Horizon COMPACT Plus™

Wireless Ethernet
Release 1.0.1

Product Manual - Volume 2
Advanced Configuration Features
Version 1.1

NOTICE

Table of Contents

List of Figures

List of Tables

1.0 User Manual Structure

This user manual is divided into three volumes:

- Volume 1 – Contains an overview of the product, basic configuration, installation and the alignment procedures that are sufficient to set up a link and have it passing traffic. Also, a list of the advanced configuration features.
- Volume 2 (this volume) – includes step-by-step configuration details for the advanced configuration features that are listed in Volume 1.
- Volume 3 – contains a complete list of the frequency tables associated with the radio bands supported by the Horizon Compact Plus
- Volume 4 - Contains configuration details relating to industry standard networking features.

This page left blank intentionally

2.0 Advanced Configuration Features

Volume 1 describes the configuration of the basic features that allow the Horizon Compact Plus to provide a wireless Ethernet link, with a throughput of up to 400 Mbps. A number of advanced configuration features provide enhanced throughput, system access and management security, link protection, quality of service and alarm management. Each advanced feature is described in detail in the following sections.

Note that all redundancy related commands (web, SNMP, CLI) are not supported in this release.

2.1 Dynamic Configuration Change

There are a number of CLI commands that normally require a **save mib** followed by a **reset system** command to take effect. This is disruptive to network traffic. Four commands that normally require this are:

- set radio config
- set ip configuration
- set network management interface
- set vlan tag

These four commands are part of the basic configuration requirements for the system (see Volume 1 of this manual for more information).

Only the Super User can invoke the CLI command **set dynamic config change on/off**. When this feature is turned on, the above four commands can be run and the various associated parameters modified and applied without resetting the system. This has advantages, **but note that if the radio link between two systems is the sole management connection, any changes to the radio configuration parameters (set radio config) on a local system will result in loss of communication and management to the far end system**.

The far end system radio configuration needs to be applied first and then the local system. In this way communicatons across the link can be reinstated and the system brought back up running with the revised radio configuration.

WARNING:

The *set radio config* CLI command may be used to change the radio configuration of an existing working link. If management of the far end Horizon Compact Plus is only via the radio link, then configure the far end radio first. Otherwise, if you change the radio configuration of the near end radio first, you will lose the link to the far end radio and be unable to manage or configure it.

This page is left blank intentionally

3.0 Upgrade/Downgrade Licensed Features

Some of the features described in this manual are only available if a license for the feature(s) is obtained from DragonWave Inc. These are as follows:

1. RLS - Rapid Link Shutdown
2. EOAM, ECFM(802.1ag/Y.1731) – EOAM and ECFM support
3. HAAM – Hitless Automatic Adaptive Modulation

To enable/disable any of these features there are CLI commands that provide information about your system that DragonWave Inc. requires before it can provide you with the necessary license upgrade key, or a refund for a downgraded feature. The first three items in the above list are called the Feature Group and are indexed 1, 2 and 3. These features can be upgraded or downgraded using the "Upgrade/Downgrade Feature Group" procedure. The fourth item in the list is upgraded/downgraded using the "Upgrade and Downgrade System License Speed" procedures.

3.1 Upgrade/Downgrade Feature Group

The following procedure shows what features in the feature group may already be enabled and how they are enabled or disabled.

Procedure 3-1
Upgrade/Downgrade Feature Group

Required Action	Steps
login	Log in using the Super user, or a NOC user, account.
List the licensed features	This command lists the licensed features available. Sequence: **get licensed feature groups** press Enter The system responds: *Index* *Licensed Feature Group* *Is Licensed* *1* *RLS* *No* *2* *EOAM,ECFM(802.1ag/Y.1731)* *No* *3* *HAAM* *No*

Required Action	Steps
List the indexed licensed feature upgrade information. Note that this information needs to be sent to DragonWave Inc. before an upgrade key can be issued. Fees apply to upgrade licenses.	This command lists the licensed features available for the Horizon Compact Plus and also indicates if they are licensed for this sytem. Sequence: **get feature group upgrade information [group index 1 to 3]** press Enter Examples: **get feature group upgrade information 1** press Enter The system responds: *Feature group 'RLS' upgrade request information:* *Count :0* *Unit Serial Number :C1N14AED0013* *MAC Address :00-07-58-03-14-AC* **get feature group upgrade information 2** press Enter The system responds: *Feature group 'EOAM,ECFM(802.1ag/Y.1731)' upgrade request information:* *Count :0* *Unit Serial Number :C1N14AED0013* *MAC Address :00-07-58-03-14-AC* **get feature group upgrade information 3** press Enter The system responds: *Feature group 'HAAM' upgrade request information:* *Count :0* *Unit Serial Number :C1N14AED0013* *MAC Address :00-07-58-03-14-AC* **Note that this information needs to be sent to DragonWave Inc. before an upgrade key can be issued. Fees apply to upgrade licenses.**
Upgrade an indexed feature	Once you have paid for and received the required upgrade key, use this command to upgrade your system. Sequence: **upgrade feature group <group index> <license key>** Example: **upgrade feature group 3 61ba1455c138af096b312efe7f321b98** press Enter The system responds: *This operation will force to save MIB. Continue? Enter Y(Yes) or N(No):**y*** *Feature group 'HAAM' is licensed!*

Required Action	Steps
Downgrade an indexed feature	Use this command to downgrade, or unlicense, a feature. Note, once downgraded you will need another license key from DragonWave in order to re-license a group. Sequence: **downgrade feature group <group index>** Example: **downgrade feature group 3** press Enter The system responds: *This operation will unlicense this feature group. Continue? Enter Y(Yes) or N(No):**y*** *The feature group is unlicensed!* *Feature group 'HAAM' downgrade confirmation information:* *Count :1* *Unit Serial Number :A1316774M090014* *MAC Address :00-07-58-02-92-10* *Confirmation Number :c32d57d9c6765f9df34a99f48dee369d*
Confirm downgrade information	This command will return the downgrade confirmation information, similar to that provided by the **downgrade feature group** command. Sequence: **get feature group downgrade information <group index>** Example: **get feature group downgrade information 3** press Enter *Feature group 'HAAM' downgrade confirmation information:* *Count :1* *Unit Serial Number :A1316774M090014* *MAC Address :00-07-58-02-92-10* *Confirmation Number :c32d57d9c6765f9df34a99f48dee369d*

3.2 Upgrade System License Speed

Upgrading the system licensed speed requires an upgrade license key obtainable from DragonWave. Upgrading the licensed speed does not cause you to lose the ability to reduce the speed and then return to the new licensed speed at a later time.

Note that the throughput of a system (current speed) can be configured to be less than, or equal to, the licensed speed. The actual throughput that the system will operate at is the lesser of the configured current speed and the System Mode.

Procedure 3-2
Upgrading Horizon Compact Plus System License Speed

Required Action	Steps
login	Log in as a NOC user.
View existing licensed and current system speeds	Returns the licensed speed key value, the current set system speed and the set mode. Sequence: **get system speed** press Enter The system responds: *Licensed speed set to : n Mbps* *Current speed set to : n Mbps* *System mode set to : <system mode>* Example: Licensed speed set to :200 Mbps Current speed set to :150 Mbps System mode set to :hy50_285_128qam Note that although the mode shows a speed of 285 Mbps, the actual speed will be limited to the current speed, or the licensed speed, whichever is the lower.

Required Action	Steps
View the information required by DragonWave Inc. in order to process a licensed speed upgrade request.	Returns the information requested by DragonWave for licensed speed upgrade purposes. Sequence: **get licensed speed upgrade information [required speed]** press Enter Example (assuming current licensed speed is 200 Mbps and we wish to increase it to 400 Mbps): **get licensed speed upgrade information 400** The system responds: *Speed upgrade information:* *Speed increment :200* *Speed count :0* *System MAC address :00-07-58-03-14-AC* *Unit serial number :C1N14AED0013* **This information must be sent to DragonWave along with the request for a speed upgrade before a license upgrade key can be issued.**
Upgrade system licensed speed	Upgrades the system to operate at a higher speed. A license upgrade key is required for this command. Contact DragonWave. Sequence: **upgrade system licensed speed [speed] [key]** press Enter Where **[speed]** is the new licensed speed, and **[key]** is the license upgrade key obtained from DragonWave Example – continued from above: **upgrade system licensed speed [400] [xxxxxxxxxxxxxxxxxxxxxx]** press Enter This will upgrade the system license speed from 200 to 400 Mbps.

3.3 Downgrade System License Speed

Downgrading the system license speed to a value lower than previously purchased is supported. Information presented by the system, when downgraded, needs to be sent to DragonWave in order to confirm the status of your license.

NOTE: Once the system license speed has been downgraded, a new license key is required if you wish to return to a higher licensed speed.

Note that the licensed speed is the maximum speed that the system can operate at, regardless of the setting of the System Mode.

Procedure 3-3
Downgrading Horizon Compact Plus System License Speed

Required Action	Steps
login	Log in as a NOC user.
View system speed	Returns the licensed speed value, the current set system speed and the set mode. Sequence: **get system speed** press Enter The system responds: *Licensed speed set to : n Mbps* *Current speed set to : n Mbps* *System mode set to : <system mode>* Example: Licensed speed set to :400 Mbps Current speed set to :400 Mbps System mode set to :hy50_364_256qam

Required Action	Steps
Downgrade system licensed speed	Downgrades the system licensed speed to operate at a lower maximum speed. **Warning: Once you issue this command your current license speed key will be lost and you will not be able to return to your original licensed speed without acquiring another license key from DragonWave.** Sequence: **downgrade system licensed speed [speed]** press Enter Where **[speed]** is the new lower licensed speed in Mbps. Example: d**owngrade system licensed speed 200** The system responds: (Example) *The current system licensed speed will be downgraded to 200 Mbps.* *This operation will force to save Mib. Continue? Enter Y(Yes) or N(No):y* *Saving MIB. Please wait for a while...* *Mib saved successfully.* *The current system licensed speed is downgraded to 200 Mbps.* *Downgrade Confirmation Information:* *Speed Decrement :200* *Speed Count :2* *Unit Serial Number :DW130AAG0100* *MAC Address :00-07-58-00-a2-16* *Confirmation Number :bc7ed7dd89a4d98adbab263630a9a27e* To determine the status of your license, the information shown above, under the heading “Downgrade Confirmation Information”, needs to be sent to DragonWave, along with the current licensed speed count (see next step).
Licensed speed count	This command returns the number of times that the licensed speed has been changed. This value is required by DragonWave, in addition to the information returned in the previous step, in order to determine the status of your license. Sequence : **get licensed speed count** press Enter The system responds : *Licensed Speed Counter is: 3* (Example)

Required Action	Steps
Licensed speed downgrade information	This command returns the licensed speed downgrade information that was presented during the downgrade process. This is the same information, along with the licensed speed count, that DragonWave needs in order to verify the status of your license. Sequence : **get licensed speed downgrade information** press Enter The system responds : (Example) *Downgrade Confirmation Information:* *Speed Decrement :200* *Speed Count :2* *Unit Serial Number :DW130AAG0100* *MAC Address :00-07-58-00-a2-16* *Confirmation Number :bc7ed7dd89a4d98adbab263630a9a27e*

4.0 Configuring Ethernet Ports 1 and 2

The option is available to independently configure the two physical Data ports, Port 1 and Port 2 as two 100/10 Base-t (Fast Ethernet) ports, or as single 1000/100/10 Base-t (Gigabit) ports. A cable splitter is required at the hardware input to Port 1 or Port 2 to provide the physical Fast Ethernet connections. When configured as two Fast Ethenet ports, Port 1 supports ports p1 and p4 and Port 2 supports ports p2 and p3.

Gb Port	Supported Data Rate	Fast E Port	Supported Data Rate
Port 1	1000/100/10 Base-t	p1	100/10 Base - t
		p4	100/10 Base - t
Port 2	1000/100/10 Base-t	p2	100/10 Base - t
		p3	100/10 Base - t

The following parameters can be configured for each of the ports:

Parameter	Gb Port 1	Gb Port 2	Fast Port 1	Fast Port 2	Fast Port 3	Fast Port 4
Port Description	✔	✔	✔	✔	✔	✔
Auto Negotiation	✔	✔	✔	✔	✔	✔
Media	Copper/Fibre	Copper	Copper	Copper	Copper	Copper
Speed Mbps	✔	✔	✔	✔	✔	✔
Optical Transceiver State	✔					
Pause Frame Enable	✔		✔			
Maximum Frame Size	✔	✔	✔	✔	✔	✔
Admin State	✔	✔	✔	✔	✔	✔
Port State					✔	✔

All ports can be configured for data or management.

