DM4100 – Series

DM4100 Metro Ethernet Series

The DM4100 product line is composed by of high-capacity switches at wire-speed to provide DATACOM customer applications with increasingly greater speeds, always with high performance and reliability.

The DM4100 Switches provide layer 2 packet switching. Spanning Tree – Classic, Rapid and Multiple – as well as ERPS and EAPS protocols are available as L2 protection mechanisms. It is also possible to aggregate physical ports, thus forming logical ports static and dynamically (LACP), allowing increase of bandwidth and automatic protection in the event of a failure.

The DM4100 Switches also feature the option of working as a layer 3 Switch Router or a Label Switch Router MPLS[(1)(4)]. It supports dynamic protocols for the establishment of LSPs with the fast convergence mechanism. They also feature VPNs structured on level 2, built on a MPLS infrastructure.

The stacking capability with speeds starting at 40Gbit/s allows the stacking of up to eight pieces of equipment for easy expansion of the applications within the same physical environment, also providing a lower-cost alternative to buying a chassis.

To ease your project, optical ports supporting SFP, SFP+ or XFP transceivers are available, depending on the transmission rate, reach and switch model. Transceivers are available as accessories and in many models.

The DM4100 product line is managed by the DmView application, CLI or HTTP as well as other commercial platforms that use open standards such as SNMP and XML. DmView is the network management platform used to manage of the entire range of DATACOM products, providing an integrated network view and unifying the operations.

The DM4100 features a Command Line Interface (CLI) via SSHv2, Telnet and RS-232. It also has an out-of-band Ethernet port and a USB(1) port. It is possible to have multiple firmware versions and set-up files for an easier upgrade and change control.

This product is homologated by ANATEL in accordance with the procedures regulated by Resolution No. 242/2000 and meets the technical requirements applied, including exposure limits of Specific Absorption Rate related to electric fields, magnetic and electromagnetic radio frequency, according to Resolution No. 303/2002.

For further information, access the website www.anatel.gov.br.

Main Characteristics

Wire Speed L2, L3 & MPLS

The DM4100 line has a commutation matrix of up to 224Gbit/s in the 48 ports model and 152Gbit/s in the 24 ports model. The entire L2, L3 (IPv4/v6) and MPLS packet switching is always performed in hardware and in wire speed, in order to ensure low switch latency. The filter/meter/ACL functions are performed by the ASIC, without impact at the CPU performance or packet forwarding.

Layer 2 and Layer 3 protocols are implemented in software in order to assemble the MAC, IP route and MPLS label push/pop/swap tables.

The DM4100 models provide high capacity of RAM memory in order to allow a high capacity for table storage in software (RIB, MRIB, LRIB, L2RIB, etc.), ensuring more than twice of capacity than the hardware supplies (FIB, MFIB, LFIB, L2FIB, etc.). Besides that, it also provides a high processing performance (CPU), enabling it to support elevated protocol sessions values, route processing and rapid convergence of traffic in hardware.

IP/MPLS Networks[1][4]

The DM4100 line supports IP routing (IPv4/v6) and both static and dynamic routing - RIP, RIPng, OSPF(v3) and BGPv4.

DM4000 may be used in MPLS network as LER (Label Edge Router) or LSR (Label Switch Router).

For the MPLS infrastructure, it is possible the establishment of LSPs or MPLS tunnels through LDP or RSVP-TE protocols, with FRR support, as well as LDP over RSVP-TE tunneling feature support.

LSPs may be assembled over interfaces 1Gbit/s (electrical or optical), 10Gbit/s (XFP) and interfaces 802.3ad (LAG).

Using LDP infrastructure, it is possible to use the VPN services in configuration such as: point-to-point (VPWS), point-multipoint (VPLS) and in hierarchical mode (H-VPLS), named L2VPNoLDP.

Using RSVP infrastructure, it is possible to implement the service L2VPN-TE, which use a RSVP tunnel as destination (L2VPNoRSVP). If the infrastructure contains the LSP and RSVP protocols, this service is named L2VPNoLDPoRSVP.

Stacking[3]

It is possible to stack up to eight pieces of equipment so that, from the management point of view, the units behave as a single switch with more ports. The features will become available among different units in a transparent manner, such as VLANs, logic ports, QoS and ports monitoring.

In order to ensure a high availability for the solution, the stacking may be implemented by forming a ring among the elements, providing protection in a failure situation. In this situation, any unit can operate as the master (1:N protection).

Power over Ethernet

The DM4100 PoE models allow passing electric power through its Ethernet Interfaces, according to IEE 802.3at e IEEE802.3af standards, transmitting data and energy along Cat.5e ou Cat.6 cables. Without external power source, the switches can provide up to 15,4W (IEEE802.3af) on all ports or up to 34,2W (IEEE802.3at) on half of the ports.

Management Facilities

A complete centralized FCAPS management is available through the DATACOM's management software DmView, with sending traps to alarms and events in the system, on a Linux, Windows or Solaris platforms, and with full redundancy. The device has a CLI – Command Line Interface – with automatic assistance in the syntax of commands and parameters, and is accessible through SSHv2, Telnet, and RS-232 Console. A SNMPv1, v2c and v3 over IPv4 and IPv6 using authentication and/or cryptography, and 4 RMON groups are also available.

