of the network, and the aggregation layer or core.

10 Gigabit Ethernet allows the aggregation layer to scale to meet the increasing demands of users and applications. It can help bring oversubscription ratios back in line with network-design best practices, and provides some important advantages over aggregating multiple Gigabit Ethernet links:

- Less fiber usage: a 10 Gigabit Ethernet link uses fewer strands compared with Gigabit Ethernet aggregation, which uses one strand per Gigabit Ethernet link. Using 10 Gigabit Ethernet reduces cabling complexity and uses existing cabling efficiently
- Greater support for large streams: traffic over aggregated 1Gigabit Ethernet links can be limited to 1 Gbps streams because of packet sequencing requirements on end devices. 10 Gigabit Ethernet can more effectively support applications that generate multi Gigabit streams due to the greater capacity in a single 10 Gigabit Ethernet link
- Longer deployment lifetimes: 10 Gigabit Ethernet provides greater scalability than multiple Gigabit Ethernet links, resulting in a more future- proof network. Up to eight 10 Gigabit Ethernet links can be aggregated into a virtual 80-Gbps connection

### Conclusion

For network connectivity, 10GBase-T, like other base-t technologies, uses the standard RJ45 Ethernet jack. This connection form factor is not only common on switches, but is also normally integrated onto servers, workstations and other PCs. Base-T usually runs up to a 100 meters, on the widely deployed, twisted pair copper cabling, such as Cat 6A type, and now more recently Cat 7 type. It is also backward compatible, auto-negotiating between higher and lower speeds – thereby not forcing an all at once network equipment upgrade. The NETGEAR M7100 series is the world-first realistic, cost-effective 10GBase-T departmental solution!



LIFETIME WARRANTY Hardware Warranty

LIFETIME WARRANTY Next Business Day

LIFETIME Tech Support

## Accessories and Modules

### Modular PSUs for M7100 series

**APS300W**
**Modular Power Supply**

**Ordering information**

- Worldwide: APS300W-10000S
- Warranty: 5 years

- PSU unit for M7100 series switches
  - M7100-24X
- Provides redundant power and hot swap replacement capability

**AFT200**
**Modular Fan Tray**

**Ordering information**

- Worldwide: AFT200-10000S
- Warranty: 5 years

- Replaceable fan tray for M7100 series switches
  - M7100-24X
- Two fan trays (two fans each) are required for M7100 series

### GBIC SFP Optics for M7100 series

| **ORDERING INFORMATION**<br>**WORLDWIDE:** SEE TABLE BELOW<br>**WARRANTY: 5 YEARS** | Multimode Fiber (MMF) | | Single mode Fiber (SMF) |
|---|---|---|---|
| | OM1 or OM2<br>62.5/125µm | OM3 or OM4<br>50/125µm | 9/125µm |
| **10 Gigabit SFP+**<br> <br>• Fits into M7100 series shared SFP+ interfaces | **AXM763**<br>10GBase-LRM long reach multimode<br>802.3aq - LC duplex connector<br>up to 220m (722 ft)<br>**AXM763-10000S (1 unit)** | **AXM763**<br>10GBase-LRM long reach multimode<br>802.3aq - LC duplex connector<br>up to 260m (853 ft)<br>**AXM763-10000S (1 unit)**<br>**AXM761**<br>10GBase-SR short reach multimode<br>LC duplex connector<br>OM3: up to 300m (984 ft)<br>OM4: up to 550m (1,804 ft)<br>**AXM761-10000S (1 unit)**<br>**AXM761P10-10000S**<br>**(pack of 10 units)** | **AXM762**<br>10GBase-LR long reach single mode<br>LC duplex connector<br>up to 10km (6.2 miles)<br>**AXM762-10000S (1 unit)**<br>**AXM762P10-10000S**<br>**(pack of 10 units)**<br>**AXM764**<br>10GBase-LR LITE single mode<br>LC duplex connector<br>up to 2km (1.2 mile)<br>**AXM764-10000S (1 unit)** |
| **Gigabit SFP**<br> <br>• Fits into M7100 series shared SFP+ interfaces | **AGM731F**<br>1000Base-SX short range multimode<br>LC duplex connector<br>up to 275m (902 ft)<br>**AGM731F (1 unit)** | **AGM731F**<br>1000Base-SX<br>short range multimode<br>LC duplex connector<br>OM3: up to 550m (1,804 ft)<br>OM4: up to 1,000m (3,280 ft)<br>**AGM731F (1 unit)** | **AGM732F**<br>1000Base-LX long range single mode<br>LC duplex connector<br>up to 10km (6.2 miles))<br>**AGM732F (1 unit)** |