Procedure 4-1
Ethernet Port Configuration

To configure the Ethernet ports use the following procedure:

Required Action	Steps
login	Log in using the Super user or a NOC account.
View current port configuration	This command displays the current configuration of the ports. Sequence: **get enet config** press Enter The system responds: --- *ETHERNET PORT CONFIGURATION* ========== *Enet Port ID :P1* *Port Descriptor :AnyName* *Auto Negotiation :on* *Port Medium :auto* *Optical Tx State :on* *Pause Frame Enable :off* *Speed :auto* *Max. Frame Size :1600* *Payload State :disable* *Admin State :on* *Enet Port ID :P2* *Port Descriptor :AnyName* *Auto Negotiation :on* *Speed :auto* *Max. Frame Size :1600* *Payload State :enable* *Admin State :on* *Enet Port ID :P3* *Port Descriptor :AnyName* *Auto Negotiation :on* *Speed :auto* *Max. Frame Size :1600* *Payload State :disable* *Port State :off* *Admin State :on* *Enet Port ID :P4* *Port Descriptor :AnyName* *Auto Negotiation :on* *Speed :auto* *Max. Frame Size :1600* *Payload State :disable* *Port State :off* *Admin State :on*

Required Action	Steps
Configure Ports	This command will allow you to configure any of the four possible ports The first example configures Port 1 (p1) as a Gigabit port. Port p4, the second port associated with Port 1, cannot be enabled if p1 is to operate at Gigabit speed. Ports p3 and p4 have been previously disabled in this example. Port p2 cannot be disabled. Note that the information shown in brackets ( ) at the end of each line shows the current configuration. Enter a new configuration and then press Enter, or just press Enter to retain the current value. Note 1: p1 is the only port that supports either a fibre or copper option. Note 2: p1 is the only port that supports pause frames. Sequence: **set enet config** and press Enter The system responds: *#Press 'Ctrl-X' to exit config process* *#Press 'Enter' to retain previous value* *Port Id[P(1-4)] (1) ?**1*** *Port Description ():AnyName* *Auto Negotiation [on(1) | off(2)] (on):* *Medium [copper(1) | fiber(2) | auto(3)] (auto):* *Speed Mbps [10 (1) | 100 (2) | 1000(3) | auto(4)] (auto):* *Optical Transceiver State [on(1) | off(2)] (off):* *Pause Frame Enable [on(1) | off(2)] (off):* *Maximum Frame Size (1600):* *Port Payload State [enable(1) | disable(2)] (disable):**1*** *Port Admin state [on(1) | off(2)] (on):* *Apply the above settings ? Enter yes(y) or no(n)y* --- *ETHERNET PORT CONFIGURATION* ========== *Enet Port ID :P1* *Port Descriptor :AnyName* *Auto Negotiation :on* *Port Medium :auto* *Optical Tx State :on* *Pause Frame Enable :off* *Speed :auto* *Max. Frame Size :1600* *Payload State :**enable*** *Admin State :on* *Enet Port ID :P2* *Port Descriptor :AnyName* *Auto Negotiation :on* *Speed :auto* *Max. Frame Size :1600* *Payload State :enable* *Admin State :on* *Enet Port ID :P3* *Port Descriptor :AnyName* *Auto Negotiation :on* *Speed :auto* *Max. Frame Size :1600* *Payload State :disable* *Port State :off* *Admin State :on* *Enet Port ID :P4* *Port Descriptor :AnyName* *Auto Negotiation :on* *Speed :auto* *Max. Frame Size :1600* *Payload State :**disable*** *Port State :off* *Admin State :on*

Required Action	Steps
Configure ports	The second example configures physical Port 2 with two 100/10 Base-t circuits p2 and p3. Note that p1 has already been configured as a GigE port as per the first example, which leaves p4 disabled. After configuring p2, repeat the procedure for p3. Sequence: **set enet config** and press Enter The system responds: *#Press 'Ctrl-X' to exit config process* *#Press 'Enter' to retain previous value* *Port Id[P(1-4)] (1) ? 2* *Port Description ():* *Auto Negotiation [on(1) | off(2)] (on):* *Speed Mbps [10 (1) | 100 (2) | 1000(3) | auto(4)] (100):* *Maximum Frame Size (1600):* *Port Payload State [enable(1) | disable(2)] (disable):* *Port Admin state [on(1) | off(2)] (on):* *Apply the above settings ? Enter yes(y) or no(n)y* --- *ETHERNET PORT CONFIGURATION* ========== *Enet Port ID :P1* *Port Descriptor :AnyName* *Auto Negotiation :on* *Port Medium :auto* *Optical Tx State :on* *Speed :auto* *Auto Mdix :on* *Pause Frame Enable :off* *Max. Frame Size :1600* *Payload State :enable* *Admin State :on* *Enet Port ID :P2* *Port Descriptor :AnyName* *Auto Negotiation :on* *Speed :auto* *Auto Mdix :on* *Pause Frame Enable :off* *Max. Frame Size :1600* *Payload State :enable* *Admin State :on* *Enet Port ID :P3* *Port Descriptor :AnyName* *Auto Negotiation :on* *Speed :auto* *Auto Mdix :on* *Pause Frame Enable :off* *Max. Frame Size :1600* *Payload State :**enable*** *Port State :off* *Admin State :on* *Enet Port ID :P4* *Port Descriptor :AnyName* *Auto Negotiation :on* *Speed :auto* *Auto Mdix :on* *Pause Frame Enable :off* *Max. Frame Size :1600* *Payload State :disable* *Port State :off* *Admin State :on*
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

5.0 Synchronous Ethernet (SyncE)

Ethernet has rapidly overtaken legacy communication technologies such as TDM, ATM and SONET/SDH within the carrier infrastructure. Ethernet is a packet based technology, which, originally, was incapable of carrying technologies requiring the transfer of accurate synchronization and clock distribution such as that required for the legacy technologies noted above. With the introduction of Synchronous Ethernet (SyncE) features, Ethernet networks are now able to provide the same level of quality and reliability as legacy technologies for use in carrier class applications.

The DragonWave Horizon Compact Plus supports SyncE to ITU/T G.8262 specifications.

Typical third party applications that can use SyncE are:

- Cellular base station synchronization
- Real time video and teleconferencing
- TDM network extension over Ethernet

SyncE allows accurate clock synchronization information to be transmitted over a DragonWave wireless Ethernet link, allowing the Horizon Compact Plus to support synchronous applications, end to end and port to port.
In order to make use of syncE, any synchronous third party product will need to take its timing information from an Ethernet port. Note that Horizon Compact Plus does not have a BITS or other direct clock output.

5.1 Master/Slave

In a Gigabit Ethernet connection, one end device always becomes the Ethernet clock master, and the other becomes the Ethernet clock slave. This happens automatically as part of Ethernet autonegotiation. On the Horizon Compact Plus, when 1000 Mbps (GigE) ports are selected as syncE member ports, the clock master/slave status of the Ethernet port concerned is automatically forced to correspond. Ethernet ports that are defined as syncE primary, or secondary, sources to the Horizon Compact Plus, are forced to appear as Ethernet clock slaves to the connected Ethernet devices, so that the connected device sources the clock to the Horizon Compact Plus. Similarly, syncE member ports which are not defined as clock sources for the Horizon Compact Plus become Ethernet clock masters, so they can send out the clock.

Any connected Ethernet device which autonegotiates master/slave status, will establish an Ethernet link as usual. However, if the far end Ethernet device also has its clock master/slave status forced to the same type as the Horizon Compact Plus port, an Ethernet link will not be established. For instance, if two Horizon Compact Plus Ethernet ports are both syncE members, and not syncE primary or secondary clock sources, then these ports are both forced to be GigE clock sources, so will not establish an Ethernet link if connected by an Ethernet cable.

For 100baseT connections, this is not a consideration, because clock information always flows both ways simultaneously on a 100baseT Ethernet clock link.

5.2 Wander Filter

To cope with potential clock drift, Ethernet systems may use optional additional wander filtering to maintain clock accuracy. There are two wander filter options – Ethernet Equipment Clock (EEC) Option 1 and EEC Option 2. The performance of these options is governed by ITU-T G.8262 standard. Option 1 is based on E1 hierarchy (Europe and Asia) and Option 2 on T1 hierarchy (predominantly North America). Ethernet systems close to the edge of the network may not need the additional filtering, but those further into the network may need it to maintain clock accuracy.

5.3 Configuring SyncE

Procedure 5-1
Configuring syncE

All the commands in the following procedure are immediately invoked. There is no need to perform a **save mib** or **reset system** to make the feature active.

Required Action	Steps
login	Log in using the Super user, NAC or an Admin account.
View current status of SyncE	This command returns the current status of the SyncE feature Sequence: **get synce status** press Enter The system responds: *Synce mode is off* OR, if SyncE mode is active (example): *Synce mode :auto* *Clock source :freerun* *Acquisition status :acquired* *Forced holdover :off*
Add ports that are to be used for SyncE to the member group	This command allows you to add all the ports that are required to handle SynchE into the member port group. Note that in order to configure the ports that are to be the primary and secondary clock sources, the ports must first be made part of the member port group. Sequence: **set synce member port [p1|p2|p3|p4|wp1|freerun]** Example: **set synce member port p4,wp1** press Enter (note the comma) The system responds: *synce members:p4,wp1,freerun* *Note: valid synce member port includes p1,p2,p3,p4,wp1; freerun is always a synce member.*

Required Action	Steps
Select the port that will be the primary (master) synchronization clock source	This command allows you to select which port is to be the primary clock source. Note that in order to configure the primary clock source port, the port must first be made part of the member port group and be configured as GigE (1000 Mbps), or 100BaseT (100 Mbps). Note, also, that if port p1 is an SFP port it cannot be used as a clock source. Sequence: **set synce primary source [p1|p2|p3|p4|wp1|freerun]** Example: **set synce primary source wp1** press Enter The system responds: *Synce mode : off* *Primary clock source : wp1* *Secondary clock source : freerun* *Synce members : p4,wp1,freerun* *Revertive mode : off* *Wander filter option :option2*
Select the port that will be the secondary synchronization clock source	This command allows you to select the port that will provide the secondary clock source. It will take over from the primary clock source if the primary clock source fails. Note that in order to configure the port that is to be the secondary clock source the port must first be made part of the member port group and be configured as GigE (1000 Mbps), or 100BaseT (100 Mbps). Note, also, that unless the revertive feature is enabled (**set synce revertive on**), if, after a switch to the secondary clock source, the primary clock source recovers, the system will not automatically switch back from secondary to the primary clock source. Sequence: **set synce secondary source [p1|p2|p3|p4|wp1|freerun]** Example: **set synce secondary source p4** press Enter The system reponds: *Synce mode : off* *Primary clock source : wp1* *Secondary clock source : p4* *Synce members : p4,wp1,freerun* *Revertive mode : off* *Wander filter option :option2*

Required Action	Steps
Enable or disable the revertive mode	This command allows you to enable or disable the revertive mode. On a primary clock source failure and provided that the SyncE mode is configured for **auto**, when revertive mode is enabled (on), it allows the system to automatically revert back from the secondary to the primary clock source, once the primary clock source has recovered and remains stable for a selected **time** in seconds. Time range is 30 to 300 seconds. The default **time** is 30 seconds. Sequence: **set synce revertive [on|off][time]** press Enter The system responds (example set to "on" with no time entered): *Synchronous Ethernet revertive mode: on, wait time 30 sec.*
Select the Wander Filter Option	This command allows the user to select either Ethernet Equipment Clock filter Option 1, or Option 2. Option 1 would be used in the E1 TDM hierarchy and Option 2 in the T1 TDM hierarchy. Option 2 is the default. Sequence: **set synce wander filter [option1|option2]** press Enter The system responds (example – option2 selected): *Synce mode :off* *Primary clock source :wp1* *Secondary clock source :p4* *Synce members :p4,wp1,freerun* *Revertive mode :on* *Wander filter option :option2*
Enable SyncE feature	Use this command to enable SyncE. Select **manual** when you want the system to go into holdover when the primary clock source fails. If the primary source recovers, the system will automatically switch back to the primary source. Select **auto** if you want the system to switch to the secondary clock source if the primary clock source fails. In **auto** the system will **not** switch back to the primary if the primary clock recovers, unless **set synce revertive on** is enabled. Sequence: **set synce mode [off|manual|auto]** The system responds (example set to auto): *Synce mode : auto* *Primary clock source :wp1* *Secondary clock source :p4* *Synce members :p4,wp1,freerun* *Revertive mode :on* *Wander filter option :option2*

Required Action	Steps
View current SyncE configuration	Use this command to return the current SyncE configursation settings. Sequence: **get synce config** press Enter The system responds: *Synce mode : auto* *Primary clock source : wp1* *Secondary clock source: p4* *Synce members : p4,wp1,freerun* *Revertive mode : on* *Wander filter option :option2*
Required for troubleshooting only. Forcing SyncE into holdover mode	This is a user troubleshooting command which forces the system into holdover mode for a configurable timeout value (**time**) in seconds. The default timout is 30 seconds. Values can be 0 to 300 seconds. 0 keeps the holdover on indefinitely. Sequence: **set synce forced holdover [on [time]|off]** Example: **set synce forced holdover on 60** press Enter The system responds: *Synchronous Ethernet is put into holdver for 60 sec.* **get synce status** press Enter The system responds: *mode: auto* *clock source: wp1* *acquisition status: holdover* *forced holdover: on* *remaining time in forced holdover: 52 sec*

6.0 RADIUS Server User Authentication

The DragonWave Remote Authentication Dial In User Service (RADIUS) server option enables users to be centrally authenticated before being allowed access to a modem. This adds another layer of security by removing user access control away from individual modems and moving it to a central server.

Up to five (5) RADIUS servers can be configured.

When one, or more, RADIUS server is configured, the username and password authentication system on the modem is bypassed, in favour of the RADIUS system. If, on attempting to log in, a user does not receive a response from a configured RADIUS server, the user will not be allowed to log in. This could be the case if the server was off line. However, the system can be configured to allow the Super user to still access the modem via the local modem access control, even when a RADIUS server does not respond.

Only the Super user can issue any of the RADIUS "set" commands and view any of the security related entries returned with "get" commands (passwords, shared key etc..)

Procedure 6-1
RADIUS Server User Authentication

Use this procedure to set up user authentication using a RADIUS server and enable the Super user to access a modem if the RADIUS server does not respond.

Note: To perform this procedure, you must be logged into the system as the Super user.

Required Action	Steps
login	Log in using the Super user account.
View radius servers	Returns a list of RADIUS servers already configured on the system. Sequence: **get radius servers** press Enter The system responds: *index active_host active_key cfgd_host cfgd_key* ===== ========== ========== ========== ========== *1 192.168.1.48 testing123 192.168.1.48 testing123* *2 192.168.1.20* *3* *4* *5* Note that the second radius server is not active because the radius key has not been configured.