The DM4100 allows the creation of complex Access Control Lists (ACLs) in hardware, with multiple comparison and action parameters, which enable the modification, routing, discard and/or prioritization of packets. Access and management inband and outband are possible through HTTP and/or HTTPs, via command line interface and console port RJ45.

Besides the protection for the equipment configuration access with passwords, it is also possible the usage of RADIUS or TACACS+ external servers to limit the commands executed by the operator.

A monitoring feature in hardware is also available. It can monitor all the switch ports or packet flow, without DM4100 performance impact, redirecting the port or packet flow traffic to a specified port.

In order to facilitate the firmware version and working configuration, is possible to store simultaneously up to two different firmware versions and ten different configurations in the equipment, allowing to choose which one will be used at equipment startup. All of ten saved configurations can be applied at any time, overwriting the current one instantaneously speeding up the operation.

Supports resolution of IPv4 and IPv6 (DNS IPv4/v6) for equipment names (hostnames), easing management actions via Telnet and SSH, for example.

QoS Implementation Facilities

The DM4100 has eight queues per port, implementing QoS in hardware, without impact in the system performance.

The QoS policies are implemented through many techniques, such as: priority algorithms, which define that a certain data flow will always have a higher priority, assign priority levels to each queue, determine minimum forwarding rates or a combination of these methods.

The traffic classification can be performed via VLANs, input ports, IEEE 802.1p standard, IP Precedence or DSCP fields, TCP and UDP ports, among other.

QoS policies can be applied to physical or logic interfaces.

The filter/meter/ACL functions are performed by the ASIC, without impact in the CPU performance or in the packets forwarding.

The bandwidth control has an 8kbit/s granularity at the CIR (Committed Information Rate) and PIR (Peak Information Rate) and may be applied to the incoming or outgoing traffic of ports or to a certain packet flow by means of filters.

The filters are quite flexible features, allowing multiple matches and actions on the packets. Some of the filter options supported are listed below:

- Match: 802.1p, all, destination-ip, destination-mac, destination-port, dscp, ethertype, protocol, source-ip, source-mac, source-port, tos-bits, tos-precedence, vlan, etc.
- Action: Permit, deny, 802.1p, 802.1p-from-tos, counter, drop-precedence, dscp, egress-block, int-802.1p, pkt-802.1p, pkt-802.1p-from-tos, redirect-port, etc.

Security

The DM4100 line has mechanisms to ensure operation and maintenance security on the installed network. Besides the usage of encryption in the communication protocols, it is possible to specify by means of filters which workstations in the network may access the equipment on an administrative level.

Using local (at least 4000 lines) and remote Syslog, user authentication, authorization and accounting (AAA) via RADIUS and TACACS+, alarm notice by e-mail, single clock via SNTP and protection against Denial of Service attacks (DoS/DDoS). In additional DM4100 implements the port authentication of multiple users via 802.1x, having 1024 users per device and 256 users per port.

For Metro Ethernet applications there are also: limitation of MAC numbers per port and per VLAN, protection mechanisms on L2 and L3 protocols against network attack, bandwidth limitation for broadcast and multicast traffic and Destination Lookup Failure (DLF).

VLANs

Virtual LANs may be built on DM4100 Switches using all of the 4094 VLANs(9) defined in IEEE 802.1q standard simultaneously, offering double tagging (Q-in-Q) functionality as well as define VLAN per protocol, MAC address and IP subnet.

The DM4100 Switch family also provide the feature Private VLAN. The Private VLAN feature enables to define sub-domains where the sub-domain members are able to communicate or not between each other, according the sub-domain type: Isolated or Community. In addition it is possible to define Promiscuous members that can communicate with all members of the Private VLAN.

Access Control Lists (ACLs)

The DM4100 allows the Access Control Lists (ACLs) / Filters creation in hardware, with multiples comparison parameters and action, which enable the modification, forwarding, discard or prioritization of packages in logical and physical interfaces. The product has ingress and egress filters which perform layer 2, 3 and 4 matches, such as: source IPv4/v6, destination IPv4/v6, TCP/UDP source port, TCP/UDP destination port, protocol, source and destination MAC address, DSCP mark, etc. The filters are capable to associate executed actions in hardware. For example: discard of packages, remark of priority 802.1q, bandwidth limitation, etc.

Filters can be associated to the counter resource in order to obtain packets statistics and/or send/received bytes. This information can be viewed through CLI interface, as well as being exported through the management interface SNMP. The many match options make possible a great variety of monitoring modes of data flow, VLAN/VPN traffic, etc.

Protection Mechanisms

In layer 2 are available the Spanning Tree protocols, including Rapid Spanning Tree (RSTP), which has shorter conversion times, Multiple Spanning Tree (MSTP) for better resource allocation and greater scalability, as well as the protocols of Ethernet Automatic Protection Switching (EAPS), Ethernet Ring Protection Switcing (ERPS), and ITU-T G.8032 (including Amendment A) protocols, which are specific for sub-50ms protection in Ethernet rings. Using the Link Aggregation (LAG) feature, it is possible to group physical ports to form logical ports, with automatic load balancing and time recovery under 200ms. This way, it is possible to build topologies featuring protection and quick failure recovery for Metro Ethernet applications.