## Accessories

### Direct Attach Cables for M7100 series

| ORDERING INFORMATION<br>**WORLDWIDE:** SEE TABLE BELOW<br>**WARRANTY: 5 YEARS** | SFP+ to SFP+ | |
|---|---|---|
| | 1 meter (3.3 ft) | 3 meters (9.8 ft) |
| **10 Gigabit DAC**<br> <br>• Fits into M7100 series shared SFP+ interfaces | **AXC761**<br>10GSFP+ Cu (passive)<br>SFP+ connectors on both end<br>**AXC761-10000S (1 unit)** | **AXC763**<br>10GSFP+ Cu (passive)<br>SFP+ connectors on both end<br>**AXC763-10000S (1 unit)** |

## Technical Specifications

- Requirements based on 11.x unified software release

| Model Name | Description | Model number |
|---|---|---|
| M7100-24X | 24 ports 10GBase-T, Layer 2+ software package | XSM7224 v1h1 |

| PHYSICAL INTERFACES | | | | | |
|---|---|---|---|---|---|
| Front | Auto-sensing RJ45<br>100/1000/10GBase-T | | Auto-sensing SFP+ ports<br>1000/10GBase-X | Storage port | Console ports |
| M7100-24X | 24 | | 4 | 1 x USB | Serial RS232 DB9,<br>Mini-USB (selectable) |
| Rear | Modular PSUs | Modular Fan Trays | M7100 series comes with one PSU, and two fan trays already installed | | |
| M7100-24X | 2 | 2 | | | |
| Total Port Count | 10 Gigabit | | | | |
| M7100-24X | 24 | | | | |

| PROCESSOR/MEMORY | | |
|---|---|---|
| Processor (CPU) | Freescale P1011 800Mhz (45nm technology) | |
| System memory (RAM) | 256 MB | |
| Code storage (flash) | 128 MB | Dual firmware image, dual configuration file |
| Packet Buffer Memory | | |
| M7100-24X | 16 Mb | Dynamically shared across only used ports |
| **PERFORMANCE SUMMARY** | | |
| Switching fabric | | |
| M7100-24X | 480 Gbps | Line-rate (non blocking fabric) |
| Throughput | | |
| M7100-24X | 357.1 Mpps | |
| Green Ethernet | | |
| Energy Efficient Ethernet (EEE) | IEEE 802.3az Energy Efficient Ethernet Task Force compliance | Deactivated by default |
| Auto-EEE Mode | Yes | Deactivated by default |
| Power Back Off | Drops power consumption by 15% to 20% when short copper cables are detected | 10GBase-T standard |
| Other Metrics | | |
| Forwarding mode | Store-and-forward | |
| Latency (64-byte frames, 100 Mbps, Copper) | <8.5 μs | |