Required Action	Steps
Configure radius server host	This command sets up a RADIUS server host. Note that once the RADIUS server host details have been entered, the server key has to be entered before the server becomes active (see next command). Sequence: **set radius server host [index] [ip address]** press Enter Where [index] is the server index 1…5 and [ip address] is the ip address of the RADIUS server concerned The system responds: *Host set. When server Host and Key are set, 'save mib'.*
Configure radius server key	Adds the required shared key to the RADIUS server host configuration. Note that the previous command has to be issued and the server key entered before the RADIUS server will become active. Sequence: **set radius server key [index] [someString]** press Enter Where [index] is the server index 1…5 and [someString] is an alpha-numeric string of up to 32 characters in length. The system responds: *Key set. When server Host and Key are set, 'save mib'.*
View radius servers	Check that servers have been set up correctly by issuing this command Sequence: **get radius servers** press Enter The system responds: *index active_host active_key cfgd_host cfgd_key* *===== ========== ========== ========== ==========* *1 192.168.1.48 testing123 192.168.1.48 testing123* *2 192.168.10.51 password4 192.168.10.51 password4* *3* *4* *5*

Required Action	Steps
Configure radius super user authentication	This commands enables or disables the Super user from accessing a modem, when the RADIUS server does not respond, or is not available. If set to “off” the Super user is allowed to log in using the name and password set in the modem. The default setting is “off”. Sequence: **set radius super user authentication strict [on/off]** press Enter The system responds: *Radius authentication for Super User is now [strict/not strict]* A save mib command will make this command effective immediately. WARNING: If super user authentication is set to ON, and the Super user name and password are not entered into the RADIUS system, the Super user will not be able to regain access to the modem after a reset.
View radius super user authentication strict	This command returns the status of the radius super user. Sequence: **get radius super user authentication strict** press Enter The system responds: *Radius authentication for Super User is [strict/not strict]* *(not strict means SU flash password still works under Radius)*

6.1 Configuring the RADIUS Server

To support the DragonWave RADIUS application, each RADIUS server on the network must be provided with a Vendor Specific Attribute (VSA) file. The VSA file contains the definition of the DragonWave user privilege level (Admin, NOC, Super-User) allocated to users. User definitions can use the DragonWave-Privilege-Level attribute to assign access privileges. If the VSA is missing, then the RADIUS logs the user in at an Admin level only. If a VSA is present, but is invalid, then access is denied.

A typical VSA file is shown below. Without the DragonWave-Privilege-Level attribute AND with “radius super user strict on”, users cannot gain access to the device using CLI.

Note that the Web server does not use RADIUS authentication at all. If you want the system to be 100% RADIUS secured, then you need to disable the Web server (set web server off).

```
#########################################################################
##
#    DragonWave VSAs
#
#########################################################################
#

VENDOR          DragonWave                  7262

BEGIN-VENDOR    DragonWave

# Used to determine the user login privilege level.
ATTRIBUTE  DragonWave-Privilege-Level              1          integer

#       Read-only access.
VALUE   DragonWave-Privilege-Level      DragonWave-Admin-User   1

#       Limited read-write access.
VALUE   DragonWave-Privilege-Level      DragonWave-NOC-User     2

#       Unlimited read-write access.
VALUE   DragonWave-Privilege-Level      DragonWave-Super-User   3

END-VENDOR DragonWave
```

7.0 Management VLAN Tagging

Note: The configuration of Horizon Compact Plus VLAN tagging is only necessary if you wish to restrict Horizon Compact Plus management communications to a specific management VLAN.

The Horizon Compact Plus system will pass user VLAN traffic transparently, independent of the Horizon Compact Plus Management VLAN settings. The VLAN settings are for Horizon Compact Plus management purposes and do not affect user data traffic.

7.1 VLAN Tagging Overview

A Local Area Network (LAN) is a single–broadcast domain. If a user broadcasts information on the LAN, every other user on the LAN receives the broadcast.

A network manager can create smaller broadcast domains and reduce network broadcasts by logically segmenting a LAN into different broadcast domains. These broadcast domains are called Virtual Local Area Networks (VLANs). Workstations on a VLAN do not have to be physically located together because they are segmented logically and not physically.

VLANs offer a number of advantages over traditional LANs including:

- performance
- security
- formation of virtual workgroups
- cost reduction

All ports on a switch are configured for a default VLAN (usually VLAN1). When a switch receives data from a workstation, the switch tags the data with a VLAN identifier that indicates the originating VLAN. The switch sends the data to the ports inside the VLAN where the data originated. The switch also sends the data to a trunking port if one is available.

Network Administrators create VLAN groups and place backbone network devices into the VLAN group to simplify administration and increase security of the devices. VLAN tagging allows network administrators to add Horizon Compact Plus nodes to the administrative network. VLAN tagging restricts administrative access to devices that are members of the VLAN group.

7.2 802.1Q Tagging

VLAN Standard: IEEE 802.1q Draft Standard. The Institute of Electrical and Electronic Engineers (IEEE) is working on a draft standard 802.1q for virtual local area networks. Currently, most products are proprietary. This means that if you wish to install VLANs, you may have to purchase all products from the same vendor. DragonWave implements Horizon Compact Plus VLAN Tagging using the IEEE 802.1q standard. For more information on the Standard, see the Web page:

http://grouper.ieee.org/groups/802/1/pages/802.1Q.html

7.3 VLAN Tagging Implementation in Horizon Compact Plus

The Horizon Compact Plus system will pass user VLAN traffic transparently, independent of the Horizon Compact Plus VLAN settings. The VLAN settings are for Horizon Compact Plus management purposes and do not affect user data or traffic. Note that the Horizon Compact Plus system handles Ethernet packet sizes up to 9600 bytes.

There are two parameters associated with Horizon Compact Plus VLAN tagging:

1. Enable or disable VLAN tagging (set VLAN tagging [on/off])
2. Identify the VLAN tag id to be used with Horizon Compact Plus (set VLAN tag [tag id])

7.4 Horizon Compact Plus VLAN Settings

The following tables describe the behavior of Horizon Compact Plus management packets with respect to VLAN settings on the Horizon Compact Plus system.

Table 7-1
VLAN tagging is OFF

In this configuration VLAN tagging is OFF, therefore no Horizon Compact Plus packets contain VLAN tags.

Condition	Horizon Compact Plus Outgoing Packet
Horizon Compact Plus incoming packet does NOT contain a VLAN tag	Horizon Compact Plus responds to the packet. There is no VLAN tag inserted.
Horizon Compact Plus incoming packet contains a VLAN tag	Horizon Compact Plus does not respond to the incoming packet. Horizon Compact Plus will not respond to packets that have a VLAN tag.
Horizon Compact Plus generates a packet (e.g. SNMP Trap)	There is no VLAN tag inserted.
FTP Server, SNMP Manager, SNMP Trap Hosts are NOT on a VLAN	Servers are reachable by Horizon Compact Plus.
FTP Server, SNMP Manager, SNMP Trap Hosts are on the same VLAN as Horizon Compact Plus	Servers are NOT reachable by Horizon Compact Plus since Horizon Compact Plus does not insert a VLAN tag into the packet.

Table 7-2
VLAN tagging is ON.

In this configuration VLAN tagging is ON, therefore ALL Horizon Compact Plus packets must contain VLAN tags.

Condition	Horizon Compact Plus Outgoing Packet
Horizon Compact Plus incoming packet does NOT contain a VLAN tag	Horizon Compact Plus does not respond to the packet. Horizon Compact Plus will only respond to packets that contain the appropriate VLAN tag.
Horizon Compact Plus incoming packet contains a VLAN tag	Horizon Compact Plus responds to the packet if the VLAN tag matches the Horizon Compact Plus programmed VLAN tag.
Horizon Compact Plus generates a packet (e.g. SNMP Trap)	Horizon Compact Plus inserts the programmed VLAN tag in the response.
FTP Server, SNMP Manager, SNMP Trap Hosts are NOT on a VLAN	Servers are NOT reachable by Horizon Compact Plus. Horizon Compact Plus does not insert a VLAN tag into the packet but the target has been programmed for VLAN.
FTP Server, SNMP Manager, SNMP Trap Hosts are on the same VLAN as Horizon Compact Plus	Servers are reachable by Horizon Compact Plus since they have the matching VLAN tag.

Procedure 7-1
Enable VLAN tagging

Perform this procedure to enable VLAN tagging for the Horizon Compact.

Note: To perform this procedure, you must have NOC user rights.

Required Action	Steps
login	Log in as a NOC user.
View vlan tagging	Displays the VLAN tagging operational state for the system. Sequence: **get vlan tagging** press Enter The system responds: *VLAN tagging: [off | on]*
Configure vlan tagging	Sets the VLAN tagging operational state for the system. Sequence: **set vlan tag** press Enter The system responds: *#Press 'Ctrl-X' to exit config process* *#Press 'Enter' to retain previous value* *VLAN tagging [on(1) | off(2)] (off): 1* *Vlan Id [1 – 4095] (1):* *Vlan Priority [0 – 7] (0)* *Would you like to save MIB ? Enter Y(Yes) or N(No): n* *Mib is not saved. Configuring management vlan…* *Config Name User Config Running Config* *---------- ---------- ----------* *Vlan Tagging : on on* *Vlan Id : 1 1* *Vlan Priority : 0 0* **Note:** If the **set dynamic config change on** command has been applied the system responses to the **set vlan tag** command are different and a **reset system** command **will** need to be applied before the setting will take effect.

Required Action	Steps
Reset system	A system reset is required to activate this feature. Sequence **reset system** press Enter The system responds: *Are you sure you want to reset? Y(yes) or N(no)* press **Y** The system will proceed to reset. You will have to log on again to regain access.

This concludes the steps to enable VLAN tagging for the Horizon Compact Plus system using the CLI manager.

8.0 Quality of Service (QoS)

QoS implementation is best done on the ingress and egress portions of the transport network. As such, QoS should be implemented on the Ethernet switches. Once that implementation is in place, the Horizon Compact Plus can be configured for QoS, should the potential for congestion exist.

The Horizon Compact Plus has two physical GigE ports (10/100/1000 Base-T). Each port can also be independently reconfigured as two fast Ethernet ports (10/100 Base-T). Incoming packets from each port are multiplexed into a single stream, with port identifiers added to each packet. Several different types of packet are supported.

8.1 Class of Service Types

Enabling QoS on Horizon Compact Plus (**set qos [on|off]**) ensures that incoming packets are handled with a priority based on the Class of Service (CoS) bits embedded in several types of data packet. Each port can be independently configured for the type of data packet it is to process. Either VLAN (802.1p) packets, Super VLAN (Q-in-Q, or double tagged) packets, or the DSCP field in IPv4 and IPv6 packet headers, and MPLS EXP can be selected.

For Super VLAN (or Q-in-Q) packets, since a standard VLAN packet is encapsulated within the Super VLAN packet, there may be two sets of CoS bits associated with the Super VLAN packet. One will be the CoS bits of the encapsulated, or inner, VLAN frame (usually associated with the “customer”) and the other will be the CoS bits of the Super VLAN packet itself, or outer, header (usually associated with the “service provider”).

The Horizon Compact Plus can be configured to use the CoS bits of either, Super VLAN inner (cos_qinq_itag), or outer (cos_qinq_otag), packets, or the CoS bits of the standard VLAN, or DSCP bits, or MPLS EXP.

To determine the type of packets on which you wish the packet filter to operate you need to configure the CoS type (**set cos type [cos_vlan|cos_qinq_itag|cos_qinq_otag|cos_dscp|cos_mplsexp]**) for each port.

8.2 Class of Service Bit Levels

The CoS bits have a derived numeric value ranging from 0 to 7, giving eight CoS priority levels. Network administrators can allocate CoS levels to data packets in order to prioritize the types of traffic. The higher the level, the higher the priority of the packet. For example, video, or VoIP traffic needs to be handled with minimal delay, whereas simple data traffic can tolerate delays in getting to its destination. For this example the video or VoIP packets will be allocated a higher CoS level than that of the data traffic.

8.3 Operation with QoS Disabled

If QoS is disabled in the Horizon Compact Plus system, all incoming user data packets are treated equally and are forwarded on a first-come first-served basis. The system operates on a first-in-first-out (FIFO) basis.

If the Pause Frames feature is enabled, pause frames will be sent to the connected switch when the input buffer is close to being full (internally set threshold). This allows time for the queue to empty prior to more frames being received and thus avoids congestion.

When QoS is enabled, the pause frame feature is not available.

By default, control frames, or slow bridge protocol packets, are always directed to a high priority buffer, ensuring that this type of traffic always has the highest priority compared with that of user data traffic.

8.4 Operation with QoS Enabled

In Horizon Compact Plus, when QoS is enabled, a configurable packet filter directs user data packets to any one of eight QoS queues based on the CoS (priority) levels assigned to each packet. The eight QoS queues are labeled Q1 to Q8.

Slow bridge protocol frames, by default, are directed to the highest priority queue Q8, however, if QoS is enabled, these frames can be directed to any one of the eight QoS queues.

Similarly, if QoS is enabled, any ECFM frames arriving from the network (not originating on the Compact Plus) can be directed to any one of the eight QoS queues. If the ECFM feature is enabled on the node, ECFM flow mapping is overridden and all ECFM frames are directed to the CPU.

Traffic statistics for each queue (Q1 to Q8) can be viewed using **get traffic statistics**.