Troubleshooting

The DM4100 Series offers many resources to assist the operator in the monitoring and, problems or abnormalities solution in the network or equipment performance.

The support to SNMP, multiples Syslog Servers and RMON allow that event information, logs and traps are centralized, enabling quick and effective analysis and diagnosis.

Through the Mirroring feature is possible to redirect a copy of traffic of one or more ports which contains "n" VLANs to one specific port (N:1), or even between ports of different equipment in a stacking topology. Mirroring also can be configured in VLAN, DSCP and 802.1p, refining the traffic filtering to be mirrored. In DM4100 Series is possible to use RSPAN, it means, to perform the traffic of many ports into one VLAN. RSPAN permits that the Protocol Analyzer or any other element does not need to be connected in the same equipment of mirrored ports.

DM4100 Series provides some tools for network and cabling infrastructure diagnosis, including Digital Diagnostic (SFF 8472). Cables may be tested for interruptions or cable failures through specific commands for diagnoses.

Multicast L2 e L3

Designed to multicast applications, the DM4100 forward the multicast packages of L2 and L3 in hardware. It supports the protocols IGMP v1/v2/v3, MLD v1/v2, PIM-SM with support in hardware for PIM-Register messages encapsulation, in accordance with RFC4601 and the PIM-SSM function, according RFC4607. It also supports Designated Router (DR) election and Rendezvous Point (RP) configuration by static mode or via BootStrap.

L2 and L3 multicast applications are supported through 4,096 L2/L3 IP groups. Are also implemented the IGMP multicast protocol (snooping and query functions), MLDv1/v2, MVR feature and PIM protocol.

OAM Ethernet

DM4100 Series support End-to-End OAM (CFM) according IEEE 802.1ag and ITU-T Y.1731. Thus, it is possible to perform a proactive monitoring of connectivity (Continuity Check) and failure isolation by Loopback Messages (L2 ping) and Linktrace Message (L2 traceroute).

The equipment provides support Point-to-Point OAM (EFM), according IEEE 802.3ah standard. It enables the failure indication, including Dying Gasp, Unidirectional Link and Critical Event. The EFM works with configurable PDU gaps, ensuring interoperability with other trademarks.

FTTx Applications

The DM4100 Series feature the provision of Fiber-to-the-Wherever services, since the equipment ports have SFP interfaces, allowing the use of different types of optical modules accordingly to the fiber type, speed and distance chosen.

The DATACOM SFP, SFP+ and XFP modules are tested to fulfill the INF-8074i and IEC60825-1 Specification. Non-approved modules do not guarantee the correct operation of the equipment and can damage the interface cards. From Firmware version 12,4 onwards, DATACOM equipment family will allow the usage of non-homologated SFPs. However, in previous firmware versions the DATACOM equipment will check if the SFP is homologated and if not, it will perform the lockout of the module. Contact the technical support of DATACOM to further information about the risks of usage of non-homologated SFP and the possibility of unlock them.

