GE
Grid Solutions

Multilink ML3000/ML3100 Ethernet Switch Series

Instruction Manual

Firmware Revision: 5.x

Manual P/N: 1601-0049-A5

GE publication code: GEK-113632D

GE Grid Solutions
650 Markland Street
Markham, Ontario
Canada L6C 0M1
Tel: +1 905 927 7070 Fax: +1 905 927 5098
Internet: http://www.gegridsolutions.com

GE Multilin's Quality Management System is registered to ISO9001:2008

QMI # 005094
UL # A3775

The Multilink ML3000/ML3100 Instruction Manual for revision 5.x.

Part number: 1601-0049-A5 (November 2017)

These instructions do not purport to cover all details or variations in equipment nor provide for every possible contingency to be met in connection with installation, operation, or maintenance. Should further information be desired or should particular problems arise which are not covered sufficiently for the purchaser's purpose, the matter should be referred to the General Electric Company.

To the extent required the products described herein meet applicable ANSI, IEEE, and NEMA standards; but no such assurance is given with respect to local codes and ordinances because they vary greatly.

NEBS is a trademark of Telcordia Technologies

Federal Communications Commission

Radio Frequency Interference Statement

This equipment generates, uses and can radiate frequency energy and if not installed and used properly in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at their own expense, will be required to take whatever measures may be required to correct the interference.

Canadian Emissions Statement

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil respecte toutes les exigences du Réglement sur le matériel du Canada. Cet appareil est Classe A..

Electrical Safety requirements:

- This product is to be installed Only in Restricted Access Areas (Dedicated Equipment Rooms, Electrical Closets, or the like).
- 48 V DC products shall be installed with a readily accessible disconnect device in the building installation supply circuit to the product.
- This product shall be provided with a maximum 10 A DC Listed fuse or circuit breaker in the supply circuit when connected to a 48 V centralized DC source.
- The external power supply for DC units shall be a Listed, Direct Plug In power unit, marked Class 2, or Listed ITE Power Supply, marked LP, which has suitably rated output voltage (i.e. 48 V DC) and suitable rated output current.
- Product does not contain user replaceable fuses. Any internal fuses can ONLY be replaced by GE Grid Solutions.
- Models with a DC power source must be supplied with a DC supply source to the equipment that is derived from a secondary circuit which is isolated from the AC Mains by Double or Reinforced Insulation (eg: UL Certified ITE power supply which provides Double or Reinforced Insulation).

GENERAL SAFETY PRECAUTIONS

- Failure to observe and follow the instructions provided in the equipment manual(s) could cause irreversible damage to the equipment and could lead to property damage, personal injury and/or death.
- Before attempting to use the equipment, it is important that all danger and caution indicators are reviewed.
- If the equipment is used in a manner not specified by the manufacturer or functions abnormally, proceed with caution. Otherwise, the protection provided by the equipment may be impaired and can result in Impaired operation and injury.
- Caution: Hazardous voltages can cause shock, burns or death.
- Installation/service personnel must be familiar with general device test practices, electrical awareness and safety precautions must be followed.
- Before performing visual inspections, tests, or periodic maintenance on this device or associated circuits, isolate or disconnect all hazardous live circuits and sources of electric power.
- Failure to shut equipment off prior to removing the power connections could expose you to dangerous voltages causing injury or death.
- All recommended equipment that should be grounded and must have a reliable and un-compromised grounding path for safety purposes, protection against electromagnetic interference and proper device operation.
- Equipment grounds should be bonded together and connected to the facility's main ground system for primary power.
- Keep all ground leads as short as possible.
- At all times, equipment ground terminal must be grounded during device operation and service.
- In addition to the safety precautions mentioned all electrical connections made must respect the applicable local jurisdiction electrical code.
- This product contains Class I lasers.
- Chassis power supply ratings must be verified for suitablility before inserting removable power supply modules.

BATTERY DISPOSAL

EN Battery Disposal

This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

CS Nakládání s bateriemi

Tento produkt obsahuje baterie, které nemohou být zneškodněny v Evropské unii jako netříděný komunální odpadu. Viz dokumentace k produktu pro informace pro konkrétní baterie. Baterie je označena tímto symbolem, který může zahrnovat i uvedena písmena, kadmium (Cd), olovo (Pb), nebo rtuť (Hg). Pro správnou recyklaci baterií vraťte svémudodavateli nebo na určeném sběrném místě. Pro více informací viz: www.recyclethis.info

DA Batteri affald

Dette produkt indeholder et batteri som ikke kan bortskaffes sammen med almindeligt husholdningsaffald i Europa. Se produktinformation for specifikke informationer om batteriet. Batteriet er forsynet med indgraveret symboler for hvad batteriet indeholder: kadmium (Cd), bly (Pb) og kviksølv (Hg). Europæiske brugere af elektrisk udstyr skal aflevere kasserede produkter til genbrug eller til leverandøren. Yderligere oplysninger findes på webstedet www.recyclethis.info.

DE Entsorgung von Batterien

Dieses Produkt beinhaltet eine Batterie, die nicht als unsortierter städtischer Abfall in der europäischen Union entsorgt werden darf. Beachten Sie die spezifischen Batterie-informationen in der Produktdokumentation. Die Batterie ist mit diesem Symbol gekennzeichnet, welches auch Hinweise auf möglicherweise enthaltene Stoffe wie Kadmium (Cd), Blei (Pb) oder Quecksilber (Hektogramm) darstellt. Für die korrekte Wiederverwertung bringen Sie diese Batterie zu Ihrem lokalen Lieferanten zurück oder entsorgen Sie das Produkt an den gekennzeichneten Sammelstellen. Weitere Informationen hierzu finden Sie auf der folgenden Website: www.recyclethis.info.

EL Απόρριψη μπαταριών

Αυτό το προϊόν περιέχει μια μπαταρία που δεν πρέπει να απορρίπτεται σε δημόσια συστήματα απόρριψης στην Ευρωπαϊκή Κοινότητα. Δείτε την τεκμηρίωση του προϊόντος για συγκεκριμένες πληροφορίες που αφορούν τη μπαταρία. Η μπαταρία είναι φέρει σήμανση με αυτό το σύμβολο, το οποίο μπορεί να περιλαμβάνει γράμματα για να δηλώσουν το κάδμιο (Cd), τον μόλυβδο (Pb), ή τον υδράργυρο (Hg). Για την κατάλληλη ανακύκλωση επιστρέψτε την μπαταρία στον προμηθευτή σας ή σε καθορισμένο σημείο συλλογής. Για περισσότερες πληροφορίες δείτε: www.recyclethis.info.

ES Eliminacion de baterias

Este producto contiene una batería que no se pueda eliminar como basura normal sin clasificar en la Unión Europea. Examine la documentación del producto para la información específica de la batería. La batería se marca con este símbolo, que puede incluir siglas para indicar el cadmio (Cd), el plomo (Pb), o el mercurio (Hg). Para el reciclaje apropiado, devuelva este producto a su distribuidor ó deshágase de él en los puntos de reciclaje designados. Para mas información: wwwrecyclethis.info.

ET Patareide kõrvaldamine

Käesolev toode sisaldab patareisid, mida Euroopa Liidus ei tohi kõrvaldada sorteerimata olmejäätmetena. Andmeid patareide kohta vaadake toote dokumentatsioonist. Patareid on märgistatud käesoleva sümboliga, millel võib olla kaadmiumi (Cd), pliid (Pb) või elavhõbedat (Hg) tähistavad tähed. Nõuetekohaseks ringlusse võtmiseks tagastage patarei tarnijale või kindlaksmääratud vastuvõtupunkti. Lisainformatsiooni saab Internetist aadressil: www.recyclethis.info.

FI Paristoje ja akkujen hävittäminen

Tuote sisältää pariston, jota ei saa hävittää Euroopan Unionin alueella talousjätteen mukana. Tarkista tuoteselosteesta tuotteen tiedot. Paristo on merkitty tällä symbolilla ja saattaa sisältää cadmiumia (Cd), lyijyä (Pb) tai elohopeaa (Hg). Oikean kierrätystavan varmistamiseksi palauta tuote paikalliselle jälleenmyyjälle tai palauta se paristojen keräyspisteeseen. Lisätietoja sivuilla www.recyclethis.info.

FR Élimination des piles

Ce produit contient une batterie qui ne peuvent être éliminés comme déchets municipaux non triés dans l'Union européenne. Voir la documentation du produit au niveau des renseignements sur la pile. La batterie est marqué de ce symbole, qui comprennent les indications cadmium (Cd), plomb (Pb), ou mercure (Hg). Pour le recyclage, retourner la batterie à votre fournisseur ou à un point de collecte. Pour plus d'informations, voir: www.recyclethis.info.

HU Akkumulátor hulladék kezelése

Ezen termék akkumulátort tartalmaz, amely az Európai Unión belül csak a kijelölt módon és helyen dobható ki. A terméken illetve a mellékelt ismertetőn olvasható a kadmium (Cd), ólom (Pb) vagy higany (Hg) tartalomra utaló betűjelzés. A hulladék akkumulátor leadható a termék forgalmazójánál új akkumulátor vásárlásakor, vagy a kijelölt elektronikai hulladékudvarokban. További információ a www.recyclethis.info oldalon.

IT Smaltimento batterie

Questo prodotto contiene una batteria che non può essere smaltita nei comuni contenitori per lo smaltimento rifiuti, nell' Unione Europea. Controllate la documentazione del prodotto per le informazioni specifiche sulla batteria. La batteria è contrassegnata con questo simbolo e può includere alcuni caratteri ad indicare la presenza di cadmio (Cd), piombo (Pb) oppure mercurio (Hg). Per il corretto smaltimento, potete restituirli al vostro fornitore locale, oppure rivolgervi e consegnarli presso i centri di raccolta preposti. Per maggiori informazioni vedere: ww.recyclethis.info.

LT Baterijų šalinimas

Šios įrangos sudėtyje yra baterijų, kurias draudžiama šalinti Europos Sąjungos viešose nerūšiuotų atliekų šalinimo sistemose. Informaciją apie baterijas galite rasti įrangos techninėje dokumentacijoje. Baterijos žymimos šiuo simboliu, papildomai gali būti nurodoma kad baterijų sudėtyje yra kadmio (Cd), švino (Pb) ar gyvsidabrio (Hg). Eksploatavimui nebetinkamas baterijas pristatykite į tam skirtas surinkimo vietas arba grąžinkite jas tiesioginiam tiekėjui, kad jos būtų tinkamai utilizuotos. Daugiau informacijos rasite šioje interneto svetainėje: www.recyclethis.info.

LV Bateriju likvidēšana

Šis produkts satur bateriju vai akumulatoru, kuru nedrīkst izmest Eiropas Savienībā esošajās sadzīves atkritumu sistēmās. Sk. produkta dokumentācijā, kur ir norādīta konkrēta informācija par bateriju vai akumulatoru. Baterijas vai akumulatora marķējumā ir šis simbols, kas var ietvert burtus, kuri norāda kadmiju (Cd), svinu (Pb) vai dzīvsudrabu (Hg). Pēc ekspluatācijas laika beigām baterijas vai akumulatori jānodod piegādātājam vai specializētā bateriju savākšanas vietā. Sīkāku informāciju var iegūt vietnē: www.recyclethis.info.

NL Verwijderen van baterijen

Dit product bevat een batterij welke niet kan verwijdert worden via de gemeentelijke huisvuilscheiding in de Europese Gemeenschap. Gelieve de product documentatie te controleren voor specifieke batterij informatie. De batterijen met deze label kunnen volgende indictaies bevatten cadium (Cd), lood (Pb) of kwik (Hg). Voor correcte vorm van kringloop, geef je de producten terug aan jou locale leverancier of geef het af aan een gespecialiseerde verzamelpunt. Meer informatie vindt u op de volgende website: www.recyclethis.info.

NO Retur av batteri

Dette produkt inneholder et batteri som ikke kan kastes med usortert kommunalt søppel i den Europeiske Unionen. Se produktdokumentasjonen for spesifikk batteriinformasjon. Batteriet er merket med dette symbolet som kan inkludere symboler for å indikere at kadmium (Cd), bly (Pb), eller kvikksølv (Hg) forekommer. Returner batteriet til leverandøren din eller til et dedikert oppsamlingspunkt for korrekt gjenvinning. For mer informasjon se: www.recyclethis.info.

PL Pozbywanie się zużytych baterii

Ten produkt zawiera baterie, które w Unii Europejskiej mogą być usuwane tylko jako posegregowane odpady komunalne. Dokładne informacje dotyczące użytych baterii znajdują się w dokumentacji produktu. Baterie oznaczone tym symbolem mogą zawierać dodatkowe oznaczenia literowe wskazujące na zawartość kadmu (Cd), ołowiu (Pb) lub rtęci (Hg). Dla zapewnienia właściwej utylizacji, należy zwrócić baterie do dostawcy albo do wyznaczonego punktu zbiórki. Więcej informacji można znaleźć na stronie internetowej www.recyclethis.info.

PT Eliminação de Baterias

Este produto contêm uma bateria que não pode ser considerado lixo municipal na União Europeia. Consulte a documentação do produto para obter informação específica da bateria. A bateria é identificada por meio de este símbolo, que pode incluir a rotulação para indicar o cádmio (Cd), chumbo (Pb), ou o mercúrio (hg). Para uma reciclagem apropriada envie a bateria para o seu fornecedor ou para um ponto de recolha designado. Para mais informação veja: www.recyclethis.info.

RU Утилизация батарей

Согласно европейской директиве об отходах электрического и электронного оборудования, продукты, содержащие батареи, нельзя утилизировать как обычные отходы на территории ЕС. Более подробную информацию вы найдете в документации к продукту. На этом символе могут присутствовать буквы, которые означают, что батарея собержит кадмий (Cd), свинец (Pb) или ртуть (Hg). Для надлежащей утилизации по окончании срока эксплуатации пользователь должен возвратить батареи локальному поставщику или сдать в специальный пункт приема. Подробности можно найти на веб-сайте: www.recyclethis.info.

SK Zaobchádzanie s batériami

Tento produkt obsahuje batériu, s ktorou sa v Európskej únii nesmie nakladať ako s netriedeným komunálnym odpadom. Dokumentácia k produktu obsahuje špecifické informácie o batérii. Batéria je označená týmto symbolom, ktorý môže obsahovať písmená na označenie kadmia (Cd), olova (Pb), alebo ortuti (Hg). Na správnu recykláciu vráťte batériu vášmu lokálnemu dodávateľovi alebo na určené zberné miesto. Pre viac informácii pozrite: www.recyclethis.info.

SL Odlaganje baterij

Ta izdelek vsebuje baterijo, ki je v Evropski uniji ni dovoljeno odstranjevati kot nesortiran komunalni odpadek. Za posebne informacije o bateriji glejte dokumentacijo izdelka. Baterija je označena s tem simbolom, ki lahko vključuje napise, ki označujejo kadmij (Cd), svinec (Pb) ali živo srebro (Hg). Za ustrezno recikliranje baterijo vrnite dobavitelju ali jo odstranite na določenem zbirališču. Za več informacij obiščite spletno stran: www.recyclethis.info.

SV Kassering av batteri

Denna produkt innehåller ett batteri som inte får kastas i allmänna sophanteringssytem inom den europeiska unionen. Se produktdokumentationen för specifik batteriinformation. Batteriet är märkt med denna symbol, vilket kan innebära att det innehåller kadmium (Cd), bly (Pb) eller kvicksilver (Hg). För korrekt återvinning skall batteriet returneras till leverantören eller till en därför avsedd deponering. För mer information, se: www.recyclethis.info. TR Pil Geri Dönüşümü Bu ürün Avrupa Birliği genel atık sistemlerine atılmaması gereken pil içermektedir. Daha detaylı pil bilgisi için ürünün kataloğunu inceleyiniz. Bu sembolle işaretlenmiş piller Kadmiyum(Cd), Kurşun(Pb) ya da Civa(Hg) içerebilir. Doğru geri dönüşüm için ürünü yerel tedarikçinize geri veriniz ya da özel işaretlenmiş toplama noktlarına atınız. Daha fazla bilgi için: www.recyclethis.info.

TR Pil Geri Dönüşümü

Bu ürün Avrupa Birliği genel atık sistemlerine atılmaması gereken pil içermektedir. Daha detaylı pil bilgisi için ürünün kataloğunu inceleyiniz. Bu sembolle işaretlenmiş piller Kadmiyum(Cd), Kurşun(Pb) ya da Civa(Hg) içerebilir. Doğru geri dönüşüm için ürünü yerel tedarikçinize geri veriniz ya da özel işaretlenmiş toplama noktlarına atınız. Daha fazla bilgi için: www.recyclethis.info.

Global Contacts

North America 1 905-927-7070

Latin America +55 11 3614 1700

Europe, Middle East, Africa +(34) 94 485 88 00

Asia +86-21-2401-3208

India +91 80 41314617

Safety words and definitions

The following symbols used in this document indicate the following conditions.

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

Indicates practices not related to personal injury.

TABLE OF CONTENTS

Multilink ML3000/ML3100

Chapter 1: Introduction

1.1 Getting Started

1.1.1 Inspecting the Package and Product

Examine the shipping container for obvious damage prior to installing this product; notify the carrier of any damage that you believe occurred during shipment or delivery. Inspect the contents of this package for any signs of damage and ensure that the items listed below are included.

This package should contain:

- MultiLink ML3000/ML3100 Ethernet Switch, base unit (configured with user-selected port module options installed)
- Set of metal “ears” for 19-inch rack mounting
- Installation and user guide (this manual)

Remove the items from the shipping container. Be sure to keep the shipping container should you need to re-ship the unit at a later date. To validate the product warranty, please complete and return the enclosed product registration card to GE Multilin as soon as possible.

In the event there are items missing or damaged, contact the party from whom you purchased the product. If the unit needs to be returned, please use the original shipping container if possible. Refer to *Troubleshooting* on page 4–74, for specific return procedures.

1.2 Ordering

1.2.1 Order Codes

The following table lists the order codes for the Multilink Ethernet Switch (ML3000/ML3100). The fiber optic LC ports are limited to a total of 12.

Table 1–1: ML3000 Order Code Table

ML3000		Slot										Mod	Description
		Gb					100 Mb						
		1	2	3	4	5	6	7	8	9	10		
Base ML3000													ML3000 Chassis with Fixed Power Supplies
Mounting	**F**	|	|	|	|	|	|	|	|	|	|		Front Mounted Ports
	B	|	|	|	|	|	|	|	|	|	|		Rear Mounted Ports
Power Supply	**HX**	|	|	|	|	|	|	|	|	|	|		Single Integrated 90 to 250V AC/DC Power Supply
	HH	|	|	|	|	|	|	|	|	|	|		Dual Integrated 90 to 250V AC/DC Power Supplies
	LX	|	|	|	|	|	|	|	|	|	|		Single Integrated 22 to 60V DC Power Supply
	LL	|	|	|	|	|	|	|	|	|	|		Dual Integrated 22 to 60V DC Power Supplies
	P1	|	|	|	|	|	|	|	|	|	|		Single Integrated 22 to 60V DC Power Supply with PoE Support
	P2	|	|	|	|	|	|	|	|	|	|		Dual Integrated 22 to 60V DC Power Supply with PoE Support
	HL	|	|	|	|	|	|	|	|	|	|		Combination of a 90 to 250V AC/DC and a 22 to 60V DC Power Supply
Modules		**A**	**A**	|	|	|	|	|	|	|	|		2 x 1000 Mbit RJ-45 Fixed Ports
		B	**B**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, mm Fiber, 550m
		C	**C**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, mm Fiber, 2km
		D	**D**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, sm Fiber, 10km
		E	**E**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, sm Fiber, 25km
		F	**F**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, sm Fiber, 40km
		G	**G**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, sm Fiber, 70km
		H	**H**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP ports (no transceivers) empty cage
		J	**J**	|	|	|	|	|	|	|	|		2 x 1000 Mbit RJ-45 fixed ports with 1588 timing
		K	**K**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, multimode Fiber, 550m with 1588 timing
		L	**L**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, multimode Fiber, 2km with 1588 timing
		M	**M**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, singlemode Fiber, 10km with 1588 timing
		N	**N**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, singlemode Fiber, 25km with 1588 timing
		P	**P**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, singlemode Fiber, 40km with 1588 timing
		Q	**Q**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP, LC Connector, singlemode Fiber, 70km with 1588 timing
		R	**R**	|	|	|	|	|	|	|	|		2 x 1000 Mbit SFP ports (no transceivers) empty cage with 1588 timing
		X	**X**	|	|	|	|	|	|	|	|		None
				A	**A**	**A**	**A**	**A**	**A**	**A**	**A**		4 x 10/100Mbit - RJ45 Copper
				B	**B**	**B**	**B**	**B**	**B**	**B**	**B**		4 x 10/100Mbit - RJ45 Copper with PoE*
				C	**C**	**C**	**C**	**C**	**C**	**C**	**C**		4 x 10/100Mbit - RJ45 Copper with PoE+*
				D	**D**	**D**	**D**	**D**	**D**	**D**	**D**		2 x 10Mbit - ST
				E	**E**	**E**	**E**	**E**	**E**	**E**	**E**		2 x 100Mbit - ST mm Fiber
				F	**F**	**F**	**F**	**F**	**F**	**F**	**F**		2 x 100Mbit - SC mm Fiber

Table 1–1: ML3000 Order Code Table

	G G G G G G G G		4 x 100Mbit - LC mm Fiber
	H H H H H H H H		4 x 100Mbit - MTRJ mm Fiber
	J J J J J J J J		2 x 100Mbit - SC sm Fiber 20km
	K K K K K K K K		4 x 100Mbit - LC sm Fiber 20km
	L L L L L L L L		2 x 100Mbit - SC sm Fiber 40km
	M M M M M M M M		4 x 100Mbit - LC sm Fiber 40km
	N N N N N N N N		4 x 100Mbit SFP ports (no transceivers) empty cage
	P P P P P P P P		4 x 10/100Mbit - RJ45 Copper with 1588 timing
	Q Q Q Q Q Q Q Q		2 x 100Mbit - ST mm Fiber with 1588 timing
	R R R R R R R R		2 x 100Mbit - SC mm Fiber with 1588 timing
	S S S S S S S S		4 x 100Mbit - LC mm Fiber with 1588 timing
	T T T T T T T T		4 x 100Mbit - MTRJ mm Fiber with 1588 timing
	U U U U U U U U		4 x 100Mbit - LC sm Fiber 20km with 1588 timing
	W W W W W W W W		2 x 100Mbit - ST sm Fiber 20km with 1588 timing
	Y Y Y Y Y Y Y Y		2 x 100Mbit - SC sm Fiber 20km with 1588 timing
	Z Z Z Z Z Z Z Z		4 x 100Mbit - LC sm Fiber 40km with 1588 timing
	X X X X X X X X		None
Environment		**X**	None
		H	Harsh Chemical Environment Conformal Coating

Table 1–2: ML3001 (Removable Power Supply) Order Code Table

ML3001	Slot										Mod	Description
	Gb		100 Mb									
	1	2	3	4	5	6	7	8	9	10		
Base ML3001												ML3001 Chassis with Removable Power Supplies
Mounting											F	Front Mounted Ports
											B	Rear Mounted Ports
Power Supply											HX	Single Removable 90 to 250V AC/DC Power Supply (Chassis supports optional second 90 to 250V AC/DC supply)
											HH	Dual 90 to 250V AC/DC Removable Power Supplies
											LX	Single Removable 22 to 60V DC Power Supply (Chassis supports optional second 22 to 60V AC/DC supply)
											LL	Dual Removable 22 to 60V DC Power Supplies
											P1	Single Removable 22 to 60V DC Power Supply with PoE Support (Chassis supports optional second 22 to 60V AC/DC supply)
											P2	Dual Removable 44 to 52V DC Power Supply with PoE Support
											HL	Combination of a 90 to 250V AC/DC and a 22 to 60V DC Removable Power Supply
Modules	A	A										2 x 1000 Mbits RJ-45 Fixed Ports
	B	B										2 x 1000 Mbit SFP, LC Connector, mm Fiber, 550m
	C	C										2 x 1000 Mbit SFP, LC Connector, mm Fiber, 2km
	D	D										2 x 1000 Mbit SFP, LC Connector, sm Fiber, 10km
	E	E										2 x 1000 Mbit SFP, LC Connector, sm Fiber, 25km
	F	F										2 x 1000 Mbit SFP, LC Connector, sm Fiber, 40km
	G	G										2 x 1000 Mbit SFP, LC Connector, sm Fiber, 70km
	H	H										2 x 1000 Mbit SFP ports (no transceivers) empty cage
	J	J										2 x 1000 Mbit RJ-45 fixed ports with 1588 timing
	K	K										2 x 1000 Mbit SFP, LC Connector, multimode Fiber, 550m with 1588 timing
	L	L										2 x 1000 Mbit SFP, LC Connector, multimode Fiber, 2km with 1588 timing
	M	M										2 x 1000 Mbit SFP, LC Connector, singlemode Fiber, 10km with 1588 timing
	N	N										2 x 1000 Mbit SFP, LC Connector, singlemode Fiber, 25km with 1588 timing
	P	P										2 x 1000 Mbit SFP, LC Connector, singlemode Fiber, 40km with 1588 timing
	Q	Q										2 x 1000 Mbit SFP, LC Connector, singlemode Fiber, 70km with 1588 timing
	R	R										2 x 1000 Mbit SFP ports (no transceivers) empty cage with 1588 timing
	X	X										None
			A	A	A	A	A	A	A	A		4 x 10/100Mbit - RJ45 Copper
			B	B	B	B	B	B	B	B		4 x 10/100Mbit - RJ45 Copper with PoE*
			C	C	C	C	C	C	C	C		4 x 10/100Mbit - RJ45 Copper with PoE+*
			D	D	D	D	D	D	D	D		2 x 10Mbit - ST
			E	E	E	E	E	E	E	E		2 x 100Mbit - ST mm Fiber
			F	F	F	F	F	F	F	F		2 x 100Mbit - SC mm Fiber
			G	G	G	G	G	G	G	G		4 x 100Mbit - LC mm Fiber
			H	H	H	H	H	H	H	H		4 x 100Mbit - MTRJ mm Fiber
			J	J	J	J	J	J	J	J		2 x 100Mbit - SC sm Fiber 20km
			K	K	K	K	K	K	K	K		4 x 100Mbit - LC sm Fiber 20km

Table 1–2: ML3001 (Removable Power Supply) Order Code Table

	L L L L L L L L		2 x 100Mbit - SC sm Fiber 40km
	M M M M M M M M		4 x 100Mbit - LC sm Fiber 40km
	N N N N N N N N		4 x 100Mbit SFP ports (no transceivers) empty cage
	P P P P P P P P		4 x 10/100Mbit - RJ45 Copper with 1588 timing
	Q Q Q Q Q Q Q Q		2 x 100Mbit - ST mm Fiber with 1588 timing
	R R R R R R R R		2 x 100Mbit - SC mm Fiber with 1588 timing
	S S S S S S S S		4 x 100Mbit - LC mm Fiber with 1588 timing
	T T T T T T T T		4 x 100Mbit - MTRJ mm Fiber with 1588 timing
	U U U U U U U U		4 x 100Mbit - LC sm Fiber 20km with 1588 timing
	W W W W W W W W		2 x 100Mbit - ST sm Fiber 20km with 1588 timing
	Y Y Y Y Y Y Y Y		2 x 100Mbit - SC sm Fiber 20km with 1588 timing
	Z Z Z Z Z Z Z Z		4 x 100Mbit - LC sm Fiber 40km with 1588 timing
	X X X X X X X X		None
Environment		**X**	None
		H	Harsh Chemical Environment Conformal Coating

Table 1–3: ML3100 Order Code Table

ML3100	Slot								Mod	Description
	Gb				100 Mb					
	1	2	3	4	5	6	7	8		
Base ML3100										ML3100 Chassis with Integrated Power Supplies
Mounting	F	|	|	|	|	|	|	|	|		Front Mounted Ports
	B	|	|	|	|	|	|	|	|		Rear Mounted Ports
Power Supply	HX	|	|	|	|	|	|	|	|		Single Integrated 90 to 250V AC/DC Power Supply
	HH	|	|	|	|	|	|	|	|		Dual Integrated 90 to 250V AC/DC Power Supplies
	LX	|	|	|	|	|	|	|	|		Single Integrated 22 to 60V DC Power Supply
	LL	|	|	|	|	|	|	|	|		Dual Integrated 22 to 60V DC Power Supplies
	P1	|	|	|	|	|	|	|	|		Single Integrated 22 to 60V DC Power Supply with PoE Support
	P2	|	|	|	|	|	|	|	|		Dual Integrated 22 to 60V DC Power Supply with PoE Support
	HL	|	|	|	|	|	|	|	|		Combination of a 90 to 250V AC/DC and a 22 to 60V DC Power Supply
Modules	A	A	A	A	|	|	|	|		2 x 1000 RJ-45 or SFP Combo Ports, ports are auto-detect, No SFT Transceivers with 1588 timing
	B	B	B	B	|	|	|	|		2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP mm Fiber, 550m with 1588 timing
	C	C	C	C	|	|	|	|		2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP mm Fiber, 2km with 1588 timing
	D	D	D	D	|	|	|	|		2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP sm Fiber, 10km with 1588 timing
	E	E	E	E	|	|	|	|		2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP sm Fiber, 25km with 1588 timing
	F	F	F	F	|	|	|	|		2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP sm Fiber, 40km with 1588 timing
	G	G	G	G	|	|	|	|		2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP sm Fiber, 70km with 1588 timing
	X	X	X	X	|	|	|	|		None
					A	A	A	A		4 x 10/100Mbit - RJ45 Copper
					C	C	C	C		4 x 10/100Mbit - RJ45 Copper with PoE+*
					D	D	D	D		2 x 10Mbit - ST
					E	E	E	E		2 x 100Mbit - ST mm Fiber
					F	F	F	F		2 x 100Mbit - SC mm Fiber
					G	G	G	G		4 x 100Mbit - LC mm Fiber
					H	H	H	H		4 x 100Mbit - MTRJ mm Fiber
					J	J	J	J		2 x 100Mbit - SC sm Fiber 20km
					K	K	K	K		4 x 100Mbit - LC sm Fiber 20km
					L	L	L	L		2 x 100Mbit - SC sm Fiber 40km
					M	M	M	M		4 x 100Mbit - LC sm Fiber 40km
					N	N	N	N		4 x 100Mbit SFP ports (no transceivers) empty cage
					P	P	P	P		4 x 10/100Mbit - RJ45 Copper with 1588 timing
					Q	Q	Q	Q		2 x 100Mbit - ST mm Fiber with 1588 timing
					R	R	R	R		2 x 100Mbit - SC mm Fiber with 1588 timing
					S	S	S	S		4 x 100Mbit - LC mm Fiber with 1588 timing
					T	T	T	T		4 x 100Mbit - MTRJ mm Fiber with 1588 timing
					U	U	U	U		4 x 100Mbit - LC sm Fiber 20km with 1588 timing
					W	W	W	W		2 x 100Mbit - ST sm Fiber 20km with 1588 timing

Table 1–3: ML3100 Order Code Table

	Y	**Y**	**Y**	**Y**	2 x 100Mbit - SC sm Fiber 20km with 1588 timing
	Z	**Z**	**Z**	**Z**	4 x 100Mbit - LC sm Fiber 40km with 1588 timing
	X	**X**	**X**	**X**	None
Environment				**X**	None
				H	Harsh Chemical Environment Conformal Coating

Table 1–4: ML3101 (Removable Power Supply) Order Code Table

ML3101	Slot								Mod	Description
	Gb				100 Mb					
	1	2	3	4	5	6	7	8		
Base ML3101										ML3101 Chassis with Removable Power Supplies
Mounting									F	Front Mounted Ports
									B	Rear Mounted Ports
Power Supply									HX	Single Removable 90 to 250V AC/DC Power Supply (Chassis supports optional second 90 to 250V AC/DC supply)
									HH	Dual 90 to 250V AC/DC Removable Power Supplies
									LX	Single Removable 22 to 60V DC Power Supply (Chassis supports optional second 22 to 60V DC supply)
									LL	Dual Removable 22 to 60V DC Power Supplies
									P1	Single Removable 22 to 60V DC Power Supply with PoE Support (Chassis supports optional second 22 to 60V DC supply)
									P2	Dual Removable 22 to 60V DC Power Supply with PoE Support
									HL	Combination of a 90 to 250V AC/DC and a 22 to 60V DC Removable Power Supply
Modules	A	A	A	A						2 x 1000 RJ-45 or SFP Combo Ports, ports are auto-detect, No SFP Transceivers with 1588 timing
	B	B	B	B						2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP mm Fiber, 550m with 1588 timing
	C	C	C	C						2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP mm Fiber, 2km with 1588 timing
	D	D	D	D						2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP sm Fiber, 10km with 1588 timing
	E	E	E	E						2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP sm Fiber, 25km with 1588 timing
	F	F	F	F						2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP sm Fiber, 40km with 1588 timing
	G	G	G	G						2 x 1000 RJ-45 or SFP Combo Ports, populated with 2x SFP sm Fiber, 70km with 1588 timing
	X	X	X	X						None
					A	A	A	A		4 x 10/100Mbit - RJ45 Copper
					C	C	C	C		4 x 10/100Mbit - RJ45 Copper with PoE+*
					D	D	D	D		2 x 10Mbit - ST
					E	E	E	E		2 x 100Mbit - ST mm Fiber
					F	F	F	F		2 x 100Mbit - SC mm Fiber
					G	G	G	G		4 x 100Mbit - LC mm Fiber
					H	H	H	H		4 x 100Mbit - MTRJ mm Fiber
					J	J	J	J		2 x 100Mbit - SC sm Fiber 20km
					K	K	K	K		4 x 100Mbit - LC sm Fiber 20km
					L	L	L	L		2 x 100Mbit - SC sm Fiber 40km
					M	M	M	M		4 x 100Mbit - LC sm Fiber 40km
					N	N	N	N		4 x 100Mbit SFP ports (no transceivers) empty cage
					P	P	P	P		4 x 10/100Mbit - RJ45 Copper with 1588 timing
					Q	Q	Q	Q		2 x 100Mbit - ST mm Fiber with 1588 timing
					R	R	R	R		2 x 100Mbit - SC mm Fiber with 1588 timing
					S	S	S	S		4 x 100Mbit - LC mm Fiber with 1588 timing
					T	T	T	T		4 x 100Mbit - MTRJ mm Fiber with 1588 timing
					U	U	U	U		4 x 100Mbit - LC sm Fiber 20km with 1588 timing

Table 1–4: ML3101 (Removable Power Supply) Order Code Table

	W W W W		2 x 100Mbit - ST sm Fiber 20km with 1588 timing
	Y Y Y Y		2 x 100Mbit - SC sm Fiber 20km with 1588 timing
	Z Z Z Z		4 x 100Mbit - LC sm Fiber 40km with 1588 timing
	X X X X		None
Environment		X	None
		H	Harsh Chemical Environment Conformal Coating

Please refer to the GE Grid Solutions website and Online Store for a complete list of modules and options

1.3 Specifications

1.3.1 Technical Specifications

PERFORMANCE

Filtering / Forwarding Rate

Ethernet (10 Mb): ..... 14, 880 pps
Fast Ethernet (100 Mb): ..... 148, 800 pps
Gigabit Ethernet (1000 Mb): .. 1, 488, 000 pps
Switching processing: ..... Store and Forward with IEEE 802.3x full-duplex flow control, non-blocking
Data rate: ..... 10 Mbps, 100 Mbps and 1000 Mbps
Address table capacity: ..... 8 K node, self-learning with address aging
Packet buffer size: ..... 512 KB for 10/100 Mb, 128 KB for Gb
Latency: ..... 6 µs + packet time max. (TX-TX, TX-FX, FX-FX, TX-G, G-G)
System aggregate forward and filter rate:
..... 11.9 Mpps

NETWORK STANDARDS AND COMPLIANCE, HARDWARE

Ethernet V1.0/V2.0 IEEE 802.3:
..... 10Base-T
IEEE 802.3u: 100Base-TX, 100Base-FX
IEEE 802.3z: ..... 1000Base-X Ethernet (Auto-negotiation)
IEEE 802.3ab: ..... 1000Base-X Ethernet
IEEE 802.1p: ..... Priority protocol
IEEE 802.1d: ..... Spanning tree protocol
IEEE 802.1w: ..... Rapid spanning tree protocol
IEEE 802.1q: ..... VLAN tagging
IEEE 802.3x: ..... Flow control
IEEE 802.3ad: ..... Link aggregation (Trunking)
IEEE 802.1x: ..... Port-based network access control
IEEE 802.3af: ..... Power over Ethernet (PoE)
IPv6 Compliance

MAXIMUM 10 MBPS ETHERNET SEGMENT LENGTHS

Unshielded twisted pair ..... 100 m (328 ft)
Shielded twisted pair ..... 150 m (492 ft)
10Base-FL multi-mode fiber optic
..... 2 km (6562 ft)

SNTP

RFC—1769 ..... Simple Network Protocol Server
RFC—2030 ..... Simple Network Protocol Server

MAXIMUM STANDARD FAST ETHERNET SEGMENT LENGTHS

10BASE-T (CAT 3, 4, 5 UTP) .... 100 m (328 ft)
100BASE-TX (CAT 5 UTP)..... 100 m (328 ft)
Shielded twisted pair..... 150 m (492 ft)
100BASE-FX, half-duplex, multi-mode
..... 412 m (1350 ft)
100BASE-FX, full-duplex, multi-mode
..... 2.0 km (6562 ft)
100BASE-FX, half-duplex, single-mode
..... 412 m (1350 ft)
100BASE-FX, full-duplex, single-mode
..... 20.0 km (66K ft)
100BASE-FX, full-duplex, Long Reach
..... 40.0 km (122K ft)

MAXIMUM STANDARD GIGABIT ETHERNET SEGMENT LENGTHS

1000BASE-T (CAT5e or higher is recommended)
..... 100 m (328 ft)
1000BASE-SX, full-duplex, multi-mode (62.5 µm cable)
..... 220 m (722 ft)
1000BASE-SX, full-duplex, multi-mode (50 µm cable)
..... 550 m (1804 ft)
1000BASE-LX, full-duplex, multi-mode (50, 62.5 µm cable)
..... 550 m (1804 ft)
1000BASE-LX, full-duplex, single-mode (9 µm cable)
..... 5 km (16.4 K ft)
1000BASE-ZX, full duplex, single-mode (9 µm cable)
..... >70 km (229.6 K ft)

FIBER MULTI-MODE CONNECTOR TYPES SUPPORTED

Fiber Port, LC-type (plug-in):
..... SFF fiber multi-mode 100BASE-FX
Fiber Port, MTRJ-type (plug-in):
..... SFF fiber multi-mode 100BASE-FX
Fiber Port, SC-type (plug-in), multi-mode 100BASE-FX
Fiber Port, ST-type (twist-lock), multi-mode 100BASE-FX
Fiber Port, 1000BASE-SX, SFP modules

FIBER SINGLE-MODE CONNECTOR TYPES

Fiber Port, LC-type, Fiber SFF single-mode, 100BASE-FX
Fiber Port, SC-type, single-mode, 100BASE-FX
Fiber Port, 1000BASE-LX, SFP modules

LEDS

Per Port ..... All ports have the following LED designations
L/A=Link/Activity ..... ON=link established
OFF=no link established
BLINKING=link activity
F/H=Full duplex/Half duplex (for copper ports)
..... ON=full duplex mode
OFF=half duplex mode, for copper ports

1.3.2 Fixed Power Supply Options

DC POWER SUPPLY (INTERNAL, FLOATING GROUND)

DC Power Connector: ..... Terminal block
(L) 24/48VDC Power Input (range 22 to 60V DC)
(H) AC/DC Power Input (range 90-250V AC or DC)
Standard 3-screw Terminal Block: "-, +, GND"

Note: for PoE applications: ... PoE 802.3af: (L) 48V DC Power Input (range 45 to 57V DC)
PoE+ 802.3at: (L) 48V DC Power Input (range 52 to 56V DC)
Standard 2-screw Terminal Block: "-, +"

AC POWER SUPPLY (INTERNAL)

AC Power Connector: ..... IEC-320/C14 type, male recessed 100-240 VAC Power Input, 47 to 63 Hz (auto-ranging)

1.3.3 Removable Power Supply Options

DC POWER SUPPLY

DC Power Connector: ..... Terminal block
(L) 24/48VDC Power Input (range 22 to 60V DC)
(H) AC/DC Power Input (range 90-250V AC or DC)
Standard 3-screw Terminal Block: "-, +, GND"

Note: for PoE applications: ... PoE 802.3af: (L) 48V DC Power Input (range 45 to 57V DC)
PoE+ 802.3at: (L) 48V DC Power Input (range 52 to 56V DC)
Standard 2-screw Terminal Block: "-, +"

AC POWER SUPPLY

AC Power Connector: ..... IEC-320/C14 type, male recessed 100-240 VAC Power Input, 47 to 63 Hz (auto-ranging)

POWER CONSUMPTION (FIXED AND REMOVABLE MODELS)

55 watts Max. (for a fully-loaded model with 4 Gb ports, sixteen 100 Mb fiber ports and sixteen RJ-45 10/100 Mb ports)

..... 30 watts typical with 32 fully-loaded copper ports
60 watts typical with 32 fully-loaded fiber ports

ALARM RELAY CONTACTS

Max: ..... 220 VDC
0.27 A

Form C, One NC indicating internal power, one NC software controllable

MANAGEMENT CONSOLE

Connector RJ45

1.3.4 Environmental Specifications

OPERATING ENVIRONMENT

Ambient Temperature:..... -40° to 140 °F (-40° to 60 °C) for UL 60950 and Component Parts rating
-40° to 195 °F (-40° to 85 °C) for IEC 60068 Type Test short term rating
Storage Temperature:..... -40° to 185 °F (-40° to 85 °C)
Ambient Relative Humidity:.. 5% to 95% (non-condensing)
Altitude:..... Up to 6560 feet (2000 m)
Pollution Degree: 2
Conformal Coating (humidity protection) optional:
..... Request quote

1.3.5 Physical Specifications

MOUNTING

Normal standard method (horizontal):
..... suitable for or rack mounting, unit supplied with rack-mounting brackets for mounting in a 19" rack

PACKAGING

Enclosure: ..... rugged high-strength sheet metal
Dimensions: ..... 2.63 in H x 17.5 in W x 12.0 in D (6.7 cm H x 44.5 cm W x 30.5 cm D)

COOLING METHOD

Convection, special (patent pending) thermal techniques

WEIGHT

ML3000/ML3100 ethernet switch14.2 lbs. (6.5 kg)

1.3.6 Compliance

TEST	REFERENCE STANDARD	TEST LEVEL
Electrostatic Discharge	EN61000-4-2	Level 4
RF immunity	EN61000-4-3	Level 3
Fast Transient Disturbance	EN61000-4-4	Level 3 & 4
Surge Immunity	EN61000-4-5	Level 4
Conducted RF Immunity	EN61000-4-6	Level 3
Power magnetic Immunity	IEC61000-4-8	Level 3
Voltage Dip & interruption	IEC61000-4-11	0, 40, 70% dips, 250/300cycle interrupts
Ringwave Surge	IEC61000-4-12	Level 3
Radiated & Conducted Emissions	CISPR22	Class A
Radiated & Conducted Emissions	FCC Part 15 Subpart B	Class A
Random Vibration	EN61373	Class A
Shock	EN61373	30g
Safety	EN60950-1	standard
Power Interruption	NEMA TS2 2.1.4 -2.1.4.1	1500 msec, 450 msec interrupts

TEST	REFERENCE STANDARD	TEST LEVEL
Power Transients high repetition	NEMA TS2 2.1.6.1	300V,2500W
Power Transients (low repetition high energy)	NEMA TS2 2.1.6.2	600V, 1 ohm impedance
Transients I/O terminals	NEMA TS2 2.1.7.1	300V, 1000 ohms impedance
Non Destructive transient Immunity	NEMA TS2 2.1.8	1000V, 1 ohm X 3
Operational frequency	NEMA TS2 2.1.3	60Hz +/- 3Hz
RF Immunity	IEEE C37.90.2	20V/m 80-1Ghz /35V/m with modulation
Trapezoid Surge	EN50155	1800 V
Oscillatory Surge	IEC61850-3	Level 4 (4 kV)
Harmonic Current Measurement	EN61000-3-2	+/- 5%
Voltage Fluctuations and Flicker	EN61000-3-3	Standard Limits
Dielectric	IEEE 1613	2KV & 500V
Impulse	IEEE 1613	5KV

1.3.7 Approvals

	APPLICABLE COUNCIL DIRECTIVE	ACCORDING TO
CE Compliance	Low voltage directive	EN60950-1
	EMC Directive	EN61000-6-2, EN61000-6-4
North America	cULus	UL60950-1
		C22.2 No. 60950-1
IEC	EMI and operating conditions class C for power substations	IEC61850-3
FCC/IC/AS/NZS		FCC part 15 subpart B Class A CFR47,part 15 subpart B,Class A ICES-003 Issue 4,2004 CAN/USA-CAI/IEC CISPR22 Class A AS/NZS CISPR 22 CLASS A
IEEE		IEEE1613 environmental standard for Electric Power substations
ISO	Manufactured under a registered quality program	ISO9001

1.4 Firmware Overview

1.4.1 Command Line Firmware

Commands typed by the user will be shown in the following color and font.

```
command
```

The MultiLink Switch Software prompt will be shown in bold and fixed-width text, with a **#** or **>** character at the end. The default prompt is indicated as follows:

ML3000#

The following hold for syntax rules:

- Syntax rules are italicized
- The command part is in bold
- Optional entries are shown in [square brackets]
- Parameter values within are shown in <pointed brackets>
- Optional parameter values are shown again in [square brackets]

Thus, the syntax

command *[parameter1=<value1>[,paramter2=<value2>]] parameter3=<value3|value4>*

indicates the following:

- parameters 1 and 2 are optional
- parameter 2 can be used optionally only if parameter 1 is specified
- parameter 3 is mandatory.

Whenever the word PC is used, it implies a UNIX, Linux, Windows, or any other operating system based workstation, computer, personal computer, laptop, notebook or any other computing device. Most of the manual uses Windows XP based examples. While effort has been made to indicate other operating system interactions, it is best to use a Windows-XP based machine when in doubt.

The documentation reflects features of MultiLink Switch Software version 1.7.x or later. If your switch is not at the current version, GE Multilin recommends upgrade to version 1.7.x or later. Please refer to the GE Multilin website for information on upgrading the MultiLink Switch Software.

1.4.2 EnerVista Software

Icons common to the EnerVista MultiLink Secure Web Management (SWM) firmware for edit, delete, save and refresh are:

-  Edit - edit the values
-  Delete - delete the current row or the value(s)
-  Save - save configuration changes
-  Refresh - repaint the screen

1.4.3 Before Starting

This section explains how to setup the GE MultiLink family of switches using the console port on the switch. Some of the functionality includes setting up the IP address of the switch, securing the switch with a user name and password, setting up VLANs and more.

Before you start, it is recommended to acquire the hardware listed below and be ready with the items listed.

For initial configuration through the serial/console port:

1. A female-female null modem cable.
2. A serial port. If your PC does not have a serial port, you may want to invest in a USB-to-serial converter or USB-to-serial cable.
3. Terminal emulation firmware such as HyperTerminal or other equivalent firmware. Ensure the firmware supports Xmodem protocol, as you may need this in the future to update the MultiLink Switch Software.
4. Enough disk space to store and retrieve the configuration files as well as copy firmware files. We recommend at least 15 MB of disk space for this purpose.
5. For access security - decide on a manager level account name and password
6. IP address, netmask, default gateway for the switch being configured.

As a default, the switch has no IP (Internet Protocol) address and subnet mask. For first time use, the IP address has to be assigned. This can only be done by using the console interface provided.

The same procedure can also be used for other configuration changes or updates (for example, changing the IP address, VLAN assignments and more). Once the IP address is assigned and a PC is networked to the switch, the switch's command line interface (CLI) can be accessed via telnet. To manage the switch through in-band (networked) access (e.g. telnet, or web browser Interface), you should configure the switch with an IP address and subnet mask compatible with your network. Also, change the manager password to control access privileges from the console.

Many other features such as optimizing the switch's performance, traffic engineering and traffic prioritizing, VLAN configuration, and improving network security can be configured through the switch's console interface as well as in-band (networked) access, once the IP address is setup. Besides the IP address, setting up the SNMP parameters allows configuration and monitoring through an SNMP network management station running a network management program.

1.5 Command Line Interface Firmware

1.5.1 Console Connection

The connection to the console is accessed through the DB-9 RJ45connector on the switch marked as the console port. This command line interface (or CLI) provides access to the switch commands. It can be accessed by attaching a PC running terminal emulation firmware to the console port.

USB-to-RJ45 adapters are also available for computers that have access to USB ports.

The interface through the console or the console management interface (or CMI) enables you to reconfigure the switch and to monitor switch status and performance.

NOTICE

Once the switch is configured with an IP address, the command line interface (or CLI) is also accessible using telnet as well as the serial port. Access to the switch can be either through the console interface or remotely over the network. Simultaneous access (that is, through the console port as well as through the network) to the MultiLink switch is not permitted.

The Command Line Interface (CLI) enables local or remote unit installation and maintenance. The MultiLink family of switches provides a set of system commands which allow effective monitoring, configuration and debugging of the devices on the network.

1.5.2 Console Setup

Connect the console port on the switch to the serial port on the computer using the serial cable listed above. The settings for the HyperTerminal firmware are shown below. Make sure the serial parameters are set as shown (or bps = 38400, data bits = 8, parity = none, stop bits = 1, flow control = none).

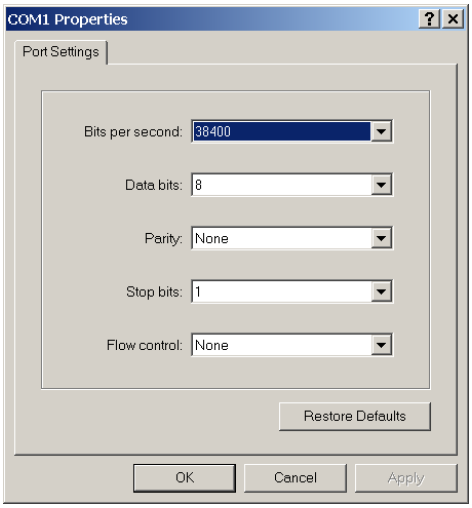


FIGURE 1–1: Serial Settings in HyperTerminal

1.5.3 Console Screen

Once the console cable is connected to the PC and the firmware configured, ML3000 legal disclaimers and other text scrolls by on the screen.

The line interface prompt appears displaying the switch model number (e.g. **ML3000#>**)

The switch has three modes of operation: *operator* (least privilege), *manager*, and *configuration*. The prompts for the switches change as the switch changes modes from operator to manager to configuration. The prompts are shown below with a brief description.

- **ML3000#>**
  Operator Level - for running operations queries
- **ML3000#**
  Manager Level - for setting and reviewing commands
- **ML3000##**
  Configuration Level - for changing the switch parameter values

For additional information on default users, user levels and more, refer to *User Management* on page 1–29.

The default user name and passwords assigned by GE are:

- Username: **manager**
  Password: **manager**
- Username: **operator**
  Password: **operator**

We recommend you login as manager for the first time to set up the IP address as well as change user passwords or create new users.

1.5.4 Automatic IP Address Configuration

The ML3000 is operational immediately after it is powered up. The advanced management and configuration capabilities of the ML3000 allows you to easily configure, manage, and secure your devices and network.

Before starting, ensure you have the following items:

- RJ45 Ethernet cable
- PC with an Ethernet port
- Microsoft Internet Explorer 6.0 or higher
- Macromedia Flash Player 5.0 or higher (available from http://www.macromedia.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash)

Ensure both firmware components are installed before proceeding.

The ML3000 can search the network for commonly used services that can issue an IP address. If the switch is connected to a network, the ML3000 uses the following process to find an IP address.

If the ML3000 is not connected to a network, then proceed to Step 3 below. or use the default IP address.

Step 1:

The ML3000 will scan the network for a DHCP server. If the server responds, the ML3000 will acquire and set the assigned IP address. To manage the switch, determine the assigned IP address and enter as follows in Internet Explorer:

https://<*assigned_IP_address*>

Ensure that **https** is entered, not **http**, and that there is connectivity (that is, you can ping the switch).

Step 2:

If there is no response from a DCHP server, the ML3000 will query for a BOOTP server. If the server responds, the ML3000 will acquire and set the assigned IP address. To manage the switch, determine the assigned IP address and enter as follows in Internet Explorer:

https://*<assigned_IP_address>*

Ensure that **https** is entered, not **http**, and that there is connectivity (that is, you can ping the switch).

Step 3:

If there is no response from either a DCHP or BOOTP server, or if the switch is not connected to a network, the switch will assign itself an IP address. The ML3000 will check to see if IP address **192.168.1.2**, with a network mask of 255.255.255.0, is free. If so, it will assume these values. If this IP address is assigned to another device, the ML3000 will repeat steps 1 through 3 to find a DCHP or BOOTP server or wait for the **192.168.1.2** address to become free.

Once connected, the browser will display a login prompt. The default login is:

- Username: **manager**
  Password: **manager**

1.5.5 Setting the IP Parameters

To setup the switch, the IP address and other relevant TCP/IP parameters have to be specified.

The IP address on the MultiLink switch is set to **192.168.1.2** from the factory. The switch is fully operational as a Layer 2 switch as a default. Setting a default IP address can potentially cause duplicate IP address problem if multiple switches are powered on and installed on the network. To manage the switch, an IP address has to be programmed.

Before starting, please ensure that the IP address assigned to the switch is known or contact your system/network administrator to get the IP address information. Follow the steps listed below to configure the switch.

- ▷ Ensure the power is off.
- ▷ Follow the steps described above for connecting the console cable and setting the console firmware.
- ▷ Power on the switch.
- ▷ Once the login prompt appears, login as manager using default password (manager).
- ▷ Configure the IP address, network mask and default gateway as per the IP addressing scheme for your network.
- ▷ Set the manager password (this step is recommended; refer to the following section).
- ▷ Save the settings (without saving, the changes made will be lost).
- ▷ Power off the switch (or a firmware reboot as discussed below).
- ▷ Power on the switch - login with the new login name and password.
- ▷ From the PC (or from the switch) ping the IP address specified for the switch to ensure connectivity.

▷ From the switch ping the default gateway specified (ensure you are connected to the network to check for connectivity) to ensure network connectivity.

Syntax:

ipconfig *[ip=<ip-address>] [mask=<subnet-mask>] [dgw=<gateway>]*

An example is shown below.

ML3000# `ipconfig ip=3.94.247.41 mask=255.255.252.0 dgw=3.94.247.41`

ML3000# `save`

This manual assumes the reader is familiar with IP addressing schemes as well as how net mask is used and how default gateways and routers are used in a network.

Reboot gives an opportunity to save the configuration prior to shutdown. For a reboot, simply type in the command `reboot`. Note that even though the passwords are not changed, they can be changed later.

ML3000# `reboot`

Proceed on rebooting the switch? ['Y' or 'N'] `Y`

Do you wish to save current configuration? ['Y' or 'N'] `Y`

ML3000#

The ML3000 forces an answer by prompting with a "Y" or a "N" to prevent accidental keystroke errors and loss of work.

The parameters can be viewed at any time by using the `show` command. The show command will be covered in more detail later in various sections throughout the document.

The example below illustrates the basic setup parameters. You can use `show setup` or `show sysconfig` commands to view setup parameters.

ML3000# `show setup`

Version: ML3000 build 1.6.1 Apr 29 2005 11:10:13
MAC Address: 00:20:06:27:0a:e0
IP Address: 3.94.247.41
Subnet Mask: 255.255.252.0
Gateway Address: 3.94.244.1
CLI Mode: Manager
System Name: ML3000
System Description: 25 Port Modular Ethernet Switch
System Contact: multilin.tech@ge.com
System Location: Markham, Ontario
System ObjectId: 1.3.6.1.4.1.13248.12.7

ML3000# `show sysconfig`

System Name: ML3000
System Contact: multilin.tech@ge.com
System Location: Markham, Ontario
Boot Mode: manual
Inactivity Timeout(min): 120
Address Age Interval(min): 300
Inbound Telnet Enabled: Yes
Web Agent Enabled: Yes

Time Zone: GMT-05hours:00minutes
Day Light Time Rule: Canada
System UpTime: 0 Days 0 Hours 45 Mins 55 Secs

ML3000#

Some of the parameters in the MultiLink family of switches are shown above. The list of parameters below indicates some of the key parameters on the switch and the recommendations for changing them (or optionally keeping them the same).

1.5.6 Privilege Levels

Two privilege levels are available - manager and operator. Operator is at privilege level 1 and the manager is at privilege level 2 (the privilege increases with the levels). For example, to set up a user for basic monitoring capabilities use lower number or operator level privilege (level 1).

The Manager level provides all operator level privileges plus the ability to perform system-level actions and configuration commands. To select this level, enter the `enable <user-name>` command at the Operator level prompt and enter the Manager password, when prompted.

enable *<user-name>*

For example, switching from an operator-level to manager-level, using the `enable` command is shown below.

ML3000> `enable manager`

Password: *****

ML3000#

Note the prompt changes with the new privilege level.

Operator privileges allow views of the current configurations but do not allow changes to the configuration. A ">" character delimits the operator-level prompt.

Manager privileges allow configuration changes. The changes can be done at the manager prompt or for global configuration as well as specific configuration. A "#" character delimits any manager prompt.

1.5.7 User Management

A maximum of five users can be added per switch. Users can be added, deleted or changed from a manager level account. There can be more than one manager account, subject to the maximum number of users on the switch being restricted to five.

To add a user, use the `add` command as shown below. The user name has to be a unique name. The password is recommended to be at least 8 characters long with a mix of upper case, lower case, numbers and special characters.

add *user=<name> level=<number>*

The following example adds a user "peter" with manager-level privilege:

ML3000# `user`

ML3000(user)## `add user=peter level=2`

Enter User Password:****

Confirm New Password:****

ML3000(user)##

To delete a user, use the `delete` command as shown below.

delete *user=<name>*

The following example deletes the user “peter”:

ML3000(user)## `delete user=peter`

Confirm User Deletion(Y/N): `Y`

User successfully deleted

ML3000(user)##

The syntax to modify a password is shown below:

passwd *user=<name>*

The following example changes the password for user “peter”.

ML3000(user)## `passwd user=peter`

Enter New Password:****

Confirm New Password :****

Password has been modified successfully

ML3000(user)##

The syntax to modify the privilege level for a specific user is shown below:

chlevel user=<name> level=<number>

The following example modifies the privilege level of user “peter” to Operator privileges.

ML3000(user)## `chlevel user=peter level=1`

Access Permission Modified

ML3000(user)##

The syntax to set the access privileges for telnet and Web services is shown below:

useraccess *user=<name> service=<telnet|web> <enable|disable>*

The following example sets the access privileges for telnet and Web services.

ML3000(user)## `useraccess user=peter service=telnet disable`

Telnet Access Disabled.

1.5.8 Help

Typing the `help` command lists the commands you can execute at the current privilege level. For example, typing `help` at the Operator level shows the following:

ML3000> `help`

logout ping set
terminal telnet walkmib

Contextless Commands:

! ? clear
enable exit help
show whoami
alarm

ML3000>

Help for any command that is available at the current context level can be viewed by typing help followed by enough of the command string to identify the command. The following syntax applies:

help *<command string>*

For example, to list the help for the `set time` command

ML3000# help set time

set time : Sets the device Time

Usage

set time hour=<0-23> min=<0-59> sec=<0-59> [zone=GMT[+/-]hh:mm]

ML3000#

The options for a specific command can be displayed by typing the command and pressing enter. The following syntax applies:

command *<Enter>*

For example, the options for the `show` command are:

ML3000# show <Enter>

Usage

show active-stp
show active-snmp
show active-vlan
show address-table
show age
show alarm
show arp
show auth <config|ports>
show backpressure
show bootmode
--more--

Other ways to display help, specifically, with reference to a command or a set of commands, use the TAB key. The following syntax applies:

<TAB>

<Command string> <TAB>

<First character of the command> <TAB>

For example, following the syntax listed above, the <TAB> key will list the available commands in the particular privilege level:

ML3000> <TAB>

?
alarm
clear
enable
exit
help
logout
ping
set
show
telnet
terminal
walkmib
whoami

ML3000>

The following example lists commands starting with a specific string:

ML3000> s <TAB>

set
show

ML3000>

In the following example, the <TAB> key completes the command:

ML3000> se<TAB>

password
timeout
vlan

ML3000> set

1.5.9 Exiting

To exit from the CLI interface and terminate the console session use the `logout` command. This command prompts to ensure that the logout was not mistakenly typed. The following syntax applies:

logout

The following example illustrates logging out from a session:

ML3000> logout

Logging out from the current session ['Y' or 'N'] Y

Connection to the host lost

1.6 EnerVista Secure Web Management

1.6.1 Logging in for the First Time

Enter the following URL in the web browser to login to the EnerVista Secure Web Management software.

```
https://<IP Address assigned to the switch>
```

NOTE

Make sure you use HTTPS (secure HTTP) and not HTTP in the URL.

In the example shown in the previous section, the URL is:

```
https://3.94.247.41
```

If your site uses name services, you can use a name instead of the IP address. Please make sure that the name is resolved to the IP address assigned to the switch.

The secure site will issue the certificate check shown below.

FIGURE 1–2: Security certificate

Once you click **Yes** on the security certificate, the browser will prompt you to login.

FIGURE 1–3: Login screen

For the first time,

▷ Login with the name **manager** and password **manager**.

▷ Click on **Login**.

After a successful login, the welcome screen is shown. Note the different information provided on the screen and different areas. The menus are used to configure settings on the switch. Users can click on a specific port to open the port configuration view.

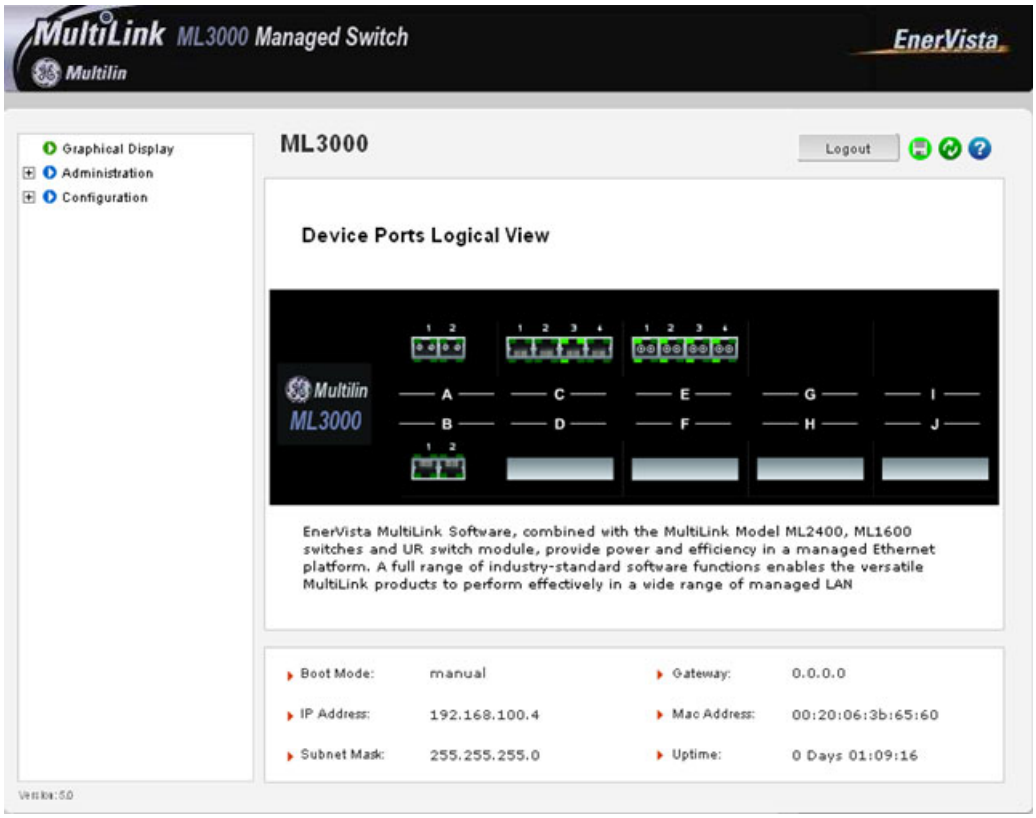


FIGURE 1–4: Welcome screen

1.6.2 Privilege Levels

- **Operator privilege users**: operator privileges allow views of the current configurations but do not allow changes to the configuration.
- **Manager privilege users**: manager privileges allow configuration changes. The changes can be done at the manager prompt or for global configuration as well as specific configuration.

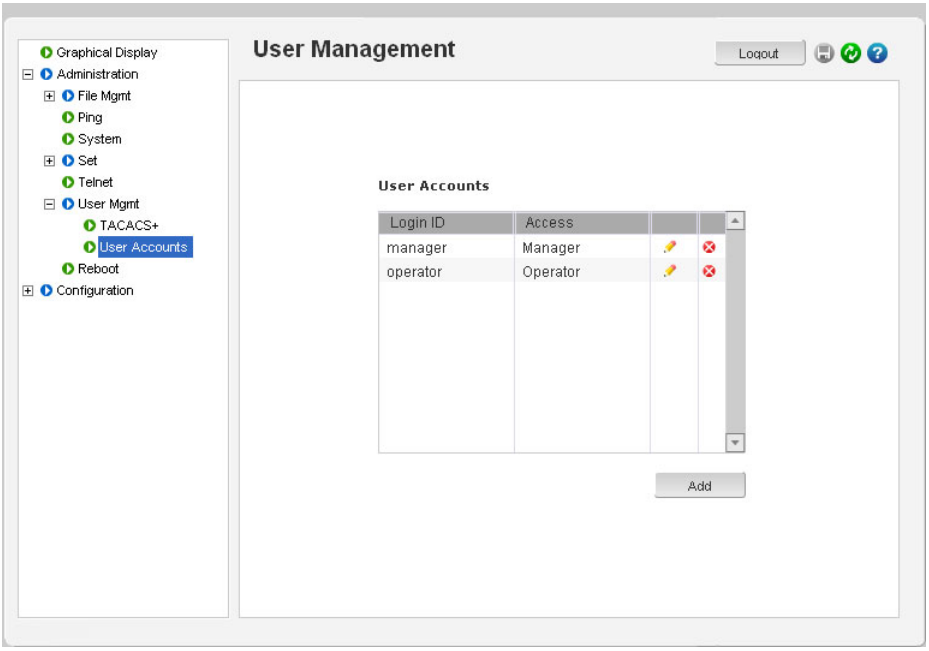
1.6.3 User Management

A maximum of five users can be added per switch. Users can be added, deleted or changed from a manager level account. There can be more than one manager account, subject to the maximum number of users on the switch being restricted to five.

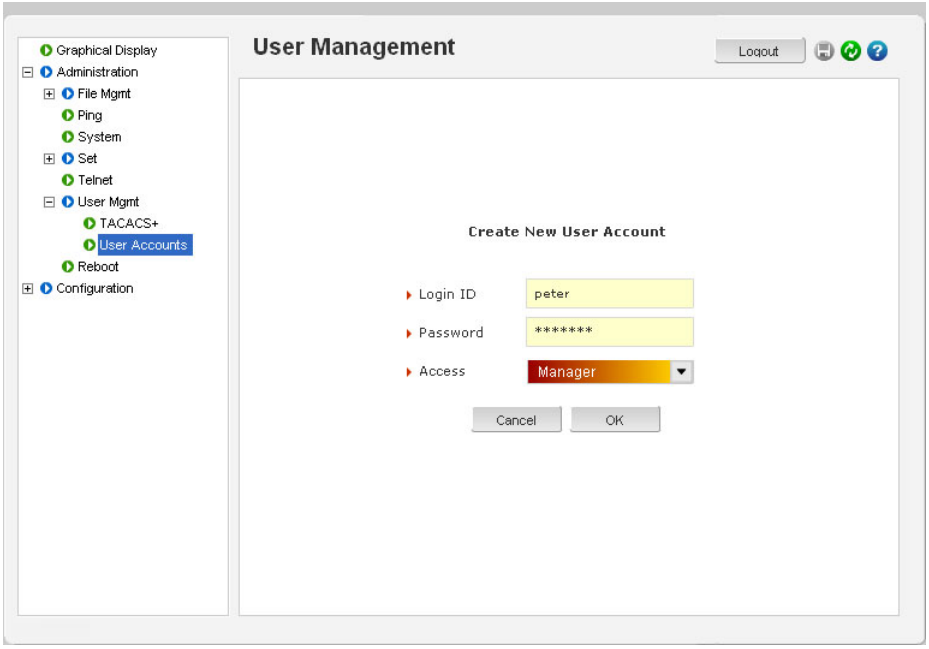
▷ Select the **Administration > User Mgmt > User Accounts** menu item.

▷ To add a user, use the add button.

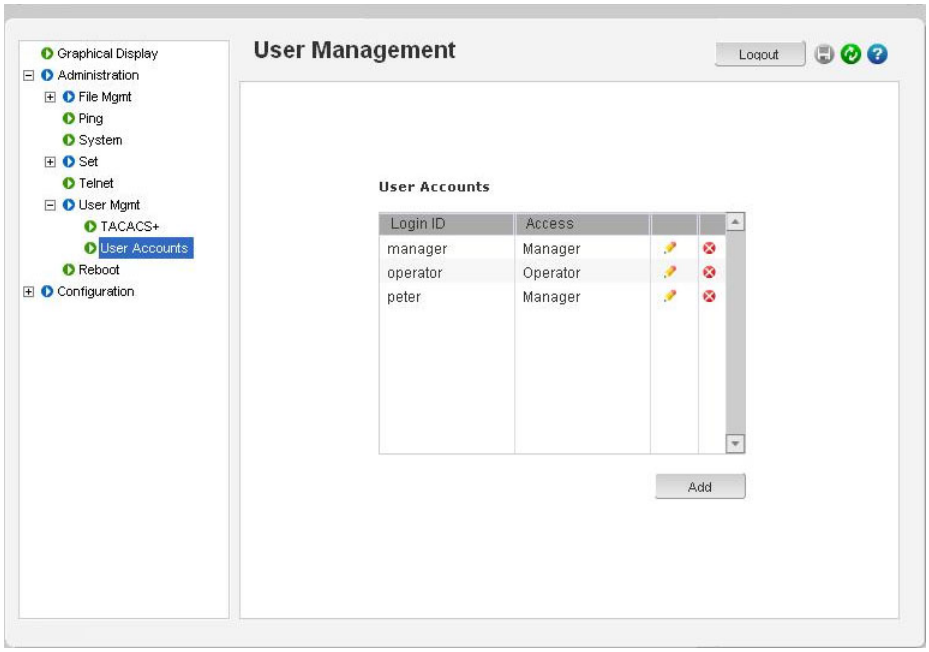
The username must be a unique name. The password is recommended to be at least 8 characters long with a mix of upper case, lower case, numbers and special characters.



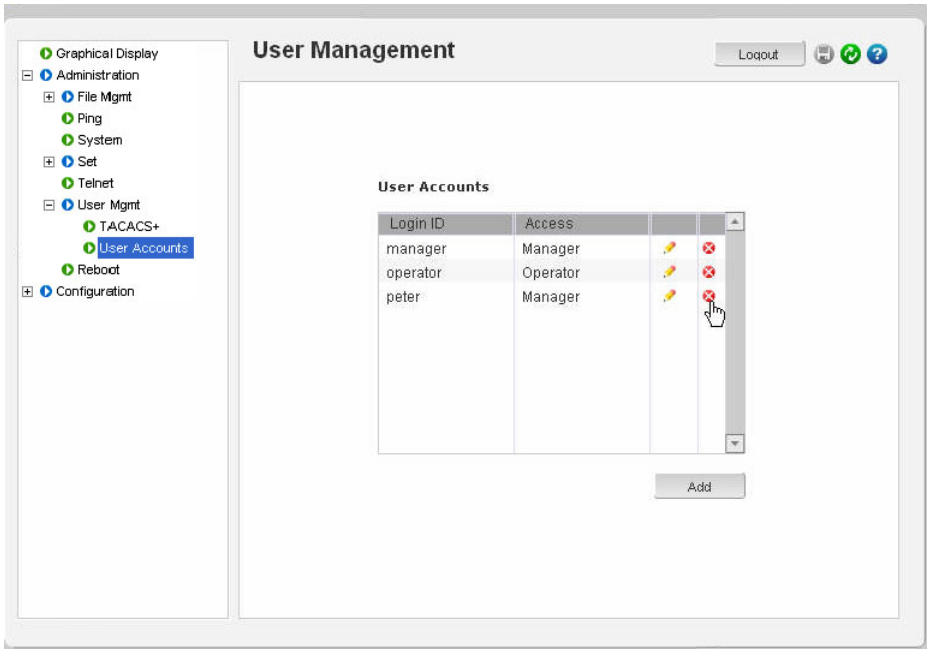
In the following example below, the user **peter** was added with manager privilege after clicking the **add** button.



After successfully adding a user, the added user is displayed in the list of users as shown below.

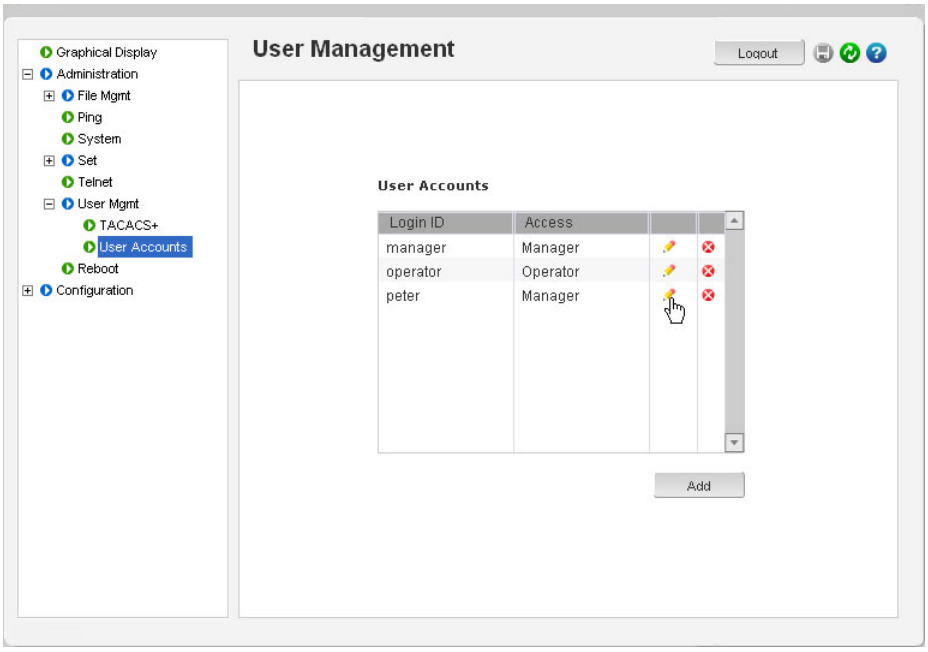


▷ To delete a user, click on the delete icon ( ) as shown below.

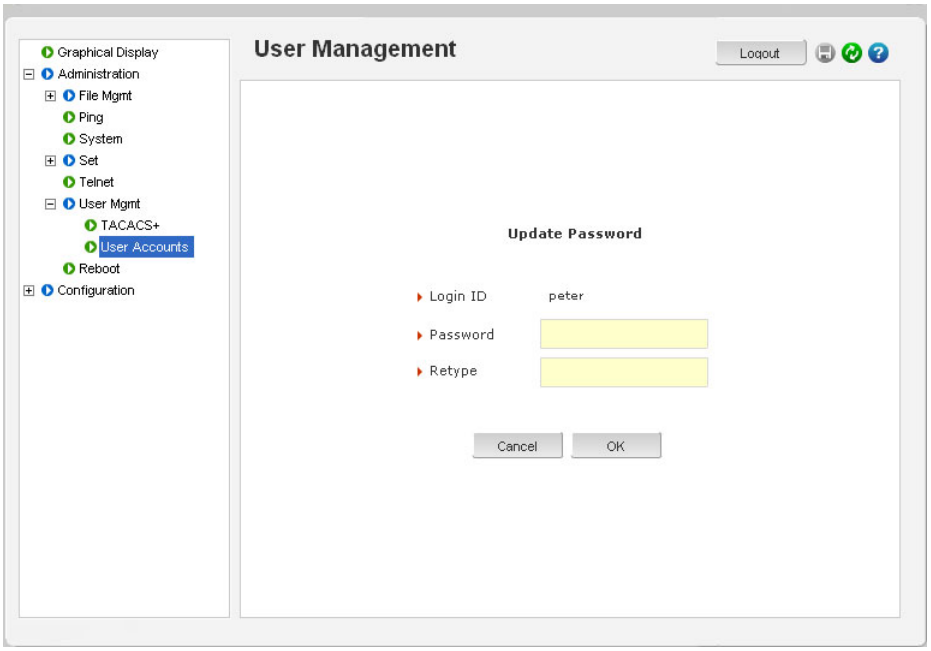


The firmware will prompt to verify the delete command.

▷ To modify the password, view the users as described above and click on the edit icon ( ).



After clicking on the **edit** icon, the screen opens up for modifying the password.



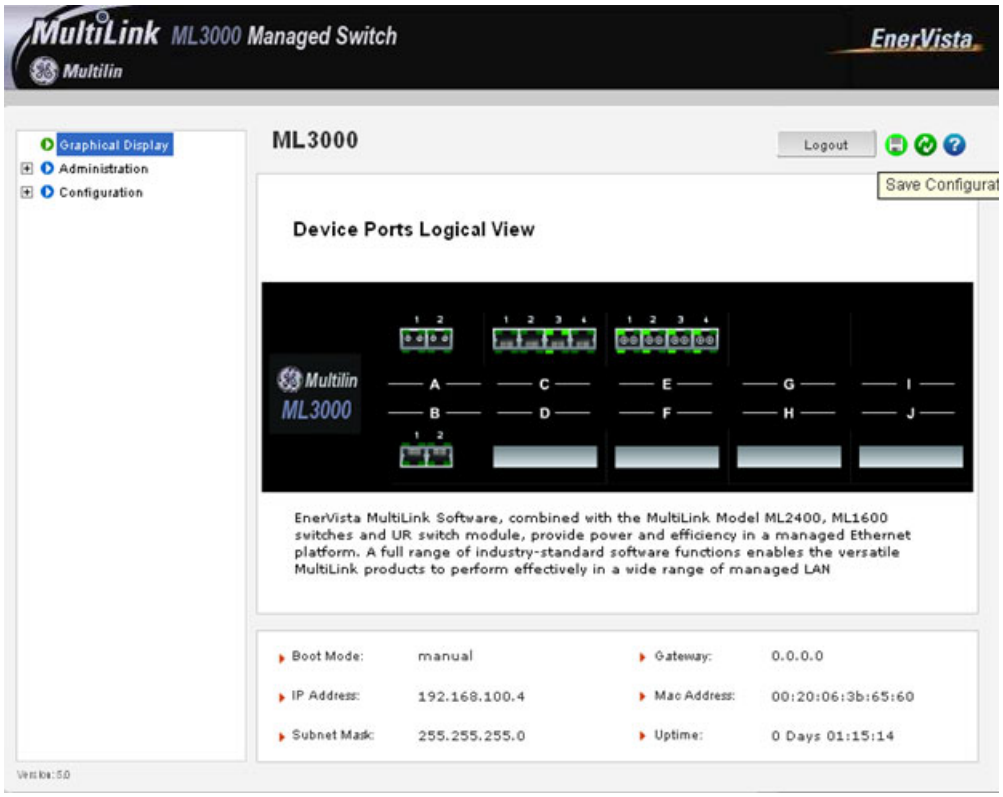
In this example, the user ID **peter** was selected for modification. The password for **peter** will be modified after the new password is entered.

1.6.4 Modifying the Privilege Level

Privilege levels cannot be changed from the EnerVista Secure Web Management (SWM) firmware. This can only be done through the CLI interface, or alternately, by deleting the user and adding the same user with the proper privilege level.

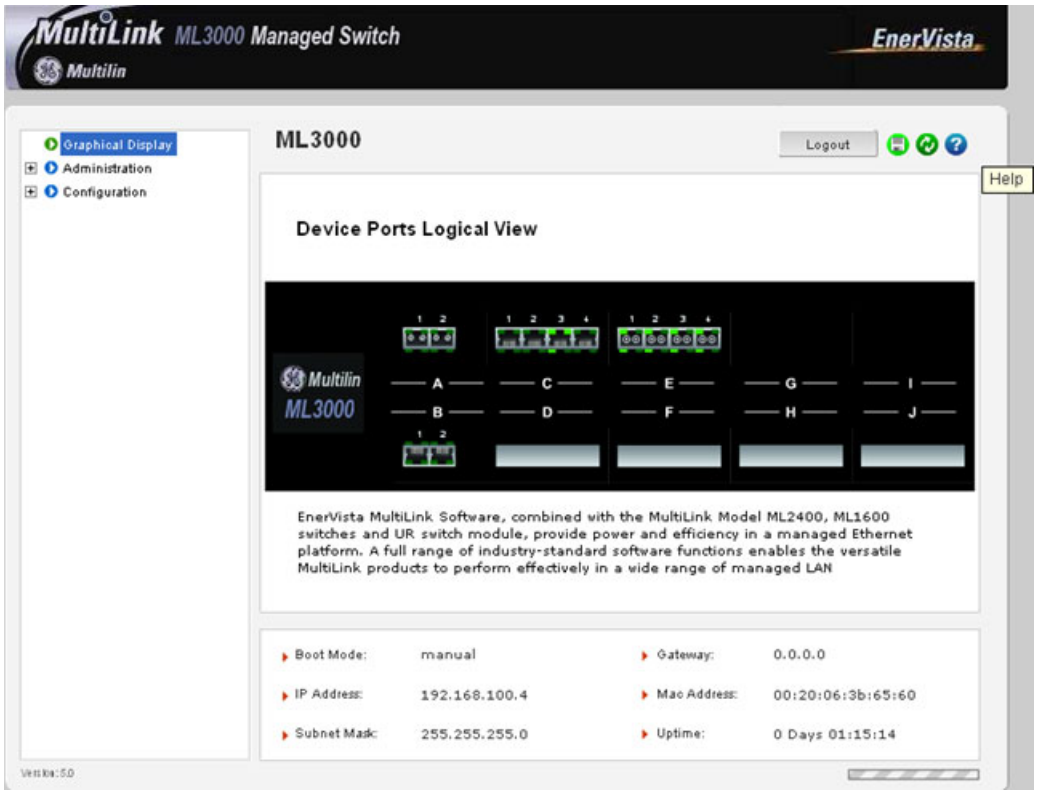
1.6.5 Help

Help for the EnerVista Secure Web Management software can be obtained by clicking on the Help icon as shown below.

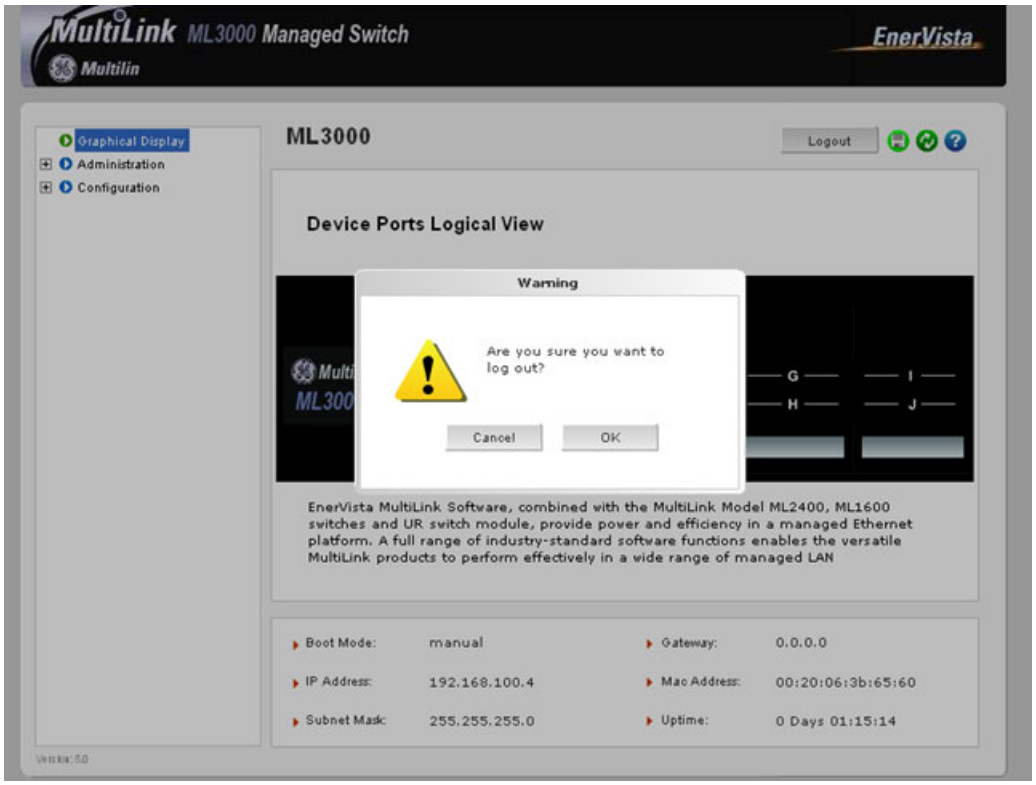


1.6.6 Exiting

▷ To exit or logout, click on the **logout** button.



▷ Confirm the logout by selecting OK in the pop-up window.



1.7 ML3000 Firmware Updates

1.7.1 Updating MultiLink Firmware

This section describes how to upgrade the firmware on a Multilink switch, either locally at the console port or remotely over the network using FTP or TFTP. Depending on the update process (serial/console port or network), ensure the necessary tools listed below are available, tested and working before you begin.

For serial port updates directly through the serial/console port, the following items are required.

1. A female-to-female null modem cable.
2. A USB-to-serial converter or cable if your PC does not have a serial port. A cable is available from GE Multilin.
3. Terminal emulation firmware such as HyperTerminal (included with Windows) or equivalent. Ensure that the firmware supports the Xmodem protocol
4. At least 15 MB of free disk space.
5. Manager level account name and password of the switch being upgraded.
6. An internet connection. Ensure the connection does not block ftp file transfers

1.7.2 Selecting the Proper Version

Ensure that the proper version of the MultiLink Switch Software is installed. The latest version of the firmware is available at http://www.GEmultilin.com.

- ▷ Connect to the ML3000 and login as manager.
- ▷ Enter the `show version` command.
- ▷ Download the latest version of MultiLink firmware from the GE Multilin website.

1.7.3 Updating through the Command Line

Use the following procedure to install firmware to the ML3000 via the serial port.

- ▷ Download the MultiLink Switch Software from the GE Multilin web site.
- ▷ Use the null-modem cable to connect to the ML3000 serial port.
- ▷ Login at the manager level with the proper password.
- ▷ Save the existing configuration (refer to *Saving Configuration* on page 5–94 for details).
- ▷ Enter the following command:

ML3000# `xmodem get type=app`

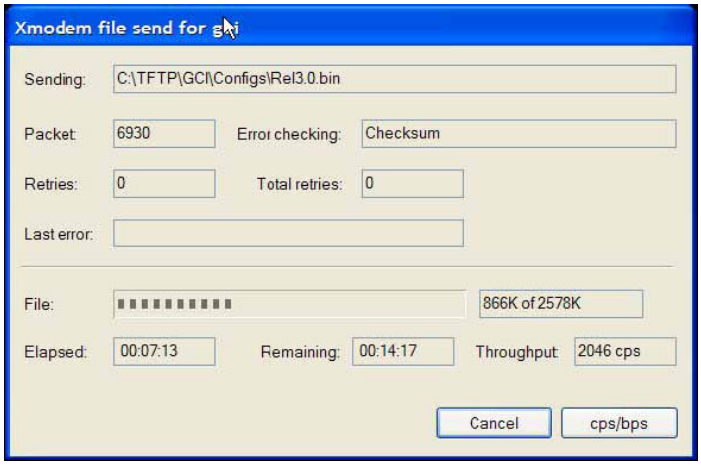
Do you wish to upgrade the image? [Y or N] Y

Please start XModem file transfer now.

Refer to *Saving Configuration* on page 5–94 for details on the `xmodem` command.

Once the upgrade is started, the terminal emulation firmware will ask for the installation file location.

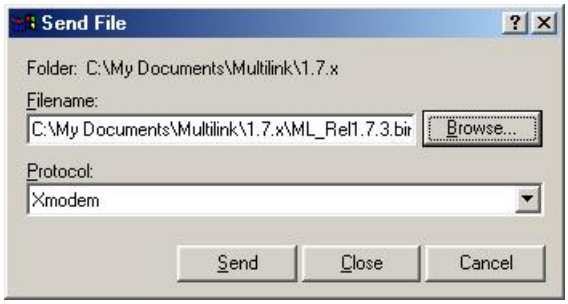
- ▷ Indicate the file location to begin the file transfer.
- ▷ Make sure the Xmodem protocol is also selected in this file location dialog window.



In some operating systems it maybe necessary to select the transfer option.

In this case,

- ▷ Return to the HyperTerminal window used in step 5.
- ▷ Select the **Transfer > Send File** menu item.
- ▷ As shown below, enter the location of the new firmware file.
- ▷ Select the Xmodem protocol.



- ▷ Select the **Send** button and to begin the file transfer.
- ▷ Once the file transfer is completed reboot the switch with the `reboot` command or by cycling power.
- ▷ Login to the switch and use the `show version` command to verify and upload the configuration file (if necessary).

1.7.4 Updating through the enervista Software

Use the following procedure to install the EnerVista Secure Web Management software.

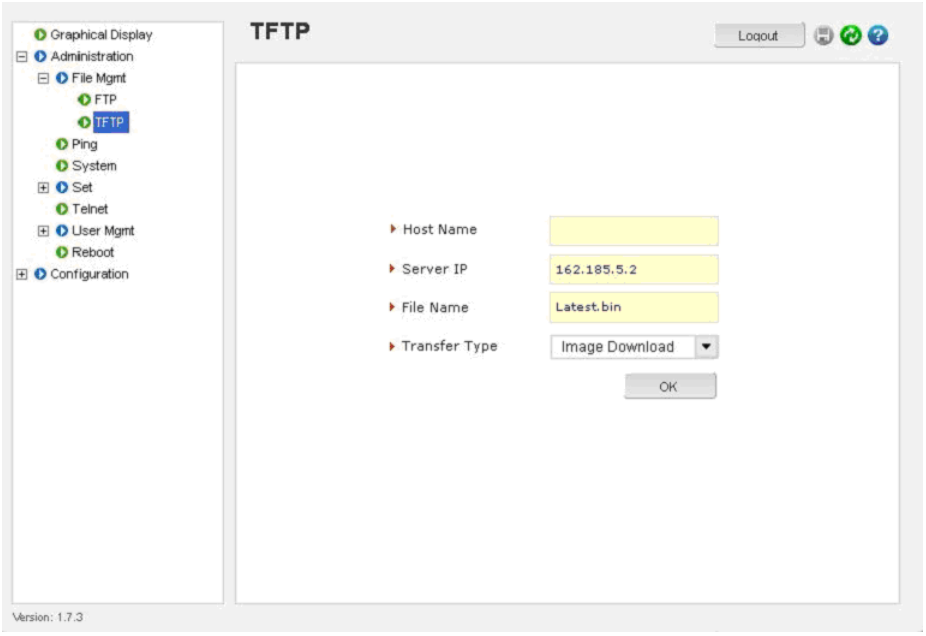
- ▷ Download the latest MultiLink firmware from the GE Multilin web site.

- Save this file on FTP or TFTP. Ensure the FTP or TFTP path is configured. If using FTP, record the FTP login name and password.
- Select the switch to upgrade. Ensure you have system administration privileges available on the switch.
- Open a EnerVista Secure Web Management software session with the switch by typing in the following URL:

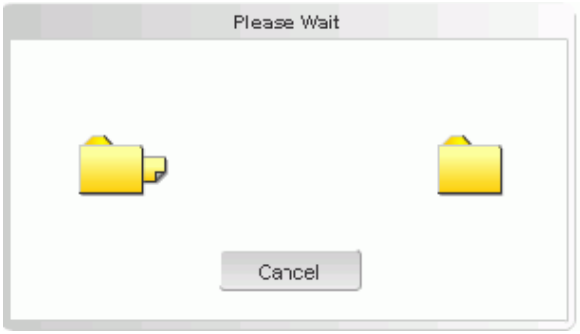
  https://<IP address of the switch>

If using FTP, save the configuration before proceeding. GE Multilin recommends a two-step update: first save the configuration to the ftp server, then load the new image and restart the switch (refer to *Saving Configuration* on page 5–94 for details on saving the configuration).

- Load the new firmware as shown below.



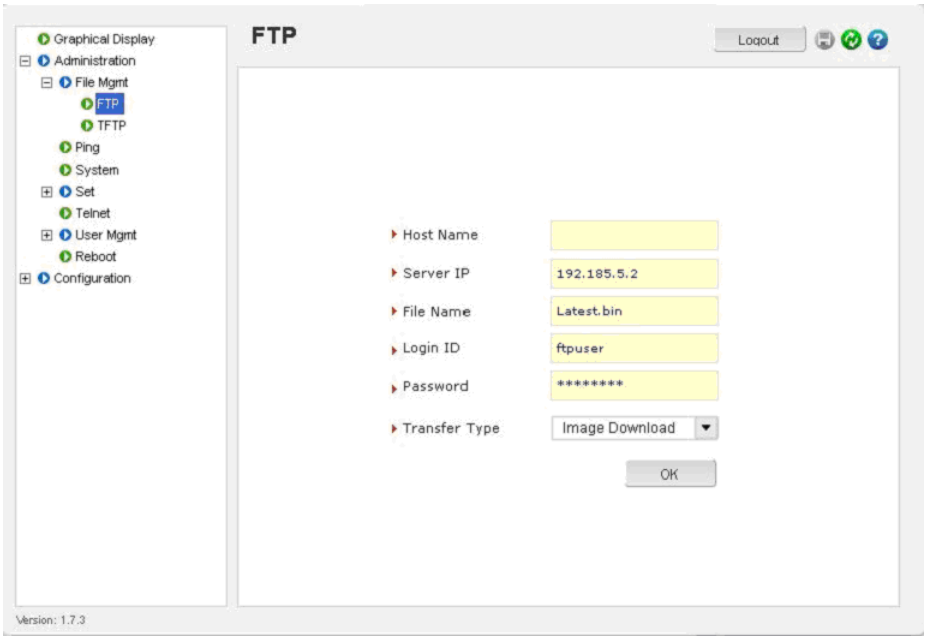
As the file is being loaded, the firmware will display the transfer in progress window.



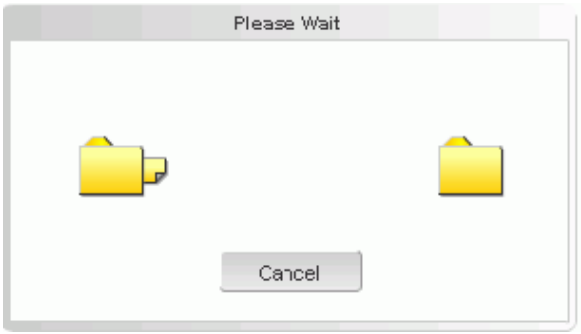
- Reboot the switch when the transfer is complete. After reboot, the firmware is ready for use.
- If using TFTP, save the configuration before proceeding. GE Multilin recommends a two-step update:

- first save the configuration to the TFTP server,
- then load the new image and restart the switch (refer to *Saving Configuration* on page 5–94 for details on saving the configuration).

▷ Load the new firmware as shown below.



As the file is being loaded, the firmware will display the transfer in progress window.



▷ Reboot the switch when the transfer is complete.

After reboot, the firmware is ready for use.

Multilink ML3000/ML3100

Chapter 2: Product Description

2.1 Overview

2.1.1 Introduction to the ML3000 series Ethernet switch family

The Multilink ML3000/ML3100 Ethernet Switch provides rack-mount space efficiency and advanced port configurability for heavy duty industrial applications where maximum fiber port count and diversity are required. New advanced thermal design techniques (patent pending) enable the ML3000/ML3100 to deliver high reliability and configurability even at extended operating temperatures. Special rack-mount cooling features include extra heat dissipation and internal heat transfer techniques that use the case as a heat sink. Cooler operation of internal electronic components leads to longer life-time and increased reliability.

The ten module slots in the ML3000 provide the configuration flexibility for network designers to choose up-to four fiber or copper Gb ports, and up-to thirty-two 100 Mb SFF fiber or copper ports. Copper ports can optionally be Power-Sourcing PoE. Modules may be configured for regular port types: PoE, or combinations.

ML3000/ML3100 Managed Switches come with field-proven Management Software. Management Software features include LAN software support including SNMP management, IPv6, Secure Web Management, IGMP, graphical user interface (GUI), redundant LANs support, and many network management security and ease-of-use features.

ML3000/ML3100 Managed Switches have rugged metal cases for regular or"Reverse" rack-mounting, and auto-ranging power supplies for operation with standard AC power worldwide, or DC power input choices. Moisture and corrosion-protecting Conformal Coating is optional.

The ML3001 Ethernet Switch offers all of the same port configurability and features as ML3000 with a Removable Power Supply Option.

2.1.2 ML3100 series Ethernet switch family

The Multilink ML3100 Ethernet Switch provides rack-mount space efficiency and advanced port configurability for heavy duty industrial applications where maximum fiber port count and diversity are required. New advanced thermal design techniques (patent pending) enable the ML3100 to deliver high reliability and configurability even at extended operating temperatures. Designed with enhanced thermal dissipation this switch offers Cooler operation of internal electronic components leads to longer life-time and increased reliability.

The Next-Generation industrial switch features, especially for power utility facilities in the Smart Grid, importantly include high precision IEEE 1588v2 timing synchronization with precision as low as single-digit nanoseconds.

The ML3100 provides an advanced level of 1588v2 timing features and accuracy, using integrated hardware and software. Advanced timing is supported on 100 Mb and Gb ports, and is configurable on both fiber and copper port types.

The eight port slots in the ML3100 provide configuration flexibility for network designers to choose up-to eight fiber or copper Gb ports, and up-to sixteen 100 Mb SFF fiber or copper ports. Copper ports can optionally be Power-Sourcing PoE. Modules may be configured for regular port types: PoE, IEEE 1588v2 Timing, or combinations.

The ML3000/ML3100 Managed Switches come with field-proven Management Software Management. Software features include LAN software support including SNMP management, IPv6, Secure Web Management, IGMP, graphical user interface (GUI), redundant LANs support, and many network management security and ease-of-use features.

ML3100 Managed Switches have rugged metal cases for regular or “Reverse” rackmounting, and auto-ranging power supplies for operation with standard AC power worldwide, or DC power input choices. Moisture and corrosion-protecting Conformal is optional.

The ML3101 Ethernet Switch offers all of the same port configurability and features as ML3100 with a Removable Power Supply Option.

2.1.3 Design Aspects

Designed for use in network traffic centers, the MultiLink ML3000/ML3100 Ethernet Switch is easy to install and use. Addresses of attached nodes are automatically learned, maintained, and aged out, adapting the switching services to network changes. LEDs provide status information on each port. The ML3000 provides high performance plug-and-play hardware operation, 802.1p packet prioritization in hardware, and industry-standard managed networks software functionality, all in convenient 1 U rack-mount packages.

The ML3000 is a 19" rack-mountable Ethernet switch with 10 slots including slots (1 to 2) as Gb only and slots (3 to 10) may be configured with a selection of fiber and copper 100 Mb ports. These configurable ports allow the ML3000 to efficiently serve a large variety of applications. The ML3000 modules are usually factory installed, but may be changed or added at a later date in the field.

Status LEDs are part of each port module and are viewable when connecting the Ethernet media. The port status data is also accessible through the MultiLink Switch Software.

The ML3100 also has a 19" rack-mountable Ethernet switch with eight slots including slots (1 to 4) as Gb only and slots (5 to 8) may be configured with a selection of fiber and copper 100 Mb ports.

2.2 ML3000/ML3100 Modules

An important feature of the ML3000 is the use of Port Modules for flexible mixed-media connectivity to RJ-45 copper and various fiber media. The first two slots (A & B) of the ML3000 Switch are fixed RJ-45 auto-negotiating copper ports or SFP (Small Form Pluggable) fiber ports with 1000Mbps capability. Additionally, the switch can accept up to eight additional Port Modules in slots 3-10 to provide the user with up to 32 additional ports providing a wide selection of Ethernet copper and fiber media connections with 10 and 100Mbps capability.

NOTE

The ML3000/ML3100 Port Modules are not identical to the port modules used in other Multilink ML2400 switch products. For information about other General Electric products, please see the applicable product manual. For a list of ML3000 Modules, refer to Section 1.2.1: Order Codes.

Each ML3000/ML3100 Port Module is individually described in the following sections.