| | | | |
|---|---|---|---|
| Latency (64-byte frames, 1 Gbps, Copper) | <2.8 µs | | |
| Latency (64-byte frames, 1 Gbps, Fiber SFP) | <2.5 µs | | |
| Latency (64-byte frames, 10 Gbps, Copper 10GBase-T) | <3.7 µs | | |
| Latency (64-byte frames, 10 Gbps, Fiber SFP+) | <1.8 µs | | |
| Addressing | 48-bit MAC address | | |
| Address database size | 32,000 MAC addresses | | |
| Number of VLANs | 1,024 VLANs (802.1Q) simultaneously | | |
| Number of multicast groups filtered (IGMP) | 2K | | |
| Number of Link Aggregation Groups (LAGs - 802.3ad) | 12 LAGs with up to 8 ports per group | | |
| Number of hardware queues for QoS | 8 queues | | |
| Number of routes<br>IPv4 | <br>128 | | |
| 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) | | |
| M7100-24X | <60 dB | | Fan speed control |
| Heat Dissipation (BTU) | | | |
| M7100-24X | 587 Btu/hr | | |
| Mean Time Between Failures (MTBF) | @ 25 °C ambient (77 °F) | @ 55 °C ambient (131 °F) | |
| M7100-24X | 172,955 hours (~19.7 years) | 35,725 hours (~4.1 years) | |
| **L2 SERVICES - VLANS** | | | |
| IEEE 802.1Q VLAN Tagging | Yes | | Up to 1,024 VLANs - 802.1Q Tagging |
| Protocol Based VLANs<br>IP subnet<br>ARP<br>IPX | Yes<br>Yes<br>Yes<br>Yes | | |
| Static VLANs | Access Ports for 802.1Q unaware endpoints and Trunk Ports for switch-to-switch links with Native VLAN | | |
| Subnet based VLANs | Yes | | |
| MAC based VLANs | Yes | | |
| Voice VLAN | Yes | | |
| Private Edge VLAN | Yes | | |
| Private VLAN | Yes | | |

| | | |
|---|---|---|
| IEEE 802.1x<br>Guest VLAN<br>RADIUS based VLAN assignment via .1x<br>RADIUS based Filter ID assignment via .1x<br>MAC-based .1x<br>Unauthenticated VLAN | Yes<br>Yes<br>Yes<br>Yes<br>Yes<br>Yes | IP phones and PCs can authenticate on the same port but under different VLAN assignment policies |
| Double VLAN Tagging (QinQ)<br>Enabling dvlan-tunnel makes interface<br>Global ethertype (TPID)<br>Interface ethertype (TPID)<br>Customer ID using PVID | Yes<br>Yes<br>Yes<br>Yes<br>Yes | |
| GARP with GVRP/GMRP | Yes | Automatic registration for membership in VLANs or in multicast groups |
| MVR (Multicast VLAN registration) | Yes | |
| **L2 SERVICES - AVAILABILITY** | | |
| IEEE 802.3ad - LAGs<br>LACP<br>Static LAGs | Yes<br>Yes<br>Yes | Up to 24 LAGs and up to 8 physical ports per LAG |
| LAG Hashing | Yes | |
| Multi Chassis Link Aggregation (MLAG)l | Yes | |
| Storm Control | Yes | |
| IEEE 802.3x (Full Duplex and flow control)<br>Per port Flow Control | Yes<br>Yes | Asymmetric and Symmetric Flow Control |
| UDLD Support<br>(Unidirectional Link Detection)<br>Normal-Mode<br>Aggressive-Mode | Yes<br>Yes<br>Yes<br>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 | |
| **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<br>Enable IGMP Snooping per VLAN<br>Snooping Querier | Yes<br>Yes<br>Yes | |
| Multicast VLAN registration (MVR) | Yes | |
| **L3 SERVICES - DHCP** | | |
| DHCP IPv4/DHCP IPv6 Client | Yes | |
| DHCP IPv4 Server | Yes | |
| DHCP Snooping IPv4 | Yes | |
| DHCP Relay IPv4 | Yes | |
| DHCP BootP IPv4 | Yes | |
| Auto Install (DHCP options 66, 67, 150) | Yes | |
| **L3 SERVICES - IPV4 ROUTING** | | |
| Static Routing | Yes | |
| Port Based Routing | Yes | |
| VLAN Routing<br>802.3ad (LAG) for router ports | Yes<br>Yes | |
| IP Helper<br>Max IP Helper entries | Yes<br>512 | |
| IP Source Guard | Yes | |
| ECMP | Yes | |
| Proxy ARP | Yes | |
| Multinetting | Yes | |
| ICMP redirect detection in hardware | Yes | |
| DNSv4 | Yes | |
| ICMP throttling | 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<br>Denial of Service Protection (control plane)<br>Denial of Service Protection (data plane) | Yes<br>Yes<br>Yes | | | Switch CPU protection<br>Switch Traffic protection |
| DoS attacks | SIPDIP | UDPPORT | L4PORT | |
| | SMACDMAC | TCPFLAGSEQ | ICMPV4 | |
| | FIRSTFRAG | TCPOFFSET | ICMPV6 | |
| | TCPFRAG | TCPSYN | ICMPFRAG | |
| | TCPFLAG | TCPSYNFIN | I | |
| | TCPPORT | TCPFINURGPSH | | |
| ICMP throttling | Yes | | Restrict ICMP, PING traffic for ICMP-based DoS attacks | |
| Management | | | | |
| Management ACL (MACAL)<br>Max Rules | Yes<br>64 | | Protects management CPU access through the LAN | |
| Radius accounting | Yes | | RFC 2565 and RFC 2866 | |
| TACACS+ | Yes | | | |
| 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 | | | |
| 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 accross switches in same Layer 2 network |
| **QUALITY OF SERVICE (QOS) - SUMMARY** | | |
| Access Lists | | |
| L2 MAC, L3 IP and L4 Port ACLs | Yes | |
| Ingress | Yes | |
| Egress | Yes | |
| 802.3ad (LAG) for ACL assignment | Yes | |
| Binding ACLs to VLANs | Yes | |
| ACL Logging | Yes | |
| Support for IPv6 fields | Yes | |
| DiffServ QoS | Yes | |
| Edge Node applicability | Yes | |
| Interior Node applicability | Yes | |
| 802.3ad (LAG) for service interface | Yes | |
| Support for IPv6 fields | Yes | |
| Ingress/Egress | Yes | |
| IEEE 802.1p COS | Yes | |
| 802.3ad (LAG) for COS configuration | Yes | |
| WRED (Weighted Deficit Round Robin) | Yes | |
| Strict Priority queue technology | 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 | Yes | |
| Dot1p Marking | Yes | |
| IP DSCP Marking | Yes | |
| **QOS - ACL FEATURE SUPPORT** | | |
| ACL Support (include L3 IP and L4 TCP/UDP) | Yes | |
| MAC ACL Support | Yes | |
| IP Rule Match Fields | | |
| Dest IP | Inbound/Outbound | |
| Dest IPv6 IP | Inbound/Outbound | |
| Dest L4 Port | Inbound/Outbound | |
| Every Packet | Inbound/Outbound | |
| IP DSCP | Inbound/Outbound | |
| IP Precedence | Inbound/Outbound | |
| IP TOS | 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 | |
| Supports Masking | Inbound/Outbound | |