Available Models

Available Models	1000Base-X Ports	10/100/1000 Base-T Ports	Combo 1000Base-X 10/100/1000 Base-T Ports	10GbE Ports	Ports with PoE+ support	Stackable	Switch Fabric (Gbps)	Packet Processing (Mpps)	MPLS Support	Power Supply	Equipm. Power	Max PoE Power
DM4100 ETH24GX+2XX+S+MPLS	24	-	-	2 XFP	-	yes[8]	140	104,2	licensable	Redundand, Hotswap AC/DC	80W	-
DM4100 ETH24GX+2XX+S+L3	24	-	-	2 XFP	-	yes[8]	140	104,2	-	Redundand, Hotswap AC/DC	80W	-
DM4100 ETH24GX+4GX+L3	28	-	-	-	-	-	56	41,7	-	Redundand, Hotswap AC/DC	80W	-
DM4100 ETH24GX+4XX+L3	24	-	-	4 XFP	-	-	128	95,2	-	Redundand, Hotswap AC/DC	85W	-
DM4100 ETH24GX+4GX+MPLS	28	-	-	-	-	-	56	41,7	licensable	Redundand, Hotswap AC/DC	80W	-
DM4100 ETH24GX+4XX+MPLS	24	-	-	4 XFP	-	-	128	95,2	licensable	Redundand, Hotswap AC/DC	85W	-
DM4100 ETH24GX+4XS+MPLS	24	-	-	4 SFP+	-	-	128	95,2	licensable	Redundand, Hotswap AC/DC	85W	-
DM4100 ETH20GT+4GC+S+MPLS	-	20	4	-	-	yes[8]	100	74,4	licensable	Redundand, Hotswap AC/DC	75W	-
DM4100 ETH20GT+4GC+2XX+S+MPLS	-	20	4	2 XFP	-	yes[8]	140	104,2	licensable	Redundand, Hotswap AC/DC	80W	-
DM4100 ETH20GT+4GC+S+L3	-	20	4	-	-	yes[8]	100	74,4	-	Redundand, Hotswap AC/DC	75W	-
DM4100 ETH20GT+4GC+2XX+S+L3	-	20	4	2 XFP	-	yes[8]	140	104,2	-	Redundand, Hotswap AC/DC	80W	-
DM4100 ETH20GT+4GC+2XS+S+L3	-	20	4	2 SFP+	-	yes[8]	140	104,2	-	Redundand, Hotswap AC/DC	80W	-
DM4100 ETH20GT+4GC+L3	-	20	4	-	-	-	48	35,7	-	Redundand, Hotswap AC/DC	75W	-
DM4100 ETH20GT+4GC+4XX+L3	-	20	4	4 XFP	-	-	128	95,2	-	Redundand, Hotswap AC/DC	85W	-
DM4100 ETH20GT+4GC+4XS+L3	-	20	4	4 SFP+	-	-	128	95,2	-	Redundand, Hotswap AC/DC	85W	-
DM4100 ETH20GT+4GC+4XX+MPLS	-	20	4	4 XFP	-	-	128	95,2	licensable	Redundand, Hotswap AC/DC	85W	-
DM4100 ETH20GP+4GC+S+L3	-	20	4	-	24	yes[8]	100	74,4	-	Internal AC	80W	411W
DM4100 ETH20GP+4GC+2XX+S+L3	-	20	4	2 XFP	24	yes[8]	140	104,2	-	Internal AC	85W	411W
DM4100 ETH20GP+4GC+2XS+S+L3	-	20	4	2 SFP+	24	yes[8]	140	104,2	-	Internal AC	85W	411W
DM4100 ETH20GP+4GC+4XX+L3	-	20	4	4 XFP	24	-	128	95,2	-	Internal AC	90W	411W
DM4100 ETH20GP+4GC+4XS+L3	-	20	4	4 SFP+	24	-	128	95,2	-	Internal AC	90W	411W
DM4100 ETH44GT+4GC+S+L3	-	44	4	-	-	yes[8]	160	119,0	-	Internal AC	160W	-
DM4100 ETH44GT+4GC+2XX+S+L3	-	44	4	2 XFP	-	yes[8]	200	148,8	-	Internal AC	165W	-
DM4100 ETH44GT+4GC+2XS+S+L3	-	44	4	2 SFP+	-	yes[8]	200	148,8	-	Internal AC	165W	-
DM4100 ETH44GT+4GC+S+MPLS	-	44	4	-	-	yes[8]	160	119,0	licensable	Internal AC	160W	-
DM4100 ETH44GT+4GC+S+MPLS (DC)	-	44	4	-	-	yes[8]	160	119,0	licensable	Redundant DC	120W	-
DM4100 ETH44GT+4GC+2XX+S+MPLS	-	44	4	2 XFP	-	yes[8]	200	148,8	licensable	Internal AC	165W	-
DM4100 ETH44GT+4GC+2XX+S+MPLS (DC)	-	44	4	2 XFP	-	yes[8]	200	148,8	licensable	Redundant DC	125W	-
DM4100 ETH44GT+4GC+4XX+L3	-	44	4	4 XFP	-	-	176	131,0	-	Internal AC	170W	-
DM4100 ETH44GT+4GC+4XS+L3	-	44	4	4 SFP+	-	-	176	131,0	-	Internal AC	170W	-
DM4100 ETH44GT+4GC+4XX+MPLS	-	44	4	4 XFP	-	-	176	131,0	licensable	Internal AC	170W	-
DM4100 ETH44GT+4GC+4XX+MPLS (DC)	-	44	4	4 XFP	-	-	176	131,0	licensable	Redundant DC	130W	-
DM4100 ETH44GP+4GC+S+L3	-	44	4	-	48	yes[8]	160	119,0	-	Internal AC	160W	822W
DM4100 ETH44GP+4GC+2XX+S+L3	-	44	4	2 XPP	48	yes[8]	200	148,8	-	Internal AC	165W	822W
DM4100 ETH44GP+4GC+2XS+S+L3	-	44	4	2 SFP+	48	yes[8]	200	148,8	-	Internal AC	165W	822W
DM4100 ETH44GP+4GC+4XX+L3	-	44	4	4 XFP	48	-	176	131,0	-	Internal AC	170W	822W
DM4100 ETH44GP+4GC+4XS+L3	-	44	4	4 SFP+	48	-	176	131,0	-	Internal AC	170W	822W

Hardware Characteristics

All DM4100 models are 1U height and ready for standard 19 inches racks.

The power sources for the have the following characteristics (according to above table):

- PSU-85: Redundant AC/DC Hotswap: removable power source unit, with AC 100V ~240V 50Hz/60Hz, DC 48V/60V+-20% ou 125VDC input;
- Internal AC: internal fixed power source unit with AC 100V~240V 50Hz/60Hz input;
- Redundant DC: two DC inputs for 48V/60V +-20%.