2.2.1 ML3000 Module LED designations

All ports have the following LED designations:

- L/A = Link / Activity
  - Off (No Link established)
  - ON (Link established)
  - BLINKING (Link Activity)
- F/H = Full Duplex / Half Duplex (for Copper ports)
  - ON (Full Duplex)
  - OFF (Half Duplex) for Copper port

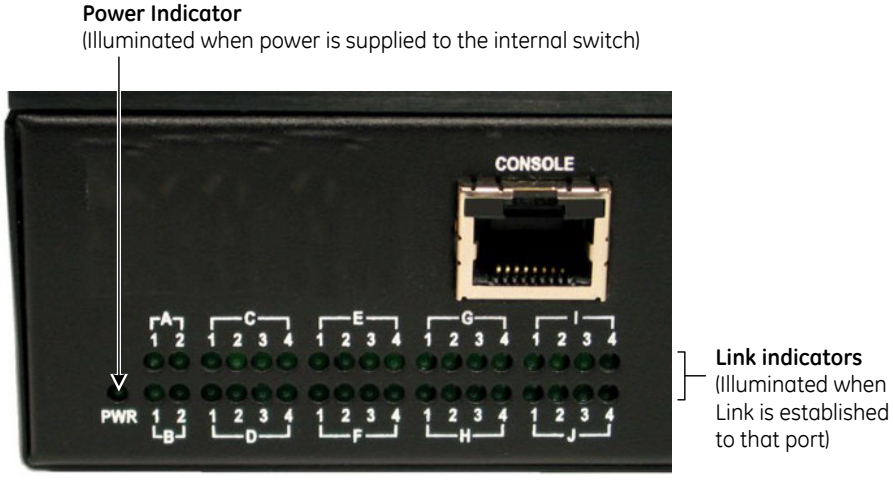


FIGURE 2–1: LED Indicators

2.2.2 Module A (100Mb) - four RJ45 ports (use in Slots 3 to 10 for ML3000 series and slots 5 to 8 for ML3100 series)

The Module A four-port copper module provides four 10/100Mb switched RJ-45 ports. The 10/100Mb switched ports normally (as a default setting) are independently N-way auto-negotiating and auto-crossover (MDIX) for operation at 10 or 100Mb speed in full- or half-duplex mode. (i.e., each independently selects a mode and speed to match the device at the other end of the twisted pair cable).

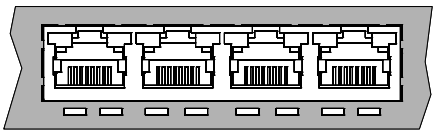


FIGURE 2–2: Module A, 100 Mb - four RJ45 ports

For auto-negotiation and MDIX details, see Section 4.1.6.

There are two LEDs per RJ-45 port on the module; one for Link/Activity and one for F/H Duplex. For the Module A LED designations, see Section 2.2.1: ML3000 Module LED designations.

A twisted pair cable must be connected into an RJ-45 port and the Link (L/A) indicator for that port must be ON (indicating there is a powered-up device at the other end of the cable) in order for the L/A LED to provide valid indications of operating conditions on that port.

Using the Multilink ML3000/ML3100 software, the user may disable auto-negotiation and fix the desired operation of each RJ-45 port. The user may select 10Mb or 100Mb speed and full- or half-duplex mode per-port as required.

NOTE

For Power Substations: In support of the IEEE 1613 Class 2 standard, GCI advises that, for substation applications, the RJ-45 ports are intended for connectivity to other communication equipment such as routers or telecommunication multiplexers installed in close proximity (i.e., less than 2 meters or 6.5 ft) to the 10KT. It is not recommended to use these ports in substation applications to interface to field devices across distances which could produce high (greater than 2500 V) levels of ground potential rise (GPR) during line-to-ground fault conditions. The 10KT passes the 1613 specifications for zero packet loss with fiber ports and with RJ-45 ports used as indicated here.

2.2.3 Module G (100 Mb) - four Multimode LC (use in Slots 3 to 10 for ML3000 series and slots 5 to 8 for ML3100 series)

The Module G four-port fiber module provides four 100Mb Multimode LC Fiber ports.

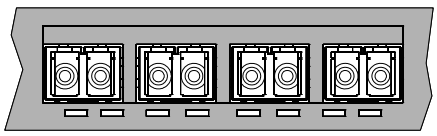


FIGURE 2–3: Module G, 100 Mb - four Multimode LC

The Module G fiber ports are Small Form Factor (SFF) LC Multimode connectors used primarily in 100Mbps fiber-to-IED links in industrial applications. When installed in an ML3000, it supports fiber optic cable distances up to the IEEE-standard 100Mbps distance limits, i.e., typically 2 km at full-duplex and 412 m at half-duplex.

The compact size of the LC Connector reduces the size of wiring panels in wiring closets while providing the advantage of "future-proof" fiber optic technology.

The cable end is a "plug-in" connector with both fiber strands terminated in one housing that cannot be improperly inserted. Each port has a Link/Activity (L/A) LED indicating proper connectivity (Link) with the remote device when lit and blinking (Activity), indicating packets being received.

2.2.4 Module K, Module M (100 Mb) - four Singlemode LC (use in Slots 3 to 10 for ML3000 series and slots 5 to 8 for ML3100 series)

The Module K 4-port Fiber module provides four 100Mb Singlemode LC Fiber ports, supporting distances up to 20km. This module provides the same functions as the Multimode version (see Section 2.2.3 for more details).

The Module M 4-port Fiber module provides four 100Mb Singlemode LC (Long Reach) Fiber ports, supporting distances up to 40km. This module provides the same functions as the Multimode version (see Section 2.2.3 for more details).

2.2.5 Module H (100 Mb) - four Multimode MTRJ (use in Slots 3 to 10 for ML3000 series and slots 5 to 8 for ML3100 series)

The Module H four-port fiber module provides four 100Mb Multimode MTRJ Fiber ports.

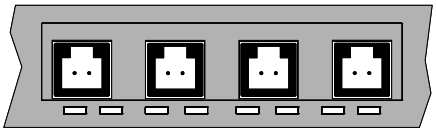


FIGURE 2–4: Module H, 100 Mb - four port fiber module

The Module H fiber port is a Small Form Factor (SFF) MTRJ Multimode connector. The MTRJ's small size and ease of connection make it a good choice for 100Mbps "fiber-to-the-desktop" Ethernet connectivity. When installed in an ML 3000/3100 Switch, it supports fiber optic cable distances up to the IEEE-standard 100Mbps distance limits, i.e., typically 2km at full-duplex and 412m at half-duplex.

The cable end is a "plug-in" connector with both fiber strands terminated in one housing that cannot be improperly inserted. Each port has a Link/Activity (L/A) LED indicating proper connectivity (Link) with the remote device when lit and blinking (Activity), indicating packets being received.

2.2.6 Module F, Module E (100 Mb) – two SC Multimode or two ST Multimode (use in Slots 3 to 10 for ML3000 series and slots 5 to 8 for ML3100 series)

The Module F (shown) two-port fiber module provides two 100Mb Multimode SC Fiber ports. This option utilizes a SC-type "push-pull" fiber optic connection.

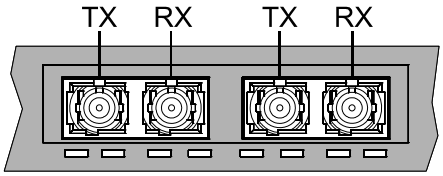


FIGURE 2–5: Module F - Upper Port module (slots 3, 5, 7, 9)

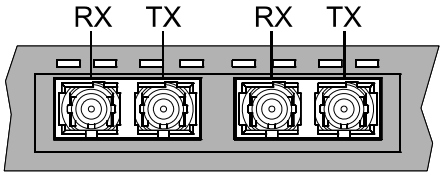


FIGURE 2–6: Module F - Lower Port module (slots 4, 6, 8, 10)

The 10K2-MST two-port fiber module provides two 100Mb Multimode ST Fiber ports. This option utilizes a ST-type "twist-lock" fiber optic connection.

The 100Mb Multimode SC and ST ports typically support fiber optic cable distances up to the IEEE standard 100Mbps distance limits, typically 2km at full-duplex.

Each port has a Link/Activity (L/A) LED indicating proper connectivity (Link) with the remote device when lit and blinking (Activity), indicating packets being received.

2.2.7 Module J, Module L (100 Mb) – two SC Singlemode (use in Slots 3 to 10 for ML3000 series and slots 5 to 8 for ML3100 series)

The Module J two-port fiber module provides two 100Mb Singlemode SC Fiber ports, supporting distances up to 20km. This module provides the same functions as the Multimode version (see Section 2.2.7 for more details).

The Module L two-port Fiber module provides two 100Mb Singlemode SC (Long Reach) Fiber ports, supporting distances up to 40km. This module provides the same functions as the Multimode version (see Section 2.2.7 for more details).

2.2.8 Module N, (100 Mb) - four open 100 Mb SFP Slots (use in Slots 3 to 10 for ML3000 series and slots 5 to 8 for ML3100 series)

The Module N four port module provides four 100 Mb open SFP ports, supporting distances up to 40 km. This module provides the same functions as Module G (see Section 2.2.3 for more details).

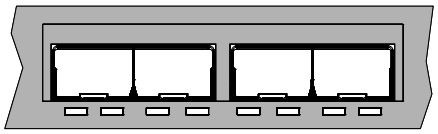


FIGURE 2–7: Module N - four open 100 Mb SFP Slots

SFP Transceivers are available with multimode 850 nm (550 m), 1310 nm (2 km), singlemode 1310 nm (10 km and 25 km) and singlemode 1550 nm (40 km and 70 km) fiber options, as well as RJ45 copper. See Section 1.2.1: Order Codes for available part numbers.

2.2.9 Module A (Gb) - two Gigabit RJ45 (use in Slots 1 and 2 for ML3000 series and Slots 1 to 4 for ML3100 series)

The Module A two-port Copper Gigabit module provides two fixed 10/100/1000 Mb RJ45 ports for configuration in slots 1 and/or 2.

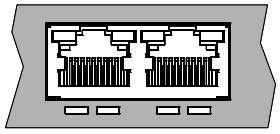


FIGURE 2–8: Module A - two Gigabit RJ45

There are two LEDs provided for each Gigabit port. Each Copper Gigabit port has LEDs that indicate Link/Activity (L/A) and Full/Half Duplex (F/H).

2.2.10 Module H (Gb) - two Gigabit SFPs (use in Slots 1 and 2 for ML3000 series and Slots 1 to 4 for ML3100 series)

The Module H two-port Fiber Gigabit module provides two SFP open transceiver ports in slot 1 and/or 2. SFP Transceivers are available with both multimode 850 nm (550 m), 1310 nm (2km), singlemode 1310 nm (10km and 25 km) and singlemode 1550 nm (40 km and 70 km) fiber options, as well as RJ45 copper. See Section 1.2.1: Order Codes for available part numbers.

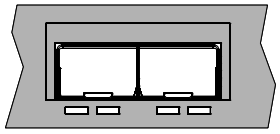


FIGURE 2–9: Module H, Two Gigabit SFPs

The 1000 Mb Gigabit SFP fiber-port modules on the ML3000 are normally set (factory default) to operate at AUTO mode for best fiber distance and performance. Each port has a Link/Activity (L/A) LED indicating proper connectivity (Link) with the remote device when lit and blinking (Activity), indicating packets being received.

2.3 Features and Benefits

2.3.1 Packet Prioritization, 802.1p QoS

Quality of Service (QoS) means providing consistent predictable data delivery to users from datagram paths that go all across a network. As a LAN device, the ML3000 can do its part to prevent any QoS degradation while it is handling Ethernet traffic through its ports and internal switch buffers.

The ML3000 switching hardware supports the IEEE 802.1p standard and fulfills its role in support of QoS, giving packet processing priority to priority tagged packets according to the 802.1p standard. In addition to hardware support for QoS, the ML3000 software supports two priority queues that can be shared across the eight levels of defined packet priorities for application-specific priority control by the user through software configuration settings.

2.3.2 Frame Buffering and Flow Control

The ML3000 is a store-and-forward switch. Each frame (or packet) is loaded into the switch's memory and inspected before forwarding can occur. This technique ensures that all forwarded frames are of a valid length and have the correct CRC, i.e., are good packets. This eliminates the propagation of bad packets, enabling all of the available bandwidth to be used for valid information.

While other switching technologies (such as “cut-through” or “express”) impose minimal frame latency, they will also permit bad frames to propagate out to the Ethernet segments connected. The “cut-through” technique permits collision fragment frames (which are a result of late collisions) to be forwarded which add to the network traffic. Since there is no way to filter frames with a bad CRC (the entire frame must be present in order for CRC to be calculated), the result of indiscriminate cut-through forwarding is greater traffic congestion, especially at peak activity. Since collisions and bad packets are more likely when traffic is heavy, the result of store-and-forward operation is that more bandwidth is available for good packets when the traffic load is greatest.

When the ML3000 detects that its free buffer queue space is low, the switch sends industry standard (full-duplex only) PAUSE packets out to the devices sending packets to cause “flow control”. This tells the sending devices to temporarily stop sending traffic, which allows a traffic catch-up to occur without dropping packets. Then, normal packet buffering and processing resumes. This flow-control sequence occurs in a small fraction of a second and is transparent to an observer.

Another feature implemented in the ML3000 is a collision-based flow-control mechanism (when operating at half-duplex only). When the switch detects that its free buffer queue space is low, the switch prevents more frames from entering by forcing a collision signal on all receiving half-duplex ports in order to stop incoming traffic.

2.3.3 MultiLink Switch Software

The ML3000 includes licensed software, allowing configuration of the ML3000 as a managed switch.

All software information, including new releases and upgrades, can be accessed and download from the GE website at http://www.gegridsolutions.com.

2.3.4 Redundant Power Supply

With the redundant power supply, the ML3000/ML3100 switch can receive power from either power supply 1 (A) or power supply 2 (B). The switch load is shared if both power supplies are available. The unit will not allow power to flow from a one input to another input (i.e. the two power sources are not mixed together by the switch).

When one power supply is present, the ML3000 will receive power even if the other power supply is absent, or if it is connected with reverse polarity, shorted, or grounded.

If reverse polarity connections should accidentally occur on either input, they will not damage the ML3000 or power supply (nor will it blow the fuse in the internal power supply) because of the blocking action of the diodes. This is true even if one input connection is reversed while the Switch is operating from the other source.

The ML3000 will not receive power (and will not work) when both inputs are simultaneously absent.

The status of the power supplies can be queried with the `show power` command.

show power

Power supply 1 on the switch is power input A and power supply 2 on the switch is power input B. For example,

ML3000# show power

Power Input A Good.
Power Input B Good.

The `show power`command is only available in switches with redundant power supplies.

2.3.5 Additional Features and Benefits

- **Managed switching for high performance Ethernet LANs**: ML3000/ML3100 Switches provide non-blocking (all ports can run at full speed at once) performance with standard Managed Network Software.
- **Switching services includes 802.1p QoS packet prioritization**: The ML3000/ML3100 switching hardware supports QoS, giving packet processing priority to priority tagged packets according to the IEEE 802.1p 4-level standard. For port-specific and application-specific priorities of data, including VLANs, the QoS software may be configured by the user.
- **Fiber Port configurability**: ML3000/ML3100 Managed Switches are designed to naturally include fiber ports, and support mixes of multi-mode, single-mode, 10 Mb and 100 Mb and 1000 Mb speed; full-duplex and half-duplex; classic FX Small Form Factor (SFF) and Small Form Pluggable (SFP) connectors for fiber cable.
- **Relay Contacts for monitoring internal power and user-defined software events**: Two Alarm Relay contacts monitor basic operations. One is for hardware, and will signal loss of power internally. The other is software controlled and will signal user-defined software events such as a security violation or a redundancy fault condition.
- **19" Rack-mounting**: The standard rack mounting provides Ethernet ports and status LEDs in front, service connections (power input and management console) in the rear. "Reverse" rack mounting provides status LEDs in front and all cabling connections in the rear. For best reliability and cooling, 1U vertical space above and below is recommended.
- **Heavy-duty design for Industrial Ethernet and extended temperature operation**: Fiber ports take more power than copper ports, but the ML3000/

ML3100 design provides for this with heavy-duty components. The ambient temperature dual-rating is 60°C per UL methods, and 85°C per IEC 60068-2-1 and IEC 60608-2-2 for 16 hours.

- **RSTP-2004 for rings and meshes, fastest fault recovery, interoperability**: RSTP-2004 provides reliable fast recovery from a fault in a redundant LAN, which may include Multilink switches and routers as well as other vendors industry-standard-RSTP products. Redundant topologies may include rings, dual-rings, and complex meshes.
- **S-Ring and Link Loss Learn for economical high availability using ring topology**: S-Ring, combined with the Link-Loss-Learn feature, provides reliable fast recovery of a fault in an economical ring topology, combining unmanaged and managed switches.

2.4 Applications

2.4.1 Description

The Multilink ML3000/ML3100 Ethernet Switch offers high performance, modularity and availability. It provides the flexibility of 100 Mbps fiber, copper, and Gigabit (1000 Mb) ports, with industry-standard LAN management software. The ML3000/ML3100 switches are easily used in a variety of applications including client/server computing, secure VLAN performance upgrades to industrial networks, and streaming traffic for VOIP and audio/video applications. They can also be used in a diversified combination of mixed media in substation automation and transportation systems applications. The performance characteristics of the ML3000/ML3100 switches enable them to inter-connect a series of subnets (one subnet per ML3000/ML3100 switch port) in a LAN traffic center. The subnet connections may be via fiber or twisted pair cabling, Gb or 100 Mbps or 10 Mbps speed, and full-duplex or half-duplex.

The mixed-media modular capability of the ML3000/ML3100 is ideal for upgrading existing Ethernet LAN networks where existing cabling must be accommodated. The fiber-built-in media capability is ideal for integrating future-proof fiber cabling into an industrial network structure.

2.4.2 ML3000/ML3100 Switch for VLAN applications

The Multilin ML3000/ML3100 Ethernet switch supports a VLAN application which provides security and performance in an industrial network center. A secure VLAN-enabled network is simply an administratively-configured broadcast domain. The network administrator determines which ports and nodes are in which broadcast domains by setting membership profiles for each of them. The ML3000/ML3100 VLAN capability can be configured for use in standard Tag-based VLAN networks.

The modularity of the ML3000/ML3100 switch makes it an attractive choice for use in applications with LAN connections to a large organization's multiple site industrial facilities. The different facilities can be easily connected together with the fiber ports supported by the switch.

Future-proof fiber media can easily connect long distance subnets and provide a stable secure network to all applications using VLANs. The SNMP management capability of the ML3000/ML3100 switch helps create a database of all the network subnets to easily manage the network. Secure web-based management is also included, with SSL authentication and encryption to keep out intruders.

2.4.3 ML3000/ML3100 for an Industrial application

The Multilin ML3000/ML3100 provides hardened enclosures, a variety of power supply options, extended temperature ratings all of which qualify this switch for any industrial power utility, surveillance and physical security, traffic control, transportation system, mining, or COTS military application. The Multilink Firmware qualifies this managed switch to operate and perform securely and reliably in mission critical applications. The industry-standard RSTP-2004 software features allow this managed switch to provide a highly available redundant network capability in any ring or mesh topology network.

The option of setting the ports at 10, 100 or 1000 Mb on copper and 100 or 1000 Mb on fiber media provide widespread options to the users to mix and match their legacy and advanced network needs. Different industrial locations can be easily connected together

with the fiber ports supported by the ML3000/ML3100 switch. A main data center in a secure area protected from earthquake or fire hazards can be connected to the Gigabit Copper or Fiber ports.

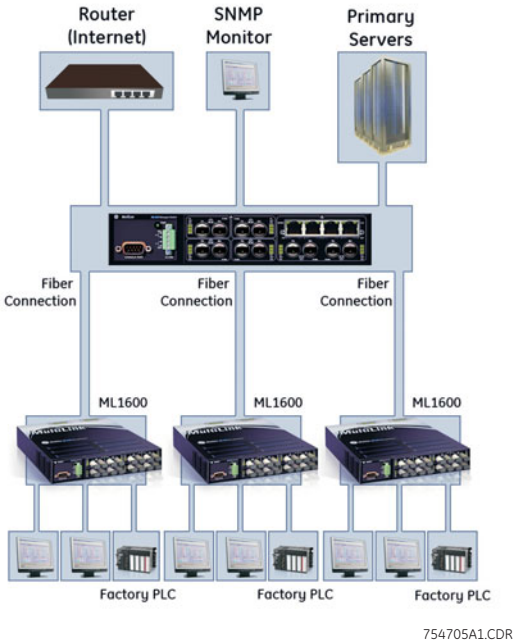


FIGURE 2–10: An industrial network application with ML1600 or ML3000

Extended temperature ratings and a variety of choices for AC/DC power supplies qualify the ML3000/ML3100 switch for use in non-temperature-controlled networks and many other temperature sensitive critical industrial applications where above normal temperatures occur while the network is in operation. The SNMP management capability of the ML3000/ML3100 switch helps create a database of all the network subnets to easily manage the network.

2.4.4 ML3000/ML3100 in a Redundant ring topology

A managed network is needed to provide a redundant ring topology for maximum reliability. In a network where any faulty cable, cable disconnection or power failure could bring down communication to the whole system, a ring topology can be configured to provide continued network operation and recovery from a fault condition. The ring topology of the network may consist of high speed LAN segments supported by 100 Mbps fiber media to provide a secure long distance LAN connection. The entire redundant network may utilize higher bandwidth Gigabit up-links to a central operations center for the vital database located in a separate secured building. The network will be manageable to provide easy, detectable, uninterrupted support through a viewable SNMP monitor.

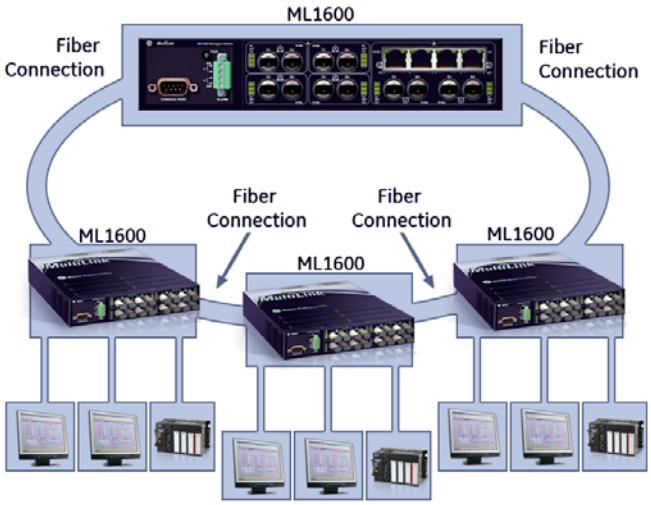


FIGURE 2–11: ML3000 or ML1600 switch with RSTP-2004 in redundant ring application

The ML3000/ML3100 Ethernet Switch with RSTP-2004 fault recovery fulfills the redundancy requirements for reliable industrial networks with fast reconfiguration time (typically 20 to 40 milliseconds) for cable breaks or similar network faults when set up in a ring topology. The Gigabit ports option boosts the bandwidth for high speed to support high traffic loads and minimize congestion.

Multilink ML3000/ML3100

Chapter 3: Installation

3.1 Preparation

3.1.1 Precautions

Before installing the equipment, it is necessary to take the following precautions if the equipment is mounted in an enclosed or multiple rack assembly:

1. Ensure the steady-state long-term environmental temperature around the equipment is less than or equal to 60 °C.
2. Ensure adequate airflow is maintained for proper and safe operation.
3. Ensure placement of the equipment does not overload or unevenly load the rack system.
4. Verify the equipment's power requirements to prevent overloading of the building's electrical circuits.
5. Verify that the equipment has a reliable and uncompromised earthing path.
6. Esnure equipment is to be installed by service personnel in a restricted operation area.

This chapter describes installation of the MultiLink ML3000/ML3100 Ethernet Switch, as well as connection of the various Ethernet media types.

3.1.2 Locating the ML3000

For mounting instructions, refer to *Mechanical Installation* on page 3–64.

The rugged metal case of the ML3000/ML3100 normally protects it from accidental damage in an industrial lab or workplace setting. Maintain an open view of the front to visually monitor the status LEDs. Keep an open area around the unit so that cooling can occur from convection while the unit is in operation. The standard ML3000/ML3100 has no fans (fans are optional), so it is silent when in operation. Internal electronics use the case as a heat sink, so the unit may normally be quite warm to the touch.

When connecting the Ethernet cabling, there is no need to power down the unit. Individual cable segments can be connected or disconnected without concern for power-related problems or damage to the unit.

3.2 Connecting Ethernet Media

3.2.1 Description

The ML3000 switches are specifically designed to support standard Ethernet media types within a single unit. This is accomplished by using a family of modules that are individually selected and configured.

The supported media types with the corresponding IEEE 802.3, 802.3D, 802.3u, 802.3AB and 802.3z standards and connector types are as follows:

Table 3–1: Ethernet media

IEEE standard	Media type	Distance
100Base-FX	multi-mode fiber	220 m
	single-mode fiber	5 km
10Base-T	twisted-pair	100 m
100Base-TX	100Base-FX	100 m

3.2.2 Connecting ST-type Fiber Optics (twist-lock)

The following procedure applies to installations using modules with ST-type fiber connectors. These are type A1, A2, A5, A6, and AF modules.

- ▷ Before connecting the fiber optic cable, remove the protective dust caps from the tips of the connectors on the module.
  Save these dust caps for future use.
- ▷ Wipe clean the ends of the dual connectors with a soft cloth or lint-free lens tissue dampened in alcohol.
  Ensure the connectors are clean before proceeding.

NOTICE

One strand of the duplex fiber optic cable is coded using color bands at regular intervals. The color-coded strand must be used on the associated ports at each end of the fiber optic segment.

- ▷ Connect the transmit (TX) port on the module (light colored post) to the receive (RX) port of the remote device.
  Begin with the color-coded strand of the cable for this first TX-to-RX connection.
- ▷ Connect the receive (RX) port on the module (dark colored post) to the transmit (TX) port of the remote device.
  Use the non-color coded fiber strand.

The LINK LED on the module will illuminate when a connection has been established at both ends (assuming power is ON). If LINK is not lit after cable connection, the cause may be improper cable polarity. Swap the fiber cables at the module connector to remedy this situation.

CAUTION

This product is fitted with Class I lasers.

3.2.3 Connecting SC-type Fiber Optics (snap-in)

The following procedure applies to installations using modules with SC-type fiber connectors. These include the A3, A7, A8, G3, G4, G5, G7, G8, GC, GF, GH, and GJ modules.

When connecting fiber media to SC connectors, simply snap on the two square male connectors into the SC female jacks of the module until it clicks and secures.

3.2.4 Connecting Single-mode Fiber Optics

When using single-mode fiber cable, be sure to use single-mode fiber port connectors. Single-mode fiber cable has a smaller diameter than multi-mode fiber cable (9/125 microns for single-mode versus 50/125 or 62.5/125 microns for multi-mode, where *xx*/*xx* represent the core diameters and the core plus cladding, respectively). Single-mode fiber allows full bandwidth at longer distances and may be used to connect 10 Mb nodes up to 10 km.

The same connection procedures for multi-mode fiber apply to single-mode fiber connectors. Follow the steps listed *Connecting ST-type Fiber Optics (twist-lock)* on page 3–61.

3.2.5 Connecting RJ45 Twisted Pair

The RJ45 ports of the ML3000 can be connected to the following two media types: 100Base-TX and 10Base-T. CAT Five cables should be used when making 100Base-TX connections. When the ports are used as 10Base-T ports, CAT.3 may be used. In either case, the maximum distance for unshielded twisted pair cabling is 100 m (328 ft.).

Use high quality CAT. 5 cables (which work with 10 Mb and 100 Mb) whenever possible to provide flexibility in a mixed-speed network, as dual-speed ports are auto-sensing for 10 and 100 Mb/s.

The following procedure describes how to connect a 10Base-T or 100Base-TX twisted pair segment to the RJ45 port. The procedure is the same for both unshielded and shielded twisted pair cables.

- ▷ Using standard twisted pair media, insert either end of the cable with an RJ45 plug into the RJ45 connector of the port.
  Even though the connector is shielded, either unshielded or shielded cables may be used.
- ▷ Connect the other end of the cable to the corresponding device.
- ▷ Use the LINK LED to ensure connectivity by noting that the LED will be illuminated when the unit is powered and connection is established.

The ML3000 RJ45 Gigabit ports can be connected to 1000Base-T, CAT.5E (or better), 100 Ω UTP, or shielded twisted-pair (STP) balanced cable media. The CAT.5E or shielded twisted pair (STP) balanced cable is recommended when making 1000Base-TX connections. In either case, the maximum distance for unshielded twisted pair cabling is 100 m (328 ft.).

NOTE

Use high quality CAT. 5E cables (which work at both 100 and 1000 Mb) whenever possible to provide flexibility in a mixed-speed network.

The following procedure describes how to connect a 1000Base-T twisted pair segment to the RJ45 port. The procedure is the same for both unshielded and shielded twisted pair cables.

1000 Base-T connections require that all four pairs or wires be connected:

- ▷ Insert either end of the cable with an RJ45 plug into the RJ45 connector on the module.
  Although the connector is shielded, either unshielded or shielded cables may be used.
- ▷ Connect the other end of the cable to the corresponding device.
- ▷ Use the LINK LED to ensure connectivity by noting that the LED will be illuminated when the unit is powered and connection is established.

3.2.6 Connecting Gigabit Media using GBICs

The Gigabit ports accept industry-standard GBICs for user selection of the gigabit media type desired. A selection of fiber and copper GBICs are available.

3.3 Mechanical Installation

3.3.1 Rack Mounting

Installation of a MultiLink ML3000/ML3100 Ethernet Switch in a 19-inch rack is a simple procedure. The units are 1 U (1.75") high. When properly installed, the front-mounted LED status indicators should be in plain view and easy to read. Rack-mount installation requires special 19-inch rack-mounted brackets and screws (included with the ML3000). These brackets attach to the front sides of the switch, which is then typically fastened on to a standard 19" RETMA rack.

The 23" brackets and the ETSI (European metric, approximately 21") brackets are also available (optional) for rack-mounting the ML3000/ML3100 switches. These brackets are popular in the telecommunications industry where they are a standard for Central Office rack-mounting purposes. The 23" and the ETSI brackets are mainly used for larger equipment.

These brackets are rack-mounted in a frame typically accessed in operation from both sides.

The bracket mounting holes in the sides of the Multilink ML3000/ML3100 permits the installation of all three types (19", ETSI, and 23") of available brackets.


NOTE

Please ensure 1U (1.75") gap is provided above each switch in the enclosure for heat dissipation.

The optional 23" brackets and the ETSI (21") brackets each come as a pair in a package, along with the necessary screws for attaching the brackets to the sides of the ML3000/ML3100 switch unit. They must be ordered as separate line items.

3.3.2 Rack-mounting, Reverse mount option

The optional Reverse ML3000/ML3100 model has all of the cabling (ethernet cabling, power cabling and console port cabling) connectors in the rear, and the status LEDs in the front. The status LEDs that are co-incident with the ports are still present, and a second or dual set of LEDs are used for status visibility in the front of the unit, showing the same data.

There are three options of brackets available to mount in the standard 19" frame, 23" frame, or ETSI (21") frame. The 19" brackets are included with each unit; the other two may be purchased as separate options.

The case of the ML3000/ML3100 has mounting holes prepared for each of the mounting arrangements. Users may choose the mounting arrangement most suitable for their installation.


NOTE

Please ensure 1U (1.75") gap is provided above each switch in the enclosure for heat dissipation.

3.4 Electrical Installation

3.4.1 Powering the ML3000 switch series

The standard high voltage (120/125 V AC/DC) or low-voltage (48 V DC) terminal block on the ML3000 is located on the rear of the unit and is equipped with three (3) screw-down lead posts. The power terminals for DC are identified as positive (+), negative (–), and ground (⏚) and for AC, as live L(+), neutral N(–), and ⏚. The chassis or safety ground is the stud located beside the terminal block.

The connection procedure is straightforward. Simply insert DC leads to the ML3000 power terminal positive (+), negative (–), or AC leads to the live L(+), neutral N(–), and ⏚. Please ensure the correct polarity. The ⏚ must be connected to the safety ground, except during dielectric testing. Ensure that each lead is securely tightened.

FIGURE 3–1: Power connection and alarm contacts

NOTICE

Always use a voltmeter to measure the voltage of the incoming power supply and properly determine the positive and negative leads.

⚠CAUTION

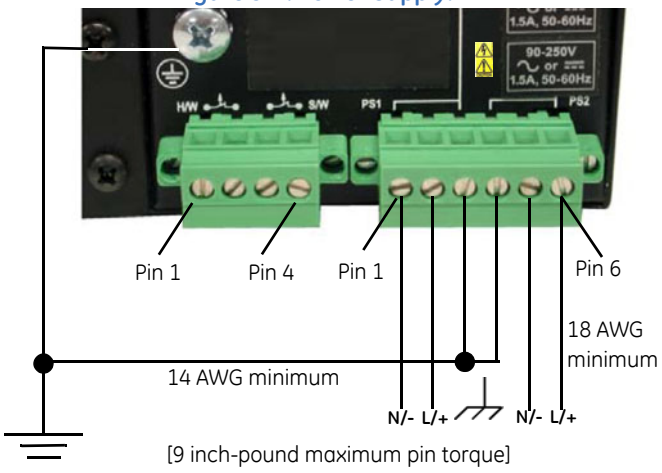
The GND should be connected first. When power is applied, the green PWR LED will illuminate.

The ML3000 is available with a redundant power supply option. If the redundant power supply is ordered, it should be wired as described above. The possible combinations of redundant power supplies are: HI-HI, HI-LO, LO-HI, and LO-LO.

Table 3–2: AC/DC Power Input

PS1 (Power Supply 1)		
Pin #	**Marking**	**Function**
Pin 1:	N/-	(Negative)/Neutral
Pin 2:	L/+	(Positive)/Live
Pin 3:	⏚	Ground
PS2 (Power Supply 2)		
Pin 4:	⏚	Ground
Pin 5:	N/-	(Negative)/Neutral
Pin 6:	L/+	(Positive)/Live

Figure 3-1: Power Supply:



3.4.2 UL/CE Requirements for DC-Powered Units

1. Minimum 18 AWG cable for connection to a centralized DC power source.
2. Minimum 14 AWG cable for connection to a earthing wiring.
3. Use only with listed 10 A circuit breaker provided in building installation, and a 20 A (maximum) branch protection for units rated 90 to 265 V.
4. "Complies with FDA radiation performance standards, 21 CFR sub-chapter J" or equivalent.
5. Fastening torque of the lugs on the terminal block: 9 inch-pound maximum.
6. For AC and HI powered units, use only with listed 20A circuit breaker provided in building installation. Circuit breaker shall be provided in end system or building as disconnect device.
7. Disconnect all power sources before servicing. Take special precautions if servicing a dual power supply unit.
8. Only CE marked external power supplies must be used on the DC-powered unit.
9. Centralized DC power source cable securing; use at least four cable ties to secure the cable to the rack at least 4 inches apart, with the first one located within 6 inches of the terminal block.

3.4.3 Alarm Contacts

The alarm contacts feature, standard on the ML3000/ML3100 ethernet switch, provides two form-C normally closed (NC) contacts to which the user can attach two sets of status monitoring wires at the alarms terminal block, see Fig 3.4.1a above or Fig 3.5a below.

The first NC alarm contact is a "software alarm" (labeled S/W), operated by user settings in the ML3000/ML3100 software. The user can disable the software alarm feature with a software configuration command if desired. When the software alarm is enabled, the form-C normally closed (NC) contact is held close during normal software operation. A user-defined software malfunction, such as an SNMP trap or a software security violation or an RSTP Fault, causes the contact to open and thus trigger an alarm in the user's monitoring system.

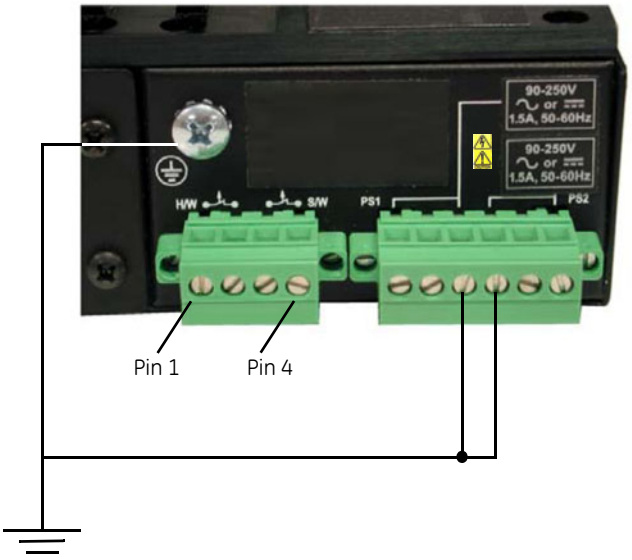
The second NC alarm contact is held closed when there is power on the main board inside of the ML3000/ML3100. This provides a "hardware alarm" (labeled H/W) because the NC contacts will open when internal power is lost, either from an external power down condition or by the failure of the power supply inside of the ML3000/ML3100.

Useful information about the alarm contacts:

1. There is one four-pin terminal block (pins 1,2,3,4) provided next to the power input.
2. The left two pins (1,2) are hardware operated
3. The right two pins (3,4) are software operated
4. These are both NC (normally closed) relays
5. The switch's software operation needs to be enabled and set to get the Alarm traps. For detailed information about the Software Alarm and software control of SNMP alarm traps, please reference the User Manual.

The alarm contacts are located to the left of the power input connection of the ML3000/ ML3100 unit and are green in color as shown in the picture.

Figure 3-2: Alarm Contacts:



Alarm contacts (in : (1,2) are hardware operated, and (3,4) are software operated

3.4.4 Dielectric Strength (hi-pot) Testing

⚠CAUTION

The shorting link between the ⏚ and safety ground must be **removed** prior to the dielectric strength test, as shown below, to protect the transient suppression circuitry of the power supply.

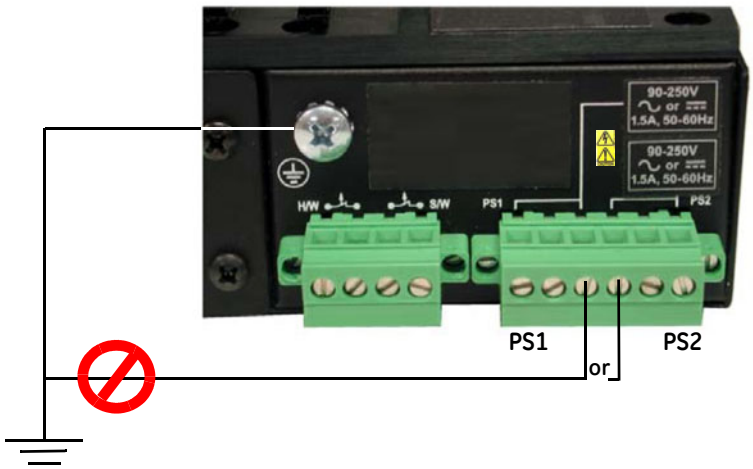


FIGURE 3–2: Dielectric strength testing

Multilink ML3000/ML3100

Chapter 4: Operation

4.1 Functionality

4.1.1 Switching Functionality

The MultiLink ML3000 provides switched connectivity at Ethernet wire-speed. The ML3000 supports10/100 Mbps for copper media and 10 or 100 Mb separate traffic domains for fiber ports to maximize bandwidth utilization and network performance. All ports can communicate to other ports in a ML3000, but local traffic on a port will not consume any of the bandwidth on any other port.

The ML3000 is a plug-and-play device. There is no software configuration necessary for basic operation, installation, or maintenance. Optional half/full-duplex mode and 10 or 100 Mbps selection for the switched ports must be configured through software as per the requirement. The internal functions of both are described below.

4.1.2 Filtering and Forwarding

Each time a packet arrives on one of the switched ports, the decision is taken to either filter or to forward the packet. Packets whose source and destination addresses are on the same port segment will be filtered, constraining them to that one port and relieving the rest of the network from having to process them. A packet whose destination address is on another port segment will be forwarded to the appropriate port, and will not be sent to the other ports where it is not needed. Traffic needed for maintaining the un-interrupted operation of the network (such as occasional multi-cast packets) are forwarded to all ports.

The ML3000 operates in the store-and-forward switching mode, which eliminates bad packets and enables peak performance when there is heavy traffic on the network.

4.1.3 Address Learning

All ML3000 units have address table capacities of 4K node addresses suitable for use in larger networks. They are self-learning, so as nodes are added, removed or moved from one segment to another, the ML3000 automatically keeps up with node locations.

An address-aging algorithm causes least-used addresses to fall out in favor of frequently-used addresses. To reset the address buffer, cycle power down-and-up.

4.1.4 Status LEDs

The following status LEDs are included:

- PWR: Power LED, ON when external power is applied to the unit.
- LK: Steady ON, link status for 10 Mbps and 100 Mbps operation.
- ACT: ON with port activity for 10 Mbps and 100 Mbps operation.
- F/H: Full/half-duplex LED, ON when the port is running full-duplex, OFF for half-duplex.
- 100/10: Speed LED, ON when the speed is 100 Mbps, OFF when the speed is 10 Mbps.

4.1.5 Up-link Manual Switches (for RJ45 port only)

The module has a manual up-link switch, located on the inside of the board next to the 10/100Mb (RJ45) port # 1 which it controls. It enables the port's cable to be cascaded (X) to a 10/100Mb repeater or switching hub in the network. The Up-link Switch position is configured as (=) straight position by default from the factory settings on all the RJ45 ports, either used for all copper module or combo module.

4.1.6 Auto-Cross(MDIX) and Auto-negotiation, for RJ-45 ports

The RJ-45 ports independently support auto-cross (MDI or MDIX) in auto-negotiation mode and will work properly with all the other connected devices with RJ-45 ports whether they support Auto-negotiation (e.g 10Mb Hub, media converter) or fixed mode at 10Mb or 100Mb Half/Full Duplex(managed switch) or not. No cross-over cable is required while using the ML3000's copper port to other devices. Operation is according to the IEEE 802.3u standard.

The Managed ML3000's Fast Ethernet copper ports can be set for either fixed 100Mb speed or for 10/100 F/H N-way auto-negotiation per the IEEE802.3u standard. The selection is made via MNS software. The factory default setting is for auto-negotiation. At 10Mb or 100Mb-fixed speed, the user may select half- or full-duplex mode by MNS Software for each RJ-45 port separately. For detail information See Section 2.3 of this manual for information to access the "6K-MNS Software user guide"

One frequently-used application for the Managed Multilink ML3000 Switch copper ports is to connect one of them using a fiber media converter to another Switch in the network backbone, or to some other remote 100Mb device. In this case, it is desirable to operate the fiber link at 100Mb speed, and at either half- or full duplex mode depending on the capabilities of the remote device. Standard commercially available Fast Ethernet media converters mostly do not support auto-negotiation properly, and require that the switched port to which they are connected be at the 100Mb fixed speed. Attachments to a 10/100 auto-negotiation port typically will not work properly. The ML3000 Switch's RJ-45 ports handle this situation by configuring the ports as per desired through MNS software port settings and can check the port status of each port after the change.

When Multilink ML3000 RJ-45 copper ports are set for auto-negotiation and are connected to another auto-negotiating device, there are 4 different speed and F/H modes possible depending on what the other device supports. These are: (1) 100Mb full-duplex, (2) 100Mb half-duplex, (3) 10 Mb full-duplex and (4) 10 Mb half-duplex.

The auto-negotiation logic will attempt to operate in descending order and will normally arrive at the highest order mode that both devices can support at that time. (Since auto-negotiation is potentially an externally controlled process, the original "highest order mode" result can change at any time depending on network changes that may occur). If the device at the other end is not an auto-negotiating device, the ML3000's RJ-45 ports will try to detect its idle signal to determine 10 or 100 speed, and will default to half-duplex at that speed per the IEEE standard.

General information:

Auto-negotiation per-port for 802.3u-compliant switches occurs when:

- the devices at both ends of the cable are capable of operation at either 10Mb or 100Mb speed and/or in full- or half-duplex mode, and can send/receive auto-negotiation pulses, and...
- the second of the two connected devices is powered up*, i.e., when LINK is established for a port, or...
- the LINK is re-established on a port after being lost temporarily.


NOTE

Some NIC cards only auto-negotiate when the computer system that they are in is powered. These are exceptions to the "negotiate at LINK – enabled" rule above, but may be occasionally encountered.

When operating in 100Mb half-duplex mode, cable distances and hop-counts may be limited within that collision domain. The Path Delay Value (PDV) bit-times must account for all devices and cable lengths within that domain. For Multilink ML3000 Fast Ethernet switched ports operating at 100Mb half-duplex, the bit time delay is 50BT.

4.1.7 Flow Control (IEEE 802.3x)

The ML3000 incorporates a flow-control mechanism for full-duplex mode. Flow-control reduces the risk of data loss if a long burst of activity causes the switch to save frames until its buffer memory is full. This is most likely to occur when data is moving from a 100 Mb port to a 10 Mb port and the 10 Mb port is unable to keep up. It can also occur when multiple 100 Mb ports are attempting to transmit to one 100 Mb port, and in other protracted heavy traffic situations.

The ML3000 implements the 802.3x flow control (non-blocking) on full-duplex ports, which provides for a "PAUSE" packet to be transmitted to the sender when the packet buffer is nearly filled and there is danger of lost packets. The transmitting device is commanded to stop transmitting into the ML3000 port for sufficient time to let the Switch reduce the buffer space used. When the available free-buffer queue increases, the Switch will send a "RESUME" packet to tell the transmitter to start sending the packets. Of course, the transmitting device must also support the 802.3x flow control standard in order to communicate properly during normal operation.


NOTE

In half-duplex mode, the ML3000 implements a back-pressure algorithm on 10/100 Mb ports for flow control. That is, the switch prevents frames from entering the device by forcing a collision indication on the half-duplex ports that are receiving. This temporary "collision" delay allows the available buffer space to improve as the switch catches up with the traffic flow.

4.1.8 Power Budget Calculations with Fiber Media

Receiver sensitivity and transmitter power are the parameters necessary to compute the power budget. To calculate the power budget of different fiber media installations using MultiLink products, the following equations should be used:

$$OPB = P_{t(min)} - P_{R(min)} \quad \textbf{(EQ 4.1)}$$

where: OPB = optical power budget
P_T = transmitter output power
P_R = Receiver Sensitivity

The worst case OPB is as follows:

$$OPB_{worst} = OPB - 1dB\ (LED\ aging) - 1dB\ (insertion\ loss) \quad \textbf{(EQ 4.2)}$$

The worst-case distance is calculated as follows:

$$distance_{worst} = \frac{worst\text{-}case\ OPB\ (in\ dB)}{cable\ loss\ (in\ dB/km)} \quad \textbf{(EQ 4.3)}$$

The cable loss in dB/km is defined in the following table:

Table 4–1: Cable losses

Cable size	Mode	Cable loss
62.5 / 125 µm	multi-mode	2.8 dB/km
50 / 125 µm	multi-mode	2.8 dB/km
100 / 140 µm	multi-mode	3.3 dB/km
9 / 125 µm	single-mode	0.5 dB/km 0.4 dB/km (LXSC25) 0.25 dB/km (LXSC40) 0.2 dB/km (LXSC70)

The following data has been collected to provide guidance to network designers and installers.

Table 4–1: Power budget values for various modules

Fiber Module	Speed, Std.	Mode	Std. km fdx (hdx)	Wave-length nm	Cable Size im	X'mitr Output PT , dBm	R'cvr Sens. PR ,dBm	Worst OPB, dBm	Worst* distance Km, fdx	typical OPB, dBm	typical* distance Km, fdx
D	10 Mb FL	Multi-	2+ (2)	850	62.5/125 100/140 50/125	-15.0 -9.5 -19.5	-31 -31 -31	14 19.5 9.5	5 5.9 3.4	17 23.5 13.5	6 7 4.8
E, F	100 Mb FX	Multi-	2+ (0.4)	1310	62.5/125 50/125	-20 -23.5	-31 -31	9.0 5.5	3.0 2.0	14 12	5 4
W	100 Mb FX	Single-	18+ (0.4)	1310	9/125	-20	-31	9	18	12.5	25
J	100 Mb FX	Single-	18+ (0.4)	1310	9/125	-20	-31	9	18	12.5	25
L	100 Mb FX	Single-	40+	1310	9/125	-5	-34	27	54	32.5	65
H, T	100 Mb FX	Multi-	2+ (0.4)	1310	62.5/125 50/125	-19 -23.5	-31 -31	10 5.5	3.5 2.0	15.8 12.2	5.5 4.0
G, S	100 Mb FX	Multi-	2+ (0.4)	1310	62.5/125	-19	-31	10	3.5	18	6.5
K, U	100 Mb FX	Single-	18+	1310	9/125	-15	-31	14	28	23	46
M, Z	100 Mb FX	Single-	40+	1310	9/125	-5	-34	27	54	32.5	65
B	1000 Mb SX (Gigabit)	Multi-	0.55+ (0.22)	850	62.5/125 50/125	-9.5	-17	5.5	2	10.5	4
C	1000 Mb SX + Extn. Dist.	Multi-	2+	1310	62.5/125 50/125	-9.0	-19	8	2.8	12	4

Table 4–1: Power budget values for various modules

Fiber Module	Speed, Std.	Mode	Std. km fdx (hdx)	Wave-length nm	Cable Size ìm	X'mitr Output PT , dBm	R'cvr Sens. PR ,dBm	Worst OPB, dBm	Worst* distance Km, fdx	typical OPB, dBm	typical* distance Km, fdx
D	1000 Mb LX (Gigabit)	Single-	10+	1310	9/125	-10.0	-22	10	22	11	24
E	1000 Mb LX (Gigabit)	Single-	25+	1310	9/125	-3.0	-21	16	40	18	45
F	1000 Mb ZX (Gigabit)	Single-	40+	1550	9/125	-5.0	-22	15	60	17	68
G	1000 Mb ZX (Gigabit)	Single-	70+	1550	9/125	-2.0	-22	18	90	20	100

The use of either multi-mode or single-mode fiber to operate at 100 Mbps speed over long distances (i.e., in excess of 400 m) can be achieved only if the following are applied:

1. The 100 Mb fiber segment must operate in full-duplex (FDX) mode (i.e. the full-duplex (factory default).
2. The worst-case OPB of the fiber link must be greater than the fiber cable's passive attenuation, where attenuation is the sum of cable loss, LED aging loss, insertion loss, and safety factor.

4.2 Troubleshooting

4.2.1 Overview

All MultiLink Ethernet products are designed to provide reliability and consistently high performance in all network environments. The installation of a ML3000 is a straightforward procedure (see chapter 2 for details)

Should problems develop during installation or operation, this section is intended to help locate, identify and correct these types of problems. Please follow the suggestions listed below prior to contacting your supplier. However, if you are unsure of the procedures described in this section or if the ML3000 is not performing as expected, do not attempt to repair the unit; instead contact your supplier for assistance or contact GE Multilin.

4.2.2 Before Calling for Assistance

1. If difficulty is encountered when installing or operating the unit, refer to chapter 2. Also ensure that the various components of the network are interoperable.
2. Check the cables and connectors to ensure that they have been properly connected and the cables/wires have not been crimped or in some way impaired during installation (about 90% of network downtime can be attributed to wiring and connector problems.)
3. If the problem is isolated to a network device other than the ML3000, it is recommended that the problem device be replaced with a known good device. Verify whether or not the problem is corrected. If not, go to the next step. If the problem is corrected, the ML3000 and its associated cables are functioning properly.
4. If the problem continues after completing the previous step, contact GE Multilin.

4.2.3 When Calling for Assistance

Please be prepared to provide the following information:

1. A complete description of the problem, including the following: the nature and duration of the problem, situations when the problem occurs, the components involved in the problem, and any particular application that appears to create the problem.
2. An accurate list of GE product model(s) involved, with serial number(s). Include the date(s) that you purchased the products from your supplier.
3. It is useful to include other network equipment models and related hardware, including personal computers, workstations, terminals and printers; plus, the various network media types being used.
4. A record of changes that have been made to your network configuration prior to the occurrence of the problem. Any changes to system administration procedures should all be noted in this record.

Multilink ML3000/ML3100

Chapter 5: IP Addressing

5.1 IP Address and System Information

5.1.1 Overview

It is assumed that the user has familiarity with IP addresses, classes of IP addresses and related netmask schemas (for example, class A, B, and C addressing).

Without an IP address, the switch operates as a standalone Layer 2 switch. Without an IP address, you cannot:

- Use the web interface to manage the switch
- Use telnet to access the CLI
- Use any SNMP Network Management software to manage the switch
- Use NTP protocol or an NTP server to synchronize the time on the switch
- Use TFTP or FTP to download the configurations or upload software updates
- Run ping tests to test connectivity

To set the IP address, please refer to *Setting the IP Parameters* on page 1–27. Once the IP address is set, the CLI can be accessed via telnet as well as the console interface. From now on, all commands discussed are accessible from the command line interface, irrespective of access methods (i.e. serial port or in band using telnet).

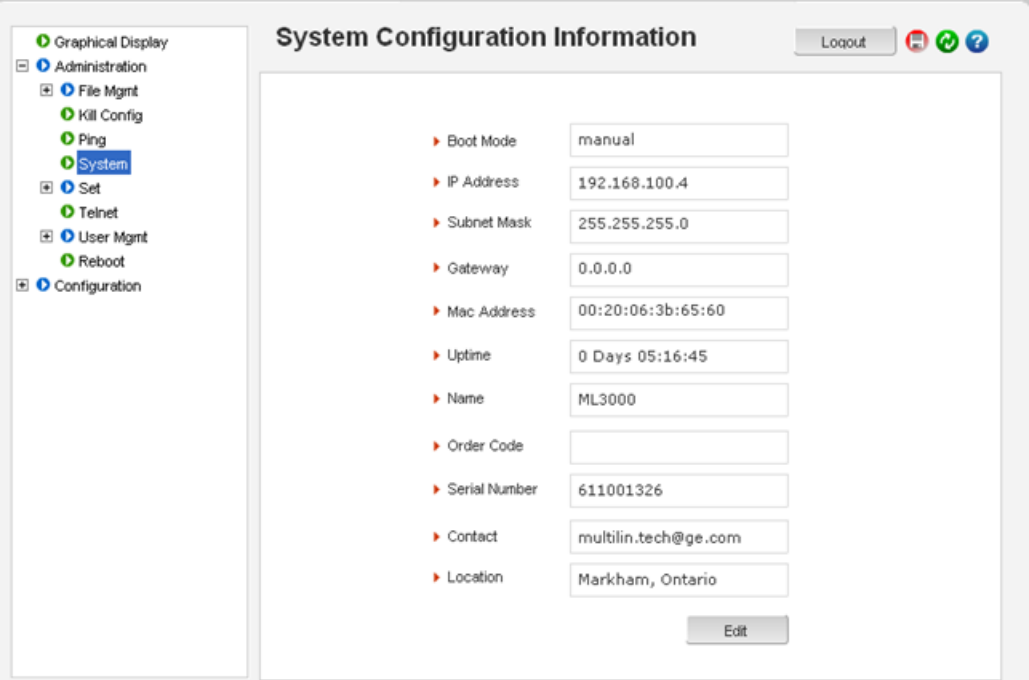
To verify the IP address settings using the command line interface, the `show ipconfig` command can be used as follows:

```
ML3000> show ipconfig

 IP Address:     3.94.247.41
 Subnet Mask:    255.255.252.0
 Default Gateway: 3.94.244.1

ML3000>
```

To verify the IP address using the EnerVista Secure Web Management software,

▷ Select the **Administration > System** menu item to view.

▷ Edit the IP address information.



Besides manually assigning IP addresses, there are other means to assign an IP address automatically. The two most common procedures are using DHCP and bootp.

5.2 Importance of an IP Address

5.2.1 DHCP and bootp

DHCP is commonly used for setting up addresses for computers, users and other user devices on the network. bootp is the older cousin of DHCP and is used for setting up IP addresses of networking devices such as switches, routers, VoIP phones and more. Both of them can work independent of each other. Both of them are widely used in the industry. It's best to check with your network administrator as to what protocol to use and what the related parameters are. DHCP and bootp require respective services on the network. DHCP and bootp can automatically assign an IP address. It is assumed that the reader knows how to setup the necessary bootp parameters (usually specified on Linux/UNIX systems in the `/etc/boopttab` directory).

5.2.2 bootp Database

Bootp keeps a record of systems supported in a database - a simple text file. On most systems, the `bootp` service is not started as a default and has to be enabled. A sample entry by which the `bootp` software will look up the database and update the IP address and subnet mask of the switch would be as follows:

ML3000:
ht=ether:
ha=002006250065:
ip=3.94.247.41:
sm=255.255.252.0:
gw=3.94.244.1:
hn:
vm=rfc1048

where:

- `ML3000` is a user-defined symbolic name for the switch.
- `ht` is the hardware type. For the MultiLink family of switches, set this to `ether` (for Ethernet). **This tag must precede the ha tag**.
- `ha` is the hardware address. Use the switch's 12-digit MAC address.
- `ip` is the IP address to be assigned to the switch.
- `sm` is the subnet mask of the subnet in which the switch is installed.

Each switch should have a unique name and MAC address specified in the `bootptab` table entry

5.2.3 Configuring DHCP/bootp/Manual/AUTO

By default, the switch is configured for auto IP configuration. DHCP/bootp/manual can be enabled with the command line interface by using the `set bootmode` command with the following syntax:

set bootmode=<*dhcp*|*bootp*|*manual*|*auto*> *bootimg*=<*enable*|*disable*> *bootcfg*=<*enable*|*disable*>

The `bootimg` argument is only valid with the `bootp` type. This option allows the switch to load the image file from the bootp server. This is useful when a new switch is placed on a network and the IT policies are set to load a specific image which is supported and tested by IT personnel.

Likewise, the **bootcfg** argument is valid only with the bootp type. This option allows the switch to load the configuration file from the bootp server. This is useful when a new switch is put on a network and the specific configurations are loaded from a centralized bootp server

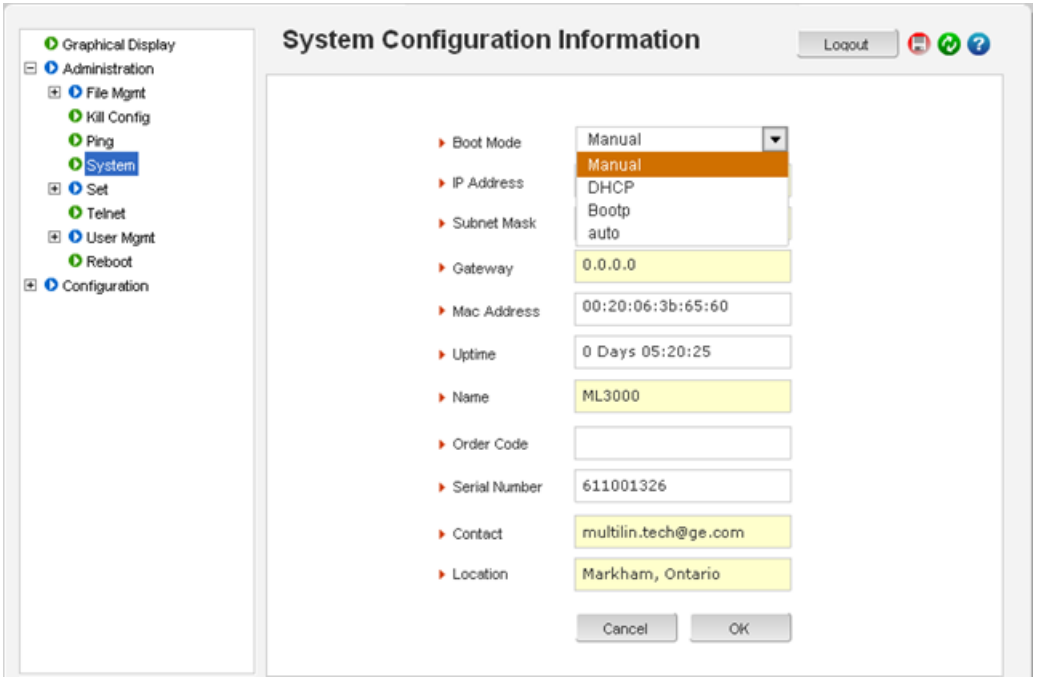
The following example changes the boot mode of the switch:

```
ML3000# set bootmode type=bootp bootimg=enable bootcfg=disable
Network application image download is enabled.
Network application config download is disabled.
Save Configuration and Restart System
ML3000#
```

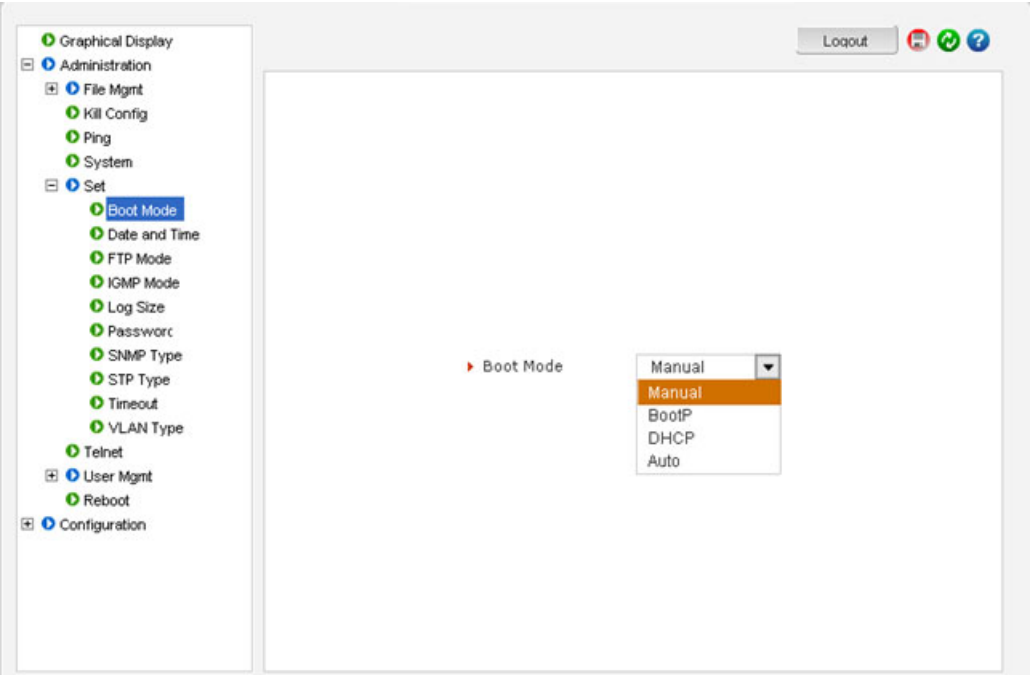
Alternatively, the DHCP/bootp/manual can be enabled through the EnerVista Secure Web Management software as shown below.

▷ Select the **Administration > System** menu item.

▷ Click **Edit**.



▷ Alternatively, select items in the **Administration > Set** menu to individually modify the boot mode, date and time, log size, etc.



▷ After the changes are completed for each section, click **OK** to register the changes.

Note that if the IP address is changed, the **http** session has to be restarted with the new IP address.

5.2.4 Using Telnet

The telnet client is enabled on the ML3000. The ML3000 supports five simultaneous sessions on a switch: four telnet sessions and one console session. This allows many users to view, discuss, or edit changes to the ML3000. This is also useful when two remote users want to view the switch settings. The telnet client can be disabled through the command line interface by using the `telnet disable` command with the following syntax:

telnet *<enable|disable>*

Telnet can also be disabled for specific users with the `useraccess` command. Refer to *Setting the IP Parameters* on page 1–27 for details.

Multiple telnet sessions started from the CLI interface or the command line are serviced by the ML3000 in a round-robin fashion (that is, one session after another). If one telnet session started from an ML3000 is downloading a file, the other windows will not be serviced until the file transfer is completed.

The following example changes the telnet access. In this case, the enable command was repeated without any effect to the switch.

ML3000# `configure access`

ML3000(access)## `telnet enable`

Access to Telnet already enabled

ML3000(access)## `exit`

ML3000#

The `show console` command can show the status of the telnet client as well as other console parameters. The following example reviews the console parameters with the `show console` command. Note that telnet is enabled.

```
ML3000# show console

Console/Serial Link

  Inbound Telnet Enabled: Yes
  Outbound Telnet Enabled: Yes
  Web Console Enabled: Yes
  SNMP Enabled: Yes
  Terminal Type: VT100
  Screen Refresh Interval (sec): 3
  Baud Rate: 38400
  Flow Control: None
  Session Inactivity Time (min): 10

ML3000#
```

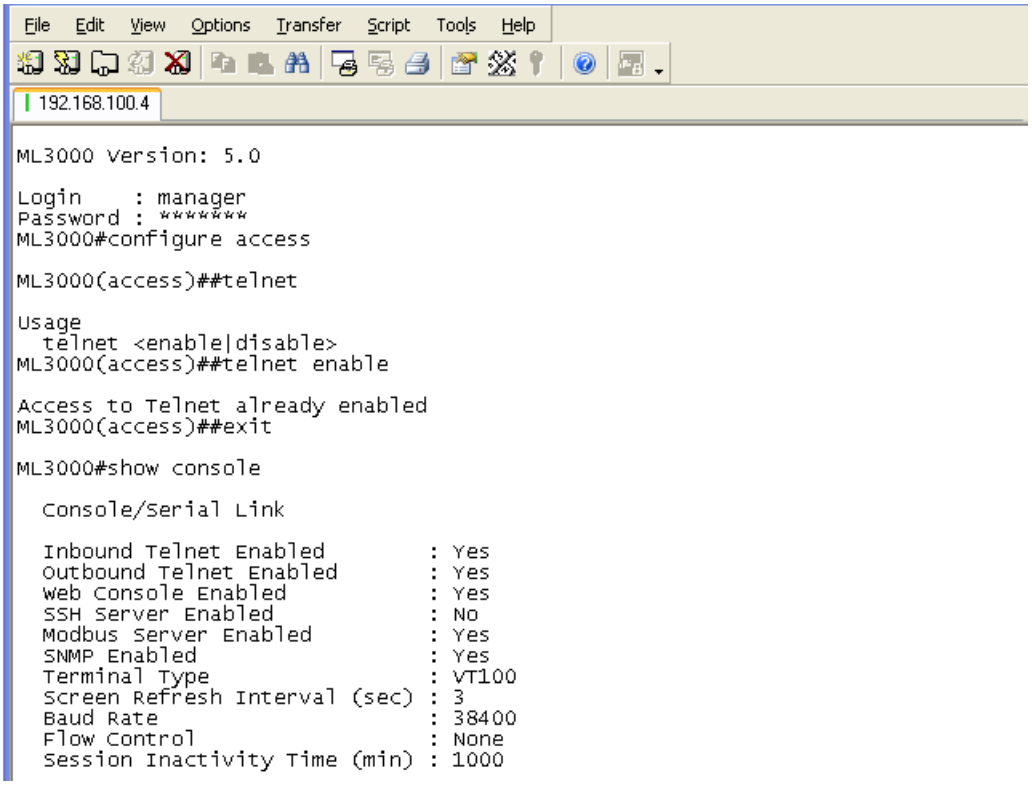
Users can telnet to a remote host from the MultiLink family of switches using the following syntax.

telnet <ipaddress> [port=<port number>]

The default port for telnet is 23.

To start a telnet session through the EnerVista Secure Web Management software,

▷ Select the **Administration > Telnet** menu item.



The default port for telnet is 23.

The ML3000 will time out an idle telnet session. It may be useful to see who is currently connected to the switch. It may also be useful for a person to remotely terminate a telnet session. To facilitate this, the ML3000 supports the following two commands:

show session

kill session *id=<session>*

For example:

```
ML3000# user
ML3000(user)## useraccess user=peter service=telnet enable
Telnet Access Enabled.
ML3000(user)## exit
ML3000# show session
Current Sessions:

SL# Sessn Id  Connection    User Name  User Mode
1   1       163.10.10.14  manager    Manager
2   2       163.11.11.1   peter      Manager
3   3       163.12.12.16  operator   Operator

ML3000# kill session id=3
Session Terminated
ML3000#
```

In the above example, the user with username "peter" is given telnet access. Then multiple users telnet into the switch. This is shown using the `show session` command. The user operator session is then terminated using the `kill session` command.

NOTE

A maximum of four simultaneous telnet sessions are allowed at any time on the switch. The commands in these telnet windows are executed in a round robin fashion; that is, if one window takes a long time to finish a command, the other windows may encounter a delay before the command is completed. For example, if one window is executing a file download, the other windows will not be able to execute the command before the file transfer is completed. As well, if a outbound telnet session is started from the switch (through a telnet window) then other windows will not be able to execute a command until the telnet session is completed.

5.3 Setting Parameters

5.3.1 Setting Serial Port Parameters

To be compliant with IT or other policies the console parameters can be changed from the CLI interface. This is best done by setting the IP address and then telnet over to the switch. Once connected using telnet, the serial parameters can be changed. If you are using the serial port, remember to set the VT-100 emulation software properties to match the new settings.

The serial port parameters are modified using the `set serial` command with the following syntax:

set serial [baud=<rate>] [data=<5|6|7|8>] [parity=<none|odd|even>] [stop=<1|1.5|2>] [flowctrl=<none|xonxoff>]

Where `<rate>` = standard supported baud rates.

NOTICE

Changing these parameters through the serial port will cause loss of connectivity. The terminal software parameters (e.g. HyperTerminal) will also have to be changed to match the new settings.

To see the current settings of the serial port, use the `show serial` command to query the serial port settings as illustrated below.

```
ML3000# show serial

Baud Rate: 38400
Data: 8
Parity: No Parity
Stop: 1
Flow Control: None
```

5.3.2 System Parameters

The system parameters can be queried and changed. To query the system parameters, two commands are frequently used: `show sysconfig` and `show setup`. Usage for both commands is illustrated below.

The following example lists system parameters using the `show setup` command. Most parameters here cannot be changed.

```
ML3000# show setup

Version: ML3000 build 1.6.1 Apr 29 2005 11:10:13
MAC Address: 00:20:06:27:0a:e0
IP Address: 3.94.247.41
Subnet Mask: 255.255.252.0
Gateway Address: 3.94.244.1
CLI Mode: Manager
System Name: ML3000
System Description: 25 Port Modular
  Ethernet Switch
System Contact: multilin.tech@ge.com
System Location: Markham, Ontario
System ObjectId: 1.3.6.1.4.1.13248.12.7

ML3000#
```

The following example lists system parameters using the `show sysconfig` command. Most parameters here can be changed.

```
ML3000# show sysconfig

 System Name: ML3000
 System Contact: multilin.tech@ge.com
 System Location: Markham, Ontario
 Boot Mode: manual
 Inactivity Timeout(min): 120
 Address Age Interval(min): 300
 Inbound Telnet Enabled: Yes
 Web Agent Enabled: Yes
 Time Zone: GMT-05hours:00minutes
 Day Light Time Rule: Canada
 System UpTime: 7 Days 12 Hours 30 Mins 46
  Secs

ML3000#
```

System variables can be changed. Below is a list of system variables which GE recommends changing.

- `System Name`: Using a unique name helps you to identify individual devices in a network.
- `System Contact` and `System Information`: This is helpful for identifying the administrator responsible for the switch and for identifying the locations of individual switches.

To set these variables, change the mode to be SNMP configuration mode from the manager mode using the following syntax

snmp

setvar *[sysname|syscontact|syslocation] =<string>*

The following command sequence sets the system name, system location and system contact information.

```
ML3000# snmp

ML3000(snmp)## setvar ?

 setvar: Configures system name, contact or
  location
 Usage: setvar
  [sysname|syscontact|syslocation]=<string>

ML3000(snmp)## setvar syslocation=Fremont

 System variable(s) set successfully

ML3000(snmp)## exit

ML3000#
```

5.3.3 Date and Time

It may be necessary to set the day, time or the time zone manually. This can be done by using the `set` command with the necessary date and time options with the following syntax:

set *timezone GMT=[+ or -] hour=<0-14>*

min=<0-59>

set *date year=<2001-2035> month=<1-12> day=<1-31> [format=<mmddyyyy|ddmmyyyy|yyyymmdd>]*

set *time hour=<0-23> min=<0-59> sec=<0-59> [zone=GMT[+/-]hh:mm]*

To set the time to be 08:10 am in the -5 hours from GMT (Eastern Standard Time) and to set the date as 11 May 2005, the following sequence of commands are used.

```
ML3000# set time hour=8 min=10 sec=0 zone=GMT-5:00

 Success in setting device time

ML3000# show time

 Time: 8:10:04

ML3000# show timezone

 Timezone: GMT-05hours:00minutes

ML3000# set date year=2005 month=5 day=11

 Success in setting device date

ML3000# show date

 System Date: Wednesday 15-11-2005 (in mm
 -dd-yyyy format)

ML3000#
```

The syntax for other date and time commands are:

set timeformat *format=<12|24>*

set daylight *country=<country name>*

The following command sequence sets the daylight location:

```
ML3000# set daylight country=Canada

 Success in setting daylight savings to the
 given location/country Canada

ML3000# show daylight

 Daylight savings location name: Canada

ML3000#
```

The date and time can only be set through the command line interface software.

5.3.4 Network Time

Many networks synchronize the time using a network time server. The network time server provides time to the different machines using the Simple Network Time Protocol (SNTP). To specify the SNTP server, one has to

1. Set the IP parameters on the switch
2. Define the SNTP parameters

To set the SNTP parameter with the command line software, enter the SNTP configuration mode from the manager. The `setsntp`, `sync`, and `sntp` commands can then be used to setup the time synchronization automatically from the SNTP server. Note it is not sufficient to setup the SNTP variables. Make sure to setup the synchronization frequency as well as enable SNTP. The syntax for the above commands is shown below.

setsntp *server = <ipaddress> timeout = <1-10> retry = <1-3>*

sync *[hour=<0-24>] [min=<0-59>] (default = 24 hours)*

sntp *[enable|disable]*

To set the SNTP server to be 3.94.210.5 (with a time out of 3 seconds and a number of retries set to 3 times); allowing the synchronization to be ever 5 hours, the following sequence of commands are used

ML3000# `sntp`

ML3000(sntp)## `setsntp server=3.94.210.5 timeout=3 retry=3`

SNTP server is added to SNTP server database

ML3000(sntp)## `sync hour=5`

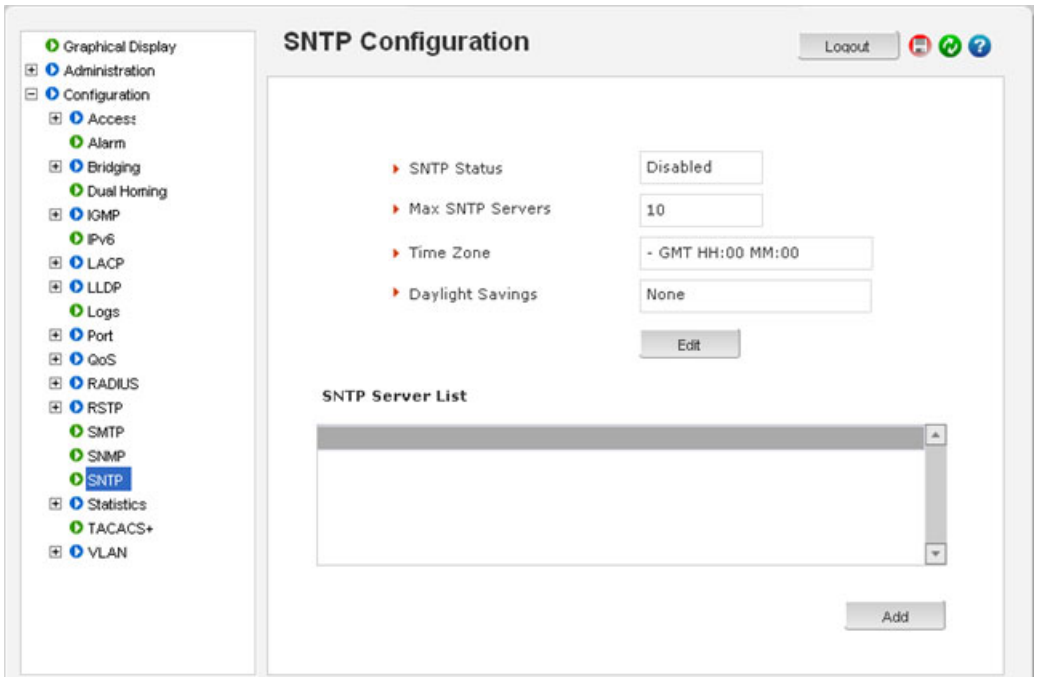
ML3000(sntp)## `sntp enable`

SNTP is already enabled.

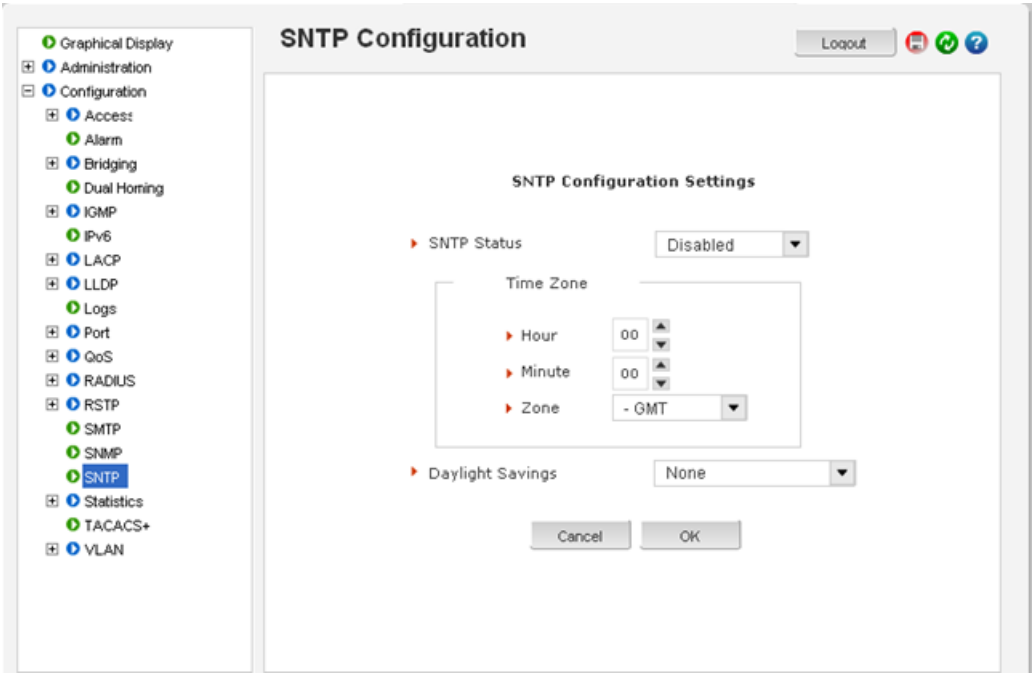
ML3000(sntp)## `exit`

ML3000(sntp)#

SNTP parameters can be configured through the EnerVista Secure Web Management software with the **Configuration > SNTP** menu item. The SNTP menu allows the time zone (hours from GMT) to be defined along with other appropriate parameters on setting the time and synchronizing clocks on network devices.



The **edit** button allows editing of the SNTP parameters as shown below. Adding or deleting SNTP servers is accomplished by using the add and delete buttons. Clicking the edit button allows the specific SNTP parameter settings to be modified.

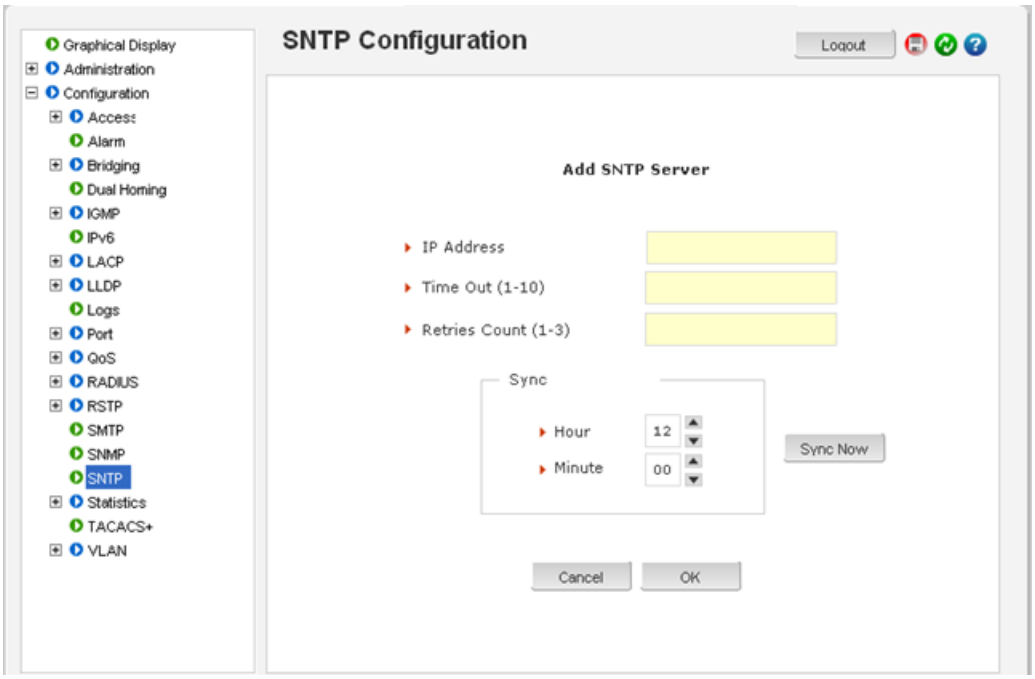


After the proper SNTP values are entered, click **OK** to register the changes, or click **Cancel** to back out from the changes made.

To add an SNTP server, click the **add** button on the **Configuration > SNTP** menu. The menu prompts you to add IP address of an SNTP server, the time out in seconds and the number of retries, before the time synchronization effort is aborted. The **Sync Now** button allows synchronization as soon as the server information is added.

NOTE

If your site has internet access, there are several SNTP servers available online. A quick search will yield information about these servers. You can use the IP address of these servers; however, please ensure the server can be reached by using the `ping` command. The `ping` command can also be launched from the EnerVista software.



The **Time Out** value is in seconds. Note the time server can be a NTP server available on the Internet. Ensure the IP parameters are configured for the switch and the device can be pinged by the switch. Once the server is added, it is listed with the other SNTP servers.

5.4 System Configuration

5.4.1 Saving and Loading – Command Line

NOTICE

Place the Switch offline while transferring Setting Files to the Switch.
When transferring Settings Files from one Switch to another, the IP address of the originating Switch will also be transferred. The user must therefore reset the IP address on the receiving Switch before connecting to the network.

Configuration changes are automatically registered but not saved; that is, the effect of the change is immediate. However, if power fails, the changes are not restored unless they saved using the `save` command. It is also a good practice to save the configuration on another network server using the tftp or ftp protocols. Once the configuration is saved, it can be loaded to restore the settings. At this time, the saved configuration parameters are not in a human readable format. The commands for saving and loading configurations on the network are:

saveconf *mode=<serial|tftp|ftp> <ipaddress> file=<name>*

loadconf *mode=<serial|tftp|ftp> <ipaddress> file=<name>*

Ensure the machine specified by the IP address has the necessary services running. For serial connections, x-modem or other alternative methods can be used. In most situations, the filename must be a unique, since overwriting files is not permitted by most ftp and tftp servers (or services). Only alphanumeric characters are allowed in the filename.

The following example illustrated how to save the configuration on a tftp server

```
ML3000# saveconf mode=tftp 3.94.240.9 file=ML3000set

Do you wish to upload the configuration?
['Y' or 'N'] Y
```

The `saveconf` and `loadconf` commands are often used to update software. Before the software is updated, it is advised to save the configurations. The re-loading of the configuration is not usually necessary; however, in certain situations it maybe needed and it is advised to save configurations before a software update. The `loadconf` command requires a reboot for the new configuration to be active. Without a reboot the older configuration is used by the MultiLink family of switches.

The `saveconf` and `loadconf` commands are often used to update software to the ML3000. These commands will be deprecated in the version 2.x and above, and replaced with the `ftp`, `tftp`, or `xmodem` commands. It is advised to begin using these commands instead of `saveconf` and `loadconf`.

5.4.2 Config file

Multilink ML3000/ML3100 Firmware can use the ftp or tftp (or xmodem if using the CLI) to upload and download information to a server running the proper services. One useful capability provided is export of the CLI commands used to configure the switch. To do this, use Config Upload/Download.

Using **Config Download**, examination of the contents of the saved file would appear as shown below:

```
<ML3000 -conf-1.0>
#####################################################################
# Copyright (c) 2001-2005 GE Multilin, Inc All rights reserved.
# RESTRICTED RIGHTS
# ---------------------------------
# Use, duplication or disclosure is subject to U.S. Government
# restrictions as set forth in Sub-division (b)(3)(ii) of the
# rights in Technical Data and Computer Software clause at
# 52.227-7013.
#
# This file is provided as a sample template to create a backup
# of GE MultiLink switches. As such, this script
# provides insights into the configuration of GE MultiLink
# switches settings. GE Multilin, Inc. recommends that modifications of this
# file and the commands should be verified by the User in a
# test environment prior to use in a "live" production network.
# All modifications are made at the User's own risk and are
# subject to the limitations of the GE MultiLink software End User
# License Agreement (EULA). Incorrect usage may result in
# network shutdown. GE Multilin, Inc. is not liable for incidental or
# consequential damages due to improper use.
#####################################################################
***This is a Machine Generated File.
***Only the SYSTEM config block is editable.
***Editing any other block will result in error while loading.
#############################################################
# Hardware Configuration - This area shows the type of          #
#                 hardware and modules installed.                                    #
#############################################################
[HARDWARE]
```

```
[SYSTEM]
***Edit below this line only***

system_name=ML3000
system_contact=support@gemultilin.com
system_location= Markham, Ontario
boot_mode=manual
system_ip=192.168.5.5
system_subnet=0.0.0.0
system_gateway=0.0.0.0
idle_timeout=10
telnet_access=enable
snmp_access=enable

web_access=enable

***Edit above this line only***
############################################################
# User Accounts - This area configures user accounts for #
#              accessing this system.              #
############################################################
...
```

FIGURE 5–1: Contents of a config file

NOTICE

1. **A config file allows only certain portions of the file to be edited by a user. Changing any other part of the file will result in the system not allowing the file to be loaded, as the CRC computed and stored in the file would not be matched. Should you want to edit, edit the System portion of the file only. GE Multilin, Inc. recommends editing the "script" file (see below)**
2. **File names cannot have special characters such as *#!@$^&* space and control characters.**

5.4.3 Displaying configuration

Using SWM, the need to display specific CLI commands for configuring capabilities is not needed. The menus are modular and are alphabetically sorted to display each necessary component in a logical manner. This section is repeated from the CLI manual, should the need arise to view the necessary commands. The best way to view these commands is to telnet to the switch using the Telnet menu from the Administration menu.

To display the configuration or to view specific modules configured, the '**show config**' command is used as described below.

Syntax **show config [module=<module-name>]**

Where module-name can be:

Name	Areas affected
system	IP Configuration, Boot mode, Users settings (e.g. login names, passwords)
event	Event Log and Alarm settings
port	Port settings, Broadcast Protection and QoS settings
bridge	Age time setting
stp	STP, RSTP and LLL settings
ps	Port Security settings
mirror	Port Mirror settings
sntp	SNTP settings
llan	VLAN settings
gvrp	GVRP settings
snmp	SNMP settings
web	Web and SSL/TLS settings
tacacs	TACACS+ settings
auth	802.1x Settings
igmp	IGMP Settings
smtp	SMTP settings

If the module name is not specified the whole configuration is displayed.

```
ML3000# show config
[HARDWARE]
type= ML3000
slotB=8 Port TP Module
############################################################
```

```
# System Manager - This area configures System related          #
#              information.                                                  #
#############################################################
[SYSTEM]
***Edit below this line only****
system_name=Main
system_contact=someone@joe.com
system_location= Markham, Ontario
boot_mode=manual
system_ip=192.168.1.15
system_subnet=0.0.0.0
system_gateway=192.168.1.11
idle_timeout=10
telnet_access=enable
snmp_access=enable
web_access=enable

--more—
...
```

FIGURE 5–2: 'show config' command output

```
ML3000# show config module=snmp
[HARDWARE]
type= ML3000
slotB=8 Port TP Module
############################################################
# Network Management - This area configures the SNMPv3      #
#                agent.                                                    #
############################################################
[SNMP]
engineid=LE_v3Engine
defreadcomm=public
defwritecomm=private
deftrapcomm=public
authtrap=disable
com2sec_count=0
group_count=0
view_count=1
view1_name=all
view1_type=included
view1_subtree=.1
view1_mask=ff

--more—
...
```

FIGURE 5–3: Displaying specific modules using the ‘show config’ command

```
ML3000# show config module=snmp,system
[HARDWARE]
type= ML3000
slotB=8 Port TP Module
############################################################
# System Manager - This area configures System related           #
#              information.                                                    #
############################################################
[SYSTEM]
***Edit below this line only****
system_name=Main
system_contact=someone@joe.com
system_location= Markham, Ontario
boot_mode=manual
system_ip=192.168.1.15
system_subnet=0.0.0.0
system_gateway=192.168.1.11
idle_timeout=10
telnet_access=enable
snmp_access=enable
web_access=enable

--more—
…
```

FIGURE 5–4: Displaying configuration for different modules.
Note – multiple modules can be specified on the command line

5.4.4 Saving Configuration

It is advisable to save the configuration before updating the software, as it may be necessary in certain situations. The `loadconf` command requires a reboot to activate the new configuration. Without a reboot, the ML3000 used the previous configuration. When reboot is selected, the user is prompted as follows:

Reboot? ['Y' or 'N']

Select "Y". The ML3000 will prompt:

Save Current Configuration?

Select "N".

Additional capabilities have been added to save and load configurations. The commands are:

ftp *<get|put|list|del> type=<app|config|oldconf|script|hosts|log> host=<hostname> ip=<ipaddress> file=<filename> user=<user> pass=<password>*

tftp *<get|put> type=<app|config|oldconf|script|hosts|log> host=<hostname> ip=<ipaddress> file=<filename>*

xmodem *<get|put> type=<app|config|oldconf|script|hosts|log>*

The arguments are describe below:

`type`: Specifies whether a log file or host file is uploaded or downloaded. This can also perform the task of exporting a configuration file or uploading a new image to the switch

`host`, `ip`, `file`, `user`, `pass`: These parameters are associated with ftp/tftp server communications.

The user can save the configuration in old (v2 format) and new (v3 format). The v3 format must be used to utilize the ASCII and CLI Script capability.

save *[format=v2|v3]*

With release 1.7 and higher, the configuration can be saved in the older format (binary object) or in a new format as an ASCII file. The new format is recommended by GE Multilin. Use the old format only if there are multiple MultiLink switches on the network running different versions of software. GE Multilin recommends upgrading all switches to the most current software release.

To ease the process of uploading and executing a series of commands, the ML3000 can create a host (equivalent to creating a host table on many systems). The command for creating a host is:

host *<add|edit|del> name=<host-name> ip=<ipaddress> user=<user> pass=<password>*

The `show host` command displays the host table entries

```
ML3000# access
ML3000(access)## host add name=server ip=192.168.5.2
Host added successfully
ML3000(access)## show host
No  Host Name  IP Address   User  Password
=========================================
1  server   192.168.5.2 --  ******
2  --       --          --  --
3  --       --          --  --
4  --       --          --  --
5  --       --          --  --
6  --       --          --  --
7  --       --          --  --
8  --       --          --  --
9  --       --          --  --
10 --       --          --  --
ML3000(access)##
```

5.4.5 Script File

Script file is a file containing a set of CLI commands which are used to configure the switch. CLI commands are repeated in the file for clarity, providing guidance to the user editing the file as to what commands can be used for modifying variables used by Firmware. The script file does not have a check sum at the end and is used for configuring a large number of switches easily. As with any configuration file that is uploaded, GE Multilin, Inc. recommends that modifications of this file and the commands should be verified by the user in a test environment prior to use in a "live" production network.

The script file will look familiar to people familiar with the CLI commands as all the commands saved in the script file are described in the CLI User Guide. A sample of the script file is shown below.

```
##################################################################
#
# Copyright (c) 2001-2005 GE Multilin, Inc All rights reserved.
# RESTRICTED RIGHTS
# --------------------------------
# Use, duplication or disclosure is subject to U.S. Government
# restrictions as set forth in Sub-division (b)(3)(ii) of the
# rights in Technical Data and Computer Software clause at
# 52.227-7013.
#
# This file is provided as a sample template to create a backup
# of GE MultiLink switches configurations. As such,
# this script provides insights into the configuration of GE MultiLink switch's settings.
# GE Multilin, Inc. recommends that modifications of this
# file and the commands should be verified by the User in a
# test environment prior to use in a "live" production network.
# All modifications are made at the User's own risk and are
# subject to the limitations of the GE MultiLink Firmware End User
# License Agreement (EULA). Incorrect usage may result in
# network shutdown. GE Multilin, Inc. is not liable for incidental or
# consequential damages due to improper use.
##################################################################
#

############################################################
# System Manager - This area configures System related                #
#              information.                                          #
############################################################

set bootmode type=manual
ipconfig ip=192.168.5.5 mask=0.0.0.0 dgw=0.0.0.0
set timeout=10
access
telnet enable
snmp enable
web=enable
exit
############################################################
# User Accounts - This area configures user accounts for              #
#             accessing this system.                                  #
############################################################

user
add user=manager level=2
passwd user=manager
manager
<additional lines deleted for succinct viewing>
```

In the above example, note that all the commands are CLI commands. This script provides an insight into the configuration of GE MultiLink switches settings. GE Multilin, Inc. recommends that modifications of this file and the commands should be verified by the User in a test environment prior to use in a "live" production network

To ease the process of uploading the script files, use the Script Upload/Download capability described above.

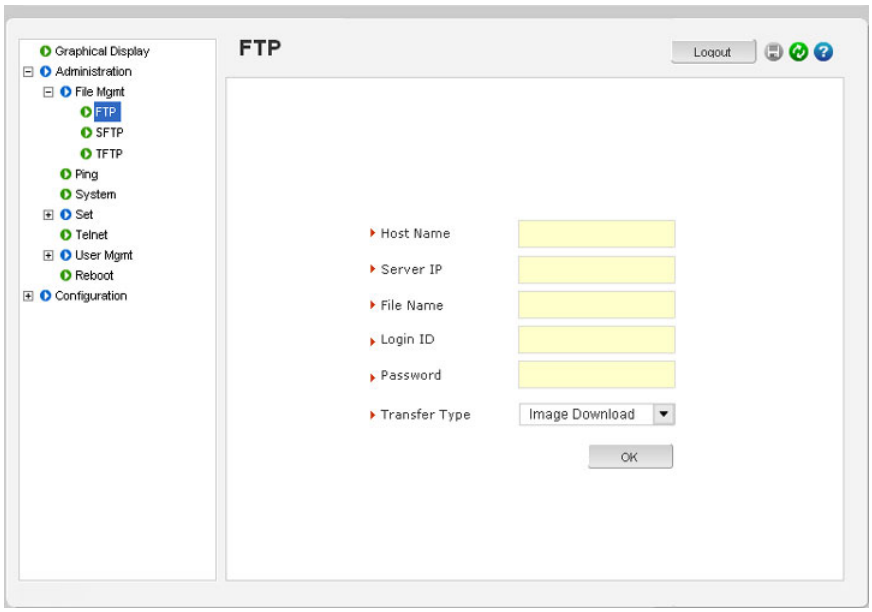
5.4.6 Saving and Loading – EnerVista Software

NOTICE

Place the Switch offline while transferring Setting Files to the Switch.
When transferring Settings Files from one Switch to another, the IP address of the originating Switch will also be transferred. The user must therefore reset the IP address on the receiving Switch before connecting to the network.

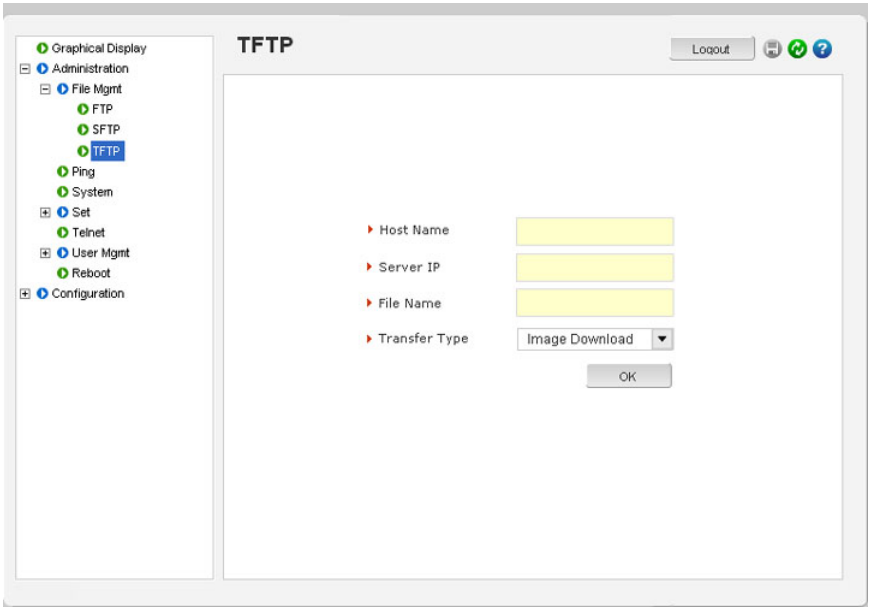
After configuration changes are made, all the changes are automatically saved. It is a good practice to save the configuration on another server on the network using the `tftp` or `ftp` protocols. Once the configuration is saved, the saved configuration can be reloaded to restore the settings. At this time, the saved or loaded configuration parameters are not in a human readable format.

The following figure illustrates the FTP window, which can be used to save the configuration, as well as up load new images or reload a saved configuration.



Ensure the machine specified by the IP address has the necessary services running on it. For serial connections, x-modem or other alternative methods can be used. Generally, the filename name must be a unique filename, as over-writing files is not permitted by most FTP and TFTP servers (or services).

The following figure illustrates saving the configuration on a TFTP server. Note that the menu is similar to the FTP screen described earlier.



This process can also be used to update new software to the managed MultiLink switches. Before the software is updated, it is advised to save the configurations. Reloading of the configuration is not usually necessary, but in certain situations it may be needed, and it is recommended that you save configurations before a software update. Make sure to reboot the switch after a new configuration is loaded.

The file transfer operations allowed are:

1. Image Download (or Image Upload): Copy the ML3000 image from server to the switch (or from the switch to the server). The "Image Download" option is commonly used to upgrade the ML3000 image on the switch.
2. Config Download (or Config Upload): Load the configuration of the switch from the server (or save the configuration from the switch to the server). This option is used to save a backup of the ML3000 configuration or restore the configuration (in case of a disaster.)
3. Script Download (or Script Upload): Load the necessary CLI commands used for configuration of the switch (or save the necessary CLI commands needed to configure the switch on the server). This option is used to ease the repetitive task of configuring multiple commands or reviewing all the commands needed to configure the ML3000.
4. Host Download (or Host Upload): Save the host information. The hosts are created by the Configuration - Access - Host commands
5. Log Upload - Save the log file on the ftp/tftp server

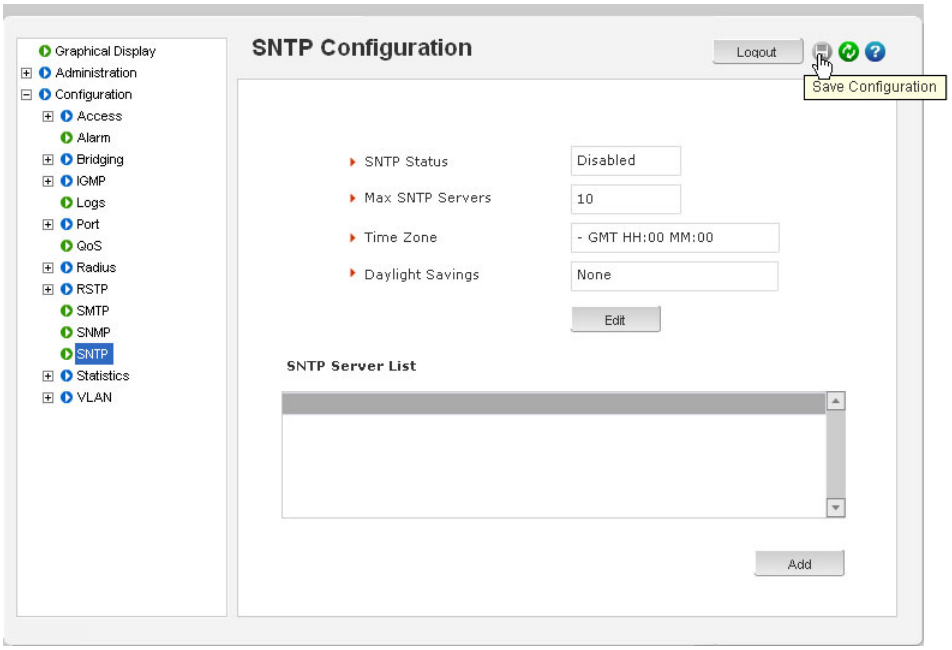
To save any changes,

▷ Click on the save ( ) icon.
The software will ask again if the changes need to be saved or ignored.