| | | |
|---|---|---|
| MAC Rule Match Fields | | |
| COS | Inbound/Outbound | |
| Dest MAC | Inbound/Outbound | |
| Dest MAC Mask | Inbound/Outbound | |
| Ethertype | Inbound/Outbound | |
| Source MAC | Inbound/Outbound | |
| Source MAC Mask | Inbound/Outbound | |
| VLAN ID | Inbound/Outbound | |
| VLAN ID2 (Secondary VLAN) | Yes | |
| Rules Attributes | | |
| Assign Queue | Inbound | |
| Logging – deny rules | Inbound/Outbound | |
| Mirror (to supported interface types only) | Inbound | |
| Redirect (to supported interface types only) | Inbound | |
| Interface | | |
| Inbound direction | Yes | |
| Outbound direction | Yes | |
| Supports LAG interfaces | 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 | Yes | |
| All | | |
| Class Match Criteria | | |
| COS | Inbound/Outbound | |
| COS2 (Secondary COS) | Inbound | |
| Dest IP (for Mask support see below) | Inbound/Outbound | |
| Dest IPv6 IP | Inbound/Outbound | |
| Dest L4 Port | Inbound/Outbound | |
| Dest 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 | Inbound | |
| Drop | Yes | |
| Mark COS | Yes | |
| Mark IP DSCP | Yes | |
| Mark IP Precedence | Yes | |
| Mirror (to supported interface types only) | Inbound | |
| Police Simple | Yes | |
| Police Color Aware Mode | Yes | |
| Policy Attributes – Outbound | Yes | |
| Drop | Yes | |
| Mark COS | Yes | |
| Mark IP DSCP | Yes | |
| Mark IP Precedence | Yes | |
| Police Simple | Yes | |
| Police Color Aware Mode | Yes | |
| Redirect (to supported interface types only) | Inbound | |
| 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 | Yes | |
| 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 | |