The following table shows the internal tables and interfaces capacities of the DM4100 products:

DM4100 Models	MAC Address Table	L3 Hosts (IPv4)	L3 Hosts (IPv6)	L3 Routes (IPv4)	L3 Routes (IPv6)	L2 Multicast Groups	L3 (IPv4) Multicast Groups	L3 (IPv6) Multicast Groups	Stacking (models with **+S** in the name only)	Access Control Lists (ACLs)	Alarms
ETH24GX, ETH20GT and ETH20GP Models	32k	4k	4k	12k	6k	1k	4k	2k	2 dedicated ports - 52Gbit/s[8] total	2k	3 inputs 1 output
ETH44GT and ETH44GP Models	32k	4k	4k	12k	6k	1k	4k	2k	2 dedicated ports - 64Gbit/s[8] total	2k	2 inputs 1 output

Software

Characteristics	Details
Flow Control	Backpressure in half duplex; PAUSE (IEEE 802.3x) in full duplex
Interface Basic Parameters	Description, MDI/MDIX, Speed Mode and Duplex Mode, Flow Control,
	Port MTU Size, GARP, Link-Flap detection, Port-Channel, switchport
Auto-negotiation	Speed, duplex mode, flow control and MDI/MDIX
Management	**HTTP/HTTPs** Access with more than one simultaneous access
	Remote Management of Network Devices through the protocol **RDM**
	SNMP v1/v2c/v3 over IPv4 and IPv6
	Command Line Interface (CLI) via SSHv2 (IPv4/IPv6), Telnet (IPv4/IPv6) and Conso RJ45, USB(1) or RS232
	RMON groups 1 (statistics), 2 (historic), 3 (alarms) and 9 (events)
	ACL configuration with multiple comparisons and actions
	Network Diagnostic Tools (telnet, traceroute, ping) IPv4 and IPv6
	Cabling Diagnostic Tool
	Up to **2 firmwares** in flash, with upgrade via SCP, TFTP or HTTP/HTTPS
	Up to **10 configurations** in flash, with upload or download via SCP, TFTP or **HTTP/HTTPS**
	Actions Scheduling through commands script
	XML Management Interface supporting cryptography
	OAM (**EFM – IEEE 802.3ah, CFM – IEEE 802.1ag, Y.1731 and E-LMI**)
	Link Layer Discovery Protocol (**LLDP – IEEE 802.1ab**)
	Traffic Monitoring via SNMP to interface traffic and CPU usage and processor memory
	Remote equipment management "**IP less**" IEEE 802.3ah extension
	SNMP access to **QoS Counter**
	Static or dynamic IP address through **DHCP Client**
	DHCP relay (RFC 2131) with option 82
Management	**DHCP** for **IPv6**

Characteristics	Details
	CPU Protection system against IPv4 or IPv6 packet flood
	Switch interface port identification through text names up to 64 characters
	NTP / SNTP
Security	**IEEE 802.1x** with **guest vlan, restricted vlan** and **vlan assignment**
	Filters in HW to **access control SNMP, Telnet and SSH**
	MAC Address Limit configurable per port and per VLAN
	Allow only **Authorized DHCP Servers**
	Syslog Local and Remote with support to **Multiples Syslog Servers**
	Mutual Authentication (two-way-party authentication), authorization and accounting (AAA) **RADIUS** and **TACACS+**
	E-mail notification (SMTP)
	Protection Mechanisms against **Denial of Service attacks (DoS/DDoS), MAC Move**
VLAN	VLAN Tagging with 4094 VIDs in simultaneous usage (**IEEE 802.1q**)
	Port-based, with ports overlap possibility
	Protocol-based (IEEE 802.1v), **MAC-based**, **IP-Subnet based** (1)
	Q-in-Q double tagging, Selective Q-in-Q
	Communication Separation between interfaces of the same **VLAN** or broadcast domain
	VLAN Translate allowing insertion, removal or swap
	Inter-VLAN Routing (IPv4/v6)
	Voice VLAN
	Link Layer Discovery Protocol for Media Endpoint Devices **(LLDP-MED)**
Protection	**Classic Spanning Tree** (IEEE 802.1d) up to 16 instances
	Rapid Spanning Tree (IEEE 802.1w) up to 16 instances
	Per-VLAN Rapid Spanning Tree up to 16 instances
	Multiple Spanning Tree (IEEE 802.1s) up to 16 instances
	Backup-Link

Characteristics	Details
	Monitoring of network link status through **Link State Tracking**
Protection	Logs of violation attempts
	Loopback Detection
	BPDU Guard
	Protection Against DOS in IP and ARP Spoofing
	Static ARP **(IMPB)**
	Link flap
	Ethernet Automatic Protection Switching **(EAPS)**
	Ethernet Ring Protection Switching **(ERPS)**
QoS: Marking Classifying Priorization	**8 queues** per port in hardware
	Packet classification though layers 2, 3 and 4
	TCI tagging (**IEEE 802.1p**), **IP Precedence/TOS** or **DSCP/TOS**
	Source/Destination IP and/or **MAC** and/or **TCP/UDP ports**
	Packet classification and marking based on MPLS-EXP field
	Filter rules
	Rate Shaping (Ingress e Egress) in hardware, with granularity of **64 kbit/s** per **port** and per **traffic flow** in **CIR** and **PIR** definition
	Weighted Round Robin, Weighted Fair Queuing, Strict Priority or a combination of these techniques as queue scheduling algorithm
	Hierarchical QoS **(HQoS)** (3)
	Weighted Random Early Detection **(WRED)** support
Link Aggregation	Dynamic or static configuration via **LACP** (IEEE 802.3ad)
	Up to **128 logical groups**, with **8 active ports** in each group
	Equivalent use to non-aggregated links for L2, L3, MPLS and QoS functions
	Configurable Load Balance Criteria (i.e MAC, IP, etc.)
	Allow Link Aggregation groups with ports from different switches in a stacked configuration
L2 Functionalities	Maximum **Broadcast, Multicast and DLF** rate, controlled by port