▷ If the changes need to be ignored, click on **Cancel** and reboot the switch.

▷ If the changes need to be saved, click on **OK**.

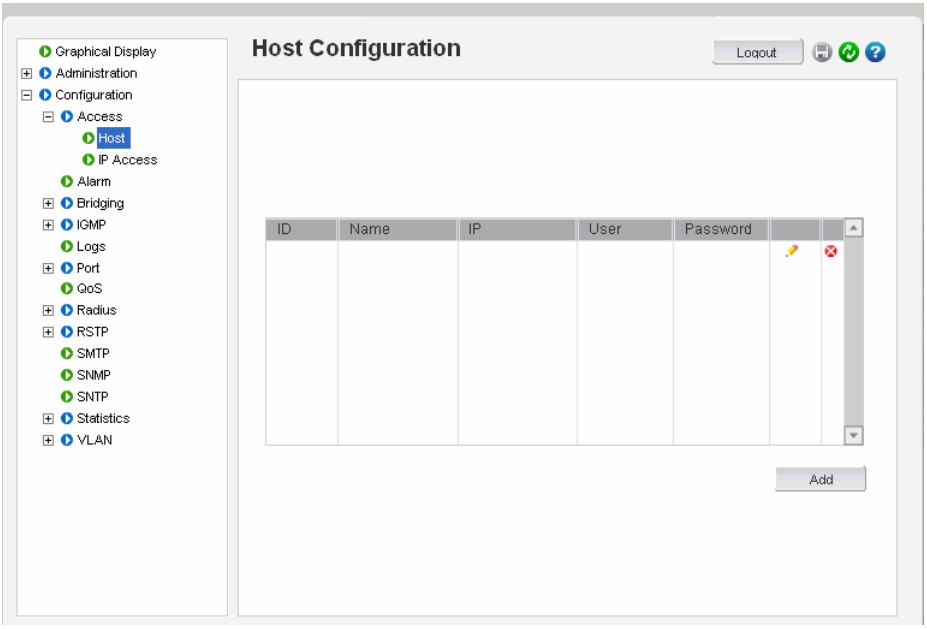
The following figures illustrate saving changes made after adding an SNTP server. This is done by clicking on the **Save** icon to save current configuration



5.4.7 Host Names

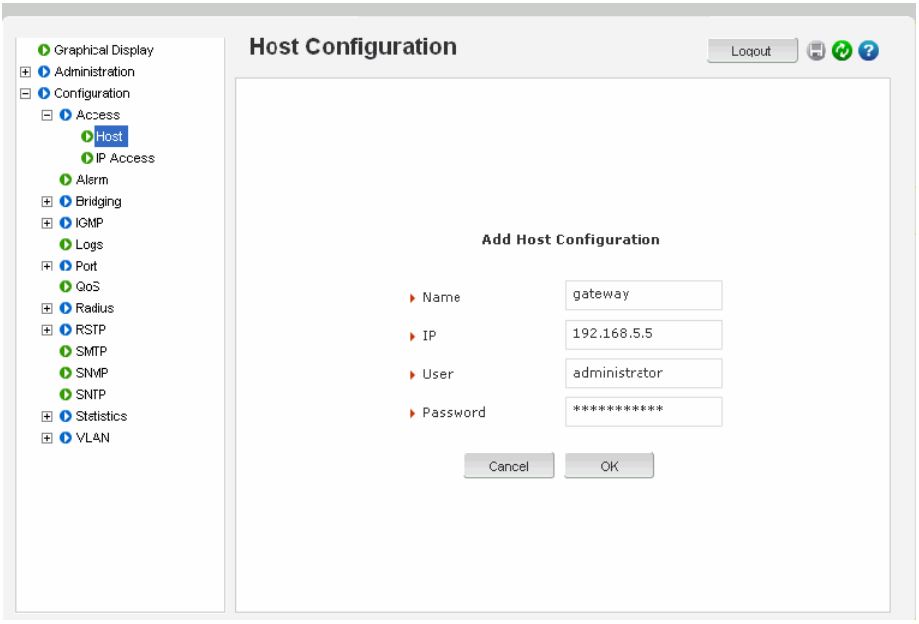
Instead of typing in IP addresses of commonly reached hosts, the ML3000 allows hosts to be created with the necessary host names, IP addresses, user names, and passwords.

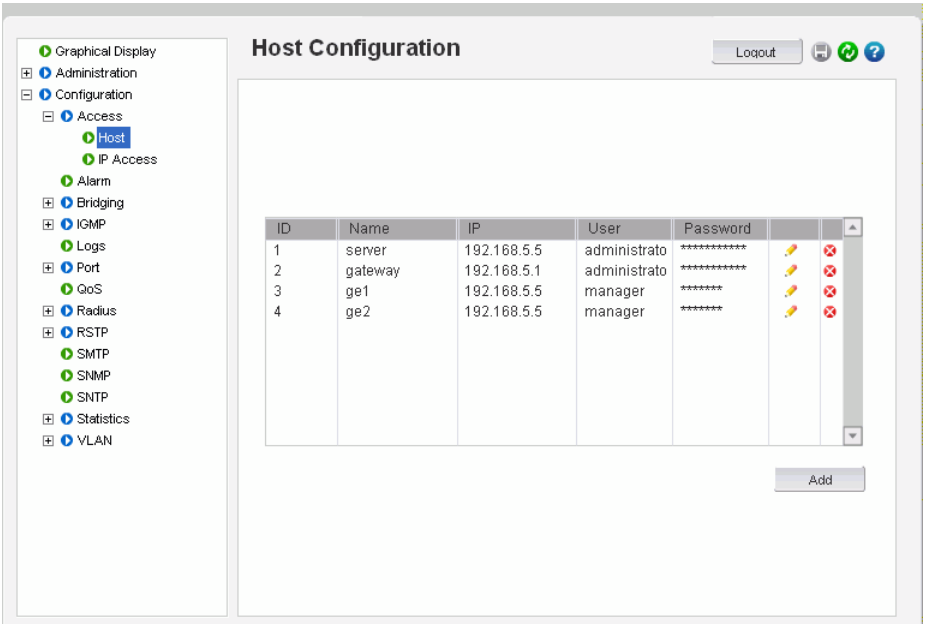
▷ Use the **Configuration > Access > Host** menu to create host entries as shown below.



▷ To add a host, click the **Add** button.

▷ Fill in all the fields below to create the necessary host entries.





▷ To delete or edit the entries, use the delete or edit icons next to each entry shown above.

5.4.8 Erasing Configuration

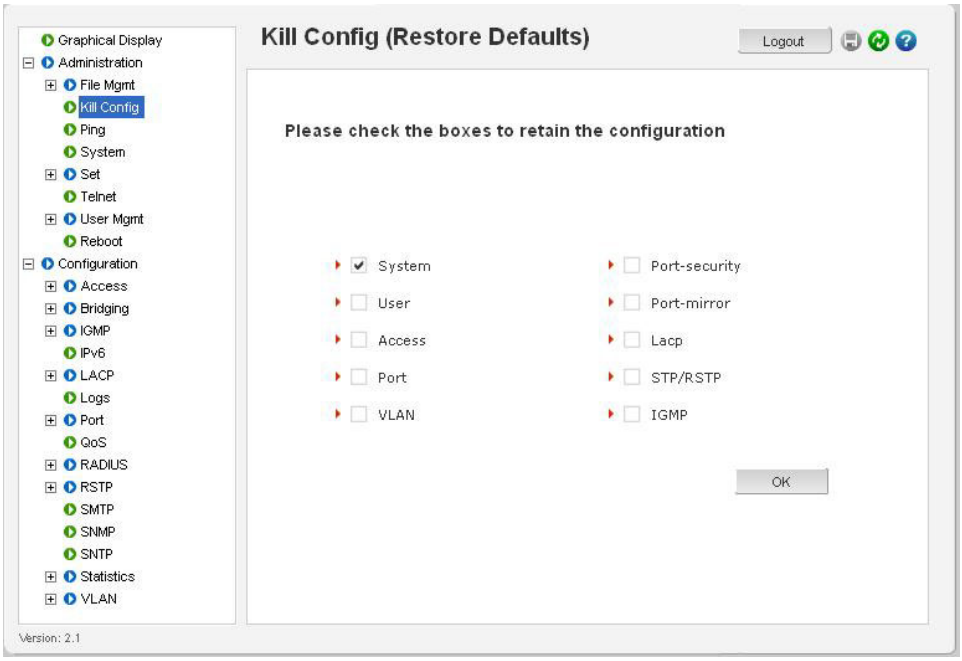
Kill Config option using SWM

To erase the configuration and reset the configurations to factory defaults, you can use the *kill config* option from Administration tab by selecting **kill config**.

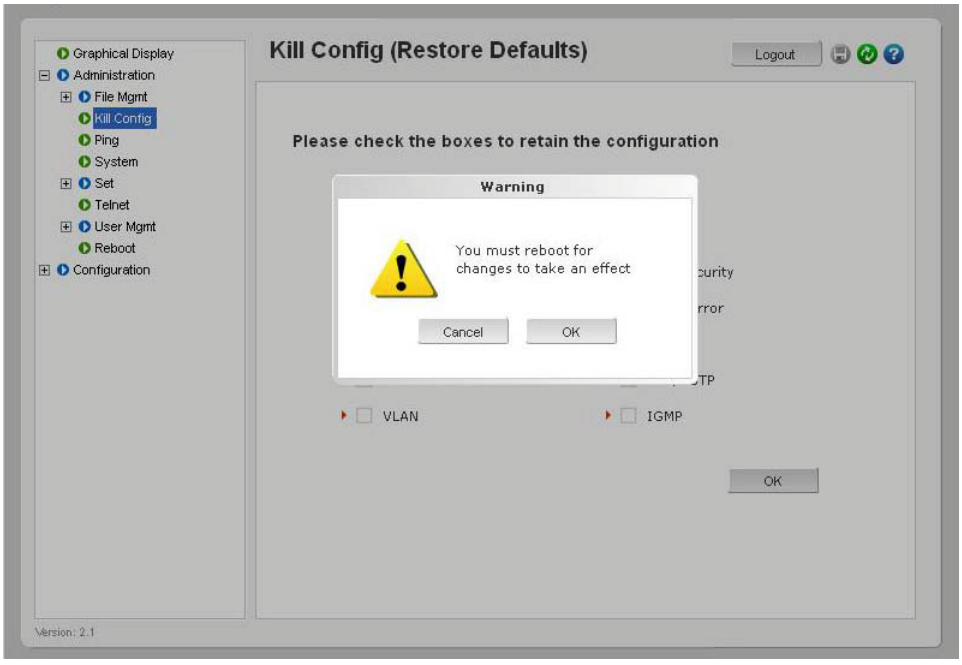
NOTE

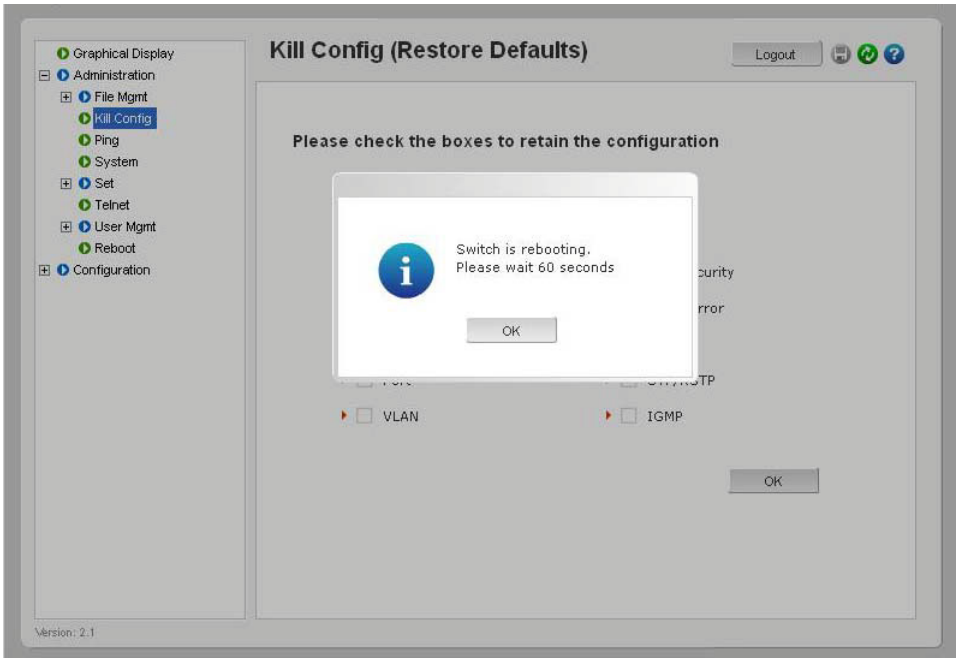
User also has the option to save one module from defaulting back to factory defaults by checking the module box before issuing kill Config command.

In the example below "system" module box has been checked. In this case after kill Config command is issued by pressing the **OK** button, the Switch will perform a factory dump restoring all the Switch settings back to factory defaults except for the "System" settings which will be retained.



When the **OK** button is pressed the Switch will issue the following warning messages; and reboot the switch for it to revert back to the factory default settings with the exceptions of modules opted not to be defaulted.





Here is a list of the modules and related settings that can be selected not to default back to factory default settings.

Name	Areas affected
System	IP Configuration, Boot mode
User	Users settings (e.g. login names, passwords)
Port	Port settings, Broadcast Protection and QoS settings
STP/RSTP	STP, RSTP settings
Port-Security	Port Security settings
Port-Mirror	Port Mirror settings
VLAN	Port/Tag VLAN settings
ACCESS	IP-Access and Host Table settings
IGMP	IGMP Settings
LACP	LACP settings

Kill Config option using CLI

This command is a "hidden command"; that is, the on-line help and other help functions normally do not display this command. The syntax for this command is:

kill Config

or

kill config save=module command

The *kill Config* command will default all the Switch settings back to factory defaults, while the *kill config save=module* will default all with the exception of module selected.

Available modules are: system, user, acces, port, vlan, ps, mirror, lacp, slp, and igmp.

It is recommended to save the configuration (using saveconf command discussed above) before using the kill config command. The following two examples illustrate how to erase all the Switch's configuration using the kill config command and the second example illustrates how to erase all the Switch's configuration with the exception of 'system' configuration.

ML3000# kill config

Do you want to erase the configuration?

['Y' or 'N'] Y

Successfully erased configuration...Please reboot.

ML3000# kill config save=system

Do you want to erase the configuration?

['Y' or 'N'] Y

Successfully erased configuration...Please reboot.

Once the configuration is erased, please reboot the switch for the changes to take effect.

5.5 IPv6

This section explains how to access the GE MultiLink switches using IPv6 instead of IPv4 addressing. IPv6 provides a much larger address space and its use is often required.

Assumptions

It is assumed here that the user is familiar with IP addressing schemes and has other supplemental material on IPv6, configuration, routing, setup and other items related to IPv6. This user guide does not discuss these details.

5.5.1 Introduction to IPv6

IPv6 is short for "Internet Protocol Version 6". IPv6 is the "next generation" protocol or IPng and was recommended to the IETF to replace the current version Internet Protocol, IP Version 4 ("IPv4"). IPv6 was recommended by the IPv6 (or IPng) Area Directors of the Internet Engineering Task Force at the Toronto IETF meeting on July 25, 1994 in RFC 1752: The Recommendation for the IP Next Generation Protocol. The recommendation in question, was approved by the Internet Engineering Steering Group and a proposed standard was created on November 17, 1994. The core set of IPv6 protocols was created as an IETF draft standard on August 10, 1998.

IPv6 is a new version of IP, designed to be an evolutionary step from IPv4. It is a natural increment to IPv4. It can be installed as a normal software upgrade in internet devices and is interoperable with the current IPv4. Its deployment strategy is designed to have no dependencies. IPv6 is designed to run well on high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and at the same time still be efficient on low bandwidth networks (e.g. wireless). In addition, it provides a platform for the new level of internet functionality that will be required in the near future.

IPv6 includes a transition mechanism designed to allow users to adopt and deploy it in a highly diffuse fashion, and to provide direct interoperability between IPv4 and IPv6 hosts. The transition to a new version of the Internet Protocol is normally incremental, with few or no critical interdependencies. Most of today's internet uses IPv4, which is now nearly twenty years old. IPv4 has been remarkably resilient in spite of its age, but it is beginning to have problems. Most importantly, there is a growing shortage of IPv4 addresses, which are needed by all new machines added to the Internet.

IPv6 fixes a number of problems in IPv4, such as the limited number of available IPv4 addresses. It also adds many improvements to IPv4 in areas such as routing and network auto configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years during the transition period.

5.5.2 What's changed in IPV6?

The changes from IPv4 to IPv6 fall primarily into the following categories:

- Expanded Routing and Addressing Capabilities – IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses.
- A new type of address called an "anycast address" is defined, that identifies sets of nodes where a packet sent to an anycast address is delivered to one of these

nodes. The use of anycast addresses in the IPv6 source route allows nodes to control the path along which their traffic flows.

- Header Format Simplification - Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to keep the bandwidth cost of the IPv6 header as low as possible despite the increased size of the addresses. Even though the IPv6 addresses are four times longer than the IPv4 addresses, the IPv6 header is only twice the size of the IPv4 header.
- Improved Support for Options - Changes in the way IP header options are encoded allow more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.
- Quality-of-Service Capabilities - A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real- time" service.
- Authentication and Privacy Capabilities - IPv6 includes the definition of extensions which provide support for authentication, data integrity, and confidentiality. This is included as a basic element of IPv6 and will be included in all implementations.

5.5.3 IPv6 Addressing

IPv6 addresses are 128-bits long and are identifiers for individual interfaces and sets of interfaces. IPv6 addresses of all types are assigned to interfaces, not nodes. Since each interface belongs to a single node, any of that node's interface's unicast addresses may be used as an identifier for the node. A single interface may be assigned multiple IPv6 addresses of any type.

There are three types of IPv6 addresses. These are unicast, anycast, and multicast. Unicast addresses identify a single interface. Anycast addresses identify a set of interfaces such that a packet sent to an anycast address will be delivered to one member of the set. Multicast addresses identify a group of interfaces, such that a packet sent to a multicast address is delivered to all the interfaces in the group. There are no broadcast addresses in IPv6. This function has been replaced by multicast addresses.

IPv6 supports addresses which are four times the number of bits as IPv4 addresses (128 vs. 32). This is 4 Billion x 4 Billion x 4 Billion (296) times the size of the IPv4 address space (232). This works out to be:

340,282,366,920,938,463,463,374,607,431,768,211,456

This is an extremely large address space. In a theoretical sense this is approximately 665,570,793,348,866,943,898,599 addresses per square meter of the surface of the planet Earth (assuming the earth surface is 511,263,971,197,990 square meters). In the most pessimistic estimate this would provide 1,564 addresses for each square meter of the surface of Earth. The optimistic estimate would allow for 3,911,873,538,269,506,102 addresses for each square meter of the surface Earth. Approximately fifteen percent of the address space is initially allocated. The remaining 85% is reserved for future use.

Details of the addressing are covered by numerous articles on the WWW as well as other literature, and are not covered here.

5.5.4 Configuring IPv6

The commands used for IPv6 are the same as those used for IPv4. Some of the commands will be discussed in more details later. The only exception is the 'ping' command where there is a special command for IPv6. That commands is 'ping6' and the syntax is as

Syntax **ping6 <IPv6 address>** - *pings an IPv6 station.*

There is also a special command to ping the status of IPv6. That command is

Syntax **show ipv6** - *displays the IPv6 information.*

To configure IPv6, the following sequence of commands can be used:

```
ML3000# ipconfig ?
ipconfig :  Configures the system IP address, subnet mask and gateway
Usage
ipconfig [ip=<ipaddress>] [mask=<subnet-mask>] [dgw=<gateway>]

ML3000# ipconfig ip=fe80::220:6ff:fe25:ed80 mask=ffff:ffff:ffff:ffff::
 Action Parameter Missing. "add" assumed.
 IPv6 Parameters Set.
ML3000# show ipv6

 IPv6 Address : fe80::220:6ff:fe25:ed80 mask : ffff:ffff:ffff:ffff::

ML3000# show ipconfig
 IP Address :  192.168.5.5
 Subnet Mask:  255.255.255.0
 Gateway Address:  192.168.5.1
 IPv6 Address:  fe80::220:6ff:fe25:ed80 mask : ffff:ffff:ffff:ffff::
 IPv6 Gateway:  ::

ML3000#
```

FIGURE 5–5: Configuring IPv6

In addition to the commands listed above, the commands which support IPv6 addressing are

Syntax **ftp <IPv6 address>** - *ftp to an IPv6 station*

Example – ftp fe80::220:6ff:fe25:ed80

Syntax **telnet <IPv6 address>** - *telnet to an IPv6 station*

Example – telnet fe80::220:6ff:fe25:ed80

Besides, if the end station supports IPv6 addressing (as most Linux and Windows systems do), one can access the switch using the IPv6 addressing as shown in the example below

http://fe80::220:6ff:fe25:ed80

5.5.5 List of commands in this chapter

Syntax **ipconfig [ip=<ip-address>] [mask=<subnet-mask>] [dgw=<gateway>] [add|del]** *– configure an IPv6 address. The add/delete option can be used to add or delete IPv4/IPv6 addresses.*

Syntax **show ipconfig** *– display the IP configuration information – including IPv6 address*

Syntax **ping6 <IPv6 address>** *- pings an IPv6 station*

Syntax **show ipv6** *- displays the IPv6 information*

Syntax **ftp <IPv6 address>** *- ftp to an IPv6 station*

Syntax **telnet <IPv6 address>** *- telnet to an IPv6 station.*

Multilink ML3000/ML3100

Chapter 6: Access Considerations

6.1 Securing Access

6.1.1 Description

This section explains how the access to the MultiLink family of switches can be secured. Further security considerations are also covered such as securing access by IP address or MAC address.

It is assumed here that the user is familiar with issues concerning security as well as securing access for users and computers on a network. Secure access on a network can be provided by authenticating against an allowed MAC address as well as IP address.

6.1.2 Passwords

The GE MultiLink family of switches have a factory default password for the manager as well as the operator account. Passwords can be changed from the user ID by using the `set password` command.

For example:

ML3000# `set password`

Enter Current Password: *****
Enter New Password:*****
Confirm New Password:*****
Password has been modified successfully

ML3000#

Other details on managing users and the passwords are covered in *User Management* on page 1–29.

6.1.3 Port Security Feature

The port security feature can be used to block computers from accessing the network by requiring the port to validate the MAC address against a known list of MAC addresses. This port security feature is provided on an Ethernet, Fast Ethernet, or Gigabit Ethernet port. In case of a security violation, the port can be configured to go into the disable mode or drop mode. The disable mode disables the port, not allowing any traffic to pass through. The drop mode allows the port to remain enabled during a security violation and drop only packets that are coming in from insecure hosts. This is useful when there are other network devices connected to the MultiLink family of switches. If there is an insecure access on the secondary device, the MultiLink family of switches allow the authorized users to continue to access the network; the unauthorized packets are dropped preventing access to the network.

Network security hinges on the ability to allow or deny access to network resources. This aspect of secure network services involves allowing or disallowing traffic based on information contained in packets, such as the IP address or MAC address. Planning for access is a key architecture and design consideration. For example, which ports are configured for port security? Normally rooms with public access (e.g. lobby, conference rooms, etc.) should be configured with port security. Once that is decided, the next few decisions are: Who are the authorized and unauthorized users? What action should be taken against authorized as well as unauthorized users? How are the users identified as authorized or unauthorized?

6.2 Configuring Port Security through the Command Line Interface

6.2.1 Commands

To configure port security, login as a level 2 user or as a manager. Once logged in, get to the port-security configuration level to setup and configure port security with the following command syntax:

configure port-security

port-security

For example, using the `configure port-security` command:

ML3000# `configure port-security`

ML3000(port-security)##

Alternately, the `port-security` command can also be used to enter the port-security configuration mode:

ML3000# `port-security`

ML3000#(port-security)##

From the port security configuration mode, the switch can be configured to:

1. Auto-learn the MAC addresses.
2. Specify individual MAC addresses to allow access to the network.
3. Validate or change the settings.

The command syntax for the above actions are:

allow *mac=<address|list|range>*
port=<num|list|range>

learn *port=<number-list> <enable|disable>*

show port-security

action *port=<num|list|range>*
<none|disable|drop>

signal *port=<num|list|range>*
<none|log|trap|logandtrap>

ps *<enable|disable>*

remove *mac=<all|address|list|range>*
port=<num|list|range>

signal *port=<num|list|range>*
<none|log|trap|logandtrap>

Where the following hold:

- `allow mac` - configures the switch to setup allowed MAC addresses on specific ports
- `learn port` - configures the switch to learn the MAC addresses associated with specific port or a group of ports
- `show port-security` - shows the information on port security programmed or learnt
- `action port` - specifies the designated action to take in case of a non authorized access
- `ps` - port security - allows port security to be enable or disabled

- `remove mac` - removes specific or all MAC addresses from port security lookup
- `signal port=<num|list|range>` - observe list of specified ports and notify if there is a security breach on the list of port specified. The signal can be a log entry, a trap to the trap receiver specified as part of the SNMP commands (where is that specified) or both


NOTE

There is a limitation of 200 MAC addresses per port and 500 MAC addresses per switch for port security.


NOTE

All commands listed above must be executed under the port security configuration mode.

Let's look at a few examples. The following command allows specific MAC addresses on a specified port. No spaces are allowed between specified MAC addresses.

ML3000(port-security)## `allow mac=00:c1:00:7f:ec:00,00:60:b0:88:9e:00 port=18`

The following command sequence sets the port security to learn the MAC addresses. Note that a maximum of 200 MAC addresses can be learned per port, to a maximum of 500 per switch. Also, the `action` on the port must be set to none before the port learns the MAC address information.

ML3000(port-security)## `action port=9,10 none`

ML3000(port-security)## `learn port=9,10 enable`

The following command sequence enables and disables port security

ML3000(port-security)## `ps enable`

Port Security is already enabled

ML3000(port-security)## `ps disable`

Port Security Disabled

ML3000 `ps enable`

Port Security Enabled

6.2.2 Allowing MAC Addresses

The Port Security feature has to be used with the combination of commands shown below in order for it to be implemented successfully.

To configure a port to allow only a certain MAC address (single or a list of max 200 MAC addresses per port and 500 MAC addresses per ML3000, as per manuals) we have to:

1. Verify that the port is in default port security status.
2. Use the following commands:

#port-security

(port-security)##ps enable

(port-security)##allow mac=<address,list,range> port=<num,list,range>

(port-security)##action port=<num,list,range>drop


NOTE

All the above commands have to be configured in this sequence, otherwise the port will remain insecure.

To deny a mac address, use the following:

#port-security

(port-security)##ps enable

(port-security)##deny mac=<address,list,range> port=<num,list,range>

(port-security)##action port=<num,list,range>drop

Example 6-1 views port security settings on a switch. Learning is enabled on port 9. This port has 6 stations connected to it with the MAC addresses as shown. Other ports have learning disabled and the MAC addresses are not configured on those ports.

Example 6-1: Viewing the port security settings

```
ML3000# show port-security
PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 9    ENABLE  LOG     NONE    ENABLE   6     00:e0:29:2a:f1:bd
                                             00:01:03:e2:27:89
                                             00:07:50:ef:31:40
                                             00:e0:29:22:15:85
                                             00:03:47:ca:ac:45
                                             00:30:48:70:71:23
 10   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 11   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 12   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 13   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 14   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 15   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 16   ENABLE  NONE    NONE    DISABLE  0     Not Configured
ML3000(port-security)##
```

Example 6-2: Enabling learning on a port

```
ML3000(port-security)## learn port=11 enable
 Port Learning Enabled on selected port(s)
ML3000(port-security)## show port-security
PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 9    ENABLE  LOG     NONE    ENABLE   6     00:e0:29:2a:f1:bd
                                             00:01:03:e2:27:89
                                             00:07:50:ef:31:40
                                             00:e0:29:22:15:85
                                             00:03:47:ca:ac:45
                                             00:30:48:70:71:23
 10   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 11   ENABLE  NONE    NONE    ENABLE   0     Not Configured
 12   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 13   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 14   ENABLE  NONE    NONE    DISABLE  0     Not Configured
```

Example 6-2 shows how to enable learning on a port. After the learning is enabled, the port security can be queried to find the status of MAC addresses learnt. If there were machines connected to this port, the MAC address would be shown on port 11 as they are shown on port 9.

Example 6-3 shows how to allow specific MAC address on specific ports. After the MAC address is specified, the port or specific ports or a range of ports can be queried as shown.

Example 6-4 shows how to remove a MAC address from port security

To set logging on a port, use the following command sequence:

```
ML3000(port-security)## signal port=11 logandtrap

 Port security Signal type set to Log and
 Trap on selected port(s)
```

The examples provided illustrate the necessary commands to setup port security. The recommended steps to setup security are:

- Set the ML3000 software to allow port security commands (use the `port-security` command).
- Enable port security (use the `enable ps` command).
- Enable learning on the required ports (for example, use the `learn port=11` enable command for port 11).
- Verify learning is enables and MAC addresses are being learnt on required ports (use the `show port-security port=11` command).
- Save the port-security configuration (use the `save` command).

Example 6-3: Allowing specific MAC addresses on specific ports

```
ML3000(port-security)## allow mac=00:c1:00:7f:ec:00 port=9,11,13

 Specified MAC address(es) allowed on selected port(s)

ML3000(port-security)## show port-security port=9,11,13

PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 9    ENABLE  LOG     NONE    ENABLE   6     00:e0:29:2a:f1:bd
                                             00:01:03:e2:27:89
                                             00:07:50:ef:31:40
                                             00:e0:29:22:15:85
                                             00:03:47:ca:ac:45
                                             00:30:48:70:71:23
                                             00:c1:00:7f:ec:00
 11   ENABLE  NONE    NONE    ENABLE   0     00:c1:00:7f:ec:00
 13   ENABLE  NONE    NONE    DISABLE  0     00:c1:00:7f:ec:00
```

Example 6-4: Removing MAC addresses from specific ports

```
ML3000(port-security)## remove mac=00:c1:00:7f:ec:00 port=13

 Specified MAC address(es) removedfrom selected
 port(s)

ML3000(port-security)## show port-security port=13

PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
```

- Disable learning on required ports (for example, use the `learn port=11,15 disable` command).
- (Optional step) Add any specific MAC addresses, if needed, to allow designated devices to access the network (use the `add mac=00:c1:00:7f:ec:00 port=11,15` command).
- Disable access to the network for unauthorized devices (Use `action port=11 <disable|drop>` depending on whether the port should be disabled or the packed dropped. Follow that with a `show port-security` command to verify the setting).
- (Optional step) Set the notification to notify the management station on security breach attempts (use the command `signal port` to make a log entry or send a trap).

Example 6-5 illustrates these steps for setting up port security on a specific port:

Once port security is setup, it is important to manage the log and review the log often. If the signals are sent to the trap receiver, the traps should also be reviewed for intrusion and other infractions.

6.2.3 Security Logs

All events occurring on the MultiLink family of switches are logged. The events can be informational (e.g. login, STP synchronization etc.), debugging logs (for debugging network and other values), critical (critical events), activity (traffic activity) and fatal events (such as

Example 6-5: Configuring port security

```
ML3000# port-security
ML3000(port-security)## ps enable
 Port Security is already enabled
ML3000(port-security)## learn port=11 enable
 Port Learning Enabled on selected port(s)
ML3000(port-security)## show port-security
PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 9    ENABLE  LOG     NONE    ENABLE   6     00:e0:29:2a:f1:bd
                                             00:01:03:e2:27:89
                                             00:07:50:ef:31:40
                                             00:e0:29:22:15:85
                                             00:03:47:ca:ac:45
                                             00:30:48:70:71:23
 10   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 11   ENABLE  NONE    NONE    ENABLE   0     00:c1:00:7f:ec:00
 12   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 13   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 14   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 15   ENABLE  NONE    NONE    DISABLE  0     Not Configured
 16   ENABLE  NONE    NONE    DISABLE  0     Not Configured
ML3000(port-security)## save
 Saving current configuration
 Configuration saved
ML3000(port-security)## learn port=11 disable
 Port Learning Disabled on selected port(s)
ML3000(port-security)## action port=11 drop
 Port security Action type set to Drop on selected
 port(s)
ML3000(port-security)## show port-security port=11
PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 11   ENABLE  NONE    DROP    ENABLE   0     00:c1:00:7f:ec:00
ML3000(port-security)## signal port=11 logandtrap
 Port security Signal type set to Log and Trap on
 selected port(s)
```

unexpected behavior). The specific types of logs can be viewed and cleared. The `show log` command displays the log information and the `clear log` command clears the log entries. The syntax for these commands is shown below:

show log *[1..5|informational|debug|fatal |critical|activity]*

clear log *[informational|debug|activity |critical|fatal]*

The `set logsize` command set the number of lines to be collected in the log before the oldest record is re-written. The syntax for this command is:

set logsize *size=<1-1000>*

Example 6-6 illustrates the `show log` and `clear log` commands. The `show log` command indicates the type of log activity in the S column. I indicates informational entries and A indicates activities which are a result of port-security setup. Notice the `clear log informational` command clears the informational entries only.

The log shows the most recent intrusion at the top of the listing. If the log is filled when the switch detects a new intrusion, the oldest entry is dropped off the listing.

As discussed in the prior section, any port can be set to monitor security as well as make a log on the intrusions that take place. The logs for the intrusions are stored on the switch. When the switch detects an intrusion on a port, it sets an "alert flag" for that port and makes the intrusion information available.

The default log size is 50 rows. To change the log size, use the `set logsize` command.

When the switch detects an intrusion attempt on a port, it records the date and time stamp, the MAC address, the port on which the access was attempted and the action taken by ML3000 software. The event log lists the most recently detected security violation attempts. This provides a chronological entry of all intrusions attempted on a specific port.

Example 6-6: Security log commands

```
ML3000# show log
S  Date       Time        Log Description
-  ----       ----        ---------------
I  12-07-2004  9:01:34 A.M   CLI:manager console login
I  12-07-2004  5:54:23 P.M   SNTP:Date and Time updated from SNTP server
I  12-08-2004  6:09:00 P.M   SNTP:Date and Time updated from SNTP server
I  12-09-2004  1:48:56 P.M   TELNET:Telnet Session Started
I  12-09-2004  1:49:23 P.M   CLI:manager console login
I  12-09-2004  4:26:26 P.M   TELNET:Telnet Session Started
I  12-09-2004  4:26:34 P.M   CLI:manager console login
I  12-09-2004  6:23:37 P.M   SNTP:Date and Time updated from SNTP server
I  12-10-2004  6:38:13 P.M   SNTP:Date and Time updated from SNTP server
I  12-11-2004  10:16:24 A.M  TELNET:Telnet Session Started
I  12-11-2004  6:52:49 P.M   SNTP:Date and Time updated from SNTP server
I  12-12-2004  12:40:35 P.M  TELNET:Telnet Session Started
I  12-12-2004  12:40:42 P.M  CLI:manager console login
A  12-17-2004  12:05:52 P.M  PS:INTRUDER 00:e0:29:6c:a4: fd@port11, packet dropped
A  12-17-2004  12:07:04 P.M  PS:INTRUDER 00:50:0f:02:33: b6@port15, packet dropped
A  12-17-2004  12:07:16 P.M  PS:INTRUDER 00:e0:29:2a:f0: 3a@port15, packet dropped
ML3000# clear log informational
 Clear Logged Events? ['Y' or 'N']
ML3000# show log
S  Date       Time        Log Description
-  ----       ----        ---------------
A  12-17-2004  12:05:52 P.M  PS:INTRUDER 00:e0:29:6c:a4: fd@port11, packet dropped
```

The event log records events as single-line entries listed in chronological order, and serves as a tool for isolating problems. Each event log entry is composed of four fields

- **Severity** - the level of severity (see below).
- **Date** - date the event occurred on. See *Date and Time* on page 5–84 for information on setting the date and time on the switch.
- **Time** - time the event occurred on. See *Date and Time* on page 5–84 for information on setting the date and time on the switch
- **Log Description** - description of event as detected by the switch

Severity has one of the following values, and depending on the severity type, is assigned a severity level.

- `I` (information, severity level 1) indicates routine events.
- `A` (activity, severity level 2) indicates the activity on the switch.
- `D` (debug, severity level 3) is reserved for GE Multilin internal diagnostic information
- `C` (critical, severity level 4) indicates that a severe switch error has occurred.
- `F` (fatal, severity level 5) indicates that a service has behaved unexpectedly.

6.2.4 Authorized Managers

Just as port security allows and disallows specific MAC addresses from accessing a network, the ML3000 software can allow or block specific IP addresses or a range of IP addresses to access the switch. The `access` command allows access to configuration mode:

access

The `allow ip` command allows specified services for specified IP addresses. IP addresses can be individual stations, a group of stations or subnets. The range is determined by the IP address and netmask settings.

allow *ip=<ipaddress> mask=<netmask> service=<name|list>*

The `deny ip` command denies access to a specific IP address(es) or a subnet. IP addresses can be individual stations, a group of stations or subnets. The range is determined by the IP address and netmask settings.

deny *ip=<ipaddress> mask=<netmask> service=<name|list>*

The `remove ip` command removes specific IP address(es) or subnet by eliminating specified entry from the authorized manager list.

remove *ip=<ipaddress> mask=<netmask>*

The `removeall` command removes all authorized managers.

removeall

The `show ip-access` command displays a list of authorized managers

show ip-access

It is assumed here that the user is familiar with IP addressing schemes (e.g. class A, B, C, etc.), subnet masking and masking issues such as how many stations are allowed for a given subnet mask.

In Example 6-7, any computer on 3.94.245.10 network is allowed (note how the subnet mask indicates this). Also, a specific station with IP address 3.94.245.25 is allowed (again note how the subnet mask is used). An older station with IP address 3.94.245.15 is removed.

Example 6-7: Allowing/blocking specific IP addresses

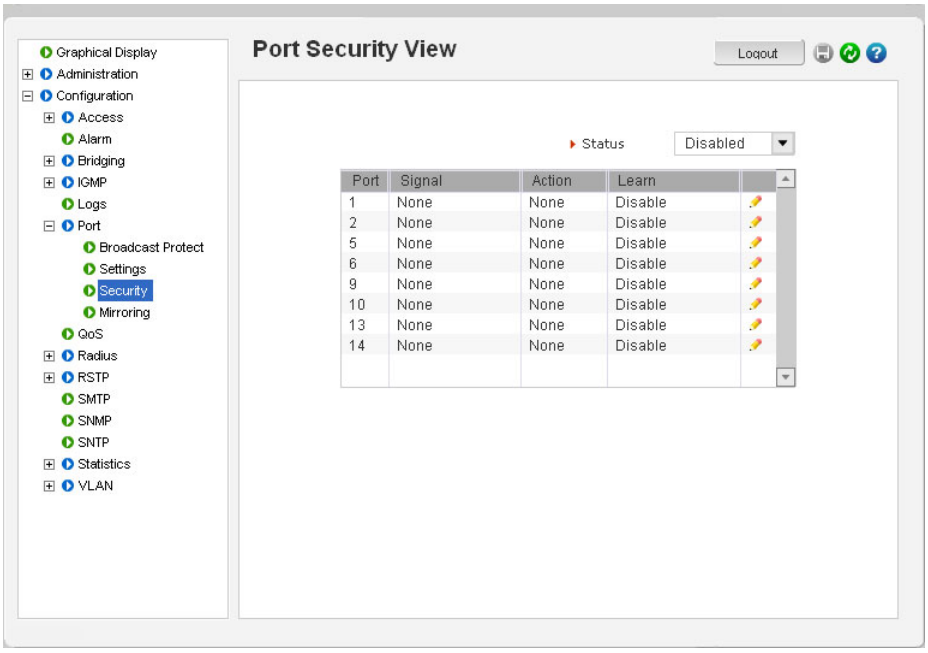
```
ML3000# access
ML3000(access)## allow ip=3.94.245.10 mask=255.255.255.0 service=telnet
 Service(s) allowed for specified address
ML3000(access)## allow ip=3.94.245.25 mask=255.255.255.255 service=telnet
 Service(s) allowed for specified address
ML3000(access)## remove ip=3.94.245.15 mask=255.255.255.255
 Access entry removed
ML3000(access)## exit
ML3000# show ip-access
  ============================================================
  IP Address    | Mask          | Telnet | Web    | SNMP |
  ============================================================
  3.94.245.10     255.255.255.0    ALLOWED  DENIED   DENIED
```

6.3 Configuring Port Security with EnerVista Software

6.3.1 Commands

After enabling the EnerVista Secure Web Management software,

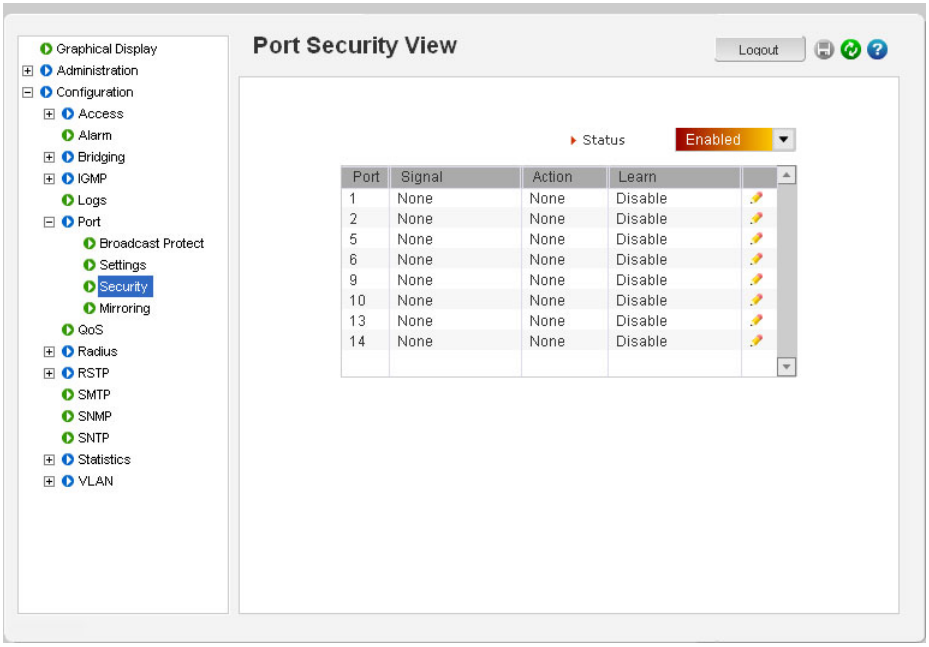
▷ Select the **Configuration > Port > Security** menu item to configure port security as shown below.



From the menu shown above, each individual port can be configured for the proper action on the port, auto learn MAC addresses and specify individual MAC addresses.

▷ To edit each port, click on the edit icon ( ).

▷ To enable or disable port security, use the **Status** drop down menu as shown below.



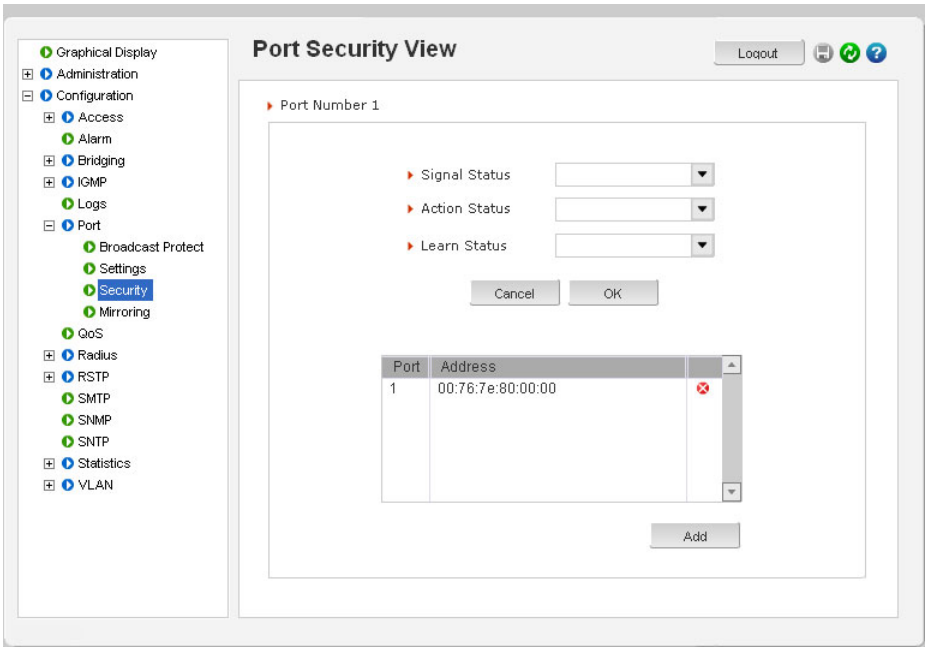
Note that the screen also provides an overview of each port on the switch. Each port can be individually configured for the proper port security action.

Each individual port can be configured by clicking on the edit icon ( ). Once the edit screen is shown, the following actions can be taken for each port:

1. The port can be specified to create a log entry or send a trap, do both or do nothing. This is done through the **Signal Status** drop down menu.
2. The port can be specified to drop the connection, disable the port or do nothing. This is indicated by the **Action Status** drop down menu.
3. The port can be put in the learn mode or the learning can be disabled. This is indicated by the **Learn Status** drop down menu.

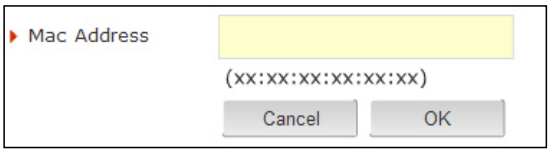
Additionally, MAC addresses can be added or deleted from the table of allowed MAC addresses.

- ▷ To delete a MAC address, click on the delete icon ( ).
- ▷ To add a MAC address, click on the **Add** button and fill in the MAC address in the MAC address window.



There is a limitation of 200 MAC addresses per port and 500 MAC addresses per switch for port security.

After clicking on the **Add** button, the following screen appears, allowing the entry of a specific MAC address

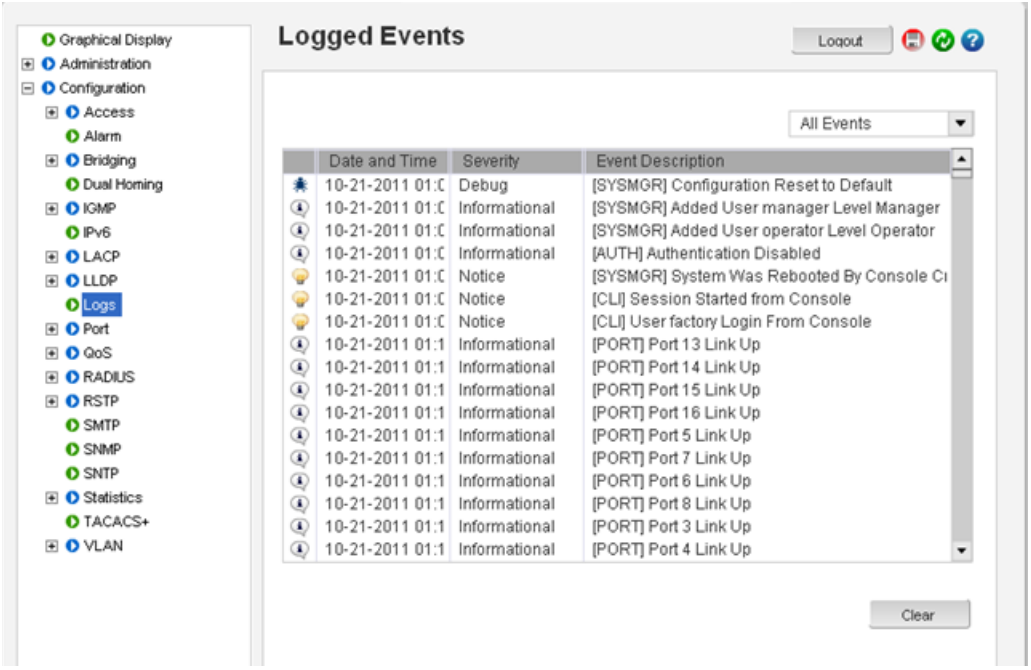


Once port security is setup, it is important to manage the log and review it often. If the signals are sent to the trap receiver, the traps should also be reviewed for intrusion and other infractions.

6.3.2 Logs

All events occurring on the Managed MultiLink switch are logged. The events can be informational (e.g. login, STP synchronization etc.), debugging logs (for debugging network and other values), critical (critical events), activity (traffic activity) and fatal events (such as

unexpected behavior). The specific types of logs can be viewed and cleared. To view the logs in the EnerVista Secure Web Management software, select the **Configuration > Logs** menu item.



Note the different types of logs. Specific logs may be viewed by using the drop down menu in the top right corner

As discussed in the previous section, any port can be set to monitor security as well as make a log on the intrusions that take place. The logs for the intrusions are stored on the switch. When the switch detects an intrusion on a port, it sets an “alert flag” for that port and makes the intrusion information available.

NOTE

The default log size is 50 rows. To change the log size, select the **Configuration > Statistics > Log Statistics** menu item.

When the switch detects an intrusion attempt on a port, it records the date and time stamp, the MAC address, the port on which the access was attempted and the action taken by the MultiLink switches. The event log lists the most recently detected security violation attempts. This provides a chronological entry of all intrusions attempted on a specific port.

The event log records events as single-line entries listed in chronological order, and serves as a tool for isolating problems. Each event log entry is composed of four fields

- **Severity** - the level of severity (see below).
- **Date** - date the event occurred on. See *Date and Time* on page 5–84 for information on setting the date and time on the switch.
- **Time** - time the event occurred on. See *Date and Time* on page 5–84 for information on setting the date and time on the switch
- **Log Description** - description of event as detected by the switch

Severity has one of the following values, and depending on the severity type, is assigned a severity level.

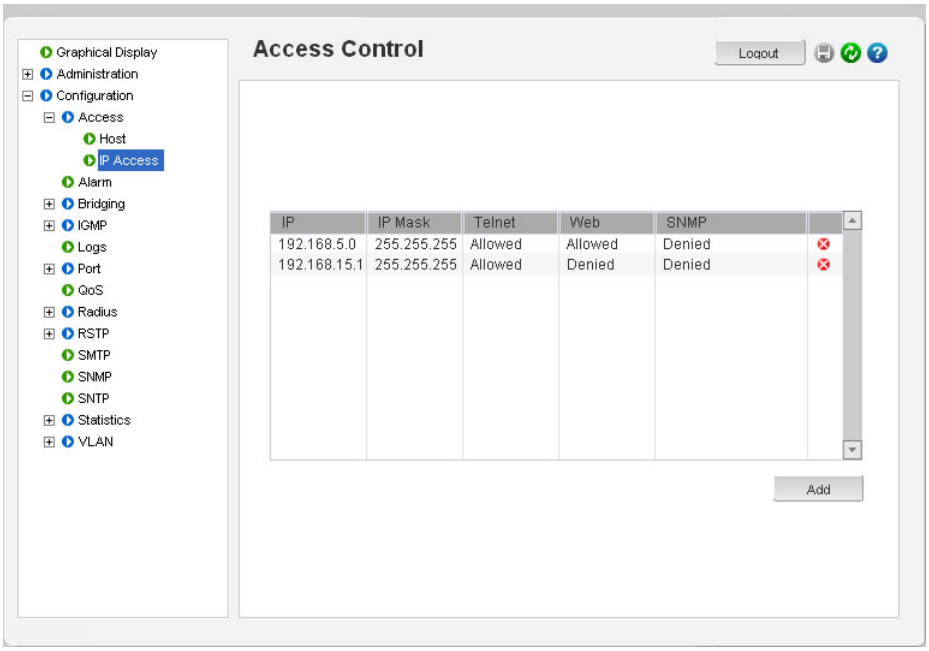
- `I` (information, severity level 1) indicates routine events.
- `A` (activity, severity level 2) indicates the activity on the switch.

- D (debug, severity level 3) is reserved for GE Multilin internal diagnostic information
- C (critical, severity level 4) indicates that a severe switch error has occurred.
- F (fatal, severity level 5) indicates that a service has behaved unexpectedly.

6.3.3 Authorized Managers

Just as port security allows and disallows specific MAC addresses from accessing a network, the EnerVista Secure Web Management software can allow or block specific IP addresses or a range of IP addresses to access the switch.

▷ Access this functionality via the **Configuration > Access > IP Access** menu item.

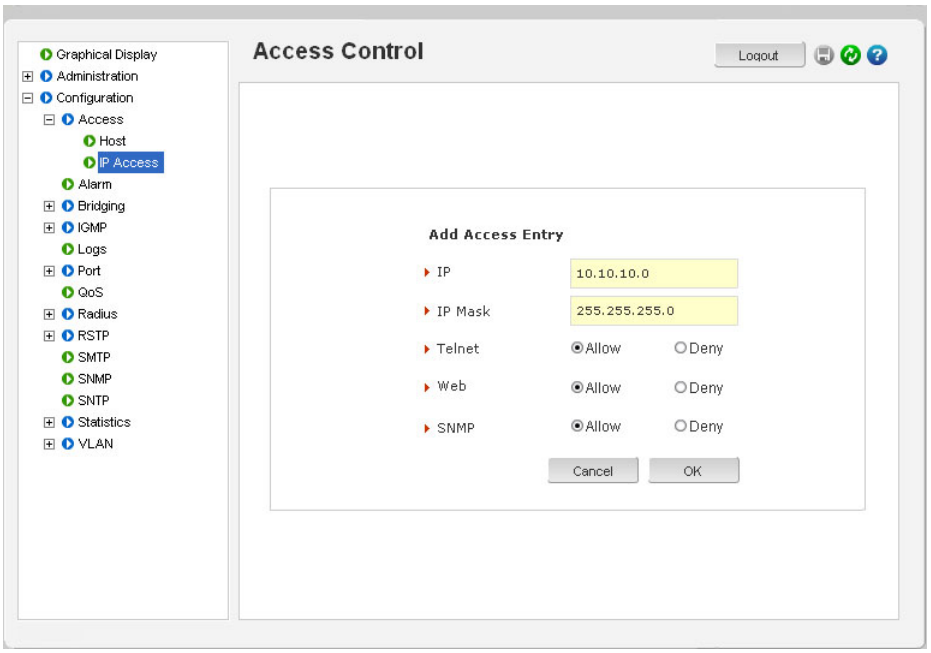


The window above show the authorized access list for managing the switch. Note specific services can be authorized. Also note that individual stations or a group of stations with IP addresses can be authorized.

NOTE

It is assumed that users are familiar with IP addressing schemes (e.g. class A, B, C etc.), subnet masking and masking issues such as how many stations are allowed for a given subnet mask.

In the following example, any computer on 10.10.10.0 sub network is allowed (note how the subnet mask is used to indicate that). Also, a specific station with IP address 192.168.15.25 is allowed (again note how the subnet mask is used to allow only one specific station in the network) and an older station with IP address 192.168.15.15 is removed.


Graphical Display
Administration
Configuration
Access
Host
IP Access
Alarm
Bridging
IGMP
Logs
Port
QoS
Radius
RSTP
SMTP
SNMP
SNTP
Statistics
VLAN
Access Control
Logout
Add Access Entry
IP
10.10.10.0
IP Mask
255.255.255.0
Telnet
Allow
Deny
Web
Allow
Deny
SNMP
Allow
Deny
Cancel
OK

Multilink ML3000/ML3100

Chapter 7: ML3000Access Using RADIUS

7.1 Introduction to 802.1x

7.1.1 Description

Remote Authentication Dial-In User Service or RADIUS is a server that has been traditionally used by many Internet Service Providers (ISP) as well as Enterprises to authenticate dial-in users. Today, many businesses use the RADIUS server for authenticating users connecting into a network. For example, if a user connects PC into the network, whether the PC should be allowed access or not provides the same issues as to whether or not a dial-in user should be allowed access into the network or not. A user has to provide a user name and password for authenticated access. A RADIUS server is well suited for controlling access into a network by managing the users who can access the network on a RADIUS server. Interacting with the server and taking corrective action(s) is not possible on all switches. This capability is provided on the MultiLink family of switches.

RADIUS servers and its uses are also described by one or more RFCs.

7.1.2 802.1x Protocol

There are three major components of 802.1x: - Supplicant, Authenticator and Authentication Server (RADIUS Server). In the figure below, the PC acts as the supplicant. The supplicant is an entity being authenticated and desiring access to the services. The switch is the authenticator. The authenticator enforces authentication before allowing access to services that are accessible via that port. The authenticator is responsible for communication with the supplicant and for submitting the information received from the supplicant to a suitable authentication server. This allows the verification of user

credentials to determine the consequent port authorization state. It is important to note that the authenticator's functionality is independent of the actual authentication method. It effectively acts as a pass-through for the authentication exchange.

FIGURE 7–1: 802.1x network components

The RADIUS server is the authentication server. The authentication server provides a standard way of providing Authentication, Authorization, and Accounting services to a network. Extensible Authentication Protocol (EAP) is an authentication framework which supports multiple authentication methods. EAP typically runs directly over data link layers such as PPP or IEEE 802, without requiring IP. EAP over LAN (EAPOL) encapsulates EAP packets onto 802 frames with a few extensions to handle 802 characteristics. EAP over RADIUS encapsulates EAP packets onto RADIUS packets for relaying to RADIUS authentication servers.

The details of the 802.1x authentication are as follows.

1. The supplicant (host) is initially blocked from accessing the network. The supplicant wanting to access these services starts with an EAPOL-Start frame.
2. The authenticator (MultiLink switch), upon receiving an EAPOL-start frame, sends a response with an EAP-Request/Identity frame back to the supplicant. This will inform the supplicant to provide its identity.
3. The supplicant then sends back its own identification using an EAP-Response/ Identity frame to the authenticator (MultiLink switch.) The authenticator then relays this to the authentication server by encapsulating the EAP frame on a RADIUS-Access-Request packet.
4. The RADIUS server will then send the authenticator a RADIUS-Access-Challenge packet.
5. The authenticator (MultiLink switch) will relay this challenge to the supplicant using an EAP-Request frame. This will request the supplicant to pass its credentials for authentication.
6. The supplicant will send its credentials using an EAP-Response packet.
7. The authenticator will relay using a RADIUS-Access-Request packet.
8. If the supplicant's credentials are valid, RADIUS-Access-Accept packet is sent to the authenticator.
9. The authenticator will then relay this on as an EAP-Success and provides access to the network.
10. If the supplicant does not have the necessary credentials, a RADIUS-Access-Deny packet is relayed to the supplicant as an EAP-Failure frame. The access to the network continues to be blocked.

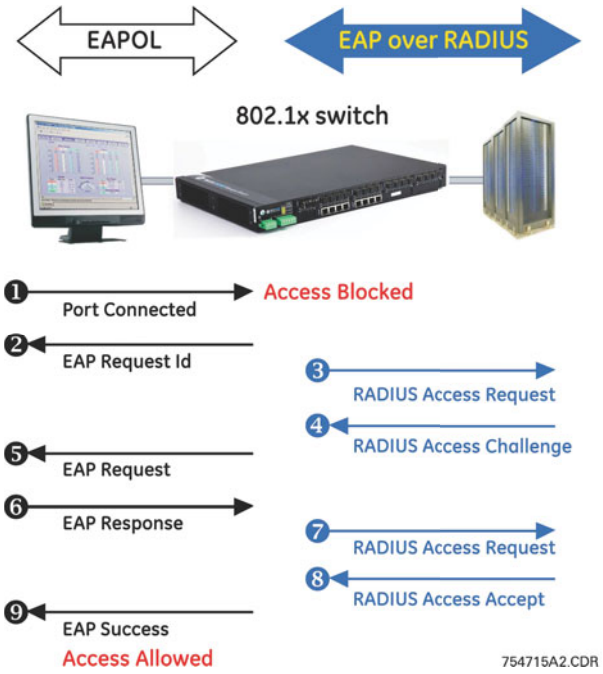


FIGURE 7–2: 802.1x authentication details

The ML3000 software implements the 802.1x authenticator. It fully conforms to the standards as described in IEEE 802.1x, implementing all the state machines needed for port-based authentication. The ML3000 software authenticator supports both EAPOL and EAP over RADIUS to communicate to a standard 802.1x supplicant and RADIUS authentication server.

The ML3000 software authenticator has the following characteristics:

- Allows control on ports using STP-based hardware functions. EAPOL frames are Spanning Tree Protocol (STP) link Bridge PDUs (BPDU) with its own bridge multicast address.
- Relays MD5 challenge (although not limited to) authentication protocol to RADIUS server
- Limits the authentication of a single host per port
- The MultiLink switch provides the IEEE 802.1x MIB for SNMP management

7.2 Configuring 802.1x through the Command Line Interface

7.2.1 Commands

On enabling 802.1x ports, make sure the port which connects to the RADIUS servers needs to be manually authenticated. To authenticate the port, use the `setport` command. The CLI commands to configure and perform authentication with a RADIUS server are described below.

The `auth` command enters the configuration mode to configure the 802.1x parameters.

auth

The `show auth` command displays the 802.1x configuration or port status.

show auth *<config|ports>*

The `authserver` command define the RADIUS server. Use the UDP socket number if the RADIUS authentication is on a port other than 1812.

authserver *[ip=<ip-addr>] [udp=<num>] [secret=<string>]*

The `auth enable` and `auth disable` commands enable or disable the 802.1x authenticator function on the MultiLink switch.

auth *<enable|disable>*

The `setport` command configures the port characteristics for an 802.1x network.

setport *port=<num|list|range> [status=<enable|disable>]*
[control=<auto|forceauth|forceunauth>] [initialize=<assert|deassert>]

The `backend port` command configure the parameters for EAP over RADIUS.

backend *port=<num|list|range>*
[supptimeout=<1-240>]
[servertimeout=<1-240] [maxreq=<1-10>]

The **`port`** argument is mandatory and represents the port(s) to be configured. The **`supptimeout`** argument is optional and represents the timeout in seconds the authenticator waits for the supplicant to respond back. The default value is 30 seconds and values can range from 1 to 240 seconds. The **`servertimeout`** argument is optional and represents the timeout in seconds the authenticator waits for the back-end RADIUS server to respond. The default value is 30 seconds and can range from 1 to 240 seconds. The **`maxreq`** argument is optional and represents the maximum number of times the authenticator will retransmit an EAP request packet to the Supplicant before it times out the authentication session. Its default value is 2 and can be set to any integer value from 1 to 10.

The `portaccess` command sets port access parameters for authenticating PCs or supplicants.

portaccess *port=<num|list|range>*
[quiet=<0-65535>] [maxreauth=<0-10>] [transmit=<1-65535>]

The **`port`** argument is mandatory and identifies the ports to be configured. The **`quiet`** argument is optional and represents the quiet period – the amount of time, in seconds, the supplicant is held after an authentication failure before the authenticator retries the supplicant for connection. The default value is 60 seconds and values can range from 0 to 65535 seconds. The **`maxreauth`** argument is optional and represents the number of re-authentication attempts permitted before the port is unauthorized. The default value is 2 and integer values can range from 0 to 10. The **`transmit`** argument is optional and represents the transmit period. This is the time in seconds the authenticator waits to transmit another request for identification from the supplicant. The default value is 30 and values range from 1 to 65535 seconds

The `reauth` command determines how the authenticator (MultiLink switch) performs the re-authentication with the supplicant or PC.

reauth *port=<num|list|range> [status=<enable|disable>] [period=<10-86400>]*

The port argument is mandatory and sets the ports to be configured. The status argument is optional and enables/disables re-authentication. The period argument is optional and represents the re-authentication period. This is the time in seconds the authenticator waits before a re-authentication process will be performed again to the supplicant. The default value is 3600 seconds (1 hour), and values range from 10 to 86400 seconds.

The `show-stats` command displays 802.1x related statistics.

show-stats *port=<num>*

The `trigger-reauth` command manually initiates a re-authentication of supplicant.

trigger-reauth *port=<num|list|range>*

7.2.2 Example

Example 7-1 demonstrates how to secure the network using port access. Ensure there is no 802.1x or RADIUS server defined. Only one RADIUS server can be defined for the entire network.

Example 7-1: Setting port control parameters

```
802.1X Authenticator Configuration
==================================
Status: Disabled
RADIUS Authentication Server
==================================
 IP Address:      0.0.0.0
 UDP Port:        1812
 Shared Secret:
ML3000# auth
ML3000(auth)## setport port=2 status=enable control=forceauth initialize=assert
 Successfully set port control parameter(s)
ML3000(auth)## auth disable
 802.1X Authenticator is disabled.
ML3000(auth)## authserver ip=3.204.240.1 secret=secret
 Successfully set RADIUS Authentication Server parameter(s)
ML3000(auth)## auth enable
 802.1X Authenticator is enabled.
ML3000(auth)## show auth ports
Port  Status   Control    Initialize  Current State
=====================================================
1    Enabled  Auto       Deasserted  Authorized
2    Enabled  ForcedAuth  Asserted    Unauthorized
3    Enabled  Auto       Deasserted  Authorized
4    Enabled  Auto       Deasserted  Unauthorized
5    Enabled  Auto       Deasserted  Unauthorized
6    Enabled  Auto       Deasserted  Unauthorized
7    Enabled  Auto       Deasserted  Unauthorized
8    Enabled  Auto       Deasserted  Unauthorized
9    Enabled  Auto       Deasserted  Unauthorized
10   Enabled  Auto       Deasserted  Unauthorized
11   Enabled  Auto       Deasserted  Unauthorized
12   Enabled  Auto       Deasserted  Unauthorized
13   Enabled  Auto       Deasserted  Unauthorized
14   Enabled  Auto       Deasserted  Unauthorized
15   Enabled  Auto       Deasserted  Unauthorized
16   Enabled  Auto       Deasserted  Unauthorized
-- Port not available
ML3000(auth)## show auth config
802.1X Authenticator Configuration
==================================
Status: Enabled
RADIUS Authentication Server
==================================
 IP Address:      3.204.240.1
```

The RADIUS server is on port 2. This port is authenticated manually. If the RADIUS server is several hops away, it may be necessary to authenticate the interconnection ports. Make sure the `setport port=2 status=enable control=forceauth initialize=assert` command is executed before the `auth enable` command.

The `auth disable` command is not necessary. However, it is shown for completeness in case a RADIUS server was defined with a previously set authentication scheme.

The RADIUS server is connected on port #2

Setting port control parameters (continued)

```
ML3000(auth)## backend port=2 supptimeout=45 servertimeout=60 maxreq=5

 Successfully set backend server authentication
 parameter(s)

ML3000(auth)## show-port backend

Port  Supp Timeout  Server Timeout  Max Request
      (sec.)        (sec.)
================================================
1       30            30          2
2       45            60          5
3       30            30          2
4       30            30          2
5       30            30          2
6       30            30          2
7       30            30          2
8       30            30          2
9       30            30          2
10      30            30          2
11      30            30          2
12      30            30          2
13      30            30          2
14      30            30          2
15      30            30          2
16      30            30          2

ML3000(auth)## portaccess port=2 quiet=120 maxreauth=7 transmit=120

 Successfully set port access parameter(s)

ML3000(auth)## show-port access

Port  Quiet Period  Max Reauth  Tx Period
      (sec.)       (sec.)
=========================================
1       60          2           30
2       120         7           120
3       60          2           30
4       60          2           30
5       60          2           30
6       60          2           30
7       60          2           30
8       60          2           30
9       60          2           30
10      60          2           30
11      60          2           30
12      60          2           30
13      60          2           30
14      60          2           30
15      60          2           30
16      60          2           30
```

This command sets timeout characteristics and the number of requests before access is denied.

The authenticator waits for the supplicant to respond back for 45 seconds; the authenticator waits for 60 seconds for the back-end RADIUS server to respond back and the authenticator will retransmit an EAP request packet 5 times to the Supplicant before it times out the authentication session.

The time the supplicant is held after an authentication failure before the authenticator retries the supplicant for connection is changed to 120 seconds, the number of re-authentication attempts permitted before the port becomes Unauthorized is set to 7, and the time the authenticator waits to transmit another request for identification from the supplicant is changed to 120 seconds. These values can be changed on all ports depending on devices being authenticated.

(continued on following page)

Setting port control parameters (continued)

```
ML3000(auth)## reauth port=1 status=enable period=300

 Successfully set re-authentication parameter(s)

ML3000(auth)## show-port reauth

Port  Reauth Status  Reauth Period (sec.)
=======================================
1       Enabled       300
2       Enabled       3600
3       Enabled       3600
4       Enabled       3600
5       Enabled       3600
6       Enabled       3600
7       Enabled       3600
8       Enabled       3600
9       Enabled       3600
10      Enabled       3600
11      Enabled       3600
12      Enabled       3600
13      Enabled       3600
14      Enabled       3600
15      Enabled       3600
16      Enabled       3600

ML3000(auth)## show-stats port=3

 Port 3 Authentication Counters

 authEntersConnecting            : 3
 authEapLogoffsWhileConnecting   : 0
 authEntersAuthenticating        : 3
 authAuthSuccessesWhileAuthenticating : 2
 authAuthTimeoutsWhileAuthenticating  : 0
 authAuthFailWhileAuthenticating      : 0
 authAuthReauthsWhileAuthenticating   : 0
 authAuthEapStartsWhileAuthenticating : 1
 authAuthEapLogoffWhileAuthenticating : 0
 authAuthReauthsWhileAuthenticated    : 0
 authAuthEapStartsWhileAuthenticated  : 0
 authAuthEapLogoffWhileAuthenticated  : 0
 backendResponses                : 5
 backendAccessChallenges         : 2
 backendOtherRequestsToSupplicant    : 0
 backendNonNakResponsesFromSupplicant : 2
 backendAuthSuccesses            : 2
 backendAuthFails                : 0

ML3000(auth)## trigger-reauth port=3

 Successfully triggered re-authentication

ML3000(auth)##
```

This command forces the authentication period on port #1 every 5 minutes; all other ports are force authenticated every hour as indicated by the `show-port reauth` command below.

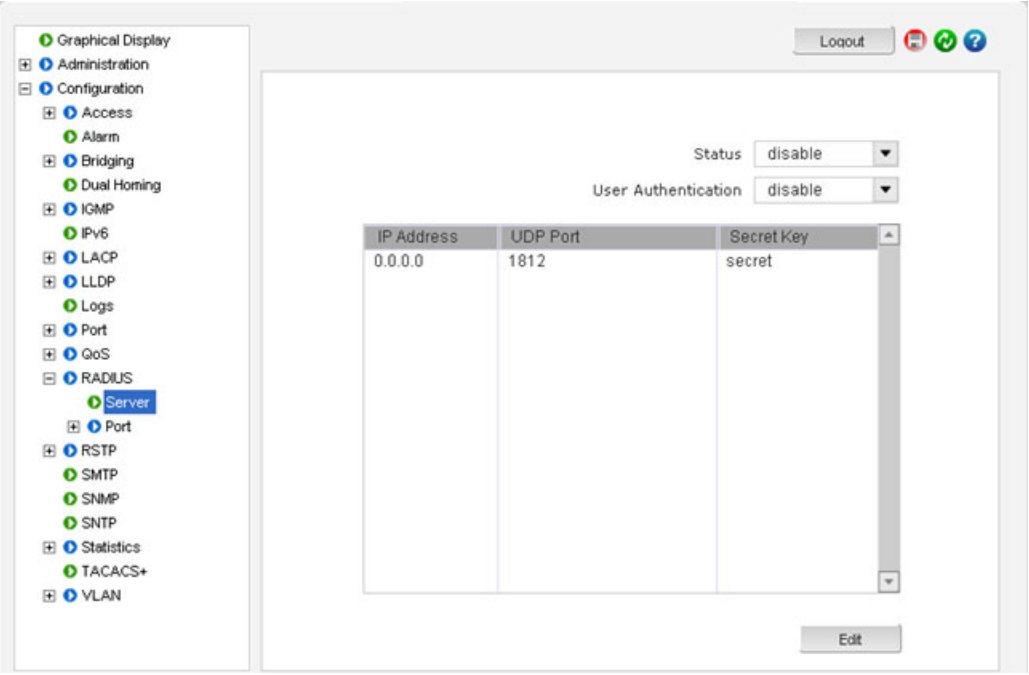
7.3 Configuring 802.1x with EnerVista Secure Web Management software

7.3.1 Commands

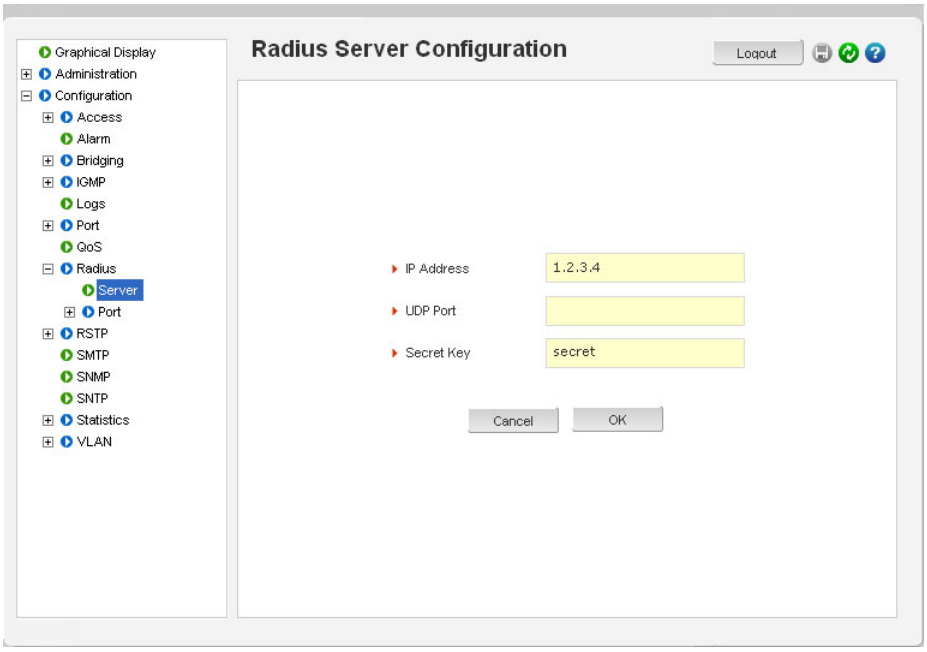
To access the 802.1x configuration window, select the **Configuration > Radius > Server** menu item.

First, select the server. *Do not enable RADIUS capabilities until you have ensured that the ports are configured properly*. After the ports are configured, enable RADIUS. Also ensure that the port connected to the RADIUS server, or the network where the RADIUS server is connected to, is not an authenticated port.

The following window shows the configuration of a RADIUS Server. Initially, the RADIUS Services are disabled and the server IP address is set to 0.0.0.0. Edit the server IP and secret to add a RADIUS server.

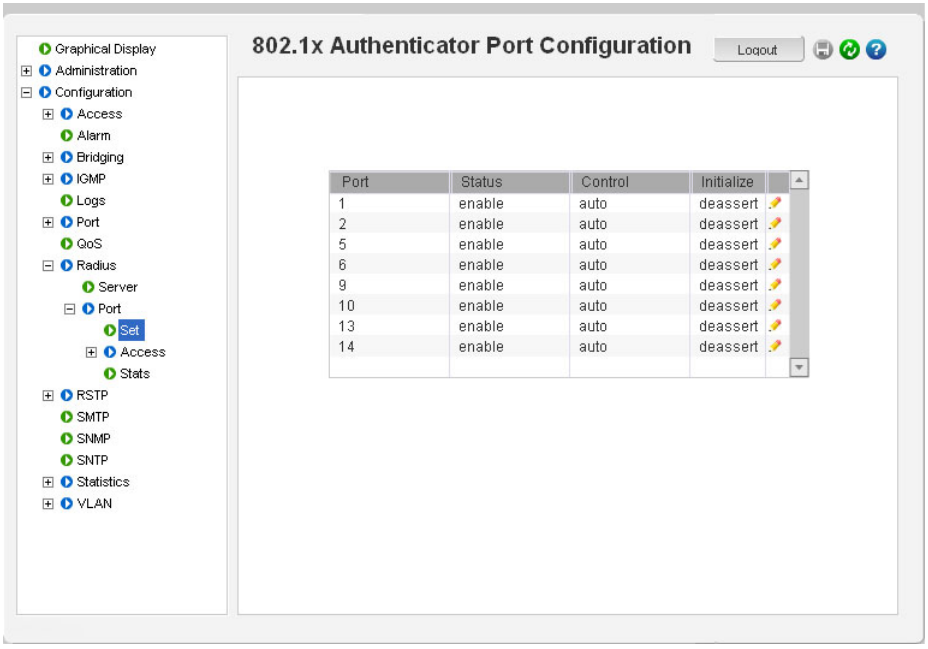


The following figure illustrates the editing of information for the RADIUS server. Note the UDP port number can be left blank and the default port 1812 is used.

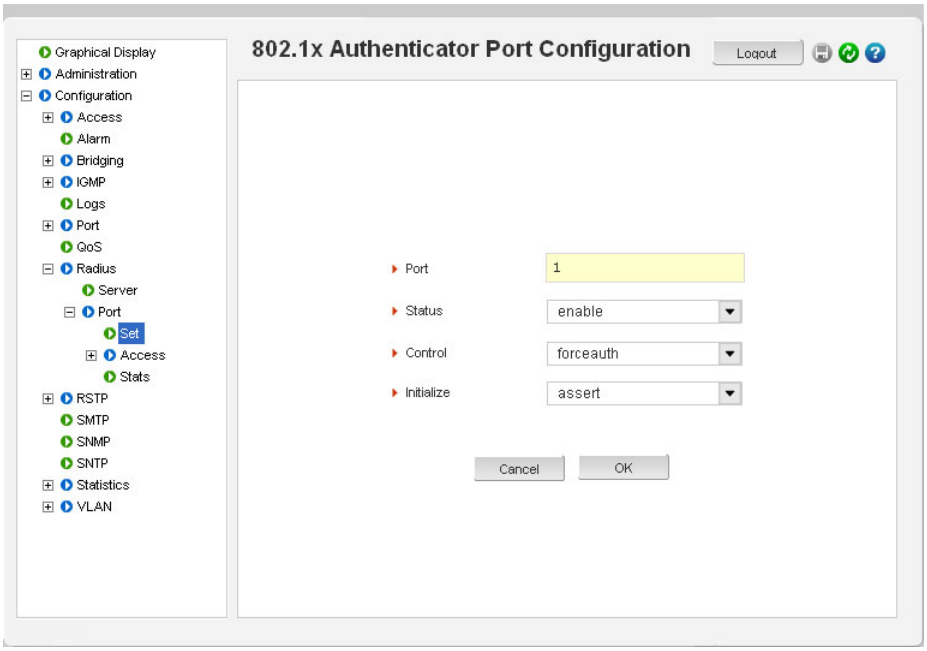


After configuring the server information, specific port information is configured.

- ▷ Select the **Configuration > Radius > Port > Set** menu item to configure the RADIUS characteristics of each port.
- ▷ To edit the port settings, click on the edit icon ( ).

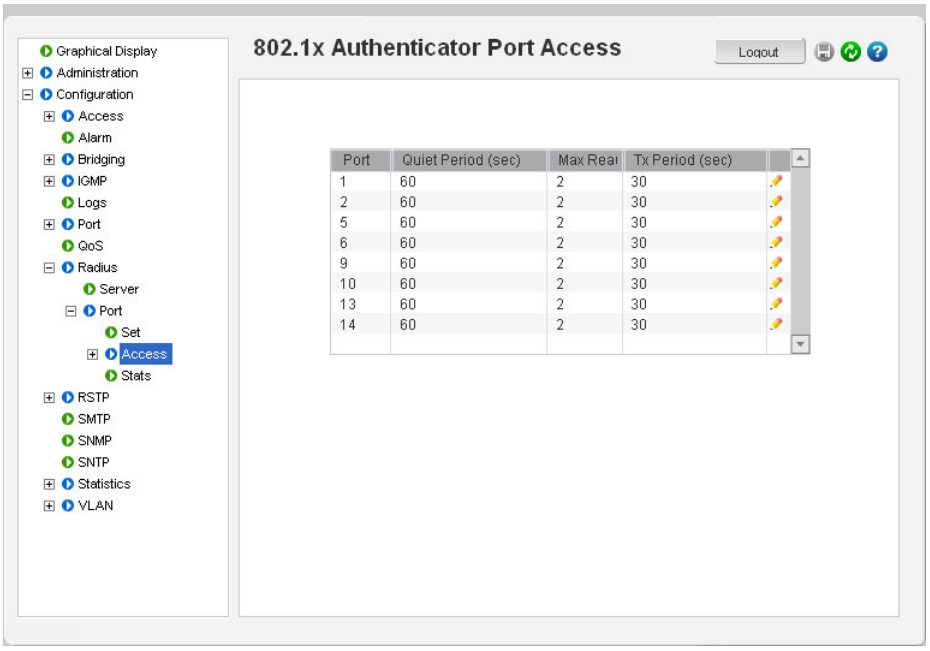


Ensure that the port which has the RADIUS server is force authorized and asserted. For other ports (user ports), it is best to leave the **Control** on auto and **Initialize** on de-asserted.



To change the port access characteristics when authenticating with a RADIUS server,

▷ Select the **Configuration > Radius > Port > Access** menu item.

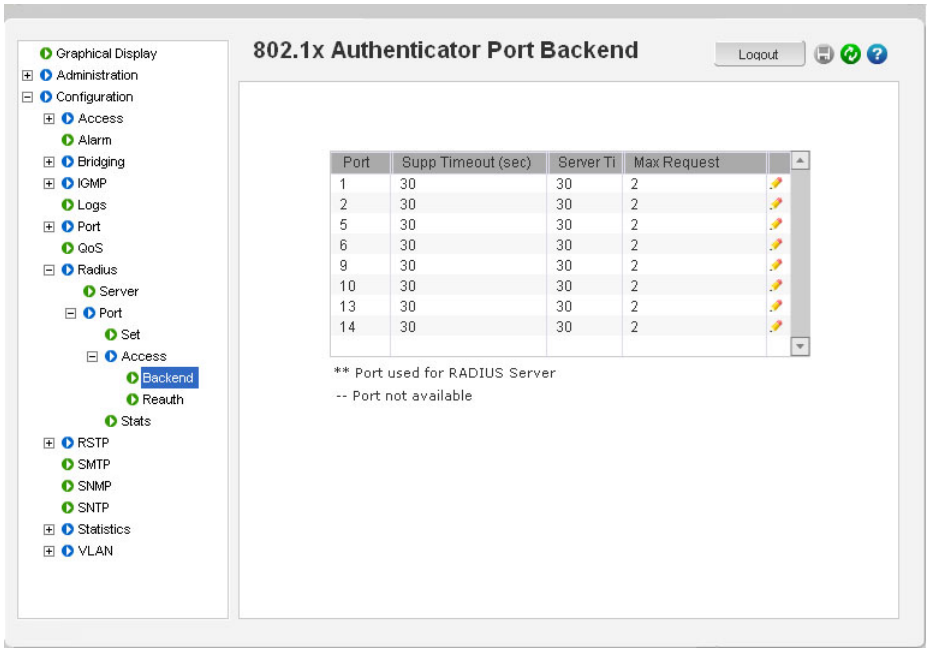


The **Quiet Period** column represents the time, in seconds, the supplicant is held after an authentication failure before the authenticator retries the supplicant for connection. The value ranges from 0 to 65535 seconds, with a default of 60.

The **Max Reauth** column shows the permitted reauthentication attempts before the port becomes unauthorized. Values are integers ranging from 0 to 10, with a default of 2.

The **Tx Period** column represents the transmit period. This is the time (in seconds) the authenticator waits to transmit another request for identification from the supplicant. The values range from 1 to 65535 seconds, with a default of 30.

The backend or communication characteristics between the ML3000 and the RADIUS Server are defined through the **Configuration > Radius > Port > Access > Backend** menu item.

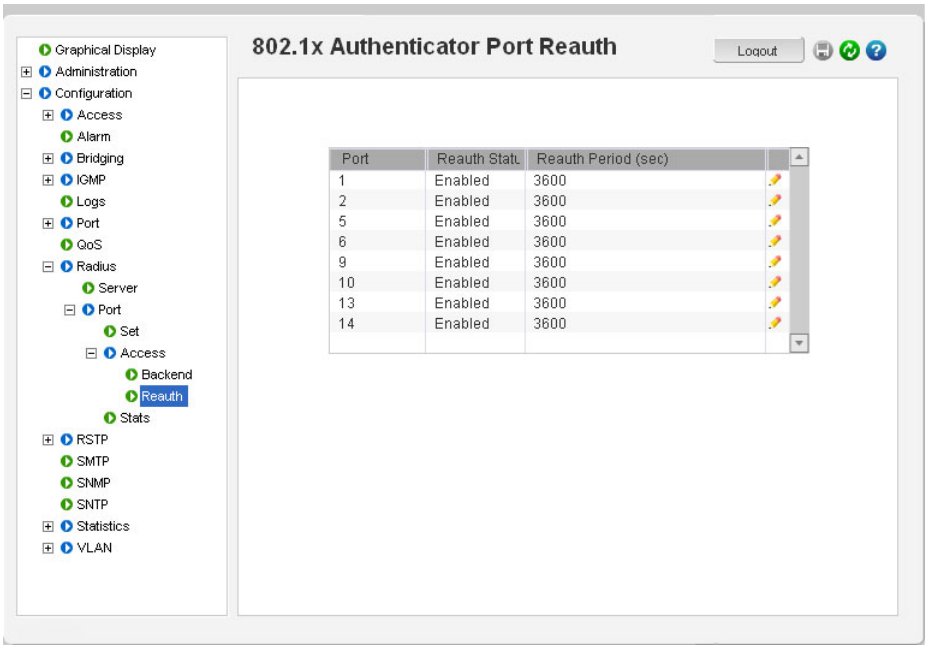


The **Supp Timeout** column represents the timeout the authenticator waits for the supplicant to respond. The values range from 1 to 240 seconds, with a default of 30.

The **Server Timeout** column represents the timeout the authenticator waits for the backend RADIUS server to respond. The values range from 1 to 240 seconds, with a default of 30.

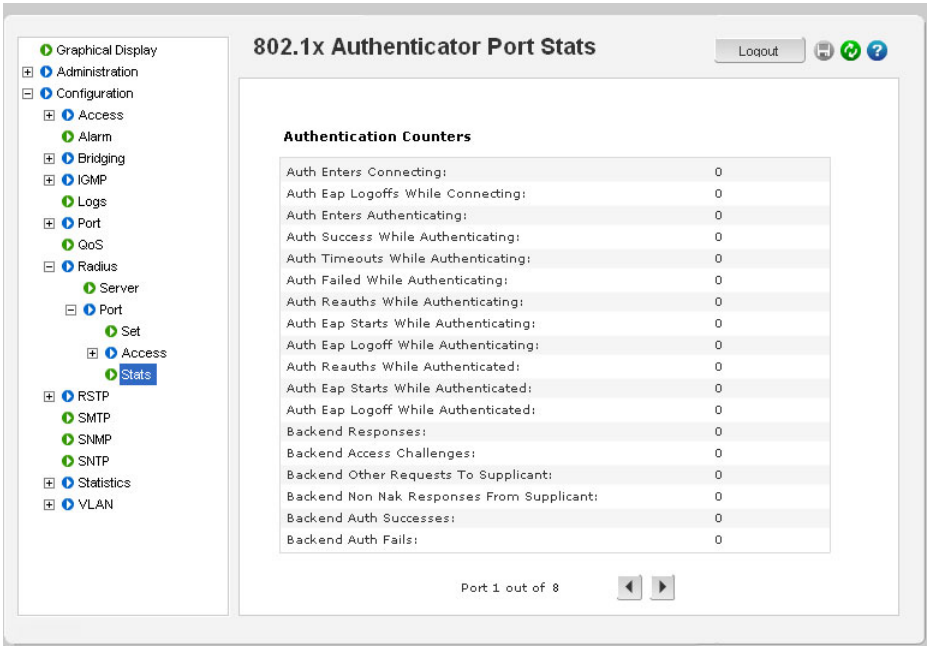
The **Max Request** column represents the maximum times the authenticator retransmits an EAP request packet to the supplicant before it times out. Values are integers ranging from 1 to 10, with a default of 2.

The port authentication characteristics define how the authenticator (ML3000 switch) does the re-authentication with the supplicant or PC. These are defined through the **Configuration > Radius > Port > Access > Reauth** menu item.



The **Reauth Period** represents the time the authenticator waits before a re-authentication process will be done again to the supplicant. Values range from 10 to 86400 seconds, with a default of 3600 (1 hour).

The **Configuration > Radius > Port > Stats** menu item illustrates the radius statistics for each port.



After all the port characteristics are enabled,

▷ **Do not forget** to save the configuration using the Save ( ) icon and enabling RADIUS from the **Configuration > Radius > Server** menu.

Multilink ML3000/ML3100

Chapter 8: Access using TACACS+

8.1 Introduction to TACACS+

8.1.1 Overview

The TACACS+ protocol (short for Terminal Access Controller Access Control System) provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon (server) or simply TACACSD. This server was normally a program running on a host. The host would determine whether to accept or deny the request and sent a response back.

The TACACS+ protocol is the latest generation of TACACS. TACACS is a simple UDP based access control protocol originally developed by BBN for the MILNET (Military Network). XTACACS is now replaced by TACACS+. TACACS+ is a TCP based access control protocol. TCP offers a reliable connection-oriented transport, while UDP offers best-effort delivery.

TACACS+ improves on TACACS and XTACACS by separating the functions of authentication, authorization and accounting and by encrypting all traffic between the Network Access Server (NAS) and the TACACS+ clients or services or daemon. It allows for arbitrary length and content authentication exchanges, which allows any authentication mechanism to be utilized with TACACS+ clients. The protocol allows the TACACS+ client to request very fine-grained access control by responding to each component of a request.

The MultiLink switch implements a TACACS+ client.

1. TACACS+ servers and daemons use TCP port 49 for listening to client requests. Clients connect to this port to send authentication and authorization packets.
2. There can be more than one TACACS+ server on the network. The MultiLink Switch Software supports a maximum of five TACACS+ servers.

8.1.2 TACACS+ Flow

TACACS works in conjunction with the local user list on the ML3000 software (operating system). Please refer to *User Management* on page 1–29 for adding users on the MultiLink Switch Software. The process of authentication as well as authorization is shown in the flow chart below.

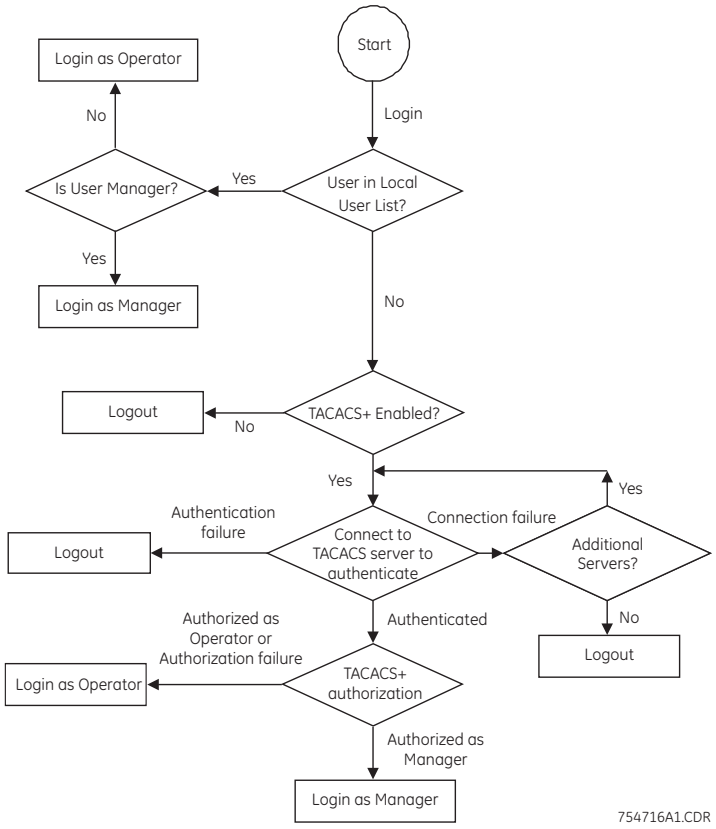


FIGURE 8–1: TACACS Authorization Flowchart

The above flow diagram shows the tight integration of TACACS+ authentication with the local user-based authentication. There are two stages a user goes through in TACACS+. The first stage is authentication where the user is verified against the network user database. The second stage is authorization, where it is determined whether the user has operator access or manager privileges.

8.1.3 TACACS+ Packet

Packet encryption is a supported and is a configurable option for the ML3000 software. When encrypted, all authentication and authorization TACACS+ packets are encrypted and are not readable by protocol capture and sniffing devices such as EtherReal or others. Packet data is hashed and shared using MD5 and secret string defined between the MultiLink switches and the TACACS+ server.

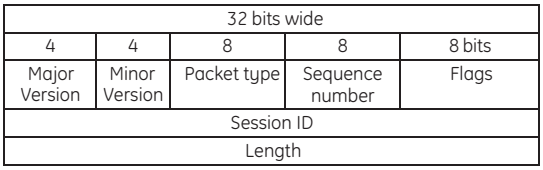


FIGURE 8–2: TACACS packet format

The portions of the TACACS packet are defined as follows:

- **Major Version**: The major TACACS+ version number.
- **Minor version**: The minor TACACS+ version number. This is intended to allow revisions to the TACACS+ protocol while maintaining backwards compatibility.
- **Packet type**: Possible values are:
- TAC_PLUS_AUTHEN:= 0x01 (authentication)
  TAC_PLUS_AUTHOR:= 0x02 (authorization)
  TAC_PLUS_ACCT:= 0x03 (accounting)
- **Sequence number**: The sequence number of the current packet for the current session.
- **Flags**: This field contains various flags in the form of bitmaps. The flag values signify whether the packet is encrypted.
- **Session ID**: The ID for this TACACS+ session.
- **Length**: The total length of the TACACS+ packet body (not including the header).

8.2 Configuring TACACS+ through the Command Line Interface

8.2.1 Commands

There are several commands to configure TACACS+.

The `show tacplus` command displays the status of TACACS or servers configured as TACACS+ servers:

```
ML3000(user)##tacplus

Usage
  tacplus [<enable|disable>] [order=<tac,local|local,tac>
ML3000(user)##tacserver

Usage
  tacserver <add|edit|delete> id=<num> [ip=<ip-addr>] [port=<tcp-port>] [encrypt=<enable|disab
le>] [key=<string>] [mgrlevel=<level>] [oprlevel=<level>]
```

show tacplus *<status|servers>*

The `tacplus enable` and `tacplus disable` commands enable or disable TACACS authentication:

tacplus *[<enable|disable>][order=<tac, local | local, tac]*

The `tacserver` command creates a list of up to five TACACS+ servers:

tacserver

The `<add|delete>` argument is mandatory and specifies whether to add or delete a TACACS+ server. The `id` argument is mandatory and sets the order to poll the TACACS+ servers for authentication. The `ip` argument is mandatory for adding and defines the IP address of the TACACS+ server. The `port` argument is mandatory for deleting and defines the TCP port number on which the server is listening. The `encrypt` argument enables or disables packet encryption and is mandatory for deleting. The `key` argument requires the secret shared key string must be supplied when encryption is enabled.

8.2.2 Example

The example below illustrates how to configure TACACS+.

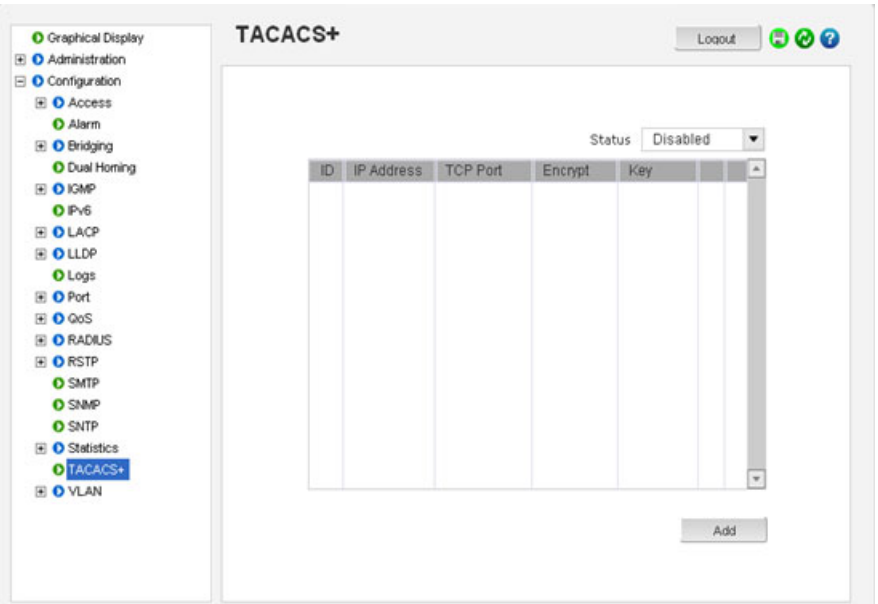
```
ML3000(user)##show tacplus servers

  ID TACACS+ Server   Port   Encrypt    Key        MgrLvl OprLvl
  ========================================================
  1  192.168.100.120  49     Enabled    secret     2      1
  2  --               --     --         --
  3  --               --     --         --
  4  --               --     --         --
  5  --               --     --         --
```

```
ML3000(user)##show tacplus status

  TACACS+ Status           : Disabled
  Authentication Order     : Local, TACPLUS
```

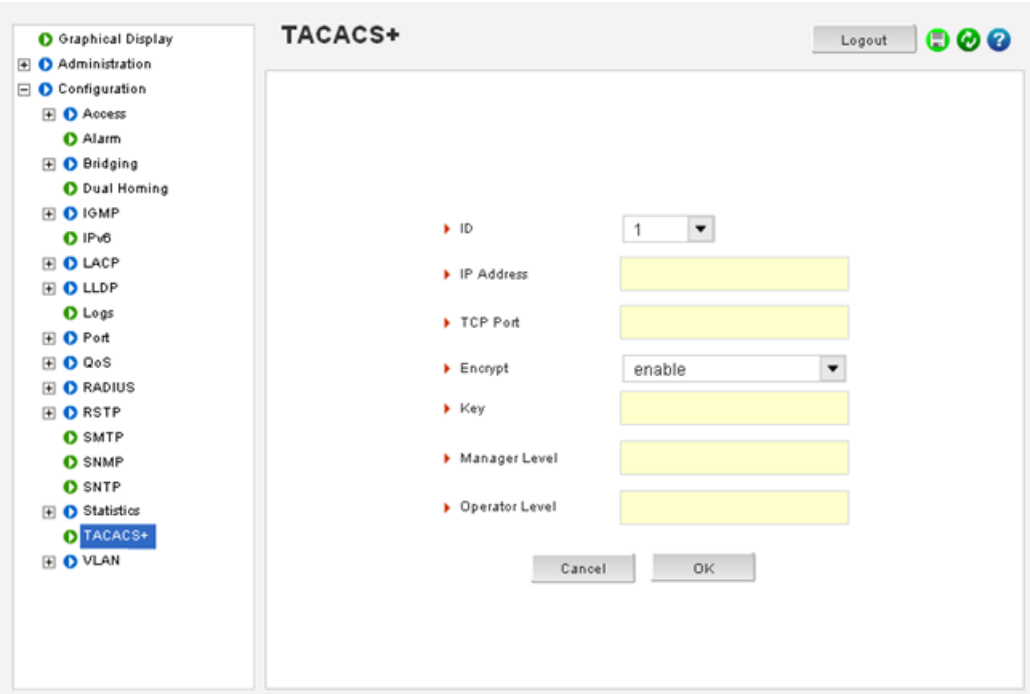
```
ML3000(user)##tacserver add id=2 ip=192.168.100.121 encrypt=enable key=some

  TACACS+ server is added.
ML3000(user)##show tacplus status

  TACACS+ Status           : Enabled
  Authentication Order     : Local, TACPLUS

ML3000(user)##show tacplus servers

  ID TACACS+ Server   Port   Encrypt    Key        MgrLvl OprLvl
  ========================================================
  1  192.168.100.120  49     Enabled    secret     2      1
  2  192.168.100.121  49     Enabled    some       2      1
  3  --               --     --         --
  4  --               --     --         --
  5  --               --     --         --

ML3000(user)##tacserver delete id=2

  TACACS+ server is deleted.
ML3000(user)##show tacplus servers

  ID TACACS+ Server   Port   Encrypt    Key        MgrLvl OprLvl
  ========================================================
  1  192.168.100.120  49     Enabled    secret     2      1
  2  --               --     --         --
  3  --               --     --         --
  4  --               --     --         --
  5  --               --     --         --

ML3000(user)##tacplus disable

  TACACS+ Tunneling is disabled.
ML3000(user)##
```

8.3 Configuring TACACS+ with EnerVista Secure Web Management software

▷ To access the TACACS servers, select the **Configuration > TACACS+** menu item.
By default, no TACACS servers are defined.