| IEEE NETWORK PROTOCOLS | | | |
|---|---|---|---|
| IEEE 802.3 Ethernet | IEEE 802.3ae<br>10-Gigabit Ethernet | IEEE 802.1D Spanning Tree (STP) | IEEE 802.1Q VLAN tagging |
| IEEE 802.3u 100BASE-T | IEEE 802.3az<br>Energy Efficient Ethernet | IEEE 802.1s Multiple Spanning Tree (MSTP) | IEEE 802.1v<br>Protocol-based VLAN |
| IEEE 802.3ab 1000BASE-T | IEEE 802.3ad<br>Trunking (LACP) | IEEE 802.1w Rapid Spanning Tree (RSTP) | IEEE 802.1p<br>Quality of Service |
| IEEE 802.3z Gigabit Ethernet 1000BASE-SX/LX | IEEE 802.1AB LLDP with ANSI/TIA-1057 (LLDP-MED) | IEEE 802.1X Radius network access control | IEEE 802.3x Flow control |

| IETF RFC STANDARDS AND MIBS | |
|---|---|
| System Facilities | |
| RFC 768 – UDP | RFC 2131 – DHCP Client/Server |
| RFC 783 – TFTP | RFC 2132 – DHCP options & BOOTP vendor extensions |
| RFC 791 – IP | RFC 2030 – Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI |
| RFC 792 – ICMP | RFC 2865 – RADIUS Client (both Switch and Management access) |
| RFC 793 – TCP | RFC 2866 – RADIUS Accounting |
| RFC 826 – Ethernet ARP | RFC 2868 – RADIUS Attributes for Tunnel Protocol support |
| RFC 894 – Transmission of IP datagrams over Ethernet networks | RFC 2869 – RADIUS Extensions |
| RFC 896 – Congestion control in IP/TCP Networks | RFC2869bis – RADIUS Support for Extensible Authentication Protocol (EAP) |
| RFC 951 – BOOTP | RFC 3164 – The BSD Syslog Protocol |
| RFC 1321 – Message-digest algorithm | RFC 3580 – 802.1X RADIUS usage guidelines (VLAN assignment via RADIUS, dynamic VLAN) |
| RFC 1534 – Interoperation between BOOTP and DHCP | |
| Switching MIB | |
| RFC 1213 – MIB-II | RFC 2620 – RADIUS Accounting MIB |
| RFC 1493 – Bridge MIB | RFC 2737 – Entity MIB version 2 |
| RFC 1643 – Ethernet-like MIB | RFC 2819 – RMON Groups 1,2,3 & 9 |
| RFC 2233 – The Interfaces Group MIB using SMI v2 | IEEE 802.1X MIB (IEEE 802.1-PAE-MIB 2004 Revision) |
| RFC 2674 – VLAN MIB | IEEE 802.1AB – LLDP MIB |
| RFC 2613 – SMON MIB | ANSI/TIA 1057 – LLDP-MED MIB |
| RFC 2618 – RADIUS Authentication Client MIB | Private Enterprise MIBs supporting switching features |
| IPv4 Routing | |
| RFC 1027 – Using ARP to implement transparent subnet Gateways (Proxy ARP) | RFC 2131 – DHCP relay |
| RFC 1256 – ICMP Router Discovery Messages<br>Layer 3 software package required | RFC 3046 – DHCP Relay Agent Information option |
| RFC 1812 – Requirements for IP Version 4 routers | VLAN routing |