Characteristics	Details
	Support to **Jumbo Frame** of up to 9KB
	IGMP (v1/v2/v3) fore **Snooping**, **Query** and **SSM Mapping** functions
	Aging L2
	Tunneling of protocols **L2 (TLS)**
	MAC Learning Disabling per port or per VLAN.
	Multicast VLAN Registration **(MVR)**
L2 Functionalities	Captive Portal
	Port Authentication **IEEE 802.1x via MAC** in Radius Server (RADA)
	Statics MAC Addresses attribution per interface, broadcast and multicast
	Traffic Monitor for **ports** (4 MTP simultaneous sessions) and/or **packets flow IPFIX rate 1:1000**(3)
	RSPAN Remote Switched Port Analyzer
L3 Functionalities	**Static Routing** (IPv4/v6(3))
	RIPv2, OSPF v2/v3(3) and **BGP v4**
	Support for up to 128 OSPFv2 adjacencies and up to 128 OSPFv2 areas
	Dual-stack Layer IPv4/IPv6(3) (RFC 4213)
	Packets Tunneling IPv6 in IPv4 (6over4)
	VRRP Redundancy (including *dual stack* IPv4/IPv6)
	PIM Protocol IPv4/IPv6(3)
	IP Local Proxy ARP
	Policy Based Routing (**PBR**) in hardware
	Equal-Cost Multi-Path **(ECMP)**
	Route Redistribution among protocols (static, RIPv2, OSPF, BGP)
	Non Stop Routing for OSPF, BGP and LDP
	MD5 Authentication for OSPFv2/v3(3) and BGP protocols
	route-map and **prefix-list** to filtering and conditional announcement of routes
	Jumbo Frame Supporting of up to 9KB

Characteristics	Details
	Support for up to 512 L3 interfaces (VLAN with configured IP)
MPLS	**VPWS** - L2 VPN over MPLS (**Draft Martini**) and **Backup PW**
	VPLS – Virtual LAN Services and H-VPLS – Hierarchical VPLS
	Support for up to 1024 pseudowires and up to 256 VPNs
	Label Distribution Protocol (**LDP**), with up to 128 sessions and up to 256 LDP target sessions
	Resource Reservation Port-Traffic Engineering (RSVP-TE) with Fast Reroute (FRR)
	Resource Reservation Protocol (**RSVP**)
	Time to Live **(TTL)** Processing in Multi-Protocol Label Switching (**MPLS**) Networks
	LDP Tunneling over RSVP-TE
MPLS	The USE of **RSVP** with IETF Integrated Service (INTERSERV)

Compliance with Main Standards

For a complete list of Standards, which DATACOM complain with, get contact with DATACOM Technical Support.

IEEE

802.1ab	Link Layer Discovery Protocol (LLDP)
802.1ad	Provider Bridges
802.1ag	Connectivity Fault Management (CFM)
802.1d	Media Access Control (MAC) Bridge
802.1p	Priority Support
802.1q	Virtual LAN
802.1q-in-q	VLAN Stacking
802.1s	Multiple Spanning Tree (MSTP)
802.1x	Port Security
802.1w	Rapid Spanning Tree
802.3	10 BASE T
802.3ab	1000 BASE T
802.3ac	Extension for VLAN Tagging
802.3ad	Link Aggregation (LAG)
802.3ah	Ethernet First Mile (EFM)
802.3ae	10G BASE-SR/LR/ER/SW/LW/EW
802.3af	Power Over Ethernet
802.3at	Power Over Ethernet +
802.3i	10BASE-T 10 Mbit/s (1.25 MB/s)
802.3u	100 BASE TX
802.3x	Flow Control
802.3z	1000 BASE SX/LX

ITU-T	
Y.1731	OAM functions and mechanisms for Ethernet based networks
MEF	
9	MEF 9 - Abstract Test Suite for Ethernet Services at the UNI
14	MEF 14 - Abstract Test Suite for Traffic Management Phase 1
24	MEF 24 - Abstract Test Suite for UNI Type 2 Part 2 E-LMI
IETF	
RFC854	Telnet Protocol Specification
RFC1027	Using ARP to Implement Transparent Subnet Gateways
RFC1492	An Access Control Protocol, Sometimes Called TACACS
RFC1812	Requirements for IP Version 4 Routers (Ipv4)
RFC1981	Path MTU Discovery for IP version 6
RFC2030	Simple Network Time Protocol (SNTP)
RFC2104	HMAC: Keyed-Hashing for Message Authentication
RFC2131	DHCP/BOOTP Relay
RFC2138	Remote Authentication Dial In User Service (RADIUS)
RFC2139	RADIUS Accounting
RFC2460	IPv6 Specification
RFC2461	IPv6 Neighbor Discovery
RFC2462	IPv6 Stateless Address Auto-Configuration
RFC2464	Transmission of IPv6 over Ethernet Networks
RFC2544	Benchmarking Methodology for Network Interconnect Devices
RFC2865	Remote Authentication Dial In User Server (RADIUS)
RFC3021	Using 31-Bit Prefixes on IPv4 Point-to-Point Links
RFC3164	The BSD Syslog Protocol
RFC3176	sFlow: A Method for Monitoring Traffic in Switched and Routed Networks
RFC3272	Overview and Principles of Internet Traffic Engineering
RFC3484	Default Address Selection for Internet Protocol version 6 (IPv6)
RFC3513	IPv6 Addressing Architecture