▷ To add a server, click on the Add button as shown below.

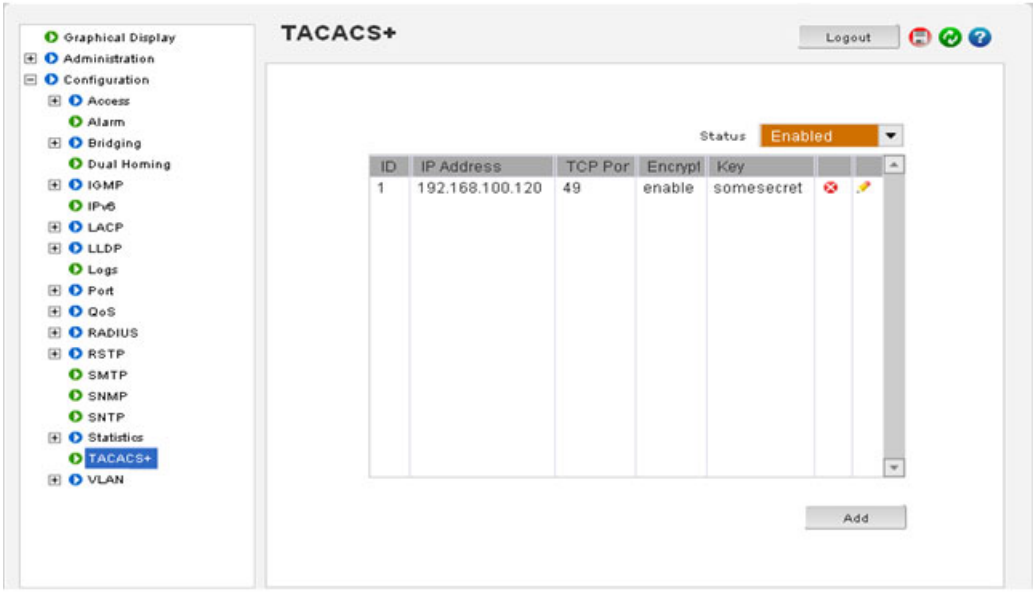


Note that the TCP port field can be left blank – port 49 is used as a default port. Up to five TACACS+ servers can be defined.

After the configuration is completed,

- ▷ Save the settings.
- ▷ Enable the TACACS+ services by using the **Status** drop down menu.

.



Multilink ML3000/ML3100

Chapter 9: Port Mirroring & Setup

9.1 Port Mirroring

9.1.1 Description

This section explains how individual characteristics of a port on a GE MultiLink switch is configured. For monitoring a specific port, the traffic on a port can be mirrored on another port and viewed by protocol analyzers. Other setup includes automatically setting up broadcast storm prevention thresholds.

An Ethernet switch sends traffic from one port to another port. Unlike a switch, a hub or a shared network device, the traffic is “broadcast” on each and every port. Capturing traffic for protocol analysis or intrusion analysis can be impossible on a switch unless all the traffic from a specific port is “reflected” on another port, typically a monitoring port. The MultiLink family of switches can be instructed to repeat the traffic from one port onto another port. This process - when traffic from one port is reflecting to another port - is called port mirroring. The monitoring port is also called a “sniffing” port. Port monitoring becomes critical for trouble shooting as well as for intrusion detection.

9.2 Port Mirroring using the Command Line Interface

9.2.1 Commands

Monitoring a specific port can be done by port mirroring. Mirroring traffic from one port to another port allows analysis of the traffic on that port.

The `show port-mirror` command displays the status of port mirroring:

show port-mirror

The `port-mirror` command enters the port mirror configuration mode.

port-mirror

The `setport monitor` command configures a port mirror.

setport *monitor=<monitor port number> sniffer=<sniffer port number>*

The `prtmr` command enables and disables port mirroring.

prtmr *<enable|disable>*

The sequence below illustrates how port 11 is mirrored on port 13. Any traffic on port 11 is also sent on port 13.

ML3000# `show port-mirror`

Sniffer Port: 0
Monitor Port: 0
Mirroring State: disabled

ML3000# `port-mirror`

ML3000(port-mirror)## `setport monitor=11 sniffer=13`

Port 11 set as Monitor Port
Port 13 set as Sniffer Port

ML3000(port-mirror)## `prtmr enable`

Port Mirroring Enabled

ML3000(port-mirror)## `exit`

ML3000# `show port-mirror`

Sniffer Port: 13
Monitor Port: 11
Mirroring State: enabled

ML3000#

Once port monitoring is completed, GE strongly recommends that the port mirroring be disabled using the `prtmr disable` command for security reasons.

1. Only one port can be set to port mirror at a time.
2. Both the ports (monitored port and mirrored port) have to belong to the same VLAN
3. The mirrored port shows bout incoming as well as outgoing traffic

9.3 Port Setup

9.3.1 Commands

Each port on the GE MultiLink family of switches can be setup specific port characteristics. The commands for setting the port characteristics are shown below.

The `device` command enters the device configuration mode:

device

The `setport` command configures the port characteristics:

setport *port=<port#|list|range> [name=<name>] [speed=<10|100>] [duplex=<half|full>] [auto=<enable|disable>] [flow=<enable|disable>] [bp=<enable|disable>] [status=<enable|disable>] [lla=<enable|disable>]*

The arguments for the `setport` command are defined as follows:

- The `device` argument sets up the MultiLink switch in the device configuration mode.
- The `name` argument assigns a specific name to the port. This name is a designated name for the port and can be a server name, user name or any other name.
- The `speed` argument sets the speed to be 10 or 100 Mbps. This works only with 10/100 ports; the value is ignored and no error shown for 10 Mbps ports.
- The `flow` argument sets up flow control on the port.
- The `bp` argument enables back pressure signaling for traffic congestion management.
- The `status` argument enabled/disables port operation

The show port command displays information about a specific port number.

show port*[=<port number>]*

In Example 9-1, ports 11 and 12 are given specific names. Ports 9 and 13 are active, as shown by the link status. Port 13 is set to 100 Mbps, and all other ports are set to 10 Mbps. All ports are set to auto sensing (speed).

The port `speed` and `duplex` (data transfer operation) settings are summarized below.

The `speed` setting defaults to auto and senses speed and negotiates with the port at the other end of the link for data transfer operation (half-duplex or full-duplex). The "auto" speed detection uses the IEEE 802.3u auto negotiation standard for 100Base-T networks. If the other device does not comply with the 802.3u standard, then the port configuration on the switch must be manually set to match the port configuration on the other device.

Possible port setting combinations for copper ports are:

- 10HDx: 10 Mbps, half-duplex
- 10FDx: 10 Mbps, full-duplex
- 100HDx: 100 Mbps, half-duplex
- 100FDx: 100 Mbps, full-duplex

Possible port settings for 100FX (fiber) ports are:

- 100FDx (default): 100 Mbps, full-duplex
- 100HDx: 100 Mbps, half-duplex

Possible port settings for 10FL (fiber) ports are:

- 10HDx (default): 10 Mbps, half-duplex
- 10FDx: 10 Mbps, full-duplex

Gigabit fiber-optic ports (Gigabit-SX and Gigabit-LX):

- 1000FDx (default): 1000 Mbps, full-duplex only
- Auto: The port operates at 1000FDx and auto-negotiates flow control with the connected device.

Example 9-1: Port setup

```
ML3000# device
ML3000(device)## setport port=11 name=JohnDoe
ML3000(device)## setport port=12 name=JaneDoe
ML3000(device)## show port
Keys: E  = Enable          D  = Disable
    H  = Half Duplex       F  = Full Duplex
    M  = Multiple VLAN's   NA = Not Applicable
    LI = Listening         LE = Learning
    F  = Forwarding        B  = Blocking

Port  Name    Control  Dplx  Media  Link  Speed  Part  Auto  VlanID  GVRP  STP
-------------------------------------------------------------------------------
 9   B1     E      H    10Tx  UP    10    No   E    1     -    -
10   B2     E      H    10Tx  DOWN  10    No   E    1     -    -
11   JohnDoe E     H    10Tx  DOWN  10    No   E    1     -    -
12   JaneDoe E     H    10Tx  DOWN  10    No   E    1     -    -
13   B5     E      F    100Tx UP    100   No   E    1     -    -
14   B6     E      H    10Tx  DOWN  10    No   E    1     -    -
15   B7     E      H    10Tx  DOWN  10    No   E    1     -    -
16   B8     E      H    10Tx  DOWN  10    No   E    1     -    -
```

To change the port speed on a transceiver port, it is required to reboot the switch.

9.3.2 Flow Control

The `flow` setting is disabled by default. In this case, the port will not generate flow control packets and drops received flow control packets. If the `flow` setting is enabled, the port uses 802.3x Link Layer Flow Control, generates flow control packets, and processes received flow control packets.

With the port speed set to auto (the default) and flow control set to enabled; the switch negotiates flow control on the indicated port. If the port speed is not set to auto, or if flow control is disabled on the port, then flow control is not used.

Use the `flowcontrol` command to set flow control:

flowcontrol *xonlimit=<value> xofflimit=<value>*

where `xonlimit` can be from 3 to 127 (default value is 4) and `xofflimit` ranges from 3 to 127 (default value is 6).

9.3.3 Back Pressure

The `backpressure` command disables/enables back pressure based flow control mechanisms. The default state is disabled. When enabled, the port uses 802.3 Layer 2 back off algorithms. Back pressure based congestion control is possible only on half-duplex, 10-Mbps Ethernet ports. Other technologies are not supported on the MultiLink family of switches.

backpressure *rxthreshold=<value>*

where the `rxthreshold` value can be from 4 to 30 (default is 28).

Back pressure and flow control are used in networks where all devices and switches can participate in the flow control and back pressure recognition. In most networks, these techniques are not used as not all devices can participate in the flow control methods and notifications. Alternately, QoS and other techniques are widely used today.

In the example below, the MultiLink family of switches are setup with flow control and back pressure.

Example 9-2: Back pressure and flow control

```
ML3000# device
ML3000(device)## show flowcontrol
 XOnLimit  : 4
 XOffLimit : 6
ML3000(device)## flowcontrol xonlimit=10 xofflimit=15
 XOn Limit set successfully
 XOff Limit set successfully
ML3000(device)## show flowcontrol
 XOnLimit  : 10
 XOffLimit : 15
ML3000(device)## show backpressure
 Rx Buffer Threshold : 28
```

Back pressure and flow control (continued)

```
ML3000(device)## backpressure rxthreshold=30

 Rx Buffer Threshold set successfully

ML3000(device)## show backpressure

 Rx Buffer Threshold : 30

ML3000(device)## show port

Keys:  E  = Enable         D  = Disable
     H  = Half Duplex      F  = Full Duplex
     M  = Multiple VLAN's   NA = Not Applicable
     LI = Listening        LE = Learning
     F  = Forwarding       B  = Blocking

Port  Name    Control  Dplx  Media  Link  Speed  Part  Auto  VlanID  GVRP  STP
--------------------------------------------------------------------------------
 9   B1     E      H    10Tx  UP   10    No   E    1     -    -
10   B2     E      H    10Tx  DOWN 10    No   E    1     -    -
11   JohnDoe E     H    10Tx  DOWN 10    No   E    1     -    -
12   JaneDoe E     H    10Tx  DOWN 10    No   E    1     -    -
13   B5     E      F    100Tx UP   100   No   E    1     -    -
14   B6     E      H    10Tx  DOWN 10    No   E    1     -    -
15   B7     E      H    10Tx  DOWN 10    No   E    1     -    -
16   B8     E      H    10Tx  DOWN 10    No   E    1     -    -

ML3000(device)## show port=11

Configuration details of port 11
-------------------------------------------------
Port Name                 : JohnDoe
Port Link State           : DOWN
Port Type                 : TP Port
Port Admin State          : Enable
Port VLAN ID              : 1
Port Speed                : 10Mbps
Port Duplex Mode          : half-duplex
Port Auto-negotiation State    : Enable
Port STP State            : NO STP
Port GVRP State           : No GVRP
Port Priority Type        : None
Port Security             : Enable
Port Flow Control         : Disable
Port Back Pressure        : Disable
Port Link Loss Alert      : Enabled

ML3000(device)## setport port=11 flow=enable bp=enable
```

(continued on next page)

Back pressure and flow control (continued)

```
ML3000(device)## show port

Keys: E = Enable        D = Disable
      H = Half Duplex   F = Full Duplex
      M = Multiple VLAN's  NA = Not Applicable
      LI = Listening    LE = Learning
      F = Forwarding    B = Blocking

Port Name    Control Dplx Media Link Speed Part Auto VlanID GVRP STP
-------------------------------------------------------------------------------
 9  B1     E     H   10Tx  UP   10   No   E   1    -   -
10  B2     E     H   10Tx  DOWN 10   No   E   1    -   -
11  JohnDoe E    H   10Tx  DOWN 10   No   E   1    -   -
12  JaneDoe E    H   10Tx  DOWN 10   No   E   1    -   -
13  B5     E     F   100Tx UP   100  No   E   1    -   -
14  B6     E     H   10Tx  DOWN 10   No   E   1    -   -
15  B7     E     H   10Tx  DOWN 10   No   E   1    -   -
16  B8     E     H   10Tx  DOWN 10   No   E   1    -   -

ML3000(device)## show port=11

Configuration details of port 11
-----------------------------------------------------
Port Name                 : JohnDoe
Port Link State           : DOWN
Port Type                 : TP Port
Port Admin State          : Enable
Port VLAN ID              : 1
Port Speed                : 10Mbps
Port Duplex Mode          : half-duplex
Port Auto-negotiation State   : Enable
Port STP State            : NO STP
Port GVRP State           : No GVRP
Port Priority Type        : None
Port Security             : Enable
```

Note that the flow control and back pressure is shown as enabled for the specific port. The global `show port` command does not provide this detail. The back pressure and flow control parameters are global – i.e., the same for all ports.

9.3.4 Broadcast Storms

One of the best features of the MultiLink family of switches is its ability to keep broadcast storms from spreading throughout a network. Network storms (or broadcast storms) are characterized by an excessive number of broadcast packets being sent over the network. These storms can occur if network equipment is configured incorrectly. Storms can reduce network performance and cause bridges, routers, workstations, servers and PCs to slow down or even crash.

The MultiLink family of switches is capable of detecting and limiting storms on each port. A network administrator can also set the maximum rate of broadcast packets (frames) that are permitted from a particular interface. If the maximum number is exceeded, a storm condition is declared. Once it is determined that a storm is occurring on an interface, any additional broadcast packets received on that interface will be dropped until the storm is determined to be over. The storm is determined to be over when a one-second period elapses with no broadcast packets received.

The `braoadcast-protect` command enables or disables the broadcast storm protection capabilities.

broadcast-protect *<enable|disable>*

The rate-threshold command set the rate limit in frames per second.

rate-threshold *port=<port|list|range> rate=<frames/sec>*

The `show broadcast-protect` command displays the broadcast storm protection settings

show broadcast-protect

In Example 9-3, the broadcast protection is turned on. The threshold for port 11 is then set to a lower value of 3500 broadcast frames/second.

Example 9-3: Preventing broadcast storms

```
ML3000# device
ML3000(device)## show broadcast-protect

==========================================================================
PORT |  STATUS  | THRESHOLD (frms/sec) | CURR RATE (frms/sec) | ACTIVE
==========================================================================
 9    Disabled   19531          0          NO
 10   Disabled   19531          0          NO
 11   Disabled   19531          0          NO
 12   Disabled   19531          0          NO
 13   Disabled   19531          0          NO
 14   Disabled   19531          0          NO
 15   Disabled   19531          0          NO
 16   Disabled   19531          0          NO

ML3000(device)## broadcast-protect enable

 Broadcast Storm Protection enabled

ML3000(device)## show broadcast-protect

==========================================================================
PORT |  STATUS  | THRESHOLD (frms/sec) | CURR RATE (frms/sec) | ACTIVE
==========================================================================
 9    Enabled    19531          0          NO
 10   Enabled    19531          0          NO
 11   Enabled    19531          0          NO
 12   Enabled    19531          0          NO
 13   Enabled    19531          0          NO
 14   Enabled    19531          0          NO
 15   Enabled    19531          0          NO
 16   Enabled    19531          0          NO

ML3000(device)## rate-threshold port=11 rate=3500

 Broadcast Rate Threshold set

ML3000(device)## show broadcast-protect

==========================================================================
PORT |  STATUS  | THRESHOLD (frms/sec) | CURR RATE (frms/sec) | ACTIVE
==========================================================================
 9    Enabled    19531          0          NO
 10   Enabled    19531          0          NO
 11   Enabled    3500           0          NO
 12   Enabled    19531          0          NO
 13   Enabled    19531          0          NO
```

9.3.5 Link Loss Alert

The GE Multilin Universal Relay (UR) family and the F650 family of relays have redundant Ethernet ports that allow for automatic switching to their secondary ports when they detect the primary path is broken. The MultiLink switches can compensate for situations where only the switch receiver fiber cable is broken. Upon detection of the broken receiver link, the ML3000 will cease sending link pulses through the relay's receive fiber cable, thereby allowing the relay to switch to its secondary path.

It is recommended to enable the Link Loss Alert (LLA) feature on ports that are connected to end devices. LLA should be disabled for switch ports connected in a ring.

The Link Loss Alert feature is enabled by default on 10 MB Fiber Optic ports, and disabled by default on 100 MB Fiber Optic ports. It can be enabled and disabled via the `lla` parameter in the `setport` command as follows:

setport port=<port#|list|range> [lla=<enable|disable>]

The following example illustrates how to enable the link loss alert feature.

Example 9-4: Link loss alert

```
ML3000# device
ML3000(device)## setport port=11 lla=disable
ML3000(device)## show port=11
Configuration details of port 11
-------------------------------------------------
Port Name                : JohnDoe
Port Link State          : DOWN
Port Type                : TP Port
Port Admin State         : Enable
Port VLAN ID             : 1
Port Speed               : 10Mbps
Port Duplex Mode         : half-duplex
Port Auto-negotiation State    : Enable
Port STP State           : NO STP
Port GVRP State          : No GVRP
Port Priority Type       : None
Port Security            : Enable
Port Flow Control        : Enable
Port Back Pressure       : Enable
Port Link Loss Alert     : Disable
ML3000(device)## setport port=11 lla=enable
 Link Loss Alert enabled
ML3000(device)## show port=11
Configuration details of port 11
-------------------------------------------------
Port Name                : JohnDoe
Port Link State          : DOWN
Port Type                : TP Port
Port Admin State         : Enable
Port VLAN ID             : 1
Port Speed               : 10Mbps
Port Duplex Mode         : half-duplex
Port Auto-negotiation State    : Enable
Port STP State           : NO STP
Port GVRP State          : No GVRP
Port Priority Type       : None
Port Security            : Enable
```

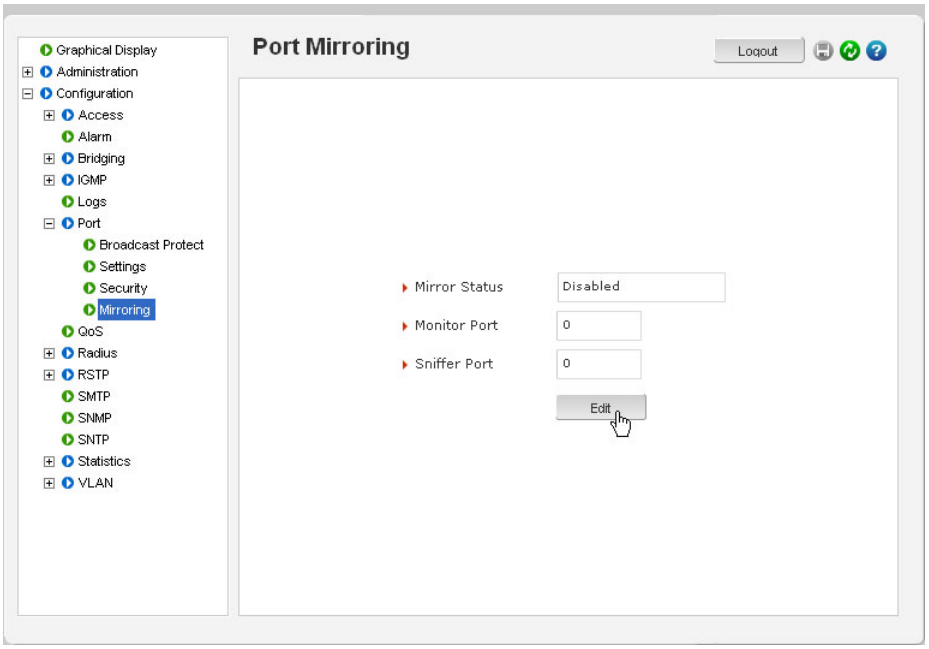
9.4 Port Mirroring using EnerVista Secure Web Management software

9.4.1 Commands

Monitoring a specific port can be done by port mirroring. Mirroring traffic from one port to another port allows analysis of the traffic on that port.

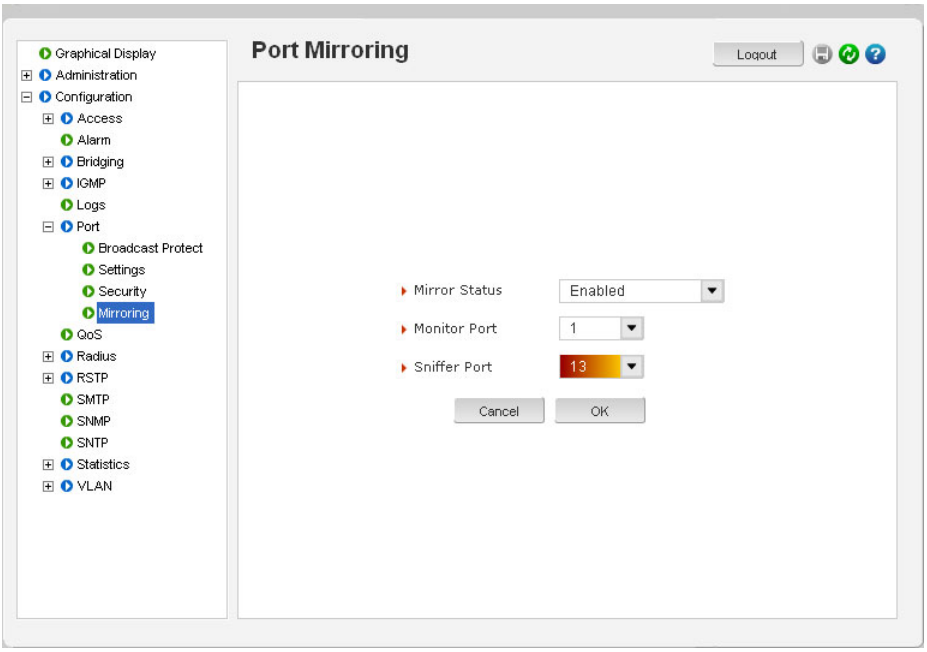
To enable port mirroring as well as setting up the ports to be “sniffed”,

▷ Select the **Configuration > Port > Mirroring** menu item.



▷ Set the sniffer port and the port on which the traffic is reflected.

▷ Make sure the **Mirror Status** is also set to enabled for mirroring:



For security reasons, GE Multilin recommends that the port mirroring be disabled using the **Edit** button and setting the **Mirror Status** to off once port monitoring is completed.

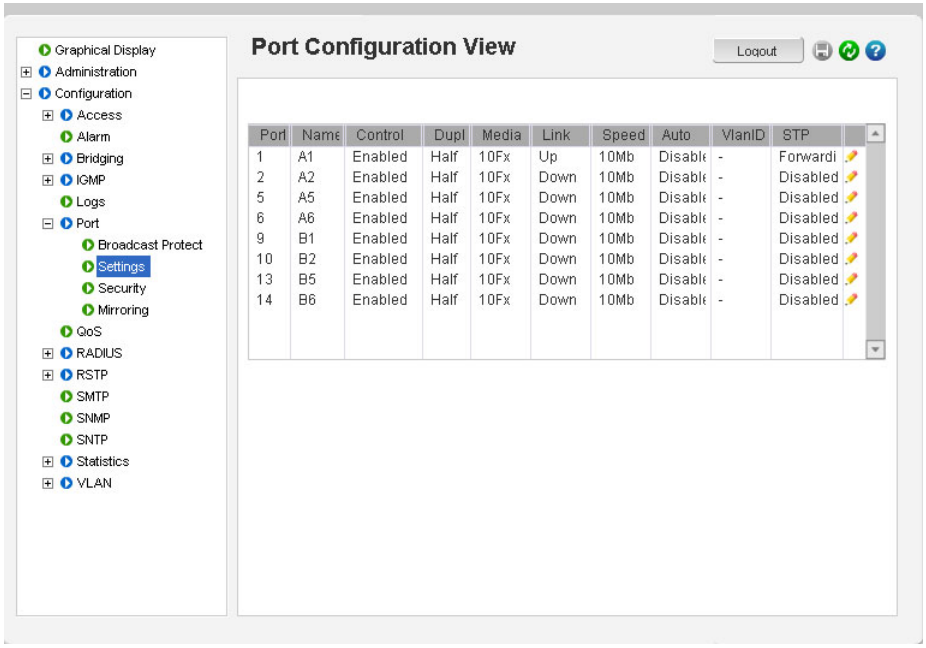
Note that:

1. Only one port can be set to port mirror at a time.
2. Both the ports (monitored port and mirrored port) have to belong to the same VLAN.
3. The mirrored port shows both incoming as well as outgoing traffic.

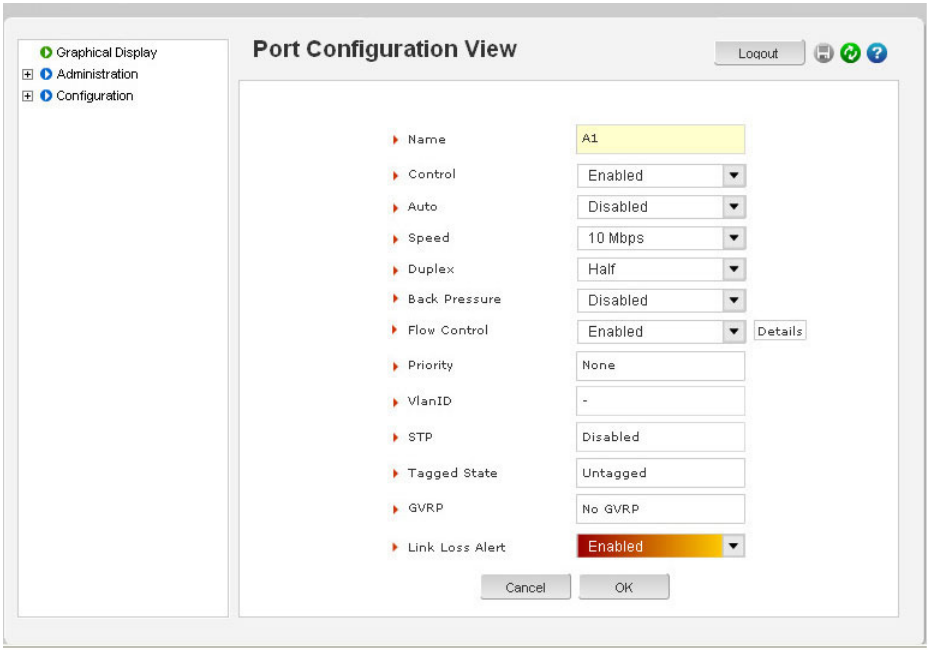
9.4.2 Port Setup

With the ML3000, the specific characteristics of each port can be individually programmed.

▷ Select a specific port by using the edit icon in the **Configuration > Port > Settings** menu.



▷ Click the edit icon to open the following window.



In these windows:

- **Port Number** represents the port number on the switch.
- **Port Name** assigns a specific name to the port. This name is a designated name for the port and can be a server name, user name or any other name.
- **Admin Status** indicates whether the port can be administered remotely.

- **Link** indicates the link status. In the figure above the link is down, implying either there is no connection or the system connected to the port is turned off.
- **Auto-Neg** sets auto negotiation for 100 Mbps and Gigabit copper ports. There is no no auto negotiation for fiber ports as their speeds are fixed.
- The **Port Speed** sets the speed to be 10 or 100 Mbps. This settings works only with 10/100 ports; it is ignored for 10 Mbps ports.
- The **Duplex** setting selects full duplex or half duplex capabilities for 10/100 Mbps ports.
- The **Back Pressure** displays the state of the back pressure setting on the port. This value can be edited in this window.
- The **Flow Control** displays the state of the flow control setting on the port. This value can be edited in this window.
- **Priority** displays the priority set for the port. This value cannot be edited in this window.
- The **VLAN ID** displays the VLAN set for the port. This value cannot be edited in this window.
- The **STP State** displays the STP settings for the port. This value cannot be edited in this window.
- The **Tagged State** displays the Tag settings on the port. This value cannot be edited in this window.
- The **GVRP State** displays the GVRP settings on the port. This value cannot be edited in this window.
- The **LLA** indicates the state of the Link Loss Alert feature.

The "Auto" (default) value for the **Port Speed** senses the speed and negotiates with the port at the other end of the link for data transfer operation (half-duplex or full-duplex). The "Auto" value uses the IEEE 802.3u auto negotiation standard for 100Base-T networks. If the other device does not comply with the 802.3u standard, then the port configuration on the switch must be manually set to match the port configuration on the other device.

Possible port setting combinations for copper ports are:

- 10HDx: 10 Mbps, half-duplex
- 10FDx: 10 Mbps, full-duplex
- 100HDx: 100 Mbps, half-duplex
- 100FDx: 100 Mbps, full-duplex

Possible port settings for 100FX (fiber) ports are:

- 100FDx (default): 100 Mbps, full-duplex
- 100HDx: 100 Mbps, half-duplex

Possible port settings for 10FL (fiber) ports are:

- 10HDx (default): 10 Mbps, half-duplex
- 10FDx: 10 Mbps, full-duplex

Possible port settings for Gigabit fiber-optic ports (Gigabit-SX and Gigabit-LX) are:

- 1000FDx (default): 1000 Mbps (1 GBPS), full duplex only
- Auto: The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port

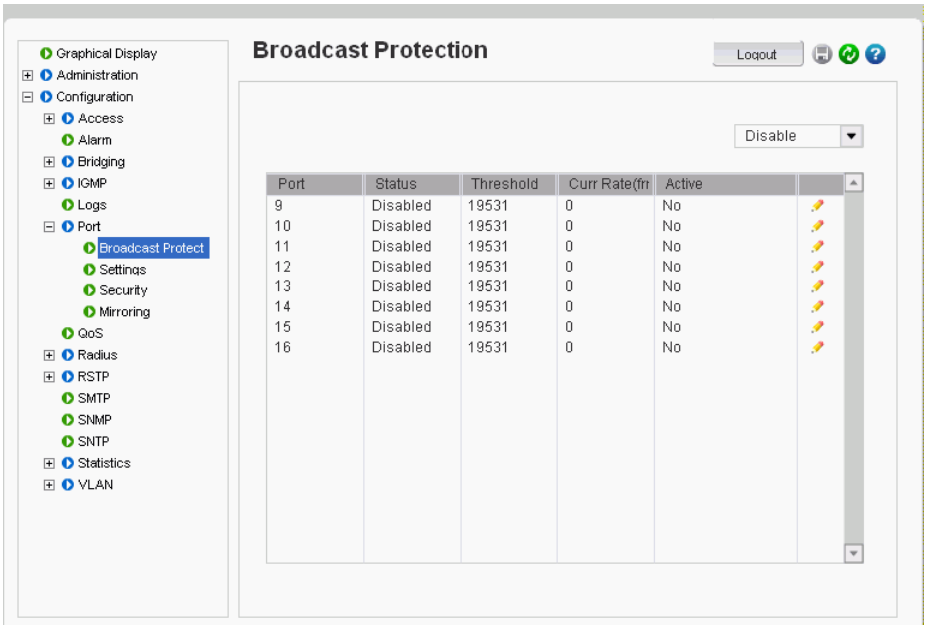
To change the port speed on a transceiver port, the switch must be rebooted

9.4.3 Broadcast Storms

One of the best features of the GE MultiLink switch is its ability to keep broadcast storms from spreading throughout a network. Network storms (or broadcast storms) are characterized by an excessive number of broadcast packets being sent over the network. These storms can occur if network equipment is configured incorrectly or the network software is not properly functioning or badly designed programs (including some network games) are used. Storms can reduce network performance and cause bridges, routers, workstations, servers and PCs to slow down or even crash.

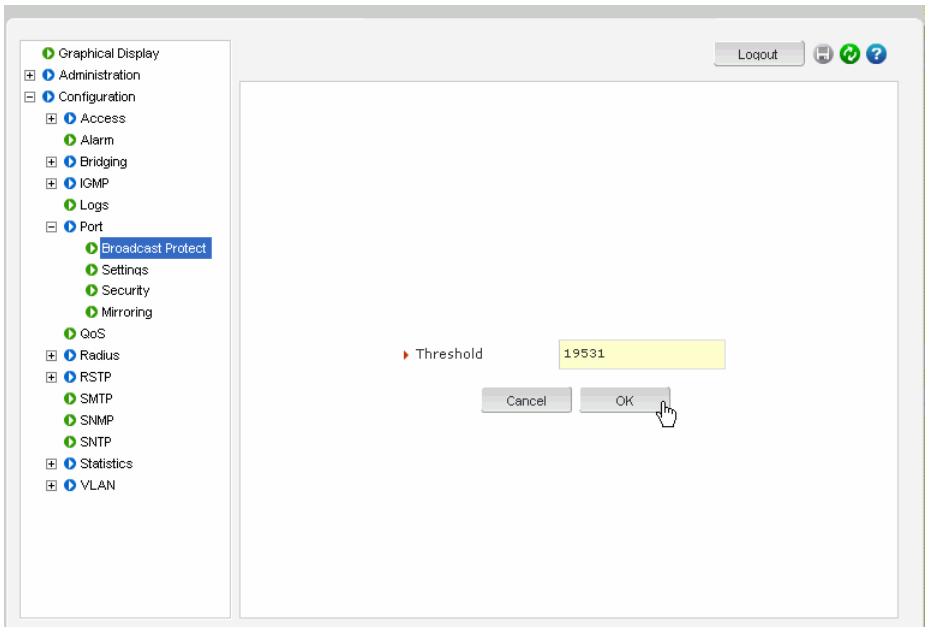
The GE MultiLink switch is capable of detecting and limiting storms on each port. A network administrator can also set the maximum rate of broadcast packets (frames) that are permitted from a particular interface. If the maximum number is exceeded, a storm condition is declared. Once it is determined that a storm is occurring on an interface, any additional broadcast packets received on that interface will be dropped until the storm is determined to be over. The storm is determined to be over when a one-second period elapses with no broadcast packets received.

Broadcast storm protection can be configured through the **Configuration > Port > Broadcast Storm** menu.



▷ To edit the threshold level, click on the edit icon as seen below.

See details in *Broadcast Storms* on page 9–156 to determine the threshold level.



▷ After changes are made, **do not forget** to save the changes using the save icon ( ).
If the switch is rebooted before the changes are made, the changes will be lost.

Multilink ML3000/ML3100

Chapter 10: VLAN

10.1 VLAN Description

10.1.1 Overview

Short for virtual LAN (VLAN), a VLAN creates separate broadcast domains or network segments that can span multiple MultiLink switches. A VLAN is a group of ports designated by the switch as belonging to the same broadcast domain. The IEEE 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames.

VLANs provide the capability of having two (or more) Ethernet segments co-exist on common hardware. The reason for creating multiple segments in Ethernet is to isolate broadcast domains. VLANs can isolate groups of users, or divide up traffic for security, bandwidth management, etc. VLANs are widely used today and are here to stay. VLANs need not be in one physical location. They can be spread across geography or topology. VLAN membership information can be propagated across multiple MultiLink switches.

The following figure illustrates a VLAN as two separate broadcast domains. The top part of the figure shows two "traditional" Ethernet segments. Up to 32 VLANs can be defined per switch.

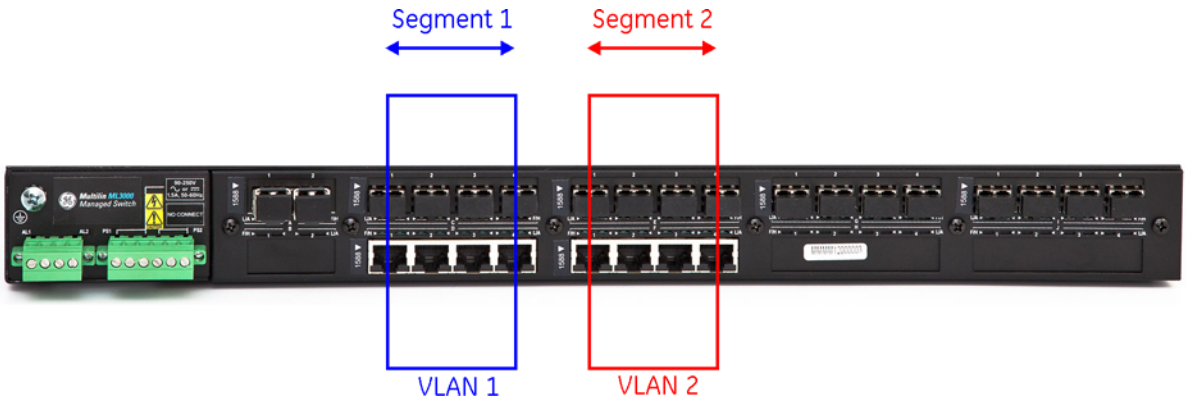


FIGURE 10–1: VLAN as two separate broadcast domains

A group of network users (ports) assigned to a VLAN form a broadcast domain. Packets are forwarded only between ports that are designated for the same VLAN. Cross-domain broadcast traffic in the switch is eliminated and bandwidth is saved by not allowing packets to flood out on all ports. For many reasons a port may be configured to belong to multiple VLANs.

As shown below, ports can belong to multiple VLANs. In this figure, a simplistic view is presented where some ports belong to VLANs 1, 2 and other ports belong to VLANs 2,3. Ports can belong to VLANs 1, 2 and 3. This is not shown in the figure.

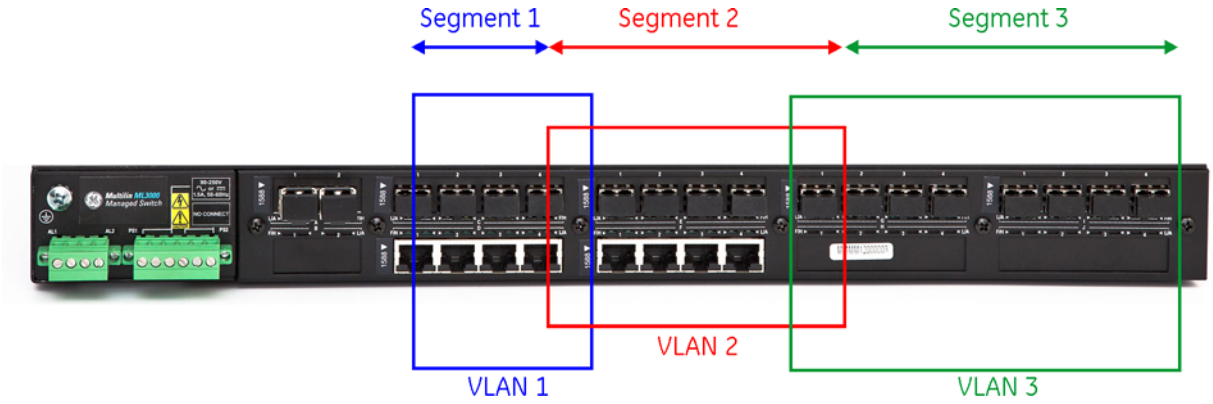


FIGURE 10–2: Ports assigned to multiple VLANs

By default, on the MultiLink family of switches, VLAN support is enabled and all ports on the switch belong to the default VLAN (DEFAULT-VLAN). This places all ports on the switch into one physical broadcast domain.

If VLANs are entirely separate segments or traffic domains - how can the VLANs route traffic (or "talk") to each other? This can be done using routing technologies (e.g., a router or a L3-switch). The routing function can be done internally to a L3-switch. One advantage of an L3 switch is that the switch can also support multiple VLANs. The L3 switch can thus route traffic across multiple VLANs easily and provides a cost effective solution if there are may VLANs defined.

As shown below, routing between different VLANs is performed using a router or a Layer 3 switch (L3-switch)

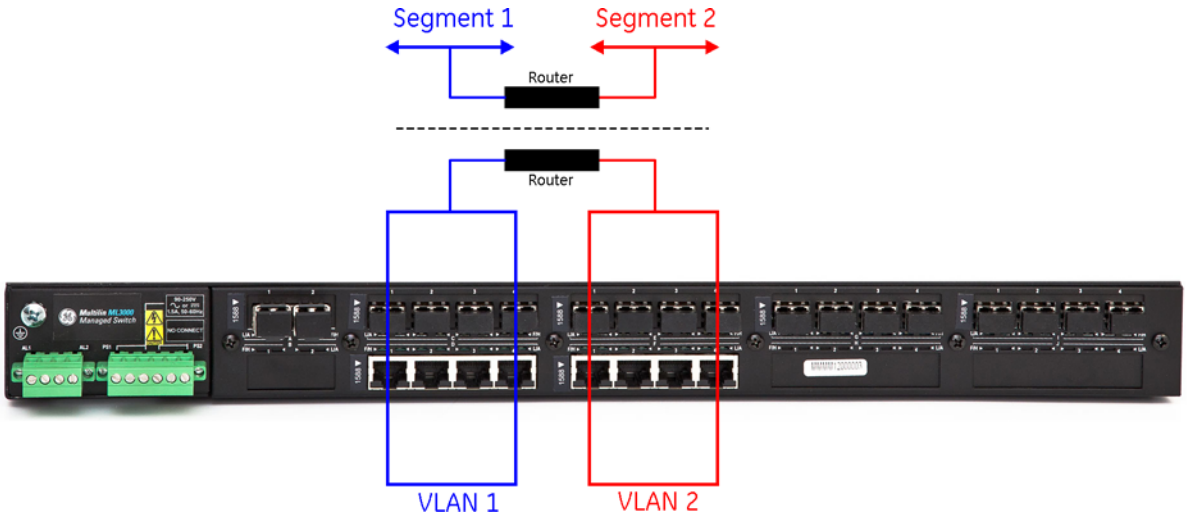


FIGURE 10–3: VLAN routing

The MultiLink family of switches supports up to 32 VLANs per switch.

10.1.2 Tag VLAN vs. Port VLAN

What is the difference between tag and port VLAN? In a nutshell - port VLAN sets a specific port or group of ports to belong to a VLAN. Port VLANs do not look for VLAN identifier (VID) information nor does it manipulate the VID information. It thus works “transparently” and propagates the VLAN information along.

In the tag VLAN, an identifier called the VLAN identifier (VID) is either inserted or manipulated. This manipulated VLAN tag allows VLAN information to be propagated across devices or switches, allowing VLAN information to span multiple switches.

As described earlier, VLAN is an administratively configured LAN or broadcast domain. Instead of going to the wiring closet to move a cable to a different LAN segment, the same task can be accomplished remotely by configuring a port on an 802.1Q-compliant switch to belong to a different VLAN. The ability to move end stations to different broadcast domains by setting membership profiles for each port on centrally managed switches is one of the main advantages of 802.1Q VLANs.

802.1Q VLANs aren't limited to one switch. VLANs can span many switches. Sharing VLANs between switches is achieved by inserting a tag with a VLAN identifier (VID) into each frame. A VID must be assigned for each VLAN. By assigning the same VID to VLANs on many switches, one or more VLAN (broadcast domain) can be extended across a large network.

802.1Q-compliant switch ports, such as those on the MultiLink family of switches, can be configured to transmit tagged or untagged frames. A tag field containing VLAN information can be inserted into an Ethernet frame. If a port has an 802.1Q-compliant device attached (such as another switch), these tagged frames can carry VLAN membership information between switches, thus letting a VLAN span multiple switches. Normally connections between switches can carry multiple VLAN information and this is call port trunking or 802.1Q trunks.

There is one important caveat: administrators must ensure ports with non-802.1Q-compliant devices attached are configured to transmit untagged frames. Many network interface cards such as those for PCs printers and other “dumb” switches are not 802.1Q-compliant. If they receive a tagged frame, they will not understand the VLAN tag and will drop the frame. In situations like these, its best to use port based VLANs for connecting to these devices.

Sometimes a port may want to listen to broadcasts across different VLANs or propagate the VLAN information on to other ports. This port must thus belong to multiple VLANs so that the broadcast information reaches the port accurately. If the port also wants to send broadcast traffic, the proper leave (sending out of information) and join rules (receiving information) have to be configured on the MultiLink family of switches.

It is recommended to use IEEE 802.1q tagged based VLANs over port based VLANs because of there multi-vendor interoperability and capability of carrying the isolated tagged VLAN information when more than one switch is involved.

10.2 Configuring Port VLANs through the Command Line Interface

10.2.1 Description

Port VLANs are rarely used in networks which use VLANs across multiple switches. Port VLANs are used when VLANs are setup up on a single switch and connectivity between the system on different VLANs is needed however the broadcasts and multicasts are isolated to the specific VLAN.

GE recommends using the set-port command for setting the port based VLAN as well.

The port-based VLAN feature supports a maximum of 1 VLAN per port. Any pre-existing VLAN tags on traffic coming into the switch on a port-based VLAN port, will be removed.

General steps for using port VLANs are

1. Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs.
2. Configure at least one VLAN in addition to the default VLAN
3. Assign the desired ports to the VLANs
4. Decide on trunking strategy - how will the VLAN information be propagated from one switch to another and also what VLAN information will be propagated across
5. (Layer 3 consideration) check to see if the routing between the VLANs is "working" by pinging stations on different VLANs

You can rename the default VLAN, but you cannot change its VID (1) or delete it from the switch

The VLAN Name field must always start with a letter. The remainder of the name field accepts all alphanumeric characters and the special characters #, _, -.

Any ports not specifically assigned to another VLAN will remain assigned to the DEFAULT-VLAN

Changing the number of VLANs supported on the switch requires the SAVE command to save the new VLAN information

10.2.2 Commands

The following commands are used for VLANs. To define the VLAN type:

set vlan *type=<port|tag|none>*

To configure a VLAN:

configure vlan *type=port*

vlan *type=port*

To add VLANs:

add *id=<vlan Id> [name=<vlan name>] port=<number|list|range>*

To start VLANs:

start *vlan=<name|number|list|range>*

To save VLAN configuration:

save

To edit VLANs:

edit *id=<vlan Id> [name=<vlan name>] port=<number|list|range>*

To display the VLAN information:

show vlan *type=<port|tag> [<id=vlanid>]*

The following command sequence shows how to configure VLANs on a MultiLink switch.

ML3000# `vlan type=port`

ML3000(port-vlan)## `add id=2 name=test port=1-10`

ML3000(port-vlan)## `start vlan=all`

ML3000(port-vlan)## `save`

Saving current configuration...
Configuration saved

To move Management Control on any VLAN:

add *id=<vlan Id> [name=<vlan name>] port=<number|list|range>*
[Forbid=<number|list|range>][<mgt|nomgt>]

To enable or disable Management Control on any VLAN:

*edit id=<vlan Id>[name=<vlan name>][port=<number|list|range>****[<mgt|nomgt>]***

10.3 Configuring Port VLANs with EnerVista Secure Web Management software

10.3.1 Description

Port VLANs are rarely used in networks which use VLANs across multiple switches. Port VLANs are used when VLANs are setup up on a single switch and connectivity between the systems on different VLANs is needed; however, the broadcasts and multicasts are isolated to the specific VLAN.

Either port VLANs or Tag VLAN can be active at any given time on a switch. Only the default VLAN (VLAN ID = 1) is active as a Tag VLAN as well as a port VLAN.

General steps for using port VLANs are

1. Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs.
2. Configure at least one VLAN in addition to the default VLAN.
3. Assign the desired ports to the VLANs
4. Decide on trunking strategy – how will the VLAN information be propagated from one switch to another and also what VLAN information will be propagated across.
5. Layer 3 consideration – check to see if the routing between the VLANs is "working" by pinging stations on different VLANs


NOTE

You can rename the default VLAN, but you cannot change its VID =1 or delete it from the switch.


NOTE

The VLAN Name field must always start with a letter. The remainder of the name field accepts all alphanumeric characters and the special characters #, _, -.

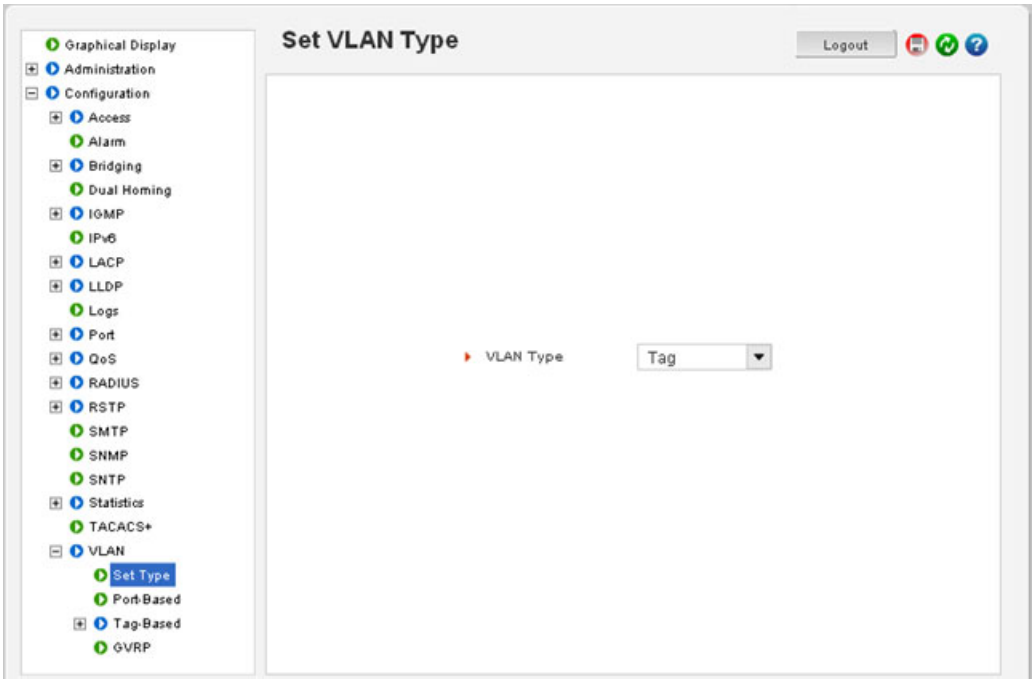

NOTE

Any ports not specifically assigned to another VLAN will remain assigned to the DEFAULT-VLAN (VID=1).


NOTE

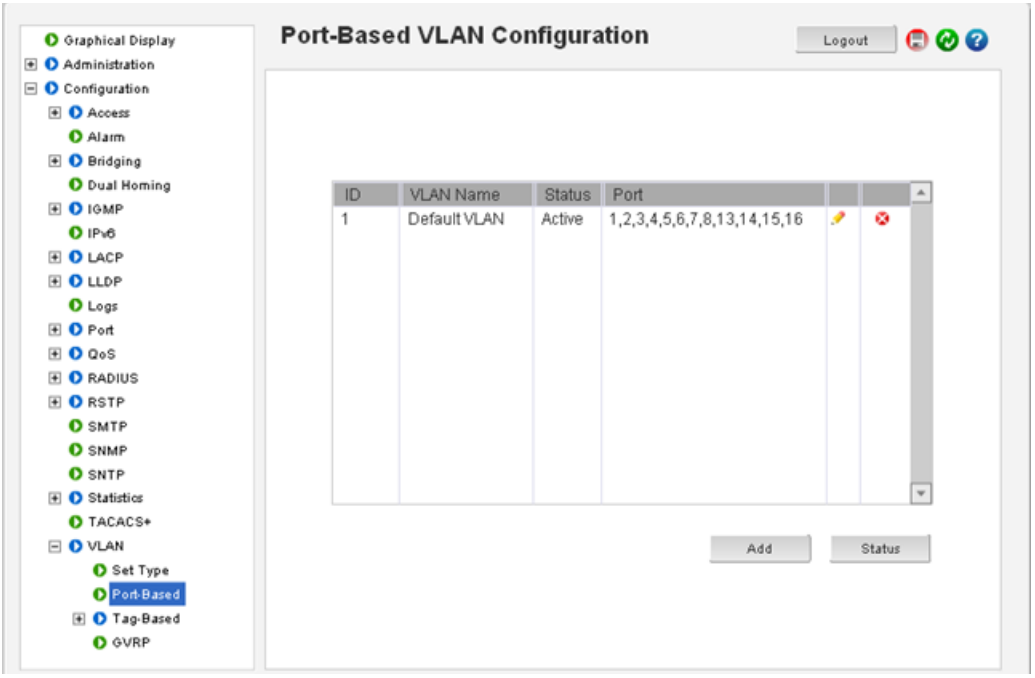
Changing the number of VLANs supported on the switch requires the changes to be saved for future use. To eliminate the changes, reboot the switch without saving the changes.

For VLAN configuration use **Configuration > VLAN** menu items as shown below. The Port VLANs are active by default.

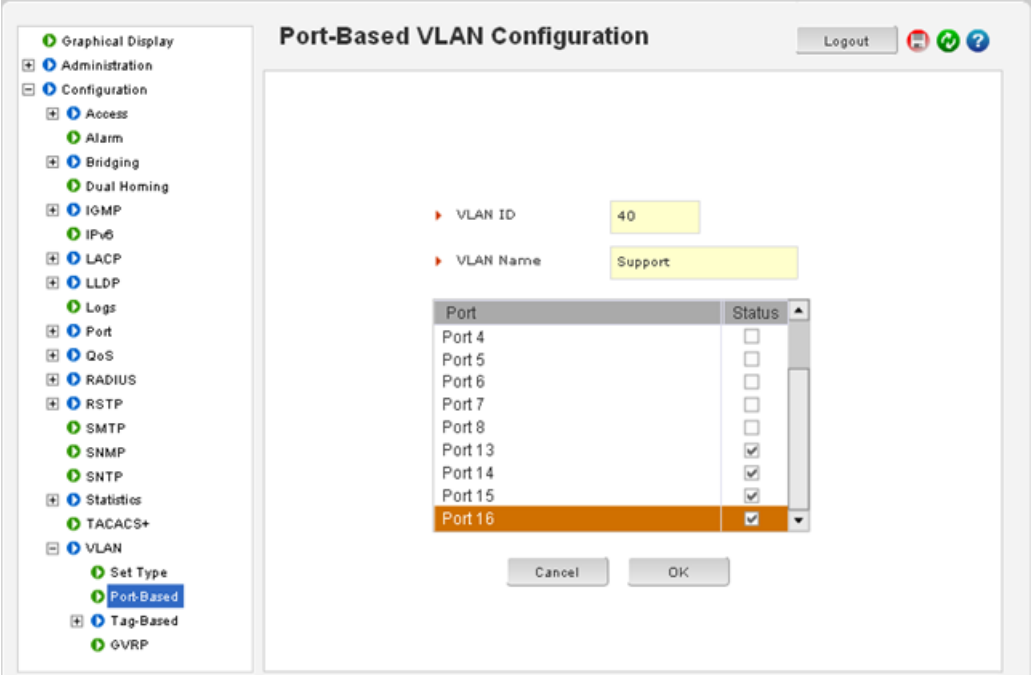


The currently assigned Port VLANs are displayed as follows:

▷ Select the **Configuration > VLAN > Port-Based** menu item.



As discussed above, ports 1, 2, 3, 4, 5, 6, 7, 8, 13, 14, 15, 16 still belong to default VLAN. We will now add another VLAN with VID=40 and VLAN name = Support.

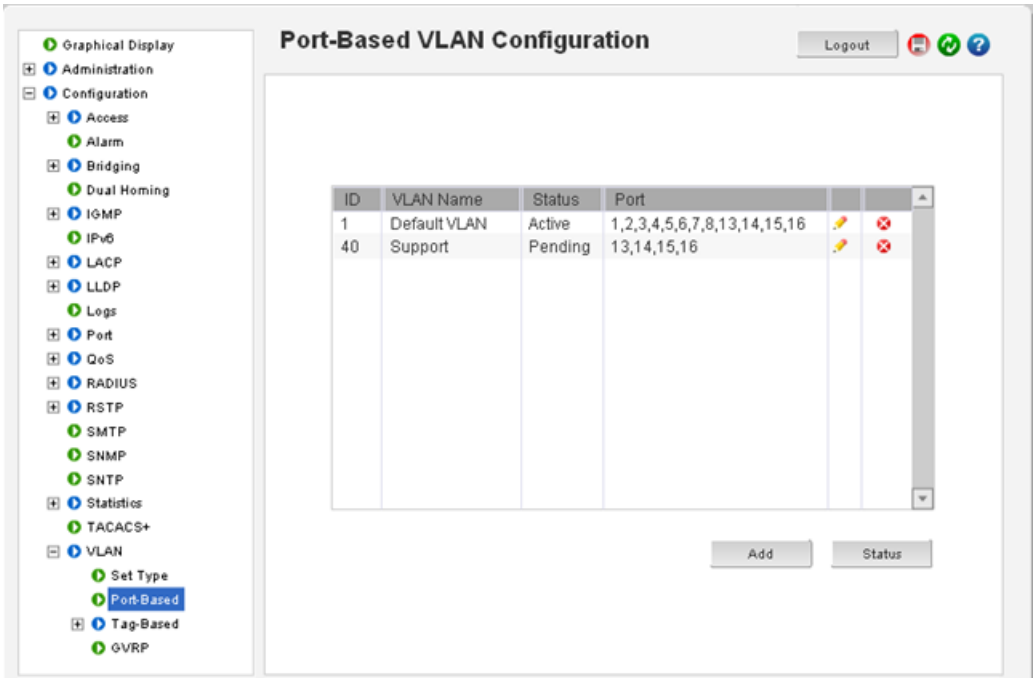


▷ Add the ports.

▷ Define the VLAN.

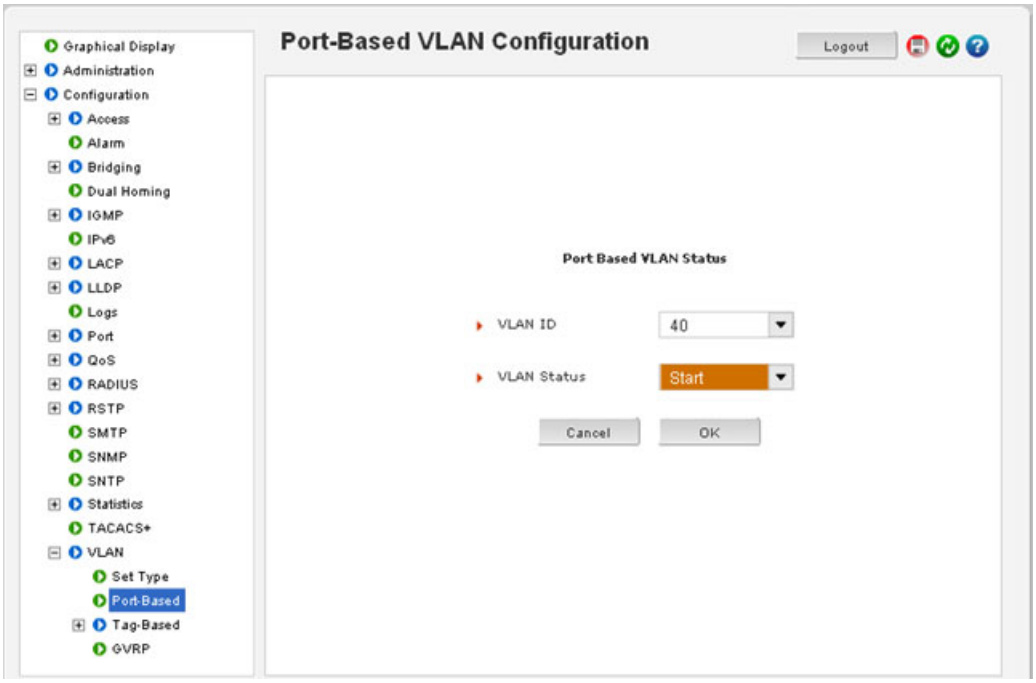
▷ Click OK.

.



After adding the VLAN, the VLAN is not active. Activating the VLAN has to be done manually.

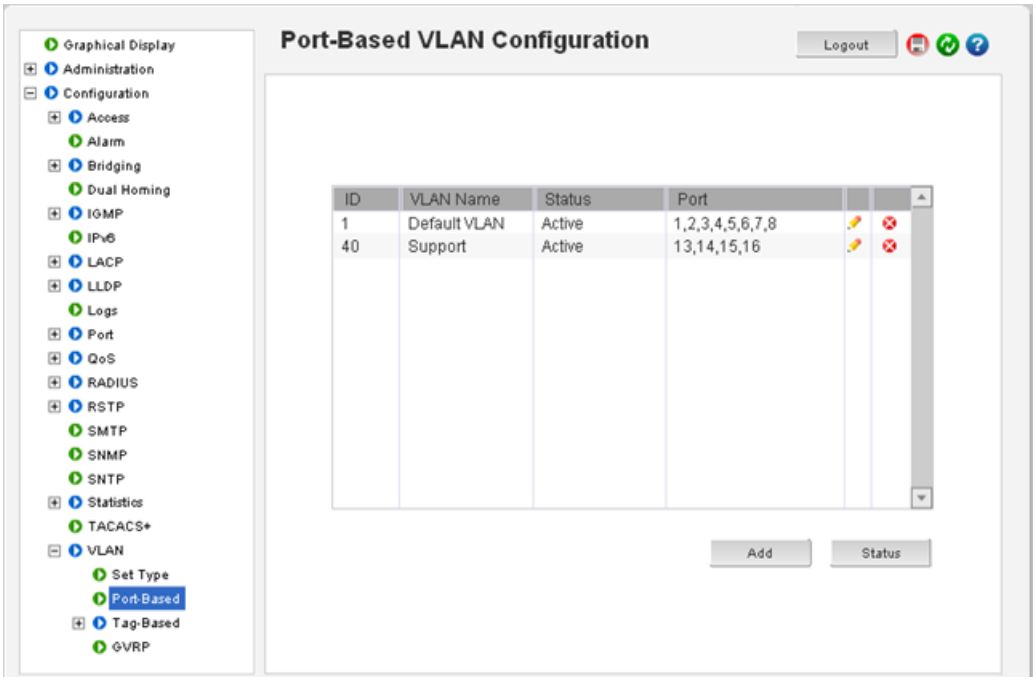
▷ To activate the VLAN, click on the **Status** button..



A specific VLAN can be activated or all VLANs can be activated (or disabled).

▷ Click **OK** to activate VLAN.

.



After activation, note that ports 13 to 16 belong to the new VLAN. The VLAN membership of the ports assigned to VLAN 40 now indicates that they are only members of VLAN 40. The default VLAN membership has been terminated on VLAN activation.

10.4 Configuring Tag VLANs through the Command Line Interface

10.4.1 Description

The VLAN information needs to be propagated on to other switches when multiple switches are connected on a network. In these situations it is best to use tag-based VLANs.

NOTE

For versions 1.6.1 and below, the use of tag VLANs needed the `set-ingress` and `set-egress` commands to set the flow of incoming and outgoing traffic. These commands are defunct as of MultiLink Switch Software version 1.6.1. For legacy purposes, these commands will still work with release 1.6.1 (and will print a message on the screen indicating the commands are deprecated), however, GE strongly recommends avoiding these commands and using the `set-port` command instead.

NOTE

The VLAN Name field must always start with a letter. The remainder of the name field accepts all alphanumeric characters and the special characters #, _, -.

10.4.2 Commands

The `set-port` command for setting Tag VLANs has the following parameters. The `default id` parameter sets the default VLAN id (termed PVID in previous versions). The default VLAN id is the VLAN id assigned to the untagged packets received on that port. For Multilink family of switches, the default VLAN id is 1

set-port *port=<number|list|range>*
default id=<number>

The `filter` parameter enables or disables the VLAN filtering function. When enabled, the switch will drop the packets coming in through a port if the port is not a member of the VLAN. For example, if port 1 is a member of VLANs 10, 20 and 30, if a packet with VLAN id 40 arrives at port 1 it will be dropped.

set-port *port=<number|list|range>*
filter status=<enable|disable>

The `tagging id` and `status` parameters define whether the outgoing packets from a port will be tagged or untagged. This definition is on a per VLAN basis. For example, the command `set-port port=1 tagging id=10 status=tagged` will instruct the switch to tag all packets going out of port 1 to belong to VLAN 10.

set-port *port=<number|list|range>*
tagging id=<number> status=<tagged|untagged>

The `join id` parameter adds the specified port(s) to the specified VLAN id. This parameter works with active or pending VLANs.

set-port *port=<number|list|range>*
join id=<number>

The `leave id` parameter releases a specific port from a VLAN. For example if port 1 belongs to VLAN 10, 20, 30, 40 the command set-port port=1 leave id=40 makes port 1 belong to VLAN 10, 20, 30, dropping VLAN 40.

set-port *port=<number|list|range>*
leave id=<number>

The `show-port` command lists all parameters related to tag VLAN for the list of ports. If the `port` parameter is omitted, it will display all ports.

show-port [port=<port|list|range>]

To move Management Control on any VLAN:

add *id=<vlan Id> [name=<vlan name>] port=<number|list|range> [Forbid=<number|list|range>][<mgt|nomgt>]*

To enable or disable Management Control on any VLAN:

*edit id=<vlan Id>[name=<vlan name>][port=<number|list|range>**[<mgt|nomgt>]***

10.4.3 Example

In the following example, we start with Port VLAN and convert to TAG VLAN. We define ports 14 through 16 to belong to VLANs 10, 20 and 30 and the rest of the ports belong to the default VLAN (in this case, VLAN 1). Filtering is enabled on ports 14-16. The VLAN setup is done before devices are plugged into ports 14-16 as a result the status of the ports show the port status as DOWN.

1. A word of caution - when Tag VLAN filtering is enabled, there can be serious connectivity repercussions - the only way to recover from that it is to reload the switch without saving the configuration or by modifying the configuration from the console (serial) port.
2. There can be either Tag VLAN or Port VLAN. Both VLANs cannot co-exit at the same time.
3. There can only be one default VLAN for the switch. The default is set to VLAN 1 and can be changed to another VLAN. A word of caution on changing the default VLAN as well - there can be repercussions on management as well as multicast and other issues.
4. Tag VLAN support VLAN ids from 1 to 4096. VLAN ids more than 2048 are reserved for specific purposes and it is recommended they not be used.

Example 10-1: Converting Port VLAN to Tag VLAN

```
ML3000# vlan type=port
ML3000(port-vlan)## show vlan type=port
 VLAN ID  : 1
 Name     : Default VLAN
 Status   : Active

 ========================
  PORT |     STATUS
 ========================
    9 |     UP
   10 |     DOWN
   11 |     DOWN
   12 |     DOWN
   13 |     UP
 VLAN ID  : 10
 Name     : engineering
 Status   : Active

 ========================
  PORT |     STATUS
 ========================
   14 |     DOWN
 VLAN ID  : 20
 Name     : sales
 Status   : Active

 ========================
  PORT |     STATUS
 ========================
   15 |     DOWN
 VLAN ID  : 30
 Name     : markteting
 Status   : Active

 ========================
  PORT |     STATUS
 ========================
   16 |     DOWN
ML3000(port-vlan)## stop vlan=all
 All active VLAN's stopped.
ML3000(port-vlan)## exit
ML3000# set vlan type=tag
 VLAN set to Tag-based.
ML3000# show active-vlan
Tag VLAN is currently active.
```

To switch to Tag VLAN, the port VLAN has to be disabled or stopped. Only one type of VLAN can co-exist at the same time. Exit out of Port VLAN configuration mode and set the VLAN type to be Tag VLAN.

(continued on next page)

Converting Port VLAN to Tag VLAN (continued)

```
ML3000# show vlan type=tag

 VLAN ID  : 1
 Name     : Default VLAN
 Status   : Active

 ==============================
  PORT | MODE     | STATUS
 ==============================
    9 | UNTAGGED | UP
   10 | UNTAGGED | DOWN
   11 | UNTAGGED | DOWN
   12 | UNTAGGED | DOWN
   13 | UNTAGGED | UP
   14 | UNTAGGED | DOWN
   15 | UNTAGGED | DOWN
   16 | UNTAGGED | DOWN
```

Note that ports 14 to 16 are "DOWN" - the VLAN configuration is preferably done before devices are plugged in to avoid connectivity repercussions.

```
ML3000# vlan type=tag

ML3000(tag-vlan)## add id=10 name=mkt port=14-16

 Tag based vlan Added Successfully.
 VLAN ID   : 10
 VLAN Name  : mkt
 Ports     : 14-16

ML3000(tag-vlan)## edit id=10 name=engineering port=14-16

 Tag based vlan Added Successfully.
 VLAN ID   : 10
 VLAN Name  : engineering
 Ports     : 14-16

ML3000(tag-vlan)## add id=20 name=sales port=14-16

 Tag based vlan Added Successfully.
 VLAN ID   : 20
 VLAN Name  : sales
 Ports     : 14-16

ML3000(tag-vlan)## add id=20 name=marketing port=14-16

 ERROR: Duplicate Vlan Id

ML3000(tag-vlan)## add id=30 name=marketing port=14-16

 Tag based vlan Added Successfully.
 VLAN ID   : 30
 VLAN Name  : marketing
 Ports     : 14-16
```

Intentionally executed to show the effect of adding a duplicate VLAN.

(continued on next page)

Converting Port VLAN to Tag VLAN (continued)

```
ML3000(tag-vlan)## show vlan type=tag

 VLAN ID  : 1
 Name     : Default VLAN
 Status   : Active

 ==============================
  PORT | MODE     | STATUS
 ==============================
    9 | UNTAGGED | UP
   10 | UNTAGGED | DOWN
   11 | UNTAGGED | DOWN
   12 | UNTAGGED | DOWN
   13 | UNTAGGED | UP
   14 | UNTAGGED | DOWN
   15 | UNTAGGED | DOWN
   16 | UNTAGGED | DOWN

 VLAN ID  : 10
 Name     : engineering
 Status   : Pending

 ==============================
  PORT | MODE     | STATUS
 ==============================
   14 | UNTAGGED | DOWN
   15 | UNTAGGED | DOWN
   16 | UNTAGGED | DOWN

 VLAN ID  : 20
 Name     : sales
 Status   : Pending

 ==============================
  PORT | MODE     | STATUS
 ==============================
   14 | UNTAGGED | DOWN
   15 | UNTAGGED | DOWN
   16 | UNTAGGED | DOWN

 VLAN ID  : 30
 Name     : marketing
 Status   : Pending

 ==============================
  PORT | MODE     | STATUS
 ==============================
   14 | UNTAGGED | DOWN
   15 | UNTAGGED | DOWN
   16 | UNTAGGED | DOWN

ML3000(tag-vlan)## start vlan=all

 All pending VLAN's started.
```

Note that the VLANs are not started as yet. Adding the VLAN does not start it by default.

(continued on next page)

Converting Port VLAN to Tag VLAN (continued)

```
ML3000(tag-vlan)## set-port port=14-16 filter status=enable
 WARNING: PVID does not match the port(15)'s VLAN ID(s).
 If you are using telnet session on this port,setting ingress might stop the session.
 Do you want to continue? ['Y' or 'N'] Y
  WARNING: PVID does not match the port(14)'s VLAN ID(s).
 If you are using telnet session on this port, setting ingress might stop the session.
 Do you want to continue? ['Y' or 'N'] Y
 WARNING: PVID does not match the port(16)'s VLAN ID(s).
 If you are using telnet session on this port, setting ingress might stop the session.
 Do you want to continue? ['Y' or 'N'] Y
Ingress Filter Enabled
ML3000(tag-vlan)## show vlan type=tag
 VLAN ID  : 1
 Name     : Default VLAN
 Status   : Active

 ==============================
  PORT | MODE     | STATUS
 ==============================
    9 | UNTAGGED | UP
   10 | UNTAGGED | DOWN
   11 | UNTAGGED | DOWN
   12 | UNTAGGED | DOWN
   13 | UNTAGGED | UP

 VLAN ID  : 10
 Name     : engineering
 Status   : Active

 ==============================
  PORT | MODE     | STATUS
 ==============================
   14 | UNTAGGED | DOWN
   15 | UNTAGGED | DOWN
   16 | UNTAGGED | DOWN

 VLAN ID  : 20
 Name     : sales
 Status   : Active

 ==============================
  PORT | MODE     | STATUS
 ==============================
   14 | UNTAGGED | DOWN
   15 | UNTAGGED | DOWN
   16 | UNTAGGED | DOWN

 VLAN ID  : 30
 Name     : marketing
 Status   : Active

 ==============================
  PORT | MODE     | STATUS
 ==============================
```

Enable filtering on the ports required. The software will prompt to ensure that connectivity is not disrupted.

VLANs are now active. However, as the packet traverses VLANs, the packet should be tagged. This is enabled next.

Converting Port VLAN to Tag VLAN (continued)

```
ML3000(tag-vlan)## set-port port=14-16 tagging id=10 status=tagged
 Port tagging enabled
ML3000(tag-vlan)## set-port port=14-16 tagging id=20 status=tagged
 Port tagging enabled
ML3000(tag-vlan)## set-port port=14-16 tagging id=30 status=tagged
 Port tagging enabled
ML3000(tag-vlan)## show vlan type=tag
 VLAN ID  : 1
 Name     : Default VLAN
 Status   : Active

 ============================
  PORT | MODE     | STATUS
 ============================
    9 | UNTAGGED | UP
   10 | UNTAGGED | DOWN
   11 | UNTAGGED | DOWN
   12 | UNTAGGED | DOWN
   13 | UNTAGGED | UP

 VLAN ID  : 10
 Name     : engineering
 Status   : Active

 ============================
  PORT | MODE     | STATUS
 ============================
   14 | TAGGED   | DOWN
   15 | TAGGED   | DOWN
   16 | TAGGED   | DOWN

 VLAN ID  : 20
 Name     : sales
 Status   : Active

 ============================
  PORT | MODE     | STATUS
 ============================
   14 | TAGGED   | DOWN
   15 | TAGGED   | DOWN
   16 | TAGGED   | DOWN

 VLAN ID  : 30
 Name     : marketing
 Status   : Active

 ============================
  PORT | MODE     | STATUS
 ============================
```

10.5 Configuring Tag VLANs with EnerVista Secure Web Management software

10.5.1 Description

When multiple switches are on a network, the VLAN information needs to be propagated on to other switches. In such situations, it is best to use tag based VLANs.

On the MultiLink ML3000 Ethernet Switch, the port VLAN type is set to none. To use Tag VLANs, first enable Tag VLANs.

In the following example, we assign various ports as VLANs 10, 20 and 30 and the remaining ports to the default VLAN (that is, VLAN 1).

The VLAN setup occurs before devices are connected to the ports. As such, the port status is shown as DOWN.

NOTICE

There can be serious connectivity repercussions when Tag VLAN filtering is enabled. The only way to recover from this it is to reload the switch without saving the configuration or by modifying the configuration from the console (serial) port.

The ML3000 can be configured for either Tag VLAN or Port VLAN. Both VLANs cannot co-exit at the same time. There can only be one default VLAN for the switch. The default is set to VLAN 1 and can be changed to another VLAN.

CAUTION

There can be repercussions on management as well as multicast and other issues when changing the default VLAN.

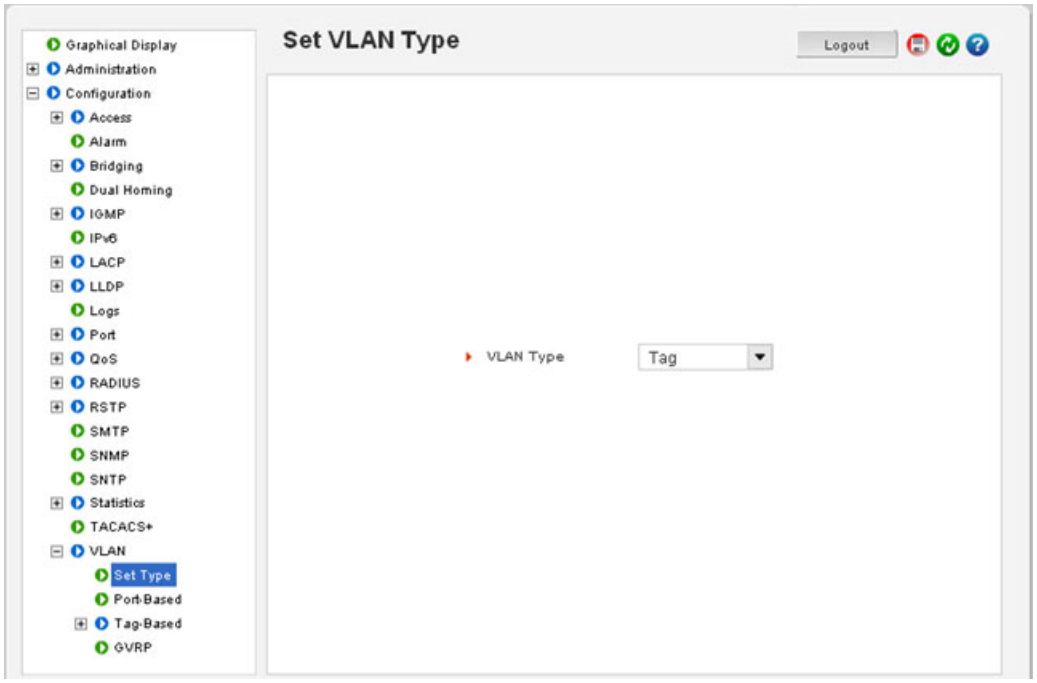
Tag VLAN supports VLAN IDs from 1 to 4096. VLAN IDs greater than 2048 are reserved for specific purposes. As such, it is recommended they not be used.

NOTE

The VLAN Name field must always start with a letter. The remainder of the name field accepts all alphanumeric characters and the special characters #, _, -.

To use the Tag VLAN, first

▷ Set the VLAN type to Tag in the **Configuration > VLAN > Set Type** menu.

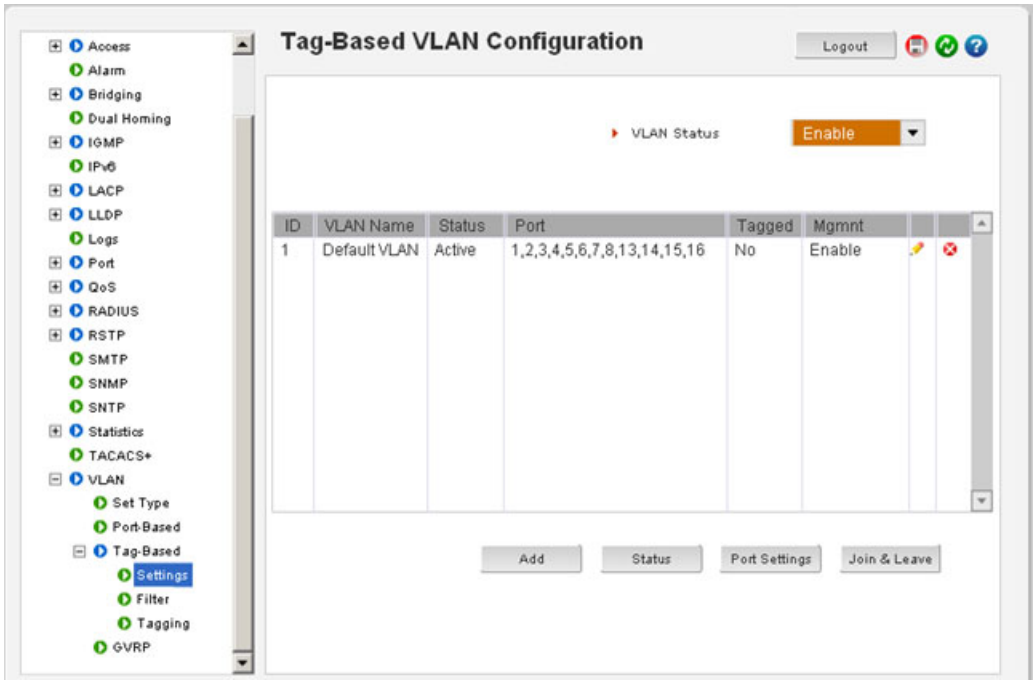


The next step is to define the VLANs needed. To do that,

▷ Click On **Configuration >vlan >tag-based >Settings** Menu.

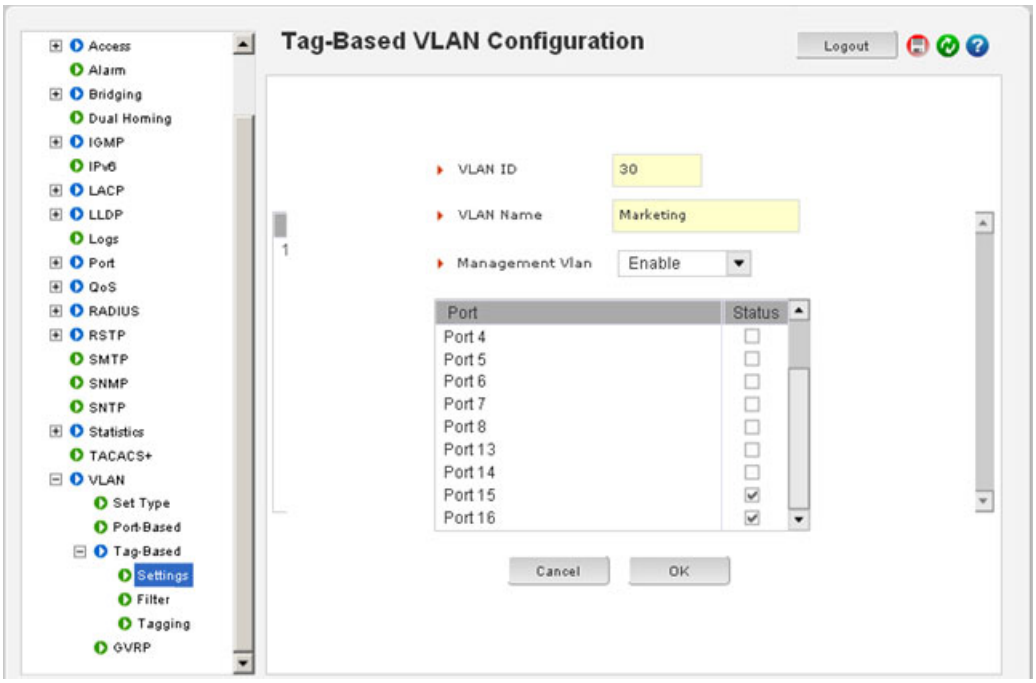
▷ Click on the **Add** button.

.



▷ Now add the necessary VLANs.
In the example below, add the VLANs in the following manner

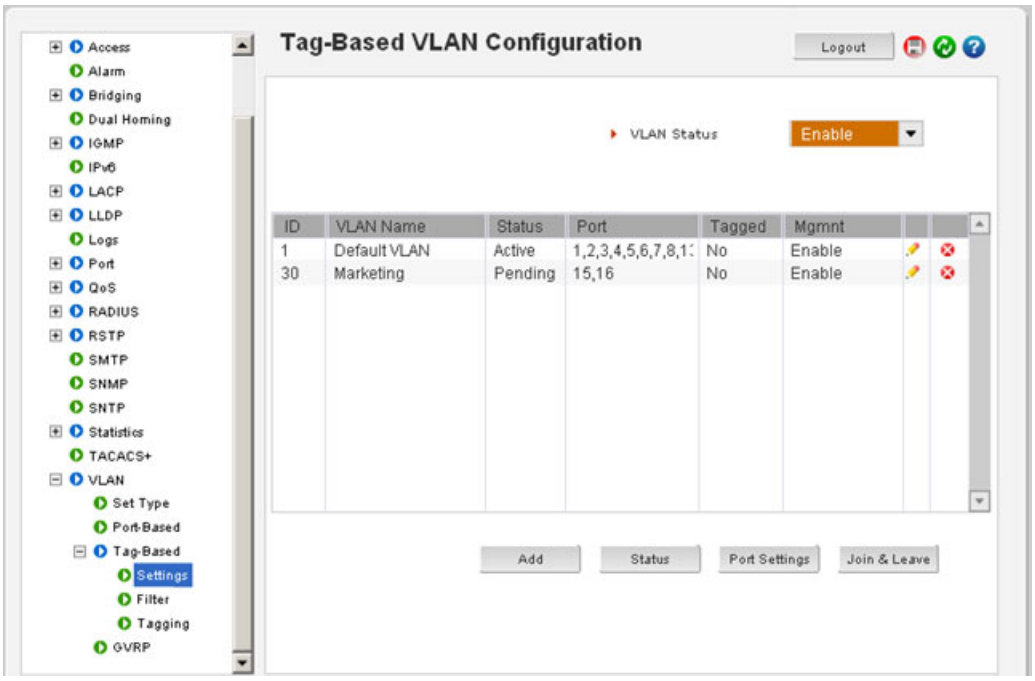
- VLAN 1, All ports - default VLAN
- VLAN 10, Engineering VLAN - ports 13, 14
- VLAN 20, Support VLAN - ports 13, 14, 15 (note that port 13 belongs to VLAN 10, 20)
- VLAN 30, Marketing VLAN -ports 15, 16 (note that port 15 belongs to VLAN 20, 30)

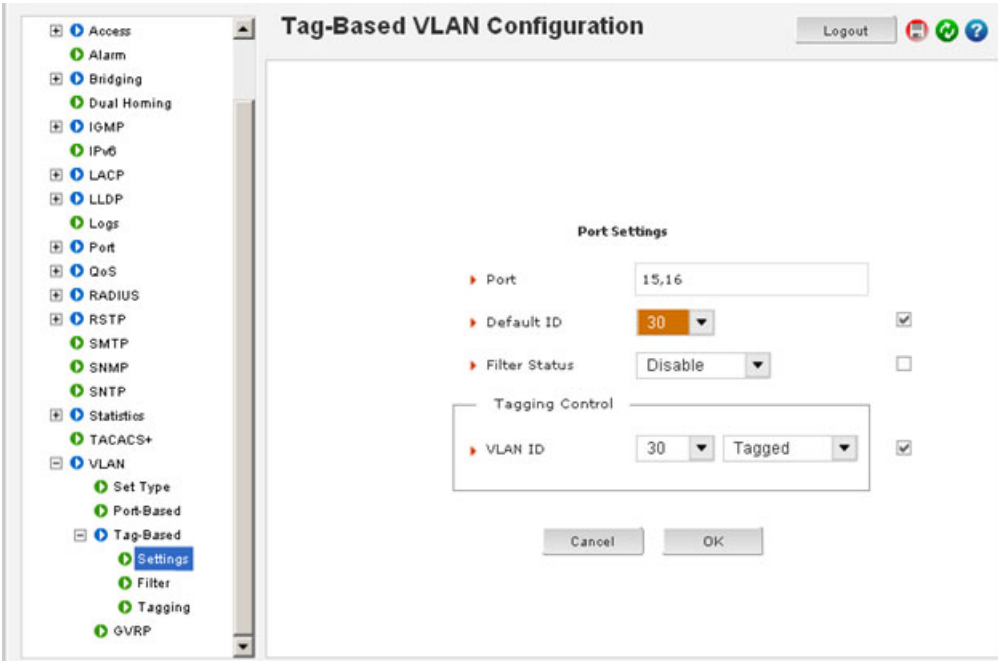


▷ After adding the ports and defining the VLAN, click **OK**.

▷ Click on **Port Settings** in the **Configuration >VLAN >Tag-Based >Settings** menu and enable the tagging for each port.

.

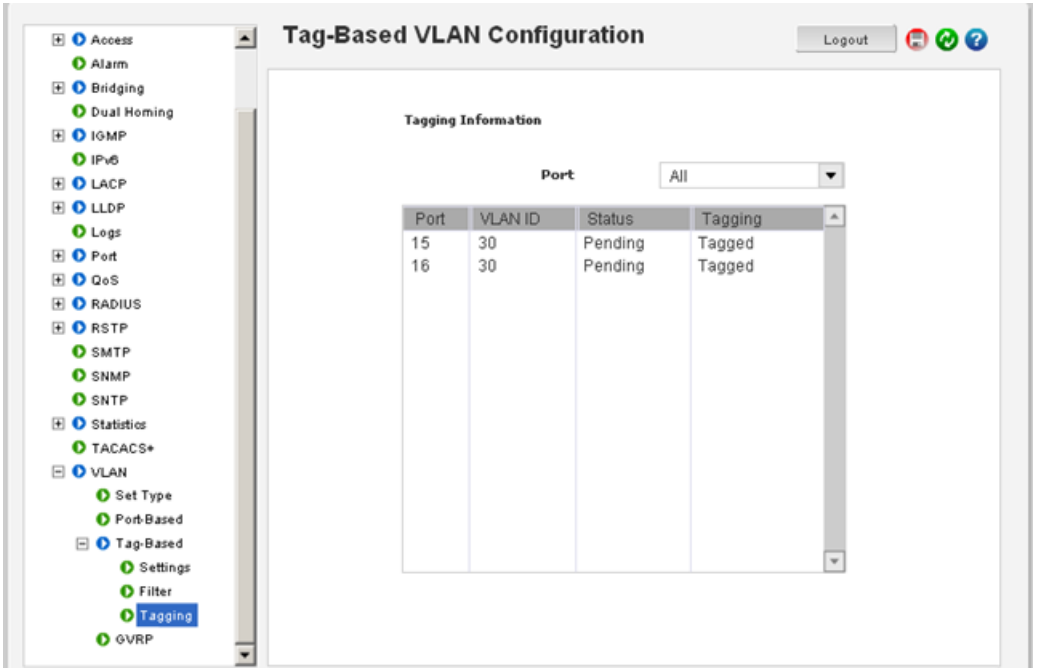




▷ Repeat the last two steps for each of the ports and each of the VLANs (click on port settings and enable the tag on the port.) After all the ports are tagged, the tagged column should change to "Yes" for all VLANs

To check the status of the tagging,

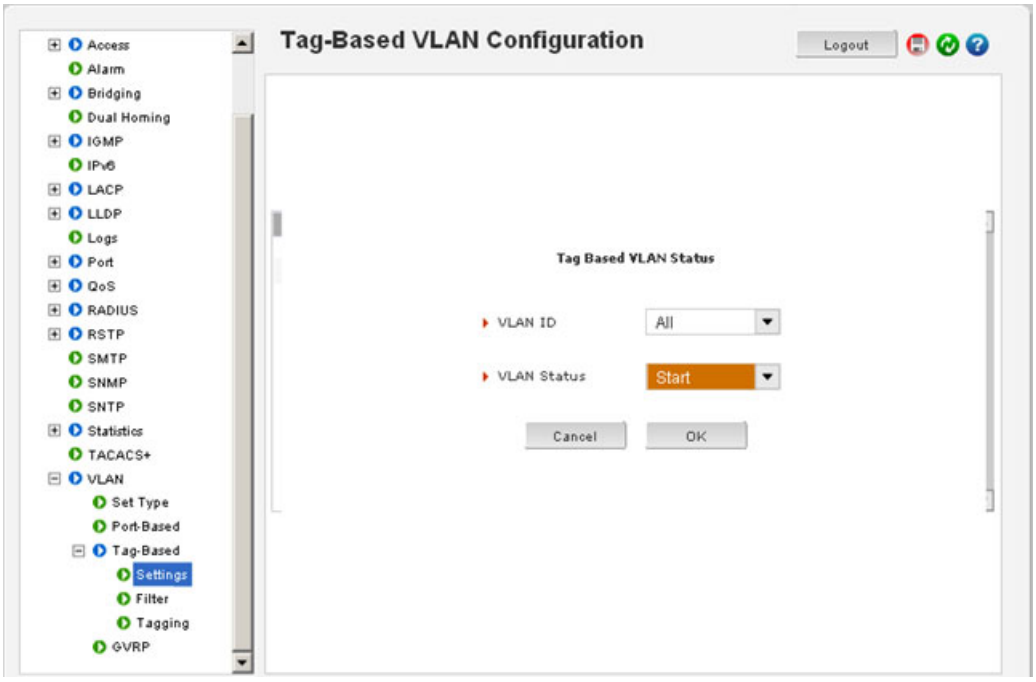
▷ Select the **Configuration > VLAN > Tag-Based > Tagging** menu.



To activate the VLAN,

▷ Click on the Status button under the **Configuration >VLAN >Tag-Based > Settings > Status** menu.

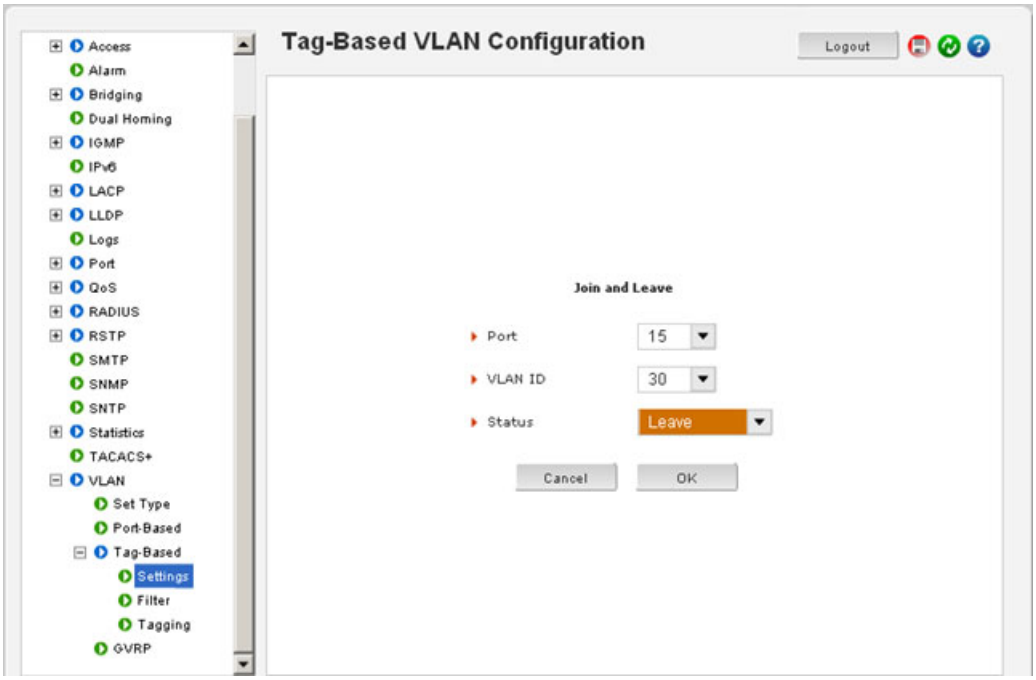
▷ Click OK.



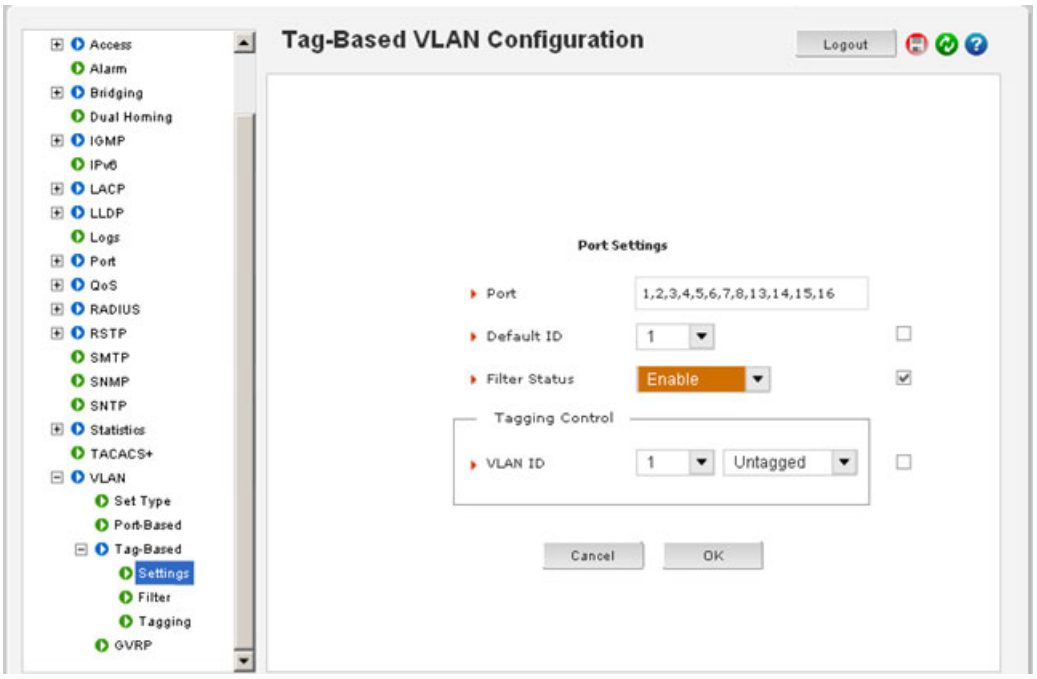
Tagged VLANs can be viewed from the **Configuration > VLAN > Tag-Based > Tagging** menu.

To add or delete specific ports from a VLAN,

▷ Click on **Join & Leave** button from the **Configuration > VLAN >. Tag-Based > Settings** menu and specify the action.
In the example below, we will take port 15 and assign it to leave VLAN 30. After the action is completed, note that port 15 will belong to VLAN 1 only.



To enable the filter capability for each port, use the **Configuration >VLAN >Tag-Based > Settings > Port Settings** menu as shown below.



Use the **Configuration >VLAN >Tag-Based > Filter** menu to view the filter information for the ports.

Multilink ML3000/ML3100

Chapter 11: VLAN Registration over GARP

11.1 Overview

11.1.1 Description

The Generic Attribute Registration Protocol (GARP) and VLAN registration over GARP is called GVRP. GVRP is defined in the IEEE 802.1q and GARP in the IEEE 802.1p standards. To utilize the capabilities of GVRP, GE Multilin recommends that the user become familiar with the concepts and capabilities of IEEE 802.1q.

11.1.2 GVRP Concepts

GVRP makes it easy to propagate VLAN information across multiple switches. Without GVRP, a network administrator has to go to each individual switch and enable the necessary VLAN information or block specific VLANs so that the network integrity is maintained. With GVRP, this process can be automated.

It is critical that all switches share a common VLAN. This VLAN typically is the default VLAN (VID=1) on most switches and other devices. GVRP uses "GVRP Bridge Protocol Data Units" ("GVRP BPDUs") to "advertise" static VLANs. We refer to GVRP BPDU is as an "advertisement".

GVRP enables the MultiLink family of switches to dynamically create 802.1q-compliant VLANs on links with other devices running GVRP. This enables the switch to automatically create VLAN links between GVRP-aware devices. A GVRP link can include intermediate devices that are not GVRP-aware. This operation reduces the chances for errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. GVRP can thus be used to propagate VLANs to other GVRP-aware devices instead of manually having to set up VLANs across the network. After the switch creates a dynamic VLAN, GVRP can also be used to dynamically enable port membership in static VLANs configured on a switch.

NOTE

There must be one common VLAN (that is, one common VID) connecting all of the GVRP-aware devices in the network to carry GVRP packets. GE Multilin recommends the default VLAN (DEFAULT_VLAN; VID = 1), which is automatically enabled and configured as untagged on every port of the MultiLink family of switches. That is, on ports used as GVRP links, leave the default VLAN set to untagged and configure other static VLANs on the ports as either "Tagged or Forbid" ("Forbid" is discussed later in this chapter).

11.1.3 GVRP Operations

A GVRP-enabled port with a tagged or untagged static VLAN sends advertisements (BPDUs, or Bridge Protocol Data Units) advertising the VLAN identification (VID) Another GVRP-aware port receiving the advertisements over a link can dynamically join the advertised VLAN. All dynamic VLANs operate as Tagged VLANs. Also, a GVRP-enabled port can forward an advertisement for a VLAN it learned about from other ports on the same switch. However, the forwarding port will not itself join that VLAN until an advertisement for that VLAN is received on that specific port.

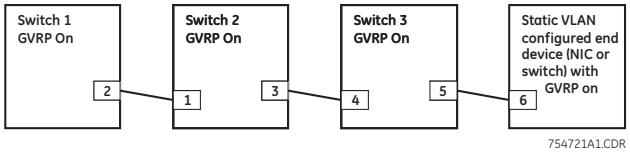


FIGURE 11–1: GVRP operation

Switch 1 with static VLANs (VID= 1, 2, and 3). Port 2 is a member of VIDs 1, 2, and 3.