| | |
|---|---|
| IPv4 Routing MIB | |
| RFC 2096 – IP Forwarding Table MIB | Private enterprise MIB supporting routing features |
| Multicast | |
| RFC 1112 – Host extensions for IP Multicasting | RFC 2710 – Multicast Listener Discovery (MLD) for IPv6 |
| RFC 2236 – Internet Group Management Protocol, Version 2 | RFC 3376 – Internet Group Management Protocol, Version 3 |
| RFC 2365 – Administratively Scoped IP Multicast | RFC 3810 – Multicast Listener Discovery Version 2 (MLDv2) for IPv6 |
| Multicast MIB | |
| Draft-ietf-magma-mgmd-mib-05 Multicast Group Membership Discovery MIB | Private Enterprise MIB supporting Multicast features |
| IPv6 Routing | |
| RFC 1981 – Path MTU for IPv6 | RFC 3484 – Default Address Selection for IPv6 |
| RFC 2460 – IPv6 Protocol specification | RFC 3493 – Basic Socket Interface for IPv6 |
| RFC 2461 – Neighbor Discovery | RFC 3542 – Advanced Sockets API for IPv6 |
| RFC 2462 – Stateless Auto Configuration | RFC 3587 – IPv6 Global Unicast Address Format |
| RFC 2464 – IPv6 over Ethernet | RFC 3736 – Stateless DHCPv6 |
| IPv6 Routing MB | |
| RFC 2465 – IPv6 MIB | RFC 2466 – ICMPv6 MIB |
| QoS | |
| RFC 2474 – Definition of Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers | RFC 3260 – New Terminology and Clarifications for DiffServ |
| RFC 2475 – An Architecture for Differentiated Services | RFC 3289 – Management Information Base for the Differentiated Services Architecture (read-only) |
| RFC 2597 – Assured Forwarding PHB Group | Private MIBs for full configuration of DiffServ, ACL and CoS functionality |
| RFC 3246 – An Expedited Forwarding PHB (Per-Hop Behavior) | |
| Management | |
| RFC 854 – Telnet | RFC 3412 – Message Processing & Dispatching |
| RFC 855 – Telnet Option | RFC 3413 – SNMP Applications |
| RFC 1155 – SMI v1 | RFC 3414 – User-Based Security Model |
| RFC 1157 – SNMP | RFC 3415 – View-based Access Control Model |
| RFC 1212 – Concise MIB Definitions | RFC 3416 – Version 2 of SNMP Protocol Operations |
| RFC 1867 – HTML/2.0 Forms with file upload extensions | RFC 3417 – Transport Mappings |
| RFC 1901 – Community-based SNMP v2 | RFC 3418 – Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) |