RFC3579	RADIUS Support for EAP
RFC3587	IPv6 Global Unicast Address Format
RFC3619	Ethernet Automatic Protection Switching (EAPS) version 1
RFC4213	Transmission Mechanisms for IPv6 Hosts/Routers – Dual Layer
RFC4250	The Secure Shell (SSH) Protocol Assigned Numbers
RFC4251	The Secure Shell (SSH) Protocol Architecture
RFC4252	The Secure Shell (SSH) Authentication Protocol
RFC4253	The Secure Shell (SSH) Transport Layer Protocol
RFC4254	The Secure Shell (SSH) Connection Protocol
RFC4291	IPv6 Addressing Architecture
RFC4443	ICMPv6
RFC4861	Neighbor Discovery for IP version 6 (IPv6)
RFC4862	IPv6 Stateless Address Autoconfiguration
RFC5517	Private VLANs: Scalable Security in a Multi-Client Environment
RFC5942	IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes

Routing

RFC1058	RIP Version 1 - Routing Information Protocol
RFC1723	RIP Version 2 - Carrying Additional Information
RFC1997	BGP Communities Attribute
RFC1998	BGP Community Attribute in Multi-Home Routing
RFC2080	RIPng (1)
RFC2082	RIP Version 2 MD5 Authentication
RFC2154	OSPF with Digital Signatures
RFC2328	OSPF Version 2
RFC2329	OSPF Standardization Report
RFC2338	Virtual Router Redundancy Protocol
RFC2370	The OSPF Opaque LSA Option
RFC2385	Protection of BGP Sessions via the TCP MD5 Signature Option

RFC2439	BGP Route Flap Damping
RFC2453	RIP Version 2
RFC2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC2740	OSPF for IPv6 (OSPFv3
RFC2796	BGP Route Reflector An Alternative to Full Mesh BGP
RFC2842	Capabilities Advertisement with BGP-4
RFC2858	Multiprotocol Extensions for BGP-4
RFC2918	Route Refresh Capability for BGP-4
RFC3021	Using 31-Bit Prefixes on IPv4 Point-to-Point Links
RFC3065	Autonomous System Confederations for BGP
RFC3101	The OSPF NSSA Option
RFC3137	OSPF Stub Router Advertisement
RFC3315	Dynamic Host Configuration Protocol for IPv6
RFC3392	Capabilities Advertisement with BGP-4
RFC3623	Graceful OSPF Restart
RFC3630	Traffic Engineering (TE) Extensions to OSPF Version 2
RFC3768	Virtual Router Redundancy Protocol (VRRP)
RFC4271	A Border Gateway Protocol 4 (BGP-4)
RFC4360	BGP Extended Communities Attribute
RFC4724	Graceful Restart Mechanism for BGP
RFC4760	Multiprotocol Extensions for BGP-4
RFC4893	BGP Support for Four-octet AS Number Space
RFC5065	Autonomous System Confederations for BGP
RFC5250	The OSPF Opaque LSA Option
RFC5291	Outbound Route Filtering Capability for BGP-47
RFC5396	Textual Representation of Autonomous System (AS) Numbers
RFC5492	Capabilities Advertisement with BGP-4

Multicast

RFC1112	Host extensions for IP multicasting
RFC2236	Internet Group Management Protocol, Version 2
RFC2710	Multicast Listener Discovery (MLD) for IPv6
RFC3376	Internet Group Management Protocol, Version 3
RFC3569	An Overview of Source-Specific Multicast (SSM)
RFC3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast
RFC4601	Protocol Independent Multicast – Sparse Mode (PIM-SM)
RFC4604	Using IGMP Version 3 for Source Specific Multicast
RFC4607	Source-Specific Multicast for IP
RFC4608	Source-Specific Protocol Independent Multicast in 232/8

MPLS

RFC2205	RSVP v1 Functional Specification
RFC2209	Resource ReSerVation Protocol (RSVP) - Version 1 Message Processing Rules
RFC2210	The USE of RSVP with IETF Integrated Service
RFC2702	Requirements for traffic engineering over MPLS
RFC2961	RSVP Refresh Overhead Reduction Extensions
RFC3031	MPLS architecture
RFC3032	MPLS label stack encoding
RFC3036	LDP specification
RFC3037	LDP applicability
RFC3209	Extensions to RSVP for LSP tunnels
RFC3210	Applicability statement for extensions to RSVP for LSP Tunnels
RFC3215	LDP state machine
RFC3270	Multi-protocol label switching (MPLS) support of differentiated services
RFC3346	Applicability Statement for Traffic Engineering with MPLS
RFC3443	TTL Processing in Multiprotocol Label Switching (MPLS) Networks
RFC3469	Framework for MPLS-based recovery