1. Port 2 advertises VIDs 1, 2, and 3.
2. On Switch 2 - Port 1 receives advertisement of VIDs 1, 2, and 3 AND becomes a member of VIDs 1, 2, and 3.
3. As discussed above, a GVRP enabled port can forward advertisement for a VLAN it learnt about. So port 3 advertises VIDs 1, 2, and 3, but port 3 is NOT a member of VIDs 1, 2, and 3 at this point, nor will it join the VLAN until and advertisement is received.
4. On Switch 3, port 4 receives advertisement of VIDs 1, 2, and 3 and becomes a member of VIDs 1, 2, and 3.
5. Port 5 advertises VIDs 1, 2,and 3, but port 5 is NOT a member of VIDs 1, 2, and 3 at this point.
6. Port 6 on the end device is statically configured to be a member of VID 3. Port 6 advertises VID 3.
7. Port 5 receives advertisement.
8. Port 4 advertises VID 3.
9. Port 3 receives advertisement of VID 3 AND becomes a member of VID 3. (Still not a member of VIDs 1 and 2 as it did not receive any advertisements for VID 1 or 2).
10. Port 1 advertises VID 3 of VID 3 AND becomes a member of VID 3. (Port 1 is still not a member of VIDs 1 and 2).
11. Port 2 receives advertisement of VID 3. (Port 2 was already statically configured for VIDs 1, 2, 3).

NOTE

If a static VLAN is configured on at least one port of a switch, and that port has established a link with another device, then all other ports of that switch will send advertisements for that VLAN.

In the following figure, tagged VLAN ports on switch “A” and switch “C” advertise VLANs 22 and 33 to ports on other GVRP-enabled switches that can dynamically join the VLANs. A port can learn of a dynamic VLAN through devices that are not aware of GVRP (Switch “B”).

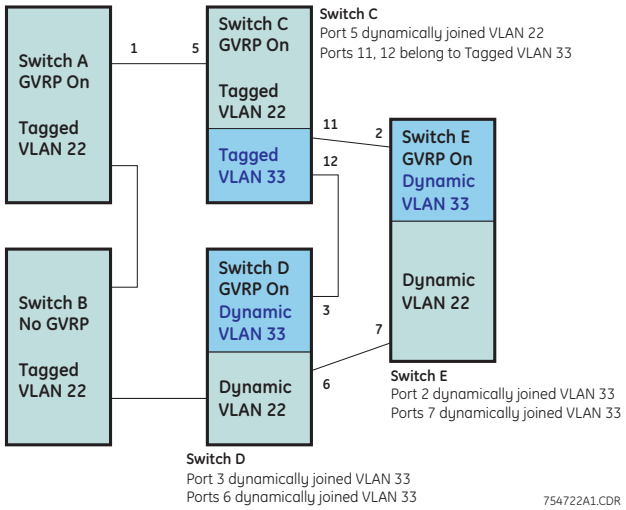


FIGURE 11–2: VLAN assignment in GVRP enabled switches

An “unknown VLAN” is a VLAN that the switch learns of by GVRP. For example, suppose that port 1 on switch “A” is connected to port 5 on switch “C”. Because switch “A” has VLAN 22 statically configured, while switch “C” does not have this VLAN statically configured, VLAN 22 is handled as an “Unknown VLAN” on port 5 in switch “C”. Conversely, if VLAN 22 was statically configured on switch C, but port 5 was not a member, port 5 would become a member when advertisements for VLAN 22 were received from switch “A”. GVRP provides a per-port join-request option which can be configured.

VLANs must be disabled in GVRP-unaware devices to allow tagged packets to pass through. A GVRP-aware port receiving advertisements has these options:

- If there is no static VLAN with the advertised VID on the receiving port, then dynamically create a VLAN with the same VID as in the advertisement, and allow that VLAN's traffic
- If the switch already has a static VLAN with the same VID as in the advertisement, and the port is configured to learn for that VLAN, then the port will dynamically join the VLAN and allow that VLAN's traffic.
- Ignore the advertisement for that VID and drop all GVRP traffic with that VID
- Don't participate in that VLAN
- A port belonging to a tagged or untagged static VLAN has these configurable options:
- Send VLAN advertisements, and also receive advertisements for VLANs on other ports and dynamically join those VLANs
- Send VLAN advertisements, but ignore advertisements received from other ports
- Avoid GVRP participation by not sending advertisements and dropping any advertisements received from other devices

Table 11–1: Port settings for GVRP operations

Unknown VLAN mode	Operations
Learn	Enables the port to dynamically join any VLAN for which it receives and advertisement, and allows the port to forward the advertisement it receives.
Block	Prevents the port from dynamically joining a VLAN that is not statically configured on the switch. The port will still forward advertisements that were received by the switch on other ports. Block should typically be used on ports in insecure networks where there is exposure to attack - such as ports where intruders can connect.
Disable	Causes the port to ignore and drop all the advertisements it receives from any source.

The `show-vlan` command displays a switch's current GVRP configuration, including the unknown VLANs.

show-vlan

A port must be enabled and configured to learn for it to be assigned to the dynamic VLAN. To send advertisements, one or more tagged or untagged static VLANs must be configured on one (or more) switches with GVRP enabled. The ML3000/ML3100 software allows a dynamic VLAN to be converted to a static VLAN with the `static` command.

static *vlan=<VID>*

The `show vlan type=tag` command will display VID in case the VID is not known.

Example 11-1 illustrates how to convert a dynamic VLAN into a static VLAN.

As the following table indicates, a port that has a tagged or untagged static VLAN has the option for both generating advertisements and dynamically joining other VLANs.

Table 11–2: GVRP options

Per-port "unknown VLAN" (GVRP) configuration	Per-port static VLAN options		
	Tagged or untagged	Auto	Forbid
Learn	Generate advertisements. Forward advertisements for other VLANs. Receive advertisements and dynamically join any advertised VLAN	Receive advertisements and dynamically join any advertised VLAN that has the same VID as the static VLAN	Do not allow the port to become a member of this VLAN
Block	Generate advertisements. Forward advertisements received from other ports to other VLANs. Do not dynamically join any advertised VLAN	Receive advertisements and dynamically join any advertised VLAN that has the same VID	Do not allow the VLAN on this port
Disable	Ignore GVRP and drop all GVRP advertisements	Ignore GVRP and drop all GVRP advertisements	Do not allow the VLAN on this port

Example 11-1: Converting a dynamic VLAN to a static VLAN

```
ML3000# gvrp
ML3000(gvrp)## show-vlan
 ================================================
  VLAN ID | NAME        | VLAN    | STATUS
 ================================================
    1    | Default VLAN | Static  | Active
    2    | Blue         | Static  | Active
   10    | dyn10        | Dynamic | Active
ML3000(gvrp)## static vlan=10
ML3000(gvrp)## show-vlan
 ================================================
  VLAN ID | NAME        | VLAN    | STATUS
 ================================================
    1    | Default VLAN | Static  | Active
    2    | Blue         | Static  | Active
```

The unknown VLAN parameters are configured on a per interface basis using the CLI. The tagged, untagged, Auto, and Forbid options are configured in the VLAN context. Since dynamic VLANs operate as tagged VLANs, and it is possible that a tagged port on one device may not communicate with an untagged port on another device, GE Multilin recommends that you use tagged VLANs for the static VLANs.

A dynamic VLAN continues to exist on a port for as long as the port continues to receive advertisements of that VLAN from another device connected to that port or until you:

- Convert the VLAN to a static VLAN
- Reconfigure the port to Block or Disable
- Disable GVRP
- Reboot the switch

The time-to-live for dynamic VLANs is 10 seconds. That is, if a port has not received an advertisement for an existing dynamic VLAN during the last 10 seconds, the port removes itself from that dynamic VLAN.

11.2 Configuring GVRP through the Command Line Interface

11.2.1 Commands

The commands used for configuring GVRP are shown below.

The `gvrp` command enables or disables GVRP.

gvrp *<enable|disable>*

The `show gvrp` command displays whether GVRP is disabled, along with the current settings for the maximum number of VLANs and the current primary VLAN.

show gvrp

The `set-ports` command set the state of the port to learn, block or disable for GVRP. Note the default state is disable.

set-ports *port=<port|list|range> state=<learn|block|disable>*

The set-forbid command sets the forbid GVRP capability on the ports specified.

set-forbid *vlan=<tag vlanid>*
forbid=<port-number|list|range>

The show-forbid command displays the ports with GVRP forbid capabilities.

show-forbid

The following example illustrates how to configure GVRP using the commands shown in this section.

11.2.2 GVRP Operation Notes

A dynamic VLAN must be converted to a static VLAN before it can have an IP address.

After converting a dynamic VLAN to a static VLAN use the “save” command to save the changes made - on a reboot the changes can be lost without the save command.

Within the same broadcast domain, a dynamic VLAN can pass through a device that is not GVRP-aware. This is because a hub or a switch that is not GVRP-aware will flood the GVRP (multicast) advertisement packets out all ports.

GVRP assigns dynamic VLANs as tagged VLANs. To configure the VLAN as untagged, first convert the tagged VLAN to a static VLAN.

Rebooting a switch on which a dynamic VLAN deletes that VLAN. However, the dynamic VLAN re-appears after the reboot if GVRP is enabled and the switch again receives advertisements for that VLAN through a port configured to add dynamic VLANs.

By receiving advertisements from other devices running GVRP, the switch learns of static VLANs from those devices and dynamically (automatically) creates tagged VLANs on the links to the advertising devices. Similarly, the switch advertises its static VLANs to other GVRP-aware devices.

A GVRP-enabled switch does not advertise any GVRP-learned VLANs out of the port(s) on which it originally learned of those VLANs.

Example 11-2: Configuring GVRP

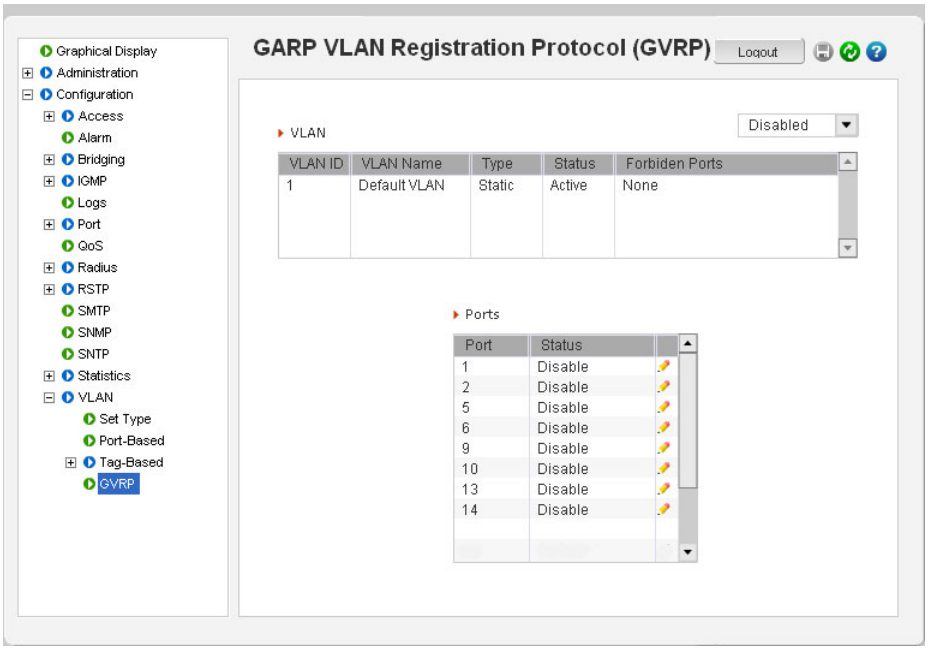
```
ML3000# gvrp
ML3000(gvrp)# show gvrp
 GVRP Status :  Enabled
ML3000(gvrp)## gvrp disable
 GVRP is now disabled
ML3000(gvrp)## gvrp enable
 GVRP enabled
ML3000(gvrp)## show-vlan
 ================================================
  VLAN ID | NAME       | VLAN    | STATUS
 ================================================
    1    | Default VLAN | Static  | Active
    2    | Blue       | Static  | Active
   10    | dyn10      | Dynamic | Active
ML3000(gvrp)## static vlan=10
ML3000(gvrp)## show-vlan
 ================================================
  VLAN ID | NAME       | VLAN    | STATUS
 ================================================
    1    | Default VLAN | Static  | Active
    2    | Blue       | Static  | Active
   10    | dyn10      | Static  | Active
ML3000(gvrp)## set-forbid vlan=2 forbid=11-15
ML3000(gvrp)## show-forbid
 ============================================
  VLAN ID | FORBIDDEN PORTS
 ============================================
    1    | None
```

11.3 Configuring GVRP with EnerVista Secure Web Management software

11.3.1 Example

To configure GVRP,

▷ Select the **Configuration > VLAN > GVRP** menu item.



From the GVRP menu screen, GVRP can be enabled or disabled using the drop down menu. Each specific port can be put in the Learn, Disable or Enable state as shown in Table 11–2: *GVRP options* on page 11–192.

The unknown VLAN parameters are configured on a per interface basis using the CLI. The tagged, untagged, Auto, and Forbid options are configured in the VLAN context. Since dynamic VLANs operate as tagged VLANs, and it is possible that a tagged port on one device may not communicate with an untagged port on another device, GE Multilin recommends that you use tagged VLANs for the static VLANs.

A dynamic VLAN continues to exist on a port for as long as the port continues to receive advertisements of that VLAN from another device connected to that port or until you:

- Convert the VLAN to a static VLAN
- Reconfigure the port to Block or Disable
- Disable GVRP
- Save the configuration
- Reboot the switch

The time-to-live for dynamic VLANs is 10 seconds. That is, if a port has not received an advertisement for an existing dynamic VLAN during the last 10 seconds, the port removes itself from that dynamic VLAN.

Refer to *GVRP Operation Notes* on page 11–194 for additional information on using GVRP.

Multilink ML3000/ML3100

Chapter 12: Spanning Tree Protocol (STP)

12.1 Overview

12.1.1 Description

The Spanning Tree Protocol was designed to avoid loops in an Ethernet network. An Ethernet network using switches can have redundant paths, which may cause loops. To prevent loops, the MultiLink Switch Software uses the spanning tree protocol (STP). Controlling the span in which traffic traverses is necessary as a manager of the software. It is also necessary to specify the parameters of STP. STP is available as the IEEE 802.1d protocol and is a standard of the IEEE.

12.1.2 Features and Operation

The switch uses the IEEE 802.1d Spanning Tree Protocol (STP). When STP is enabled, it ensures that only one path at a time is active between any two nodes on the network. In networks where more than one physical path exists between two nodes, STP ensures only a single path is active by blocking all redundant paths. Enabling STP is necessary to avoid loops and duplicate messages. This duplication leads to a “broadcast storm” or other erratic behavior that can bring down the network.

As recommended in the IEEE 802.1Q VLAN standard, the MultiLink family of switches uses single-instance STP. This means a single spanning tree is created to make sure there are no network loops associated with any of the connections to the switch. This works regardless of whether VLANs are configured on the switch. Thus, these switches do not distinguish between VLANs when identifying redundant physical links.

The switch automatically senses port identity and type, and automatically defines port cost and priority for each type. The software allows a manager to adjust the cost, priority, the mode for each port as well as the global STP parameter values for the switch.

While allowing only one active path through a network at any time, STP retains any redundant physical path to serve as a backup (blocked) path in case the existing active path fails. Thus, if an active path fails, STP automatically activates (unblocks) an available backup to serve as the new active path for as long as the original active path is down.

The table below lists the default values of the STP variables. Refer to the following section for detailed explanation on the variables. By default, STP is disabled. To use STP, it has to be manually enabled.

Table 12–1: STP default values

Variable or attribute	Default value
STP capabilities	Disabled
Reconfiguring general operation priority	32768
Bridge maximum age	20 seconds
Hello time	2 seconds
Forward delay	15 seconds
Reconfiguring per-port STP path cost	0
Priority	32768
Mode	Normal
Monitoring of STP	Not available
Root Port	Not set

12.2 Configuring STP

The `show stp` command lists the switch's full STP configuration, including general settings and port settings, regardless of whether STP is enabled or disabled (default).

show stp *<config|ports>*

Example 12-1 illustrates the `show stp` command with the `config` parameter.

The variables listed in this example are defined as follows

- **Spanning Tree Enabled (Global)**: Indicates whether STP is enabled or disabled globally; that is, if the values is YES, all ports have STP enabled. Otherwise, all ports have STP disabled.
- **Spanning Tree Enabled (Ports)**: Indicates which ports have STP enabled. In the example, ports 9 through 16 have STP enabled, but STP functionality is not enabled. As such, STP will not perform on these ports.
- **Bridge Priority**: Specifies the switch (bridge) priority value. This value is used along with the switch MAC address to determine which switch in the network is the root device. Lower values indicate higher priority, and values range from 0 to 65535 with a default value of 32768.
- **Bridge Forward Delay**: Indicates the duration the switch waits from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds, with a default of 15.
- **Bridge Hello Time**: When the switch is the root device, this is the time between messages being transmitted. The value is from 1 to 10 seconds, with a default of 2.
- **Bridge Max Age**: This is the maximum time a message with STP information is allowed by the switch before the switch discards the information and updates the address table. Value range from 6 to 40 seconds with default value of 20.
- **Root Port**: Indicates the port number elected as the root port of the switch. A root port of "0" indicates STP is disabled.
- **Root Path Cost**: A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost indicates more loops, a lower cost indicates fewer loops. More loops equal more traffic and a tree which requires a long time to converge - resulting in a slower system.
- **Designated Root**: Displays the MAC address of the bridge in the network elected or designated as the root bridge. When STP is not enabled, the switch designates itself as the root switch.
- **Designated Root Priority**: Shows the designated root bridge's priority. The default value is 32768.

- **Root Bridge Forward Delay**: Indicates the designated root bridge forward delay. This is the time the switch waits before switching from the listening to the forwarding state. The default is 15 seconds, with a range of 4 to 30 seconds.
- **Root Bridge Hello Time**: Indicates the designated root bridge's hello time. Hello information is transmitted every 2 seconds.
- **Root Bridge Max Age**: Indicates the designated root bridge maximum age, after which it discards the information as being old and receives new updates.

These variables can be changed using the "priority", "cost", "port" and "timers" commands described later in this chapter.

Example 12-2 illustrates the `show stp` command with the `ports` parameter. The variables listed in this example are defined as follows:

- ***Port#***: indicates the port number. Value ranges from 01 to max number of ports in the switch

Example 12-1: Viewing STP configuration

```
ML3000# show stp config
 STP CONFIGURATION
 -----------------
 Spanning Tree Enabled(Global) : NO
 Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
 Protocol                 : Normal STP
 Bridge ID                : 80:00:00:20:06:25:ed:80
 Bridge Priority          : 32768
 Bridge Forward Delay     : 15
 Bridge Hello Time        : 2
 Bridge Max Age           : 20
 Root Port                : 0
 Root Path Cost           : 0
 Designated Root          : 80:00:00:20:06:25:ed:80
 Designated Root Priority : 32768
 Root Bridge Forward Delay : 15
 Root Bridge Hello Time   : 2
 Root Bridge Max Age      : 20

 RSTP CONFIGURATION
 -----------------
```

Example 12-2: Viewing STP ports

```
ML3000# show stp ports
 STP Port Configuration

 ------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State     Des. Bridge          Des. Port
 ------------------------------------------------------------------------------
 09    TP(10/100)  128       100       Disabled  80:00:00:20:06:25:ed:80  80:09
 10    TP(10/100)  128       100       Disabled  80:00:00:20:06:25:ed:80  80:0a
 11    TP(10/100)  128       100       Disabled  80:00:00:20:06:25:ed:80  80:0b
 12    TP(10/100)  128       100       Disabled  80:00:00:20:06:25:ed:80  80:0c
 13    TP(10/100)  128       100       Disabled  80:00:00:20:06:25:ed:80  80:0d
 14    TP(10/100)  128       100       Disabled  80:00:00:20:06:25:ed:80  80:0e
 15    TP(10/100)  128       100       Disabled  80:00:00:20:06:25:ed:80  80:0f
 16    TP(10/100)  128       100       Disabled  80:00:00:20:06:25:ed:80  80:10
```

- ***Type***: indicates the type of port - TP indicates Twisted Pair
- ***Priority***: STP uses this to determine which ports are used for forwarding. Lower the number means higher priority. Value ranges from 0 to 255. Default is 128
- ***Path Cost***: This is the assigned port cost value used for the switch to determine the forwarding points. Values range from 1 to 65535
- ***State***: indicates the STP state of individual ports. Values can be Listening, Learning, Forwarding, Blocking and Disabled.
- ***Des. Bridge***: This is the port's designated root bridge
- ***Des. Port***: This is the port's designated root port

To enable or disable STP, enter the STP configuration mode via the `stp` command and use the `stp enable` or `stp disable` command.

To `stp` command enters STP configuration mode:

stp

The `enable` and `disable` parameters start (enable) or stop (disable) STP.

stp *<enable|disable>*

The `stp` and `rstp` parameters set the spanning tree protocol to be IEEE 802.1d or 802.1w (Rapid Spanning Tree Protocol).

set stp *type=<stp|rstp>*

The `show active-stp` command display which version of STP is currently active.

show active-stp

NOTICE

Incorrect STP settings can adversely affect network performance. GE recommends starting with the default STP settings. Changing the settings requires a detailed understanding of STP. For more information on STP, please refer to the IEEE 802.1d standard.

NOTE

It is always a good idea to check which mode of STP is active. If the proper mode is not active, the configuration command `stp` will not be understood. To set the proper mode, use the `set stp` command.

Example 12-3 shows how to enable STP using the above commands.

Example 12-3: Enabling STP

```
ML3000# show active-stp
 Current Active Mode: RSTP.
 RSTP is Disabled.
ML3000# stp
 ERROR: Invalid Command
ML3000# set stp type=stp
 STP Mode set to STP.
ML3000# stp
ML3000(stp)## stp enable
 Successfully set the STP status
ML3000(stp)## show stp config
 STP CONFIGURATION
 -----------------
 Spanning Tree Enabled(Global) : YES
 Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
 Protocol                : Normal STP
 Bridge ID               : 80:00:00:20:06:25:ed:80
 Bridge Priority          : 32768
 Bridge Forward Delay     : 15
 Bridge Hello Time        : 2
 Bridge Max Age           : 20
 Root Port               : 0
 Root Path Cost           : 0
 Designated Root          : 80:00:00:20:06:25:ed:80
 Designated Root Priority    : 32768
 Root Bridge Forward Delay   : 15
 Root Bridge Hello Time      : 2
 Root Bridge Max Age         : 20
 RSTP CONFIGURATION
 -----------------
 Rapid STP/STP Enabled(Global) : NO
ML3000(stp)## show stp ports
 STP Port Configuration
 ------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State       Des. Bridge           Des. Port
 ------------------------------------------------------------------------------------
 09    TP(10/100)  128       100        Forwarding  80:00:00:20:06:25:ed:80  80:09
 10    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
 11    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
 12    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
 13    TP(10/100)  128       19         Forwarding  80:00:00:20:06:25:ed:80  80:0d
 14    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
```

The `priority` command specifies the port or switch level priority. When a port(s) are specified the priority is associated with ports and their value is 0 to 255. If no ports are specified, then the switch (bridge) priority is specified and its value is 0 to 65535. This value is used along with the switch MAC address to determine which switch in the network is the root device. Lower values mean higher priority. The default value is 32768.

priority *[port=<number|list|range>]*
value=<0-255 | 0-65535>

The `cost` command is port specific. A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost means the link is "more expensive" to use and falls in the passive mode compared to the link with a lower cost. Value ranges from 0 to 65535, with a default value of 32768.

cost *port=<number|list|range>*
value=<0-65535>

The `port` command assigns ports to STP. If you are unsure, let the software make the decisions. The `status` parameter enables or disables a port from participating in STP discovery. Its best to only allow trunk ports to participate in STP. End stations need not participate in STP process.

port *port=<number|list|range>*
status=<enable|disable>

The `timers` command changes the STP forward delay, hello timer and aging timer values. The `forward-delay` parameter indicates the time duration the switch will wait from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds with a default value of 15. When the switch is the root device, the `hello` parameter represents the time between messages being transmitted. The value is from 1 to 10 seconds with a default value is 2. The `age` parameter is the maximum time a message with STP information is allowed by the switch before the switch discards the information and updates the address table again. Value ranges from 6 to 40 seconds with default value of 20.

timers *forward-delay=<4-30> hello=<1-10> age=<6-40>*

Example 12-4: Configuring STP parameters

```
ML3000(stp)## show stp config
 STP CONFIGURATION
 -----------------
 Spanning Tree Enabled(Global) : NO
 Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
 Protocol                 : Normal STP
 Bridge ID                : 80:00:00:20:06:25:ed:80
 Bridge Priority          : 32768
 Bridge Forward Delay     : 15
 Bridge Hello Time        : 2
 Bridge Max Age           : 20
 Root Port                : 0
 Root Path Cost           : 0
 Designated Root          : 80:00:00:20:06:25:ed:80
 Designated Root Priority : 32768
 Root Bridge Forward Delay : 15
 Root Bridge Hello Time   : 2
 Root Bridge Max Age      : 20

 RSTP CONFIGURATION
 -----------------
 Rapid STP/STP Enabled(Global) : NO
ML3000(stp)## show stp ports
 STP Port Configuration

 ------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State     Des. Bridge           Des. Port
 ------------------------------------------------------------------------------------
 09    TP(10/100)  128      100       Disabled   80:00:00:20:06:25:ed:80  80:09
 10    TP(10/100)  128      100       Disabled   80:00:00:20:06:25:ed:80  80:0a
 11    TP(10/100)  128      100       Disabled   80:00:00:20:06:25:ed:80  80:0b
 12    TP(10/100)  128      100       Disabled   80:00:00:20:06:25:ed:80  80:0c
 13    TP(10/100)  128      100       Disabled   80:00:00:20:06:25:ed:80  80:0d
 14    TP(10/100)  128      100       Disabled   80:00:00:20:06:25:ed:80  80:0e
 15    TP(10/100)  128      100       Disabled   80:00:00:20:06:25:ed:80  80:0f
 16    TP(10/100)  128      100       Disabled   80:00:00:20:06:25:ed:80  80:10
ML3000(stp)## stp enable
```

Configuring STP parameters (continued)

```
ML3000(stp)## show stp config

 STP CONFIGURATION
 -----------------
 Spanning Tree Enabled(Global) : YES
 Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
 Protocol                : Normal STP
 Bridge ID               : 80:00:00:20:06:25:ed:80
 Bridge Priority         : 32768
 Bridge Forward Delay    : 15
 Bridge Hello Time       : 2
 Bridge Max Age          : 20
 Root Port               : 0
 Root Path Cost          : 0
 Designated Root         : 80:00:00:20:06:25:ed:80
 Designated Root Priority    : 32768
 Root Bridge Forward Delay   : 15
 Root Bridge Hello Time      : 2
 Root Bridge Max Age         : 20

 RSTP CONFIGURATION
 -----------------
 Rapid STP/STP Enabled(Global) : NO

ML3000(stp)## show stp ports

 STP Port Configuration

 ------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State       Des. Bridge           Des. Port
 ------------------------------------------------------------------------------------
 09     TP(10/100)  128      100        Forwarding  80:00:00:20:06:25:ed:80  80:09
 10     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:0a
 11     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:0b
 12     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:0c
 13     TP(10/100)  128      19         Forwarding  80:00:00:20:06:25:ed:80  80:0d
 14     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:0e
 15     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:0f
 16     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:10

ML3000(stp)## priority value=15535

 Successfully set the bridge priority

ML3000(stp)## show stp config

 STP CONFIGURATION
 -----------------
 Spanning Tree Enabled(Global) : YES
 Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
 Protocol                : Normal STP
 Bridge ID               : 80:00:00:20:06:25:ed:80
 Bridge Priority         : 15535
 Bridge Forward Delay    : 15
 Bridge Hello Time       : 2
 Bridge Max Age          : 20
 Root Port               : 0
 Root Path Cost          : 0
 Designated Root         : 80:00:00:20:06:25:ed:80
 Designated Root Priority    : 15535
```

Ports that have connected devices now participate in STP.

STP is now enabled. Note the default values for the discussed variables.

Configuring STP parameters (continued)

```
RSTP CONFIGURATION
-----------------
Rapid STP/STP Enabled(Global) : NO
ML3000(stp)## priority port=13 value=20
Successfully set the priority for port 13
ML3000(stp)## show stp ports
STP Port Configuration
-------------------------------------------------------------------------------------
Port#  Type       Priority  Path Cost  State       Des. Bridge           Des. Port
-------------------------------------------------------------------------------------
09    TP(10/100)  128       100        Forwarding  80:00:00:20:06:25:ed:80  80:09
10    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
11    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
12    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
13    TP(10/100)  20        19         Forwarding  80:00:00:20:06:25:ed:80  80:0d
14    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
15    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
16    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:10
ML3000(stp)## cost port=13 value=20
Setting cost for STP...Successfully set the path cost for port 13
ML3000(stp)## show stp ports
STP Port Configuration
-------------------------------------------------------------------------------------
Port#  Type       Priority  Path Cost  State       Des. Bridge           Des. Port
-------------------------------------------------------------------------------------
09    TP(10/100)  128       100        Forwarding  80:00:00:20:06:25:ed:80  80:09
10    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
11    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
12    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
13    TP(10/100)  20        20         Forwarding  80:00:00:20:06:25:ed:80  80:0d
14    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
15    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
16    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:10
ML3000(stp)## port port=9 status=disable
Successfully set the STP status for port 9
ML3000(stp)## show stp ports
STP Port Configuration
-------------------------------------------------------------------------------------
Port#  Type       Priority  Path Cost  State       Des. Bridge           Des. Port
-------------------------------------------------------------------------------------
10    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
11    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
12    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
13    TP(10/100)  20        20         Forwarding  80:00:00:20:06:25:ed:80  80:0d
14    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
15    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
16    TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:10
```

Since port 9 does not participate in STP, it is not listed here. Any changes made to STP parameters on port 9 will be ignored

Configuring STP parameters (continued)

```
ML3000(stp)## port port=9 status=enable
 Successfully set the STP status for port 9
ML3000(stp)## show stp ports
 STP Port Configuration
 ----------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State       Des. Bridge           Des. Port
 ----------------------------------------------------------------------------------------
 09     TP(10/100)  128      100        Forwarding  80:00:00:20:06:25:ed:80  80:09
 10     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:0a
 11     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:0b
 12     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:0c
 13     TP(10/100)  20       20         Forwarding  80:00:00:20:06:25:ed:80  80:0d
 14     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:0e
 15     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:0f
 16     TP(10/100)  128      100        Disabled    80:00:00:20:06:25:ed:80  80:10
ML3000(stp)## show stp config
 STP CONFIGURATION
 -----------------
 Spanning Tree Enabled(Global) : YES
 Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
 Protocol                  : Normal STP
 Bridge ID                 : 80:00:00:20:06:25:ed:80
 Bridge Priority           : 15535
 Bridge Forward Delay      : 15
 Bridge Hello Time         : 2
 Bridge Max Age            : 20
 Root Port                 : 0
 Root Path Cost            : 0
 Designated Root           : 80:00:00:20:06:25:ed:80
 Designated Root Priority  : 15535
 Root Bridge Forward Delay : 15
 Root Bridge Hello Time    : 2
 Root Bridge Max Age       : 20

 RSTP CONFIGURATION
 -----------------
 Rapid STP/STP Enabled(Global) : NO
ML3000(stp)## timers forward-delay=20 hello=5 age=40
 ERROR:  Invalid Values
       Max Age <= (2*(Forward-Delay-1)) and Max Age >= (2*(Hello-Time+1))
ML3000(stp)## timers forward-delay=20 hello=5 age=30
 Successfully set the bridge time parameters
```

The age parameter is out of range as per the IEEE 802.1d specifications.

(continued on next page)

Configuring STP parameters (continued)

```
ML3000(stp)## show stp config
 STP CONFIGURATION
 -----------------
 Spanning Tree Enabled(Global) : YES
 Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
 Protocol                  : Normal STP
 Bridge ID                 : 80:00:00:20:06:25:ed:80
 Bridge Priority           : 15535
 Bridge Forward Delay      : 20
 Bridge Hello Time         : 5
 Bridge Max Age            : 30
 Root Port                 : 0
 Root Path Cost            : 0
 Designated Root           : 80:00:00:20:06:25:ed:80
 Designated Root Priority  : 15535
 Root Bridge Forward Delay : 20
 Root Bridge Hello Time    : 5
 Root Bridge Max Age       : 30

 RSTP CONFIGURATION
 ------------------
```

Multilink ML3000/ML3100

Chapter 13: Rapid Spanning Tree Protocol

13.1 Overview

13.1.1 Description

The Rapid Spanning Tree Protocol (RTSP), like STP, was designed to avoid loops in an Ethernet network. Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w) is an evolution of the Spanning Tree Protocol (STP) (802.1d standard) and provides for faster spanning tree convergence after a topology change.

13.1.2 RSTP Concepts

The IEEE 802.1d Spanning Tree Protocol (STP) was developed to allow the construction of robust networks that incorporate redundancy while pruning the active topology of the network to prevent loops. While STP is effective, it requires that frame transfer must halt after a link outage until all bridges in the network are sure to be aware of the new topology. Using STP (IEEE 802.1d) recommended values, this period lasts 30 seconds.

The Rapid Spanning Tree Protocol (IEEE 802.1w) is a further evolution of the 802.1d Spanning Tree Protocol. It replaces the settling period with an active handshake between switches (bridges) that guarantees topology information to be rapidly propagated through the network. RSTP converges in less than one second. RSTP also offers a number of other significant innovations. These include

- Topology changes in STP must be passed to the root bridge before they can be propagated to the network. Topology changes in RSTP can be originated from and acted upon by any designated switch (bridge), leading to more rapid propagation of address information
- STP recognizes one state - blocking for ports that should not forward any data or information. RSTP explicitly recognizes two states or blocking roles - alternate and backup port including them in computations of when to learn and forward and when to block
- STP relays configuration messages received on the root port going out of its designated ports. If an STP switch (bridge) fails to receive a message from its

neighbor it cannot be sure where along the path to the root a failure occurred. RSTP switches (bridges) generate their own configuration messages, even if they fail to receive one from the root bridge. This leads to quicker failure detection

- RSTP offers edge port recognition, allowing ports at the edge of the network to forward frames immediately after activation while at the same time protecting them against loops
- An improvement in RSTP allows configuration messages to age more quickly preventing them from "going around in circles" in the event of a loop

RSTP has three states. They are discarding, learning and forwarding.

The ***discarding*** state is entered when the port is first taken into service. The port does not learn addresses in this state and does not participate in frame transfer. The port looks for STP traffic in order to determine its role in the network. When it is determined that the port will play an active part in the network, the state will change to ***learning***. The learning state is entered when the port is preparing to play an active member of the network. The port learns addresses in this state but does not participate in frame transfer. In a network of RSTP switches (bridges) the time spent in this state is usually quite short. RSTP switches (bridges) operating in STP compatibility mode will spend between 6 to 40 seconds in this state. After 'learning' the bridge will place the port in the ***forwarding*** state. While in this state the port both learns addresses and participates in frame transfer while in this state.

The result of these enhanced states is that the IEEE 802.1d version of spanning tree (STP) can take a fairly long time to resolve all the possible paths and to select the most efficient path through the network. The IEEE 802.1w Rapid reconfiguration of Spanning Tree significantly reduces the amount of time it takes to establish the network path. The result is reduced network downtime and improved network robustness. In addition to faster network reconfiguration, RSTP also implements greater ranges for port path costs to accommodate the higher connection speeds that are being implemented.

Proper implementations of RSTP (by switch vendors) is designed to be compatible with IEEE 802.1d STP. GE recommends that you employ RSTP or STP in your network.

13.1.3 Transition from STP to RSTP

IEEE 802.1w RSTP is designed to be compatible with IEEE 802.1D STP. Even if all the other devices in your network are using STP, you can enable RSTP on the MultiLink family of switches. The default configuration values of the RSTP available in ML3000 software will ensure that your switch will inter-operate effectively with the existing STP devices. RSTP automatically detects when the switch ports are connected to non-RSTP devices using spanning tree and communicates with those devices using 802.1d STP BPDU packets.

Even though RSTP inter-operates with STP, RSTP is more efficient at establishing the network path and network convergence in case of a very fast failure. As such, GE recommends that all network devices be updated to support RSTP. RSTP offers convergence times typically less than one second. However, to make best use of RSTP and achieve the fastest possible convergence times, there are some changes required to the RSTP default configuration.

1. Under some circumstances, it is possible for the rapid state transitions employed by RSTP to result in an increase in the rates of frame duplication and the order in which the frames are sent and received. To allow RSTP switches to support applications and protocols that may be sensitive to frame duplication and out of sequence frames, RSTP may have to be explicitly set to be compatible with STP. This requires setting the "Force Protocol Version" parameter to be STP compatible. This parameter should be set to all ports on a given switch.

2. As indicated above, one of the benefits of RSTP is the implementation of a larger range of port path costs that accommodates higher network speeds. New default values have been implemented for path costs associated with the different network speeds. This may create incompatibility between devices running the older implementations of STP a switch running RSTP.
3. At any given time, the software can support either STP or RSTP but not both.

13.2 Configuring RSTP through the Command Line Interface

13.2.1 Normal RSTP

The commands to setup and configure RSTP are as follows. The `set stp` command sets the switch to support RSTP or STP. It is necessary to save and reboot the switch after this command.

set stp *type=<stp|rstp>* -

The `rstp` command enters the RSTP configuration mode and enables/disabled RSTP. By default, RSTP is disabled and has to be manually activated.

rstp

rstp *<enable|disable>*

rstp *<romode|normal>*

The syntax for the `port` command on RSTP is shown below.

port *port=<number|list|range> [status=<enable|disable>] [migration=<enable>] [edge=<enable|disable>] [p2p=<on|off|auto>]*

The `p2p` parameter sets the "point-to-point" value to off on all ports connected to shared LAN segments (i.e. connections to hubs). The default value is `auto`. P2P ports would typically be end stations or computers on the network.

The `edge` parameter enables/disables all ports connected to other hubs, bridges and switches as edge ports.

The `migration` parameter is set for all ports connected to devices such as hubs, bridges and switches known to support IEEE 802.1d STP services but not RSTP services

The `show active-stp` command displays whether STP or RSTP is running.

show active-stp

The `show stp` command display the RSTP or STP parameters.

show stp *<config|ports>*

Users may notice extended recovery time if there is a mix of firmware revisions in the Mesh or Ring.

The variables listed by the `show stp config` command are:

- **Rapid Spanning Tree Enabled (Global)**: Indicates whether STP is enabled or disabled globally i.e. if the values is YES, all ports have STP enabled, otherwise, all ports have STP disabled.
- **Rapid Spanning Tree Enabled Ports**: Indicates which ports have RSTP enabled.
- **Protocol**: Indicates whether STP or RSTP is being used. It also indicates if RSTP is used in Smart RSTP (ring-only mode) or normal mode.
- **Bridge Priority**: Specifies the switch (bridge) priority value. This value is used along with the switch MAC address to determine which switch in the network is the root device. Lower values mean higher priority. Values range from 0 to 65535 with a default of 0.
- **Bridge Forward Delay**: Indicates the time duration the switch will wait from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds with a default of 15.

- **Bridge Hello Time**: When the switch is the root device, this is the time between messages being transmitted. The value is from 1 to 10 seconds with a default of 2.
- **Bridge Max Age**: This is the maximum time a message with STP information is allowed by the switch before the switch discards the information and updates the address table again. Values range from 6 to 40 seconds with a default value of 20.
- **Root Port**: Indicates the port number, which is elected as the root port of the switch. A root port of "0" indicates STP is disabled.
- **Root Path Cost**: A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost means more loops; a lower cost means fewer loops. More loops equal more traffic and a tree which takes a long time to converge, resulting in a slower system.
- **Designated Root**: Shows the MAC address of the bridge in the network elected or designated as the root bridge.
- **Designated Root Priority**: Shows the designated root bridge's priority. The default value is 0.
- **Root Bridge Forward Delay**: Indicates the designated root bridge's forward delay. This is the time the switch waits before it switches from the listening to the forwarding state. This value can be set between 4 to 30 seconds, with a default of 15.
- **Root Bridge Hello Time**: Indicates the designated root bridge's hello time. Hello information is sent out every 2 seconds.
- **Root Bridge Max Age**: Indicates the designated root bridge's maximum age, after which it discards the information as being old and receives new updates.
- **Topology Change Count**: Since the last reboot, the number of times the topology has changed. Use this in conjunction with "show uptime" to find the frequency of the topology changes.
- **Time Since topology Change**: The number of seconds since the last topology change.

Example 13-1: Enabling RSTP and reviewing the RSTP variables

```
ML3000# rstp
ML3000(rstp)## show stp config
 RSTP CONFIGURATION
 ----------------
 Rapid STP/STP Enabled(Global) : NO
ML3000(rstp)## rstp enable
 Successfully set the RSTP status
ML3000(rstp)## show active-stp
 Current Active Mode: RSTP.
 RSTP is Enabled.
ML3000(rstp)## show stp config
 RSTP CONFIGURATION
 ----------------
 Rapid STP/STP Enabled(Global) : YES
 RSTP/STP Enabled Ports      : 9,10,11,12,13,14,15,16
 Protocol                    : Normal RSTP
 Bridge ID                   : 80:00:00:20:06:25:ed:89
 Bridge Priority             : 0
 Bridge Forward Delay        : 15
 Bridge Hello Time           : 2
 Bridge Max Age              : 20
 Root Port                   : 0
 Root Path Cost              : 0
 Designated Root             : 80:00:00:20:06:25:ed:89
 Designated Root Priority    : 0
 Root Bridge Forward Delay   : 15
 Root Bridge Hello Time      : 2
 Root Bridge Max Age         : 20
 Topology Change Count       : 0
 Time Since Topology Chg     : 12
ML3000(rstp)## show stp config
 RSTP CONFIGURATION
 ----------------
 Rapid STP/STP Enabled(Global) : YES
 RSTP/STP Enabled Ports      : 9,10,11,12,13,14,15,16
 Protocol                    : Normal RSTP Ring Only Mode
 Bridge ID                   : 80:00:00:20:06:25:ed:89
 Bridge Priority             : 0
 Bridge Forward Delay        : 15
 Bridge Hello Time           : 2
 Bridge Max Age              : 20
 Root Port                   : 0
 Root Path Cost              : 0
 Designated Root             : 80:00:00:20:06:25:ed:89
 Designated Root Priority    : 0
 Root Bridge Forward Delay   : 15
 Root Bridge Hello Time      : 2
 Root Bridge Max Age         : 20
```

The variables listed by the `show stp ports` command are:

- **Port#**: Indicates the port number. The value ranges from 1 to the maximum number of ports in the switch.
- **Type**: Indicates the type of port. TP indicates twisted pair.
- **Priority**: STP uses this to determine which ports are used for forwarding. Lower numbers indicate higher priority. The values range from 0 to 255, with a default of 128.
- **Path Cost**: This is the assigned port cost value used for the switch to determine the forwarding points. Values range from 1 to 2000000. Lower values indicate a lower cost and hence the preferred route. The costs for different Ethernet speeds are indicated below. The Path cost in STP is compared to the path cost in RSTP.

Table 13–1: Path cost as defined in IEEE 802.1d / 802.1w

Port type	STP path cost	RSTP path cost
10 Mbps	100	2000000
100 Mbps	19	200000
1 Gbps	4	20000
10 Gbps	2	2000

- **State**: Indicates the STP state of individual ports. Values can be Listening, Learning, Forwarding, Blocking and Disabled.
- **Des. Bridge**: This is the port's designated root bridge
- **Des. Port**: This is the port's designated root port

Example 13-2: Reviewing the RSTP port parameters

```
ML3000(rstp)## show stp ports
 RSTP Port Configuration

 ------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State       Des. Bridge           Des. Port
 ------------------------------------------------------------------------------------
 09     TP(10/100)  128      2000000    Forwarding  80:00:00:20:06:25:ed:89  80:09
 10     TP(10/100)  128      2000000    Disabled                    80:0a
 11     TP(10/100)  128      2000000    Disabled                    80:0b
 12     TP(10/100)  128      2000000    Disabled                    80:0c
 13     TP(10/100)  20       200000     Forwarding  80:00:00:20:06:25:ed:89  80:0d
 14     TP(10/100)  128      2000000    Disabled                    80:0e
 15     TP(10/100)  128      2000000    Disabled                    80:0f
 16     TP(10/100)  128      2000000    Disabled                    80:10
```

Another example of the same command, from a larger network with several switches is shown in Example 13-3. Note the `show stp ports` command can be executed from the manager level prompt or from RSTP configuration state as shown in the screen captures earlier.

Example 13-3: RSTP information from a network with multiple switches

```
ML3000(rstp)## show stp ports
 RSTP Port Configuration

 ----------------------------------------------------------------------------------
 Port# Type       Priority Path Cost State      Des. Bridge          Des. Port
 ----------------------------------------------------------------------------------
 01   TP(10/100) 128      2000000   Disabled                        00:01
 02   TP(10/100) 128      2000000   Disabled                        00:02
 03   TP(10/100) 128      2000000   Disabled                        00:03
 04   TP(10/100) 128      2000000   Disabled                        00:04
 05   TP(10/100) 20       2000000   Disabled                        00:05
 06   TP(10/100) 128      200000    Forwarding 80:00:00:20:06:30:00:01 00:06
 07   TP(10/100) 128      200000    Disacrding 80:00:00:20:06:2b:0f:e1 00:07
 08   TP(10/100) 128      2000000   Disabled                        00:08
 09   Gigabit    128      20000     Forwarding 80:00:00:20:06:2b:0f:e1 00:09
 10   Gigabit    128      20000     Forwarding 80:00:00:20:06:30:00:01 00:0a
```

In this example, ports 9 and 10 have a path cost of 20000 and are the least cost paths. These ports are connected to other switches and the ports are enabled as forwarding ports. Ports 6 and 7 are also connected to other switches. From the state column, it indicates that port 7 is in a standby state as that port is discarding all traffic.

More CLI commands associated with RSTP in the RSTP configuration mode are shown below. The `forceversion` command sets the STP or RSTP compatibility mode.

forceversion *<stp|rstp>*

The `show-forceversion` command displays the current forced version.

show-forceversion

The `show-timers` command displays the values of the timers set for RSTP.

show-timers

The `priority` command specifies the switch (bridge) priority value. This value is used along with the switch MAC address to determine which switch in the network is the root device. Lower values mean higher priority. The value ranges from 0 to 65535 with a default of 32768. When port are specified, the priority is associated with ports and their value is 0 to 255.

priority *[port=<number|list|range>]*
value=<0-255|0-65535>

A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost means the link is "more expensive" to use and falls in the passive mode compared to the link with a lower cost. The value of the `cost` command ranges from 0 to 65535, with a default of 32768.

cost *port=<number|list|range>*
value=<0-65535>

The `port` command assigns ports for RSTP. Note that specific ports may not need to participate in RSTP process. These ports typically would be end-stations. If unsure, it is best to let the software make the decisions.

port *port=<number|list|range> status=<enable|disable>*

The `status` parameter enables or disables a port from participating in RSTP discovery. Its best to only allow trunk ports to participate in RSTP; end stations need not participate in the RSTP process.

The `timers` command changes the STP forward delay, hello timer and aging timer values.

timers *forward-delay=<4-30> hello=<1-10> age=<6-40>*

The `forward-delay` parameter indicates the time duration the switch will wait from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds with a default of 15.

The `hello` parameter represents the time between messages being transmitted when the switch is the root device. The value is 1 to 10 seconds, with a default of 2.

The `age` parameter is the maximum time a message with STP information is allowed by the switch before the switch discards the information and updates the address table again. Value ranges from 6 to 40 seconds with default value of 20.

Example 13-4: Configuring RSTP

```
ML3000# rstp
ML3000(rstp)## show stp config

 RSTP CONFIGURATION
 ------------------
 Rapid STP/STP Enabled(Global) : NO
ML3000(rstp)## show active-stp

 Current Active Mode: RSTP.
 RSTP is Disabled.
ML3000(rstp)## rstp enable

 Successfully set the RSTP status
ML3000(rstp)## show active-stp

 Current Active Mode: RSTP.
 RSTP is Enabled.
ML3000(rstp)## show stp config

 RSTP CONFIGURATION
 ------------------
 Rapid STP/STP Enabled(Global) : YES
 RSTP/STP Enabled Ports      : 9,10,11,12,13,14,15,16
 Protocol                    : Normal RSTP
 Bridge ID                   : 80:00:00:20:06:25:ed:89
 Bridge Priority             : 0
 Bridge Forward Delay        : 15
 Bridge Hello Time           : 02
 Bridge Max Age              : 20
 Root Port                   : 0
 Root Path Cost              : 0
 Designated Root             : 80:00:00:20:06:25:ed:89
 Designated Root Priority    : 0
 Root Bridge Forward Delay   : 15
 Root Bridge Hello Time      : 02
 Root Bridge Max Age         : 20
 Topology Change Count       : 0
 Time Since Topology Chg     : 33
ML3000(rstp)## show stp ports

 RSTP Port Configuration

 ------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State       Des. Bridge           Des. Port
 ------------------------------------------------------------------------------------
 09     TP(10/100)  128      2000000    Forwarding  80:00:00:20:06:25:ed:89  00:09
 10     TP(10/100)  128      2000000    Disabled                             00:0a
 11     TP(10/100)  128      2000000    Disabled                             00:0b
 12     TP(10/100)  128      2000000    Disabled                             00:0c
 13     TP(10/100)  128      200000     Forwarding  80:00:00:20:06:25:ed:89  00:0d
 14     TP(10/100)  128      2000000    Disabled                             00:0e
 15     TP(10/100)  128      2000000    Disabled                             00:0f
 16     TP(10/100)  128      2000000    Disabled                             00:10
ML3000(rstp)## forceversion rstp

 Error: Force Version already set to Normal RSTP
```

Check the status of STP or RSTP. These commands show if STP or RSTP is enabled.

Configuring RSTP (continued)

```
ML3000(rstp)## forceversion stp
ML3000(rstp)## show-forceversion
 Force Version : Force to STP only
ML3000(rstp)## show stp config
 RSTP CONFIGURATION
 ----------------
 Rapid STP/STP Enabled(Global) : YES
 RSTP/STP Enabled Ports      : 9,10,11,12,13,14,15,16
 Protocol                    : Force to STP only
 Bridge ID                   : 80:00:00:20:06:25:ed:89
 Bridge Priority             : 0
 Bridge Forward Delay        : 15
 Bridge Hello Time           : 02
 Bridge Max Age              : 20
 Root Port                   : 0
 Root Path Cost              : 0
 Designated Root             : 80:00:00:20:06:25:ed:89
 Designated Root Priority    : 0
 Root Bridge Forward Delay   : 15
 Root Bridge Hello Time      : 02
 Root Bridge Max Age         : 20
 Topology Change Count       : 0
 Time Since Topology Chg     : 100
ML3000(rstp)## forceversion rstp
ML3000(rstp)## show-forceversion
 Force Version : Normal RSTP
ML3000(rstp)## show stp config
 RSTP CONFIGURATION
 ----------------
 Rapid STP/STP Enabled(Global) : YES
 RSTP/STP Enabled Ports      : 9,10,11,12,13,14,15,16
 Protocol                    : Normal RSTP
 Bridge ID                   : 80:00:00:20:06:25:ed:89
 Bridge Priority             : 0
 Bridge Forward Delay        : 15
 Bridge Hello Time           : 02
 Bridge Max Age              : 20
 Root Port                   : 0
 Root Path Cost              : 0
 Designated Root             : 80:00:00:20:06:25:ed:89
 Designated Root Priority    : 0
 Root Bridge Forward Delay   : 15
 Root Bridge Hello Time      : 02
 Root Bridge Max Age         : 20
 Topology Change Count       : 0
 Time Since Topology Chg     : 141
ML3000(rstp)## show-timers
 Forward Delay Timer : 15 sec
 Hello Timer         : 2 sec
```

The `forceversion` capability can be used for compatibility with STP devices. In this example, the switch is forced to STP mode.

Using `forceversion`, the switch is now operating using RSTP. Note the `show stp config` command also indicates the switch protocol is RSTP.

Configuring RSTP (continued)

```
ML3000(rstp)## show stp ports
 RSTP Port Configuration

 ---------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State       Des. Bridge          Des. Port
 ---------------------------------------------------------------------------------------
 09     TP(10/100)  128      2000000    Forwarding  80:00:00:20:06:25:ed:89  00:09
 10     TP(10/100)  128      2000000    Disabled                     00:0a
 11     TP(10/100)  128      2000000    Disabled                     00:0b
 12     TP(10/100)  128      2000000    Disabled                     00:0c
 13     TP(10/100)  128      200000     Forwarding  80:00:00:20:06:25:ed:89  00:0d
 14     TP(10/100)  128      2000000    Disabled                     00:0e
 15     TP(10/100)  128      2000000    Disabled                     00:0f
 16     TP(10/100)  128      2000000    Disabled                     00:10
ML3000(rstp)## priority port=13 value=100
ML3000(rstp)## show stp ports
 RSTP Port Configuration

 ---------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State       Des. Bridge          Des. Port
 ---------------------------------------------------------------------------------------
 09     TP(10/100)  128      2000000    Forwarding  80:00:00:20:06:25:ed:89  00:09
 10     TP(10/100)  128      2000000    Disabled                     00:0a
 11     TP(10/100)  128      2000000    Disabled                     00:0b
 12     TP(10/100)  128      2000000    Disabled                     00:0c
 13     TP(10/100)  100      200000     Forwarding  80:00:00:20:06:25:ed:89  00:0d
 14     TP(10/100)  128      2000000    Disabled                     00:0e
 15     TP(10/100)  128      2000000    Disabled                     00:0f
 16     TP(10/100)  128      2000000    Disabled                     00:10
ML3000(rstp)## cost port=13 value=250000
ML3000(rstp)## show stp ports
 RSTP Port Configuration

 ---------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State       Des. Bridge          Des. Port
 ---------------------------------------------------------------------------------------
 09     TP(10/100)  128      2000000    Forwarding  80:00:00:20:06:25:ed:89  00:09
 10     TP(10/100)  128      2000000    Disabled                     00:0a
 11     TP(10/100)  128      2000000    Disabled                     00:0b
 12     TP(10/100)  128      2000000    Disabled                     00:0c
 13     TP(10/100)  100      250000     Forwarding  80:00:00:20:06:25:ed:89  00:0d
 14     TP(10/100)  128      2000000    Disabled                     00:0e
 15     TP(10/100)  128      2000000    Disabled                     00:0f
 16     TP(10/100)  128      2000000    Disabled                     00:10
ML3000(rstp)## port port=9 status=disable
```

(continued on next page)

Configuring RSTP (continued)

```
ML3000(rstp)## show stp ports

 RSTP Port Configuration

 ---------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State       Des. Bridge           Des. Port
 ---------------------------------------------------------------------------------------
 09     TP(10/100)  128      2000000    No STP                          00:09
 10     TP(10/100)  128      2000000    Disabled                        00:0a
 11     TP(10/100)  128      2000000    Disabled                        00:0b
 12     TP(10/100)  128      2000000    Disabled                        00:0c
 13     TP(10/100)  100      250000     Forwarding  80:00:00:20:06:25:ed:89  00:0d
 14     TP(10/100)  128      2000000    Disabled                        00:0e
 15     TP(10/100)  128      2000000    Disabled                        00:0f
 16     TP(10/100)  128      2000000    Disabled                        00:10

ML3000(rstp)## port port=9 status=enable

ML3000(rstp)## show stp ports

 RSTP Port Configuration

 ---------------------------------------------------------------------------------------
 Port#  Type       Priority  Path Cost  State       Des. Bridge           Des. Port
 ---------------------------------------------------------------------------------------
 09     TP(10/100)  128      2000000    Forwarding  80:00:00:20:06:25:ed:89  00:09
 10     TP(10/100)  128      2000000    Disabled                        00:0a
 11     TP(10/100)  128      2000000    Disabled                        00:0b
 12     TP(10/100)  128      2000000    Disabled                        00:0c
 13     TP(10/100)  100      250000     Forwarding  80:00:00:20:06:25:ed:89  00:0d
 14     TP(10/100)  128      2000000    Disabled                        00:0e
 15     TP(10/100)  128      2000000    Disabled                        00:0f
 16     TP(10/100)  128      2000000    Disabled                        00:10

ML3000(rstp)## timers forward-delay=20 hello=5 age=30

 Successfully set the bridge time parameters

ML3000(rstp)## show stp config

 RSTP CONFIGURATION
 ------------------
 Rapid STP/STP Enabled(Global) : YES
 RSTP/STP Enabled Ports       : 9,10,11,12,13,14,15,16
 Protocol                 : Normal RSTP
 Bridge ID                : 80:00:00:20:06:25:ed:89
 Bridge Priority          : 0
 Bridge Forward Delay     : 20
 Bridge Hello Time        : 05
 Bridge Max Age           : 30
 Root Port                : 0
 Root Path Cost           : 0
 Designated Root          : 80:00:00:20:06:25:ed:89
 Designated Root Priority     : 0
 Root Bridge Forward Delay    : 20
 Root Bridge Hello Time       : 05
 Root Bridge Max Age          : 30
 Topology Change Count        : 0
 Time Since Topology Chg      : 567
```

13.2.2 Smart RSTP (Ring-Only Mode) through the Command Line Interface

A special case of a mesh structure is a ring. In many networks, network managers prefer to create a ring structure for redundancy and simplicity of the topology. In a ring structure:

1. All switches in the network are GE Multilin switches.
2. RSTP is enabled on all the switches.
3. The topology is a ring.
4. All switches in the ring have been configured to use the Smart RSTP (ring only mode) (as shown below).
5. All switches in the ring must use the same firmware revision.

The ring structure can demonstrate fast recovery times, typically faster than what RSTP can recover from a single fault. In many situations RSTP will recover in seconds, whereas smart RSTP (ring-only mode) will recover in milliseconds.

To configure Ring-Only mode, ensure the first three of the four situations described above are met.

RSTP mode has to be enabled before any configuration to the ring-only mode.

The RSTP command enters the RSTP configuration mode and enables/disables RSTP. By default, RSTP is disabled and has to be manually activated.

rstp
rstp *<enable|disable>*

The syntax for the *romode* command on RSTP is shown below.

romode add port=<port|list|range>
romode del port=<port|list|range>
romode <enable|disable>
romode show

The sequence of commands for enabling ring-only mode is shown in the following example:

Example 13-5: Configuring smart RSTP, ring-only mode

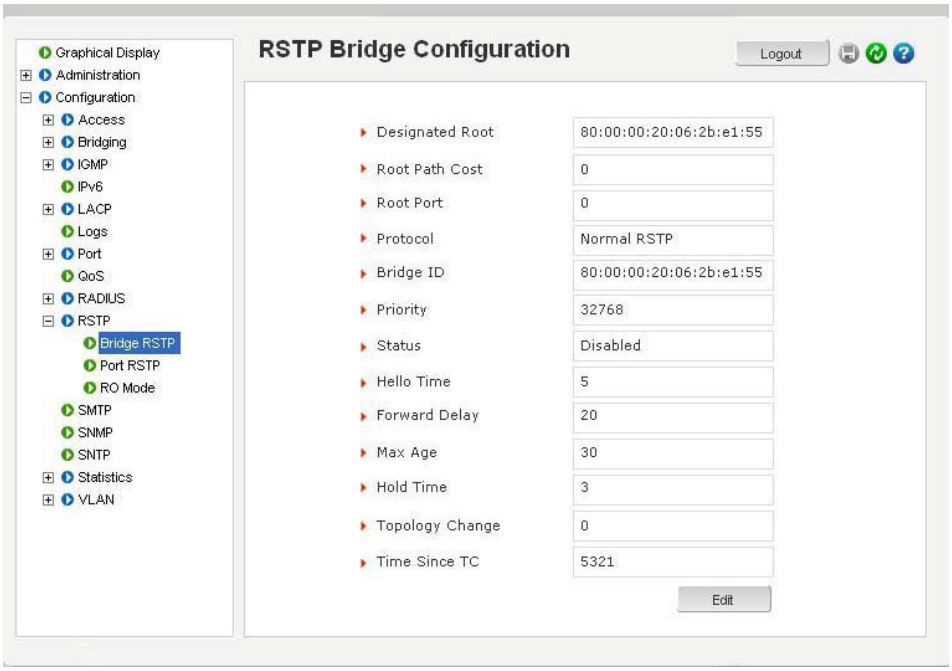
```
ML3000# rstp

ML3000(rstp)##rstp enable
Successfully set the RSTP status

ML3000(rstp)##romode show
 RO-MODE status      : Disabled
 RO-MODE set on ports : NONE

ML3000(rstp)##romode add port=1,2
      Added Ports: 1,2

ML3000(rstp)##romode enable
RSTP Ring Only Mode Enabled.

ML3000(rstp)##romode show
 RO-MODE status      : Enabled
 RO-MODE set on ports : 1,2

ML3000(rstp)##romode disable
RSTP Ring Only Mode Disabled.
```

13.3 Configuring STP/RSTP with EnerVista Secure Web Management software

13.3.1 Normal RSTP

To setup and configure RSTP, select the **Configure > RSTP** menu items. In setting up RSTP or STP, it is advised that the system defaults are used for weights and other parameters. Only when specific ports are required to be the active link should the default values change.

In the window below, RSTP or STP is disabled. The designated root is set to zero as RSTP is disabled.

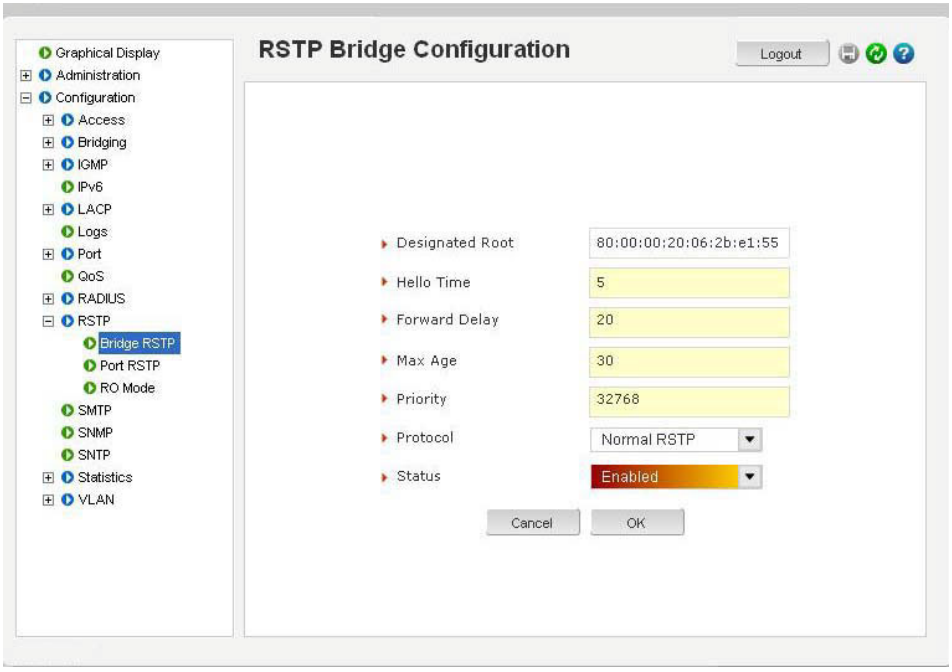


The RSTP bridge configuration parameters are defined below.

- **Designated Root**: Shows the MAC address of the bridge in the network elected or designated as the root bridge. Normally, when STP is not enabled, the switch designates itself as the root switch.
- **Root Path Cost**: A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost means more loops; a lower cost fewer loops. More loops equal more traffic and a tree which takes a long time to converge, resulting in a slower system
- **Root Port**: Indicates the port number, which is elected as the root port of the switch. A root port of "0" indicates STP is disabled.
- **Protocol**: Indicates whether STP or RSTP is being used. It also indicates if RSTP is used in Smart RSTP (ring-only mode) or normal mode.
- **Bridge ID**: Indicates the MAC address of the current bridge over which traffic will flow.
- **Bridge Priority**: Specifies the switch (bridge) priority value. This value is used along with the switch MAC address to determine which switch in the network is the root device. Lower values mean higher priority. The value ranges from 0 to 65535, with a default of 32768
- **Status**: Indicates whether STP or RSTP is enabled.

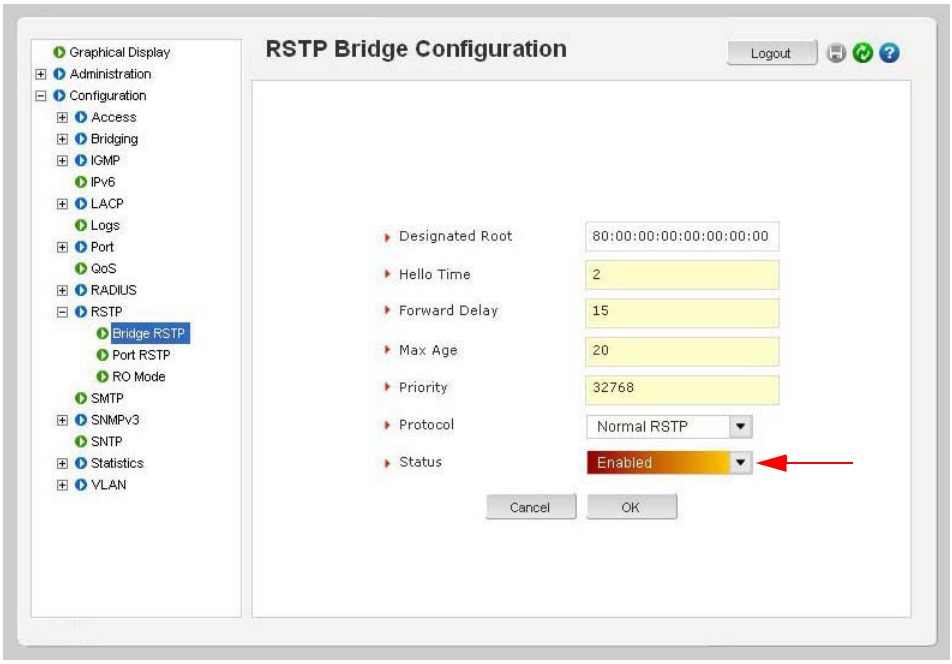
- **Bridge Hello Time**: When the switch is the root device, this is the time between messages being transmitted. The value is from 1 to 10 seconds, with a default of 2.
- **Bridge Forward Delay**: Indicates the time duration the switch will wait from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds, with a default of 15.
- **Bridge Max Age**: This is the maximum time a message with STP information is allowed by the switch before the switch discards the information and updates the address table again. The value ranges from 6 to 40 seconds with a default 20.
- **Hold Time**: This is the minimum time period to elapse between the transmissions of configuration BPDUs through a given LAN Port. At most one configuration BPDU shall be transmitted in any hold time period. This parameter is a fixed parameter, with values as specified in RSTP standard (3 seconds).
- **Topology Change**: A counter indicating the number of times topology has changed.
- **Time since TC**: Indicates time that has elapsed since the last topology change. Use this in conjunction with uptime on the graphical display (screen shown after a successful login) to find the frequency of the topology changes.

▷ Click on **Edit** to make any changes.
On this screen, you can select and enable STP or RSTP.



▷ Under protocol, select “Force to STP” if there are legacy or other third party devices that do not support RSTP.

▷ Otherwise it is recommended to enable “Normal RSTP”.

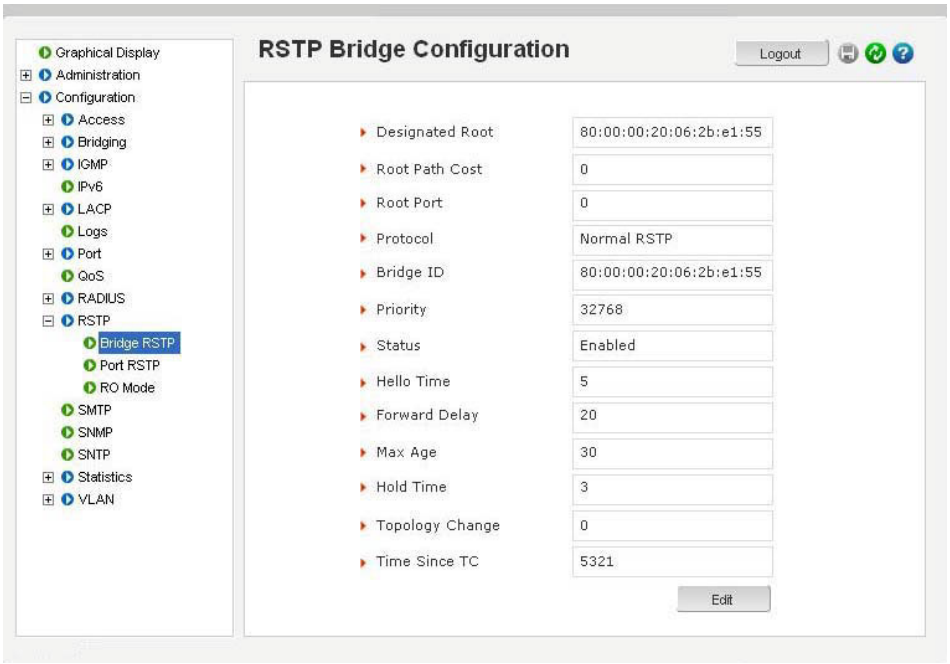


Once again, if you are not familiar with the STP or RSTP parameter settings, is best to use the default values.

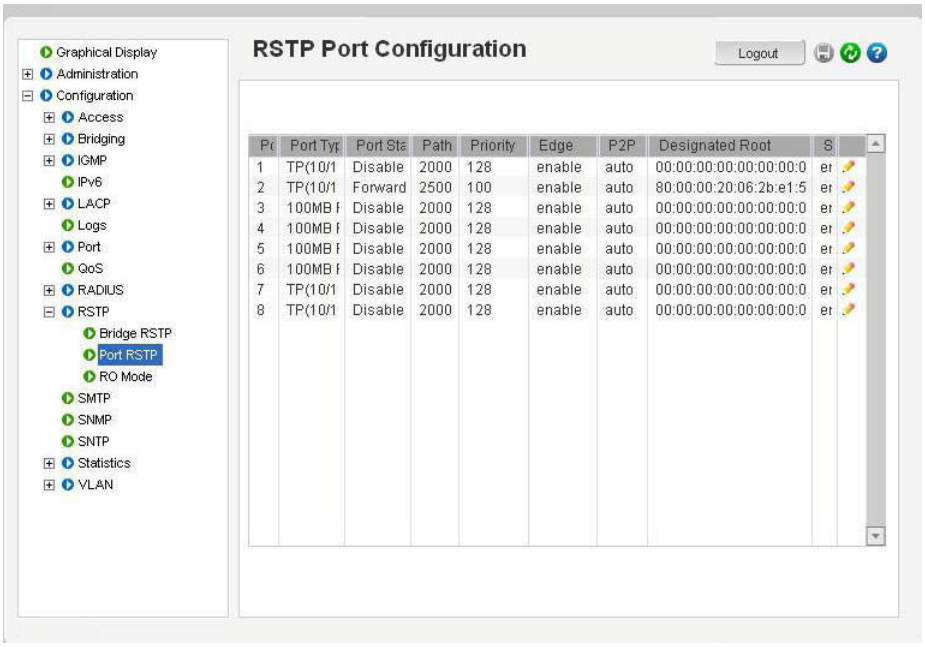
▷ Simply enable RSTP (or STP) and let the system default values prevail.

After RSTP is enabled, the fields are updated.

▷ Note the **Status**, **Time since TC**, and **Designated Root** values.



The port specific values for RSTP or STP are shown below.



▷ Click on the edit icon ( ) to edit the values for a specific port.

The columns in the above window are defined as follows:

- **Port#**: Indicates the port number. Value ranges from 1 to the maximum number of ports in the switch.
- **Port Type**: Indicates the type of port and speed; TP indicates twisted-pair.
- **Port State**: Forwarding implies traffic is forwarded onto the next switch or device connected the port. Disabled implies that the port may be turned off or the device connected to it may be unplugged or turned off. Values can be Listening, Learning, Forwarding, Blocking and Disabled.
- **Path Cost**: This is the assigned port cost value used for the switch to determine the forwarding points. Values range from 1 to 2000000. The lower the value, the lower the cost and hence the preferred route. The costs for different Ethernet speeds are shown below. The STP path cost is compared to the RSTP path cost.

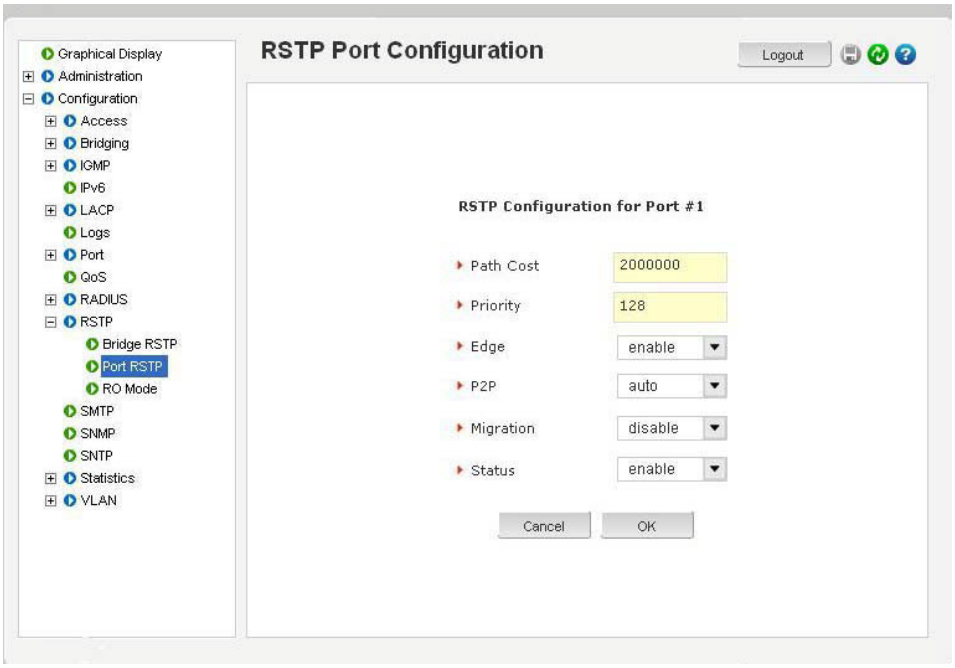
Table 13–2: Path cost defined in IEEE 802.1d and 802.1w

Port Type	STP Path cost	RSTP Path cost
10 Mbps	100	2 000 000
100 Mbps	19	200 000
1 Gbps	4	20 000
10 Gbps	2	2000

- **Priority**: STP uses this to determine which ports are used for forwarding. Lower the number means higher priority. Value ranges from 0 to 255. Default is 128
- **Edge Ports**: RSTP offers edge port recognition, allowing ports at the edge of the network to forward frames immediately after activation while at the same time protecting them against loops.

- **P2P Ports**: set the "point-to-point" value to off on all ports that are connected to shared LAN segments (i.e. connections to hubs). The default value is auto. P2P ports would typically be end stations or computers on the network.
- **Designated Root**: MAC Address of the Root Bridge in the tree
- **Status**: status of STP/RSTP for the port.

The STP or RSTP values can be changed for each port as shown below.



Migration is enabled for all ports connected to other devices such as hubs, bridges and switches known to support IEEE 802.1d STP services and cannot support RSTP services.

Status is normally enabled - in certain cases the Status can be set to disabled to turn off RSTP or STP on that port.

13.3.2 Smart RSTP (Ring-Only Mode) with EnerVista Secure Web Management Software

13.3.2.1 For Switches Running on Firmware Version 3.x

A ring is a special case mesh structure. In many networks, network managers prefer to create a ring structure for topological redundancy and simplicity. In a ring structure:

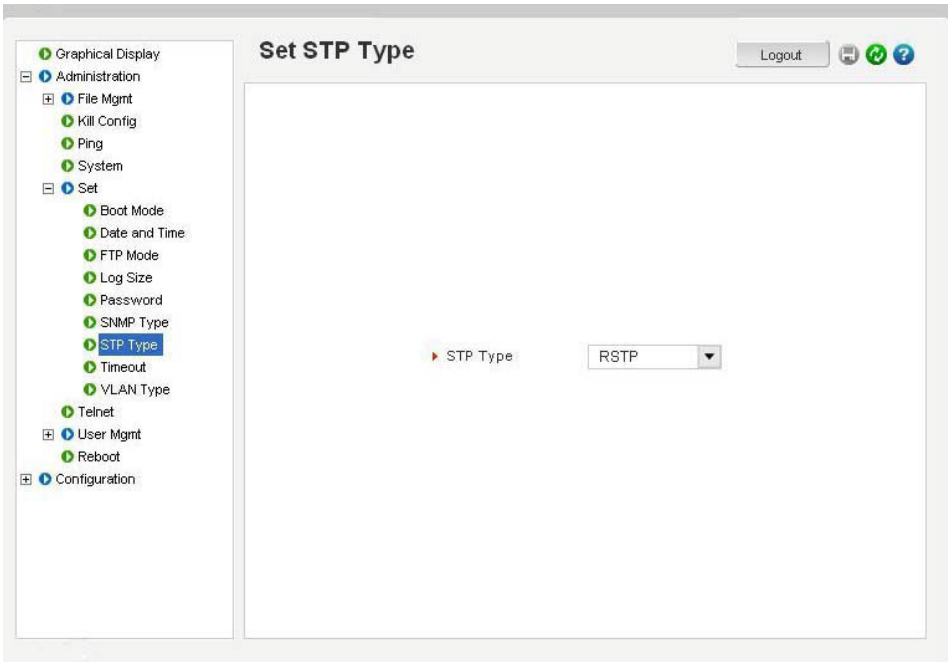
1. All switches in the network are GE Multilin switches.
2. RSTP is enabled on all the switches.
3. The topology is a ring.
4. All switches in the ring have been configured to use the ring-only mode (as shown below).
5. All switches in the ring myst use the same firmware revision.

The ring structure can demonstrate fast recovery times, typically faster than what RSTP can recover from a single fault. In many situations RSTP will recover in seconds, whereas smart RSTP (Ring-Only mode) will recover in milliseconds.

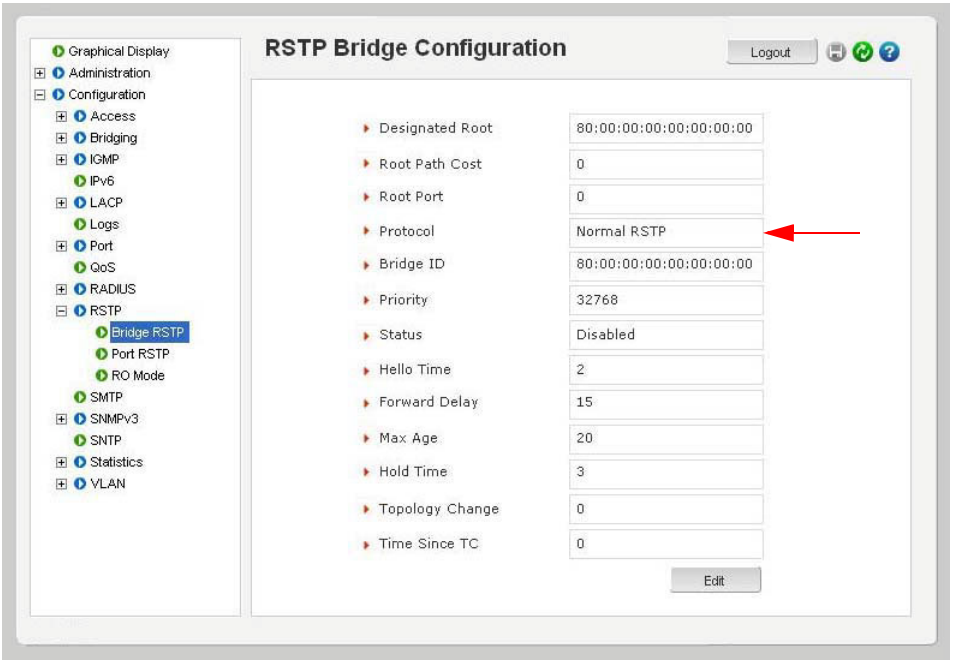
To configure ring-only mode, ensure the first three of the four situations described above are met.

To enable ring-only mode, first

▷ Enable RSTP by setting the **STP Type** to RSTP in the **Administration > Set > STP Type** menu:



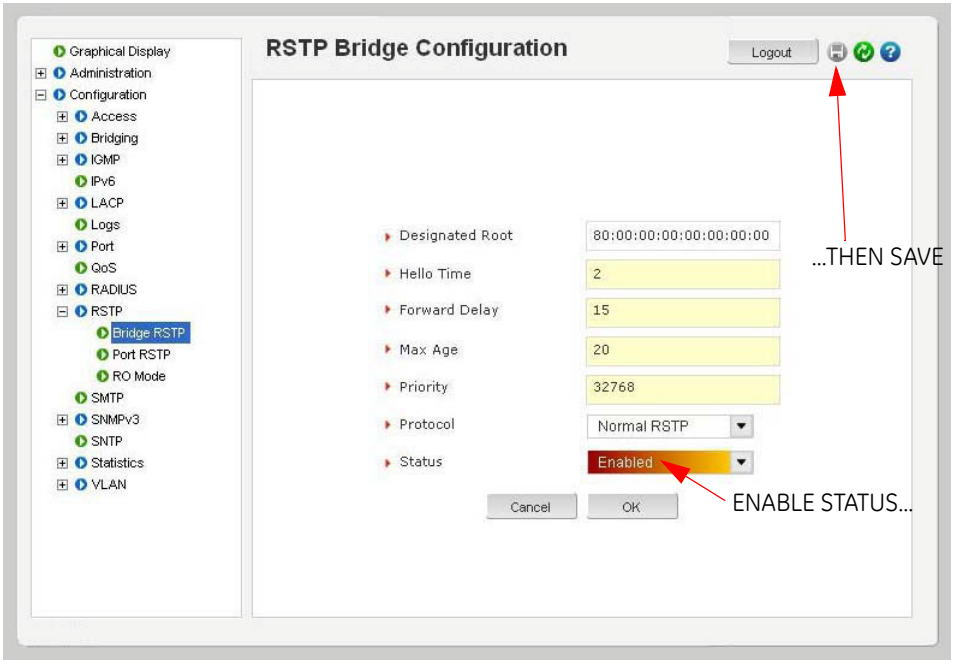
▷ Select the **Configuration > RSTP > Bridge RSTP** menu as shown below.



▷ Click the Edit button to configure RSTP.

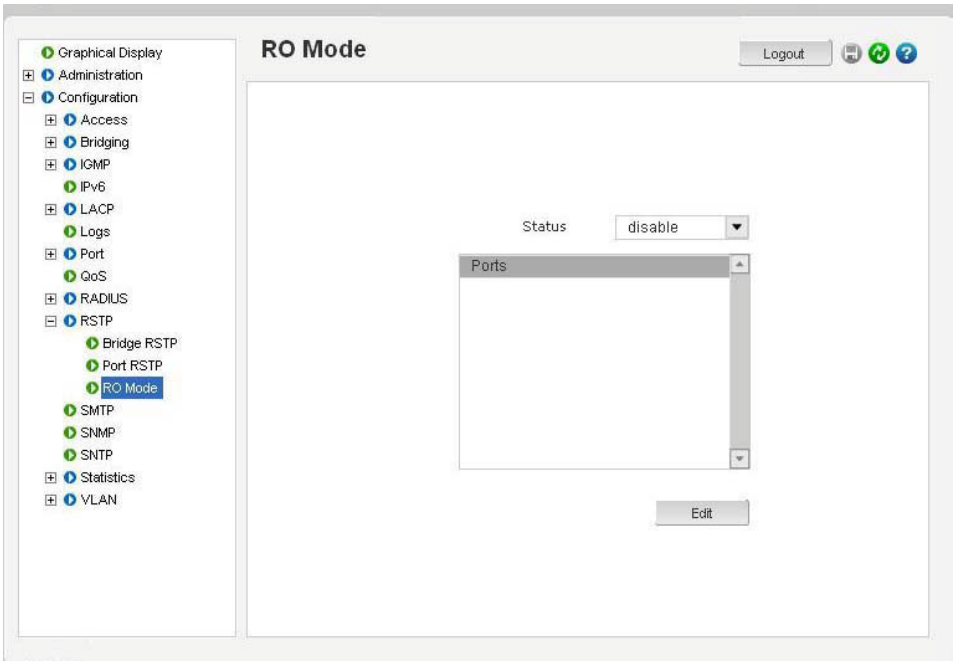
▷ Once in Edit mode, change the Status to Enable.

▷ Save Configuration.



To reset RSTP back to normal mode, select "Normal RSTP" for the **Protocol** setting. Save the configuration by clicking on the icon.

▷ Select the **Configuration > RSTP > RO Mode** menu as shown below:

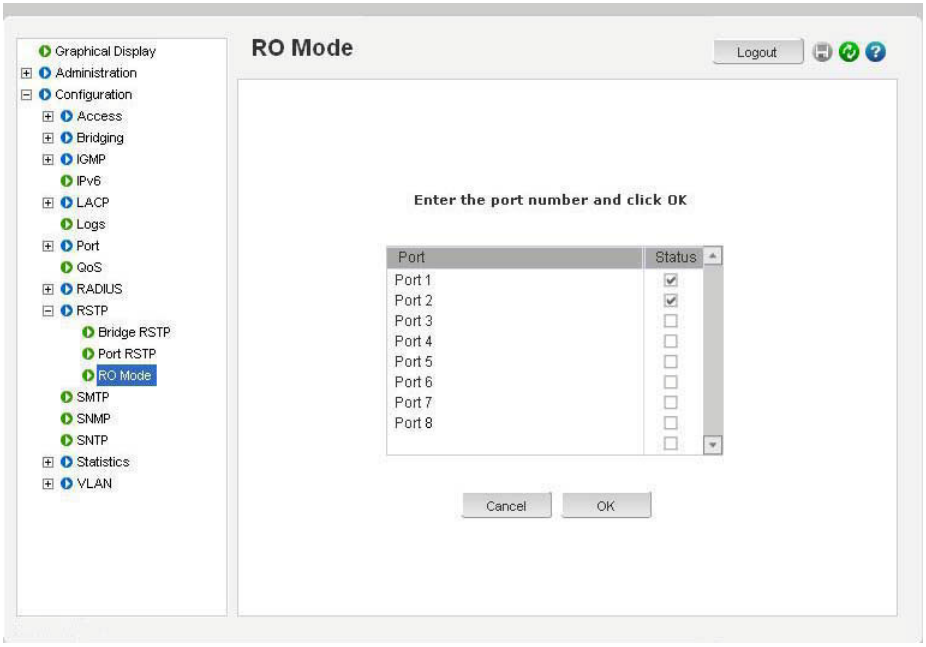


▷ Click the **Edit** button to configure RO Mode.

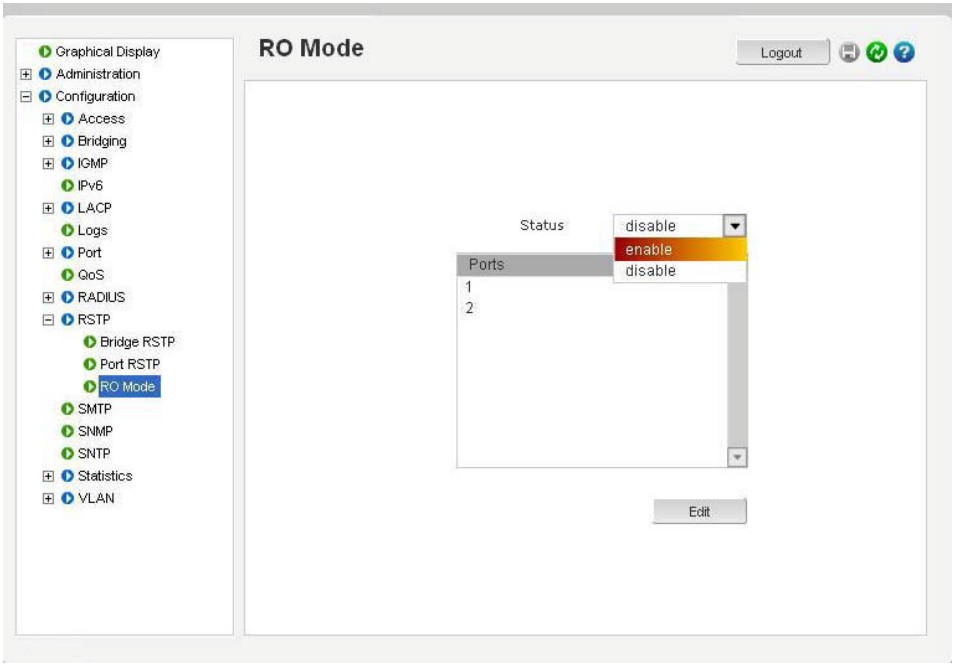
▷ Select the desired ports as shown below, then click **OK** to exit.

NOTE

Only 2 ports can be selected to Ring Only Mode.



▷ Select the **Enabled** option for the Status setting as shown below:



▷ Save the configuration by clicking on the icon.

13.3.2.2 For One or More Switches Running on Firmware Version 2.x or Lower

A ring is a special case mesh structure. In many networks, network managers prefer to create a ring structure for topological redundancy and simplicity. In a ring structure special case:

1. All switches in the network are GE Multilin switches.

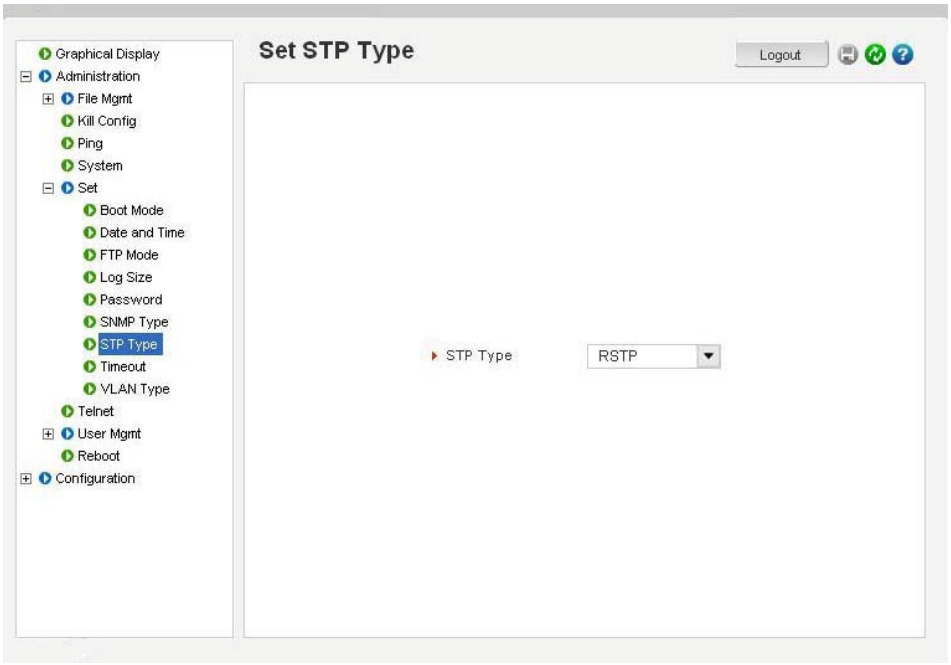
2. RSTP is enabled on all the switches.
3. The topology is a ring.
4. All switches in the ring have been configured to use the ring-only mode (as shown below).

The ring structure can demonstrate fast recovery times, typically faster than what RSTP can recover from a single fault. In many situations RSTP will recover in seconds, whereas smart RSTP (ring-only mode) will recover in milliseconds.

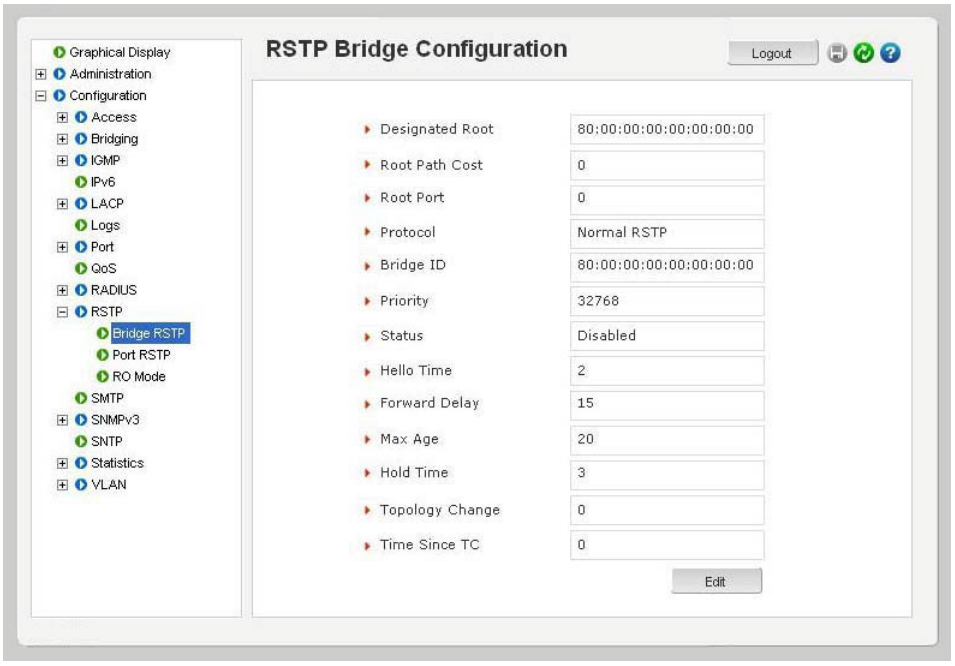
To configure ring-only mode, ensure the first three of the four situations described above are met.

To enable ring-only mode, first

▷ Enable RSTP by setting the STP Type to RSTP in the **Administration > Set > STP Type** menu:



▷ Select the **Configuration > RSTP > Bridge RSTP** menu as shown below.



▷ Click the **Edit** button to configure RSTP.

▷ Select the "Ring Only Mode" (RO Mode) option for the Protocol setting as shown below.

To reset RSTP back to normal mode, select "Normal RSTP" for the Protocol setting. Save the configuration by clicking on the icon.

Multilink ML3000/ML3100

Chapter 14: Quality of Service

14.1 QoS Overview

14.1.1 Description

Quality of Service (QoS) refers to the capability of a network to provide different priorities to different types of traffic. Not all traffic in the network has the same priority. Being able to differentiate different types of traffic and allowing this traffic to accelerate through the network improves the overall performance of the network and provides the necessary quality of service demanded by different users and devices. The primary goal of QoS is to provide priority including dedicated bandwidth.

14.1.2 QoS Concepts

The MultiLink family of switches supports QoS as specified in the IEEE 802.1p and IEEE 802.1q standards. QoS is important in network environments where there are time-critical applications, such as voice transmission or video conferencing, which can be adversely effected by packet transfer delays or other latency in a network.

Most switches today implement buffers to queue incoming packets as well as outgoing packets. In a queue mechanism, normally the packet which comes in first leaves first (FIFO) and all the packets are serviced accordingly. Imagine, if each packet had a priority assigned to it. If a packet with a higher priority than other packets were to arrive in a queue, the packet would be given a precedence and moved to the head of the queue and would go out as soon as possible. The packet is thus preempted from the queue and this method is called preemptive queuing.

Preemptive queuing makes sense if there are several levels of priorities, normally more than two. If there are too many levels, then the system has to spend a lot of time managing the preemptive nature of queuing. IEEE 802.1p defines and uses eight levels of priorities. The eight levels of priority are enumerated 0 to 7, with 0 the lowest priority and 7 the highest.

To make the preemptive queuing possible, most switches implement at least two queue buffers. The MultiLink family of switches has two priority queues, 1 (low) and 0 (high).When tagged packets enter a switch port, the switch responds by placing the packet into one of the two queues, and depending on the precedence levels the queue could be rearranged to meet the QoS requirements.

14.1.3 DiffServ and QoS

QoS refers to the level of preferential treatment a packet receives when it is being sent through a network. QoS allows time sensitive packets such as voice and video, to be given priority over time insensitive packets such as data. Differentiated Services (DiffServ or DS) are a set of technologies defined by the IETF (Internet Engineering Task Force) to provide quality of service for traffic on IP networks.

DiffServ is designed for use at the edge of an Enterprise where corporate traffic enters the service provider environment. DiffServ is a layer-3 protocol and requires no specific layer-2 capability, allowing it to be used in the LAN, MAN, and WAN. DiffServ works by tagging each packet (at the originating device or an intermediate switch) for the requested level of service it requires across the network.

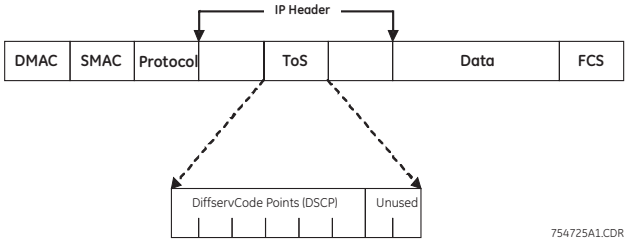


FIGURE 14–1: ToS and DSCP

DiffServ inserts a 6-bit DiffServ code point (DSCP) in the Type of Service (ToS) field of the IP header, as shown in the picture above. Information in the DSCP allows nodes to determine the Per Hop Behavior (PHB), which is an observable forwarding behavior for each packet. Per hop behaviors are defined according to:

- Resources required (e.g., bandwidth, buffer size)
- Priority (based on application or business requirements)
- Traffic characteristics (e.g., delay, jitter, packet loss)

Nodes implement PHBs through buffer management and packet scheduling mechanisms. This hop-by-hop allocation of resources is the basis by which DiffServ provides quality of service for different types of communications traffic.

14.1.4 IP Precedence

IP Precedence utilizes the three precedence bits in the IPv4 header's Type of Service (ToS) field to specify class of service for each packet. You can partition traffic in up to eight classes of service using IP precedence. The queuing technologies throughout the network can then use this signal to provide the appropriate expedited handling.

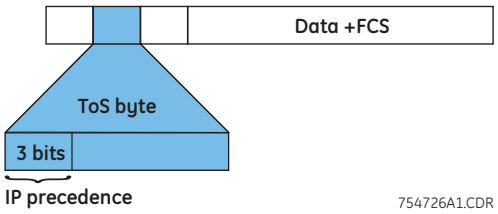


FIGURE 14–2: IP Precedence ToS Field in an IP Packet Header

The three most significant bits (correlating to binary settings 32, 64, and 128) of the Type of Service (ToS) field in the IP header constitute the bits used for IP precedence. These bits are used to provide a priority from 0 to 7 for the IP packet.

Because only three bits of the ToS byte are used for IP precedence, you need to differentiate these bits from the rest of the ToS byte.

The MultiLink family of switches has the capability to provide QoS at Layer 2. At Layer 2, the frame uses Type of Service (ToS) as specified in IEEE 802.1p. ToS uses 3 bits, just like IP precedence, and maps well from Layer 2 to layer 3, and vice versa.

The switches have the capability to differentiate frames based on ToS settings. With two queues present - high or low priority queues or buffers in MultiLink family of switches, frames can be placed in either queue and serviced via the weight set on all ports. This placement of queues, added to the weight set plus the particular tag setting on a packet allows each queue to have different service levels.

MultiLink QoS implementations provide mapping of ToS (or IP precedence) to Class of Service (CoS). A CoS setting in an Ethernet Frame is mapped to the ToS byte of the IP packet, and vice versa. A ToS level of 1 equals a CoS level of 1. This provides end-to-end priority for the traffic flow when MultiLink switches are deployed in the network.

NOTE

Not all packets received on a port have high priority. IGMP and BPDU packets have high priority by default.

The MultiLink family of switches has the capability to set the priorities based on three different functions. They are

- **Port QoS**: assigns a high priority to all packets received on a port, regardless of the type of packet.
- **TAG QoS**: if a packet contains a tag, the port on which the packet was received then looks to see at which level that tag value is set. Regardless of the tag value, if there is a tag, that packet is automatically assigned high priority (sent to the high priority queue)
- **ToS QoS**: (Layer 3) when a port is set to ToS QoS, the most significant 6-bits of the IPv4 packet (which has 64 bits) are used. If the 6 bits are set to ToS QoS for the specific port number the packet went to, that packet is assigned high priority by that port

14.2 Configuring QoS through the Command Line Interface

14.2.1 Commands

MultiLink switches support three types of QoS - Port based, Tag based and ToS based.

QoS is disabled by default on the switch. QoS needs to be enabled and configured.

The `qos` command enters the QoS configuration mode.

qos

The usage of the `setqos` command varies depending on the type of QOS. For example, for QOS type tag, the tag levels have to be set, and for QOS type ToS, the ToS levels have to be set. If the priority field is not set, it then defaults to low priority. ToS has 64 levels and the valid values are 0-63 and a tagged packet has 8 levels and the valid values are 0-7

setqos *type=<port|tag|tos|none> port=<port|list|range> [priority=<high|low>] [tos=<0-63|list|range>]*
[tag=<0-7|list|range>]

Setting the `type` parameter to none will clear the QoS settings.