8.4.1 Assigning User Data to QoS Queues

There are eight QoS Queues within Horizon Compact Plus, numbered Q1 to Q8, with Q8 having the highest priority. On any port any of the eight CoS levels can be assigned to any of the eight QoS Queues. A configurable packet filter (**set cos queue mapping [mapping]**) directs frames to the assigned QoS queue based on the CoS level of that packet. You can configure the system so that packets with a higher CoS level would be directed to a higher queue number.

Any packet arriving with no CoS level assigned to it can be assigned a level (0 – 7) based on the configured default CoS value (**set cos default value [0 though 7**). This CoS level is stripped from the packet after processing through the QoS system.

Once queues are populated with packets, a “scheduler” is responsible for moving queued packets out of the queues in a specific order. The scheduling policy decides the behavior of the scheduler.

8.4.2 Slow Bridge Protocol Frames

Slow bridge protocol frames are those that are destined for the **01-80-C2-00-00-xx** MAC addresses. Examples: STP, RSTP, MSTP LACP, Pause Frames, GARP (GMRP,GVRP), bridge broadcasts, OAM, LLDP, Port based authentication, are all transmitted in an expedited fashion.

By default, slow bridge protocol packets are handled by queue Q8. Q8 is the highest priority queue in the system and it ensures slow bridge protocol packets are passed at the highest priority.

However, when QoS is enabled, Compact Plus can also be configured to direct slow bridge protocol packets to any one of the eight QoS queues, allowing the user to control the priority of slow bridge protocol packets. This feature is called Class of Service Control Flow Mapping. If this feature is not configured, then slow bridge protocol packets are directed only to Q8, regardless of the status of QoS.

Similarly, when QoS is enabled, Compact Plus can be configured to direct ECFM frames arriving over the network (not generated on the node) to any one of the eight QoS queues, allowing the user to control the priority of the ECFM frames. This feature is called Class of Service ECFM Flow Mapping. Note that this feature is overridden if the ECFM feature on the node is enabled and all ECFM frames would be directed to the CPU.

Other frames, such as “keep-alive” frames and MRP frames, that the user determines must be treated with a desired priority, must be assigned a CoS within a connected switch, then assigned to the appropriate QoS queue within Horizon Compact Plus.

Note that you have to be carefull assigning regular user traffic to Q8 as that may starve the slow protocol/ECFM traffic flow if those flows are assigned to Q8.

8.4.3 Committed Information Rate (CIR)

The Horizon Compact Plus system allows the user to assign a percentage of the maximum bandwidth available to the data in each of the eight QoS queues (**set cos queue cir [0-100 0-100 0-100 1-100 0-100 0-100 0-100 1-100]**). The default is 100% for each queue.

The behavior of the CIR is different for the two scheduling policies (Priority Queuing or Weighted Fair Queuing - see Section 8.5). For the priority queuing policy the CIR for each queue can be set to any value up to 100%. The “Expedite” option is not available in the Priority Queuing policy.

For Weighted Fair Queuing, with the expedite feature disabled, the sum of all CIR values in all queues must not exceed 100%. With the expedite feature enabled, the sum of all CIR values in the non expedite queues must not exceed 100%, but each of the expedite queues can be assigned CIR’s up to 100% of system speed.

8.4.4 Committed Burst Size (CBS)

Since IP traffic is “bursty” by nature, the Horizon Compact Plus provides a feature, called QoS queue Committed Burst Size (CBS), to handle Ethernet bursts. The Horizon Compact Plus system contains a data buffer that is used to accommodate bursts of traffic in excess of the user allocated amount as specified through the CIR setting for each queue.

The CBS defines the portion of the total amount of burst buffer available that is allocated to each queue. At GigE rate, there is a total of 100 mS (16 MB) of buffer allocated to QoS queues. Each queue can be allocated a percentage of this memory (**set cos queue cbs [0-100 0-100 0-100 1-100 0-100 0-100 0-100 1-100]**). The default CBS allocation for QoS queues Q1 through Q7 is 12%, with Q8 being allocated 16%. The total percentage assigned to all queues must equal 100%.

The CBS function helps in smoothiong out the bursty input and transmit at the CIR of the queue by queuing the traffic.

The CBS operates as a FIFO for each individual queue. Burst traffic will be queued as it arrives. This may have the effect of creating a short delay for subsequent traffic arriving at that queue if the subsequent traffic is at the CIR level of that queue. Conversely, if the burst is followed by traffic that is less than the CIR level, then no delay should occur.

For example: Q3 has 25% CIR or 25 Mbps on a 100 Mbps link. The Q3 CBS is set to 25% or 25 mS at GigE rate. If Q3 receives a burst of traffic in excess of 25 Mbps then Q3 would continue to transmit at 25 Mbps until the “burst buffer” is empty, regardless of whether or not the traffic source is sending packets. If the traffic source continues to send packets, the packets will be queues whilr the que is emptied at the set CIR. If there is no space in the queue, the incoming packets will be dropped.

8.5 QoS Scheduler Policies

A scheduler services all the queues, Q1 through Q8. Each of the eight queues, Q1 to Q8, is serviced by a scheduler in a manner dependant on one of three selectable queuing policies (**set qos policy [strict_priority | wfq]**).

These policies are:

- Strict Priority Queuing
- Weighted Fair Queuing
- Weighted Fair Queuing Expedite Mode

Regardless of the policy used, Q8 always gets serviced first. However, this is not strictly true if the Cut Through option is enabled.

8.5.1 Cut Through

Any traffic assigned to a Cut Through queue is serviced at the highest priorty (regardless of the order of that particular queue among other priority queues) by stopping the in-transition frames from other queues. If a frame is being forwarded over the air from another queue and traffic arrives on the Cut-Through queue, the transmission of the traffic from the other queue is stopped, and the frames from the Cut through Queue are inserted for transmission. After the transmission of the Cut Through frames is complete, the frames from the other queue which was stopped (i.e. being cut-through) is resumed. This results in extremly low latency and jittter in the Cut Through frames.

In **Priority Queuing** mode any one of the priority queues (Q8 to Q1) can be selected as a cut-through queue.

In **Weighted Fair Queuing**, only when Expedite Mode is on, any one of the configured expedite queues can be selected as a Cut Through queue.

8.5.2 Strict Priority Queuing

If the Strict Priority Queuing policy is enabled in the Horizon Compact Plus system, the scheduling mechanism can be described as follows:

1. Select the highest priority queue (Q8 to Q1) which has a frame in it, and hasn't used up its CIR budget
2. Send that frame

The priority queues are serviced by the scheduler always in the order Q8, Q7, Q6, Q5, Q4, Q3, Q2, Q1 with Q8 always being polled first out of the eight queues.

The operation of the Scheduler is affected by both the user-configurable CIR and CBS settings as described above. In the priority queuing mode the CIR of each of the eight queues may be assigned up to 100% of the system speed (system current speed).

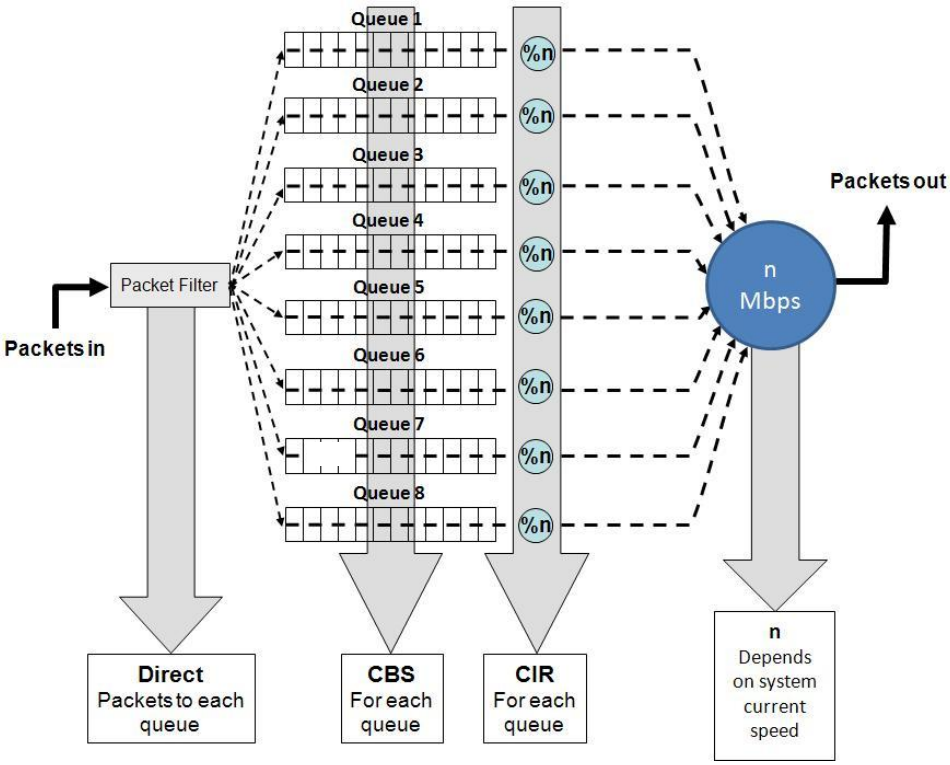


Figure 8-1 CoS Queues can be allocated a CIR and a Committed Burst Size (CBS).

8.5.3 Weighted Fair Queuing (WFQ)

Priority Queuing scheduling has the drawback of wasting bandwidth when any of the bandwidth requirements of the queues are below the set CIR for that queue. Any unused bandwidth allocated to a queue cannot be redistributed to the other queues. Also, there is a possibility of starving the lower priority queues when the higher priority queues are over subscribed. WFQ helps in solving these problems.

In WFQ, each of the queues are assigned a weight (0 – 64). Each queue is also assigned a CIR which guarantees the minimum bandwidth for the traffic in that queue when congestion occurs. The bandwidth is allocated to each queue in proportional to the assigned weight up to the allocated CIR if the queue has packets to send. After the CIR is met, a queue is allocated unused bandwidth (which means all queues have met their CIR, or queues which have not met the CIR don't have any packets queued) proportional to assigned weights.

Note that the sum of all CIRs must not exceed 100%, but can be less if desired. When a queue meets its CIR, it is serviced only when bandwidth is not consumed by the other queues which have not met their CIR. See **Figure 8-2** for a graphical representation of the above statements.

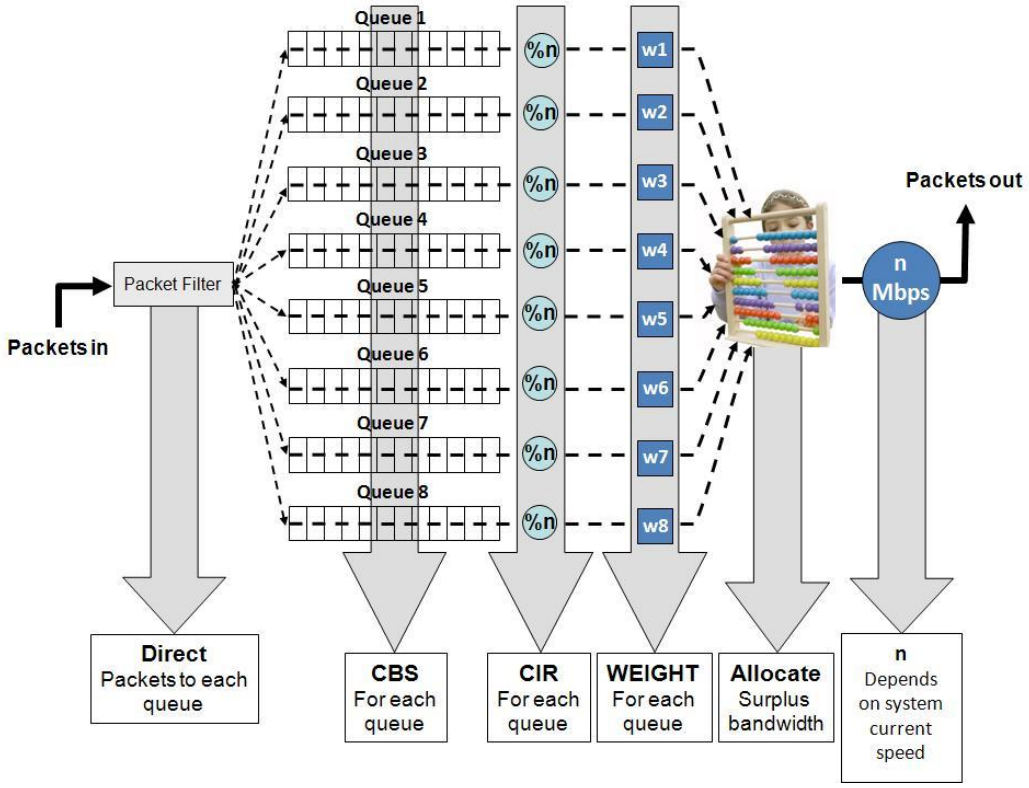


Figure 8-2 Weighted Fair Queuing Concept.

The user sets the CIR and the weight (**set cos wfq weight [w1 w2 w3 w4 w5 w6 w7 w8]** for each queue and the scheduler processes each queue based on those parameters.

Up to four expedite queues (Q8 to Q5) can be configured (see Section 8.5.4).

The queues are serviced in a round-robin fashion (in order Q8, Q7, Q6, Q5, Q4, Q3, Q2, Q1) except for the expedite queue(s) (if enabled) which are serviced with highest priority.

Any queue can utilize any excess bandwidth, proportional to its assigned weight, provided all queues with pending packets have their CIR met.

When all the queues meet their CIR, the remaining bandwidth is distributed amongst the queues, proportional to their weights.