| | | |
|---|---|---|
| RFC 1908 – Coexistence between SNMP v1 & SNMP v2 | SSL 3.0 and TLS 1.0<br>- RFC 2246 – The TLS Protocol, Version 1.0<br>- RFC 2818 – HTTP over TLS<br>- RFC 2346 – AES Ciphersuites for Transport Layer Security | |
| 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 | | |
| RFC 2296 – Remote Variant Selection; RSVA/ 1.0 State Management "cookies" – draft-ietf-http-state-mgmt-05 | SSH 1.5 and 2.0<br>- RFC 4253 – SSH Transport Layer Protocol<br>- RFC 4252 – SSH Authentication Protocol<br>- RFC 4254 – SSH Connection Protocol<br>- RFC 4251 – SSH Protocol Architecture<br>- RFC 4716 – SECSH Public Key File Format<br>- RFC 4419 – Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol | |
| 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 | | |
| MANAGEMENT | | |
| Password management | Yes | |
| Configurable Management VLAN | Yes | |
| 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 |
| 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 | Industry standard CLI commands scripts for automation |
| 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<br>Max History entries<br>Max buckets per History entry<br>Max Alarm entries<br>Max Event entries<br>Max Log entries per Event entry | Yes<br>3 * (number of ports in the stack + LAG + 10)<br>10<br>3 * (number of ports in the stack + LAG + 10)<br>3 * (number of ports in the stack + LAG + 10)<br>10 | |
| Port Mirroring<br>Number of monitor sessions<br>Tx/Rx<br>Many to One Port Mirroring<br>LAG supported as source ports<br>Max source ports in a session | Yes<br>1<br>Yes<br>Yes<br>Yes<br>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 |
| Traceroute feature | Yes | |
| Outbound Telnet | Yes | |
| SSH<br>SSH Session Configuration | v1/v2<br>Yes | Secure Shell |
| 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 | |
| Syslog (RFC 3164) | Yes | |
| Persistent log supported | Yes | |
| **USER ADMIN MANAGEMENT** | | |
| User ID configuration<br>Max number of configured users<br>Support multiple READWRITE Users<br>Max number of IAS users (internal user database) | Yes<br>6<br>Yes<br>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 | |
| **M7100 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 | 1K | |
| VLAN ID Range | 1 - 4093 | |
| Number of 802.1p Traffic Classes | 8 classes | |
| IEEE 802.1x<br>Number of .1x clients per port | <br>48 | |
| Number of LAGs | 12 LAGs with up to 8 ports per group | |
| Maximum multiple spanning tree instances | 32 | |
| MAC based VLANS<br>Number supported | Yes<br>256 | |
| Number of log messages buffered | 200 | |
| Static filter entries<br>Unicast MAC and source port<br>Multicast MAC and source port<br>Multicast MAC and destination port (only) | <br>20<br>20<br>256 | |
| Subnet based VLANs<br>Number supported | Yes<br>128 | |
| Protocol Based VLANs<br>Max number of groups<br>Max protocols | Yes<br>128<br>16 | |
| Maximum Multicast MAC Addresses entries | 2K | |
| Jumbo Frame Support<br>Max Size Supported | Yes<br>12k | |
| Number of DHCP snooping bindings | 32K | |
| Number of DHCP snooping static entries | 1024 | |
| LLDP-MED number of remote nodes | 48 | |
| Port MAC Locking<br>Dynamic addresses per port<br>Static addresses per port | Yes<br>4096<br>48 | |
| sFlow<br>Number of samplers<br>Number of pollers<br>Number of receivers | <br>32<br>52<br>8 | |
| Radius<br>Max Authentication servers<br>Max Accounting servers | <br>5<br>1 | |
| Number of routing interfaces (including port/vlan) | 128 | |

| | | |
|---|---|---|
| Number of static routes (v4) | 128 | |
| Routing Heap size | | |
| IPv4 | 26M | |
| DHCP Server | | |
| Max number of pools | 16 | |
| Total max leases | 1024 | |
| DNS Client | | |
| Concurrent requests | 16 | |
| Name server entries | 8 | |
| Seach list entries | 6 | |
| Static host entries | 64 | |
| Cache entries | 128 | |
| Domain search list entries | 32 | |
| Number of Host Entries (ARP/NDP) | | |
| IPv4 build | 6K | |
| Static v4 ARP Entries | 128 | |
| Number of ECMP Next Hops per Route | 4 | |
| ACL Limits | | |
| Maximum Number of ACLs (any type) | 100 | |
| Maximum Number Configurable Rules per List | 1023 ingress/512 egress | |
| Maximum ACL Rules per Interface and Direction (IPv4/L2) | 1023 ingress/511 egress | |
| Maximum ACL Rules per Interface and Direction (IPv6) | 509 ingress/255 egress | |
| Maximum ACL Rules (system-wide) | 16384 | |
| Maximum ACL Logging Rules (system-wide) | 128 | |
| COS Device Characteristics | | |
| Configurable Queues per Port | 8 queues | |
| Configurable Drop Precedence Levels | 3 | |
| DiffServ Device Limits | | |
| Number of Queues | 8 queues | |
| 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 | 58 interfaces | |
| Max Table Entries | | |
| Class Table | 32 | |
| Class Rule Table | 192 | |
| Policy Table | 64 | |
| Policy Instance Table | 640 | |
| Policy Attribute Table | 1920 | |
| Max Nested Class Chain Rule Count | 26 | |
| AutoVoIP number of voice calls | 16 | |
| iSCSI Flow Acceleration | | |
| Max Monitored TCP Ports/IP Addresses | 16 | |
| Max Sessions | 192 | |
| Max Connections | 192 | |