RFC3916	Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
RFC3985	Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
RFC4090	Fast reroute extensions to RSVP-TE for LSP tunnels
RFC4182	Removing a restriction on the use of MPLS explicit NULL
RFC4221	MPLS management overview
RFC4377	OAM Requirements for MPLS Networks
RFC4378	A framework for MPLS Operation and Management
RFC4446	IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)
RFC4447	Pseudowire Setup and Maintenance Using the LDP
RFC4448	Encapsulation methods for transport of Ethernet over MPLS
RFC4664	Framework for L2VPNs
RFC4665	Service Requirements for Layer 2 Provider-Provisioned VPN
RFC4762	Virtual Private LAN Service (VPLS) Using LDP Signaling
RFC4905	Encapsulation Methods for Transport of Layer 2 Frames Over MPLS
RFC4906	Transport of Layer 2 Frames Over MPLS
RFC5036	LDP Specification

QoS

RFC2309	Queue Management and Congestion Avoidance in the Internet
RFC2474	Definition of the differentiated services field (DS) in Ipv4
RFC2475	An architecture for differentiated services
RFC2597	Assured Forwarding PHB Group
RFC2598	An Expedited Forwarding PHB
RFC2697	A single rate three color marker
RFC2698	A two rate three color marker
RFC3140	Per hop behavior identification codes
RFC3246	An expedited forwarding PHB
RFC3644	Policy quality of service (QoS) Information model
RFC3670	Information model for describing network device QoS datapath mechanism

MIB e SNMP

RFC1157	Simple Network Management Protocol (SNMP)
RFC1212	Concise MIB Definitions
RFC1213	MIB for Network Management of TCP/IP-based internets:MIB-II
RFC1215	A Convention for Defining Traps for use with the SNMP
RFC1229	Extensions to the generic-interface MIB
RFC1441	SNMPv2 Protocol Framework
RFC1493	Definitions of Managed Objects for Bridges
RFC1573	Evolution of the Interfaces Group of MIB-II
RFC1643	Definitions of Managed Objects for the Ethernet-like InterfaceTypes
RFC1650	Definitions of Managed Objects for the Ethernet-like IF Types using SMIv2
RFC1724	RIP Version 2 MIB Extension
RFC1757	Remote Network Monitoring Management Information Base
RFC1850	OSPF Version 2 Management Information Base
RFC1901	Introduction to Community-based SNMPv2
RFC1902	Structure of Management Information for Version 2 of SNMPv2
RFC1903	Textual Conventions for Version 2 of SNMPv2
RFC1904	Conformance Statements for Version 2 of SNMPv2
RFC1905	Protocol Operations for Version 2 of SNMPv2
RFC1906	Transport Mappings for SNMPv2
RFC1907	Management Information Base (MIB) for SNMPv2
RFC1908	Coexistence between V1 and V2 of the Internet-standard NMF
RFC2021	Remote Network Monitoring MIBv2 using SMIv2
RFC2037	Entity MIB using SMIv2
RFC2233	The Interfaces Group MIB using SMIv2
RFC2570	Introduction to V3 of the Internet-standard NMF
RFC2571	An Architecture for Describing SNMP Management Framework
RFC2572	Message Processing and Dispatching for SNMP

RFC2573	SNMP Applications
RFC2574	USM for version 3 of SNMPv3
RFC2575	VACM for SNMP
RFC2576	Coexistence between SNMP v1,v2,v3
RFC2578	Structure of Management Information for SNMPv2
RFC2579	Textual Conventions for SNMPv2
RFC2580	Conformance Statements for SMIv2
RFC2665	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC2674	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
RFC2819	Remote Network Monitoring MIB
RFC2863	The Interfaces Group MIB
RFC3411	An Architecture for Describing SNMP Management Framework
RFC3412	Message Processing and Dispatching for SNMP
RFC3413	SNMP Application
RFC3414	User-based Security Model for SNMPv3
RFC3415	View-based Access Control Model for SNMP
RFC3416	Protocol Operations for SNMPv2
RFC3812	MPLS Traffic Engineering Management Information Base7
RFC3813	MPLS LSR Management Information Base
RFC3814	MPLS FEC-To-NHLFE Management Information Base
RFC3815	Definitions of Managed Objects for the MPLS, LDP
RFC4188	Definitions of Managed Objects for Bridges
RFC4273	Definitions of Managed Objects for BGP-4 using SMIv27
RFC4292	IP Forwarding Table MIB
RFC4293	MIB for the Internet Protocol
RFC4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions

Accessories

- PSU 85 100-250 VAC/48-60 VDC / 125VDC modular supply, full range, hot-swappable, redundant
- Stacking Cable: length 0,50m
- Stacking Cable: length 1,00m

---

1 Check for availability according purchased hardware and software versions
2 Check equipment manual or tables for the switch fabric capacity per HW model
3 Dependent on hardware model
4 Dependent on software license
5 Class 3 devices
6 Class 4 devices
7 For maximum reach, check attenuation
8 Stacking functionalities available for L2 and L3 applications. For MPLS applications, get contact with DATACOM's Technical Support
9 Some VLANs can be required for internal use, remaining 4094 VLANs for effective usage
10 When assembled in a stacking topology, the maximum value will be the lower of the available for each model

Specifications and product availability presented may change without notice.