Example:

Each queue, Q1 to Q8, is configured with a weight of w1, w2, w3, w4, w5, w6, w7 and w8 respectively (values 0 – 64). Assuming a total bandwidth capability of 200 Mbps (system current speed), and the CIR for each queue is set to 10% (20 Mbps), this means that there is a surplus bandwidth of 200 – 80 = 120 Mbps if all queues are meeting their CIR. This surplus bandwidth is made available to all queues in a proportion determined by the weight assigned to each queue, if they need it.

The surplus bandwidth share of queues Q1 to Q8 shall be:

Q1 = 120 * w1 / (w1+w2+w3+w4+w5+w6+w7+w8)

Q2 = 120 * w2 / (w1+w2+w3+w4+w5+w6+w7+w8)

Q3 = 120 * w3 / (w1+w2+w3+w4+w5+w6+w7+w8

Q4 = 120 * w4 / (w1+w2+w3+w4+w5+w6+w7+w8)

Q5 = 120 * w5 / (w1+w2+w3+w4+w5+w6+w7+w8)

Q6 = 120 * w6 / (w1+w2+w3+w4+w5+w6+w7+w8)

Q7 = 120 * w7 / (w1+w2+w3+w4+w5+w6+w7+w8)

Q8 = 120 * w8 / (w1+w2+w3+w4+w5+w6+w7+w8)

If Q1 does not have any traffic at a given time then the surplus bandwidth will increase to 120 + 20 = 140 Mbps. The surplus bandwidth share will now be distributed amongst the remaining queues as follows:

Q2 = 140 * w2 / (w2+w3+w4+w5+w6+w7+w8)

Q3 = 140 * w3 / (w2+w3+w4+w5+w6+w7+w8

Q4 = 140 * w4 / (w2+w3+w4+w5+w6+w7+w8)

Q5 = 140 * w5 / (w2+w3+w4+w5+w6+w7+w8)

Q6 = 140 * w6 / (w2+w3+w4+w5+w6+w7+w8)

Q7 = 140 * w7 / (w2+w3+w4+w5+w6+w7+w8)

Q8 = 140 * w8 / (w2+w3+w4+w5+w6+w7+w8)

The benefits of WFQ include :

- the queues are serviced in a fair way
- bandwidth is not wasted when system is not congested.
- CIR to queues is guaranteed.
- The expedite queue, if enabled, will have the highest scheduling priority until the CIR is met.

The peak information rate (PIR) of each queue is the same as the configured system current speed.

8.5.4 Weighted Fair Queuing – Expedite Mode

In the **WFQ** policy, between one and four queues (default is two) (Q8 to Q5 only) can be configured as expedite (priority) queues. This is achieved by enabling the expedite function (**set cos expedite queue [on|off]**) and selecting the required number of priority queues. The traffic directed to the priority queue(s) will now be given priority up to their assigned CIR, but the priority queue(s) will not be able to access any available surplus bandwidth in the system. This will be shared by the remaining non expedite queues based on their weighting values.

Note that all queues that are NOT configured as expedite queues cannot have the sum of all assigned CIR's exceeding 100% of the system current speed. Queues configured as expedite queues can each be assigned a CIR of up to 100% of the system current speed.

Note of caution: It is recommended that the sum of the CIR of all queues, including priority queues, be set to <=100. If this rule is not followed, the WFQ behavior of the queues cannot be guaranteed.

Procedure 8-1
Enable Quality of Service

Perform this procedure to enable Quality of Service for the Horizon Compact Plus.

Note: To perform this procedure, you must have either SuperUser or NOC user rights.

Required Action	Steps
login	Log in as a SuperUser or NOC user.
Enable Quality of Service	Enables or disables (on or off) quality of service (QoS) on the Horizon Compact Plus system. QoS is part of the 802.1P specification. Sequence: **set qos [on|off]** press Enter where **on** will enable QoS and **off** will disable QoS The system responds: *qos is : [on/off]* **get qos** press Enter The system responds: *qos is [on/off]* Default setting is off.

Required Action	Steps
Select the priority bits type to use	Sets the QoS system to use priority bits provided by standard VLAN frames, Super VLAN (Q-in-Q) inner or outer tags, mpls exp, or dscp priority bits. This applies to all configured ports. Sequence: **set cos type [cos_vlan/cos_qinq_itag/cos_qinq_otag/cos_dscp/cos_mplsexp]** press Enter The system responds: *CoS type is set to : cos_vlan/cos_qinq_itag/cos_qinq_otag/cos_dscp/cos_mplsexp* Note: cos_vlan uses the priority tag of standard VLAN frames cos_qinq_itag uses the inner priority tag of a Q-in-Q frame cos_qinq_otag uses the outer priority tag of a Q-in-Q frame cos_dscp uses the 3 bit priority information in the DSCP field of the IP header (also referred to as ToS). cos_mplsexp uses the 3bits of the EXP field in the outer MPLS header of the frame **get cos type** press Enter The system responds (example): *Cos type is : cos_vlan.* *Available cos types in the system are :* *cos_vlan cos_qinq_itag cos_qinq_otag cos_dscp cos_mplsexp.* Default setting: cos_vlan

Required Action	Steps
Assign the CoS priority bits to a queue	Maps each of the incoming 802.1P CoS levels on any enabled port, to any of the eight Horizon Compact Plus QoS Queues. The Horizon Compact Plus system supports all eight 802.1P CoS levels (0-7). Sequence: **set cos queue mapping [port] [x x x x x x x x]** press Enter where **port** can be any enabled port p1, p2, p3, or p4, and each **x** is a value in the range 1 to 8, representing the Horizon Compact Plus QoS Queues allocated to each of the CoS levels (0-7) in order. Any values not explicitly assigned a queue by the user will not be affected by the command. The system responds: *On port (port id) dot1p Queue assignment is as follows :* *dot1p value CoSQueue* *---------- -- ---------* *0 [x]* *1 [x]* *2 [x]* *3 [x]* *4 [x]* *5 [x]* *6 [x]* *7 [x]* *Where [x] is a value in the range 1 to 8* *Examples:* **set cos queue mapping p1 1 1 2 3 4 5 7 7** press Enter For port p1, will allocate CoS levels 0 and 1 to Horizon Compact Plus QoS Queue 1, CoS level 2 to QoS Queue 2, CoS level 3 to QoS Queue 3, CoS level 4 to QoS Queue 4, CoS level 5 to Q5 and CoS levels 6 and 7 to Q7. Note that there is a space between each of the digits in the command. The system responds: *On port p1, dot1p queue assignment is as follows :* *dot1p value CoSQueue* *---------- -- ---------* *0 1* *1 1* *2 2* *3 3* *4 4* *5 5* *6 7* *7 7* *Default value: Q4 for all CoS values.*

Required Action	Steps
Select the QoS policy	Selects the Priority Queuing or Weighted Fair Queuing policy. Sequence: **set qos policy [strict_priority | wfq]** press Enter where **strict_priority** selects Prority Queuing and **wfg** selects Weighted Fair Queuing. The system responds: *Qos is set to : [strict_priority | wfq*] Default value: strict_priority
****Strict Priority Queuing Only**** Set the queue CIR and allocate expedite queues if required	Sets the Committed Information Rate (CIR) for each of the 4 QoS queues. The CIR defines the minimum amount of bandwidth allocated for that queue. Note that queues set as Expedite Queues can override the CIR for other queues should congestion occur. Sequence: **set cos queue cir [%1 %2 %3 %4 %5 %6 %7 %8]** press Enter where **%1 %2 %3 %4 %5 %6 %7 %8** is the percentage of the available bandwidth to be allocated to QoS queues 1 through 8 respectively. The total cannot exceed 100% unless Expedite Queuing has been enabled. The system responds: (example shown using 25% settings for each queue - default) *Expedite queue is :off.* *All queues bandwidth are guaranteed.* *Queue CIR(%) CIR(Mbps)* *1 25 25* *2 25 25* *3 25 25* *4 25 25* *5 25 25* *6 25 25* *7 25 25* *8 25 25* Default value: all queues are allocated 100%
****Strict Priority Queuing Only**** Enable the Cut Through queue as desired	This command enables or disables the Cut Through queue feature. Sequence: **set cos cut through queue [on|off] [queue name (q1 – q8)]** press Enter The system responds: *Cut through state is set to : on|off* *Cut through queue is set to : q1 – q8*

Required Action	Steps
****For Weighted Fair Queuing Only**** Set the queue CIR	Sets the Committed Information Rate (CIR) for each of the 8 QoS queues. The CIR defines the minimum amount of bandwidth allocated for that queue. Sequence: **set cos queue cir [%1 %2 %3 %4 %5 %6 %7 %8]** press Enter where **%1 %2 %3 %4 %5 %6 %7 %8** is the percentage of the available bandwidth to be allocated to CoS Queues 1 through 8 respectively. The total cannot exceed 100% , but can be less than 100% if desired. The system responds: (example shown) *Expedite queue is :off.* *All queues bandwidth are guaranteed.* *Queue CIR(%) CIR(Mbps)* *1 5 5* *2 10 10* *3 10 10* *4 10 10* *5 10 10* *6 10 10* *7 15 15* *8 30 30*

Required Action	Steps
****For Weighted Fair Queuing Only**** If wfq policy is selected, then apply weights to each queue and allocate an expedite queue if required.	Applies weights to each of the four priority queues. The higher the weighting value, the greater the share of surplus bandwidth is allocated to that queue. Sequence: **set cos wfq weight [w1 w2 w3 w4 w5 w6 w7 w8]** press Enter where **w1** is the weighting for QoS queue 1, **w2** is the weighting for QoS queue 2, **w3** is the weighting for QoS queue 3, **w4** is the weighting for QoS queue 4 and so on. All values are integers. Valid weight values 0 – 63. Example w1= 1, w2 = 3, w3 = 5, w4 = 7 etc. The system responds (using the above example and default values for queues Q5 to Q8): *Queue* *Weight* *1* *1* *2* *3* *3* *5* *4* *7* *5* *8* *6* *8* *7* *8* *8* *8* Default values: all queues are allocated a weight of 8

Required Action	Steps
****For Weighted Fair Queuing Only**** Enable the expedite queue function	Enables or disables the expedite queue function. When this option is enabled, the user also selects the desired number of expedite queues. Up to four expedite queues can be configured. The expedite queues will always be selected from Q8 through Q5. Example: if the number of expedite queues is to be 4, Q8, Q7, Q6, and Q5 will be the expedite queues and the rest will be WFQ. If the number of expedite queues is to be 1, then only Q8 will be the expedite queue and the rest will be WFQ. The sum of the CIR of all WFQ queues should not exceed 100. However the expedite queues can be allocated 0-100% bandwidth. The behavior of the WFQ can not be guaranteed if the sum of the CIR's of all queues exceeds 100%. Sequence: **set cos expedite queue [on/off][number of queues]** press Enter Example: set cos expedite on 2 press Enter **get cos expedite queue** press Enter The system responds: *Expedite queue is set to : on* *Number of expedite queue is : 2* *Expedite queue : q8, q7*
****For Weighted Fair Queuing Only**** Enable the Cut Through queue as desired	This command enables or disables the Cut Through queue feature. The expedite function must be enabled before this command can be applied. The queue name must be any one of the configured expedite queues q8 to q5 Sequence: **set cos cut through queue [on|off] [queue name (q8 – q5)]** press Enter The system responds: *Cut through state is set to : on|off* *Cut through queue is set to : q8 – q5*

Required Action	Steps
Set the committed burst size for each queue	Sets the committed burst size for each of the eight QoS queues (and QC if ecfm or control flow mapping is enabled**), as a percentage of the total queue memory available. There is a total of 100 msec worth (16MB) of memory space allocated to QoS queues. A percentage of this space is allocated to each of the eight queues. Sequence: **set cos queue cbs [%1 %2 %3 %4 %5 %6 %7 %8]** press Enter where **%1 %2 %3 %4 *%5 %6 %7 %8** is the percentage of the total queue memory to be allocated to QoS Queues 1 through 8 respectively. Note that the total of all queues must equal 100%. The system responds: *Queue* *Size (%)* *1* *%1* *2* *%2* *3* *%3* *4* *%4* *5* *%5* *6* *%6* *7* *%7* *8* *%8* Example: **get cos queue cbs** press Enter The system responds (default values shown): *Queue* *Size (%)* *1* *12* *2* *12* *3* *12* *4* *12* *5* *12* *6* *12* *7* *12* *8* *16* **set cos queue cbs 6 6 10 10 15 15 16 22** press Enter The system responds: *Queue* *Size (%)* *1* *6* *2* *6* *3* *10* *4* *10* *5* *15* *6* *15* *7* *16* *8* *22*

Required Action	Steps
set the default CoS level for packets not having a level already assigned.	Assigns packets that do not have CoS levels to any one of the eight 802.1p CoS levels (0-7). Sequence: **set cos default value [port name p1-p4] [n]** press Enter where “port name” is any port p1, p2, p3, or p4 and “n” is any number 0 through 7. Example: **set cos default value p1 0** press Enter On port p1, packets without a vlan tag are treated as a CoS value 0. **get cos default value** press Enter The system responds: *Default cos value for packet without vlan tag is as follows:* *port name default cos value* *--------- ----------* *p1 0* *p2 0* *Note: this setting can be applied only to the enabled ports.*
save mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

This concludes the steps to configuring Quality of Service using the CLI manager.

8.6 User Flow Mapping

This feature allows the user to uniquely indentify a particular packet flow and then assign, or map, that flow to a specific queue. In this release there are three predefined flows. The user cannot construct a flow. However, the user can inidividually enable/disable these flows, and when enabled can assign them to a queue. The three flows are;

1. ECFM flow (Ethernet type 8902) without vlan tag
2. ECFM flow with vlan tag
3. Control frames (in the range 01-80-c2-00-xx-xx)

The flow can be mapped to a queue independently on each ethernet port.