| | | |
|---|---|---|
| LED | | |
| Per port | Speed, Link, Activity | |
| Per device | Power supply 1, Power supply 2, Fan trays status | |
| PHYSICAL SPECIFICATIONS | | |
| Dimensions | 440 x 430 x 44 mm (17.32 x 16.93 x 1.73 in) | |
| Weight<br>M7100-24X | 6.984 kg (15.40 lb) | |
| POWER CONSUMPTION | | |
| Worst case, all ports used, line-rate traffic<br>M7100-24X | 200W (90VAC@47Hz) max | |
| ENVIRONMENTAL SPECIFICATIONS | | |
| Operating:<br>Temperature<br>Humidity<br>Altitude | 32° to 122°F (0° to 50°C)<br>90% maximum relative humidity, non-condensing<br>10,000 ft (3,000 m) maximum | |
| Storage:<br>Temperature<br>Humidity<br>Altitude | – 4° to 158°F (–20° to 70°C)<br>95% maximum relative humidity, non-condensing<br>10,000 ft (3,000 m) maximum | |
| ELECTROMAGNETIC EMISSIONS AND IMMUNITY | | |
| Certifications | CE mark, commercial<br>FCC Part 15 Class A, VCCI Class A<br>Class A EN 55022 (CISPR 22) Class A<br>Class A C-Tick<br>EN 50082-1<br>EN 55024 | |
| SAFETY | | |
| Certifications | CE mark, commercial<br>CSA certified (CSA 22.2 #950)<br>UL listed (UL 1950)/cUL IEC 950/EN 60950 | |
| PACKAGE CONTENT | | |
| All models | ProSAFE® M7100 series switch equipped with 1 x PSU and 2 x Fan trays<br>Power cord<br>Rubber footpads for tabletop installation<br>Rubber caps for the SFP+ sockets<br>Rack-mounting kit<br>Mini-USB to USB cable for console<br>Resource CD with links to online documentation, installation guides, USB drivers, software manual, CLI admin guide, Web GUI guide | |
| OPTIONAL MODULES AND ACCESSORIES | | |
| **All models:** | | **Ordering SKU:** |
| AGM731F | 1000Base-SX SFP GBIC (Multimode) | AGM731F |
| AGM732F | 1000Base-LX SFP GBIC (Single mode) | AGM732F |

| | | |
|---|---|---|
| AXC761 | 10GSFP+ Cu (passive) SFP+ to SFP+ Direct Attach Cable 1m | AXC761-10000S |
| AXC763 | 10GSFP+ Cu (passive) SFP+ to SFP+ Direct Attach Cable 3m | AXC763 -10000S |
| AXM761 | 10GBase-SR SFP+ GBIC (OM3 Multimode) | AXM761-10000S |
| AXM761 (Pack of 10 units) | 10GBase-SR SFP+ GBIC (OM3 Multimode) | AXM761P10-10000S |
| AXM762 | 10GBase-LR SFP+ GBIC (Single mode) | AXM762-10000S |
| AXM762 (Pack of 10 units) | 10GBase-LR SFP+ GBIC (Single mode) | AXM762P10-10000S |
| AXM763 | 10GBase-LRM SFP+ GBIC (Long Reach Multimode, OM1, OM2 or OM3) | AXM763-10000S |
| AXM764 | 10GBase-LR LITE SFP+ GBIC (Single mode) | AXM764-10000S |
| **M7100-24X** | | |
| APS300W | Modular Power Supply | APS300W-10000S |
| AFT200 | Modular Fan Tray | AFT200-10000S |
| 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 | | |
| PMB0334-10000S<br>OnCall 24x7 3-year CAT 4 | M7100-24X<br>OnCall 24x7 extends the 90-day warranty entitled technical support (phone and email) for standard and advanced features to the length of the contract term | |
| ORDERING INFORMATION | | |
| M7100-24X<br>Americas, Europe<br>Asia Pacific<br>China | XSM7224-100NES<br>XSM7224-100AJS<br>XSM7224-100PRS | V1H1<br>V1H1<br>V1H1 |

* 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.