The `set-weight` command sets the port priority weight for All the ports. Once the weight is set, all the ports will be the same weight across the switch. The valid value for weight is 0-7

set-weight *weight=<0-7>*

A weight is a number calculated from the IP precedence setting for a packet. This weight is used in an algorithm to determine when the packet will be serviced

The `show-portweight` command displays the weight settings on a port.

show-portweight

As mentioned previously, the switch is capable of detecting higher-priority packets marked with precedence by the IP forwarder and can schedule them faster, providing superior response time for this traffic. The IP Precedence field has values between 0 (the default) and 7. As the precedence value increases, the algorithm allocates more bandwidth to that traffic to make sure that it is served more quickly when congestion occurs. The MultiLink family of switches can assign a weight to each flow, which determines the transmit order for queued packets. In this scheme, lower weights (set on all ports) are provided more service. IP precedence serves as a divisor to this weighting factor. For instance, traffic with an IP Precedence field value of 7 gets a lower weight than traffic with an IP Precedence field value of 3, and thus has priority in the transmit order.

Once the port weight is set, the hardware will interpret the weight setting for all ports as outlined below (assuming the queues are sufficiently filled - if there are no packets, for example, in the high priority queue, packets are serviced on a first come first served - FCFS - basis from the low priority queue).

Table 14–1: Port weight settings

Value	Hardware traffic queue behavior
0	No priority - traffic is sent alternately from each queue and packets are queued alternately in each queue.
1	Two packets are sent from the HIGH priority queue and one packet from LOW priority queue.
2	Four packets are sent from the HIGH priority queue and one packet from LOW priority queue.
3	Six packets are sent from the HIGH priority queue and one packet from LOW priority queue.
4	Eight packets are sent from the HIGH priority queue and one packet from LOW priority queue.
5	Ten packets are sent from the HIGH priority queue and one packet from LOW priority queue.
6	Twelve packets are sent from the HIGH priority queue and one packet from LOW priority queue.
7	All packets are sent from the HIGH priority queue and none are sent from LOW priority queue.

The `show qos` command displays the QoS settings

show qos *[type=<port|tag|tos>] [port=<port|list|range>]*

Sometimes it is necessary to change the priority of the packets going out of a switch. For example, when a packet is received untagged and has to be transmitted with an addition of the 802.1p priority tag, the tag can be assigned depending on the `untag` value set. For example if the `untag` command is set to `port=1 tag=2 priority=low`, untagged packets received on that port will be tagged with a priority low upon transmit.

The `untag` command defines the 802.1p user priority assigned to untagged received packets to be transmitted as tagged from the priority queue.

set-untag *port=<port|list|range> priority=<high|normal|medium|low> tag=<0-7>*

14.2.2 Example

The following example shows how to configure QoS.

```
ML3000#show port

Keys: E  = Enable            D  = Disable
      H  = Half Duplex       F  = Full Duplex
      M  = Multiple VLAN's   NA = Not Applicable
      LI = Listening         LE = Learning
      F  = Forwarding        B  = Blocking

Port Name       Status Dplx Media  Link Trunk Speed Poe Auto Vlan GVRP STP
-------------------------------------------------------------------------------
 1   A1          E      H   1000SF DOWN No    1000  No    E      1    -    -
 2   A2          E      H   1000SF DOWN No    1000  No    E      1    -    -
 3   B1          E      H   3Spd   DOWN No    10    No    E      1    -    -
 4   B2          E      H   3Spd   DOWN No    10    No    E      1    -    -
 5   C1          E      H   10Tx   DOWN No    10    No    E      1    -    D
 6   C2          E      H   10Tx   DOWN No    10    No    E      1    -    D
 7   C3          E      F   100Tx  UP   No    100   No    E      1    -    -
 8   C4          E      F   100Tx  UP   No    100   No    E      1    -    -
13   E1          E      F   100Fx  DOWN No    100   No    D      1    -    -
14   E2          E      F   100Fx  DOWN No    100   No    D      1    -    -
15   E3          E      F   100Fx  DOWN No    100   No    D     30    -    -
16   E4          E      F   100Fx  DOWN No    100   No    D     30    -    -

ML3000#
ML3000#qos

ML3000(qos)##show qos

TAG Priority Map:
   Low: 0-7
   Medium: None
   Normal: None
   High: None

TOS Priority Map:
   Low: 0-63
   Medium: None
   Normal: None
   High: None

  ====================================
    PORT | DEFAULT |  TAG    |   TOS
  ====================================
     1   |   None    | Disable | Disable
     2   |   None    | Disable | Disable
     3   |   None    | Disable | Disable
     4   |   None    | Disable | Disable
     5   |   None    | Disable | Disable
     6   |   None    | Disable | Disable
     7   |   None    | Disable | Disable
     8   |   None    | Disable | Disable
    13   |   None    | Disable | Disable
    14   |   None    | Disable | Disable
    15   |   None    | Disable | Disable
    16   |   None    | Disable | Disable

ML3000(qos)##
```

```
ML3000(qos)##setqos port=13 priority=high type=port

Successfully set QOS.
ML3000(qos)##show qos type=port

  ================================
    PORT |    PRIORITY    | STATUS
  ================================
       1  |        None    |   DOWN
       2  |        None    |   DOWN
       3  |        None    |   DOWN
       4  |        None    |   DOWN
       5  |        None    |   DOWN
       6  |        None    |   DOWN
       7  |        None    |     UP
       8  |        None    |     UP
      13  |        HIGH    |   DOWN
      14  |        None    |   DOWN
      15  |        None    |   DOWN
      16  |        None    |   DOWN

ML3000(qos)##
```

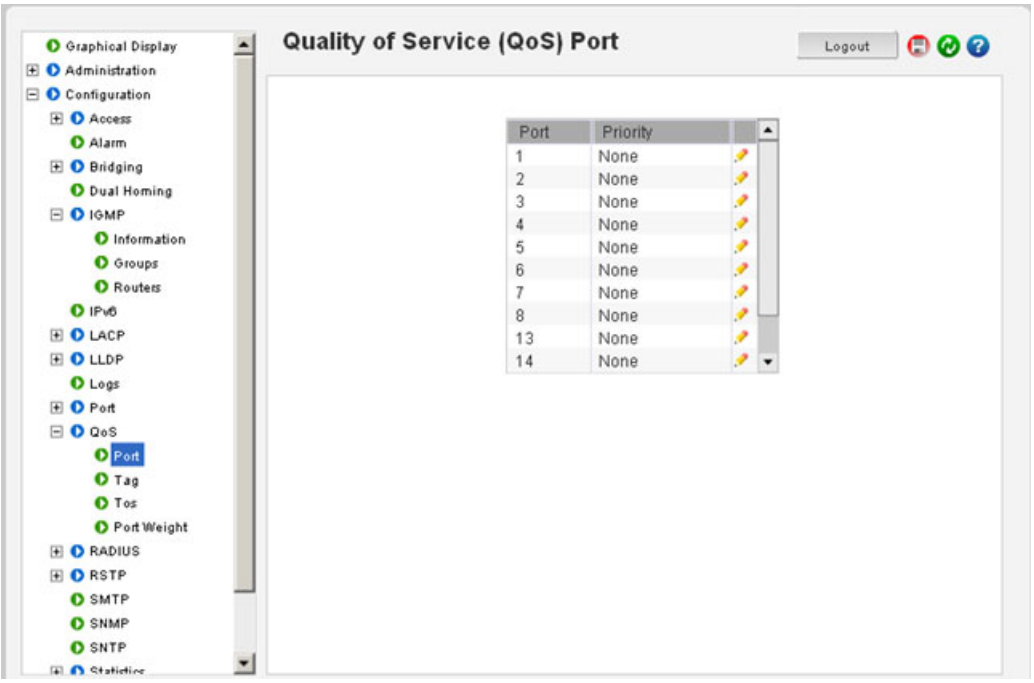
```
ML3000(qos)##setqos port=14 priority=high type=tag tag=6

Successfully set QOS.
ML3000(qos)##show qos

TAG Priority Map:
   Low: 0-7
   Medium: None
   Normal: None
   High: None

TOS Priority Map:
   Low: 0-63
   Medium: None
   Normal: None
   High: None

  ====================================
    PORT | DEFAULT |  TAG    |   TOS
  ====================================
     1   |    None    | Disable | Disable
     2   |    None    | Disable | Disable
     3   |    None    | Disable | Disable
     4   |    None    | Disable | Disable
     5   |    None    | Disable | Disable
     6   |    None    | Disable | Disable
     7   |    None    | Disable | Disable
     8   |    None    | Disable | Disable
    13   |    None    | Disable | Disable
    14   |    None    |  Enable | Disable
    15   |    None    | Disable | Disable
    16   |    None    | Disable | Disable

ML3000(qos)##
ML3000(qos)##show qos type=tag

  ========================================
  PORT | Pri for VPT | STATUS
       |   76543210  |
  ========================================
     1 |   --------  | DOWN
     2 |   --------  | DOWN
     3 |   --------  | DOWN
     4 |   --------  | DOWN
     5 |   --------  | DOWN
     6 |   --------  | DOWN
     7 |   --------  | UP
     8 |   --------  | UP
    13 |   --------  | DOWN
    14 |   LHLLLLLL  | DOWN
    15 |   --------  | DOWN
    16 |   --------  | DOWN

ML3000(qos)##

ML3000(qos)##setqos port=15 priority=hightype=tag tag=5

Successfully set QOS.
ML3000(qos)##show qos type=tag

  ========================================
  PORT | Pri for VPT | STATUS
       |   76543210  |
  ========================================
     1 |   --------  | DOWN
     2 |   --------  | DOWN
     3 |   --------  | DOWN
     4 |   --------  | DOWN
     5 |   --------  | DOWN
     6 |   --------  | DOWN
     7 |   --------  | UP
     8 |   --------  | UP
    13 |   --------  | DOWN
    14 |   LHLLLLLL  | DOWN
    15 |   LLHLLLLL  | DOWN
    16 |   --------  | DOWN

ML3000(qos)##
```

14.3 Configuring QoS with EnerVista Secure Web Management software

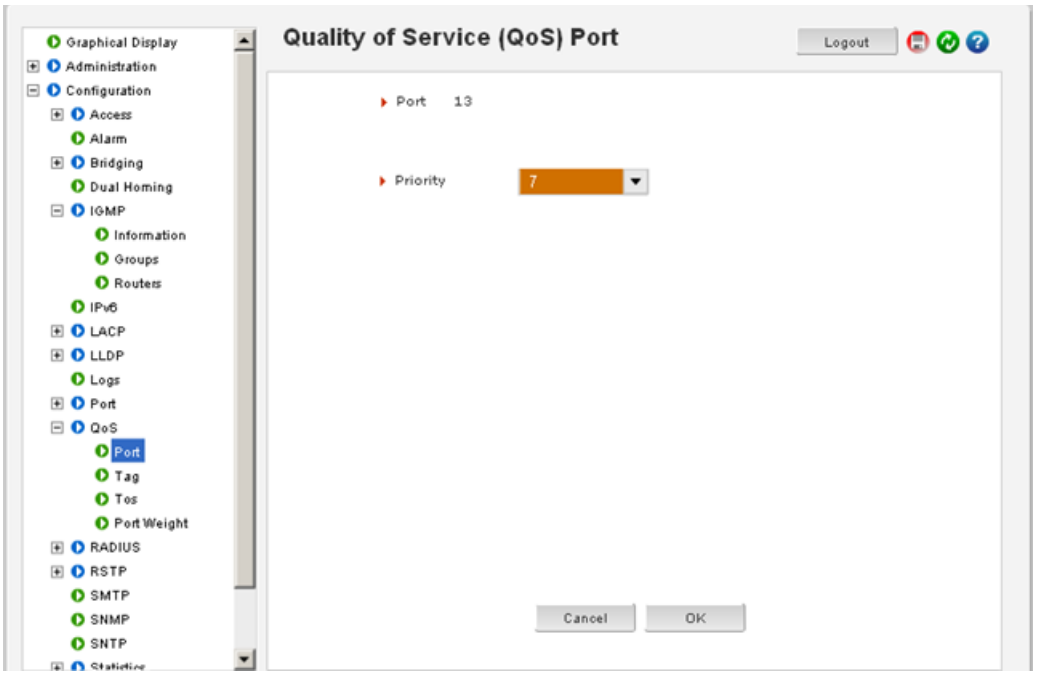
14.3.1 Description

To access QoS settings,

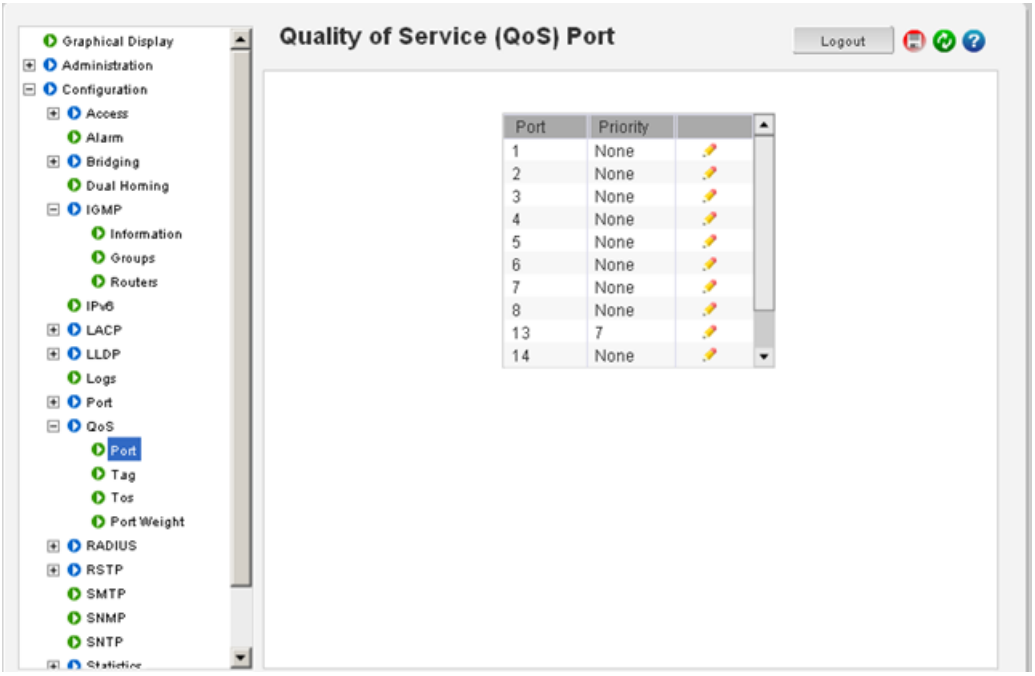
▷ Select the **Configuration > QoS** menu items.



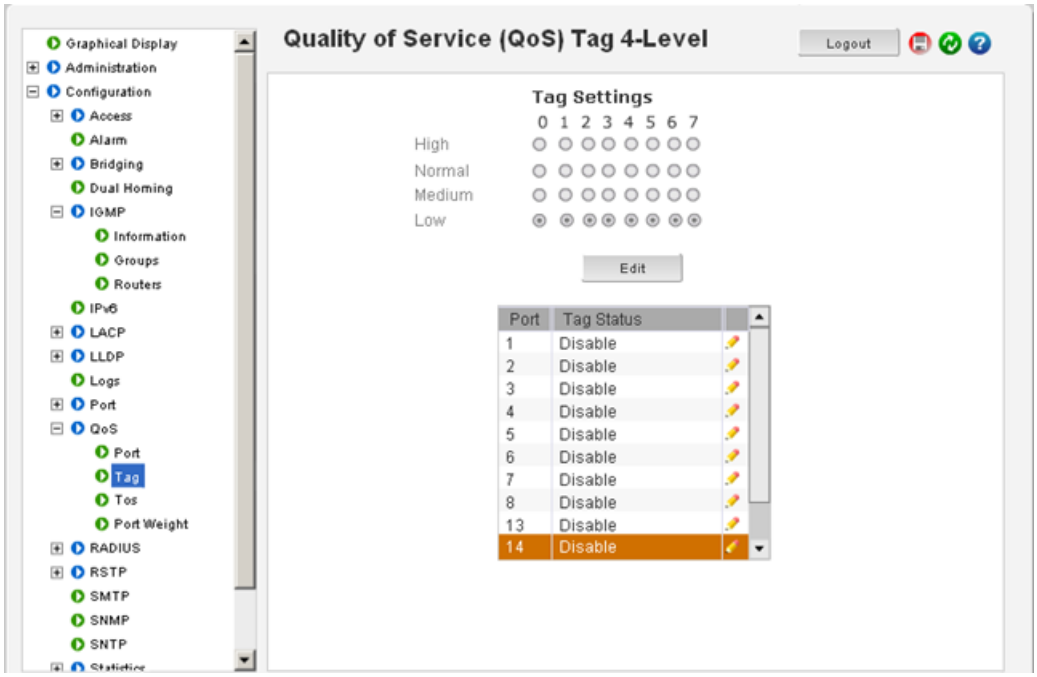
▷ Select the **Port** and the port number then edit to set up the Priority. The following window illustrates the setting of port 13 for port-based QoS with a priority. Note the sections on Tag and TOS are ignored for Port settings.



After the port QoS settings are completed, the changes are reflected on the QoS menu screen. The port 13 QoS settings indicate high priority set.

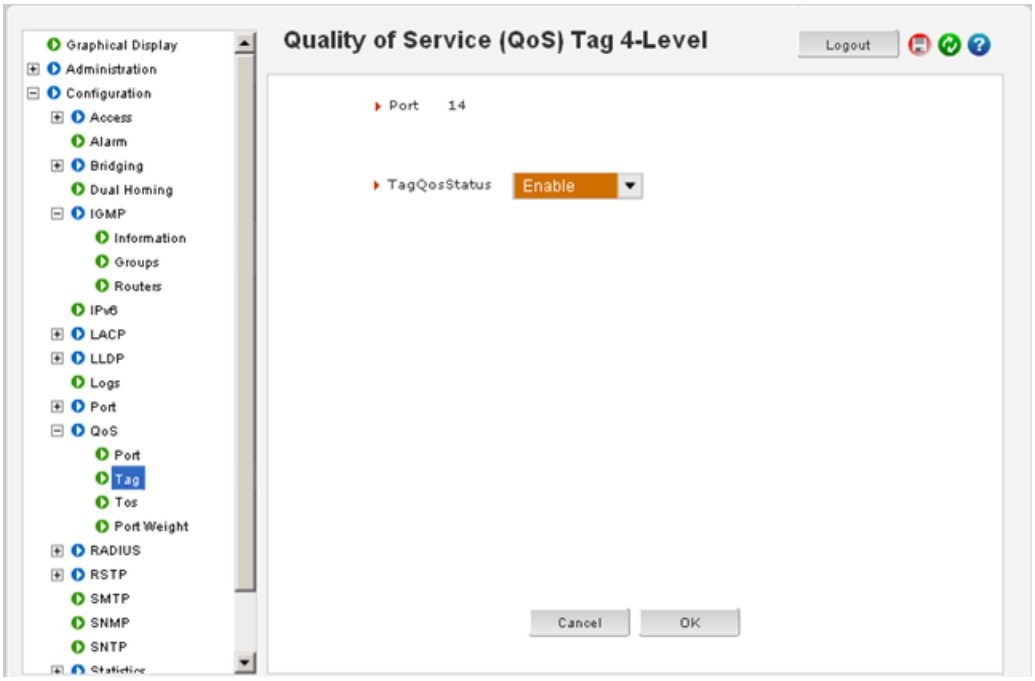


Next, to enable a tag-based QoS on port 14, select edit port 14 then enable tag QoS status. Note that only the menu area for the tag setting is relevant.

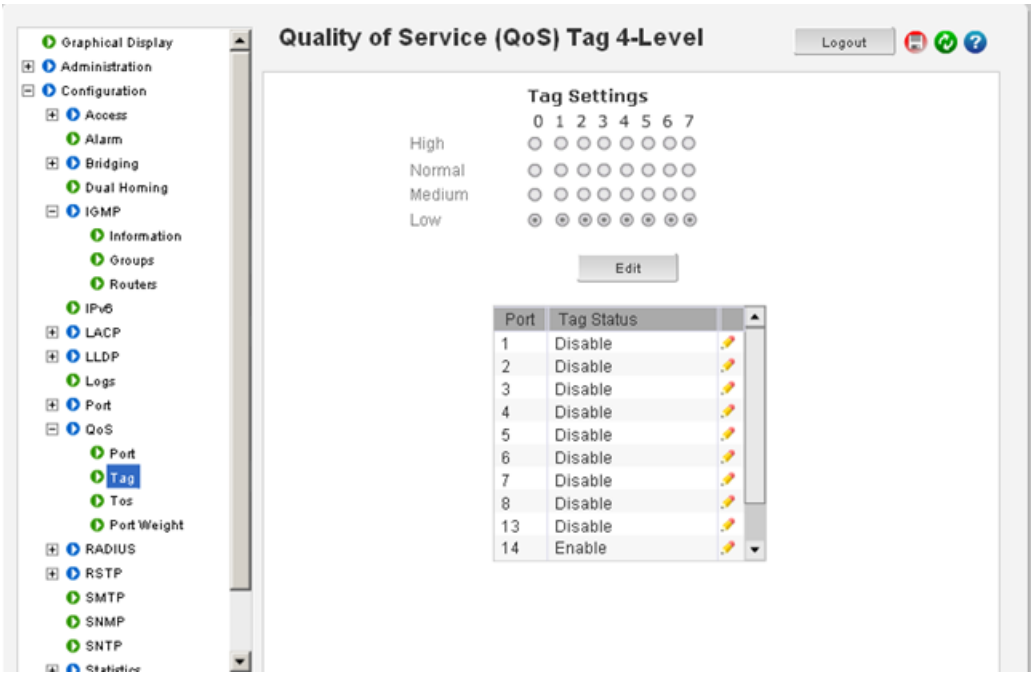


To set the tag-level settings, select Edit in the Tag settings screen.

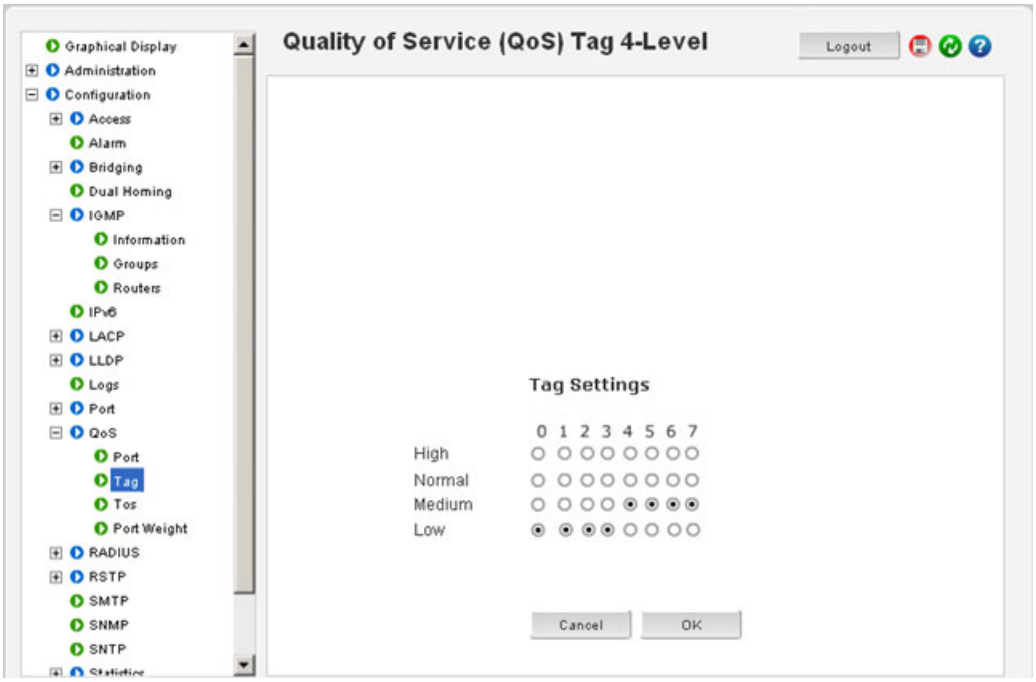
After the Tag QoS settings are completed, the changes are reflected on the QoS tag menu screen.



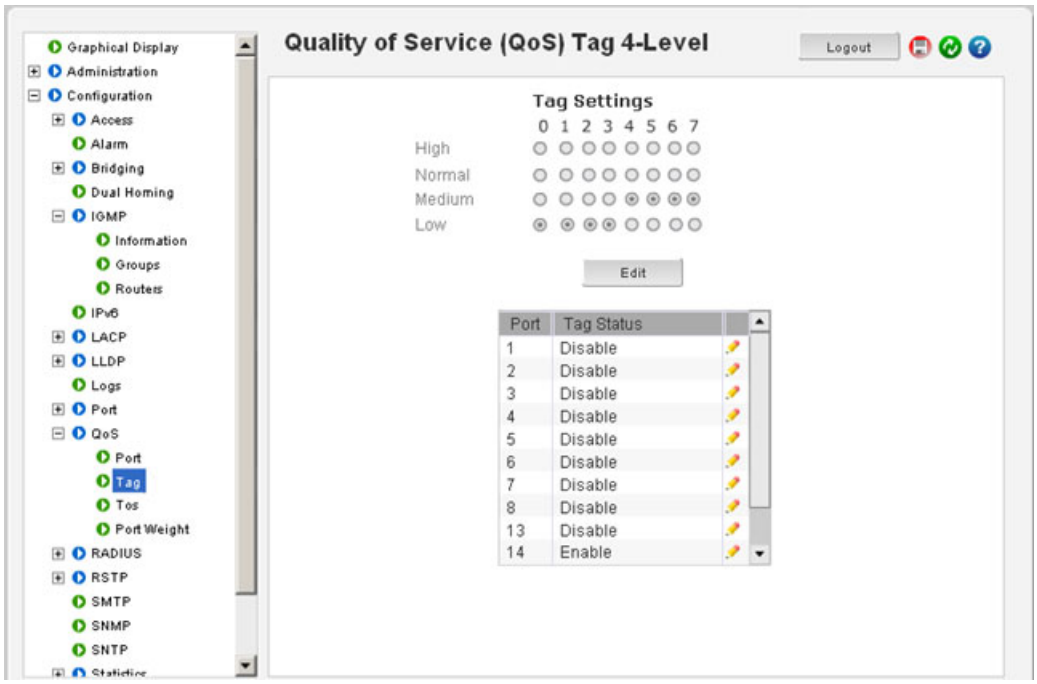
In the following window, a ToS is enabled on Port 8. As before, only the ToS level settings are relevant.

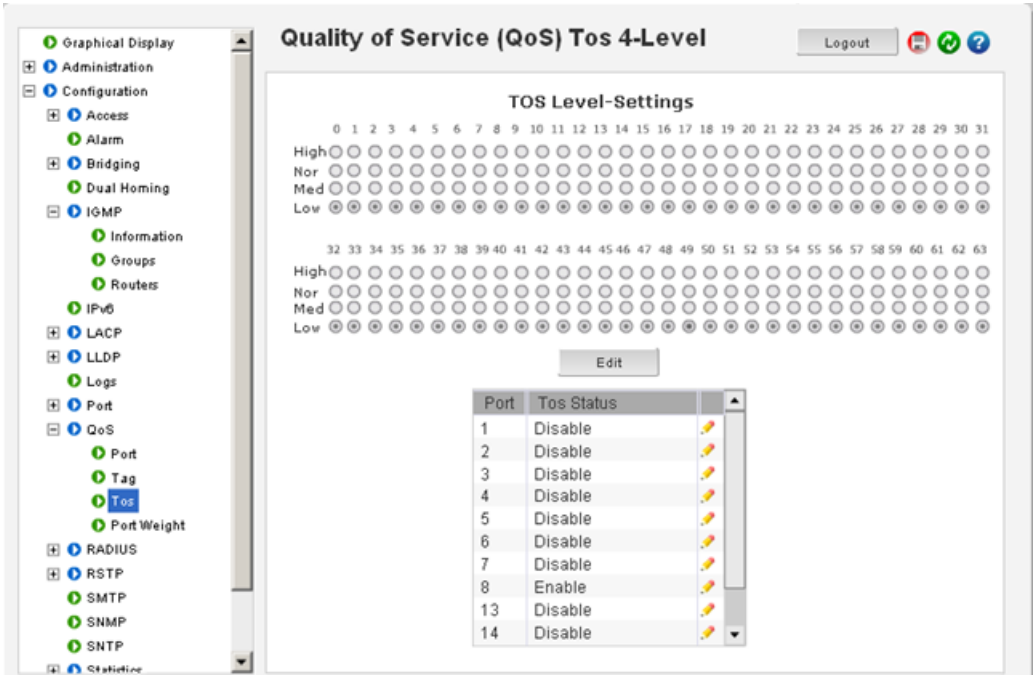


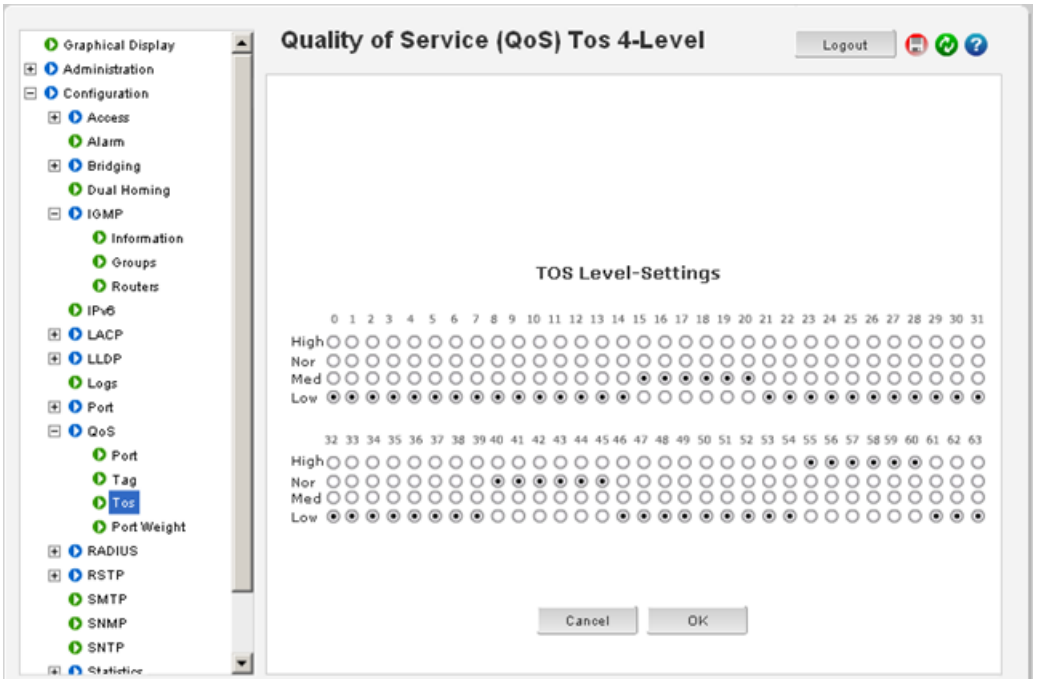
Select the edit, to set ToS level settings in the ToS level setting screen..

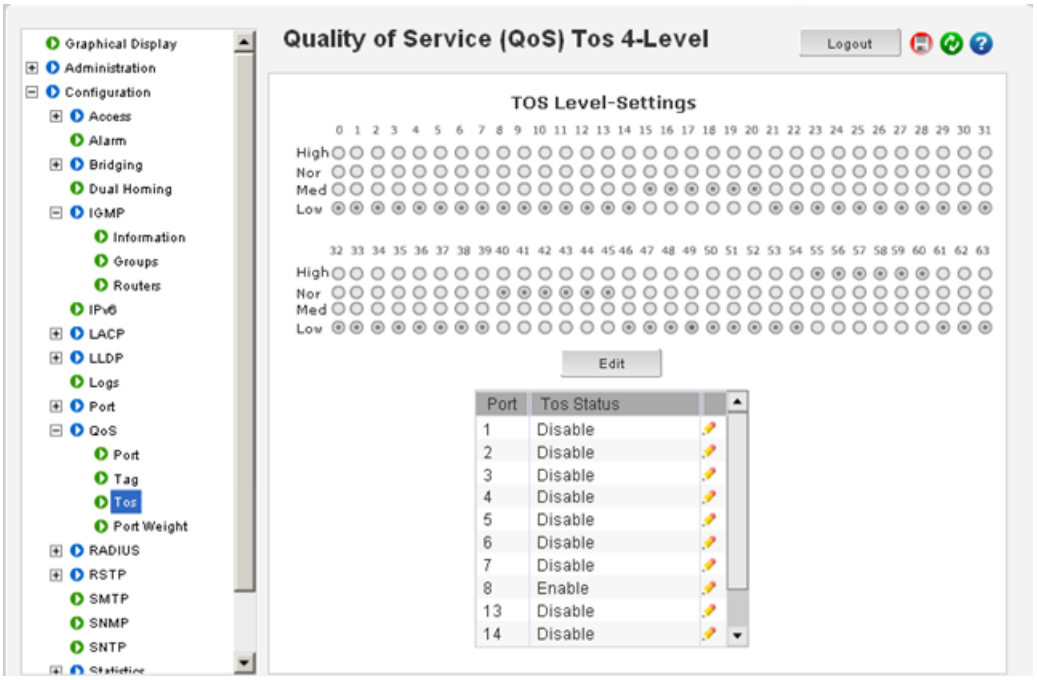


▷ After all changes are made, save the changes using the save icon ( ).


Graphical Display
Administration
Configuration
Access
Alarm
Bridging
Dual Homing
IGMP
Information
Groups
Routers
IPv6
LACP
LLDP
Logs
Port
QoS
Port
Tag
Tos
Port Weight
RADIUS
RSTP
SMTP
SNMP
SNTP
Quality of Service (QoS) Tag 4-Level
Logout
Tag Settings
0 1 2 3 4 5 6 7
High
Normal
Medium
Low
Edit
Port
Tag Status
1 Disable
2 Disable
3 Disable
4 Disable
5 Disable
6 Disable
7 Disable
8 Disable
13 Disable
14 Enable


Graphical Display
Administration
Configuration
Access
Alarm
Bridging
Dual Homing
IGMP
Information
Groups
Routers
IPv6
LACP
LLDP
Logs
Port
QoS
Port
Tag
Tos
Port Weight
RADIUS
RSTP
SMTP
SNMP
SNTP
Quality of Service (QoS) Tos 4-Level
Logout
TOS Level-Settings
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
High
Nor
Med
Low
32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
High
Nor
Med
Low
Edit
Port
Tos Status
1 Disable
2 Disable
3 Disable
4 Disable
5 Disable
6 Disable
7 Disable
8 Enable
13 Disable
14 Disable


Graphical Display
Administration
Configuration
Access
Alarm
Bridging
Dual Homing
IGMP
Information
Groups
Routers
IPv6
LACP
LLDP
Logs
Port
QoS
Port
Tag
Tos
Port Weight
RADIUS
RSTP
SMTP
SNMP
SNTP
Quality of Service (QoS) Tos 4-Level
Logout
TOS Level-Settings
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
High
Nor
Med
Low
32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
High
Nor
Med
Low
Cancel
OK


Graphical Display
Administration
Configuration
Access
Alarm
Bridging
Dual Homing
IGMP
Information
Groups
Routers
IPv6
LACP
LLDP
Logs
Port
QoS
Port
Tag
Tos
Port Weight
RADIUS
RSTP
SMTP
SNMP
SNTP
Quality of Service (QoS) Tos 4-Level
Logout
TOS Level-Settings
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
High
Nor
Med
Low
32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
High
Nor
Med
Low
Edit
Port
Tos Status
1 Disable
2 Disable
3 Disable
4 Disable
5 Disable
6 Disable
7 Disable
8 Enable
13 Disable
14 Disable

Multilink ML3000/ML3100

Chapter 15: IGMP

15.1 Overview

15.1.1 Description

Internet Group Management Protocol (IGMP) is defined in RFC 1112 as the standard for IP multicasting in the Internet. It is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allows a host to inform its local router, using Host Membership Reports that it wants to receive messages addressed to a specific multicast group. All hosts conforming to level 2 of the IP multicasting specification require IGMP.

15.1.2 IGMP Concepts

The ML3000 supports IGMP L2 standards as defined by RFC 1112. IGMP is disabled by default and needs to be enabled on the MultiLink family of switches. IP multicasting is defined as the transmission of an IP datagram to a “host group”, a set of zero or more hosts identified by a single IP destination address. A multicast datagram is delivered to all members of its destination host group with the same “best-efforts” reliability as regular unicast IP datagrams, i.e. the datagram is not guaranteed to arrive at all members of the destination group or in the same order relative to other datagrams.

The membership of a host group is dynamic; that is, hosts may join and leave groups at any time. There is no restriction on the location or number of members in a host group, but membership may be restricted to only those hosts possessing a private access key. A host may be a member of more than one group at a time. A host need not be a member of a group to send datagrams to it.

A host group may be permanent or transient. A permanent group has a well-known, administratively assigned IP address. It is the address and not the membership that is permanent – at any time, a permanent group may have any number of members, even zero. On the other hand, a transient group is dynamically assigned an address when the group is created, at the request of a host. A transient group ceases to exist, and its address becomes eligible for reassignment, when its membership drops to zero.

The creation of transient groups and the maintenance of group membership is the responsibility of "multicast agents", entities that reside in internet gateways or other special-purpose hosts. There is at least one multicast agent directly attached to every IP network or sub-network that supports IP multicasting. A host requests the creation of new groups, and joins or leaves existing groups by exchanging messages with a neighboring agent.

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, multicast routers, and hosts that support IGMP (in the MultiLink implementation of IGMP, a multicast router is not necessary as long as a switch is configured to support IGMP with the querier feature enabled). A set of hosts, routers, and/or switches that send or receive multicast data streams to or from the same source(s) is termed a multicast group, and all devices in the group use the same multicast group address. The multicast group running version 2 of IGMP uses three fundamental types of messages to communicate:

- **Query**: A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, then the switch must assume this function in order to elicit group membership information from the hosts on the network (if you need to disable the querier feature, you can do so using the IGMP configuration MIB).
- **Report**: A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
- **Leave Group**: A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group. Thus, IGMP identifies members of a multicast group (within a subnet) and allows IGMP-configured hosts (and routers) to join or leave multicast groups.

When IGMP is enabled on the MultiLink family of switches, it examines the IGMP packets it receives to:

- Learn which ports are linked to IGMP hosts and multicast routers/queriers belonging to any multicast group.
- Become a querier if a multicast router/querier is not discovered on the network.

Once the switch learns the port location of the hosts belonging to any particular multicast group, it can direct group traffic to only those ports, resulting in bandwidth savings on ports where group members do not reside. The following example illustrates this operation.

The figure below shows a network running IGMP.

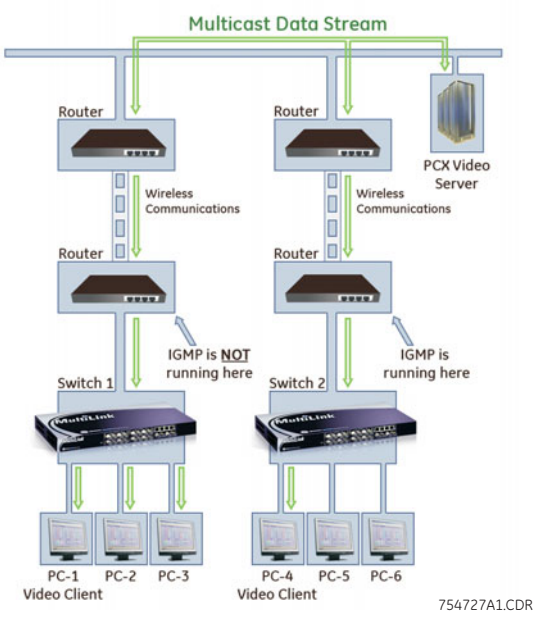


FIGURE 15–1: Advantages of using IGMP

In the above diagram:

- PCs 1 and 4, switch 2, and all of the routers are members of an IP multicast group (the routers operate as queriers).
- Switch 1 ignores IGMP traffic and does not distinguish between IP multicast group members and non-members. Thus, sends large amounts of unwanted multicast traffic to PCs 2 and 3.
- Switch 2 is recognizing IGMP traffic and learns that PC 4 is in the IP multicast group receiving multicast data from the video server (PC X). Switch 2 then sends the multicast data only to PC 4, thus avoiding unwanted multicast traffic on the ports for PCs 5 and 6.

The next figure (below) shows a network running IP multicasting using IGMP without a multicast router. In this case, the IGMP-configured switch runs as a querier. PCs 2, 5, and 6 are members of the same IP multicast group. IGMP is configured on switches 3 and 4.

Either of these switches can operate as querier because a multicast router is not present on the network. (If an IGMP switch does not detect a querier, it automatically assumes this role, assuming the querier feature is enabled-the default-within IGMP.)

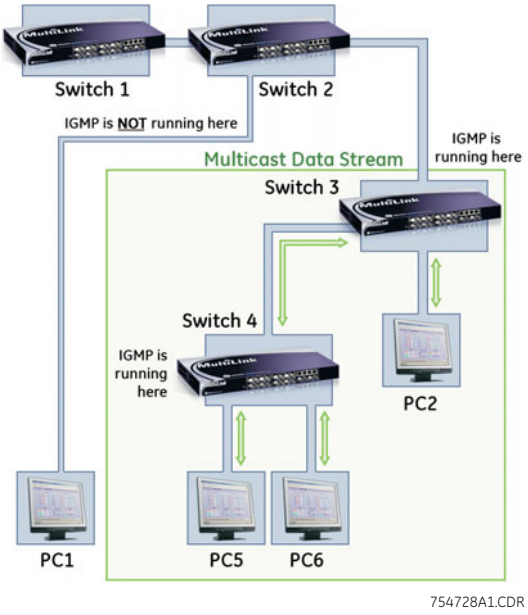


FIGURE 15–2: Isolating multicast traffic in a network

In the above figure, the multicast group traffic does not go to switch 1 and beyond. This is because either the port on switch 3 that connects to switch 1 has been configured as blocked or there are no hosts connected to switch 1 or switch 2 that belong to the multicast group.

For PC 1 to become a member of the same multicast group without flooding IP multicast traffic on all ports of switches 1 and 2, IGMP must be configured on both switches 1 and 2, and the port on switch 3 that connects to switch 1 must be unblocked.

15.1.3 IP Multicast Filters

IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multicast address range of 01005e-000000 through 01005e-7fffff in hexadecimal.) Devices such as the MultiLink family of switches having static Traffic/Security filters configured with a "Multicast" filter type and a "Multicast Address" in this range will continue in effect unless IGMP learns of a multicast group destination in this range. In that case, IGMP takes over the filtering function for the multicast destination address(es) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the static filter resumes control over traffic to the multicast address formerly controlled by IGMP.

15.1.4 Reserved Addresses Excluded from IP Multicast (IGMP) Filtering

Traffic to IP multicast groups in address range 224.0.0.0 to 224.0.0.255 will always be flooded because addresses in this range are "well known" or "reserved". Thus, if IP Multicast is enabled and there is an IP multicast group within the reserved address range, traffic to that group will be flooded instead of filtered by the switch.

15.1.5 IGMP Support

The MultiLink family of switches support IGMP version 1 and version 2. The switch can act either as a querier or a nonquerier. The querier router periodically sends general query messages to solicit group membership information. Hosts on the network that are members of a multicast group send report messages. When a host leaves a group, it sends a leave group message. The difference between Version 1 and Version 2 is that version 1 does not have a “Leave” mechanism for the host. The MultiLink family of switches do pruning when there is a leave message or a time expires on a port, we prune the multicast group membership on that port.

1. The MultiLink switch supports only the default VLAN. It can be enabled within a port VLAN, tagged VLAN, or no VLAN. It can snoop up to 256 multi-cast Groups.
2. IGMP is disabled as a default. It has to be enabled to leverage the benefits of IGMP.
3. The MultiLink switch supports only the default VLAN. It can be enabled within a port VLAN, tagged VLAN, or no VLAN. It can snoop up to 256 multi-cast Groups.
4. IGMP works only on default VLAN (DEFAULT_VLAN or VID = 1).

15.2 Configuring IGMP through the Command Line Interface

15.2.1 Commands

The `igmp` command enters IGMP configuration mode and enables or disables IGMP on the switch.

igmp

igmp *<enable/disable>*

The `show igmp` command displays the IGMP status.

show igmp

The following command sequence illustrates how to enable and query the status of IGMP.

```
ML3000# igmp

ML3000(igmp)## igmp enable

 IGMP is enabled

ML3000(igmp)## show igmp

 IGMP State              : Enabled
 ImmediateLeave          : Disabled
 Querier                 : Enabled
 Querier Interval        : 125
 Querier Response Interval   : 10
 Multicasting Unknown Streams  : Enable

ML3000(igmp)## igmp disable

 IGMP is disabled

ML3000(igmp)## show igmp

 IGMP State              : Disabled
 ImmediateLeave          : Disabled
 Querier                 : Enabled
 Querier Interval        : 125
 Querier Response Interval   : 10
 Multicasting Unknown Streams  : Enable

ML3000(igmp)##
```

The output of the `show igmp` command provides the following useful information:

- **IGMP State** shows if IGMP is turned on (Enable) or off (Disable).
- **Immediate Leave** provides a mechanism for a particular host that wants to leave a multicast group. It disables the port (where the leave message is received) ability to transmit multicast traffic.
- **Querier** shows where the switch is a querier or a non-querier. In our example, the switch is the querier.
- **Querier Interval** shows the time period in seconds on which the switch sends general host-query messages.
- **Querier Response Interval** specifies maximum amount of time in seconds that can elapse between when the querier sends a host-query message and when it receives a response from a host.
- **Multicasting Unknown Streams** shows if the control of multicast streams is on (Enabled) or off (Disabled).

The show-group command displays the multicast groups.

show-group

The following command sequence illustrates how to display IGMP groups:

```
ML3000(igmp)## show-group

 GroupIp     PortNo  Timer  LeavePending
 ----------------------------------------
 224.1.0.1   9      155   0
 224.0.1.40  9       155   0

ML3000(igmp)##
```

The output of the show-group command displays the following information:

- **Group IP** column shows the multicast groups.
- **Port No** shows the port where the multicast group is being detected.
- **Timer** shows the amount of time left in seconds before the group port will be deleted (or will not be able to route multicast traffic) if the switch does not receive a membership report.
- **Leave Pending** column shows the number of leave messages received from this port

Every port can be individually set to three different IGMP modes - auto, block and forward.

- **Auto** - lets IGMP control whether the port should or should not participate sending multicast traffic
- **Block** - manually configures the port to always block multicast traffic
- **Forward** - manually configures the port to always forward multicast traffic

To set the port characteristics, use the set-port command in the IGMP configuration mode.

set-port *port=< port|list|range> mode=<auto|forward|block>*

The show-port command displays the port characteristics for IGMP.

show-port

The show-router command displays detected IGMP-enabled router ports.

show-router

The set-leave command enables or disables the switch to immediately process a host sending a leave message rather that wait for the timer to expire.

set-leave *<enable|disable>*

The set-querier command enables or disables a switch as IGMP querier.

set-querier *<enable|disable>*

The set-qi command sets the IGMP querier router to periodically send general host-query messages. These messages are sent to ask for group membership information. This is sent to the all-system multicast group address, 224.0.0.1. The valid range can be from 60 to 127 seconds, with a default of 125.

set-qi *interval=<value>*

The set-qri command sets the query response interval representing the maximum amount of time that can elapse between when the querier router sends a host-query message and when it receives a response from a host. The range can be from 2 to 270 seconds, with a default of 10. Restrictions apply to the maximum value because of an internal calculation that is dependent on the value of the query interval.

set-qri *interval=<value>*

15.2.2 Example

The following example shows how to configure IGMP.

Example 15-1: Configuring IGMP

```
ML3000(igmp)## set-port port=10-12 mode=forward
 Port mode is set.
ML3000(igmp)## show-port
 ---------------------
 Port | Mode
 ---------------------
 09   | Auto
 10   | Forwarding
 11   | Forwarding
 12   | Forwarding
 13   | Auto
 14   | Auto
 15   | Auto
 16   | Auto
ML3000(igmp)## show-router
 RouterIp        PortNo   Timer
 ---------------------------------
 10.21.1.250        9    25
```

(continued on next page)

Configuring IGMP (continued)

```
ML3000(igmp)## set-leave enable

 IGMP immediate leave status is enabled

ML3000(igmp)## show igmp

 IGMP State              : Enabled
 ImmediateLeave          : Enabled
 Querier                 : Enabled
 Querier Interval        : 125
 Querier Response Interval   : 10
 Multicasting Unknown Streams : Enabled

ML3000(igmp)## set-leave disable

 IGMP immediate leave status is disabled

ML3000(igmp)## show igmp

 IGMP State              : Enabled
 ImmediateLeave          : Disabled
 Querier                 : Enabled
 Querier Interval        : 125
 Querier Response Interval   : 10
 Multicasting Unknown Streams : Enabled

ML3000(igmp)## set-querier enable

 IGMP querier status is enabled

ML3000(igmp)## show igmp

 IGMP State              : Enabled
 ImmediateLeave          : Disabled
 Querier                 : Enabled
 Querier Interval        : 125
 Querier Response Interval   : 10
 Multicasting Unknown Streams : Enabled

ML3000(igmp)## set-querier disable

 IGMP querier status is disabled

ML3000(igmp)## show igmp

 IGMP State              : Enabled
 ImmediateLeave          : Disabled
 Querier                 : Disabled
 Querier Interval        : 125
 Querier Response Interval   : 10
 Multicasting Unknown Streams : Enabled

ML3000(igmp)## set-qi interval=127

 Query interval successfully set

ML3000(igmp)## show igmp

 IGMP State              : Enabled
 ImmediateLeave          : Disabled
 Querier                 : Disabled
 Querier Interval        : 127
 Querier Response Interval   : 10
 Multicasting Unknown Streams : Enabled

ML3000(igmp)## set-qri interval=11
```

Configuring IGMP (continued)

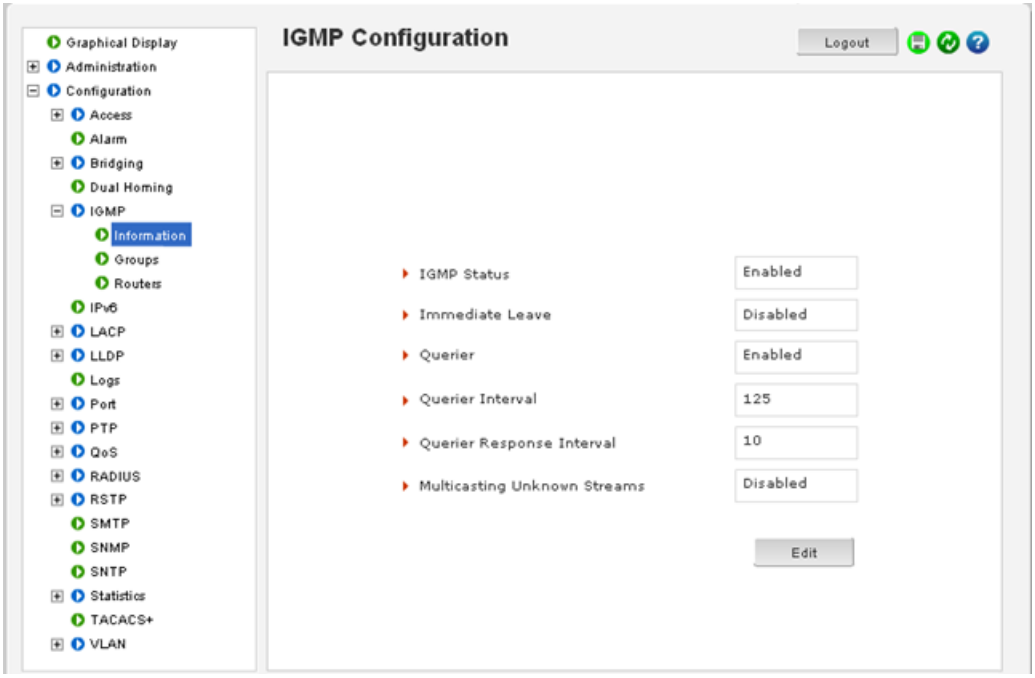
```
ML3000(igmp)## show igmp

 IGMP State              : Enabled
 ImmediateLeave          : Disabled
 Querier                 : Disabled
 Querier Interval        : 127
 Querier Response Interval   : 11
 Multicasting Unknown Streams  : Enabled

ML3000(igmp)## mcast disable

 MCAST is disabled

ML3000(igmp)## show igmp

 IGMP State              : Enabled
 ImmediateLeave          : Disabled
 Querier                 : Disabled
 Querier Interval        : 127
 Querier Response Interval   : 11
 Multicasting Unknown Streams  : Disabled

ML3000(igmp)## mcast enable

 MCAST is enabled

ML3000(igmp)## show igmp

 IGMP State              : Enabled
 ImmediateLeave          : Disabled
 Querier                 : Disabled
 Querier Interval        : 127
```

15.3 Configuring IGMP with EnerVista Secure Web Management software

15.3.1 Example

For configuring IGMP,

▷ Select the **Configuration > IGMP** menu item.
The menu allows the IGMP parameters to be set and provides information on IGMP groups and routers.



The menu allows the IGMP parameters described earlier to be set. It also provides the necessary information of IGMP groups and routers.

▷ Click on the **Edit** button to edit the IGMP parameters. This screen also enables and disables IGMP.

Changes are reflected on the **Configuration > IGMP > Information** screen. The groups and routers screen displays the IGMP Groups and IGMP Routers information. All edits to IGMP are done through the **Information** screen.

Multilink ML3000/ML3100

Chapter 16: SNMP

16.1 Overview

16.1.1 Description

SImple Network Management Protocol (SNMP) enables management of the network. There are many software packages which provide a graphical interface and a graphical view of the network and its devices. These graphical interface and view would not be possible without SNMP. SNMP is thus the building block for network management.

16.1.2 SNMP Concepts

SNMP provides the protocol to extract the necessary information from a networked device and display the information. The information is defined and stored in a Management Information Base (MIB). MIB is the "database" of the network management information.

SNMP has evolved over the years (since 1988) using the RFC process. Several RFCs define the SNMP standards. The most common standards for SNMP are SNMP v1 (the original version of SNMP); SNMP v2 and finally SNMP v3.

SNMP is a poll based mechanism. SNMP manager polls the managed device for information and display the information retrieved in text or graphical manner. Some definitions related to SNMP are

- **Authentication** - The process of ensuring message integrity and protection against message replays. It includes both data integrity and data origin authentication
- **Authoritative SNMP engine** - One of the SNMP copies involved in network communication designated to be the allowed SNMP engine which protects against message replay, delay, and redirection. The security keys used for authenticating and encrypting SNMPv3 packets are generated as a function of the authoritative SNMP engine's engine ID and user passwords. When an SNMP message expects a response (for example, get exact, get next, set request), the receiver of these messages is authoritative. When an SNMP message does not expect a response, the sender is authoritative
- **Community string** - A text string used to authenticate messages between a management station and an SNMP v1/v2c engine

- **Data integrity** - A condition or state of data in which a message packet has not been altered or destroyed in an unauthorized manner
- **Data origin authentication** - The ability to verify the identity of a user on whose behalf the message is supposedly sent. This ability protects users against both message capture and replay by a different SNMP engine, and against packets received or sent to a particular user that use an incorrect password or security level
- **Encryption** - A method of hiding data from an unauthorized user by scrambling the contents of an SNMP packet
- **Group** - A set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define what SNMP objects can be read, written to, or created. In addition, the group defines what notifications a user is allowed to receive
- **Notification host** - An SNMP entity to which notifications (traps and informs) are to be sent
- **Notify view** - A view name (not to exceed 64 characters) for each group that defines the list of notifications that can be sent to each user in the group
- **Privacy** - An encrypted state of the contents of an SNMP packet where they are prevented from being disclosed on a network. Encryption is performed with an algorithm called CBC-DES (DES-56)
- **Read view** - A view name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are accessible for reading by users belonging to the group
- **Security level** - A type of security algorithm performed on each SNMP packet. The three levels are: noauth, auth, and priv. noauth authenticates a packet by a string match of the user name. auth authenticates a packet by using either the HMAC MD5 algorithms. priv authenticates a packet by using either the HMAC MD5 algorithms and encrypts the packet using the CBC-DES (DES-56) algorithm.
- **Security model** - The security strategy used by the SNMP agent. Currently, ML3000 supports three security models: SNMPv1, SNMPv2c, and SNMPv3.
- **Simple Network Management Protocol (SNMP)** - A network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
- **Simple Network Management Protocol Version 2c (SNMPv2c)** - The second version of SNMP, it supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.
- **SNMP engine** - A copy of SNMP that can either reside on the local or remote device.
- **SNMP group** - A collection of SNMP users that belong to a common SNMP list that defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of these attributes defined by the group.
- **SNMP user** - A person for which an SNMP management operation is performed. The user is the person on a remote SNMP engine who receives the information.
- **SNMP view** - A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.
- **Write view** - A view name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.

16.1.3 Standards

There are several RFCs defining SNMP. The ML3000/ML3100 supports the following RFCs and standards.

SNMPv1 standards

- Security via configuration of SNMP communities
- Event reporting via SNMP
- Managing the switch with an SNMP network management tool Supported Standard MIBs include:
- SNMP MIB-II (RFC 1213)
- Bridge MIB (RFC 1493) (ifGeneralGroup, ifRcvAddressGroup, ifStackGroup)
- RMON MIB (RFC 1757)
- RMON: groups 1, 2, 3, and 9 (Statistics, Events, Alarms, and History)
- Version 1 traps (Warm Start, Cold Start, Link Up, Link Down, Authentication Failure, Rising Alarm, Falling Alarm)

RFC 1901-1908 – SNMPv2

RFC 2271-2275 – SNMPv3

- RFC 1901, Introduction to Community-Based SNMPv2. SNMPv2 Working Group
- RFC 1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group
- RFC 1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group
- RFC 1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group
- RFC 1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group
- RFC 1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2). SNMPv2 Working Group
- RFC 1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework. SNMPv2 Working Group
- RFC 2104, Keyed Hashing for Message Authentication
- RFC 2271, An Architecture for Describing SNMP Management Frameworks
- RFC 2272, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 2273, SNMPv3 Applications
- RFC 2274, User-Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 2275, View-Based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

16.2 Configuring SNMP through the Command Line Interface

16.2.1 Commands

There are several commands and variable which can be set for configuring SNMP. The basic SNMP v1 parameters can be set by referring to the section on System Parameters. Most commands here refer to SNMP v3 commands and how the variables for SNMP v3 can be configured.

The `snmp` command enters the SNMP configuration mode.

snmp

The `snmpv3` command enters the SNMP V3 configuration mode. It is still necessary to enable SNMP V3 by using the `set snmp` command after entering configuration mode.

snmpv3

The `set snmp` command defines the SNMP version. The ML3000 supports all versions (v1, v2 and v3) or only v1. By default, SNMP v1only is enabled.

set snmp *type=<v1|all>*

The `show snmp` command displays the SNMP configuration information.

show snmp

The `setvar` command sets the system name, contact and location. All parameters are optional but a user must supply at least one parameter.

setvar *[sysname|syscontact|syslocation]=<string>*

The `quickcfg` command automatically configures a default VACM (view-based access control model). This allows any manager station to access the ML3000 either via SNMP v1, v2c or v3. The community name is “public”. This command is only intended for first time users and values can be changed by administrators who want more strict access.

quickcfg

The `engineid` command allows the user to change the engine ID. Every agent has to have an `engineID` (name) to be able to respond to SNMPv3 messages.

engineid *string=<string>*

The `authtrap` command enables or disables authentication traps generation.

authtrap *<enable|disable>*

The `show-authtrap` command displays the current value of authentication trap status.

show-authtrap

The `deftrap` command defines the default community string to be used when sending traps. When user does not specify the trap community name when setting a trap station using the `trap` command, the default trap community name is used.

deftrap *community=<string>*

The `show-deftrap` command displays the current value of default trap.

show-deftrap

The `trap` command defines the trap and inform manager stations. The station can receive v1, v2 traps and/or inform notifications. An inform notification is an acknowledgments that a trap has been received. A user can add up to 5 stations.

trap *<add|delete> id=<id> [type=<v1|v2|inform>] [host=<host-ip>] [community=<string>] [port=<1-65534>]*

The show-trap command shows the configured trap stations in tabular format. The `id` argument is optional and is the number corresponding to the trap entry number in the table.

show-trap *[id=<id#>]*

The `com2sec` command specifies the mapping from a source/community pair to a security name. Up to 10 entries can be specified. This part of the View based Access Control Model (VACM) as defined in RFC 2275.

com2sec *<add|delete> id=<id> [secname=<name>] [source=<source>] [community=<community>]*

The `group` command defines the mapping from sec model or a sec name to a group. A sec model is one of v1, v2c, or usm. Up to 10 entries can be specified. This part of the View based Access Control Model (VACM) as defined in RFC 2275.

group *<add|delete> id=<id> [groupname=<name>] [model=<v1|v2c|usm>] [com2secid=<com2sec-id>]*

The `show-group` command displays all or specific group entries. The `id` argument is optional and is the number corresponding to the group entry number in the table

show-group *[id=<id>]*

The `view` command defines a manager or group or manager stations what it can access inside the MIB object tree. Up to 10 entries can be specified. This part of the View based Access Control Model (VACM) as defined in RFC 2275

view *<add|delete> id=<id> [viewname=<name>] [type=<included|excluded>] [subtree=<oid>] [mask=<hex-string>]*

The `show-view` command display all or specific view entries. The `id` argument is optional and is the number corresponding to the view entry number in the table.

show-view *[id=<id>]*

The `user` command adds user entries. The ML3000 allows up to 5 users to be added. Currently, the ML3000 agent only support `noauth` and `auth-md5` for v3 authentication and `auth-des` for `priv` authentication.

user *<add|delete> id=<id> [username=<name>] [usertype=<readonly|readwrite>] [authpass=<pass-phrase>]*
[privpass=<pass-phrase>] [level=<noauth|auth|priv>] [subtree=<oid>]

The `show-user` command displays all or specific view entries. The `id` is optional and is the number corresponding to the view entry number in the table.

show-user *[id=<id>]*

16.2.2 Example

The following example shows how to configure SNMP.

Example 16-1: Configuring SNMP

```
ML3000# set snmp type=v1
 SNMP version support is set to "v1"
ML3000# show snmp
 SNMP CONFIGURATION INFORMATION
 ------------------------------
 SNMP Get Community Name  :  public
 SNMP Set Community Name  :  private
 SNMP Trap Community Name :  public
 AuthenTrapsEnableFlag    :  disabled
 SNMP Access Status       :  enabled
 SNMP MANAGERS INFO
 ------------------
 SNMP TRAP STATIONS INFO
 -----------------------
ML3000# set snmp type=all
 SNMP version support is set to "v1, v2c, v3"
ML3000# show snmp
 SNMP v3 Configuration Information
 ==============================
 System Name           : ML3000
 System Location       : Markham, ON
 System Contact        : multilin.tech@ge.com
 Authentication Trap   : Disabled
 Default Trap Comm.    : public
 V3 Engine ID          : ML_V3 Engine
ML3000# snmpv3
ML3000(snmpv3)## setvar sysname=ML3000 syscontact=admin syslocati
ML3000(snmpv3)# quickcfg
 This will enable default VACM.
 Do you wish to proceed? ['Y' or 'N' ] Y
 Quick configuration done, default VACM enabled
ML3000(snmpv3)## engineid string=Multi_3000
 Engine ID is set successfully
ML3000(snmpv3)## authtrap enable
 Authentication trap status is set successfully
ML3000(snmpv3)## show-authtrap
 Authentication Trap Status: Enabled
ML3000(snmpv3)## deftrap community=mysecret
 Default trap community is set successfully
ML3000(snmpv3)## show-deftrap
```

Configuring SNMP (continued)

```
ML3000(snmpv3)## trap add id=1 type=v1 host=3.94.200.107
 Entry is added successfully
ML3000(snmpv3)## show-trap
 ID  Trap Type  Host IP       Community  Port
 ================================================
 1  v1      3.94.200.107   --      --
 2  --      --         --     --
 3  --      --         --     --
 4  --      --         --     --
 5  --      --         --     --
ML3000(snmpv3)## show-trap id=1
 Trap ID   : 1
 Trap Type  : v1
 Host IP   : 3.94.200.107
 Community  : --
 Auth. Type : --
ML3000(snmpv3)## com2sec add id=1 secname=public source=default community=pu
 Entry is added successfully
ML3000(snmpv3)## com2sec add id=2
 ERROR: "secname" parameter is required for "add" directive
ML3000(snmpv3)## com2sec add id=2 secname=BCM
 Entry is added successfully
ML3000(snmpv3)## show-com2sec
 ID  Sec. Name     Source       Community
 ================================================
 1  public       default      public
 2  BCM          default      public
 3  --           --           --
 4  --           --           --
 5  --           --           --
 6  --           --           --
 7  --           --           --
 8  --           --           --
 9  --           --           --
 10  --           --           --
ML3000(snmpv3)## show-com2sec id=2
 Com2Sec ID   : 2
 Security Name : BCM
 Source      : default
 Community    : public
ML3000(snmpv3)## group add id=1 groupname=v1 model=v1 com2secid=1
 Entry is added successfully
```

(continued on next page)

Configuring SNMP (continued)

```
ML3000(snmpv3)## show-group
 ID  Group Name    Sec. Model    Com2Sec ID
 ==========================================
 1  v1         v1        1
 2  public       v2c        1
 3  public       usm        1
 4  --         --        --
 5  --         --        --
 6  --         --        --
 7  --         --        --
 8  --         --        --
 9  --         --        --
 10 --         --        --
ML3000(snmpv3)## show-group id=1
 Group ID   : 1
 Group Name : v1
 Model      : v1
 Com2Sec ID : 1
ML3000(snmpv3)## view add id=1 viewname=all type=included subtree=.1
 Entry is added successfully
ML3000(snmpv3)## show-view
 ID  View Name     Type        Subtree  Mask
 ============================================
 1  all         included    1     ff
 2  --          --        --     --
 3  --          --        --     --
 4  --          --        --     --
 5  --          --        --     --
 6  --          --        --     --
 7  --          --        --     --
 8  --          --        --     --
 9  --          --        --     --
 10 --          --        --     --
ML3000(snmpv3)## show-view id=1
 View ID   : 1
 View Name  : all
 Type      : included
 Subtree   : .1
 Mask      : ff
ML3000(snmpv3)## access add id=1 accessname=v1 model=v1 level=noauth read=1
write=none notify=none
 Entry is added successfully
```

(continued on next page)

Configuring SNMP (continued)

```
ML3000(snmpv3)## show-access
 ID View Name   Model   Level   R/View  W/View  N/View  Context     Prefix
 ================================================================================
 1  v1       v1     noauth  1     none    none    ""        exact
 2  --       --     --    --    --    --    --        --
 3  --       --     --    --    --    --    --        --
 4  --       --     --    --    --    --    --        --
 5  --       --     --    --    --    --    --        --
 6  --       --     --    --    --    --    --        --
 7  --       --     --    --    --    --    --        --
 8  --       --     --    --    --    --    --        --
 9  --       --     --    --    --    --    --        --
 10 --       --     --    --    --    --    --        --
ML3000(snmpv3)## show-access id=1
 Access ID     : 1
 Access Name   : v1
 Sec. Model    : v1
 Sec. Level    : noauth
 Read View ID  : 1
 Write View ID : none
 Notify View ID : none
 Context       : ""
 Prefix        : exact
ML3000(snmpv3)## user add id=1 username=jsmith usertype=readwrite authpass=something
 Entry is added successfully
ML3000(snmpv3)## show-user
 ID User Name    UType    AuthPass   PrivPass   AType   Level   Subtree
 ================================================================================
 1  jsmith       RW       something  --       MD5    auth    --
 2  --         --       --       --       --     --     --
 3  --         --       --       --       --     --     --
 4  --         --       --       --       --     --     --
 5  --         --       --       --       --     --     --
ML3000(snmpv3)## show-user id=2
 ERROR: Entry is not active
ML3000(snmpv3)## show-user id=1
 User ID    : 1
 User Name  : jsmith
 User Type  : read-write
 Auth. Pass : something
 Priv. Pass :
 Auth. Type : MD5
 Auth. Level : auth
 Subtree    :
ML3000(snmpv3)## exit
ML3000#
```

16.3 Configuring SNMP with EnerVista Secure Web Management software

16.3.1 Example

Most SNMP v1 capabilities can be set using the EnerVista Secure Web Management software. For SNMP v2 and v3 parameters, please refer to *Configuring SNMP through the Command Line Interface* on page 16–264.

SNMP variables are used in conjunction with Alert definitions. Alert Definitions are covered in the next chapter.

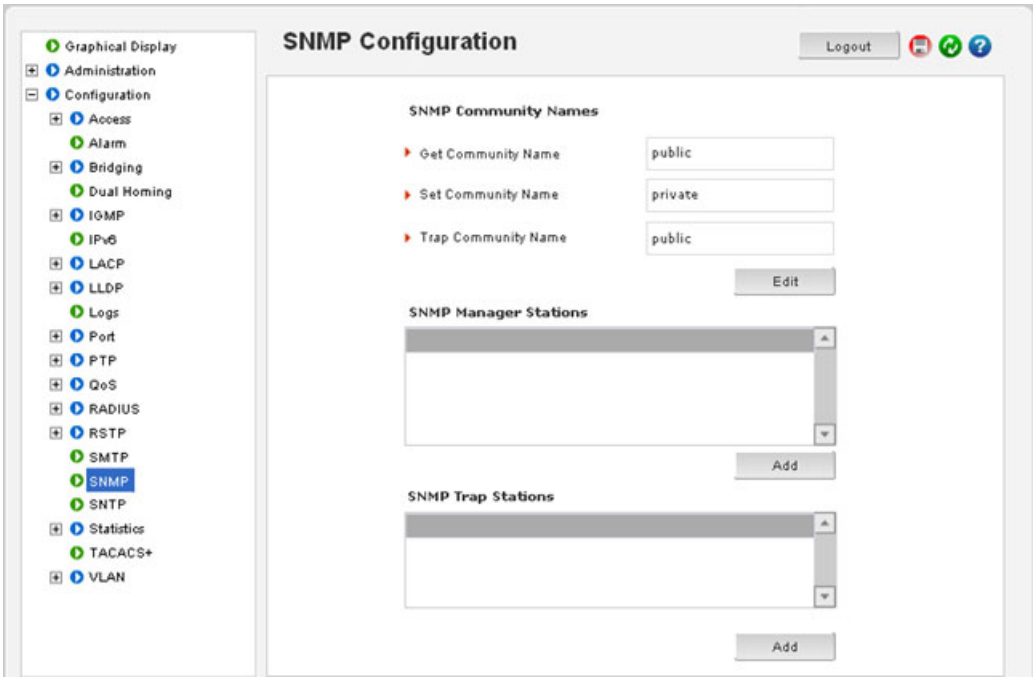
To configure SNMP,

▷ Select the **Configuration > SNMP** menu item.

▷ Use the **Edit** button to change the SNMP community parameters.

▷ Use the **Add** buttons to add the management and trap receivers.

The following window illustrates changes to the SNMP community parameters. It is recommended to change the community strings from the default values of public and private to other values.



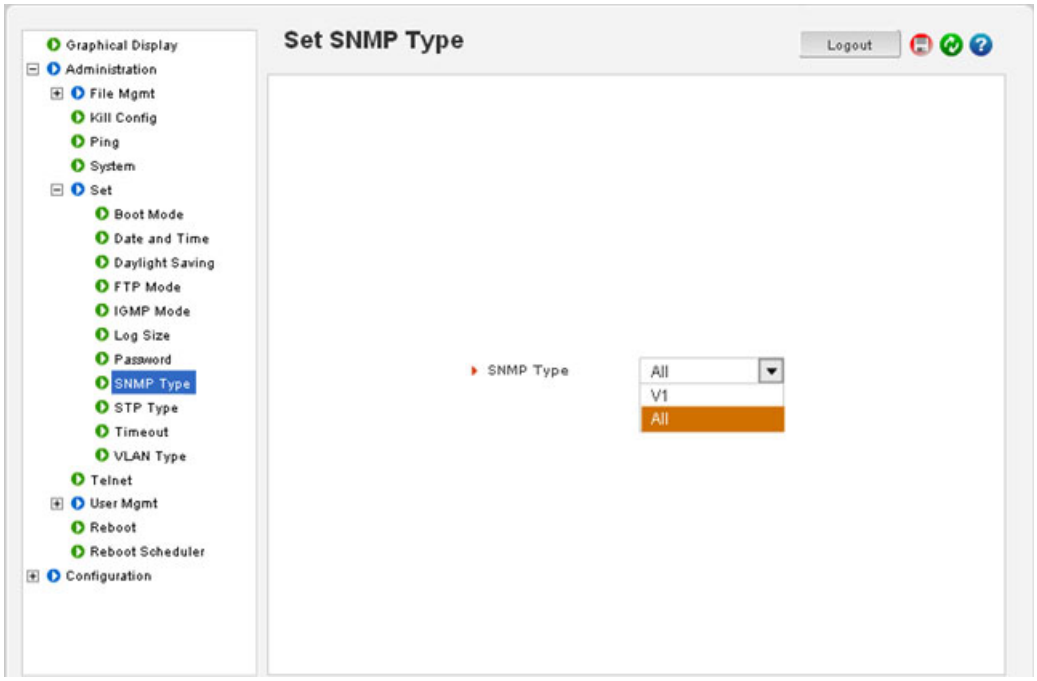
▷ When done changing the community strings, click **OK**.

Multiple managers can be added as shown below.

▷ When adding SNMP manager stations, click on the **Add** button on the SNMP menu screen.

▷ Make sure that each station can be pinged from the switch by using the **Configuration > Ping** menu.

▷ When done adding stations, click **OK**.

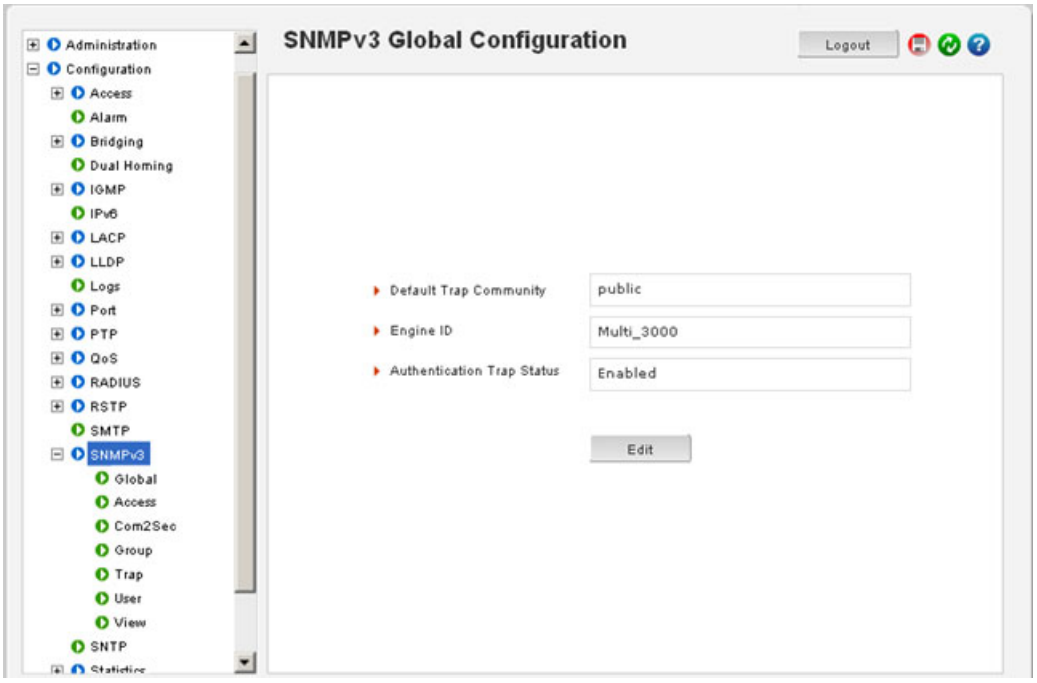


▷ When adding SNMP trap receivers, click on the Add button on the SNMP menu screen.

▷ Make sure that each station can be pinged from the switch by using the **Administration > Ping** menu.

▷ Determine which sorts of traps each station will receive, as shown above. If not sure, select all three types.

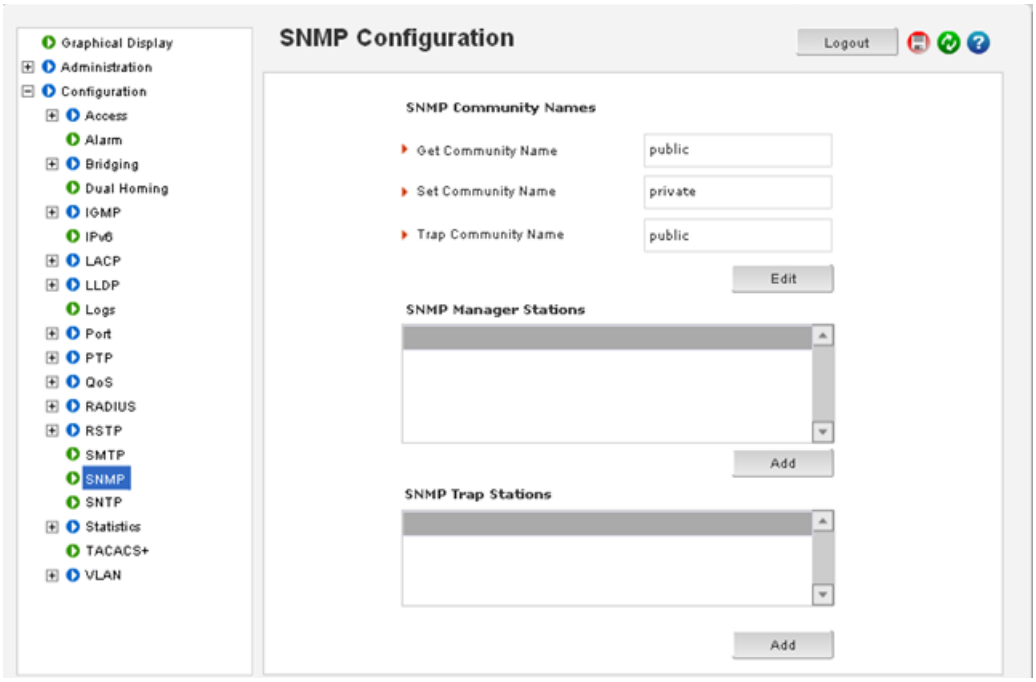
▷ When done adding trap receivers, click **OK**.

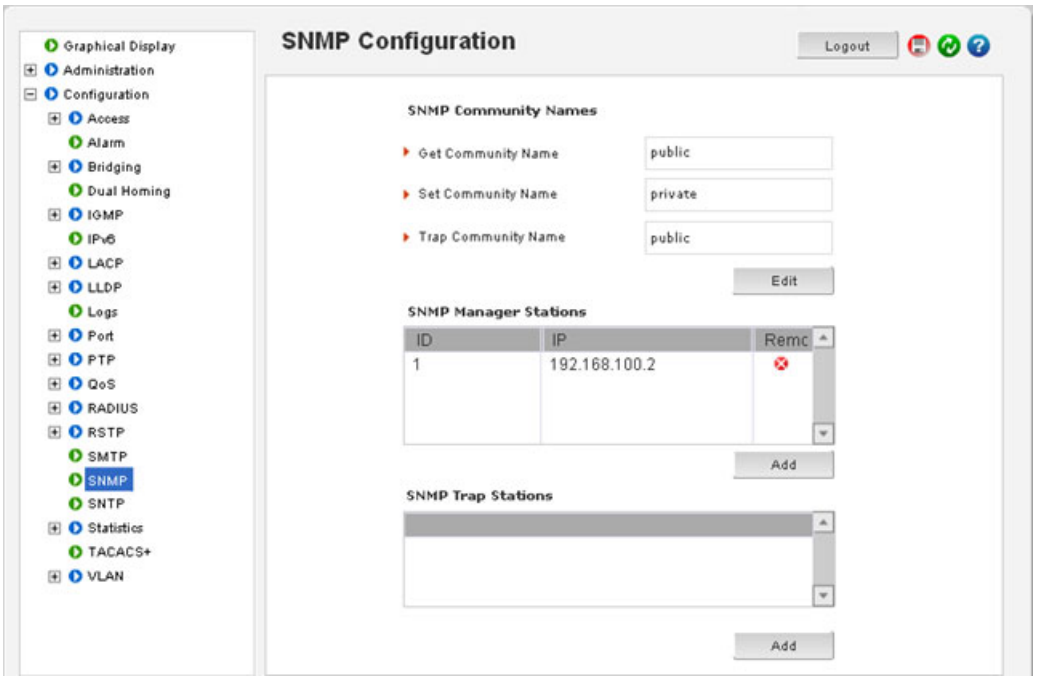


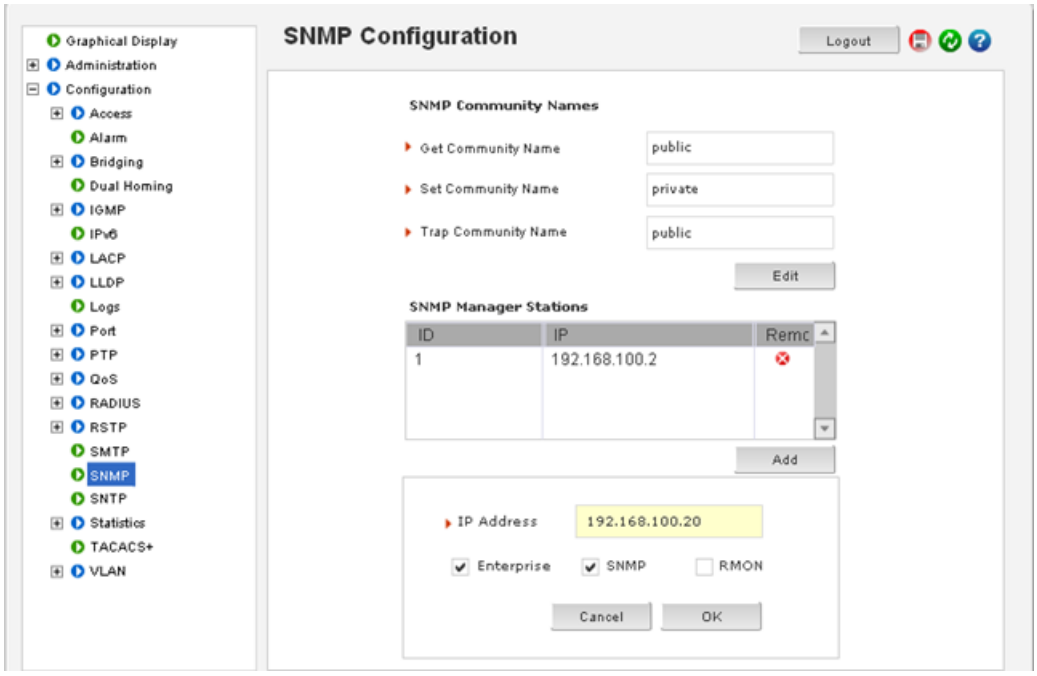
Note the different types of trap receivers added.

Stations can be deleted using the delete icon ( ). To change the stations characteristics or IP addresses, it is recommended to delete the station and add a new one.

▷ After all changes are made, save the changes using the save icon ( ).






Graphical Display
Administration
Configuration
Access
Alarm
Bridging
Dual Homing
IGMP
IPv6
LACP
LLDP
Logs
Port
PTP
QoS
RADIUS
RSTP
SMTP
SNMP
SNTP
Statistics
TACACS+
VLAN
SNMP Configuration
Logout
SNMP Community Names
Get Community Name
public
Set Community Name
private
Trap Community Name
public
Edit
SNMP Manager Stations
ID
IP
Remc
1
192.168.100.2
Add
IP Address
192.168.100.20
Enterprise
SNMP
RMON
Cancel
OK

16.4 Configuring RMON

16.4.1 Description

The switch supports RMON (Remote Monitoring) on all connected network segments. This allows for troubleshooting and optimizing your network. The MultiLink family of switches provides hardware-based RMON counters. The switch manager or a network management system can poll these counters periodically to collect the statistics in a format that compiles with the RMON MIB definition.

The following RMON groups are supported:

- **Ethernet statistics group** - maintains utilization and error statistics for the switch port being monitored.
- **History group** - gathers and stores periodic statistical samples from previous statistics group.
- **Alarm group** - allows a network administrator to define alarm thresholds for any MIB variable.
- **Log and event group** - allows a network administrator to define actions based on alarms. SNMP traps are generated when RMON alarms are triggered.

16.4.2 Commands

The following RMON communities, when defined, enable the specific RMON group as show above. The `rmon` command enter the RMON configuration mode to setup RMON groups and communities.

rmon

The `history` command defines the RMON history group and the community string associated with the group.

history *def-owner=<string> def-comm=<string>*

The `statistics` command defines the RMON statistics group and the community string associated with the group.

statistics *def-owner=<string>*

The `alarm` command defines the RMON alarm group and the community string associated with the group.

alarm *def-owner=<string> def-comm=<string>*

The `event` command defines the RMON event group and the community string associated with the group.

event *def-owner=<string> def-comm=<string>*

The `show rom` command lists the specific RMON data as defined by the group type.

show rmon *<stats|hist|event|alarm>*

The following command sequence illustrates how to configure RMON groups.

```
ML3000(rmon)## rmon
ML3000(rmon)## event def-owner=test def-comm=somestring
 RMON Event Default Owner is set
 RMON Event Default Community is set
ML3000(rmon)## show rmon event
 RMON Event Default Owner     : test
 RMON Event Default Community : somestring
ML3000(rmon)## exit
ML3000#
```

Multilink ML3000/ML3100

Chapter 17: LACP

17.1 Increase Network throughput and reliability

17.1.1 LACP Concepts

The IEEE802.3ad standard provides for the formation of a single Layer 2 link from two or more standard Ethernet links using the Link Aggregation Control Protocol (LACP). LACP provides a robust means of assuring that both ends of the link are up and agree to be members of the aggregation before the link member is activated. LACP trunking is a method of combining physical network links into a single logical link for increased bandwidth. With LACP the effective bandwidth of a trunk and network availability is increased. Two or more Fast Ethernet connections are combined as one logical trunk in order to increase the bandwidth and to create resilient and redundant links. By taking multiple LAN connections and treating them as a unified, aggregated link, Link Aggregation provides the following important benefits:

- Higher link availability – in case a link fails, the other links continue to operate
- Increased link capacity – the effective throughput is increased
- Better port utilization – allows unused ports to be used as trunk ports allowing better throughput and availability
- Interoperability – being a standard allows LACP to work across different hardware platforms where LACP is supported

Failure of any one physical link does not impact the logical link defined using LACP. The loss of a link within an aggregation reduces the available capacity, but the connection is maintained and the data flow is not interrupted.

The performance is improved because the capacity of an aggregated link is higher than each individual link alone. 10 Mbps or 10/100 Mbps or 100 Mbps ports can be grouped together to form one logical link.

Instead of adding new hardware to increase speed on a trunk – one can now use LACP to incrementally increase the throughput in the network, preventing or deferring hardware upgrades. Some known issues with LACP on the Multilink 3000 family of switches are:

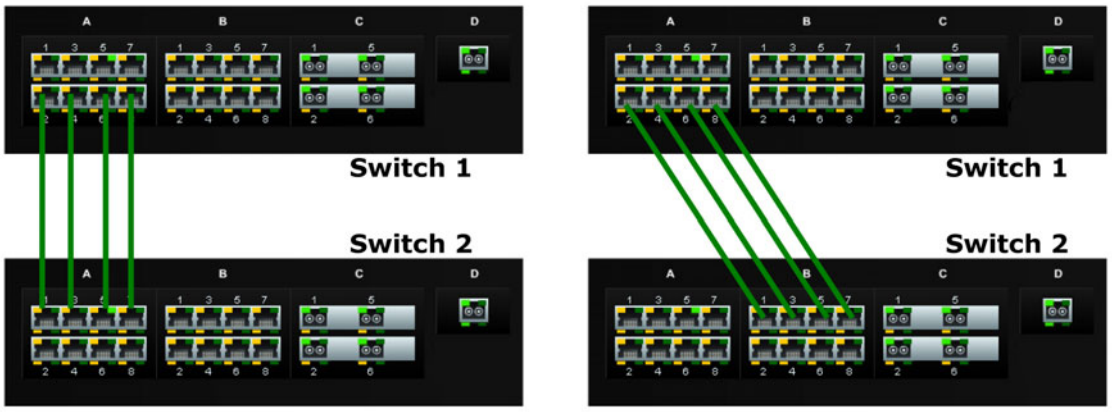
- LACP does not work on Half Duplex ports

- All trunk ports must be on the same module. Trunk ports cannot be spread out across different modules
- All trunk ports MUST have the same speed setting. If the speed is different, LACP shows an error indicating speed mismatch
- Many switches do not forward the LACPDUs by default. So, it is possible to hook up multiple ports to these switches and create an Ethernet loop. (In many cases this is prevented by Spanning Tree running on these switches)
- All ports in a trunk group should be members of the same VLAN. Each port can be a member of multiple VLANs, but each port should have at least one VLAN that is common to both the port groups
- The LACPDU packets are sent out every 30 seconds. It is possible that in configuring LACP, a loop can be created until LACP notification is completed. It is recommended to configure LACP first and then physically connect the ports to avoid this potential issue
- Port Security does not work with the ports configured for LACP
- IGMP works with the primary LACP port only. All IGMP traffic is sent via a primary port. If needed, this port can be mirrored for traffic analysis
- RSTP has to be enabled to ensure a quick recovery. If RSTP is not enabled, STP is used for link recovery and it will be slow

17.2 LACP Configuration

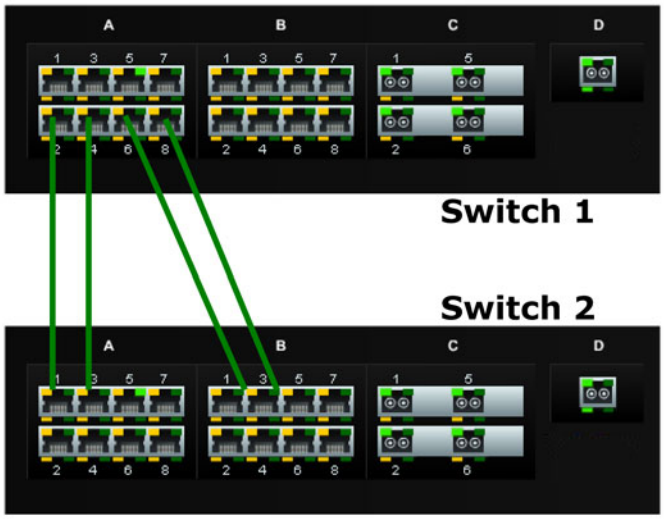
For LACP to work on the Multilink 3000 family of switches, only one trunk per module can be created. Some valid connections are shown in the picture below.

Figure 17-1: Valid LACP Configuarations



Should trunks be created so as to span multiple ports, a "trunk mismatch" error message is printed on the console. An example of an incorrect configuration is shown below.

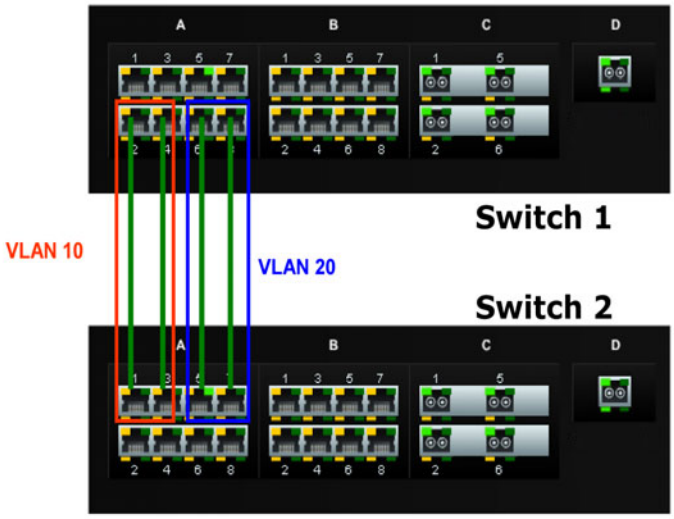
Figure 17-2: Incorrect LACP Connection.



All LACP trunk ports must be on the same module and cannot span different modules.

Another example is highlighted below where some ports belong to VLAN 10 (shown in red) and other ports belong to VLAN 20 (shown in blue). If the port groups do not have a common VLAN between them, LACP does not form a connection.

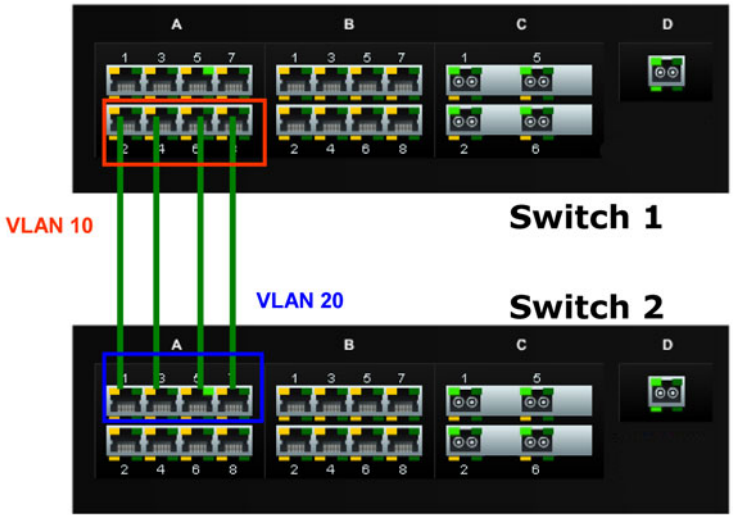
Figure 17-3: Another Incorrect LACP Connection



In this figure, even though the connections are from one module to another, this is still not a valid configuration (for LACP using 4 ports) as the trunk group belongs to two different VLANs.

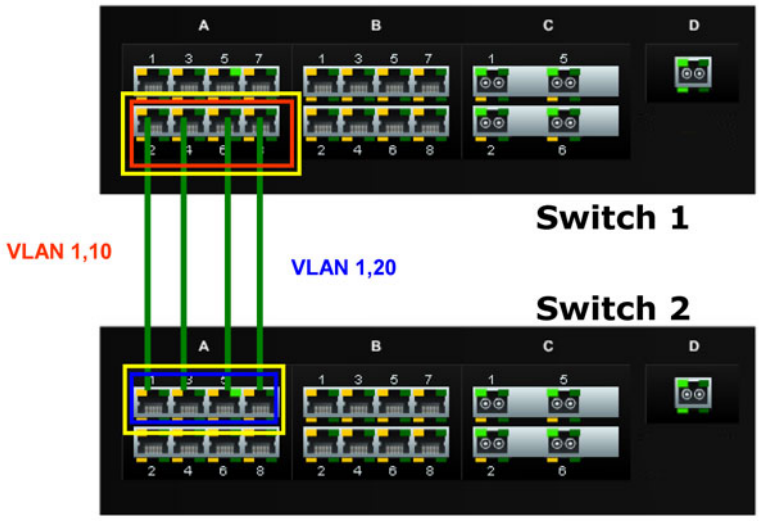
However – on each switch, the set of ports can belong to same VLANs as shown in the figure below. While the ports belong to the same VLANs, there is no common VLAN between the switches and hence the LACPDU cannot be transmitted. This configuration does not work in the LACP mode.

Figure 17-4: No Common VLAN Between 2 Ports



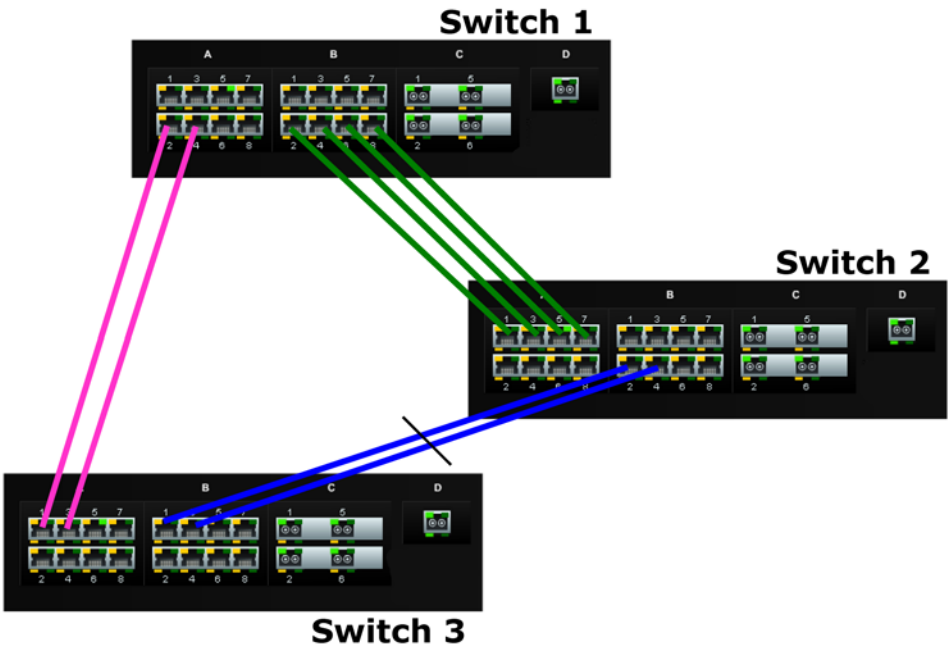
In the figure above, there is no common VLAN between the two sets of ports, so packets from one VLAN to another cannot be forwarded. There should be at least one VLAN common between the two switches and the LACP port groups.

Figure 17-5: Valid Common VLAN Configuration



This configuration is similar to the previous configuration, except there is a common VLAN (VLAN 1) between the two sets of LACP ports.

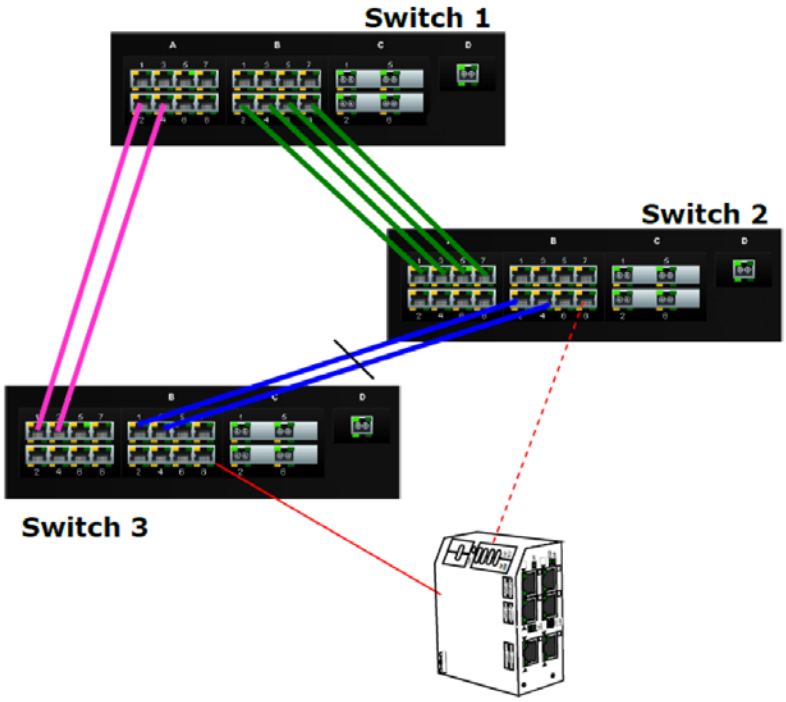
Figure 17-6: Redundant Link Architecture with RSTP and LACP



In the architecture above, using RSTP and LACP allows multiple switches to be configured together in meshed redundant link architecture. First define the RSTP Configuration on the switches. Then define the LACP ports. Then finally connect the ports together to form the meshed redundant link topology as shown above.

Using the Multilink switch with dual-homing allows the edge devices to have link level redundancy as well – bringing the fault tolerance from the network to the edge.