Note that user flow mapping is not applicable when QoS is disabled (off).

Procedure 8-2
User flow mapping

Use the following procedure to set up User Flow Maping.

Required Action	Steps
login	Log in as a SuperUser or NOC user.
View the current status of User Flow Mapping	This command returns the current status of User Flow Mapping. Sequence: **get cos user flow** press Enter The system responds (example): *CoS User Flow Queue Mapping* ========== *User Flow | Status | User Class | Port 1 | Port 2* ========== *flow 1 | disable | class 1 | queue 8 | queue 8* ---------- *flow 2 | disable | class 2 | queue 8 | queue 8* ---------- *flow 3 | enable | class 3 | queue 6 | queue 6* ---------- *The user flow mappings are not applicable when QoS is off.*

Required Action	Steps
Configure User Flow Mapping	This command enables you to configure any of the three predefined flows. Sequence: **set cos user flow** press Enter The system responds: *#Press 'Ctrl-X' to exit config process* *#Press 'Enter' to retain previous value* *Flow Id [1-3] (1) ? 1* *Flow Mapping Status [enable(1), disable(2)] (disable) ? 1* *Port 1 User Flow Mapping to Queue (8) ? 7* *Port 2 User Flow Mapping to Queue (8) ? 5* *CoS User Flow Queue Mapping* *==========* *User Flow | Status | User Class | Port 1 | Port 2* *==========* *flow 1 | enable | class 1 | queue 7 | queue 5* *----------* *flow 2 | disable | class 2 | queue 8 | queue 8* *----------* *flow 3 | enable | class 3 | queue 6 | queue 6* *----------* *The user flow mappings are not applicable when QoS is off.*

This page is left blank intentionally

9.0 Pause Frames

Pause frames are generated by the weaker (slower) link when its forward pipe gets full. Pause frames inform the upstream device to “pause and stop sending traffic for a period of a specific ‘quanta’” (refer to ieee 802.3 standard for the definition of ‘quanta’). When the Pause Frame feature is enabled, Horizon Compact Plus generates pause frames to the Ethernet switch when the Horizon Compact Plus receiving buffer hits the internally set threshold. The receiving buffer threshold is close to 100 msec at GigE rate. At data rates lower than GigE, the data buffer will accommodate a lesser amount of data. The Pause Frame feature cannot be used when CoS/QoS is enabled.

When the pause frame feature is enabled the system sends pause frames to an attached network switch. If the system receives a pause frame it is sent transparently over the air to the other end of the link. Pause frames are treated as slow bridge protocol frames (destination MAC 01-80-c2-00-xx-xx) and the same QoS behavior is applied to them as slow bridge protocol frames (see Section 8.4.2.).

The pause frame feature can only be enabled on port p1 and is configured as part of **set enet config command** (see Section 3.0).

This page is left blank intentionally

10.0 Bandwidth Management

When you purchase a Horizon Compact Plus system you receive a unit capable of giving a throughput speed of up to 400 Mbps. However, the actual throughput speed achievable for any given system depends on the specific licensed speed key that you purchased with the system

You can upgrade your system to a higher licensed speed (see Section 3.2) by purchasing an upgrade key and reprogramming your system. Any upgraded system can be reconfigured to a lower system speed (CLI command **set system speed**) as required, without losing the ability to return to the upgraded licensed speed.

You may also downgrade the licensed speed (see Section 3.3) to a lower value. Once downgraded new upgrade keys will be required for future upgrading.

System speeds do not have to be symmetrical (same speed in both directions on the link). Asymmetric speeds (different speeds in each direction) can also be configured.

10.1 Maximum Throughput Speed

The maximum throughput speed is determined by the Horizon Compact Plus licensed speed key you purchase, however, it is important to note that the maximum speed is also determined by the Channel bandwidth associated with the configured radio band, and the modulation scheme used. The channel bandwidth is a function of the radio band and the modulation scheme is selected depending on the desired maximum throughput. Configuring the Radio Band and System Mode determines the maximum throughput capability and the modulation scheme applied.

Note that if a System Mode is set with a maximum throughput capability that exceeds the licensed speed key purchased from DragonWave, then the maximum speed attainable will be limited to the licensed speed purchased. By default the system speed is set to the licensed speed key purchased, however, it can be reduced to a lower level without losing the ability to return to the purchased licensed speed.

Table 10-1 shows some examples of the modulation schemes that are selected for various System Modes (combination of channel bandwidth and average throughput).

Table 10-1 System Mode and Modulation Scheme Example

Modulation scheme	Channel Bandwidth 50 MHz			Channel Bandwidth 40 MHz			Channel Bandwidth 30 MHz		
	Throughput Mbps	TX Power dB	RX Sensitivity dB	Throughput Mbps	TX Power dB	RX Sensitivity dB	Throughput Mbps	TX Power dB	RX Sensitivity dB
QPSK	66	23.7	-83.2	52	23.7	-84.2	39	23.7	-85.5
16 QAM	154	21.1	-75.8	122	21.1	-76.8	92	21.1	-78.1
32 QAM	198	21.4	-72.5	157	21.4	-73.5	118	21.4	-74.8
64 QAM	241	20.0	-69.4	192	20.0	-70.4	144	20.0	-71.7
128 QAM	285	19.4	-66.3	227	19.4	-67.3	170	19.4	-68.6
256 QAM	329	19.5	-63.4	262	19.5	-64.4	196	19.5	-65.7
256 QAM (2)	351	19.5	-61.0	279	19.5	-62.0	209	19.5	-63.2
Modulation scheme	**Channel Bandwidth 55/56 MHz**			**Channel Bandwidth 28 MHz**			**Channel Bandwidth 14 MHz**		
	Throughput Mbps	**TX Power dB**	**RX Sensitivity dB**	**Throughput Mbps**	**TX Power dB**	**RX Sensitivity dB**	**Throughput Mbps**	**TX Power dB**	**RX Sensitivity dB**
QPSK	71	23.7	-82.9	38	23.7	-85.7	19	23.7	-88.7
16 QAM	166	21.1	-75.5	88	21.1	-78.3	43	21.1	-81.3
32 QAM	214	21.4	-72.2	113	21.4	-75.0	56	21.4	-78.0
64 QAM	261	20.0	-69.1	138	20.0	-71.9	68	20.0	-74.9
128 QAM	308	19.4	-66.0	163	19.4	-68.8	80	19.4	-71.8
256 QAM	356	19.5	-63.1	188	19.5	-65.9	93	19.5	-68.9
256 QAM (2)	380	19.5	-60.6	201	19.5	-63.4	99	19.5	-66.5

Procedure 10-1
Configure Horizon Compact Plus Throughput Speed (Symmetrical Throughput)

Required Action	Steps
login	Log in as a NOC user.
View system speed	Returns the licensed speed key value, the current set system speed and the set mode. Sequence: **get system speed** press Enter The system responds: *Licensed speed set to : n Mbps* *Current speed set to : n Mbps* *System mode set to : <system mode>* Example: *Licensed speed set to :50 Mbps* *Current speed set to :50 Mbps* *System mode set to :hy50_67_qpsk* Note that although the mode shows a speed of 67 Mbps, the actual speed will be limited to the current speed, or the licensed speed, whichever is the lower.
View system mode	Returns the current system mode and a list of available system modes. Sequence: **get system mode** press Enter System responds: *Current system mode is :hy50_67_qpsk* (Example) *System modes available in the system:* *cw_test hy50_67_qpsk hy50_110_16qam* *hy50_171_32qam hy50_215_64qam hy50_271_128qam* *hy50_322_256qam hy50_371_256qam*

Required Action	Steps
Configure system mode	Sets the system mode (channel bandwidth, maximum throughput speed and modulation scheme). You can only select any one of the modes shown as available when the **get system mode** command is used. Sequence: **set system mode < hy[bandwidth]_[throughput]_[modulation]>** Where **[bandwidth]** is the channel bandwidth of the configured radio band; **[throughput]** is the maximum throughput capability in Mbps; **[modulation]** is the modulation scheme. Example: **set system mode hy50_67_qpsk** press Enter (50 MHz channel bandwidth, 67 Mbps throughput and QPSK modulation. System responds: *System mode set to :hy50_67_qpsk*
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*
Reset system	A system reset is required to activate this feature. Sequence **reset system** press Enter The system responds: *Are you sure you want to reset? Y(yes) or N(no)* press **Y** The system will proceed to reset. You will have to log on again to regain access.

Note that all required radio parameters need to be correctly set for the system to be functional. See Volume 1 of this manual for basic configuration procedures.

10.2 Asymmetric Throughput Speed

Asymmetric throughput can be achieved by installing the same Horizon Compact Plus hardware type at each end of the link, and configuring one end with a different system speed. Note, that the System Mode, must be identical at each end of the link for this to work. The variable will be the system speed figure.

Procedure 10-2
Configure Horizon Compact Plus Throughput Speed (Asymmetric)

Required Action	Steps
login	Log in as a NOC user.
View system mode	Returns the current system mode and a list of available system modes. Sequence: **get system mode** press Enter System responds: *Current system mode is :hy50_67_qpsk* (Example) *System modes available in the system:* *cw_test* *hy50_67_qpsk* *hy50_110_16qam* *hy50_171_32qam* *hy50_215_64qam* *hy50_271_128qam* *hy50_322_256qam* *hy50_371_256qam*
Configure system mode	Sets the system mode (channel bandwidth, maximum throughput speed and modulation scheme). Sequence: **set system mode <hy[bandwidth]_[throughput]_[modulation]>** Example: **set system mode hy50_110_16qam** press Enter (50 MHz channel bandwidth, 110 Mbps throughput and 16QAM modulation. System responds: *System mode set to :hy50_110_16qam* Note: For asymmetric speeds, the system mode must be set identically at each end of the link.

Required Action	Steps
Configure system speed	Sets the system speed. (Cannot exceed the speed key purchased with your system). Sequence: **set system current speed 50** press Enter System responds: *System speed set to 50 Mbps* Note**:** For asymmetric speeds the speed at the other end of the link would be set to a different value. Example: Near end – **set system current speed 50** press Enter Far end – **set system current speed 100** press Enter Note: if the speed at one end was to be the purchased speed (default), then this command would not need to be invoked at that end.
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*
Reset system	A system reset is required to activate this feature. Sequence **reset system** press Enter The system responds: *Are you sure you want to reset? Y(yes) or N(no)* press **Y** The system will proceed to reset. You will have to log on again to regain access.

10.3 Throughput (Bandwidth) Logging

As discussed earlier, the maximum throughput speed, or bandwidth, of a system is determined by the purchased licensed speed key. This allows a service provider to provide a limited bandwidth and to bill for it accordingly.

Another billing method is to use Bandwidth Logging. This feature monitors bandwidth consumption over time and the customer would be billed for the actual bandwidth consumed and not for a preset maximum bandwidth. As with the speed key, you will need to consult with DragonWave Inc. if you wish to make use of this option.

Note that Horizon Compact Plus does not support Bandwidth Logging in the “secondary_hsb_1wire” redundancy mode, or the “secondary_x2” wireless link aggregation mode (WLAG).

The Bandwidth Logging feature creates records that indicate the bandwidth utilization over a set reporting period. At the end of the reporting period the record is written to flash. Up to 60 records can be stored in flash memory. After 60 records have been written, the oldest records are overwritten. Each record (0 through 59) represents the bandwidth utilization accrued over a 24 hour period and may be selectively viewed. A record that is currently being accrued may also be viewed.

The bandwidth logging report generator will be restarted when the user changes the utilization threshold bin counters. That means that the next report will come 24 hours following the utilization threshold change.

The bandwidth utilization is computed as the egress speed (i.e. the peer’s egress speed) divided by the current speed of the link. It is important to note that the bandwidth utilization will be affected by changes to the current speed. In general, when the current speed is halved the bandwidth utilization is doubled.

Procedure 10-3
Bandwidth Logging

Required Action	Steps
login	Log in as the Super User.
Configure bandwidth record thresholds	Up to ten bandwidth utilization thresholds can configured. This command will set the bandwidth utilization threshold integers as a percentage. The ten integers are entered separated by spaces. The values shown below are the default. Sequence: **set bandwidth record thresholds 10 20 30 40 50 60 70 80 90 95** press Enter The system responds: *Bandwidth Utilization Thresholds set to: 10 20 30 40 50 60 70 80 90 95* Note that the average period and the reporting period are preset values.

Required Action	Steps
View bandwidth record thresholds	This command returns the bandwidth record settings. Sequence: **get bandwidth record thresholds** press Enter The system responds: *Bandwidth Utilization Thresholds:* *10 20 30 40 50 60 70 80 90 95*
Start bandwidth logging	This command turns logging on or off. Note that reports are saved to flash memory irresepective of whether this is on or off. Sequence: **set bandwidth record logging [on|off]** press Enter The system responds: *Bandwidth utilization logging to both event log and syslog set to 'on|off'*
View status of bandwidth logging	This command will return the logging status. Sequence: **get bandwidth record logging** press Enter The system responds: *Bandwidth logging to syslog and flashlog set to 'on|off'*
View the administrative status of bandwidth logging	The command will return the administrative status of bandwidth logging. Also shown is the operational status, which can be off, when redundancy mode "secondary_hsb_1wire", or WLAG wireless link aggregation mode (x2) "secondary_x2" options are configured. **Note that any redundancy related command is not supported in this release.** Sequence: **get bandwidth record admin** press Enter The system responds: *Bandwidth logging admin status set to 'on'* *Bandwidth logging oper status is 'off'* *Reason: disabled for secondary_hsb_1wire* OR *Reason: disabled for secondary_x2*

Required Action	Steps
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: MIB saved successfully.
View bandwidth records in brief	Up to 60 records are maintained in flash memory. A brief view of all records can be obtained using the following CLI command. Sequence: **get bandwidth record brief** press Enter The system responds: *Inst Serial Date of Report Date of Max Utilization Util* *---- ------ ---------- ---------- ----* *0 1 02/05/2009 15:52:38 01/05/2009 17:45:15 88%* *1 2 03/05/2009 15:52:39 03/05/2009 10:25:09 84%* *2 3 07/05/2009 15:46:56 07/05/2009 12:14:36 43%* *3 4 09/05/2009 17:15:10 08/05/2009 18:16:35 33%* ⋮ *59 60 10/06/2009 17:15:13 09/06/2009 17:46:52 77%*

Required Action	Steps
View a specific bandwidth record in detail	A specified record (0 – 59) can be viewed in detail by using the following command. Sequence: **get bandwidth record instance (0-59)** press Enter The system responds: *Serial Number: : 1* *Report ending : 02/05/2009 15:52:38* *Maximum utilization* *Utilization was : 88%* *Time and date was : 01/05/2009 17:45:15* *Egress Speed was : 397 Mbps* *Peer Current Speed was : 450 Mbps* *Egress bytes were : 178713641492* *Elapsed cycles were : 90021622135* *Reporting period duration was : 86400s* *Unit serial number was : DW109ABC1016* *Peer unit serial number was : DW110ABH1013* *Peer Current Speed was : 450 Mbps* *MAC Address was : 00075800C01A* *Instantaneous Utilization Counts were (average sample duration 1012ms):* *10%: 85045 (86088 seconds)* *20%: 84986 (86028 seconds)* *30%: 84925 (85966 seconds)* *40%: 84893 (85934 seconds)* *50%: 84720 (85759 seconds)* *60%: 84719 (85758 seconds)* *70%: 84699 (85737 seconds)* *80%: 84103 (85134 seconds)* *90%: 2114 (2139 seconds)* *95%: 1713 (1734 seconds)*

Required Action	Steps
View the current record	This command returns the values currently being accrued, but not yet written to a record. It shows the time left in the sampling period (1319 seconds in the example below) before the running average is valid (the running average period must elapse before the running average is valid). The record will be written to flash in 86400s – 2281s = 84119s. Sequence: **get bandwidth record current** press Enter The system responds: *Current Running-Average Bandwidth Utilization: 90% (valid in 1319s)* *Maximum Running-Average Bandwidth Utilization (averaging period = 3600s):* *Date and Time: not available (ready in 1319s)* *Utilization: 0%* *Elapsed time in reporting period (period = 86400s): 2281s* *Instantaneous Utilization Counts were (average sample duration 1046ms):* *10%: 2048 (2143 seconds)* *20%: 2048 (2143 seconds)* *30%: 2044 (2138 seconds)* *40%: 2037 (2131 seconds)* *50%: 2036 (2130 seconds)* *60%: 1951 (2041 seconds)* *70%: 1950 (2040 seconds)* *80%: 1947 (2037 seconds)* *90%: 1944 (2034 seconds)* *95%: 1935 (2024 seconds)*

11.0 Adaptive Transmit Power Control (ATPC)

Adaptive Transmit Power Control (ATPC) allows a Horizon Compact Plus system to adjust its transmit power to compensate for far end signal loss caused by changes in atmospheric conditions e.g. heavy rain. ATPC maintains the RSL at the ATPC threshold, which is system mode dependant, and adjusts the transmit power as necessary in order to maintain the ATPC threshold during fade conditions.

RSL threshold levels that trigger power changes, the maximum power change allowed is preset at values which optimize the operation of the Horizon Compact Plus system. A fade factor of 60dB/second can be handled.

The Horizon Compact Plus system is able to discriminate between RSL levels that are reduced as a result of interference and those as a result of genuine path loss, so that ATPC is not invoked unnecessarily. An ATPC log is available for debugging the system. Use the CLI command ***get atpc log***. The log can be cleared using the CLI command ***clear atpc log***.

Some jurisdictions require the use of ATPC so that power levels are kept as low as possible when wireless communication conditions are good.

When ATPC is to be used, if it can be shown that the maximum power of the system would be used only on infrequent occasions, some jurisdictions will allow a lower power level to be used in the calculations that determine interference criteria. This offers some advantage to the installation. This lower power is termed the “coordinated power”. The DragonWave ATPC feature supports a coordinated power parameter called the coordinated power “offset”. This offset value represents the offset from the maximum transmit power level of the radio.

There are two situations when ATPC can be used. The first is when a link is engineered to prevent receiver saturation (normal link installation). The second is when, due to extreme rain conditions, a link is engineered to have receiver saturation during clear weather (short range between systems). This allows more margin for ATPC to operate and thus maintain a link operational during severe rain. The configuration of ATPC is different for each case.

11.1 Normal Link

Procedure 11-1
Configure Horizon Compact Plus Adaptive Transmit Power Control – Normal Installation

Required Action	Steps
login	Log in as a NOC user.
View atpc status	Returns the current status of the atpc Sequence: **get atpc status** press Enter System responds (example): *ATPC STATUS* --- *State : Running* *Transmit Power (Actual) : 6.9 dBm* *Transmit Power Range : (-0.6 - 19.4) dBm* *RSL (Peer) : -52.0 dBm* *RSL Target : -52.0 dBm*

Required Action	Steps
Return the current atpc configuration	This command displays the current atpc configuration. Sequence: **get atpc config** press Enter The system responds: *ATPC CONFIGURATION LOCAL PEER* *Status : Disabled Disabled* *Coordinated Power Offset : 5.0 dBm Disabled*
Configure atpc	Enables or disables atpc, enables or disables coordinated power and provides a coordinated power offset value in dB. Atpc may be invoked with or without a coordinated power parameter. **set atpc config [on/off] [coord power on/off] [0-10]** press Enter Sequence Example: **set atpc config on on 6** press Enter System responds: *ATPC CONFIGURATION LOCAL PEER* *Status : Enabled Disabled* *Coordinated Power Offset : 6.0 dBm Disabled*

Required Action	Steps
Review the atpc log	This command returns the list of events from the atpc log. Sequence: **get atpc log** press Enter The system responds (example): *ATPC LOGS* *RSL (dBm)* / *TRANSMIT POWER (dBm)* *Time* — *LOS* — *PEER* — *TARGET* — *RANGE* — *ACTUAL* *2011-09-29 17:51:47.870* N -45.3 -46.0 -0.5 - 10.0 2.9 *2011-09-29 17:51:47.762* N -46.2 -46.0 -0.5 - 10.0 3.6 *2011-09-29 17:51:41.468* N -46.6 -46.0 -0.5 - 10.0 3.0 *2011-09-29 17:51:41.367* N -45.8 -46.0 -0.5 - 10.0 2.4 *2011-09-29 15:44:35.313* N -46.2 -46.0 -0.5 - 10.0 3.1 *2011-09-29 15:41:05.414* N -45.7 -46.0 -0.5 - 10.0 2.5 *2011-09-29 15:38:54.512* N -46.2 -46.0 -0.5 - 10.0 3.1 *2011-09-29 15:38:24.611* N -45.8 -46.0 -0.5 - 10.0 2.4 *2011-09-29 15:38:20.714* N -46.2 -46.0 -0.5 - 10.0 3.1 *2011-09-29 15:38:04.354* N -45.8 -46.0 -0.5 - 10.0 2.4 *2011-09-28 21:38:21.707* N -45.0 -46.0 -0.5 - 10.0 3.0 *2011-09-28 21:38:21.644* N -47.6 -46.0 -0.5 - 10.0 4.0 *2011-09-28 21:38:21.620* N -47.6 -46.0 -0.5 - 10.0 2.4 *2011-09-28 21:38:21.594* N -44.2 -46.0 -0.5 - 10.0 0.8 *2011-09-28 21:38:21.566* N -38.6 -46.0 -0.5 - 10.0 2.6 *2011-09-28 21:38:21.012* Y -99.9 -99.9 -0.5 - 10.0 10.0 The log can be cleared by using the CLI command **clear atpc log** press Enter.
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

11.2 Saturated Link

Procedure 11-2
Configure Horizon Compact Plus Adaptive Transmit Power Control – Saturated Installation

Use this procedure to set up ATPC for a link engineered for receiver saturation (short range).

This procedure assumes that the link has been properly aligned at a low transmit power, with ATPC turned off, before the following steps are performed.

Required Action	Steps
login	Log in as a NOC user.
Turn on ATPC	Align the link with ATPC turned off and with low power, to prevent receiver saturation during alignment. Once the link is aligned, use this command to turn ATPC on. Enables or disables atpc, enables or disables coordinated power and provides a coordinated power offset value in dB. Atpc may be invoked with or without a coordinated power parameter. **set atpc [on/off] [on/off] [0-10]** Example 1 Sequence: **set atpc on** System responds: *ATPC CONFIGURATION LOCAL PEER* *Status : Enabled Enabled* *Coordinated Power Offset : Disabled Disabled* Example 2 Sequence: **set atpc on on 6** press Enter System responds: *ATPC CONFIGURATION LOCAL PEER* *Status : Enabled Enabled* *Coordinated Power Offset : 6.0 dBm Disabled*
Increase the transmit power to the maximum for the radio in use.	This command changes the output power for the radio. The actual value depends on the radio band and radio concerned. Sequence: **set transmit power n** Where **n** is the desired transmit power in dBm. Example 18 The system responds (example): *This may affect user traffic. Continue? Enter Y(Yes) or N(No)* ***:y*** *System is programmed to 18.0 dBm and presently transmitting at :-0.6 dBm.*

Required Action	Steps
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: MIB saved successfully.

11.3 Coordinated Power Alarm

The coordinated power alarm will get triggered when ATPC is on and the system is transmitting at full power (i.e. no atpc attenuation) for the last 5 minutes.
Example:
On a link with the atpc threshold at -50 dBm, and the system RSL at -44 dBm, ATPC will add 6 dBm of attenuation to bring the link RSL down to –50 dBm. While the link is in this state, a heavy rain storm occurs for 10 minutes, causing ATPC to remove all of the attenuation to keep the link at -50. Now the attenuation is 0 and after 5 minutes in this state the coordinated power alarm will be activated. When the alarm is activated, the system transmit power will be changed to (set txpower - coordinated power offset) dBm.

To clear a coordinated power alarm execute **set atpc on** again, or **set atpc off**.

This page is left blank intentionally

12.0 Authentication

This feature is only necessary if you wish to restrict forwarding the user payload from a Horizon Compact Plus unit to a specific peer or to a group of Horizon Compact Plus units. Authentication is generally used as a security measure. It is not recommended to enable Authentication prior to alignment of the radios.

Authentication restricts a Horizon Compact Plus unit from forwarding the user payload to other Horizon Compact Plus units unless the other units match an authentication string. There are three types of authentication:

1. No Authentication
2. Unique Authentication
3. Group Authentication

A new Horizon Compact Plus system inline with the signal cannot authenticate and receive data if another Horizon Compact Plus system is already authenticated. The system authenticates its peer(s) at an interval of approximately five seconds.

The Horizon Compact Plus system does not accept data from other manufacturers' systems.

12.1 No Authentication

No Authentication is the default mode of operation for Horizon Compact. The Horizon Compact Plus does not attempt to create a dialogue or establish authentication between Horizon Compact Plus nodes. For No Authentication Mode, setting the failure condition has no effect since there is no dialogue or authentication between Horizon Compact Plus systems. Any other Horizon Compact Plus node transmitting on exactly the same frequency can send Ethernet data to the corresponding Horizon Compact Plus node. The Horizon Compact Plus only accepts data from other Horizon Compact Plus nodes that:

a. are transmitting on the same frequency;
b. are properly aligned in polarity; and
c. have adequate signal strength.

The Horizon Compact Plus system does not accept data from any other manufacturers' products.

12.2 Unique Authentication

Unique authentication establishes a dialogue between two Horizon Compact Plus nodes. Unique authentication is used in a point-to-point configuration where two Horizon Compact Plus systems communicate only with each other and not any additional Horizon Compact Plus systems. Once Unique Authentication is set, the Horizon Compact Plus only accepts Ethernet data from its authenticated peer. It ignores all other sources of traffic arriving over the airwaves. Each node is programmed with its peer's identification number. Use CLI command **get hw inventory**. The Unit Serial Number is the identification number to be used. The identification number corresponds to the Unit Serial Number of the peer node. For example, endpoint A has a Unit Serial Number '1234' and endpoint B has Unit Serial Number '5678'. The peer identifier for endpoint B is '1234' (serial number of its peer) and the peer identifier for endpoint A is '5678' (serial number of its peer).

When you select Unique Authentication, you must set the authentication failure action.

12.3 Group Authentication

Group authentication is used when it is desireable to use the same authentication key over multiple nodes in a network. This allows the authentication key management to be done at the network level rather than at the link level.

A group of Horizon Compact Plus nodes uses a group ID to establish inter-node communication. Administrators create a group ID string consisting of up to eight characters. You must program the group ID string on each node. The group ID string can consist of the characters 0 to 9, a to z, and A to Z. Illegal characters that cannot be used are {! @ # $ % ^ &* (,) ; : ’ ” + - ~}.

12.4 Authentication Failure Action

If authentication fails, you can specify how the Horizon Compact Plus system responds:

- allow Ethernet traffic to continue to flow
- block the flow of Ethernet traffic.

12.5 Configure Authentication

Should you require more security than offered by the default authentication mode of No Authentication, you will need to configure the authentication key to suit your requirements. Follow the steps in the following procedure.

Procedure 12-1
Setting Unique Authentication

Perform this procedure to set system authentication to unique.
Note: You must perform the authentication procedures in the sequence that they appear in this manual.