Figure 17-7: Redundancy using LACP, RSTP and STP



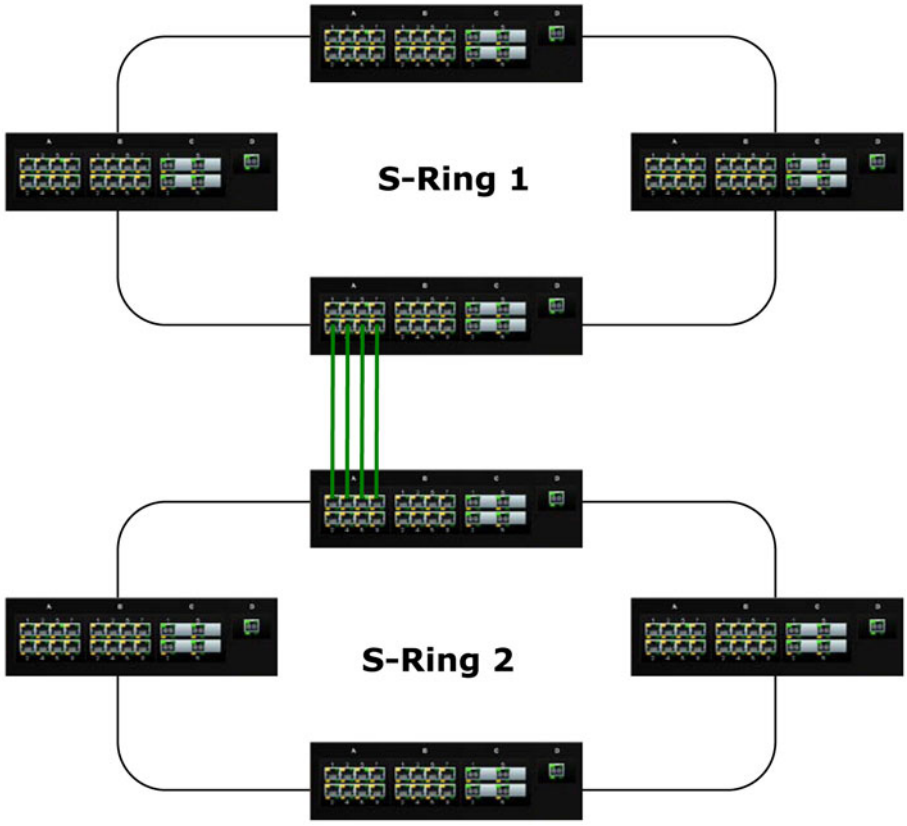
LACP, along with RSTP/STP brings redundancy to the network core or backbone. Using this reliable core with a dual homed edge switch brings reliability and redundancy to the edge of the network.

NOTE

Do not to use LACP with S-Ring at this time.

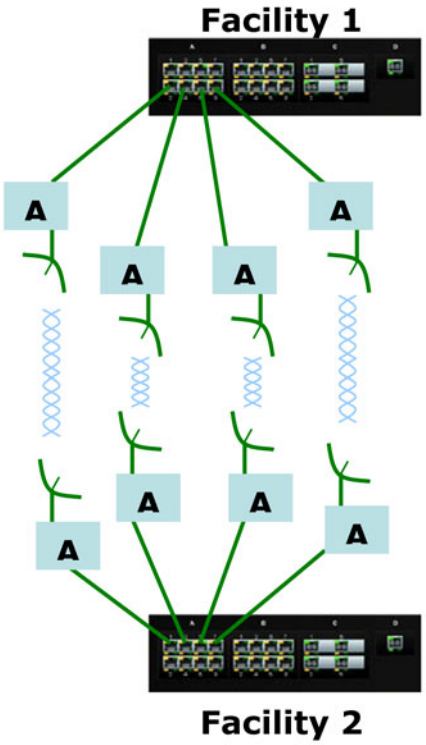
Since S-Ring and LACP use the same BPDUs (called LACPDUs), the architecture shown below is not supported in this release.

Figure 17-8: S-Ring Architecture is Not Supported



LACP can be used for creating a reliable network between two facilities connected via a wireless bridge. As shown in the figure below, four trunk ports are connected to four wireless bridge pairs. This increases the effective throughput of the wireless connections and also increases the reliability. If one of the bridges were to stop functioning, the other three continues to operate, providing a very reliable infrastructure.

Figure 17-9: Wire Bridge Connection between 2 Facilities



Creating a reliable infrastructure using wireless bridges (between two facilities) and LACP is shown in the figure above. "A" indicates a Wi-Fi wireless Bridge or other wireless Bridges.

Another definition worth noting is primary port. Primary port is the port over which specific traffic like Multicast (IGMP), unknown Unicast and broadcast traffic is transmitted. As shown by the add port command, the port with the lowest priority value has the highest priority and is designated as the primary port. If traffic analysis is required, it is recommended to mirror the primary port (and physically disconnect the other ports if all traffic needs to be captured).

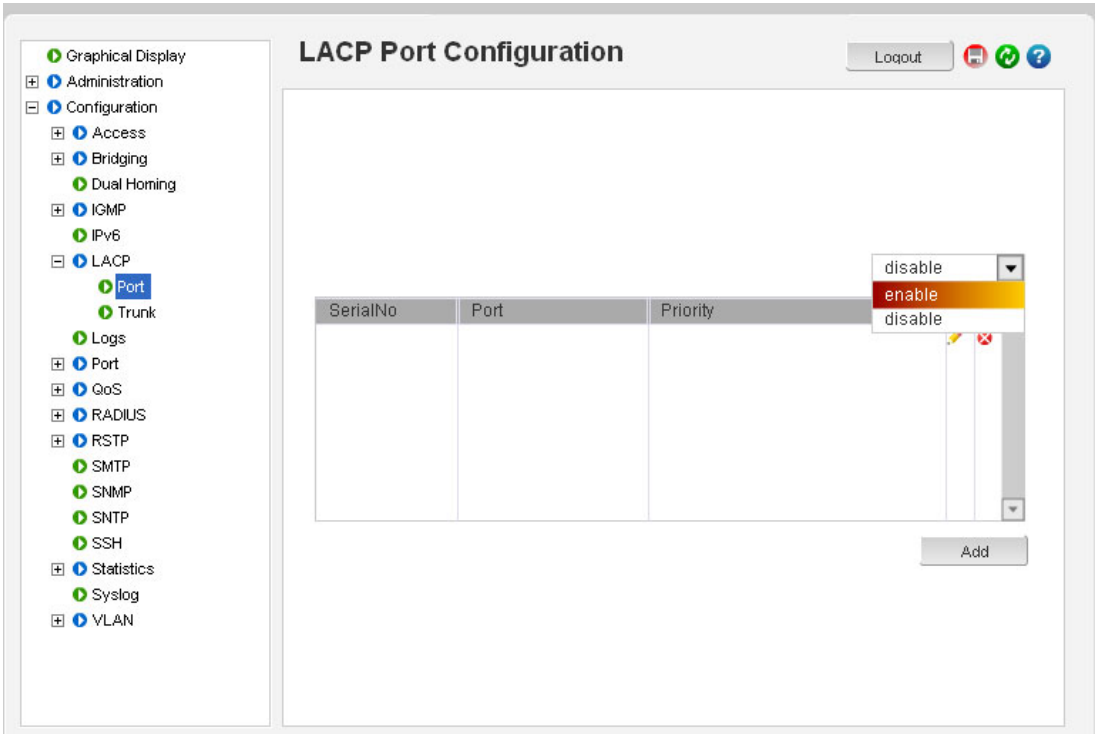
If multiple ports have the same priority, the first port physically connected becomes the primary port. In case the ports are already connected, the port with the lowest port count becomes the primary port i.e. if ports 12, 13, 14 are designated as the LACP group, port 12 would become the primary port.

If the primary port fails, the next available secondary port is designated as the primary port. So in the example above, if port 12 fails, port 13 is designated as the primary port.

To configure LACP, first define the set of ports which make up the trunk. Next define the set of trunks. In the example below, we define ports 12, 13 as a set of ports for the trunk.

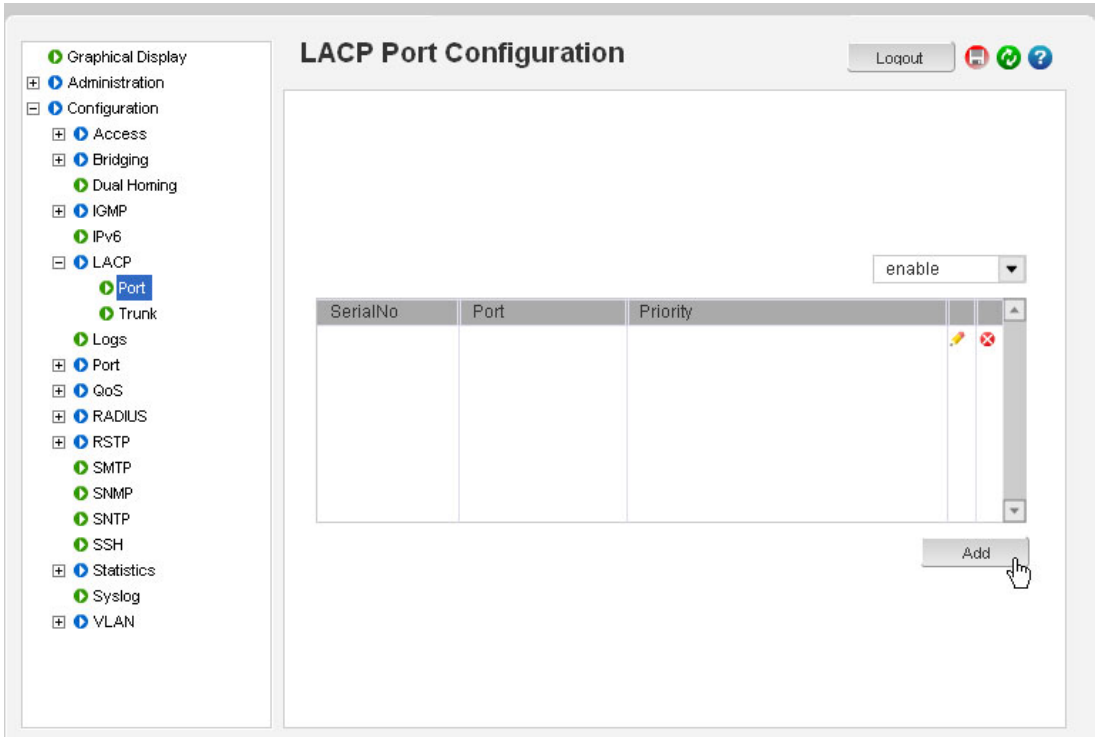
For the LACP menu, use Configuration → LACP → Port as shown below.

Figure 17-10: Enable LACP



Enable LACP first.

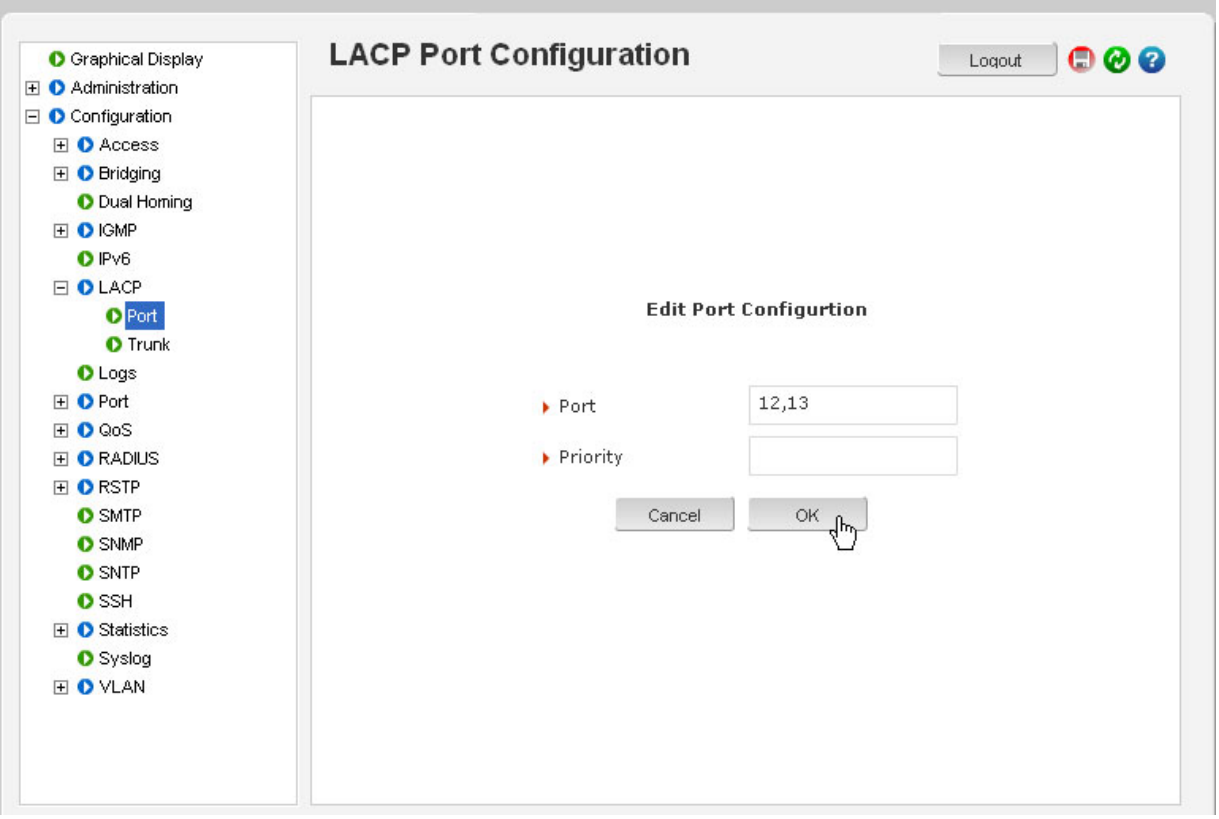
Figure 17-11: Add Ports



Add the necessary ports to define the trunk.

Define ports 12 and 13 as the set of ports for the first trunk, see figure below.

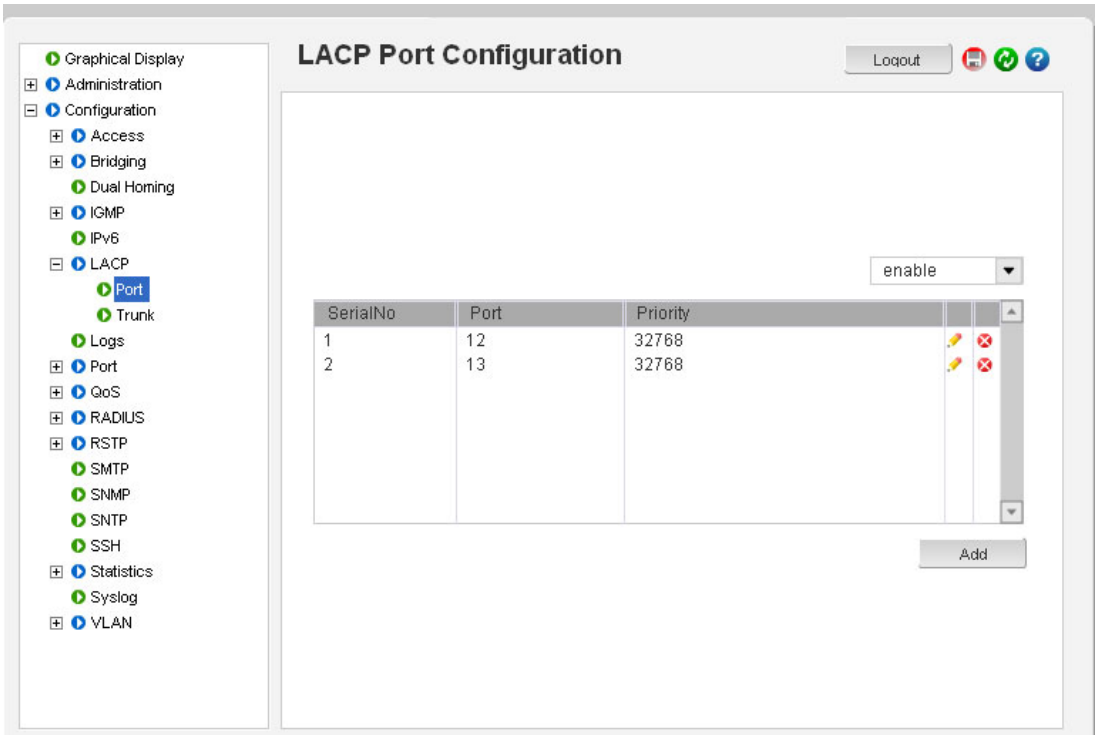
Figure 17-12: Add Ports to the Trunk



Add the ports which make up the trunk. The priorities are automatically assigned – this field can be left blank.

The priorities can be changed to manipulate on which links the Ethernet traffic traverses on.

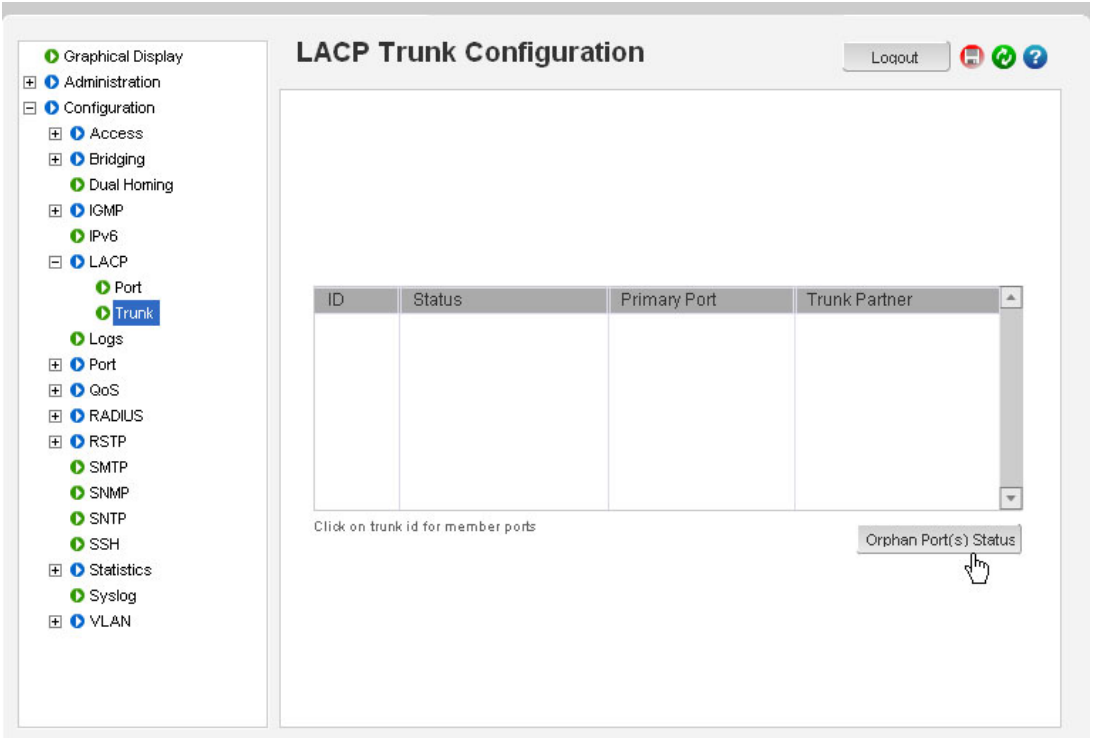
Figure 17-13: Edit Port Values



After the ports are added, the values can be edited if needed or the ports deleted using the edit or delete icons on the menu.

Once the ports are added, the trunk status is checked by viewing the Configuration → LACP → Trunk menu as shown below.

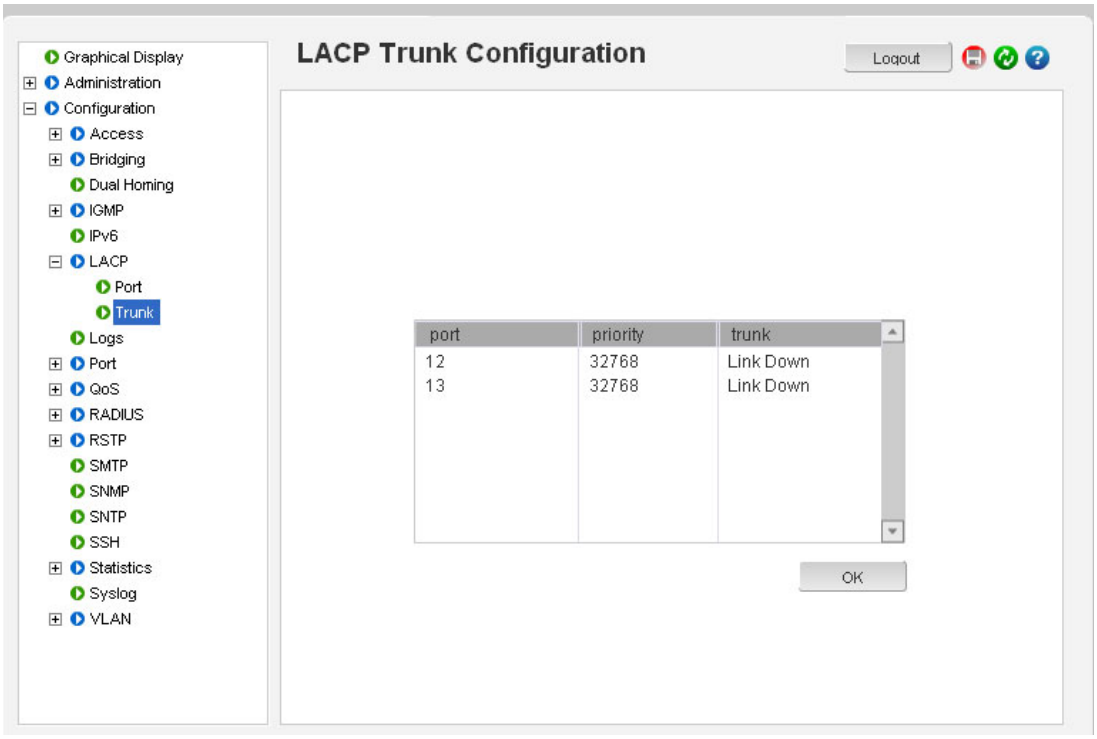
Figure 17-14: Check the Trunk Status



One would expect the trunk status to display the trunk which was just added. However in this situation, no trunk is displayed. Clicking on the Orphan Port(s) status, as shown above, l displays the status of the “orphan” ports or ports which are not members of any LACP trunks.

The orphan status displays the reason why the ports were not members of the LACP trunk. The links are down – i.e. the ports were not connected. After the other switch is configured with the proper LACP settings, the RJ-45 cables should be plugged in to enable LACP.

Figure 17-15: Orphan Status Display



Only after the other switch is configured with the proper LACP settings, the Ethernet cables should be plugged into both the switches to enable LACP. After that is done, the Trunk menu displays the LACP trunks which are active.

Finally – save the configuration using the Save icon.

Multilink ML3000/ML3100

Chapter 18: PTP 1588

18.1 Precision Time Protocol (PTP) 1588

Time can be synchronized using SNTP or other protocols. The timing accuracy attained by these protocols is not accurate enough for substations. Substations deal with multiple sources of power such as those from solar farms, off-shore wind turbines, wind turbine farms, and geothermal sources.

The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout the network. On a LAN it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control of systems.

18.1.1 Overview

In the SNTP Chapter, time synchronization using SNTP was presented. While SNTP is sufficient for security activities such as SYSLOG, intrusion detection, and others, the accuracy of timing synchronization using SNTP is not sufficient for Smart Grid Applications. For example, a 41 nanosecond difference amounts to one degree offset between two sources of power. The offset causes an increase in “virtual” power, which ultimately translates to revenues which are lost as “wasted” energy. This is especially critical today with different power sources. Power sources vary – power can be generated using coal, natural gas, or other fossil fuels. Power can also be generated from natural occurring energy sources such as sun, wind, tides, geo-thermals etc. These power sources are generally termed as renewable sources or green energy (as they typically do not emit CO2.) However, these renewable sources are not as consistent as fossil fuel.

The Precision Time Protocol (PTP) is a high-precision time protocol for synchronization used in measurement and control systems which reside on a local area network. Using PTP, accuracy in the sub-microsecond range may be achieved with low-cost implementations. PTP was originally defined in the IEEE 1588-2002 standard, officially entitled "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems". In 2008 a revised standard, IEEE 1588-2008, was released. This new version, also known as PTP Version 2, improves accuracy,precision, and robustness but Version 2 is not backwards compatible with the original 2002 version (called Version 1). IEEE 1588 is designed to fill a niche not well served by either of the two dominant protocols: NTP and

GPS. IEEE 1588 is designed for local systems requiring accuracies beyond those attainable using NTP. It is also designed for applications that cannot bear the cost of a GPS receiver at each node, or when GPS signals are inaccessible.

Architecture - The IEEE 1588 standards describe hierarchical master-slave architecture for clock distribution. Under this architecture, a time distribution system consists of one or more communication mediums (network segments), and one or more clocks.

The **ordinary clock** is a device with a single network connection and is either the source of (master) or destination for (slave) synchronization reference.

The **boundary clock** has multiple network connections and can accurately bridge synchronization from one network segment to another.

A **synchronization master** is elected for each of the network segments in the system. The root timing reference is called the **grandmaster**. The grandmaster transmits synchronization information to the clocks residing on its network segment. The boundary clocks with a presence on that segment then relay accurate time to the other segments to which they are connected.

A simplified PTP system frequently consists of ordinary clocks connected to a single network. No boundary clocks are used. A grandmaster is elected and all other clocks synchronize directly to it.

IEEE 1588-2008 introduces a clock associated with network equipment used to convey PTP messages. The transparent clock modifies PTP messages as they pass through the device. Timestamps in the messages are corrected for time spent traversing the network equipment. This scheme improves distribution accuracy by compensating for delivery variability across the network.

Some features of IEEE 1588 protocol can be summarized as:

- International standard
- Timing synchronization can be implemented over packet based networks e.g., Ethernet
- High accuracy – sub microsecond synchronization
- Simple – can be implemented in hardware or software
- Minimal overhead – network, processor, management
- Protocol – can be implemented on different networks

The ML3000/3100 switch implements the PTP protocol. The examples below show how the ML3000/3100 switch can be used for setting up a network with PTP.

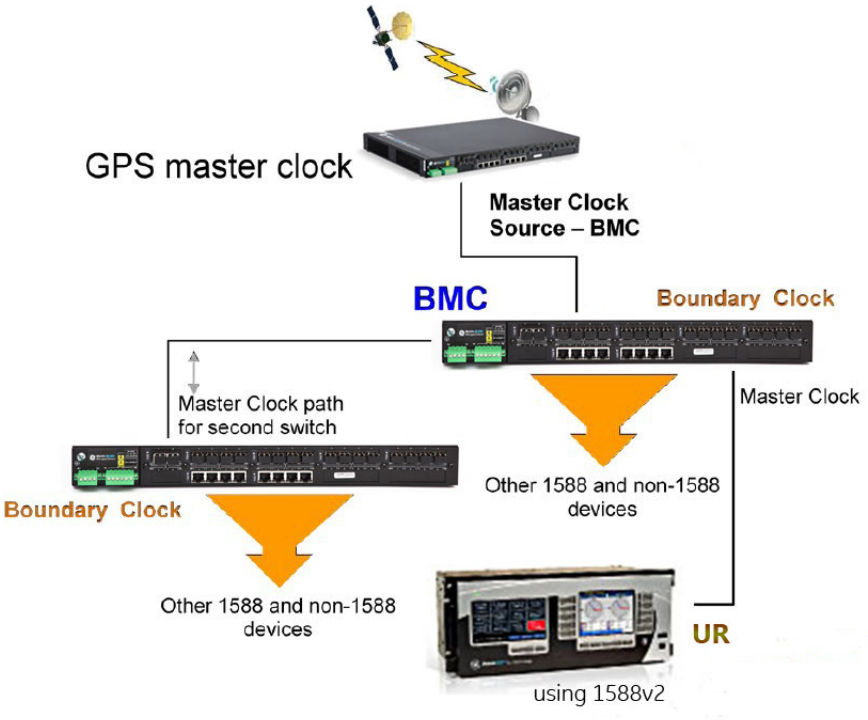


FIGURE 18–1: Use the ML3000/3100 as a Boundary Clock with a Grandmaster Clock

In the figure above an ML3000/3100 is used as a boundary clock along with a grandmaster clock. The SCADA device works as an ordinary clock as it has one source and adjusts its time from the PTP packets.

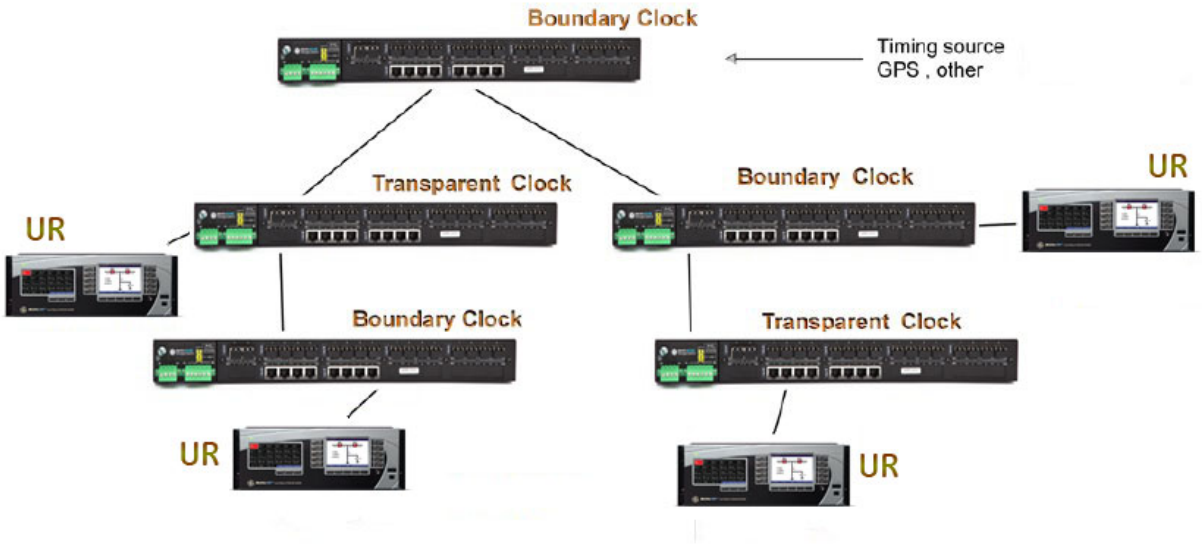


FIGURE 18–2: Use the ML3000/3100 switch as a Boundary Clock (BC) or Transparent Clock (TC)

In the figure above the ML3000/3100 switch is shown in a setup where it used as a Boundary Clock (BC) or Transparent Clock (TC) depending on the devices being connected and the hierarchy.

IEEE 1588 is implemented as a message-based protocol. For example, event messages such as sync, delay-request, follow up, and delay response are used by ordinary clocks and boundary clocks to synchronize timing information. Similarly event messages are used by transparent clocks to measure and compensate for delays.

General messages are used for non-critical timing functions. For example, signaling messages are used for non-critical information and Announce messages are used to develop a clock hierarchy. Management messages are used to configure and manage PTP.

All PTP messages are sent using multicast messaging. IEEE 1588-2008 introduces an option for devices to negotiate unicast transmission on a port-by-port basis. PTP messages may use the Internet Protocol (IP) for transport. The original specification used only IPv4 transports, but this has been extended to IPv6. Over IP, messages use the User Datagram Protocol (UDP). Datagrams are transmitted using IP multicast addressing, for which multicast group addresses are defined for IPv4 and IPv6. Event messages are sent to port number 319. General messages use port number 320. Replies to Management messages are always returned to the unicast address of the originator. The messages used by PTP are multicast messages. Encapsulation is also defined for bare IEEE 802.3 Ethernet, DeviceNet, ControlNet and PROFIBUS. PTP uses Ethertype 0x88F7 and an Ethernet multicast destination address of 01-1B-19-00-00-00 for all but peer delay messages. Peer delay messages are sent to 01-80-C2-00-00-0E.

The ML3000/3100 switch software uses the defined MAC addresses in IEEE 1588v2 protocol to designate an IEEE 1588v2 timing UDP packet. They are 01-1B-19-00-00-00 and 01-80-C2-00-00-0E as discussed above.

18.1.2 Configuring PTP

Note that the commands entered by the user are shown in bolded text below. In addition the parameters values are shown as follows:

- Optional entries are shown in [square brackets]
- Parameter values within are shown in < pointed brackets >
- Optional parameter values are shown again in [square brackets]

The commands used to configure PTP are as follows:

*Syntax **ptp** - enter the PTP sub group of commands*

*Syntax **ptp <enable|disable>** - enable or disable the ptp capabilities*

*Syntax **announce= announce interval=<1|2|4|8|16>** - shows the intervals of the ptp configuration*

*Syntax **power-profile= [<enable|disable>] [vlan=<none|0-4095>] [prio=<0..7>] [gmid=<3-254>]***

*Syntax **sync interval=<250|500|1000|2000|4000|8000|16000>** - set the sync interval (in milliseconds)*

*Syntax **setptp [clock=<auto|tc|bc>] [priority1=<0-255>] [priority2=<0-255>] [domain=<0..127] [sync=<enable|disable>] [delay=<e2e|p2p>]**- set the behavior of the clock as a boundary clock or transparent clock. Priority 1 and Priority 2 are used by network administrators to deterministically set which clock becomes the master clock in case there is a resolution conflict or "tie"*

The master clock algorithm is such that there could be several master clocks in a network. Even though the occurrence could be rare, there is a finite probability that such an event could happen. In situations like this, the combination of *Priority 1* and *Priority 2* are used to determine which clock becomes the master.

For example, if there are two switches in the network with the settings as follows:

Switch1	Priority1 = 1	Priority 2 = 200
Switch2	Priority1 = 5	Priority 2 = 5

Switch 1 will become the master as Priority 1 is a lower value. In situations where Priority 1 values are the same, Priority 2 values are used.

Default values for Priority 1 and Priority 2 are 128.

*Syntax **setport port=<port|list|range> [mode=<auto|mac|udp>] [<enable|disable>]** - define the ports where PTP packets are examined for time synchronization*

*Syntax **show modules** - show the modules in the system. If there is a IEEE 1588 module present it will display that module.*

*Syntax **show-port=***

Port | Mode
01 AUTO-MAC
02 AUTO-MAC
03 AUTO-MAC
04 AUTO-MAC
05 AUTO-MAC
06 AUTO-MAC
07 AUTO-MAC
08 AUTO-MAC
09 AUTO-MAC
10 AUTO-MAC
11 AUTO-MAC
12 AUTO-MAC
13 AUTO-MAC
14 AUTO-MAC
15 AUTO-MAC
16 AUTO-MAC --
---more-------

show the ports and the modes.

*Syntax **show ptp** - show the status of PTP (enabled or disabled)*

A sequence of commands for configuring PTP are shown below.

.

ML3000(ptp)## *ptp*
ML3000(ptp)## *sync interval=4000*
Sync Interval Set.
ML3000(ptp)## *setptp clock=auto*
Clock Type Set
ML3000(ptp)## *ptp enable*
PTP is enabled.
ML3000(ptp)## *show ptp*
PTP CONFIGURATION

PTP Status: ENABLED
Ports Currently Enabled : 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
21,22,23,24,29,32,33,36
PTP Sync Interval: 4 Sec
CLOCK Configuration: AUTO
CLOCK Operating Mode: Master
Delay Measurement Mechanism: End-to-End
Priority1: 128
Priority2: 128
ML3000(ptp)## *announce*
announce interval=<1|2|4|8|16>
ML3000(ptp)## *show modules*
SLOT DESCRIPTION

C 4 Port TP-MDIX Module
D 4 Port TP-MDIX Module
E 4 Port TP-MDIX Module
F 4 Port TP-MDIX Module
G 4 Port Fiber100 with IEEE1588 ? ?
I 2 Port Fiber100 Module
J 2 Port Fiber100 Module
ML3000(ptp)## *power-profile*
power-profile [<enable|disable>] [vlan=<none|0-4095>] [prio=<0..7>] [gmid=<3-254>]
ML3000(ptp)## *setport port=5-36 disable*
ML3000(ptp)## *setport port=17-20 enable*
ML3000(ptp)## *show-port*

Port | Mode
---
01 AUTO-MAC
02 AUTO-MAC
03 AUTO-MAC

```
04 AUTO-MAC
05 AUTO-MAC
06 AUTO-MAC
07 AUTO-MAC
08 AUTO-MAC
09 AUTO-MAC
10 AUTO-MAC
11 AUTO-MAC
12 AUTO-MAC
13 AUTO-MAC
14 AUTO-MAC
15 AUTO-MAC
16 AUTO-MAC
--more—
ML3000(ptp)## show ptp
PTP CONFIGURATION
-----------------
PTP Status : ENABLED
Ports Currently Enabled : 17,18,19,20
PTP Sync Interval : 4 Sec
CLOCK Configuration : AUTO
CLOCK Operating Mode : Master
Delay Measurement Mechanism : End-to-End
Priority1 : 128
Priority2 : 128
ML3000(ptp)## exit
ML3000
```

FIGURE 18–3: Configuration and Setup of PTP Commands

The show modules command displays which module has Syntax **ptp** - enter the PTP sub group of commands.

18.1.3 List of Commands in this Chapter

*Syntax **ptp <enable|disable>** - enable or disable the ptp capabilities*

*Syntax **announce= announce interval=<1|2|4|8|16>** - shows the intervals of the ptp configuration*

*Syntax **power-profile= [<enable|disable>] [vlan=<none|0-4095>] [prio=<0..7>] [gmid=<3-254>]** - show the power-profile of the ptp configurations*

*Stntax **sync interval=<250|500|1000|2000|4000|8000|16000>** - set the sync interval (in milliseconds)*

*Syntax **setptp [clock=<auto|tc|bc>] [priority1=<0-255>] [priority2=<0-255>] [domain=<0..127] [sync=<enable|disable>] [delay=<e2e|p2p>]**- set the behavior of the clock as a boundary clock or transparent clock. Priority 1 and Priority 2 are used by*

network administrators to deterministically set which clock becomes the master clock in case there is a resolution conflict or "tie". PTP mode should explicitly be set to "tc" (transparent clock) or "bc" (boundary clock).

*Syntax **setport port=<port|list|range> [mode=<auto|mac|udp>] [<enable|disable>]** - define the ports where PTP packets are examined for time synchronization*

*Syntax **show-port=*** *show the ports and the modes.*

Port | Mode
01 AUTO-MAC
02 AUTO-MAC
03 AUTO-MAC
04 AUTO-MAC
05 AUTO-MAC
06 AUTO-MAC
07 AUTO-MAC
08 AUTO-MAC
09 AUTO-MAC
10 AUTO-MAC
11 AUTO-MAC
12 AUTO-MAC
13 AUTO-MAC
14 AUTO-MAC
15 AUTO-MAC
16 AUTO-MAC --
---more-------

*Syntax **show ptp** - show the status of PTP (enabled or disabled)*

*Syntax **show modules** - show the modules in the system. If there is a IEEE 1588 module present it will display that module.*

Multilink ML3000/ML3100

Chapter 19: Miscellaneous commands

19.1 Alarm Relays

19.1.1 Description

In a wiring closet, it would be helpful if there were a visual indication for faults on components on the network. Normally, these would be performed by LEDs. While the MultiLink switches have the necessary LEDs to provide the information needed, they also have provision for tripping or activating an external relay to electrically trigger any circuit desired. These could be an indicator light, a flashing strobe light, an audible alarm or other devices.

The MultiLink family of switches has a software (optional) controlled relay contact that can be use to report alarm conditions. The relay is held closed in normal circumstances and will go to the open position during alarm conditions.

Two types of alarm signals are defined in the alarm system.

- SUSTAINED
- MOMENTARY

The SUSTAINED mode is used to report a continuing error condition. The MOMENTARY mode is used to report a single event.

The following pre-defined events are currently supported on the ML3000 and the relay which can be triggered by software:

Table 19–1: Pre-defined conditions for the ML3000/ML3100

Event ID	Description	Signal type
2	Cold Start	MOMENTARY
3	Warm Start	MOMENTARY
4	Link Up	MOMENTARY
5	Link Down	MOMENTARY
6	Authentication Failure	MOMENTARY
7	RMON Rising Alarm	MOMENTARY
8	RMON Falling Alarm	MOMENTARY
9	Intruder Alarm	MOMENTARY
11	Broadcast Storm Detected	MOMENTARY
12	STP/RSTP Reconfigured	MOMENTARY

19.1.2 Configuring Alarm Relays through the Command Line Interface

To customize these capabilities, the ML3000 provides additional software capabilities and commands for configuring the alarm relays.

The `alarm` command enters the alarm configuration mode

alarm

The `add` command enables alarm action in response to the specified event ID.

add *event=<event-id|list|range|all>*

The `period` command sets the duration of relay action for the momentary type signal. This may be needed to adjust to the behavior of the circuit or relay. The time is in seconds, with a default of 3.

period *time=<1..10>*

The `del` command disables alarm action in response to the specified event ID.

del *event=<event-id|list|range|all>*

The `alarm` command globally enables or disables the alarm action.

alarm *<enable|disable>*

The `show alarm` command displays the current status of alarm system

show alarm

An example of setting up the external relays and alerts is shown below.

```
ML3000#alarm

ML3000(alarm)##show alarm
Alarm Events Configuration
--------------------------

  Alarm Status: DISABLED
  Relay Closure Time Period: 3 Seconds

EventId Description                    Mode                FlagStatus

     2  Cold Start                     NOT ENABLED           RESET
     3  Warm Start                     NOT ENABLED           RESET
     4  Link Up                        NOT ENABLED           RESET
     5  Link Down                      NOT ENABLED           RESET
     6  Authentication Failure         NOT ENABLED           RESET
     7  RMON Raising Alarm             NOT ENABLED           RESET
     8  RMON Falling Alarm             NOT ENABLED           RESET
     9  Intruder Alarm                 NOT ENABLED           RESET
    11  Broadcast Storm Detected       NOT ENABLED           RESET
    12  STP/RSTP Reconfigured          NOT ENABLED           RESET

ML3000(alarm)##add event=2
Alarm Event(s) Added: 2
ML3000(alarm)##show alarm
Alarm Events Configuration
--------------------------

  Alarm Status: DISABLED
  Relay Closure Time Period: 3 Seconds

EventId Description                    Mode                FlagStatus

     2  Cold Start                     MOMENTARY             RESET
     3  Warm Start                     NOT ENABLED           RESET
     4  Link Up                        NOT ENABLED           RESET
     5  Link Down                      NOT ENABLED           RESET
     6  Authentication Failure         NOT ENABLED           RESET
     7  RMON Raising Alarm             NOT ENABLED           RESET
     8  RMON Falling Alarm             NOT ENABLED           RESET
     9  Intruder Alarm                 NOT ENABLED           RESET
    11  Broadcast Storm Detected       NOT ENABLED           RESET
    12  STP/RSTP Reconfigured          NOT ENABLED           RESET
```

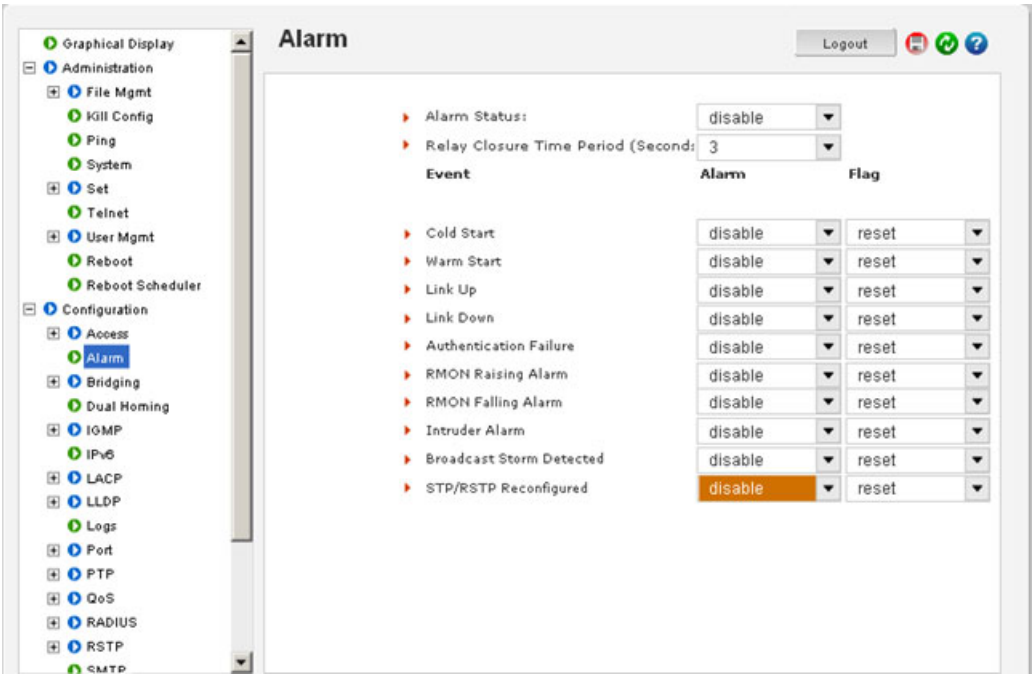
```
ML3000(alarm)##alarm enable
Alarm system Enabled

ML3000(alarm)##show alarm
Alarm Events Configuration
--------------------------

  Alarm Status: ENABLED
  Relay Closure Time Period: 3 Seconds

EventId Description                    Mode                FlagStatus

     2  Cold Start                     MOMENTARY             RESET
     3  Warm Start                     NOT ENABLED           RESET
     4  Link Up                        NOT ENABLED           RESET
     5  Link Down                      NOT ENABLED           RESET
     6  Authentication Failure         NOT ENABLED           RESET
     7  RMON Raising Alarm             NOT ENABLED           RESET
     8  RMON Falling Alarm             NOT ENABLED           RESET
     9  Intruder Alarm                 NOT ENABLED           RESET
    11  Broadcast Storm Detected       NOT ENABLED           RESET
    12  STP/RSTP Reconfigured          NOT ENABLED           RESET
```

```
ML3000(alarm)##alarm disable
Alarm system Disabled

ML3000(alarm)##del event=3,5,7
Event 3 is Already Disabled.
Event 5 is Already Disabled.
Event 7 is Already Disabled.

ML3000(alarm)##show alarm
Alarm Events Configuration
--------------------------

  Alarm Status: DISABLED
  Relay Closure Time Period: 3 Seconds

EventId Description                          Mode                 FlagStatus

     2  Cold Start                         MOMENTARY              RESET
     3  Warm Start                         NOT ENABLED            RESET
     4  Link Up                            NOT ENABLED            RESET
     5  Link Down                          NOT ENABLED            RESET
     6  Authentication Failure             NOT ENABLED            RESET
     7  RMON Raising Alarm                 NOT ENABLED            RESET
     8  RMON Falling Alarm                 NOT ENABLED            RESET
     9  Intruder Alarm                     NOT ENABLED            RESET
    11  Broadcast Storm Detected           NOT ENABLED            RESET
    12  STP/RSTP Reconfigured              NOT ENABLED            RESET

ML3000(alarm)##del event=2
Alarm Event(s) Deleted: 2
ML3000(alarm)##show alarm
Alarm Events Configuration
--------------------------

  Alarm Status: DISABLED
  Relay Closure Time Period: 3 Seconds

EventId Description                          Mode                 FlagStatus

     2  Cold Start                         NOT ENABLED            RESET
     3  Warm Start                         NOT ENABLED            RESET
     4  Link Up                            NOT ENABLED            RESET
     5  Link Down                          NOT ENABLED            RESET
     6  Authentication Failure             NOT ENABLED            RESET
     7  RMON Raising Alarm                 NOT ENABLED            RESET
     8  RMON Falling Alarm                 NOT ENABLED            RESET
     9  Intruder Alarm                     NOT ENABLED            RESET
    11  Broadcast Storm Detected           NOT ENABLED            RESET
    12  STP/RSTP Reconfigured              NOT ENABLED            RESET
```

19.1.3 Configuring Alarm Relays with EnerVista Secure Web Management software

To customize the alarm relays,

▷ Select the **Configuration > Alarms** menu item.



Each alarm can be enabled or disabled form the screen shown above. All alarms can be enabled or disabled using the Alarm Status drop down menu. Relay closure times can be set using the drop down menu.

▷ After changing the Alarm settings, save the configuration using the save icon ( ),

19.2 E-mail

19.2.1 Description

SMTP (RFC 821) is a TCP/IP protocol used in sending e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or Internet Message Access Protocol (IMAP) that lets the user save messages in a server mailbox and download them as needed from the server. In other words, users typically use a program that uses SMTP for sending e-mails (out going - e.g. replying to an e-mail message) and either POP3 or IMAP for receiving messages that have been arrived from the outside world. While SMTP (and its related protocols such as POP3, IMAP etc.) are useful transports for sending and receiving e-mails, it is extremely beneficial for a network administrator to receive e-mails in case of faults and alerts. The MultiLink family of switches can be setup to send and e-mail alert when a trap is generated.

If this capability is used, please ensure that SPAM filters and other filters are not set to delete these e-mails.

GE Multilin recommends that a rule be setup on the mail server so that all e-mails indicating SMTP faults are automatically stored in a folder or redirected to the necessary administrators.

The SMTP alerts can be configured using the MultiLink Switch Software for the following:

- Send e-mail alert according to the configuration rules when a specific event category happens.
- Send e-mail alert according to the configuration rules when a specific trap SNMP trap category happens.
- Provide configuration and customization commands for users to specify SMTP server to connect to, TCP ports, user recipients and filters.
- The SMTP alerts provide the following capabilities:
- SMTP alerts can be enabled or disabled globally.
- User can defined a global default SMTP server identified by its IP address, TCP port and retry count.
- User can add up to five SMTP alert recipients. Each recipient is identified by an ID and e-mail address. The e-mail address needs to be a valid address and can be an alias setup for distribution to a larger audience.
- Filters are provided for each recipient to allow only certain categories of traps and events be sent by e-mail.
- Each recipient can have its own SMTP server and TCP port number, if this is not defined on a certain recipient, the default SMTP server and TCP port number is used.

19.2.2 Commands

The `smtp` command configures the SNMP alerts to be sent via e-mail.

smtp

smtp *<enable|disable>*

The `show smtp` command displays the current SMTP global settings and recipients displays the currently configured recipients of e-mail alerts.

show smtp *<config|recipients>*

The add command adds a specific id, where id represents the recipient identification and ranges from 1 to 5. The software allows a maximum of 5 recipients

add *id=<1-5> email=<email-addr> [traps=<all|none|S|R|E>] [events=<all|none|I|A|C|F|D>] [ip=<ip-addr>] [port=<1-65535>] [domain=<domain>]*

The add command has the following additional parameters:

- The email parameter is the e-mail address of the recipient.
- The optional traps parameter represents the trap filter. If value is all, all traps of any type will be sent to this recipient. If value is none, no traps are sent to this recipient. Value can also be a combination of 'S' (SNMP), 'R' (RMON) and 'E' (enterprise). For example, trap=SR means that SNMP and RMON traps will be sent via e-mail to the recipient. If this option is not defined, the recipient will have a default value of "all".
- The optional events parameter is the event filter. Value can be "all" - all event severity types will be sent to recipient, "none" - no event will be sent to recipient or a combination of 'I' (informational), 'A' (activity), 'C' (critical), 'F' (fatal) and 'D' (debug). With "event=ACF" implies that events of severity types activity, critical and fatal will be sent to recipients by e-mail. If this option is not defined, a value of "all" is taken.
- The optional ip parameter represents the SMTP server IP address. This is the SMTP server to connect to for this particular user. If this option is not defined, the global/ default SMTP server is used.
- The optional port parameter specifies the TCP port of the SMTP server. If this is not defined, the global default TCP port is used.

The optional domain parameter specifies the domain name of the SMTP server. If this is not defined, the global default domain name is used.

The delete command deletes the specific id specified. The deleted id no longer receives the traps via e-mail. The id is added using the add command

delete *id=<1-5>*

The sendmail command customizes (and also sends a test e-mail to check SMTP settings) the e-mail delivered by specifying the e-mail subject field, server address, to field and the body of the text. See the example in this section for details.

sendmail *server=<ip-addr> to=<email-addr> from=<email-addr> subject=<string> body=<string>*

The server command configures the global SMTP server settings.

server *ip=<ip-addr> [port=<1-65535>] [retry=<0-3>] [domain=<domain>]*

For this command, ip represents the SMTP server IP address, port the TCP port to be used for SMTP communications (default is 25), and retry specifies how many times to retry if an error occurs when sending e-mail (from 0 to 3 with default of 0).

The optional domain parameter specifies the domain name of the SMTP server.

19.2.3 Example

The following example shows how to set SMTP to receive SNMP trap information via e-mail.

E-mail alerts can be forwarded to be received by other devices such as cellphones and pages. Most interfaces to SMTP are already provided by the service provider.

Example 19-1: Configuring SMTP to receive SNMP trap information via e-mail

```
ML3000#smtp
ML3000(smtp)##server ip=3.94.210.25 port=25 retry=3 domain=ge.com
 Successfully set global SMTP server configuration
ML3000(smtp)##show smtp config
      SMTP Global Configuration
 ========================================
 Status         : Disabled
 SMTP Server Host  : 3.94.210.25
 SMTP Server Domain :  ge.com
 SMTP Server Port  : 25
 Retry Count      : 3
ML3000(smtp)##add id=1 email=jsmith@ge.com traps=s events=CF
 Recipient successfully added
ML3000(smtp)##add id=2 email=xyz@abc.com traps=all events=all ip=3.30.154.28 port=2
domain=abc.com
 Recipient successfully added
ML3000(smtp)##show smtp recipients
ID E-mail Address  SMTP Server   From Domain   Port  Traps Events
=================================================================
1  jsmith@ge.com  3.94.210.25    ge.com      25    S     FC
2  xyz@abc.com    3.30.154.28    abc.com     25    All   All
3  --          --         --        --    --    --
4  --          --         --        --    --    --
5  --          --         --        --    --    --
ML3000(smtp)##delete id=2
 Recipient successfully deleted
ML3000(smtp)##show smtp recipients
ML3000(smtp)##show smtp recipients
ID E-mail Address  SMTP Server   From Domain   Port  Traps Events
=================================================================
1  jsmith@ge.com  3.94.210.25    ge.com      25    S     FC
2  --          --         --        --    --    --
3  --          --         --        --    --    --
```

19.3 Statistics

19.3.1 Viewing Port Statistics with EnerVista Secure Web Management software

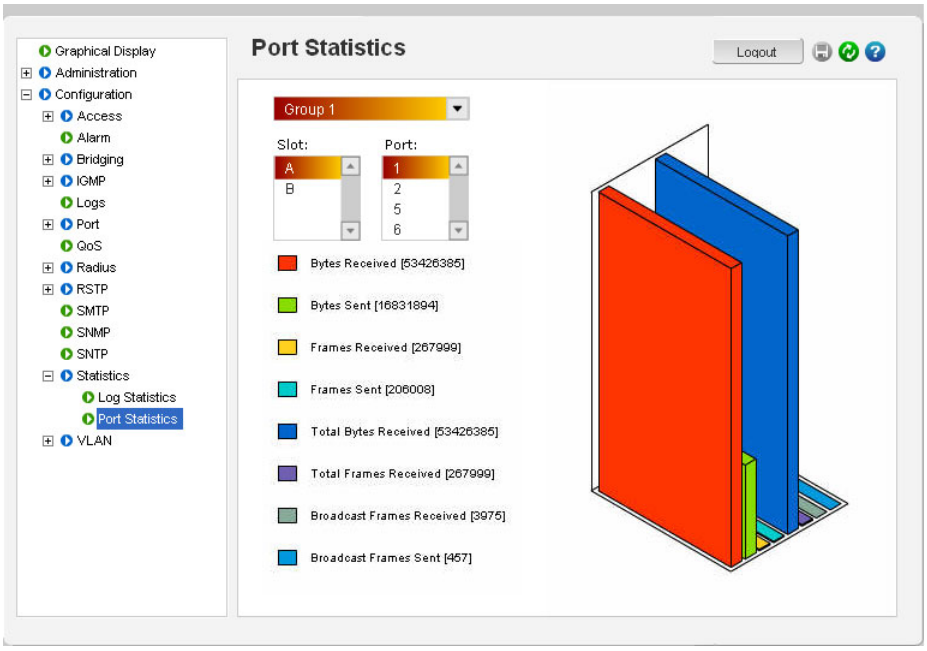
The EnerVista Secure Web Management software allows for the display of several statistics in a graphical format. These are described below.

To view statistics,

▷ Select the **Configuration > Statistics** menu item.

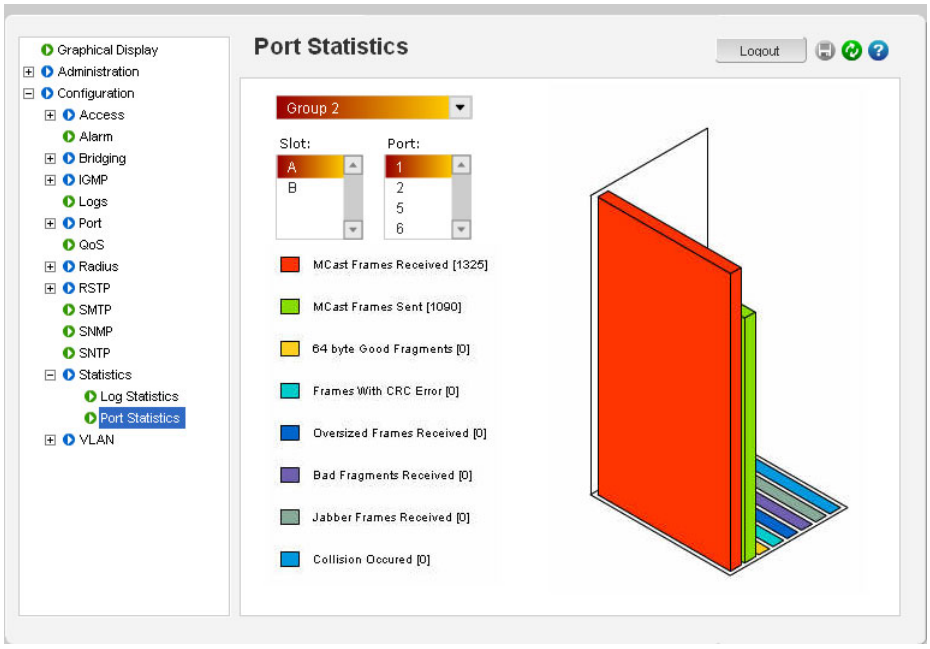
To view port-specific statistics,

▷ Select the **Configuration > Statistics > Port Statistics** menu item.

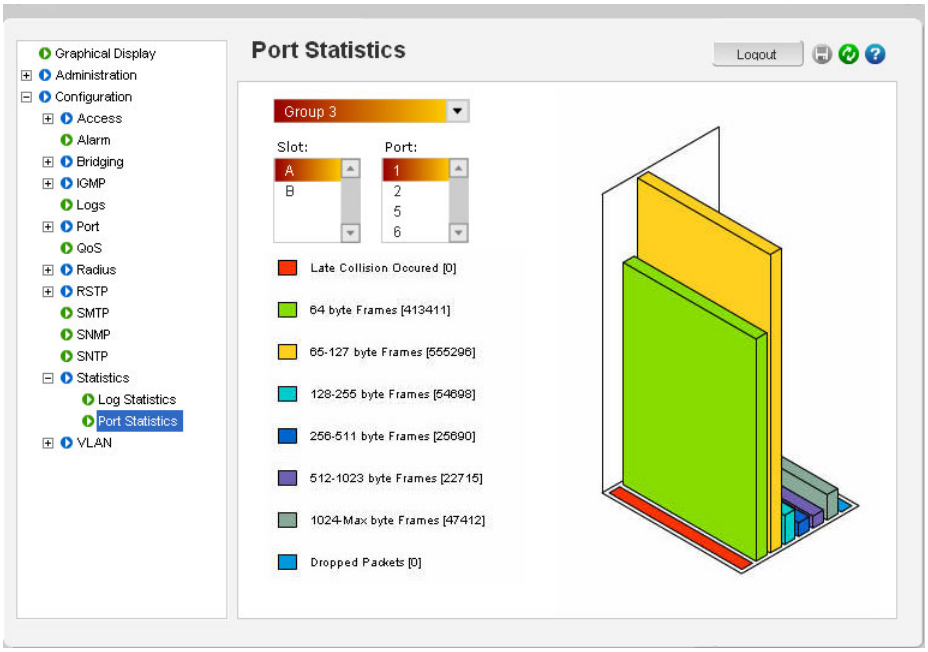


Each port can be viewed by clicking on the back or forward buttons. Each group represents different statistics.

The following figure displays the port statistics for group 2.



The following figure displays the port statistics for group 3.



19.4 Serial Connectivity

19.4.1 Description

When using the serial connectivity with applications such as HyperTerminal, it may be necessary to optimize the character delays so that the FIFO buffer used in the MultiLink switches is not overrun. The important parameters to set for any serial connectivity software is to set the line delay to be 500 ms and the character delay to be 50 ms. For example, using HyperTerminal this can be set under **File > Properties**. When the **Properties** window is open, click on the **ASCII Setup** button and in the **Line Delay** entry box enter in 500 and in the **Character Delay** entry box enter in 50 as shown below.

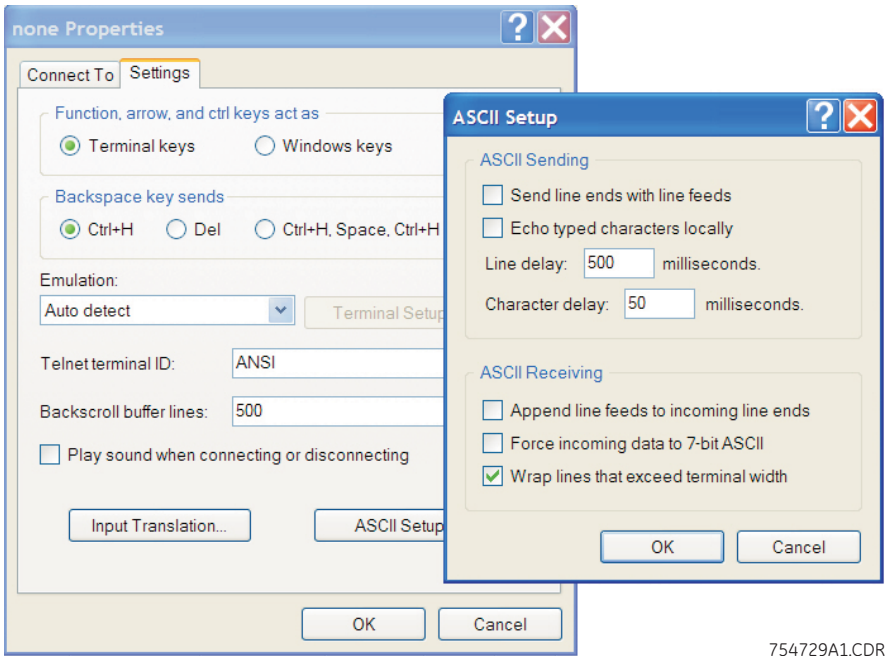


FIGURE 19–1: Optimizing serial connection in HyperTerminal

19.5 History

19.5.1 Commands

The commands below may be useful in repeating commands and obtaining history information.

The `!!` command repeats the last command.

!!

The `!1`, `!2`,..., `!n` commands repeat the *n*th command (as indicated by a show history).

!<n>

The `show history` command displays the last 25 executed commands. If less than 25 commands were executed, only those commands executed are shown.

show history

The history is cleared if the user logs out or if the switch times out. The history count restarts when the user logs in.

The `show version` command displays the current software version.

show version

19.6 Ping

19.6.1 Ping through the Command Line Interface

The `ping` command can be used to test connectivity to other devices as well as checking to see if the IP address is setup correctly. The command syntax is:

ping *<ipaddress> [count=<1-999>] [timeout=<1-256>]*

For example:

ML3000# `ping 3.94.248.61`

3.94.248.61 is alive, count 1, time = 40ms

ML3000# `ping 3.94.248.61 count=3`

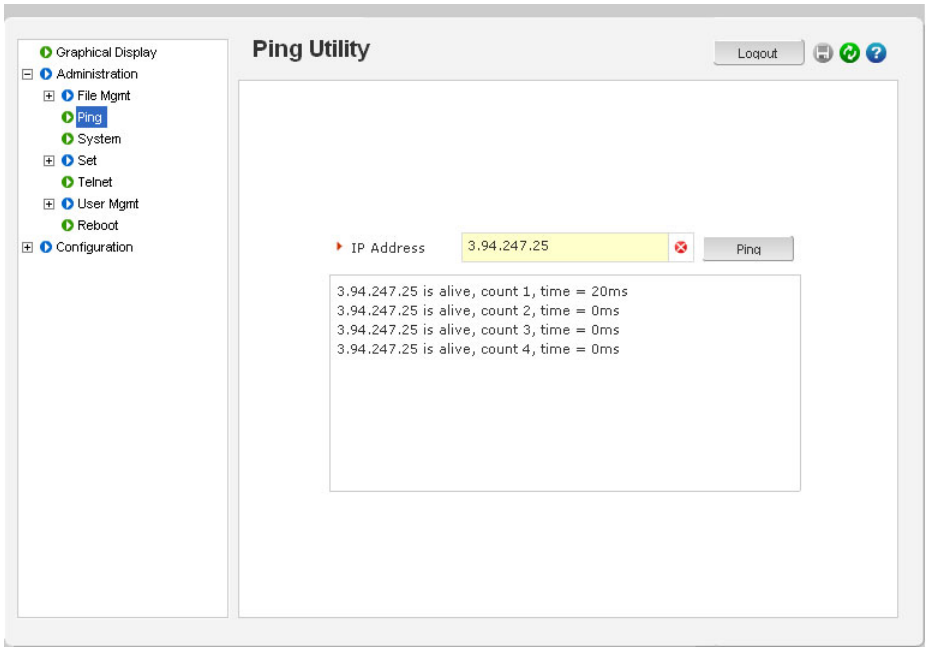
3.94.248.61 is alive, count 1, time = 20ms
3.94.248.61 is alive, count 2, time = 20ms
3.94.248.61 is alive, count 3, time = 40ms

ML3000#

Many devices do not respond to `ping` or block `ping` commands. Make sure that the target device responds or the network allows the ping packets to propagate.

19.6.2 Ping through EnerVista Secure Web Management software

The `ping` command can be used from EnerVista Secure Web Management software to test connectivity to other devices as well as checking to see if the IP address is correct. Select the **Administration > Ping** menu item to use ping.



As mentioned earlier, many devices do not respond to `ping` commands. Make sure that the target device responds or the network allows ping packets to propagate.

19.7 Prompt

19.7.1 Changing the Command Line Prompt

Setting a meaningful host prompt can be useful when a network administrator is managing multiple switches and has multiple telnet or console sessions. To facilitate this, the ML3000 allows administrators to define custom prompts. The command to set a prompt is:

set prompt *<prompt string>*

The length of the prompt is limited to 60 characters.

There are predefined variables that can be used to set the prompt. These are:

- $n: system name
- $c: system contact
- $l: system location
- $i: system IP address
- $m: system MAC address
- $v: version
- $$: the "$" (dollar sign) character
- $r: new line
- $b: space

A few examples on how the system prompt can be setup are shown below.

ML3000# snmp

ML3000(snmp)## `setvar sysname=Core`

System variable(s) set successfully

ML3000(snmp)## `exit`

ML3000# `set prompt $n`

Core# `set prompt $n$b$i`

Core 192.168.5.5# `set prompt $n$b$i$b`

Core 192.168.5.5 # `snmp`

Core 192.168.5.5 (snmp)## `setvar sysname=ML3000`

System variable(s) set successfully

Core 192.168.5.5 (snmp)## `exit`

Core 192.168.5.5 # `set prompt $b$b$i$b`

192.168.5.5 # `set prompt $n$b$i$b`

ML3000 192.168.5.5 #

ML3000 192.168.5.5 # `set prompt Some$bthing$i`

Some thing192.168.5.5# `set prompt Some$bthing$b$i`

Some thing 192.168.5.5#

19.8 System Events

19.8.1 Description

The event log records operating events as single-line entries listed in chronological order, and are a useful tool for isolating problems. Each event log entry is composed of four fields as shown below:

- **Severity** field: Indicates one of the following
- I (Information) indicates routine events; A (Activity) indicates activity on the switch; D (Debug) is reserved for GE Multilin; C (Critical) indicates that a severe switch error has occurred; and F (Fatal). indicates that a service has behaved unexpectedly.
- **Date** field: the date in mm/dd/yy format (as per configured) that the entry was placed in the log.
- **Time** field: is the time in hh:mm:ss format (as per configured) that the entry was placed in the log.
- **Description** field: is a brief description of the event.

The event log holds up to 1000 lines in chronological order, from the oldest to the newest. Each line consists of one complete event message. Once the log has received 1000 entries, it discards the current oldest line (with information level severity only) each time a new line is received. The event log window contains 22 log entry lines and can be positioned to any location in the log.

19.8.2 Command Line Interface Example

The following example illustrates a typical event log.

Example 19-2: Typical system event log

```
ML3000# show log
 S  DATE       TIME         Log Description
 -- ----------  -----------  ------------------------------------------------------
 I  03-02-2005   5:14:43 P.M  SYSMGR:System Subnet Mask changed
 I  01-01-2001  12:00:00 A.M  SYSMGR:successfully registered with DB Manager
 I  01-01-2001  12:00:00 A.M  SYSMGR:successfully read from DB
 A  01-01-2001  12:00:00 A.M  VLAN:Vlan type set to Port VLAN
 I  01-01-2001  12:00:00 A.M  SYSMGR:system was reset by user using CLI command
 I  01-01-2001  12:00:00 A.M  SNTP:Date/Time set to 01-01-2001 12:00AM
 I  01-01-2001  12:00:00 A.M  SNTP:Client started
 I  03-03-2005   4:32:48 A.M  SNTP:Date and Time updated from SNTP server
 I  03-03-2005   9:31:59 A.M  TELNET:Telnet Session Started
 I  03-03-2005   9:32:04 A.M  CLI:manager console login|
 A  03-03-2005   9:32:11 A.M  IGMP:IGMP Snooping is enabled
 A  03-03-2005   9:35:40 A.M  IGMP:IGMP Snooping is disabled
 A  03-03-2005   9:41:46 A.M  IGMP:IGMP Snooping is enabled
```

Event logs can be exported to a ftp or a tftp server on the network for further analysis. The CLI command is used to facilitate the export of the event log

exportlog *mode=<serial|tftp|ftp> <ipaddress> file=<name> doctype=<raw|html>*

Where `mode` is the mode of transfer, `ipaddress` is the IP address of the ftp or TFTP server, `file` is the filename, and `doctype` indicates the log is saved as a text file (raw) or as an HTML file.

Please ensure the proper extension is used for the `file` argument (for example, "html" for an HTML file).

ML3000# `exportlog mode=tftp 192.168.5.2 file=eventlog doctype=html`

Do you wish to export the event logs? ['Y' or 'N'] Y

Successfully uploaded the event log file.

ML3000# `exportlog mode=tftp 192.168.5.2 file=eventlog.txt doctype=raw`

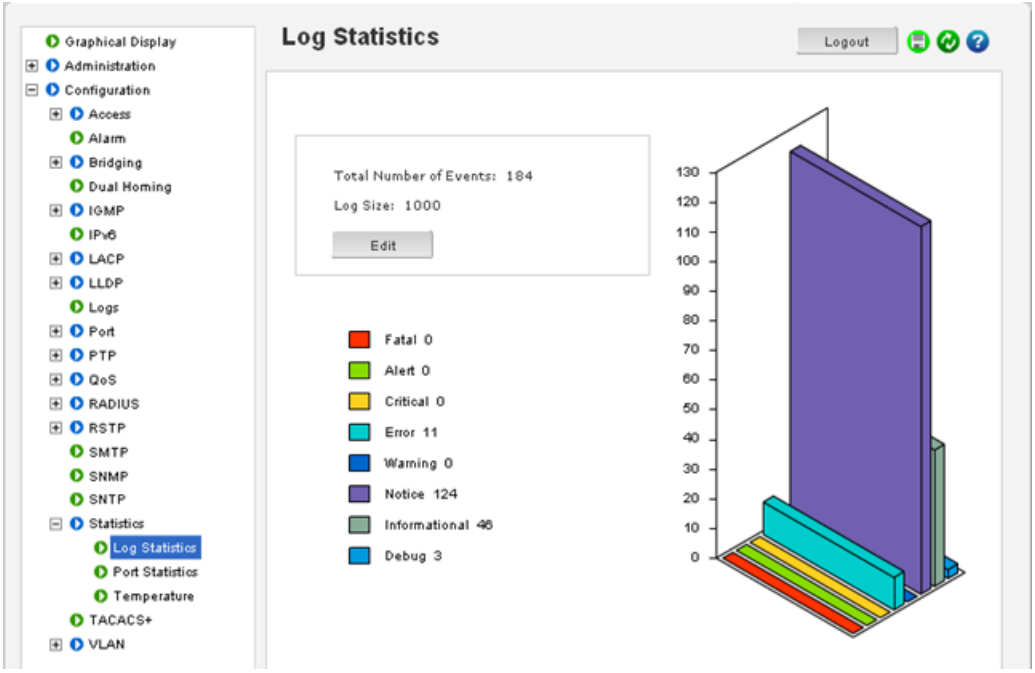
Do you wish to export the event logs? ['Y' or 'N'] Y

Successfully uploaded the event log file.

19.8.3 EnerVista Example

The EnerVista Secure Web Management software provides and overview of the type of Logs by reviewing the statistics. Each specific log can be viewed by viewing the logs menu. To view the log statistics,

▷ select the **Configuration > Statistics > Log Statistics** menu item.

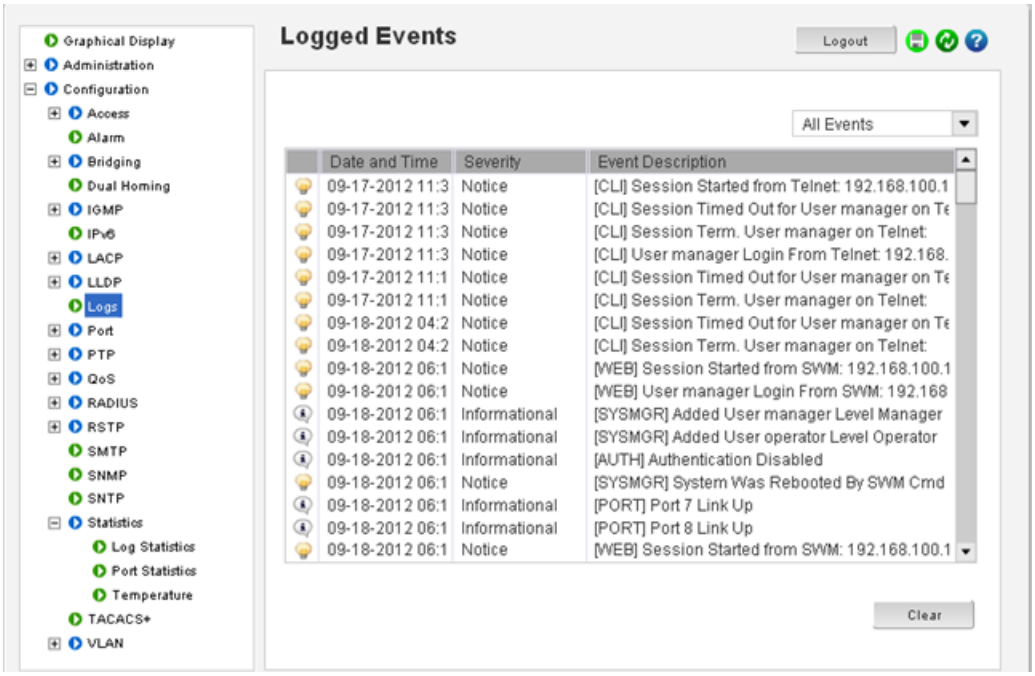


The **Log Statistics** window displays the logged events received – most logs are typically informational and activity.

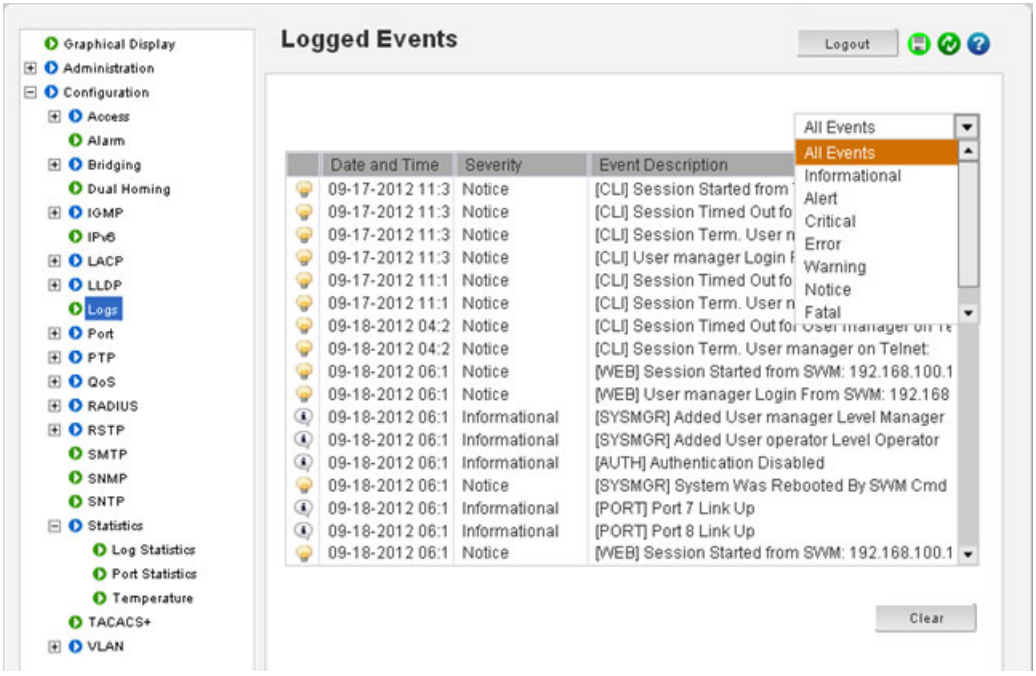
The log buffer size can be controlled through this menu.

For viewing each specific log,

▷ Select the **Configuration > Logs** menu item.



Each specific type of log can be viewed by using the drop down menu as shown below. In this example only informational logs are displayed.



The Clear button clears all the logs. To prevent accidental erasures, you will be prompted again if the logs should be deleted.

The Event Log records operating events as single-line entries listed in chronological order. For details on event log records, refer to *Description* on page 19–313.

19.9 Command Reference

19.9.1 Main Commands

The main commands can be categorized as show commands, set commands, and context-less commands. The show commands are listed below.

- `show active-snmp`: displays currently active SNMP support
- `show active-stp`: displays currently active STP
- `show active-vlan`: displays currently active VLAN
- `show address-table`: displays address table parameters
- `show age`: displays the address table age limit
- `show arp`: displays the arp details
- `show auth` <config|ports>
- `show backpressure`
- `show bootmode`: displays the current bootmode value
- `show broadcast-protect`: displays broadcast storm protection parameters
- `show config`: displays the saved configuration as a whole or by module
- `show console`: displays console serial link settings
- `show date`: displays system date
- `show daylight`: displays the configured daylight savings settings
- `show dualhome`
- `show flowcontrol`
- `show fans`
- `show hwrev`
- `show ftp`
- `show gateway`: displays the gateway of the system
- `show gvrp`: displays the GVRP parameters
- `show host`: displays the host table for FTP users
- `show igmp`: displays the IGMP parameters
- `show interfaces`: display the interface information
- `show ip`: displays the system IP address
- `show ip-access`: displays the IP address access list
- `show ipconfig`: displays the IP configuration
- `show lacp`
- `show lldp`
- `show log`: displays log information
- `show logsize`: displays the current event log size
- `show mac`: displays the system MAC address
- `show modbus`: displays Modbus settings
- `show modules`: displays the module information
- `show port`: displays the port information

- `show port-mirror`: displays the port mirroring parameters
- `show port-security`: displays the port security configuration parameters
- `show power`: displays condition of power supplies, in redundant power supply switches only
- `show qos`: displays the QOS settings
- `show rmon`: displays the rmon configuration parameters
- `show setup`: displays the setup parameters of the system
- `show smtp`: displays e-mail (SMTP) alert information
- `show snmp`: displays information related to SNMP
- `show sntp`: displays the configured SNTP servers details
- `show stats`: displays the port statistics
- `show stp`: displays Spanning Tree Bridge parameters
- `show subnet`: displays the Subnet Mask of the system
- `show ssl`
- `show sysconfig`: displays system configurable parameters
- `show syscontact`: displays the current system contact
- `show syslocation`: displays the current system location
- `show sysname`: displays the current system name
- `show time`: displays the system time
- `show timeout`: displays the system inactivity time out
- `show timezone`: displays the configured time zone of the device
- `show uptime`: displays up time of the system
- `show users`: displays all configured users
- `show version`: displays current version of the software
- `show vlan`: displays the VLAN parameters of a specified type
- `show web`

The set commands are listed below.

- `set bootmode`
- `set date year`
- `set daylight country`
- `set prompt`
- `set logsize`
- `set password`: sets the current user password
- `set snmp`
- `set stp`
- `set time`
- `set timeformat`
- `set timeout`: sets the system inactivity time out
- `set timezone`
- `set vlan`: sets the VLAN type

The context-less commands are listed below.

- clear: clears the event log, command history, or screen
- climode: to set the interactive CLI mode
- enable: allows to login as another user
- help
- more: to set more pipe in screen outputs
- save
- whoami: display the user information
- reboot
- authorize
- degrade
- exportlog mode
- ftp
- help
- ipconfig
- kill
- kill session id
- logout: logs out from the current user
- ping: to send the ping requests
- tftp
- telnet: connects to the remote system through telnet
- terminal: to set the terminal size
- xmodem

19.9.2 Configuration commands

The access commands are shown below.

- allow: allows the IP address
- deny: denies the IP address
- modbus: enables or disables access to Modbus map
- remove
- removeall
- snmp: enables or disables SNMP
- ssl
- sslv
- telnet
- web

The alarm commands are shown below. Refer to *Alarm Relays* on page 19–299 for details on using these commands.

- add
- alarm
- del

- period

The authorization commands are shown below.

- auth
- authserver
- backend
- clear-stats
- portaccess
- reauth
- setport
- show-port
- show-stats
- trigger-reauth
- user auth

The device commands are shown below.

- device
- backpressure
- broadcast-protect: enables or disables broadcast storm protection globally
- flowcontrol
- rate-time
- rate-threshold: sets the broadcast rate threshold (frames/sec)
- setage: sets the mgtagetime
- setport: sets the port configuration

The VLAN registration over GARP (GVRP) commands are shown below. Refer to *Configuring GVRP through the Command Line Interface* on page 11–194 for details.

- gvrp
- help gvrp: configures GVRP parameters for dynamic VLAN
- set-forbid: sets forbidden ports for a tag-based VLAN
- show-ports: show ports current GVRP state
- show-forbid: show forbidden ports for tag-based VLAN
- set-ports: set GVRP port state usage
- show-vlan: shows dynamic/static tag-based VLANs
- static: convert dynamic VLAN to static VLAN

The IGMP commands are shown below. Refer to *Commands* on page 15–254 for additional details.

- group
- igmp
- mode
- mcast
- set-leave: enables or disables IGMP immediate leave status
- set-port: sets the port mode
- set-qi: sets the query interval (60 to 127) for router ports

- `set-qri`
- `set-querier`: enables or disables switch as querier
- `show-group`: displays IGMP group list
- `show-port`: displays IGMP port mode
- `show-router`: displays IGMP router list

The Link Aggregation Control Protocol (LACP) commands are shown below.

- `lacp`
- `add port`
- `del port`
- `edit port`

The port mirroring commands are shown below. Refer to *Port Mirroring* on page 9–149 for additional details.

- `help port-mirror`
- `prtmr`: enables/disables port mirroring functionality
- `setport`: defines the port mirroring ports

The port security commands are shown below. Refer to *Securing Access* on page 6–109 for additional details.

- `action`: sets the action type of secured port
- `allow`: allows MAC addressing per port
- `help port-security`
- `learn`: enables/disables security for a single port or group of ports
- `ps`: enables/disables security in system
- `remove`: removes MAC addressing per port
- `signal`: sets the signal type of the secured port

The quality of service (QoS) commands are shown below. Refer to *Commands* on page 14–238 for additional details.

- `map`
- `setpoint`
- `help qos`
- `setqos`: configures QOS configuration usage
- `set-untag`
- `set-weight`: sets the port priority weights for all the ports in all the device
- `show-portweight`: displays the current port weight priority

The remote monitoring (RMON) commands are shown below. Refer to *Configuring RMON* on page 16–275 for additional details.

- `alarm`: sets the owner for the alarm group
- `event`: sets the owner for the event group
- `help rmon`
- `history`: sets the owner for the history group
- `statistics`: sets the owner for the statistics group

The Rapid Spanning Tree Protocol (RSTP) commands are shown below. Refer to *Configuring RSTP through the Command Line Interface* on page 13–212 for additional details.

- `cost`: sets the path cost of ports
- `forceversion`: set the force version of STP
- `help rstp`
- `port`: sets the RSTP administration status of ports
- `priority`: changes the priority of ports or bridge
- `rstp`: changes the RSTP administrative status of the bridge
- `show-forceversion`: shows the current force version of RSTP
- `show-mode`: shows the port mode status
- `show-timers`: shows the bridge time parameters
- `timers`: changes the bridge time parameters

The Simple Mail Transfer Protocol (SMTP) commands for e-mail are shown below. Refer to *E-mail* on page 19–304 for additional details.

- `add`: adds a recipient
- `delete`: deletes a recipient
- `help smtp`
- `sendmail`: sends e-mail
- `server`: sets the global SMTP server configuration
- `smtp`: enables/disables SMTP e-mail alert

The Simple Network Management Protocol (SNMP) commands are shown below. Refer to *Configuring SNMP through the Command Line Interface* on page 16–264 for additional details.

- `authentraps`: enable/disables the authentication traps
- `community`: configures SNMP community names
- `help snmp`
- `mgrip`: adds or deletes the SNMP manager IP
- `setvar`: configures system name, contact, or location
- `traps`: adds or deletes a trap receiver

The Simple Network Time Protocol (SNTP) commands are shown below. Refer to *Network Time* on page 5–84 for additional details.

- `delete`: deletes the SNTP server from SNTP server database
- `help sntp`
- `setsntp`: adds SNTP server into the SNTP server database
- `sntp`: configures parameters for SNTP system
- `sync`: sets the interval for synchronization time with an NTP server

The Spanning Tree Protocol (STP) commands are shown below. Refer to *Spanning Tree Protocol (STP)* on page 12–197 for additional details.

- `cost`
- `port`
- `priority`
- `stp`
- `timers`

The user commands are shown below. Refer to the *User Management* on page 1–29 for additional details.

- `add`: adds a new user
- `chlevel`: changes the user access permissions
- `delete`: deletes an existing user
- `help user`
- `passwd`: change the user password
- `tacplus`
- `tacserver`
- `userauthorder`

The VLAN commands are shown below. Refer to *VLAN* on page 10–167 for additional details.

- `add`
- `delete`
- `edit`
- `save`
- `set-egress`
- `set-ingress`
- `set-port`
- `show-egress`
- `show-ingress`
- `show-port`
- `start`
- `stop`
- `vlan`

Multilink ML3000/ML3100

Chapter 20: Modbus Protocol

20.1 Modbus Configuration

20.1.1 Overview

Modicon programmable controllers as well as other PLCs can communicate with each other and other devices over a variety of networks. The common language used by all Modicon controllers is the Modbus protocol. This protocol defines a message structure that controllers recognize and use regardless of the networks over which they communicate. It describes the process a controller uses to request access to another device, how it will respond to requests from the other devices, and how errors will be detected and reported. It establishes a common format for the layout and contents of message fields. The Modbus protocol thus operates at the layer 7 of the OSI 7 layer stack. Additional information on Modbus can be found at http://www.modbus.org and other related sites.

RFC 1122 Requirements for Internet Hosts - Communication Layers defines how Modbus packets can be carried over a TCP/IP transport and how Modicon controllers or other PLC devices can communicate over a TCP/IP network. To facilitate this communications, the GE Multilink switches allow Modbus connectivity.

As per this RFC, Modbus communications take place on TCP port 502. Please make sure the network security devices do not block port 502. If port 502 is blocked, which is the normal case with many firewall and other security devices, the communications between two Modbus devices over a TCP/IP network will not succeed.

20.1.2 Command Line Interface Settings

The following command-line interface settings are available:

modbus *<enable|disable>*

modbus *port=<port|default>*

modbus *device=<device|default>*

show modbus

The commands enable the Modbus protocol and set the relevant Modbus slave address and communication port values.

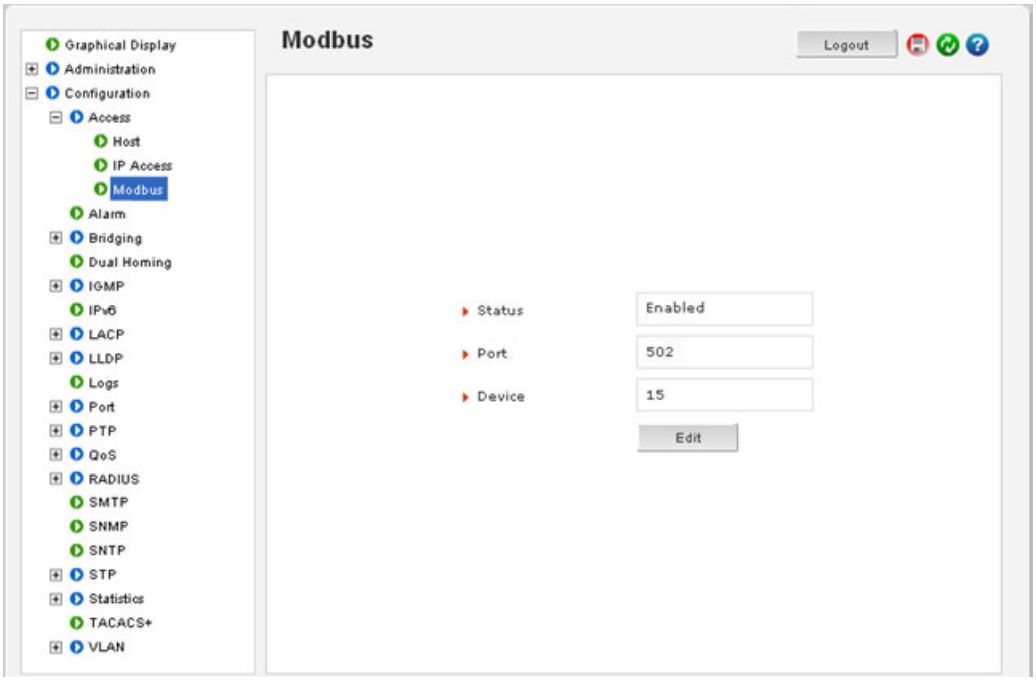
For example,

```
ML3000# show ipconfig

 IP Address:     192.168.1.5
 Subnet Mask:    255.255.255.0
 Default Gateway: 192.168.1.10

ML3000# show modbus

 Access to Modbus disabaled
 Modbus is Using Port: 502
 Modbus is Using Device: 5

ML3000# access

ML3000(access)## modbus enable

 Enabling Access to Modbus

ML3000(access)## show modbus

 Access to Modbus enabled
 Modbus is Using Port: 502
 Modbus is Using Device: 5

ML3000(access)## modbus port=602

 Modbus Port is set

ML3000(access)## show modbus

 Access to Modbus enabled
 Modbus is Using Port: 602
 Modbus is Using Device: 5

ML3000(access)## modbus port=default

 Modbus Port Set to Default

ML3000(access)## show modbus

 Access to Modbus enabled
 Modbus is Using Port :502
 Modbus is Using Device :5
```

20.1.3 EnerVista Settings

To modify the Modbus settings through EnerVista Secure Web Management software,

▷ Select the **Configuration > Access > Modbus** menu item.


Graphical Display
Administration
Configuration
Access
Host
IP Access
Modbus
Alarm
Bridging
Dual Homing
IGMP
IPv6
LACP
LLDP
Logs
Port
PTP
QoS
RADIUS
SMTP
SNMP
SNTP
STP
Statistics
TACACS+
VLAN
Modbus
Logout
Status
Enabled
Port
502
Device
15
Edit

20.2 Memory Mapping

20.2.1 Modbus Memory Map

The Modbus memory map is shown below. Refer to *Format Codes* on page 20–365 for details on the items in the format column.

Table 20–1: Modbus memory map (Sheet 1 of 40)

Address	Description	Range	Step	Format	Default
0000	System name (12 registers)	-	-	String	Varies
000C	System contact (12 registers)	-	-	String	multilin.tech @ge.com
0018	System location (12 registers)	-	-	String	Markham, Ontario
0024	Software version (6 registers)	-	-	String	Varies
002A	IP address (byte 0)	1 to 254	1	F1	0
002B	IP address (byte 1)	1 to 254	1	F1	0
002C	IP address (byte 2)	1 to 254	1	F1	0
002D	IP address (byte 3)	1 to 254	1	F1	0
002E	Netmask (byte 0)	1 to 254	1	F1	0
002F	Netmask (byte 1)	1 to 254	1	F1	0
0030	Netmask (byte 2)	1 to 254	1	F1	0
0031	Netmask (byte 3)	1 to 254	1	F1	0
0032	Gateway (byte 0)	1 to 254	1	F1	0
0033	Gateway (byte 1)	1 to 254	1	F1	0
0034	Gateway (byte 2)	1 to 254	1	F1	0
0035	Gateway (byte 3)	1 to 254	1	F1	0
0036	MAC address (3 registers)	-	-	String	Varies
0039	Order code (16 registers)	-	-	String	Varies
0049	Power alarm 1	0 to 1	1	F2	0
004A	Power alarm 2	0 to 1	1	F2	0
004B	Stp State	0 to 1	1	F3	0
004C	Number of ports	1 to 32	1	F1	Varies
004E	Port present map	-	-	Bitmap	Varies
0050	Port link map	-	-	Bitmap	0
0052	Port stp state map	-	-	Bitmap	0
0054	Port activity map	-	-	Bitmap	0
0056	Port 1 type	0 to 6	1	F4	Varies
0057	Port 2 type	0 to 6	1	F4	Varies
0058	Port 3 type	0 to 6	1	F4	Varies
0059	Port 4 type	0 to 6	1	F4	Varies
005A	Port 5 type	0 to 6	1	F4	Varies
005B	Port 6 type	0 to 6	1	F4	Varies
005C	Port 7 type	0 to 6	1	F4	Varies
005D	Port 8 type	0 to 6	1	F4	Varies
005E	Port 9 type	0 to 6	1	F4	Varies
005F	Port 10 type	0 to 6	1	F4	Varies
0060	Port 11 type	0 to 6	1	F4	Varies
0061	Port 12 type	0 to 6	1	F4	Varies

Table 20–1: Modbus memory map (Sheet 2 of 40)

Address	Description	Range	Step	Format	Default
0062	Port 13 type	0 to 6	1	F4	Varies
0063	Port 14 type	0 to 6	1	F4	Varies
0064	Port 15 type	0 to 6	1	F4	Varies
0065	Port 16 type	0 to 6	1	F4	Varies
0066	Port 17 type	0 to 6	1	F4	Varies
0067	Port 18 type	0 to 6	1	F4	Varies
0068	Port 19 type	0 to 6	1	F4	Varies
0069	Port 20 type	0 to 6	1	F4	Varies
006A	Port 21 type	0 to 6	1	F4	Varies
006B	Port 22 type	0 to 6	1	F4	Varies
006C	Port 23 type	0 to 6	1	F4	Varies
006D	Port 24 type	0 to 6	1	F4	Varies
006E	Port 25 type	0 to 6	1	F4	Varies
006F	Port 26 type	0 to 6	1	F4	Varies
0070	Port 27 type	0 to 6	1	F4	Varies
0071	Port 28 type	0 to 6	1	F4	Varies
0072	Port 29 type	0 to 6	1	F4	Varies
0073	Port 30 type	0 to 6	1	F4	Varies
0074	Port 31 type	0 to 6	1	F4	Varies
0075	Port 32 type	0 to 6	1	F4	Varies
0076	Port 1 link status	0 to 1	1	F3	0
0077	Port 2 link status	0 to 1	1	F3	0
0078	Port 3 link status	0 to 1	1	F3	0
0079	Port 4 link status	0 to 1	1	F3	0
007A	Port 5 link status	0 to 1	1	F3	0
007B	Port 6 link status	0 to 1	1	F3	0
007C	Port 7 link status	0 to 1	1	F3	0
007D	Port 8 link status	0 to 1	1	F3	0
007E	Port 9 link status	0 to 1	1	F3	0
007F	Port 10 link status	0 to 1	1	F3	0
0080	Port 11 link status	0 to 1	1	F3	0
0081	Port 12 link status	0 to 1	1	F3	0
0082	Port 13 link status	0 to 1	1	F3	0
0083	Port 14 link status	0 to 1	1	F3	0
0084	Port 15 link status	0 to 1	1	F3	0
0085	Port 16 link status	0 to 1	1	F3	0
0086	Port 17 link status	0 to 1	1	F3	0
0087	Port 18 link status	0 to 1	1	F3	0
0088	Port 19 link status	0 to 1	1	F3	0
0089	Port 20 link status	0 to 1	1	F3	0
008A	Port 21 link status	0 to 1	1	F3	0
008B	Port 22 link status	0 to 1	1	F3	0
008C	Port 23 link status	0 to 1	1	F3	0
008D	Port 24 link status	0 to 1	1	F3	0
008E	Port 25 link status	0 to 1	1	F3	0
008F	Port 26 link status	0 to 1	1	F3	0

Table 20–1: Modbus memory map (Sheet 3 of 40)

Address	Description	Range	Step	Format	Default
0090	Port 27 link status	0 to 1	1	F3	0
0091	Port 28 link status	0 to 1	1	F3	0
0092	Port 29 link status	0 to 1	1	F3	0
0093	Port 30 link status	0 to 1	1	F3	0
0094	Port 31 link status	0 to 1	1	F3	0
0095	Port 32 link status	0 to 1	1	F3	0
0096	Port 1 STP state	0 to 1	1	F3	0
0097	Port 2 STP state	0 to 1	1	F3	0
0098	Port 3 STP state	0 to 1	1	F3	0
0099	Port 4 STP state	0 to 1	1	F3	0
009A	Port 5 STP state	0 to 1	1	F3	0
009B	Port 6 STP state	0 to 1	1	F3	0
009C	Port 7 STP state	0 to 1	1	F3	0
009D	Port 8 STP state	0 to 1	1	F3	0
009E	Port 9 STP state	0 to 1	1	F3	0
009F	Port 10 STP state	0 to 1	1	F3	0
00A0	Port 11 STP state	0 to 1	1	F3	0
00A1	Port 12 STP state	0 to 1	1	F3	0
00A2	Port 13 STP state	0 to 1	1	F3	0
00A3	Port 14 STP state	0 to 1	1	F3	0
00A4	Port 15 STP state	0 to 1	1	F3	0
00A5	Port 16 STP state	0 to 1	1	F3	0
00A6	Port 17 STP state	0 to 1	1	F3	0
00A7	Port 18 STP state	0 to 1	1	F3	0
00A8	Port 19 STP state	0 to 1	1	F3	0
00A9	Port 20 STP state	0 to 1	1	F3	0
00AA	Port 21 STP state	0 to 1	1	F3	0
00AB	Port 22 STP state	0 to 1	1	F3	0
00AC	Port 23 STP state	0 to 1	1	F3	0
00AD	Port 24 STP state	0 to 1	1	F3	0
00AE	Port 25 STP state	0 to 1	1	F3	0
00AF	Port 26 STP state	0 to 1	1	F3	0
00B0	Port 27 STP state	0 to 1	1	F3	0
00B1	Port 28 STP state	0 to 1	1	F3	0
00B2	Port 29 STP state	0 to 1	1	F3	0
00B3	Port 30 STP state	0 to 1	1	F3	0
00B4	Port 31 STP state	0 to 1	1	F3	0
00B5	Port 32 STP state	0 to 1	1	F3	0
00B6	Port 1 activity	0 to 1	1	F3	0
00B7	Port 2 activity	0 to 1	1	F3	0
00B8	Port 3 activity	0 to 1	1	F3	0
00B9	Port 4 activity	0 to 1	1	F3	0
00BA	Port 5 activity	0 to 1	1	F3	0
00BB	Port 6 activity	0 to 1	1	F3	0
00BC	Port 7 activity	0 to 1	1	F3	0
00BD	Port 8 activity	0 to 1	1	F3	0

Table 20–1: Modbus memory map (Sheet 4 of 40)

Address	Description	Range	Step	Format	Default
00BE	Port 9 activity	0 to 1	1	F3	0
00BF	Port 10 activity	0 to 1	1	F3	0
00C0	Port 11 activity	0 to 1	1	F3	0
00C1	Port 12 activity	0 to 1	1	F3	0
00C2	Port 13 activity	0 to 1	1	F3	0
00C3	Port 14 activity	0 to 1	1	F3	0
00C4	Port 15 activity	0 to 1	1	F3	0
00C5	Port 16 activity	0 to 1	1	F3	0
00C6	Port 17 activity	0 to 1	1	F3	0
00C7	Port 18 activity	0 to 1	1	F3	0
00C8	Port 19 activity	0 to 1	1	F3	0
00C9	Port 20 activity	0 to 1	1	F3	0
00CA	Port 21 activity	0 to 1	1	F3	0
00CB	Port 22 activity	0 to 1	1	F3	0
00CC	Port 23 activity	0 to 1	1	F3	0
00CD	Port 24 activity	0 to 1	1	F3	0
00CE	Port 25 activity	0 to 1	1	F3	0
00CF	Port 26 activity	0 to 1	1	F3	0
00D0	Port 27 activity	0 to 1	1	F3	0
00D1	Port 28 activity	0 to 1	1	F3	0
00D2	Port 29 activity	0 to 1	1	F3	0
00D3	Port 30 activity	0 to 1	1	F3	0
00D4	Port 31 activity	0 to 1	1	F3	0
00D5	Port 32 activity	0 to 1	1	F3	0
00D6	Port 1: Number of bytes received	0 to 4294967295	1	F9	0
00D8	Port 1: Number of bytes sent	0 to 4294967295	1	F9	0
00DA	Port 1: Number of frames received	0 to 4294967295	1	F9	0
00DC	Port 1: Number of frames sent	0 to 4294967295	1	F9	0
00DE	Port 1: Total bytes received	0 to 4294967295	1	F9	0
00E0	Port 1: Total frames received	0 to 4294967295	1	F9	0
00E2	Port 1: Number of broadcast frames received	0 to 4294967295	1	F9	0
00E4	Port 1: Number of multicast frames received	0 to 4294967295	1	F9	0
00E6	Port 1: Number of frames with CRC error	0 to 4294967295	1	F9	0
00E8	Port 1: Number of oversized frames received	0 to 4294967295	1	F9	0
00EA	Port 1: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
00EC	Port 1: Number of jabber frames received	0 to 4294967295	1	F9	0
00EE	Port 1: Number of collisions occurred	0 to 4294967295	1	F9	0
00F0	Port 1: Number of late collisions occurred	0 to 4294967295	1	F9	0
00F2	Port 1: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
00F4	Port 1: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
00F6	Port 1: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
00F8	Port 1: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
00FA	Port 1: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
00FC	Port 1: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
00FE	Port 1: Number of MAC error packets	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 5 of 40)

Address	Description	Range	Step	Format	Default
0100	Port 1: Number of dropped received packets	0 to 4294967295	1	F9	0
0102	Port 1: Number of multicast frames sent	0 to 4294967295	1	F9	0
0104	Port 1: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0106	Port 1: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0108	Port 2: Number of bytes received	0 to 4294967295	1	F9	0
010A	Port 2: Number of bytes sent	0 to 4294967295	1	F9	0
010C	Port 2: Number of frames received	0 to 4294967295	1	F9	0
010E	Port 2: Number of frames sent	0 to 4294967295	1	F9	0
0110	Port 2: Total bytes received	0 to 4294967295	1	F9	0
0112	Port 2: Total frames received	0 to 4294967295	1	F9	0
0114	Port 2: Number of broadcast frames received	0 to 4294967295	1	F9	0
0116	Port 2: Number of multicast frames received	0 to 4294967295	1	F9	0
0118	Port 2: Number of frames with CRC error	0 to 4294967295	1	F9	0
011A	Port 2: Number of oversized frames received	0 to 4294967295	1	F9	0
011C	Port 2: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
011E	Port 2: Number of jabber frames received	0 to 4294967295	1	F9	0
0120	Port 2: Number of collisions occurred	0 to 4294967295	1	F9	0
0122	Port 2: Number of late collisions occurred	0 to 4294967295	1	F9	0
0124	Port 2: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0126	Port 2: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0128	Port 2: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
012A	Port 2: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
012C	Port 2: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
012E	Port 2: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0130	Port 2: Number of MAC error packets	0 to 4294967295	1	F9	0
0132	Port 2: Number of dropped received packets	0 to 4294967295	1	F9	0
0134	Port 2: Number of multicast frames sent	0 to 4294967295	1	F9	0
0136	Port 2: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0138	Port 2: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
013A	Port 3: Number of bytes received	0 to 4294967295	1	F9	0
013C	Port 3: Number of bytes sent	0 to 4294967295	1	F9	0
013E	Port 3: Number of frames received	0 to 4294967295	1	F9	0
0140	Port 3: Number of frames sent	0 to 4294967295	1	F9	0
0142	Port 3: Total bytes received	0 to 4294967295	1	F9	0
0144	Port 3: Total frames received	0 to 4294967295	1	F9	0
0146	Port 3: Number of broadcast frames received	0 to 4294967295	1	F9	0
0148	Port 3: Number of multicast frames received	0 to 4294967295	1	F9	0
014A	Port 3: Number of frames with CRC error	0 to 4294967295	1	F9	0
014C	Port 3: Number of oversized frames received	0 to 4294967295	1	F9	0
014E	Port 3: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0150	Port 3: Number of jabber frames received	0 to 4294967295	1	F9	0
0152	Port 3: Number of collisions occurred	0 to 4294967295	1	F9	0
0154	Port 3: Number of late collisions occurred	0 to 4294967295	1	F9	0
0156	Port 3: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0158	Port 3: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 6 of 40)

Address	Description	Range	Step	Format	Default
015A	Port 3: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
015C	Port 3: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
015E	Port 3: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0160	Port 3: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0162	Port 3: Number of MAC error packets	0 to 4294967295	1	F9	0
0164	Port 3: Number of dropped received packets	0 to 4294967295	1	F9	0
0166	Port 3: Number of multicast frames sent	0 to 4294967295	1	F9	0
0168	Port 3: Number of broadcast frames sent	0 to 4294967295	1	F9	0
016A	Port 3: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
016C	Port 4: Number of bytes received	0 to 4294967295	1	F9	0
016E	Port 4: Number of bytes sent	0 to 4294967295	1	F9	0
0170	Port 4: Number of frames received	0 to 4294967295	1	F9	0
0172	Port 4: Number of frames sent	0 to 4294967295	1	F9	0
0174	Port 4: Total bytes received	0 to 4294967295	1	F9	0
0176	Port 4: Total frames received	0 to 4294967295	1	F9	0
0178	Port 4: Number of broadcast frames received	0 to 4294967295	1	F9	0
017A	Port 4: Number of multicast frames received	0 to 4294967295	1	F9	0
017C	Port 4: Number of frames with CRC error	0 to 4294967295	1	F9	0
017E	Port 4: Number of oversized frames received	0 to 4294967295	1	F9	0
0180	Port 4: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0182	Port 4: Number of jabber frames received	0 to 4294967295	1	F9	0
0184	Port 4: Number of collisions occurred	0 to 4294967295	1	F9	0
0186	Port 4: Number of late collisions occurred	0 to 4294967295	1	F9	0
0188	Port 4: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
018A	Port 4: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
018C	Port 4: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
018E	Port 4: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0190	Port 4: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0192	Port 4: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0194	Port 4: Number of MAC error packets	0 to 4294967295	1	F9	0
0196	Port 4: Number of dropped received packets	0 to 4294967295	1	F9	0
0198	Port 4: Number of multicast frames sent	0 to 4294967295	1	F9	0
019A	Port 4: Number of broadcast frames sent	0 to 4294967295	1	F9	0
019C	Port 4: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
019E	Port 5: Number of bytes received	0 to 4294967295	1	F9	0
01A0	Port 5: Number of bytes sent	0 to 4294967295	1	F9	0
01A2	Port 5: Number of frames received	0 to 4294967295	1	F9	0
01A4	Port 5: Number of frames sent	0 to 4294967295	1	F9	0
01A6	Port 5: Total bytes received	0 to 4294967295	1	F9	0
01A8	Port 5: Total frames received	0 to 4294967295	1	F9	0
01AA	Port 5: Number of broadcast frames received	0 to 4294967295	1	F9	0
01AC	Port 5: Number of multicast frames received	0 to 4294967295	1	F9	0
01AE	Port 5: Number of frames with CRC error	0 to 4294967295	1	F9	0
01B0	Port 5: Number of oversized frames received	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 7 of 40)

Address	Description	Range	Step	Format	Default
01B2	Port 5: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
01B4	Port 5: Number of jabber frames received	0 to 4294967295	1	F9	0
01B6	Port 5: Number of collisions occurred	0 to 4294967295	1	F9	0
01B8	Port 5: Number of late collisions occurred	0 to 4294967295	1	F9	0
01BA	Port 5: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
01BC	Port 5: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
01BE	Port 5: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
01C0	Port 5: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
01C2	Port 5: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
01C4	Port 5: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
01C6	Port 5: Number of MAC error packets	0 to 4294967295	1	F9	0
01C8	Port 5: Number of dropped received packets	0 to 4294967295	1	F9	0
01CA	Port 5: Number of multicast frames sent	0 to 4294967295	1	F9	0
01CC	Port 5: Number of broadcast frames sent	0 to 4294967295	1	F9	0
01CE	Port 5: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
01D0	Port 6: Number of bytes received	0 to 4294967295	1	F9	0
01D2	Port 6: Number of bytes sent	0 to 4294967295	1	F9	0
01D4	Port 6: Number of frames received	0 to 4294967295	1	F9	0
01D6	Port 6: Number of frames sent	0 to 4294967295	1	F9	0
01D8	Port 6: Total bytes received	0 to 4294967295	1	F9	0
01DA	Port 6: Total frames received	0 to 4294967295	1	F9	0
01DC	Port 6: Number of broadcast frames received	0 to 4294967295	1	F9	0
01DE	Port 6: Number of multicast frames received	0 to 4294967295	1	F9	0
01E0	Port 6: Number of frames with CRC error	0 to 4294967295	1	F9	0
01E2	Port 6: Number of oversized frames received	0 to 4294967295	1	F9	0
01E4	Port 6: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
01E6	Port 6: Number of jabber frames received	0 to 4294967295	1	F9	0
01E8	Port 6: Number of collisions occurred	0 to 4294967295	1	F9	0
01EA	Port 6: Number of late collisions occurred	0 to 4294967295	1	F9	0
01EC	Port 6: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
01EE	Port 6: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
01F0	Port 6: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
01F2	Port 6: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
01F4	Port 6: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
01F6	Port 6: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
01F8	Port 6: Number of MAC error packets	0 to 4294967295	1	F9	0
01FA	Port 6: Number of dropped received packets	0 to 4294967295	1	F9	0
01FC	Port 6: Number of multicast frames sent	0 to 4294967295	1	F9	0
01FE	Port 6: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0200	Port 6: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0202	Port 7: Number of bytes received	0 to 4294967295	1	F9	0
0204	Port 7: Number of bytes sent	0 to 4294967295	1	F9	0
0206	Port 7: Number of frames received	0 to 4294967295	1	F9	0
0208	Port 7: Number of frames sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 8 of 40)

Address	Description	Range	Step	Format	Default
020A	Port 7: Total bytes received	0 to 4294967295	1	F9	0
020C	Port 7: Total frames received	0 to 4294967295	1	F9	0
020E	Port 7: Number of broadcast frames received	0 to 4294967295	1	F9	0
0210	Port 7: Number of multicast frames received	0 to 4294967295	1	F9	0
0212	Port 7: Number of frames with CRC error	0 to 4294967295	1	F9	0
0214	Port 7: Number of oversized frames received	0 to 4294967295	1	F9	0
0216	Port 7: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0218	Port 7: Number of jabber frames received	0 to 4294967295	1	F9	0
021A	Port 7: Number of collisions occurred	0 to 4294967295	1	F9	0
021C	Port 7: Number of late collisions occurred	0 to 4294967295	1	F9	0
021E	Port 7: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0220	Port 7: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0222	Port 7: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0224	Port 7: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0226	Port 7: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0228	Port 7: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
022A	Port 7: Number of MAC error packets	0 to 4294967295	1	F9	0
022C	Port 7: Number of dropped received packets	0 to 4294967295	1	F9	0
022E	Port 7: Number of multicast frames sent	0 to 4294967295	1	F9	0
0230	Port 7: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0232	Port 7: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0234	Port 8: Number of bytes received	0 to 4294967295	1	F9	0
0236	Port 8: Number of bytes sent	0 to 4294967295	1	F9	0
0238	Port 8: Number of frames received	0 to 4294967295	1	F9	0
023A	Port 8: Number of frames sent	0 to 4294967295	1	F9	0
023C	Port 8: Total bytes received	0 to 4294967295	1	F9	0
023E	Port 8: Total frames received	0 to 4294967295	1	F9	0
0240	Port 8: Number of broadcast frames received	0 to 4294967295	1	F9	0
0242	Port 8: Number of multicast frames received	0 to 4294967295	1	F9	0
0244	Port 8: Number of frames with CRC error	0 to 4294967295	1	F9	0
0246	Port 8: Number of oversized frames received	0 to 4294967295	1	F9	0
0248	Port 8: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
024A	Port 8: Number of jabber frames received	0 to 4294967295	1	F9	0
024C	Port 8: Number of collisions occurred	0 to 4294967295	1	F9	0
024E	Port 8: Number of late collisions occurred	0 to 4294967295	1	F9	0
0250	Port 8: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0252	Port 8: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0254	Port 8: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0256	Port 8: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0258	Port 8: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
025A	Port 8: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
025C	Port 8: Number of MAC error packets	0 to 4294967295	1	F9	0
025E	Port 8: Number of dropped received packets	0 to 4294967295	1	F9	0
0260	Port 8: Number of multicast frames sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 9 of 40)

Address	Description	Range	Step	Format	Default
0262	Port 8: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0264	Port 8: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0266	Port 9: Number of bytes received	0 to 4294967295	1	F9	0
0268	Port 9: Number of bytes sent	0 to 4294967295	1	F9	0
026A	Port 9: Number of frames received	0 to 4294967295	1	F9	0
026C	Port 9: Number of frames sent	0 to 4294967295	1	F9	0
026E	Port 9: Total bytes received	0 to 4294967295	1	F9	0
0270	Port 9: Total frames received	0 to 4294967295	1	F9	0
0272	Port 9: Number of broadcast frames received	0 to 4294967295	1	F9	0
0274	Port 9: Number of multicast frames received	0 to 4294967295	1	F9	0
0276	Port 9: Number of frames with CRC error	0 to 4294967295	1	F9	0
0278	Port 9: Number of oversized frames received	0 to 4294967295	1	F9	0
027A	Port 9: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
027C	Port 9: Number of jabber frames received	0 to 4294967295	1	F9	0
027E	Port 9: Number of collisions occurred	0 to 4294967295	1	F9	0
0280	Port 9: Number of late collisions occurred	0 to 4294967295	1	F9	0
0282	Port 9: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0284	Port 9: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0286	Port 9: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0288	Port 9: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
028A	Port 9: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
028C	Port 9: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
028E	Port 9: Number of MAC error packets	0 to 4294967295	1	F9	0
0290	Port 9: Number of dropped received packets	0 to 4294967295	1	F9	0
0292	Port 9: Number of multicast frames sent	0 to 4294967295	1	F9	0
0294	Port 9: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0296	Port 9: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0298	Port 10: Number of bytes received	0 to 4294967295	1	F9	0
029A	Port 10: Number of bytes sent	0 to 4294967295	1	F9	0
029C	Port 10: Number of frames received	0 to 4294967295	1	F9	0
029E	Port 10: Number of frames sent	0 to 4294967295	1	F9	0
02A0	Port 10: Total bytes received	0 to 4294967295	1	F9	0
02A2	Port 10: Total frames received	0 to 4294967295	1	F9	0
02A4	Port 10: Number of broadcast frames received	0 to 4294967295	1	F9	0
02A6	Port 10: Number of multicast frames received	0 to 4294967295	1	F9	0
02A8	Port 10: Number of frames with CRC error	0 to 4294967295	1	F9	0
02AA	Port 10: Number of oversized frames received	0 to 4294967295	1	F9	0
02AC	Port 10: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
02AE	Port 10: Number of jabber frames received	0 to 4294967295	1	F9	0
02B0	Port 10: Number of collisions occurred	0 to 4294967295	1	F9	0
02B2	Port 10: Number of late collisions occurred	0 to 4294967295	1	F9	0
02B4	Port 10: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
02B6	Port 10: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
02B8	Port 10: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
02BA	Port 10: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 10 of 40)

Address	Description	Range	Step	Format	Default
02BC	Port 10: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
02BE	Port 10: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
02C0	Port 10: Number of MAC error packets	0 to 4294967295	1	F9	0
02C2	Port 10: Number of dropped received packets	0 to 4294967295	1	F9	0
02C4	Port 10: Number of multicast frames sent	0 to 4294967295	1	F9	0
02C6	Port 10: Number of broadcast frames sent	0 to 4294967295	1	F9	0
02C8	Port 10: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
02CA	Port 11: Number of bytes received	0 to 4294967295	1	F9	0
02CC	Port 11: Number of bytes sent	0 to 4294967295	1	F9	0
02CE	Port 11: Number of frames received	0 to 4294967295	1	F9	0
02D0	Port 11: Number of frames sent	0 to 4294967295	1	F9	0
02D2	Port 11: Total bytes received	0 to 4294967295	1	F9	0
02D4	Port 11: Total frames received	0 to 4294967295	1	F9	0
02D6	Port 11: Number of broadcast frames received	0 to 4294967295	1	F9	0
02D8	Port 11: Number of multicast frames received	0 to 4294967295	1	F9	0
02DA	Port 11: Number of frames with CRC error	0 to 4294967295	1	F9	0
02DC	Port 11: Number of oversized frames received	0 to 4294967295	1	F9	0
02DE	Port 11: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
02E0	Port 11: Number of jabber frames received	0 to 4294967295	1	F9	0
02E2	Port 11: Number of collisions occurred	0 to 4294967295	1	F9	0
02E4	Port 11: Number of late collisions occurred	0 to 4294967295	1	F9	0
02E6	Port 11: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
02E8	Port 11: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
02EA	Port 11: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
02EC	Port 11: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
02EE	Port 11: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
02F0	Port 11: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
02F2	Port 11: Number of MAC error packets	0 to 4294967295	1	F9	0
02F4	Port 11: Number of dropped received packets	0 to 4294967295	1	F9	0
02F6	Port 11: Number of multicast frames sent	0 to 4294967295	1	F9	0
02F8	Port 11: Number of broadcast frames sent	0 to 4294967295	1	F9	0
02FA	Port 11: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
02FC	Port 12: Number of bytes received	0 to 4294967295	1	F9	0
02FE	Port 12: Number of bytes sent	0 to 4294967295	1	F9	0
0300	Port 12: Number of frames received	0 to 4294967295	1	F9	0
0302	Port 12: Number of frames sent	0 to 4294967295	1	F9	0
0304	Port 12: Total bytes received	0 to 4294967295	1	F9	0
0306	Port 12: Total frames received	0 to 4294967295	1	F9	0
0308	Port 12: Number of broadcast frames received	0 to 4294967295	1	F9	0
030A	Port 12: Number of multicast frames received	0 to 4294967295	1	F9	0
030C	Port 12: Number of frames with CRC error	0 to 4294967295	1	F9	0
030E	Port 12: Number of oversized frames received	0 to 4294967295	1	F9	0
0310	Port 12: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 11 of 40)

Address	Description	Range	Step	Format	Default
0312	Port 12: Number of jabber frames received	0 to 4294967295	1	F9	0
0314	Port 12: Number of collisions occurred	0 to 4294967295	1	F9	0
0316	Port 12: Number of late collisions occurred	0 to 4294967295	1	F9	0
0318	Port 12: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
031A	Port 12: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
031C	Port 12: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
031E	Port 12: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0320	Port 12: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
0322	Port 12: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0324	Port 12: Number of MAC error packets	0 to 4294967295	1	F9	0
0326	Port 12: Number of dropped received packets	0 to 4294967295	1	F9	0
0328	Port 12: Number of multicast frames sent	0 to 4294967295	1	F9	0
032A	Port 12: Number of broadcast frames sent	0 to 4294967295	1	F9	0
032C	Port 12: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
032E	Port 13: Number of bytes received	0 to 4294967295	1	F9	0
0330	Port 13: Number of bytes sent	0 to 4294967295	1	F9	0
0332	Port 13: Number of frames received	0 to 4294967295	1	F9	0
0334	Port 13: Number of frames sent	0 to 4294967295	1	F9	0
0336	Port 13: Total bytes received	0 to 4294967295	1	F9	0
0338	Port 13: Total frames received	0 to 4294967295	1	F9	0
033A	Port 13: Number of broadcast frames received	0 to 4294967295	1	F9	0
033C	Port 13: Number of multicast frames received	0 to 4294967295	1	F9	0
033E	Port 13: Number of frames with CRC error	0 to 4294967295	1	F9	0
0340	Port 13: Number of oversized frames received	0 to 4294967295	1	F9	0
0342	Port 13: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0344	Port 13: Number of jabber frames received	0 to 4294967295	1	F9	0
0346	Port 13: Number of collisions occurred	0 to 4294967295	1	F9	0
0348	Port 13: Number of late collisions occurred	0 to 4294967295	1	F9	0
034A	Port 13: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
034C	Port 13: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
034E	Port 13: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0350	Port 13: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0352	Port 13: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
0354	Port 13: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0356	Port 13: Number of MAC error packets	0 to 4294967295	1	F9	0
0358	Port 13: Number of dropped received packets	0 to 4294967295	1	F9	0
035A	Port 13: Number of multicast frames sent	0 to 4294967295	1	F9	0
035C	Port 13: Number of broadcast frames sent	0 to 4294967295	1	F9	0
035E	Port 13: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0360	Port 14: Number of bytes received	0 to 4294967295	1	F9	0
0362	Port 14: Number of bytes sent	0 to 4294967295	1	F9	0
0364	Port 14: Number of frames received	0 to 4294967295	1	F9	0
0366	Port 14: Number of frames sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 12 of 40)

Address	Description	Range	Step	Format	Default
0368	Port 14: Total bytes received	0 to 4294967295	1	F9	0
036A	Port 14: Total frames received	0 to 4294967295	1	F9	0
036C	Port 14: Number of broadcast frames received	0 to 4294967295	1	F9	0
036E	Port 14: Number of multicast frames received	0 to 4294967295	1	F9	0
0370	Port 14: Number of frames with CRC error	0 to 4294967295	1	F9	0
0372	Port 14: Number of oversized frames received	0 to 4294967295	1	F9	0
0374	Port 14: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0376	Port 14: Number of jabber frames received	0 to 4294967295	1	F9	0
0378	Port 14: Number of collisions occurred	0 to 4294967295	1	F9	0
037A	Port 14: Number of late collisions occurred	0 to 4294967295	1	F9	0
037C	Port 14: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
037E	Port 14: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0380	Port 14: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0382	Port 14: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0384	Port 14: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
0386	Port 14: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0388	Port 14: Number of MAC error packets	0 to 4294967295	1	F9	0
038A	Port 14: Number of dropped received packets	0 to 4294967295	1	F9	0
038C	Port 14: Number of multicast frames sent	0 to 4294967295	1	F9	0
038E	Port 14: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0390	Port 14: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0392	Port 15: Number of bytes received	0 to 4294967295	1	F9	0
0394	Port 15: Number of bytes sent	0 to 4294967295	1	F9	0
0396	Port 15: Number of frames received	0 to 4294967295	1	F9	0
0398	Port 15: Number of frames sent	0 to 4294967295	1	F9	0
039A	Port 15: Total bytes received	0 to 4294967295	1	F9	0
039C	Port 15: Total frames received	0 to 4294967295	1	F9	0
039E	Port 15: Number of broadcast frames received	0 to 4294967295	1	F9	0
03A0	Port 15: Number of multicast frames received	0 to 4294967295	1	F9	0
03A2	Port 15: Number of frames with CRC error	0 to 4294967295	1	F9	0
03A4	Port 15: Number of oversized frames received	0 to 4294967295	1	F9	0
03A6	Port 15: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
03A8	Port 15: Number of jabber frames received	0 to 4294967295	1	F9	0
03AA	Port 15: Number of collisions occurred	0 to 4294967295	1	F9	0
03AC	Port 15: Number of late collisions occurred	0 to 4294967295	1	F9	0
03AE	Port 15: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
03B0	Port 15: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
03B2	Port 15: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
03B4	Port 15: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
03B6	Port 15: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
03B8	Port 15: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
03BA	Port 15: Number of MAC error packets	0 to 4294967295	1	F9	0
03BC	Port 15: Number of dropped received packets	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 13 of 40)

Address	Description	Range	Step	Format	Default
03BE	Port 15: Number of multicast frames sent	0 to 4294967295	1	F9	0
03C0	Port 15: Number of broadcast frames sent	0 to 4294967295	1	F9	0
03C2	Port 15: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
03C4	Port 16: Number of bytes received	0 to 4294967295	1	F9	0
03C6	Port 16: Number of bytes sent	0 to 4294967295	1	F9	0
03C8	Port 16: Number of frames received	0 to 4294967295	1	F9	0
03CA	Port 16: Number of frames sent	0 to 4294967295	1	F9	0
03CC	Port 16: Total bytes received	0 to 4294967295	1	F9	0
03CE	Port 16: Total frames received	0 to 4294967295	1	F9	0
03D0	Port 16: Number of broadcast frames received	0 to 4294967295	1	F9	0
03D2	Port 16: Number of multicast frames received	0 to 4294967295	1	F9	0
03D4	Port 16: Number of frames with CRC error	0 to 4294967295	1	F9	0
03D6	Port 16: Number of oversized frames received	0 to 4294967295	1	F9	0
03D8	Port 16: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
03DA	Port 16: Number of jabber frames received	0 to 4294967295	1	F9	0
03DC	Port 16: Number of collisions occurred	0 to 4294967295	1	F9	0
03DE	Port 16: Number of late collisions occurred	0 to 4294967295	1	F9	0
03E0	Port 16: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
03E2	Port 16: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
03E4	Port 16: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
03E6	Port 16: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
03E8	Port 16: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
03EA	Port 16: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
03EC	Port 16: Number of MAC error packets	0 to 4294967295	1	F9	0
03EE	Port 16: Number of dropped received packets	0 to 4294967295	1	F9	0
03F0	Port 16: Number of multicast frames sent	0 to 4294967295	1	F9	0
03F2	Port 16: Number of broadcast frames sent	0 to 4294967295	1	F9	0
03F4	Port 16: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
03F6	Port 17: Number of bytes received	0 to 4294967295	1	F9	0
03F8	Port 17: Number of bytes sent	0 to 4294967295	1	F9	0
03FA	Port 17: Number of frames received	0 to 4294967295	1	F9	0
03FC	Port 17: Number of frames sent	0 to 4294967295	1	F9	0
03FE	Port 17: Total bytes received	0 to 4294967295	1	F9	0
0400	Port 17: Total frames received	0 to 4294967295	1	F9	0
0402	Port 17: Number of broadcast frames received	0 to 4294967295	1	F9	0
0404	Port 17: Number of multicast frames received	0 to 4294967295	1	F9	0
0406	Port 17: Number of frames with CRC error	0 to 4294967295	1	F9	0
0408	Port 17: Number of oversized frames received	0 to 4294967295	1	F9	0
040A	Port 17: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
040C	Port 17: Number of jabber frames received	0 to 4294967295	1	F9	0
040E	Port 17: Number of collisions occurred	0 to 4294967295	1	F9	0
0410	Port 17: Number of late collisions occurred	0 to 4294967295	1	F9	0
0412	Port 17: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0414	Port 17: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 14 of 40)

Address	Description	Range	Step	Format	Default
0416	Port 17: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0418	Port 17: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
041A	Port 17: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
041C	Port 17: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
041E	Port 17: Number of MAC error packets	0 to 4294967295	1	F9	0
0420	Port 17: Number of dropped received packets	0 to 4294967295	1	F9	0
0422	Port 17: Number of multicast frames sent	0 to 4294967295	1	F9	0
0424	Port 17: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0426	Port 17: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0428	Port 18: Number of bytes received	0 to 4294967295	1	F9	0
042A	Port 18: Number of bytes sent	0 to 4294967295	1	F9	0
042C	Port 18: Number of frames received	0 to 4294967295	1	F9	0
042E	Port 18: Number of frames sent	0 to 4294967295	1	F9	0
0430	Port 18: Total bytes received	0 to 4294967295	1	F9	0
0432	Port 18: Total frames received	0 to 4294967295	1	F9	0
0434	Port 18: Number of broadcast frames received	0 to 4294967295	1	F9	0
0436	Port 18: Number of multicast frames received	0 to 4294967295	1	F9	0
0438	Port 18: Number of frames with CRC error	0 to 4294967295	1	F9	0
043A	Port 18: Number of oversized frames received	0 to 4294967295	1	F9	0
043C	Port 18: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
043E	Port 18: Number of jabber frames received	0 to 4294967295	1	F9	0
0440	Port 18: Number of collisions occurred	0 to 4294967295	1	F9	0
0442	Port 18: Number of late collisions occurred	0 to 4294967295	1	F9	0
0444	Port 18: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0446	Port 18: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0448	Port 18: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
044A	Port 18: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
044C	Port 18: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
044E	Port 18: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0450	Port 18: Number of MAC error packets	0 to 4294967295	1	F9	0
0452	Port 18: Number of dropped received packets	0 to 4294967295	1	F9	0
0454	Port 18: Number of multicast frames sent	0 to 4294967295	1	F9	0
0456	Port 18: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0458	Port 18: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
045A	Port 19: Number of bytes received	0 to 4294967295	1	F9	0
045C	Port 19: Number of bytes sent	0 to 4294967295	1	F9	0
045E	Port 19: Number of frames received	0 to 4294967295	1	F9	0
0460	Port 19: Number of frames sent	0 to 4294967295	1	F9	0
0462	Port 19: Total bytes received	0 to 4294967295	1	F9	0
0464	Port 19: Total frames received	0 to 4294967295	1	F9	0
0466	Port 19: Number of broadcast frames received	0 to 4294967295	1	F9	0
0468	Port 19: Number of multicast frames received	0 to 4294967295	1	F9	0
046A	Port 19: Number of frames with CRC error	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 15 of 40)

Address	Description	Range	Step	Format	Default
046C	Port 19: Number of oversized frames received	0 to 4294967295	1	F9	0
046E	Port 19: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0470	Port 19: Number of jabber frames received	0 to 4294967295	1	F9	0
0472	Port 19: Number of collisions occurred	0 to 4294967295	1	F9	0
0474	Port 19: Number of late collisions occurred	0 to 4294967295	1	F9	0
0476	Port 19: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0478	Port 19: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
047A	Port 19: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
047C	Port 19: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
047E	Port 19: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
0480	Port 19: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0482	Port 19: Number of MAC error packets	0 to 4294967295	1	F9	0
0484	Port 19: Number of dropped received packets	0 to 4294967295	1	F9	0
0486	Port 19: Number of multicast frames sent	0 to 4294967295	1	F9	0
0488	Port 19: Number of broadcast frames sent	0 to 4294967295	1	F9	0
048A	Port 19: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
048C	Port 20: Number of bytes received	0 to 4294967295	1	F9	0
048E	Port 20: Number of bytes sent	0 to 4294967295	1	F9	0
0490	Port 20: Number of frames received	0 to 4294967295	1	F9	0
0492	Port 20: Number of frames sent	0 to 4294967295	1	F9	0
0494	Port 20: Total bytes received	0 to 4294967295	1	F9	0
0496	Port 20: Total frames received	0 to 4294967295	1	F9	0
0498	Port 20: Number of broadcast frames received	0 to 4294967295	1	F9	0
049A	Port 20: Number of multicast frames received	0 to 4294967295	1	F9	0
049C	Port 20: Number of frames with CRC error	0 to 4294967295	1	F9	0
049E	Port 20: Number of oversized frames received	0 to 4294967295	1	F9	0
04A0	Port 20: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
04A2	Port 20: Number of jabber frames received	0 to 4294967295	1	F9	0
04A4	Port 20: Number of collisions occurred	0 to 4294967295	1	F9	0
04A6	Port 20: Number of late collisions occurred	0 to 4294967295	1	F9	0
04A8	Port 20: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
04AA	Port 20: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
04AC	Port 20: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
04AE	Port 20: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
04B0	Port 20: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
04B2	Port 20: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
04B4	Port 20: Number of MAC error packets	0 to 4294967295	1	F9	0
04B6	Port 20: Number of dropped received packets	0 to 4294967295	1	F9	0
04B8	Port 20: Number of multicast frames sent	0 to 4294967295	1	F9	0
04BA	Port 20: Number of broadcast frames sent	0 to 4294967295	1	F9	0
04BC	Port 20: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
04BE	Port 21: Number of bytes received	0 to 4294967295	1	F9	0
04C0	Port 21: Number of bytes sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 16 of 40)

Address	Description	Range	Step	Format	Default
04C2	Port 21: Number of frames received	0 to 4294967295	1	F9	0
04C4	Port 21: Number of frames sent	0 to 4294967295	1	F9	0
04C6	Port 21: Total bytes received	0 to 4294967295	1	F9	0
04C8	Port 21: Total frames received	0 to 4294967295	1	F9	0
04CA	Port 21: Number of broadcast frames received	0 to 4294967295	1	F9	0
04CC	Port 21: Number of multicast frames received	0 to 4294967295	1	F9	0
04CE	Port 21: Number of frames with CRC error	0 to 4294967295	1	F9	0
04D0	Port 21: Number of oversized frames received	0 to 4294967295	1	F9	0
04D2	Port 21: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
04D4	Port 21: Number of jabber frames received	0 to 4294967295	1	F9	0
04D6	Port 21: Number of collisions occurred	0 to 4294967295	1	F9	0
04D8	Port 21: Number of late collisions occurred	0 to 4294967295	1	F9	0
04DA	Port 21: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
04DC	Port 21: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
04DE	Port 21: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
04E0	Port 21: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
04E2	Port 21: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
04E4	Port 21: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
04E6	Port 21: Number of MAC error packets	0 to 4294967295	1	F9	0
04E8	Port 21: Number of dropped received packets	0 to 4294967295	1	F9	0
04EA	Port 21: Number of multicast frames sent	0 to 4294967295	1	F9	0
04EC	Port 21: Number of broadcast frames sent	0 to 4294967295	1	F9	0
04EE	Port 21: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
04F0	Port 22: Number of bytes received	0 to 4294967295	1	F9	0
04F2	Port 22: Number of bytes sent	0 to 4294967295	1	F9	0
04F4	Port 22: Number of frames received	0 to 4294967295	1	F9	0
04F6	Port 22: Number of frames sent	0 to 4294967295	1	F9	0
04F8	Port 22: Total bytes received	0 to 4294967295	1	F9	0
04FA	Port 22: Total frames received	0 to 4294967295	1	F9	0
04FC	Port 22: Number of broadcast frames received	0 to 4294967295	1	F9	0
04FE	Port 22: Number of multicast frames received	0 to 4294967295	1	F9	0
0500	Port 22: Number of frames with CRC error	0 to 4294967295	1	F9	0
0502	Port 22: Number of oversized frames received	0 to 4294967295	1	F9	0
0504	Port 22: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0506	Port 22: Number of jabber frames received	0 to 4294967295	1	F9	0
0508	Port 22: Number of collisions occurred	0 to 4294967295	1	F9	0
050A	Port 22: Number of late collisions occurred	0 to 4294967295	1	F9	0
050C	Port 22: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
050E	Port 22: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0510	Port 22: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0512	Port 22: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0514	Port 22: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
0516	Port 22: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 17 of 40)

Address	Description	Range	Step	Format	Default
0518	Port 22: Number of MAC error packets	0 to 4294967295	1	F9	0
051A	Port 22: Number of dropped received packets	0 to 4294967295	1	F9	0
051C	Port 22: Number of multicast frames sent	0 to 4294967295	1	F9	0
051E	Port 22: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0520	Port 22: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0522	Port 23: Number of bytes received	0 to 4294967295	1	F9	0
0524	Port 23: Number of bytes sent	0 to 4294967295	1	F9	0
0526	Port 23: Number of frames received	0 to 4294967295	1	F9	0
0528	Port 23: Number of frames sent	0 to 4294967295	1	F9	0
052A	Port 23: Total bytes received	0 to 4294967295	1	F9	0
052C	Port 23: Total frames received	0 to 4294967295	1	F9	0
052E	Port 23: Number of broadcast frames received	0 to 4294967295	1	F9	0
0530	Port 23: Number of multicast frames received	0 to 4294967295	1	F9	0
0532	Port 23: Number of frames with CRC error	0 to 4294967295	1	F9	0
0534	Port 23: Number of oversized frames received	0 to 4294967295	1	F9	0
0536	Port 23: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0538	Port 23: Number of jabber frames received	0 to 4294967295	1	F9	0
053A	Port 23: Number of collisions occurred	0 to 4294967295	1	F9	0
053C	Port 23: Number of late collisions occurred	0 to 4294967295	1	F9	0
053E	Port 23: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0540	Port 23: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0542	Port 23: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0544	Port 23: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0546	Port 23: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
0548	Port 23: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
054A	Port 23: Number of MAC error packets	0 to 4294967295	1	F9	0
054C	Port 23: Number of dropped received packets	0 to 4294967295	1	F9	0
054E	Port 23: Number of multicast frames sent	0 to 4294967295	1	F9	0
0550	Port 23: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0552	Port 23: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0554	Port 24: Number of bytes received	0 to 4294967295	1	F9	0
0556	Port 24: Number of bytes sent	0 to 4294967295	1	F9	0
0558	Port 24: Number of frames received	0 to 4294967295	1	F9	0
055A	Port 24: Number of frames sent	0 to 4294967295	1	F9	0
055C	Port 24: Total bytes received	0 to 4294967295	1	F9	0
055E	Port 24: Total frames received	0 to 4294967295	1	F9	0
0560	Port 24: Number of broadcast frames received	0 to 4294967295	1	F9	0
0562	Port 24: Number of multicast frames received	0 to 4294967295	1	F9	0
0564	Port 24: Number of frames with CRC error	0 to 4294967295	1	F9	0
0566	Port 24: Number of oversized frames received	0 to 4294967295	1	F9	0
0568	Port 24: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
056A	Port 24: Number of jabber frames received	0 to 4294967295	1	F9	0
056C	Port 24: Number of collisions occurred	0 to 4294967295	1	F9	0
056E	Port 24: Number of late collisions occurred	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 18 of 40)

Address	Description	Range	Step	Format	Default
0570	Port 24: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0572	Port 24: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0574	Port 24: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0576	Port 24: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0578	Port 24: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
057A	Port 24: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
057C	Port 24: Number of MAC error packets	0 to 4294967295	1	F9	0
057E	Port 24: Number of dropped received packets	0 to 4294967295	1	F9	0
0580	Port 24: Number of multicast frames sent	0 to 4294967295	1	F9	0
0582	Port 24: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0584	Port 24: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0586	Port 25: Number of bytes received	0 to 4294967295	1	F9	0
0588	Port 25: Number of bytes sent	0 to 4294967295	1	F9	0
058A	Port 25: Number of frames received	0 to 4294967295	1	F9	0
058C	Port 25: Number of frames sent	0 to 4294967295	1	F9	0
058E	Port 25: Total bytes received	0 to 4294967295	1	F9	0
0590	Port 25: Total frames received	0 to 4294967295	1	F9	0
0592	Port 25: Number of broadcast frames received	0 to 4294967295	1	F9	0
0594	Port 25: Number of multicast frames received	0 to 4294967295	1	F9	0
0596	Port 25: Number of frames with CRC error	0 to 4294967295	1	F9	0
0598	Port 25: Number of oversized frames received	0 to 4294967295	1	F9	0
059A	Port 25: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
059C	Port 25: Number of jabber frames received	0 to 4294967295	1	F9	0
059E	Port 25: Number of collisions occurred	0 to 4294967295	1	F9	0
05A0	Port 25: Number of late collisions occurred	0 to 4294967295	1	F9	0
05A2	Port 25: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
05A4	Port 25: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
05A6	Port 25: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
05A8	Port 25: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
05AA	Port 25: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
05AC	Port 25: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
05AE	Port 25: Number of MAC error packets	0 to 4294967295	1	F9	0
05B0	Port 25: Number of dropped received packets	0 to 4294967295	1	F9	0
05B2	Port 25: Number of multicast frames sent	0 to 4294967295	1	F9	0
05B4	Port 25: Number of broadcast frames sent	0 to 4294967295	1	F9	0
05B6	Port 25: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
05B8	Port 26: Number of bytes received	0 to 4294967295	1	F9	0
05BA	Port 26: Number of bytes sent	0 to 4294967295	1	F9	0
05BC	Port 26: Number of frames received	0 to 4294967295	1	F9	0
05BE	Port 26: Number of frames sent	0 to 4294967295	1	F9	0
05C0	Port 26: Total bytes received	0 to 4294967295	1	F9	0
05C2	Port 26: Total frames received	0 to 4294967295	1	F9	0
05C4	Port 26: Number of broadcast frames received	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 19 of 40)

Address	Description	Range	Step	Format	Default
05C6	Port 26: Number of multicast frames received	0 to 4294967295	1	F9	0
05C8	Port 26: Number of frames with CRC error	0 to 4294967295	1	F9	0
05CA	Port 26: Number of oversized frames received	0 to 4294967295	1	F9	0
05CC	Port 26: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
05CE	Port 26: Number of jabber frames received	0 to 4294967295	1	F9	0
05D0	Port 26: Number of collisions occurred	0 to 4294967295	1	F9	0
05D2	Port 26: Number of late collisions occurred	0 to 4294967295	1	F9	0
05D4	Port 26: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
05D6	Port 26: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
05D8	Port 26: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
05DA	Port 26: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
05DC	Port 26: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
05DE	Port 26: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
05E0	Port 26: Number of MAC error packets	0 to 4294967295	1	F9	0
05E2	Port 26: Number of dropped received packets	0 to 4294967295	1	F9	0
05E4	Port 26: Number of multicast frames sent	0 to 4294967295	1	F9	0
05E6	Port 26: Number of broadcast frames sent	0 to 4294967295	1	F9	0
05E8	Port 26: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
05EA	Port 27: Number of bytes received	0 to 4294967295	1	F9	0
05EC	Port 27: Number of bytes sent	0 to 4294967295	1	F9	0
05EE	Port 27: Number of frames received	0 to 4294967295	1	F9	0
05F0	Port 27: Number of frames sent	0 to 4294967295	1	F9	0
05F2	Port 27: Total bytes received	0 to 4294967295	1	F9	0
05F4	Port 27: Total frames received	0 to 4294967295	1	F9	0
05F6	Port 27: Number of broadcast frames received	0 to 4294967295	1	F9	0
05F8	Port 27: Number of multicast frames received	0 to 4294967295	1	F9	0
05FA	Port 27: Number of frames with CRC error	0 to 4294967295	1	F9	0
05FC	Port 27: Number of oversized frames received	0 to 4294967295	1	F9	0
05FE	Port 27: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0600	Port 27: Number of jabber frames received	0 to 4294967295	1	F9	0
0602	Port 27: Number of collisions occurred	0 to 4294967295	1	F9	0
0604	Port 27: Number of late collisions occurred	0 to 4294967295	1	F9	0
0606	Port 27: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0608	Port 27: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
060A	Port 27: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
060C	Port 27: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
060E	Port 27: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
0610	Port 27: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0612	Port 27: Number of MAC error packets	0 to 4294967295	1	F9	0
0614	Port 27: Number of dropped received packets	0 to 4294967295	1	F9	0
0616	Port 27: Number of multicast frames sent	0 to 4294967295	1	F9	0
0618	Port 27: Number of broadcast frames sent	0 to 4294967295	1	F9	0
061A	Port 27: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 20 of 40)

Address	Description	Range	Step	Format	Default
061C	Port 28: Number of bytes received	0 to 4294967295	1	F9	0
061E	Port 28: Number of bytes sent	0 to 4294967295	1	F9	0
0620	Port 28: Number of frames received	0 to 4294967295	1	F9	0
0622	Port 28: Number of frames sent	0 to 4294967295	1	F9	0
0624	Port 28: Total bytes received	0 to 4294967295	1	F9	0
0626	Port 28: Total frames received	0 to 4294967295	1	F9	0
0628	Port 28: Number of broadcast frames received	0 to 4294967295	1	F9	0
062A	Port 28: Number of multicast frames received	0 to 4294967295	1	F9	0
062C	Port 28: Number of frames with CRC error	0 to 4294967295	1	F9	0
062E	Port 28: Number of oversized frames received	0 to 4294967295	1	F9	0
0630	Port 28: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0632	Port 28: Number of jabber frames received	0 to 4294967295	1	F9	0
0634	Port 28: Number of collisions occurred	0 to 4294967295	1	F9	0
0636	Port 28: Number of late collisions occurred	0 to 4294967295	1	F9	0
0638	Port 28: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
063A	Port 28: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
063C	Port 28: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
063E	Port 28: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0640	Port 28: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
0642	Port 28: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0644	Port 28: Number of MAC error packets	0 to 4294967295	1	F9	0
0646	Port 28: Number of dropped received packets	0 to 4294967295	1	F9	0
0648	Port 28: Number of multicast frames sent	0 to 4294967295	1	F9	0
064A	Port 28: Number of broadcast frames sent	0 to 4294967295	1	F9	0
064C	Port 28: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
064E	Port 29: Number of bytes received	0 to 4294967295	1	F9	0
0650	Port 29: Number of bytes sent	0 to 4294967295	1	F9	0
0652	Port 29: Number of frames received	0 to 4294967295	1	F9	0
0654	Port 29: Number of frames sent	0 to 4294967295	1	F9	0
0656	Port 29: Total bytes received	0 to 4294967295	1	F9	0
0658	Port 29: Total frames received	0 to 4294967295	1	F9	0
065A	Port 29: Number of broadcast frames received	0 to 4294967295	1	F9	0
065C	Port 29: Number of multicast frames received	0 to 4294967295	1	F9	0
065E	Port 29: Number of frames with CRC error	0 to 4294967295	1	F9	0
0660	Port 29: Number of oversized frames received	0 to 4294967295	1	F9	0
0662	Port 29: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0664	Port 29: Number of jabber frames received	0 to 4294967295	1	F9	0
0666	Port 29: Number of collisions occurred	0 to 4294967295	1	F9	0
0668	Port 29: Number of late collisions occurred	0 to 4294967295	1	F9	0
066A	Port 29: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
066C	Port 29: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
066E	Port 29: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0670	Port 29: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0672	Port 29: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 21 of 40)

Address	Description	Range	Step	Format	Default
0674	Port 29: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0676	Port 29: Number of MAC error packets	0 to 4294967295	1	F9	0
0678	Port 29: Number of dropped received packets	0 to 4294967295	1	F9	0
067A	Port 29: Number of multicast frames sent	0 to 4294967295	1	F9	0
067C	Port 29: Number of broadcast frames sent	0 to 4294967295	1	F9	0
067E	Port 29: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0680	Port 30: Number of bytes received	0 to 4294967295	1	F9	0
0682	Port 30: Number of bytes sent	0 to 4294967295	1	F9	0
0684	Port 30: Number of frames received	0 to 4294967295	1	F9	0
0686	Port 30: Number of frames sent	0 to 4294967295	1	F9	0
0688	Port 30: Total bytes received	0 to 4294967295	1	F9	0
068A	Port 30: Total frames received	0 to 4294967295	1	F9	0
068C	Port 30: Number of broadcast frames received	0 to 4294967295	1	F9	0
068E	Port 30: Number of multicast frames received	0 to 4294967295	1	F9	0
0690	Port 30: Number of frames with CRC error	0 to 4294967295	1	F9	0
0692	Port 30: Number of oversized frames received	0 to 4294967295	1	F9	0
0694	Port 30: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0696	Port 30: Number of jabber frames received	0 to 4294967295	1	F9	0
0698	Port 30: Number of collisions occurred	0 to 4294967295	1	F9	0
069A	Port 30: Number of late collisions occurred	0 to 4294967295	1	F9	0
069C	Port 30: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
069E	Port 30: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
06A0	Port 30: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
06A2	Port 30: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
06A4	Port 30: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
06A6	Port 30: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
06A8	Port 30: Number of MAC error packets	0 to 4294967295	1	F9	0
06AA	Port 30: Number of dropped received packets	0 to 4294967295	1	F9	0
06AC	Port 30: Number of multicast frames sent	0 to 4294967295	1	F9	0
06AE	Port 30: Number of broadcast frames sent	0 to 4294967295	1	F9	0
06B0	Port 30: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
06B2	Port 31: Number of bytes received	0 to 4294967295	1	F9	0
06B4	Port 31: Number of bytes sent	0 to 4294967295	1	F9	0
06B6	Port 31: Number of frames received	0 to 4294967295	1	F9	0
06B8	Port 31: Number of frames sent	0 to 4294967295	1	F9	0
06BA	Port 31: Total bytes received	0 to 4294967295	1	F9	0
06BC	Port 31: Total frames received	0 to 4294967295	1	F9	0
06BE	Port 31: Number of broadcast frames received	0 to 4294967295	1	F9	0
06C0	Port 31: Number of multicast frames received	0 to 4294967295	1	F9	0
06C2	Port 31: Number of frames with CRC error	0 to 4294967295	1	F9	0
06C4	Port 31: Number of oversized frames received	0 to 4294967295	1	F9	0
06C6	Port 31: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
06C8	Port 31: Number of jabber frames received	0 to 4294967295	1	F9	0
06CA	Port 31: Number of collisions occurred	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 22 of 40)

Address	Description	Range	Step	Format	Default
06CC	Port 31: Number of late collisions occurred	0 to 4294967295	1	F9	0
06CE	Port 31: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
06D0	Port 31: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
06D2	Port 31: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
06D4	Port 31: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
06D6	Port 31: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
06D8	Port 31: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
06DA	Port 31: Number of MAC error packets	0 to 4294967295	1	F9	0
06DC	Port 31: Number of dropped received packets	0 to 4294967295	1	F9	0
06DE	Port 31: Number of multicast frames sent	0 to 4294967295	1	F9	0
06E0	Port 31: Number of broadcast frames sent	0 to 4294967295	1	F9	0
06E2	Port 31: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
06E4	Port 32: Number of bytes received	0 to 4294967295	1	F9	0
06E6	Port 32: Number of bytes sent	0 to 4294967295	1	F9	0
06E8	Port 32: Number of frames received	0 to 4294967295	1	F9	0
06EA	Port 32: Number of frames sent	0 to 4294967295	1	F9	0
06EC	Port 32: Total bytes received	0 to 4294967295	1	F9	0
06EE	Port 32: Total frames received	0 to 4294967295	1	F9	0
06F0	Port 32: Number of broadcast frames received	0 to 4294967295	1	F9	0
06F2	Port 32: Number of multicast frames received	0 to 4294967295	1	F9	0
06F4	Port 32: Number of frames with CRC error	0 to 4294967295	1	F9	0
06F6	Port 32: Number of oversized frames received	0 to 4294967295	1	F9	0
06F8	Port 32: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
06FA	Port 32: Number of jabber frames received	0 to 4294967295	1	F9	0
06FC	Port 32: Number of collisions occurred	0 to 4294967295	1	F9	0
06FE	Port 32: Number of late collisions occurred	0 to 4294967295	1	F9	0
0700	Port 32: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0702	Port 32: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0704	Port 32: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0706	Port 32: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0708	Port 32: Number of 512 to 1023 byte frames received/ sent	0 to 4294967295	1	F9	0
070A	Port 32: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
070C	Port 32: Number of MAC error packets	0 to 4294967295	1	F9	0
070E	Port 32: Number of dropped received packets	0 to 4294967295	1	F9	0
0710	Port 32: Number of multicast frames sent	0 to 4294967295	1	F9	0
0712	Port 32: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0714	Port 32: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0716	Serial Number	---	---	String	Varies
071C	Port Present Map Extended	---	---	Bitmap	Varies
071E	Port Link Map Extended	---	---	Bitmap	0
0720	Port Stp State Map Extended	---	---	Bitmap	0
0722	Port Activity Map Extended	---	---	Bitmap	0
0724	Port 33 Type	0 to 6	1	F1	Varies

Table 20–1: Modbus memory map (Sheet 23 of 40)

Address	Description	Range	Step	Format	Default
0725	Port 34 Type	0 to 6	1	F1	Varies
0726	Port 35 Type	0 to 6	1	F1	Varies
0727	Port 36 Type	0 to 6	1	F1	Varies
0744	Port 33 Link Status	0 to 1	1	F1	0
0745	Port 34 Link Status	0 to 1	1	F1	0
0746	Port 35 Link Status	0 to 1	1	F1	0
0747	Port 36 Link Status	0 to 1	1	F1	0
0764	Port 33 STP State	0 to 1	1	F1	Varies
0765	Port 34 STP State	0 to 1	1	F1	Varies
0766	Port 35 STP State	0 to 1	1	F1	Varies
0767	Port 36 STP State	0 to 1	1	F1	Varies
0784	Port 33 Activity	0 to 1	1	F1	0
0785	Port 34 Activity	0 to 1	1	F1	0
0786	Port 35 Activity	0 to 1	1	F1	0
0787	Port 36 Activity	0 to 1	1	F1	0
07A4	Port33 - Number of bytes received	0 to 4294967295	-	F9	0
07A6	Port33 - Number of bytes sent	0 to 4294967295	-	F9	0
07A8	Port33 - Number of frames received	0 to 4294967295	-	F9	0
07AA	Port33 - Number of frames sent	0 to 4294967295	-	F9	0
07AC	Port33 - Total bytes received	0 to 4294967295	-	F9	0
07AE	Port33 - Total frames received	0 to 4294967295	-	F9	0
07B0	Port33 - Number of broadcast frames received	0 to 4294967295	-	F9	0
07B2	Port33 - Number of multicast frames received	0 to 4294967295	-	F9	0
07B4	Port33 - Number of frames with CRC error	0 to 4294967295	-	F9	0
07B6	Port33 - Number of oversized frames received	0 to 4294967295	-	F9	0
07B8	Port33 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	-	F9	0
07BA	Port33 - Number of jabber frames received	0 to 4294967295	-	F9	0
07BC	Port33 - Number of collisions occured	0 to 4294967295	-	F9	0
07BE	Port33 - Number of late collisions occured	0 to 4294967295	-	F9	0
07C0	Port33 - Number of 64-byte frames rcvd/sent	0 to 4294967295	-	F9	0
07C2	Port33 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	-	F9	0
07C4	Port33 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	-	F9	0
07C6	Port33 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	-	F9	0
07C8	Port33 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	-	F9	0
07CA	Port33 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	-	F9	0
07CC	Port33 - Number of Mac Error Packets	0 to 4294967295	-	F9	0
07CE	Port33 - Number of dropped received packets	0 to 4294967295	-	F9	0
07D0	Port33 - Number of multicast frames sent	0 to 4294967295	-	F9	0
07D2	Port33 - Number of broadcast frames sent	0 to 4294967295	-	F9	0
07D4	Port33 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	-	F9	0
07D6	Port34 - Number of bytes received	0 to 4294967295	-	F9	0
07D8	Port34 - Number of bytes sent	0 to 4294967295	-	F9	0
07DA	Port34 - Number of frames received	0 to 4294967295	-	F9	0
07DC	Port34 - Number of frames sent	0 to 4294967295	-	F9	0
07DE	Port34 - Total bytes received	0 to 4294967295	-	F9	0
07E0	Port34 - Total frames received	0 to 4294967295	-	F9	0

Table 20–1: Modbus memory map (Sheet 24 of 40)

Address	Description	Range	Step	Format	Default
07E2	Port34 - Number of broadcast frames received	0 to 4294967295	-	F9	0
07E4	Port34 - Number of multicast frames received	0 to 4294967295	-	F9	0
07E6	Port34 - Number of frames with CRC error	0 to 4294967295	-	F9	0
07E8	Port34 - Number of oversized frames received	0 to 4294967295	-	F9	0
07EA	Port34 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	-	F9	0
07EC	Port34 - Number of jabber frames received	0 to 4294967295	-	F9	0
07EE	Port34 - Number of collisions occured	0 to 4294967295	-	F9	0
07F0	Port34 - Number of late collisions occured	0 to 4294967295	-	F9	0
07F2	Port34 - Number of 64-byte frames rcvd/sent	0 to 4294967295	-	F9	0
07F4	Port34 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	-	F9	0
07F6	Port34 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	-	F9	0
07F8	Port34 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	-	F9	0
07FA	Port34 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	-	F9	0
07FC	Port34 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	-	F9	0
07FE	Port34 - Number of Mac Error Packets	0 to 4294967295	-	F9	0
800	Port34 - Number of dropped received packets	0 to 4294967295	-	F9	0
802	Port34 - Number of multicast frames sent	0 to 4294967295	-	F9	0
804	Port34 - Number of broadcast frames sent	0 to 4294967295	-	F9	0
806	Port34 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	-	F9	0
808	Port35 - Number of bytes received	0 to 4294967295	-	F9	0
080A	Port35 - Number of bytes sent	0 to 4294967295	-	F9	0
080C	Port35 - Number of frames received	0 to 4294967295	-	F9	0
080E	Port35 - Number of frames sent	0 to 4294967295	-	F9	0
810	Port35 - Total bytes received	0 to 4294967295	-	F9	0
812	Port35 - Total frames received	0 to 4294967295	-	F9	0
814	Port35 - Number of broadcast frames received	0 to 4294967295	-	F9	0
816	Port35 - Number of multicast frames received	0 to 4294967295	-	F9	0
818	Port35 - Number of frames with CRC error	0 to 4294967295	-	F9	0
081A	Port35 - Number of oversized frames received	0 to 4294967295	-	F9	0
081C	Port35 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	-	F9	0
081E	Port35 - Number of jabber frames received	0 to 4294967295	-	F9	0
820	Port35 - Number of collisions occured	0 to 4294967295	-	F9	0
822	Port35 - Number of late collisions occured	0 to 4294967295	-	F9	0
824	Port35 - Number of 64-byte frames rcvd/sent	0 to 4294967295	-	F9	0
826	Port35 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	-	F9	0
828	Port35 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	-	F9	0
082A	Port35 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	-	F9	0
082C	Port35 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	-	F9	0
082E	Port35 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	-	F9	0
830	Port35 - Number of Mac Error Packets	0 to 4294967295	-	F9	0
832	Port35 - Number of dropped received packets	0 to 4294967295	-	F9	0
834	Port35 - Number of multicast frames sent	0 to 4294967295	-	F9	0
836	Port35 - Number of broadcast frames sent	0 to 4294967295	-	F9	0
838	Port35 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	-	F9	0
083A	Port36 - Number of bytes received	0 to 4294967295	-	F9	0
083C	Port36 - Number of bytes sent	0 to 4294967295	-	F9	0

Table 20–1: Modbus memory map (Sheet 25 of 40)

Address	Description	Range	Step	Format	Default
083E	Port36 - Number of frames received	0 to 4294967295	-	F9	0
840	Port36 - Number of frames sent	0 to 4294967295	-	F9	0
842	Port36 - Total bytes received	0 to 4294967295	-	F9	0
844	Port36 - Total frames received	0 to 4294967295	-	F9	0
846	Port36 - Number of broadcast frames received	0 to 4294967295	-	F9	0
848	Port36 - Number of multicast frames received	0 to 4294967295	-	F9	0
084A	Port36 - Number of frames with CRC error	0 to 4294967295	-	F9	0
084C	Port36 - Number of oversized frames received	0 to 4294967295	-	F9	0
084E	Port36 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	-	F9	0
850	Port36 - Number of jabber frames received	0 to 4294967295	-	F9	0
852	Port36 - Number of collisions occured	0 to 4294967295	-	F9	0
854	Port36 - Number of late collisions occured	0 to 4294967295	-	F9	0
856	Port36 - Number of 64-byte frames rcvd/sent	0 to 4294967295	-	F9	0
858	Port36 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	-	F9	0
085A	Port36 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	-	F9	0
085C	Port36 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	-	F9	0
085E	Port36 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	-	F9	0
860	Port36 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	-	F9	0
862	Port36 - Number of Mac Error Packets	0 to 4294967295	-	F9	0
864	Port36 - Number of dropped received packets	0 to 4294967295	-	F9	0
866	Port36 - Number of multicast frames sent	0 to 4294967295	-	F9	0
868	Port36 - Number of broadcast frames sent	0 to 4294967295	-	F9	0
086A	Port36 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	-	F9	0
086C	Port37 - Number of bytes received	0 to 4294967295	1	F9	0
086E	Port37 - Number of bytes sent	0 to 4294967295	1	F9	0
870	Port37 - Number of frames received	0 to 4294967295	1	F9	0
872	Port37 - Number of frames sent	0 to 4294967295	1	F9	0
874	Port37 - Total bytes received	0 to 4294967295	1	F9	0
876	Port37 - Total frames received	0 to 4294967295	1	F9	0
878	Port37 - Number of broadcast frames received	0 to 4294967295	1	F9	0
087A	Port37 - Number of multicast frames received	0 to 4294967295	1	F9	0
087C	Port37 - Number of frames with CRC error	0 to 4294967295	1	F9	0
087E	Port37 - Number of oversized frames received	0 to 4294967295	1	F9	0
880	Port37 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
882	Port37 - Number of jabber frames received	0 to 4294967295	1	F9	0
884	Port37 - Number of collisions occured	0 to 4294967295	1	F9	0
886	Port37 - Number of late collisions occured	0 to 4294967295	1	F9	0
888	Port37 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
088A	Port37 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
088C	Port37 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
088E	Port37 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
890	Port37 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
892	Port37 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
894	Port37 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
896	Port37 - Number of dropped received packets	0 to 4294967295	1	F9	0
898	Port37 - Number of multicast frames sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 26 of 40)

Address	Description	Range	Step	Format	Default
089A	Port37 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
089C	Port37 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
089E	Port38 - Number of bytes received	0 to 4294967295	1	F9	0
08A0	Port38 - Number of bytes sent	0 to 4294967295	1	F9	0
08A2	Port38 - Number of frames received	0 to 4294967295	1	F9	0
08A4	Port38 - Number of frames sent	0 to 4294967295	1	F9	0
08A6	Port38 - Total bytes received	0 to 4294967295	1	F9	0
08A8	Port38 - Total frames received	0 to 4294967295	1	F9	0
08AA	Port38 - Number of broadcast frames received	0 to 4294967295	1	F9	0
08AC	Port38 - Number of multicast frames received	0 to 4294967295	1	F9	0
08AE	Port38 - Number of frames with CRC error	0 to 4294967295	1	F9	0
08B0	Port38 - Number of oversized frames received	0 to 4294967295	1	F9	0
08B2	Port38 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
08B4	Port38 - Number of jabber frames received	0 to 4294967295	1	F9	0
08B6	Port38 - Number of collisions occured	0 to 4294967295	1	F9	0
08B8	Port38 - Number of late collisions occured	0 to 4294967295	1	F9	0
08BA	Port38 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
08BC	Port38 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
08BE	Port38 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
08C0	Port38 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
08C2	Port38 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
08C4	Port38 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
08C6	Port38 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
08C8	Port38 - Number of dropped received packets	0 to 4294967295	1	F9	0
08CA	Port38 - Number of multicast frames sent	0 to 4294967295	1	F9	0
08CC	Port38 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
08CE	Port38 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
08D0	Port39 - Number of bytes received	0 to 4294967295	1	F9	0
08D2	Port39 - Number of bytes sent	0 to 4294967295	1	F9	0
08D4	Port39 - Number of frames received	0 to 4294967295	1	F9	0
08D6	Port39 - Number of frames sent	0 to 4294967295	1	F9	0
08D8	Port39 - Total bytes received	0 to 4294967295	1	F9	0
08DA	Port39 - Total frames received	0 to 4294967295	1	F9	0
08DC	Port39 - Number of broadcast frames received	0 to 4294967295	1	F9	0
08DE	Port39 - Number of multicast frames received	0 to 4294967295	1	F9	0
08E0	Port39 - Number of frames with CRC error	0 to 4294967295	1	F9	0
08E2	Port39 - Number of oversized frames received	0 to 4294967295	1	F9	0
08E4	Port39 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
08E6	Port39 - Number of jabber frames received	0 to 4294967295	1	F9	0
08E8	Port39 - Number of collisions occured	0 to 4294967295	1	F9	0
08EA	Port39 - Number of late collisions occured	0 to 4294967295	1	F9	0
08EC	Port39 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
08EE	Port39 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
08F0	Port39 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
08F2	Port39 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
08F4	Port39 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 27 of 40)

Address	Description	Range	Step	Format	Default
08F6	Port39 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
08F8	Port39 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
08FA	Port39 - Number of dropped received packets	0 to 4294967295	1	F9	0
08FC	Port39 - Number of multicast frames sent	0 to 4294967295	1	F9	0
08FE	Port39 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
900	Port39 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
902	Port40 - Number of bytes received	0 to 4294967295	1	F9	0
904	Port40 - Number of bytes sent	0 to 4294967295	1	F9	0
906	Port40 - Number of frames received	0 to 4294967295	1	F9	0
908	Port40 - Number of frames sent	0 to 4294967295	1	F9	0
090A	Port40 - Total bytes received	0 to 4294967295	1	F9	0
090C	Port40 - Total frames received	0 to 4294967295	1	F9	0
090E	Port40 - Number of broadcast frames received	0 to 4294967295	1	F9	0
910	Port40 - Number of multicast frames received	0 to 4294967295	1	F9	0
912	Port40 - Number of frames with CRC error	0 to 4294967295	1	F9	0
914	Port40 - Number of oversized frames received	0 to 4294967295	1	F9	0
916	Port40 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
918	Port40 - Number of jabber frames received	0 to 4294967295	1	F9	0
091A	Port40 - Number of collisions occured	0 to 4294967295	1	F9	0
091C	Port40 - Number of late collisions occured	0 to 4294967295	1	F9	0
091E	Port40 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
920	Port40 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
922	Port40 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
924	Port40 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
926	Port40 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
928	Port40 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
092A	Port40 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
092C	Port40 - Number of dropped received packets	0 to 4294967295	1	F9	0
092E	Port40 - Number of multicast frames sent	0 to 4294967295	1	F9	0
930	Port40 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
932	Port40 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
934	Port41 - Number of bytes received	0 to 4294967295	1	F9	0
936	Port41 - Number of bytes sent	0 to 4294967295	1	F9	0
938	Port41 - Number of frames received	0 to 4294967295	1	F9	0
093A	Port41 - Number of frames sent	0 to 4294967295	1	F9	0
093C	Port41 - Total bytes received	0 to 4294967295	1	F9	0
093E	Port41 - Total frames received	0 to 4294967295	1	F9	0
940	Port41 - Number of broadcast frames received	0 to 4294967295	1	F9	0
942	Port41 - Number of multicast frames received	0 to 4294967295	1	F9	0
944	Port41 - Number of frames with CRC error	0 to 4294967295	1	F9	0
946	Port41 - Number of oversized frames received	0 to 4294967295	1	F9	0
948	Port41 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
094A	Port41 - Number of jabber frames received	0 to 4294967295	1	F9	0
094C	Port41 - Number of collisions occured	0 to 4294967295	1	F9	0
094E	Port41 - Number of late collisions occured	0 to 4294967295	1	F9	0
950	Port41 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 28 of 40)

Address	Description	Range	Step	Format	Default
952	Port41 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
954	Port41 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
956	Port41 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
958	Port41 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
095A	Port41 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
095C	Port41 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
095E	Port41 - Number of dropped received packets	0 to 4294967295	1	F9	0
960	Port41 - Number of multicast frames sent	0 to 4294967295	1	F9	0
962	Port41 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
964	Port41 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
966	Port42 - Number of bytes received	0 to 4294967295	1	F9	0
968	Port42 - Number of bytes sent	0 to 4294967295	1	F9	0
096A	Port42 - Number of frames received	0 to 4294967295	1	F9	0
096C	Port42 - Number of frames sent	0 to 4294967295	1	F9	0
096E	Port42 - Total bytes received	0 to 4294967295	1	F9	0
970	Port42 - Total frames received	0 to 4294967295	1	F9	0
972	Port42 - Number of broadcast frames received	0 to 4294967295	1	F9	0
974	Port42 - Number of multicast frames received	0 to 4294967295	1	F9	0
976	Port42 - Number of frames with CRC error	0 to 4294967295	1	F9	0
978	Port42 - Number of oversized frames received	0 to 4294967295	1	F9	0
097A	Port42 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
097C	Port42 - Number of jabber frames received	0 to 4294967295	1	F9	0
097E	Port42 - Number of collisions occured	0 to 4294967295	1	F9	0
980	Port42 - Number of late collisions occured	0 to 4294967295	1	F9	0
982	Port42 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
984	Port42 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
986	Port42 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
988	Port42 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
098A	Port42 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
098C	Port42 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
098E	Port42 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
990	Port42 - Number of dropped received packets	0 to 4294967295	1	F9	0
992	Port42 - Number of multicast frames sent	0 to 4294967295	1	F9	0
994	Port42 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
996	Port42 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
998	Port43 - Number of bytes received	0 to 4294967295	1	F9	0
099A	Port43 - Number of bytes sent	0 to 4294967295	1	F9	0
099C	Port43 - Number of frames received	0 to 4294967295	1	F9	0
099E	Port43 - Number of frames sent	0 to 4294967295	1	F9	0
09A0	Port43 - Total bytes received	0 to 4294967295	1	F9	0
09A2	Port43 - Total frames received	0 to 4294967295	1	F9	0
09A4	Port43 - Number of broadcast frames received	0 to 4294967295	1	F9	0
09A6	Port43 - Number of multicast frames received	0 to 4294967295	1	F9	0
09A8	Port43 - Number of frames with CRC error	0 to 4294967295	1	F9	0
09AA	Port43 - Number of oversized frames received	0 to 4294967295	1	F9	0
09AC	Port43 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 29 of 40)

Address	Description	Range	Step	Format	Default
09AE	Port43 - Number of jabber frames received	0 to 4294967295	1	F9	0
09B0	Port43 - Number of collisions occured	0 to 4294967295	1	F9	0
09B2	Port43 - Number of late collisions occured	0 to 4294967295	1	F9	0
09B4	Port43 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
09B6	Port43 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
09B8	Port43 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
09BA	Port43 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
09BC	Port43 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
09BE	Port43 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
09C0	Port43 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
09C2	Port43 - Number of dropped received packets	0 to 4294967295	1	F9	0
09C4	Port43 - Number of multicast frames sent	0 to 4294967295	1	F9	0
09C6	Port43 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
09C8	Port43 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
09CA	Port44 - Number of bytes received	0 to 4294967295	1	F9	0
09CC	Port44 - Number of bytes sent	0 to 4294967295	1	F9	0
09CE	Port44 - Number of frames received	0 to 4294967295	1	F9	0
09D0	Port44 - Number of frames sent	0 to 4294967295	1	F9	0
09D2	Port44 - Total bytes received	0 to 4294967295	1	F9	0
09D4	Port44 - Total frames received	0 to 4294967295	1	F9	0
09D6	Port44 - Number of broadcast frames received	0 to 4294967295	1	F9	0
09D8	Port44 - Number of multicast frames received	0 to 4294967295	1	F9	0
09DA	Port44 - Number of frames with CRC error	0 to 4294967295	1	F9	0
09DC	Port44 - Number of oversized frames received	0 to 4294967295	1	F9	0
09DE	Port44 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
09E0	Port44 - Number of jabber frames received	0 to 4294967295	1	F9	0
09E2	Port44 - Number of collisions occured	0 to 4294967295	1	F9	0
09E4	Port44 - Number of late collisions occured	0 to 4294967295	1	F9	0
09E6	Port44 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
09E8	Port44 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
09EA	Port44 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
09EC	Port44 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
09EE	Port44 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
09F0	Port44 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
09F2	Port44 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
09F4	Port44 - Number of dropped received packets	0 to 4294967295	1	F9	0
09F6	Port44 - Number of multicast frames sent	0 to 4294967295	1	F9	0
09F8	Port44 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
09FA	Port44 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
09FC	Port45 - Number of bytes received	0 to 4294967295	1	F9	0
09FE	Port45 - Number of bytes sent	0 to 4294967295	1	F9	0
0A00	Port45 - Number of frames received	0 to 4294967295	1	F9	0
0A02	Port45 - Number of frames sent	0 to 4294967295	1	F9	0
0A04	Port45 - Total bytes received	0 to 4294967295	1	F9	0
0A06	Port45 - Total frames received	0 to 4294967295	1	F9	0
0A08	Port45 - Number of broadcast frames received	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 30 of 40)

Address	Description	Range	Step	Format	Default
0A0A	Port45 - Number of multicast frames received	0 to 4294967295	1	F9	0
0A0C	Port45 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0A0E	Port45 - Number of oversized frames received	0 to 4294967295	1	F9	0
0A10	Port45 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0A12	Port45 - Number of jabber frames received	0 to 4294967295	1	F9	0
0A14	Port45 - Number of collisions occured	0 to 4294967295	1	F9	0
0A16	Port45 - Number of late collisions occured	0 to 4294967295	1	F9	0
0A18	Port45 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A1A	Port45 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A1C	Port45 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A1E	Port45 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A20	Port45 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A22	Port45 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A24	Port45 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0A26	Port45 - Number of dropped received packets	0 to 4294967295	1	F9	0
0A28	Port45 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0A2A	Port45 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0A2C	Port45 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0A2E	Port46 - Number of bytes received	0 to 4294967295	1	F9	0
0A30	Port46 - Number of bytes sent	0 to 4294967295	1	F9	0
0A32	Port46 - Number of frames received	0 to 4294967295	1	F9	0
0A34	Port46 - Number of frames sent	0 to 4294967295	1	F9	0
0A36	Port46 - Total bytes received	0 to 4294967295	1	F9	0
0A38	Port46 - Total frames received	0 to 4294967295	1	F9	0
0A3A	Port46 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0A3C	Port46 - Number of multicast frames received	0 to 4294967295	1	F9	0
0A3E	Port46 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0A40	Port46 - Number of oversized frames received	0 to 4294967295	1	F9	0
0A42	Port46 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0A44	Port46 - Number of jabber frames received	0 to 4294967295	1	F9	0
0A46	Port46 - Number of collisions occured	0 to 4294967295	1	F9	0
0A48	Port46 - Number of late collisions occured	0 to 4294967295	1	F9	0
0A4A	Port46 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A4C	Port46 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A4E	Port46 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A50	Port46 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A52	Port46 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A54	Port46 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A56	Port46 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0A58	Port46 - Number of dropped received packets	0 to 4294967295	1	F9	0
0A5A	Port46 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0A5C	Port46 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0A5E	Port46 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0A60	Port47 - Number of bytes received	0 to 4294967295	1	F9	0
0A62	Port47 - Number of bytes sent	0 to 4294967295	1	F9	0
0A64	Port47 - Number of frames received	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 31 of 40)

Address	Description	Range	Step	Format	Default
0A66	Port47 - Number of frames sent	0 to 4294967295	1	F9	0
0A68	Port47 - Total bytes received	0 to 4294967295	1	F9	0
0A6A	Port47 - Total frames received	0 to 4294967295	1	F9	0
0A6C	Port47 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0A6E	Port47 - Number of multicast frames received	0 to 4294967295	1	F9	0
0A70	Port47 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0A72	Port47 - Number of oversized frames received	0 to 4294967295	1	F9	0
0A74	Port47 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0A76	Port47 - Number of jabber frames received	0 to 4294967295	1	F9	0
0A78	Port47 - Number of collisions occured	0 to 4294967295	1	F9	0
0A7A	Port47 - Number of late collisions occured	0 to 4294967295	1	F9	0
0A7C	Port47 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A7E	Port47 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A80	Port47 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A82	Port47 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A84	Port47 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A86	Port47 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0A88	Port47 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0A8A	Port47 - Number of dropped received packets	0 to 4294967295	1	F9	0
0A8C	Port47 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0A8E	Port47 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0A90	Port47 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0A92	Port48 - Number of bytes received	0 to 4294967295	1	F9	0
0A94	Port48 - Number of bytes sent	0 to 4294967295	1	F9	0
0A96	Port48 - Number of frames received	0 to 4294967295	1	F9	0
0A98	Port48 - Number of frames sent	0 to 4294967295	1	F9	0
0A9A	Port48 - Total bytes received	0 to 4294967295	1	F9	0
0A9C	Port48 - Total frames received	0 to 4294967295	1	F9	0
0A9E	Port48 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0AA0	Port48 - Number of multicast frames received	0 to 4294967295	1	F9	0
0AA2	Port48 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0AA4	Port48 - Number of oversized frames received	0 to 4294967295	1	F9	0
0AA6	Port48 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0AA8	Port48 - Number of jabber frames received	0 to 4294967295	1	F9	0
0AAA	Port48 - Number of collisions occured	0 to 4294967295	1	F9	0
0AAC	Port48 - Number of late collisions occured	0 to 4294967295	1	F9	0
0AAE	Port48 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AB0	Port48 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AB2	Port48 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AB4	Port48 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AB6	Port48 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AB8	Port48 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0ABA	Port48 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0ABC	Port48 - Number of dropped received packets	0 to 4294967295	1	F9	0
0ABE	Port48 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0AC0	Port48 - Number of broadcast frames sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 32 of 40)

Address	Description	Range	Step	Format	Default
0AC2	Port48 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0AC4	Port49 - Number of bytes received	0 to 4294967295	1	F9	0
0AC6	Port49 - Number of bytes sent	0 to 4294967295	1	F9	0
0AC8	Port49 - Number of frames received	0 to 4294967295	1	F9	0
0ACA	Port49 - Number of frames sent	0 to 4294967295	1	F9	0
0ACC	Port49 - Total bytes received	0 to 4294967295	1	F9	0
0ACE	Port49 - Total frames received	0 to 4294967295	1	F9	0
0AD0	Port49 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0AD2	Port49 - Number of multicast frames received	0 to 4294967295	1	F9	0
0AD4	Port49 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0AD6	Port49 - Number of oversized frames received	0 to 4294967295	1	F9	0
0AD8	Port49 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0ADA	Port49 - Number of jabber frames received	0 to 4294967295	1	F9	0
0ADC	Port49 - Number of collisions occured	0 to 4294967295	1	F9	0
0ADE	Port49 - Number of late collisions occured	0 to 4294967295	1	F9	0
0AE0	Port49 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AE2	Port49 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AE4	Port49 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AE6	Port49 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AE8	Port49 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AEA	Port49 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0AEC	Port49 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0AEE	Port49 - Number of dropped received packets	0 to 4294967295	1	F9	0
0AF0	Port49 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0AF2	Port49 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0AF4	Port49 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0AF6	Port50 - Number of bytes received	0 to 4294967295	1	F9	0
0AF8	Port50 - Number of bytes sent	0 to 4294967295	1	F9	0
0AFA	Port50 - Number of frames received	0 to 4294967295	1	F9	0
0AFC	Port50 - Number of frames sent	0 to 4294967295	1	F9	0
0AFE	Port50 - Total bytes received	0 to 4294967295	1	F9	0
0B00	Port50 - Total frames received	0 to 4294967295	1	F9	0
0B02	Port50 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0B04	Port50 - Number of multicast frames received	0 to 4294967295	1	F9	0
0B06	Port50 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0B08	Port50 - Number of oversized frames received	0 to 4294967295	1	F9	0
0B0A	Port50 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0B0C	Port50 - Number of jabber frames received	0 to 4294967295	1	F9	0
0B0E	Port50 - Number of collisions occured	0 to 4294967295	1	F9	0
0B10	Port50 - Number of late collisions occured	0 to 4294967295	1	F9	0
0B12	Port50 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B14	Port50 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B16	Port50 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B18	Port50 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B1A	Port50 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B1C	Port50 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 33 of 40)

Address	Description	Range	Step	Format	Default
0B1E	Port50 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0B20	Port50 - Number of dropped received packets	0 to 4294967295	1	F9	0
0B22	Port50 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0B24	Port50 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0B26	Port50 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0B28	Port51 - Number of bytes received	0 to 4294967295	1	F9	0
0B2A	Port51 - Number of bytes sent	0 to 4294967295	1	F9	0
0B2C	Port51 - Number of frames received	0 to 4294967295	1	F9	0
0B2E	Port51 - Number of frames sent	0 to 4294967295	1	F9	0
0B30	Port51 - Total bytes received	0 to 4294967295	1	F9	0
0B32	Port51 - Total frames received	0 to 4294967295	1	F9	0
0B34	Port51 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0B36	Port51 - Number of multicast frames received	0 to 4294967295	1	F9	0
0B38	Port51 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0B3A	Port51 - Number of oversized frames received	0 to 4294967295	1	F9	0
0B3C	Port51 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0B3E	Port51 - Number of jabber frames received	0 to 4294967295	1	F9	0
0B40	Port51 - Number of collisions occured	0 to 4294967295	1	F9	0
0B42	Port51 - Number of late collisions occured	0 to 4294967295	1	F9	0
0B44	Port51 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B46	Port51 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B48	Port51 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B4A	Port51 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B4C	Port51 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B4E	Port51 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B50	Port51 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0B52	Port51 - Number of dropped received packets	0 to 4294967295	1	F9	0
0B54	Port51 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0B56	Port51 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0B58	Port51 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0B5A	Port52 - Number of bytes received	0 to 4294967295	1	F9	0
0B5C	Port52 - Number of bytes sent	0 to 4294967295	1	F9	0
0B5E	Port52 - Number of frames received	0 to 4294967295	1	F9	0
0B60	Port52 - Number of frames sent	0 to 4294967295	1	F9	0
0B62	Port52 - Total bytes received	0 to 4294967295	1	F9	0
0B64	Port52 - Total frames received	0 to 4294967295	1	F9	0
0B66	Port52 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0B68	Port52 - Number of multicast frames received	0 to 4294967295	1	F9	0
0B6A	Port52 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0B6C	Port52 - Number of oversized frames received	0 to 4294967295	1	F9	0
0B6E	Port52 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0B70	Port52 - Number of jabber frames received	0 to 4294967295	1	F9	0
0B72	Port52 - Number of collisions occured	0 to 4294967295	1	F9	0
0B74	Port52 - Number of late collisions occured	0 to 4294967295	1	F9	0
0B76	Port52 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B78	Port52 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 34 of 40)

Address	Description	Range	Step	Format	Default
0B7A	Port52 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B7C	Port52 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B7E	Port52 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B80	Port52 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0B82	Port52 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0B84	Port52 - Number of dropped received packets	0 to 4294967295	1	F9	0
0B86	Port52 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0B88	Port52 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0B8A	Port52 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0B8C	Port53 - Number of bytes received	0 to 4294967295	1	F9	0
0B8E	Port53 - Number of bytes sent	0 to 4294967295	1	F9	0
0B90	Port53 - Number of frames received	0 to 4294967295	1	F9	0
0B92	Port53 - Number of frames sent	0 to 4294967295	1	F9	0
0B94	Port53 - Total bytes received	0 to 4294967295	1	F9	0
0B96	Port53 - Total frames received	0 to 4294967295	1	F9	0
0B98	Port53 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0B9A	Port53 - Number of multicast frames received	0 to 4294967295	1	F9	0
0B9C	Port53 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0B9E	Port53 - Number of oversized frames received	0 to 4294967295	1	F9	0
0BA0	Port53 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0BA2	Port53 - Number of jabber frames received	0 to 4294967295	1	F9	0
0BA4	Port53 - Number of collisions occured	0 to 4294967295	1	F9	0
0BA6	Port53 - Number of late collisions occured	0 to 4294967295	1	F9	0
0BA8	Port53 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BAA	Port53 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BAC	Port53 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BAE	Port53 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BB0	Port53 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BB2	Port53 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BB4	Port53 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0BB6	Port53 - Number of dropped received packets	0 to 4294967295	1	F9	0
0BB8	Port53 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0BBA	Port53 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0BBC	Port53 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0BBE	Port54 - Number of bytes received	0 to 4294967295	1	F9	0
0BC0	Port54 - Number of bytes sent	0 to 4294967295	1	F9	0
0BC2	Port54 - Number of frames received	0 to 4294967295	1	F9	0
0BC4	Port54 - Number of frames sent	0 to 4294967295	1	F9	0
0BC6	Port54 - Total bytes received	0 to 4294967295	1	F9	0
0BC8	Port54 - Total frames received	0 to 4294967295	1	F9	0
0BCA	Port54 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0BCC	Port54 - Number of multicast frames received	0 to 4294967295	1	F9	0
0BCE	Port54 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0BD0	Port54 - Number of oversized frames received	0 to 4294967295	1	F9	0
0BD2	Port54 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0BD4	Port54 - Number of jabber frames received	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 35 of 40)

Address	Description	Range	Step	Format	Default
0BD6	Port54 - Number of collisions occured	0 to 4294967295	1	F9	0
0BD8	Port54 - Number of late collisions occured	0 to 4294967295	1	F9	0
0BDA	Port54 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BDC	Port54 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BDE	Port54 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BE0	Port54 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BE2	Port54 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BE4	Port54 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0BE6	Port54 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0BE8	Port54 - Number of dropped received packets	0 to 4294967295	1	F9	0
0BEA	Port54 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0BEC	Port54 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0BEE	Port54 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0BF0	Port55 - Number of bytes received	0 to 4294967295	1	F9	0
0BF2	Port55 - Number of bytes sent	0 to 4294967295	1	F9	0
0BF4	Port55 - Number of frames received	0 to 4294967295	1	F9	0
0BF6	Port55 - Number of frames sent	0 to 4294967295	1	F9	0
0BF8	Port55 - Total bytes received	0 to 4294967295	1	F9	0
0BFA	Port55 - Total frames received	0 to 4294967295	1	F9	0
0BFC	Port55 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0BFE	Port55 - Number of multicast frames received	0 to 4294967295	1	F9	0
0C00	Port55 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0C02	Port55 - Number of oversized frames received	0 to 4294967295	1	F9	0
0C04	Port55 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0C06	Port55 - Number of jabber frames received	0 to 4294967295	1	F9	0
0C08	Port55 - Number of collisions occured	0 to 4294967295	1	F9	0
0C0A	Port55 - Number of late collisions occured	0 to 4294967295	1	F9	0
0C0C	Port55 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C0E	Port55 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C10	Port55 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C12	Port55 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C14	Port55 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C16	Port55 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C18	Port55 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0C1A	Port55 - Number of dropped received packets	0 to 4294967295	1	F9	0
0C1C	Port55 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0C1E	Port55 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0C20	Port55 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0C22	Port56 - Number of bytes received	0 to 4294967295	1	F9	0
0C24	Port56 - Number of bytes sent	0 to 4294967295	1	F9	0
0C26	Port56 - Number of frames received	0 to 4294967295	1	F9	0
0C28	Port56 - Number of frames sent	0 to 4294967295	1	F9	0
0C2A	Port56 - Total bytes received	0 to 4294967295	1	F9	0
0C2C	Port56 - Total frames received	0 to 4294967295	1	F9	0
0C2E	Port56 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0C30	Port56 - Number of multicast frames received	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 36 of 40)

Address	Description	Range	Step	Format	Default
0C32	Port56 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0C34	Port56 - Number of oversized frames received	0 to 4294967295	1	F9	0
0C36	Port56 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0C38	Port56 - Number of jabber frames received	0 to 4294967295	1	F9	0
0C3A	Port56 - Number of collisions occured	0 to 4294967295	1	F9	0
0C3C	Port56 - Number of late collisions occured	0 to 4294967295	1	F9	0
0C3E	Port56 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C40	Port56 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C42	Port56 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C44	Port56 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C46	Port56 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C48	Port56 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C4A	Port56 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0C4C	Port56 - Number of dropped received packets	0 to 4294967295	1	F9	0
0C4E	Port56 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0C50	Port56 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0C52	Port56 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0C54	Port57 - Number of bytes received	0 to 4294967295	1	F9	0
0C56	Port57 - Number of bytes sent	0 to 4294967295	1	F9	0
0C58	Port57 - Number of frames received	0 to 4294967295	1	F9	0
0C5A	Port57 - Number of frames sent	0 to 4294967295	1	F9	0
0C5C	Port57 - Total bytes received	0 to 4294967295	1	F9	0
0C5E	Port57 - Total frames received	0 to 4294967295	1	F9	0
0C60	Port57 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0C62	Port57 - Number of multicast frames received	0 to 4294967295	1	F9	0
0C64	Port57 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0C66	Port57 - Number of oversized frames received	0 to 4294967295	1	F9	0
0C68	Port57 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0C6A	Port57 - Number of jabber frames received	0 to 4294967295	1	F9	0
0C6C	Port57 - Number of collisions occured	0 to 4294967295	1	F9	0
0C6E	Port57 - Number of late collisions occured	0 to 4294967295	1	F9	0
0C70	Port57 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C72	Port57 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C74	Port57 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C76	Port57 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C78	Port57 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C7A	Port57 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0C7C	Port57 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0C7E	Port57 - Number of dropped received packets	0 to 4294967295	1	F9	0
0C80	Port57 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0C82	Port57 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0C84	Port57 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0C86	Port58 - Number of bytes received	0 to 4294967295	1	F9	0
0C88	Port58 - Number of bytes sent	0 to 4294967295	1	F9	0
0C8A	Port58 - Number of frames received	0 to 4294967295	1	F9	0
0C8C	Port58 - Number of frames sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 37 of 40)

Address	Description	Range	Step	Format	Default
0C8E	Port58 - Total bytes received	0 to 4294967295	1	F9	0
0C90	Port58 - Total frames received	0 to 4294967295	1	F9	0
0C92	Port58 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0C94	Port58 - Number of multicast frames received	0 to 4294967295	1	F9	0
0C96	Port58 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0C98	Port58 - Number of oversized frames received	0 to 4294967295	1	F9	0
0C9A	Port58 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0C9C	Port58 - Number of jabber frames received	0 to 4294967295	1	F9	0
0C9E	Port58 - Number of collisions occured	0 to 4294967295	1	F9	0
0CA0	Port58 - Number of late collisions occured	0 to 4294967295	1	F9	0
0CA2	Port58 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CA4	Port58 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CA6	Port58 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CA8	Port58 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CAA	Port58 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CAC	Port58 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CAE	Port58 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0CB0	Port58 - Number of dropped received packets	0 to 4294967295	1	F9	0
0CB2	Port58 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0CB4	Port58 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0CB6	Port58 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0CB8	Port59 - Number of bytes received	0 to 4294967295	1	F9	0
0CBA	Port59 - Number of bytes sent	0 to 4294967295	1	F9	0
0CBC	Port59 - Number of frames received	0 to 4294967295	1	F9	0
0CBE	Port59 - Number of frames sent	0 to 4294967295	1	F9	0
0CC0	Port59 - Total bytes received	0 to 4294967295	1	F9	0
0CC2	Port59 - Total frames received	0 to 4294967295	1	F9	0
0CC4	Port59 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0CC6	Port59 - Number of multicast frames received	0 to 4294967295	1	F9	0
0CC8	Port59 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0CCA	Port59 - Number of oversized frames received	0 to 4294967295	1	F9	0
0CCC	Port59 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0CCE	Port59 - Number of jabber frames received	0 to 4294967295	1	F9	0
0CD0	Port59 - Number of collisions occured	0 to 4294967295	1	F9	0
0CD2	Port59 - Number of late collisions occured	0 to 4294967295	1	F9	0
0CD4	Port59 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CD6	Port59 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CD8	Port59 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CDA	Port59 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CDC	Port59 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CDE	Port59 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0CE0	Port59 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0CE2	Port59 - Number of dropped received packets	0 to 4294967295	1	F9	0
0CE4	Port59 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0CE6	Port59 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0CE8	Port59 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 38 of 40)

Address	Description	Range	Step	Format	Default
0CEA	Port60 - Number of bytes received	0 to 4294967295	1	F9	0
0CEC	Port60 - Number of bytes sent	0 to 4294967295	1	F9	0
0CEE	Port60 - Number of frames received	0 to 4294967295	1	F9	0
0CF0	Port60 - Number of frames sent	0 to 4294967295	1	F9	0
0CF2	Port60 - Total bytes received	0 to 4294967295	1	F9	0
0CF4	Port60 - Total frames received	0 to 4294967295	1	F9	0
0CF6	Port60 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0CF8	Port60 - Number of multicast frames received	0 to 4294967295	1	F9	0
0CFA	Port60 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0CFC	Port60 - Number of oversized frames received	0 to 4294967295	1	F9	0
0CFE	Port60 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0D00	Port60 - Number of jabber frames received	0 to 4294967295	1	F9	0
0D02	Port60 - Number of collisions occured	0 to 4294967295	1	F9	0
0D04	Port60 - Number of late collisions occured	0 to 4294967295	1	F9	0
0D06	Port60 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D08	Port60 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D0A	Port60 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D0C	Port60 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D0E	Port60 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D10	Port60 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D12	Port60 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0D14	Port60 - Number of dropped received packets	0 to 4294967295	1	F9	0
0D16	Port60 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0D18	Port60 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0D1A	Port60 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0D1C	Port61 - Number of bytes received	0 to 4294967295	1	F9	0
0D1E	Port61 - Number of bytes sent	0 to 4294967295	1	F9	0
0D20	Port61 - Number of frames received	0 to 4294967295	1	F9	0
0D22	Port61 - Number of frames sent	0 to 4294967295	1	F9	0
0D24	Port61 - Total bytes received	0 to 4294967295	1	F9	0
0D26	Port61 - Total frames received	0 to 4294967295	1	F9	0
0D28	Port61 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0D2A	Port61 - Number of multicast frames received	0 to 4294967295	1	F9	0
0D2C	Port61 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0D2E	Port61 - Number of oversized frames received	0 to 4294967295	1	F9	0
0D30	Port61 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0D32	Port61 - Number of jabber frames received	0 to 4294967295	1	F9	0
0D34	Port61 - Number of collisions occured	0 to 4294967295	1	F9	0
0D36	Port61 - Number of late collisions occured	0 to 4294967295	1	F9	0
0D38	Port61 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D3A	Port61 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D3C	Port61 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D3E	Port61 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D40	Port61 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D42	Port61 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D44	Port61 - Number of Mac Error Packets	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 39 of 40)

Address	Description	Range	Step	Format	Default
0D46	Port61 - Number of dropped received packets	0 to 4294967295	1	F9	0
0D48	Port61 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0D4A	Port61 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0D4C	Port61 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0D4E	Port62 - Number of bytes received	0 to 4294967295	1	F9	0
0D50	Port62 - Number of bytes sent	0 to 4294967295	1	F9	0
0D52	Port62 - Number of frames received	0 to 4294967295	1	F9	0
0D54	Port62 - Number of frames sent	0 to 4294967295	1	F9	0
0D56	Port62 - Total bytes received	0 to 4294967295	1	F9	0
0D58	Port62 - Total frames received	0 to 4294967295	1	F9	0
0D5A	Port62 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0D5C	Port62 - Number of multicast frames received	0 to 4294967295	1	F9	0
0D5E	Port62 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0D60	Port62 - Number of oversized frames received	0 to 4294967295	1	F9	0
0D62	Port62 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0D64	Port62 - Number of jabber frames received	0 to 4294967295	1	F9	0
0D66	Port62 - Number of collisions occured	0 to 4294967295	1	F9	0
0D68	Port62 - Number of late collisions occured	0 to 4294967295	1	F9	0
0D6A	Port62 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D6C	Port62 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D6E	Port62 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D70	Port62 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D72	Port62 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D74	Port62 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D76	Port62 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0D78	Port62 - Number of dropped received packets	0 to 4294967295	1	F9	0
0D7A	Port62 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0D7C	Port62 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0D7E	Port62 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0D80	Port63 - Number of bytes received	0 to 4294967295	1	F9	0
0D82	Port63 - Number of bytes sent	0 to 4294967295	1	F9	0
0D84	Port63 - Number of frames received	0 to 4294967295	1	F9	0
0D86	Port63 - Number of frames sent	0 to 4294967295	1	F9	0
0D88	Port63 - Total bytes received	0 to 4294967295	1	F9	0
0D8A	Port63 - Total frames received	0 to 4294967295	1	F9	0
0D8C	Port63 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0D8E	Port63 - Number of multicast frames received	0 to 4294967295	1	F9	0
0D90	Port63 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0D92	Port63 - Number of oversized frames received	0 to 4294967295	1	F9	0
0D94	Port63 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0D96	Port63 - Number of jabber frames received	0 to 4294967295	1	F9	0
0D98	Port63 - Number of collisions occured	0 to 4294967295	1	F9	0
0D9A	Port63 - Number of late collisions occured	0 to 4294967295	1	F9	0
0D9C	Port63 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0D9E	Port63 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0DA0	Port63 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0

Table 20–1: Modbus memory map (Sheet 40 of 40)

Address	Description	Range	Step	Format	Default
0DA2	Port63 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0DA4	Port63 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0DA6	Port63 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0DA8	Port63 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0DAA	Port63 - Number of dropped received packets	0 to 4294967295	1	F9	0
0DAC	Port63 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0DAE	Port63 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0DB0	Port63 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0
0DB2	Port64 - Number of bytes received	0 to 4294967295	1	F9	0
0DB4	Port64 - Number of bytes sent	0 to 4294967295	1	F9	0
0DB6	Port64 - Number of frames received	0 to 4294967295	1	F9	0
0DB8	Port64 - Number of frames sent	0 to 4294967295	1	F9	0
0DBA	Port64 - Total bytes received	0 to 4294967295	1	F9	0
0DBC	Port64 - Total frames received	0 to 4294967295	1	F9	0
0DBE	Port64 - Number of broadcast frames received	0 to 4294967295	1	F9	0
0DC0	Port64 - Number of multicast frames received	0 to 4294967295	1	F9	0
0DC2	Port64 - Number of frames with CRC error	0 to 4294967295	1	F9	0
0DC4	Port64 - Number of oversized frames received	0 to 4294967295	1	F9	0
0DC6	Port64 - Number of bad fragments rcvd(<64 bytes)	0 to 4294967295	1	F9	0
0DC8	Port64 - Number of jabber frames received	0 to 4294967295	1	F9	0
0DCA	Port64 - Number of collisions occured	0 to 4294967295	1	F9	0
0DCC	Port64 - Number of late collisions occured	0 to 4294967295	1	F9	0
0DCE	Port64 - Number of 64-byte frames rcvd/sent	0 to 4294967295	1	F9	0
0DD0	Port64 - Number of 65-127 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0DD2	Port64 - Number of 128-255 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0DD4	Port64 - Number of 256-511 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0DD6	Port64 - Number of 512-1023 byte frames rcvd/sent	0 to 4294967295	1	F9	0
0DD8	Port64 - Number of 1023-MAX byte frames rcvd/sent	0 to 4294967295	1	F9	0
0DDA	Port64 - Number of Mac Error Packets	0 to 4294967295	1	F9	0
0DDC	Port64 - Number of dropped received packets	0 to 4294967295	1	F9	0
0DDE	Port64 - Number of multicast frames sent	0 to 4294967295	1	F9	0
0DE0	Port64 - Number of broadcast frames sent	0 to 4294967295	1	F9	0
0DE2	Port64 - Number of <64 byte fragments w/ good CRC	0 to 4294967295	1	F9	0

20.2.2 Format Codes

- **Bitmap**: 32-bit group of bits, packed into two registers. Encoded in big endian.
- **F1**: 16-bit unsigned integer
- **F2**: Enumeration - power alarm

  0 = power supply good
  1 = power supply fail
- **F3**: Enumeration - OFF/ON

0 = Off
1 = On

- **F4**: Enumeration: port type

  0 = Giga - GBIC
  1 = Copper - TP
  2 = Fiber - 10
  3 = Fiber - 100
  4 = Giga - 10/100/1000 (triple speed)
  5 = Giga - Copper 1000 TP
  6 = Giga - SFP

- **F9**: 32-bit unsigned long
- **String**: A sequence of octets, packed 2 to one register in sequence.

Multilink ML3000/ML3100

Chapter 21: Appendix

21.1 Change Notes

21.1.1 Revision History

Table 21–1: Revision history

Part Number	Revision	Release Date
1601-0049-A1 (New Manual)	5.0	20 September 2012
1601-0049-A2	5.0	25 September 2013
1601-0049-A3	5.0	11 January 2016
1601-0049-A4	5.0	2 May 2016
1601-0049-A4	5.0	2 November 2017

21.1.2 Changes to the ML3000/ML3100 manual

Table 21–2: Major Updates for ML3000/ML3100 Revision A5

Page/Section	Change	Description
N/A	Changed	Branding to Grid Solutions throughout
N/A	Changed	Minor corrections throughout

Table 21–3: Major Updates for ML3000/ML3100 Revision A4

Page/Section	Change	Description
1.2	Changed	Updated order codes for C and L options.

Table 21–4: Major Updates for ML3000/ML3100 Revision A3

Page/Section	Change	Description
3.4.1	Changed	Removed AC power supply references

Table 21–4: Major Updates for ML3000/ML3100 Revision A3

Page/Section	Change	Description
5.4.6	Changed	Corrected definitions of upload and download.
10	Added	Added a note explaining that the VLAN Name field must start with a letter.

Table 21–5: Major Updates for ML3000/ML3100 Revision A2

Page/Section	Change	Description
1.2	Add	order code tables: ML3001, ML3100, ML3101
1.3	Changed	power supply specification to include Fixed and Removable
3.3	Add	suggested unit spacing for heat dissipation
18	Add	PTP 1588 chapter
General	Add	added ML3100 text throughout

21.2 Warranty

21.2.1 GE Multilin Warranty Statement

General Electric Multilin Inc. (GE Multilin) warrants each switch it manufactures to be free from defects in material and workmanship under normal use and service for a period of 24 months from date of shipment from factory.

In the event of a failure covered by warranty, GE Multilin will undertake to repair or replace the relay providing the warrantor determined that it is defective and it is returned with all transportation charges prepaid to an authorized service centre or the factory. Repairs or replacement under warranty will be made without charge.

Warranty shall not apply to any relay which has been subject to misuse, negligence, accident, incorrect installation or use not in accordance with instructions nor any unit that has been altered outside a GE Multilin authorized factory outlet.

GE Multilin is not liable for special, indirect or consequential damages or for loss of profit or for expenses sustained as a result of a relay malfunction, incorrect application or adjustment.

For complete text of Warranty (including limitations and disclaimers), refer to GE Multilin Standard Conditions of Sale.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W