Required Action	Steps
login	Log in as a NOC user on both ends of the system and run the CLI command **get hw inventory** as shown below, to retrieve the unique authentication keys (serial number of node) from each unit.
View hw inventory to find the serial number of the nodes	Displays the serial numbers of the various sections in the system. Perform this command at each end of the link and record the authentication keys (**Unit Serial Number**) for each end. Sequence: **get hw inventory** press Enter The system responds: *Frequency File PartNumber : number* ***Unit Serial Number : number*** *Unit Assembly Number : number* *NCC Serial Number : number* *NCC Assembly Number : number* *IF Serial Number : number* *IF Assembly Number : number* *Radio Serial Number : number* *Radio Assembly Number : number* *Diplexer Serial Number : number* *Diplexer Assembly Number : number*
Set the suthentication type used to authenticate the peer unit.	Sets the authentication type. For unique authentication this needs to be set to **unique**. The default type is none. Sequence: **set peer authentication type [none|unique|group]** press Enter where **[none, unique, group]** identifies the authentication type. Use **unique** on this occasion. The system responds: *Peer Authentication Type : unique* **get peer authentication type** press Enter (will confirm type) *Peer Authentication Type : unique*

Required Action	Steps
Configure unique peer authentication key <xxxx>	Sets the unique peer authentication key of the peer node with which you wish to authenticate, generally the far-end unit. Sequence: **set peer authentication unique key <xxxx>** press Enter where **<xxxx>** is the Unit Serial Number of the **far-end** unit determined from the **get hw inventory** command performed earlier. The system responds: *Peer Authentication Unique Key: xxxx* **get peer authentication unique key** press Enter (will confirm key) *Peer Authentication Unique Key: xxxx* **Note:** You will need to repeat this procedure for each of the two units.
NOTE:	Once the unique authentication key is set, you will need to verify the authentication settings and set the authentication failure parameter before saving the mib and resetting the system. See Procedure 11-3.

This concludes the steps to setting authentication to unique.

Procedure 12-2
Setting Group authentication

Perform this procedure to set group authentication using the CLI manager.

Required Action	Steps
login	Log in as a NOC user.
Configure air interface authentication type	Sets the authentication type. This needs to be set to **group**. The default type is none. Sequence: **set peer authentication type [none, unique, group]** press Enter where **[none, unique, group]** identifies the authentication type. Use **group** on this occasion. The system responds: *Peer Authentication Type : group* **get peer authentication type** press Enter (will verify type) *Peer Authentication Type : group*
Configure group authentication key	Sets the group authentication key. Sequence: **set peer authentication group key <xxxxxxxx>** press Enter where **<xxxxxxxx>** is a character string consisting of up to 35 characters that may be: 0 to 9, a to z, and A to Z but may not contain any of the following: !@#$%^&*(,);:'"+-~ The system responds: *Peer Authentication Group Key: xxxxxxxx.* **Note:** The <xxxxxxxx> is the unique, up to 32 character string you have assigned to be the group authentication key. You will need to repeat this procedure for each unit in the group that uses the same group key. **get peer authentication group key** press Enter (will verify key) *Peer Authentication Group Key: xxxxxxxx.*
NOTE:	Once the group authentication key is set, you will need to verify the authentication settings and set the authentication failure parameter before saving the mib and resetting the system. See Procedure 11-3**.**

This concludes the steps to set the group authentication key using the CLI manager

Procedure 12-3
Verify Authentication status

Use this procedure to verify the authentication action for the system.
Note: To perform this procedure, you must be logged into the system as an NOC user.

Required Action	Steps
login	Log in using a NOC account.
View authentication status	Displays the authentication status between two corresponding Horizon Compact Plus systems. Sequence: **get peer authentication status** press Enter The system responds: *Peer Authentication status:* *[Authenticated|NotAuthenticated|ExplicitAuthenticationFailure]* Explanations: If authentication has failed: check the setting for action on authentication failure; and ensure it is not set to Block Traffic (unless that is the intended action). If authentication has not failed: check to see if traffic is now flowing. If traffic is flowing then the authentication has been re-established and the system is operating normally If traffic is not flowing, the problem is not due to authentication.
Configure authentication failure [block_traffic/pass_traffic]	Configures the action to take when authentication fails. Sequence: **set peer authentication failure action [block_traffic/pass_traffic]** press Enter The system responds: *System will [block_traffic/pass_traffic] on peer Authentication Failure.* **get peer authentication failure action** press Enter (to verify action) *System will [block_traffic/pass_traffic] on peer Authentication Failure.*
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

This concludes the steps to verify the authentication status using the CLI manager.

13.0 Threshold Alarms

Horizon Compact Plus provides Threshold Alarms to assist in managing the performance of the system. Threshold alarms are available for the following parameters, showing default setttings:

- RSL (Receive Signal Level) -70 dB for 10 seconds
- Bandwidth Utilization 100% for 10 seconds
- Dropped Frames (for all data queues) 100% for 10 seconds
  In addition to the total Dropped Frames threshold, each of the eight QoS queues can be allocated an individual threshold alarm
- Queue Utilization (for all data queues) 100% for 10 seconds
  Each queue can be allocated an individual queue utilization alarm
- SNR (Signal To Noise) 0 dB*

Most Threshold Alarms have two associated alarm parameters:

1. Threshold value
2. A time limit over which the Threshold value must be exceeded before the alarm is reported.

The combination of the value and the time limit is user defined. The proper combination of the two parameters will prevent false alarms from occurring.

* For the SNR parameter, only the threshold level can be set, the time limit, or hysteresis, being a preset value.

Procedure 13-1
Configure Threshold Alarms

Perform this procedure to configure the Threshold Alarms for the Horizon Compact Plus system. Each Threshold Alarm may be configured independently of each other, and each end of the link may be configured for different values.

Note: To perform this procedure, you must have NOC user rights.

Required Action	Steps
login	Log in as a NOC user.

Required Action	Steps
View RSL threshold alarm settings	Displays the current settings for the Threshold Alarm for the Receive Signal Level (RSL). Once the RSL Value Threshold is reached and continues for the Time Limit duration then an alarm is raised. Sequence: **get rsl threshold** press Enter The system responds: *RSL threshold set to : <rsl value> dbm* *RSL timelimit set to : <timelimit> secs* Where **<rsl value>** is the current RSL value in integers, given in dBm. **<timelimit>** is the current time limit that the condition must occur before the alarm is raised. Timelimit is in integers, given in number of seconds
Configure RSL threshold alarm settings	Sets the current settings for the Threshold Alarm for the Receive Signal Level (RSL). Once the RSL Value Threshold is reached and continues for the Time Limit duration then an alarm is raised. Sequence: **set rsl threshold <rsl value> <timelimit>** press Enter Where **<rsl value>** is the desired RSL value in integers, given in dBm. **<timelimit>** is the desired time limit that the condition must occur before the alarm is raised. Timelimit is in integers, given in number of seconds The system responds: *RSL threshold set to : <rsl value> dbm* *RSL timelimit set to : <timelimit> secs*
View snr threshold	Returns the current signal to noise ratio alarm threshold. Sequence: **get snr threshold** press Enter The system responds: *SNR threshold set to : n* Where *n* is the current SNR threshold setting

Required Action	Steps
Configure snr threshold	Sets the SNR level below which a threshold alarm will be raised. Sequence: **set snr threshold <snr value>** press Enter Where <snr value> is in dB and between 0 and 30 The system responds: *SNR threshold set to : n* Where *n* is the new SNR threshold setting
View bandwidth utilization threshold alarm settings	Displays the current settings for the Bandwidth Utilization Threshold Alarm. Sequence: **get bandwidth utilization threshold** press Enter The system responds: *Bandwidth utilization threshold set to : <value> % Bandwidth utilization timelimit set to : <timelimit> secs.* Where **<value>** is the current bandwidth utilization value expressed in percentage **<timelimit>** is the desired time limit that the condition must occur before the alarm is raised. Timelimit is in integers, given in number of seconds
Configure bandwidth utilization threshold alarm settings	Sets the values for the Threshold Alarm for the Bit Error Rate (BER) as calculated by the Horizon Compact Plus modem. Once the BER Value Threshold is reached and continues to remain between the Threshold value and the hysteresis value, then an alarm is raised. Once the value drops below the hysteresis value then the alarm is cleared. Sequence: **set bandwidth utilization threshold <value> <timelimit>** press Enter Where **<value>** is the current bandwidth utilization value expressed in percentage **<timelimit>** is the desired time limit that the condition must occur before the alarm is raised. Timelimit is in integers, given in number of seconds. Default value is 10 seconds The system responds: *Bandwidth utilization threshold set to : <value> % Bandwidth utilization timelimit set to : <timelimit> secs.*

Required Action	Steps
View dropped frames threshold alarm settings	Displays the current settings for the Dropped Ethernet Frames Threshold Alarm. Note that the values for all CoS queues, as well as the total for the system, are displayed. Sequence: **get dropped frames threshold** press Enter The system responds: *Tot Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8* *Dropped frames thresholds set to :100 100 100 100 100 100 100 100 100 %* *Dropped frames timelimits set to : 10 10 10 10 10 10 10 10 10 secs*
Configure **total** dropped frames threshold alarm settings	Sets the values for the **total** Dropped Ethernet Frames Threshold Alarm. As the Horizon traffic rate from the LAN side exceeds the programmed limit, frames are dropped in order to maintain the limit. Sequence : **set dropped frames threshold <value> <timelimit>** press Enter Where **<value>** is the desired total dropped frames value expressed as a percentage **<timelimit>** is the desired time limit over which the condition must occur before the alarm is raised. Timelimit is in integers, given in number of seconds. Default value is 10 seconds. Example : **set dropped frames threshold 50 5** press Enter The system responds: *Bandwidth utilization threshold set to : 50 %* *Bandwidth utilization timelimit set to : 5 secs.* **get dropped frames threshold** press Enter *Tot Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8* *Dropped frames thresholds set to : 50 100 100 100 100 100 100 100 100 %* *Dropped frames timelimits set to : 5 10 10 10 10 10 10 10 10 secs*

Required Action	Steps
Configure **per queue** dropped frames threshold alarm settings	Sets the values for the **per queue** Dropped Ethernet Frames Threshold Alarm. As the Horizon traffic rate from the LAN side exceeds the programmed limit, frames are dropped in order to maintain the limit. Sequence : **set dropped frames threshold <queue> <value> <timelimit>** press Enter Where **<queue>** is the number of the queue for which a change is required **<value>** is the desired dropped frames value for that queue expressed as a percentage **<timelimit>** is the desired time limit over which the condition must occur before the alarm is raised. Timelimit is in integers, given in number of seconds. Default value is 10 seconds. Example: **set dropped frames threshold 3 75 20** press Enter The system responds: *Dropped frames threshold set to :75 %* *Dropped frames timelimit set to :20 secs* **get dropped frames threshold** press Enter *Tot Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8* *Dropped frames thresholds set to : 50 100 100 75 100 100 100 100 100 %* *Dropped frames timelimits set to : 5 10 10 20 10 10 10 10 10 secs*
View the utilization thresholds for each queue.	Returns the values of the utilization threshold set for each date queue. Sequence: **get queue utilization threshold** press Enter The system responds: *Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8* *Queue Depth thresholds set to : 100 100 100 100 100 100 100 100 %* *Queue Depth timelimits set to : 10 10 10 10 10 10 10 10 secs*

Required Action	Steps
Configure the queue utilization threshold for each queue	This command enables you to set the queue utilization threshold for each of the five QoS queues in the system. Sequence: **set queue utilization threshold <queue> <%> <timelimit>** press Enter Where **<queue>** is the queue number (1 to 5), **<%>** is the percent of utilization threshold desired and **<timelimit>** is the desired time limit (in seconds) over which the condition must occur before the alarm is raised. Example: **set queue utilization threshold 4 75 25** press Enter The system responds : *Queue Depth threshold set to :75 %* *Queue Depth timelimit set to :25 secs* **get queue utilization threshold** press Enter *Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8* *Queue Depth thresholds set to : 100 100 100 75 100 100 100 100 %* *Queue Depth timelimits set to : 10 10 10 25 10 10 10 10 secs*
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

This concludes the steps to configure Threshold Alarms for the Horizon Compact Plus system using the CLI manager.

14.0 Rapid Link Shutdown (RLS)

Networks containing alternate or redundant routing paths will typically rely on protocols such as Rapid Spanning Tree Protocol (RSTP) to invoke a reroute when communications to the far end unit fail or experience high data error rates. The protocols are implemented on the Ethernet switch and rely on polling or messaging to determine that communications to the far end has been disrupted. Although very effective, these protocols can result in slow reaction times to determine link issues. It is desirable to inform a switch or router of a network issue in the quickest manner possible. The Horizon Compact Plus system provides the Rapid Link Shutdown feature for this purpose. Notification to the switch or router is provided by shutting down the Ethernet ports connecting the Horizon Compact Plus systems to the network. The Ethernet ports at both ends of the link are shut down. The Ethernet switch immediately recognizes the loss of Ethernet connection and invokes its alternate path algorithm.

The default setting for RLS is OFF, meaning that the Ethernet port will remain connected during failure conditions.

Notes:

1. RLS is not compatible with the Horizon Compact Plus redundancy* option and should NOT be enabled when the redundancy* option is employed.
2. RLS cannot be invoked when the x2 enhanced throughput feature is enabled.
3. RLS cannot be invoked if Hitless Automatic Adaptive Modulation (HAAM) is enabled, or if 1+1 Redundancy* is enabled.
4. RLS should be disabled during link alignment to prevent the condition where a link goes in and out of synchronization resulting in the RLS being invoked and released causing loss of Ethernet management to the systems.
5. A disconnected Ethernet cable at one end of the link will trigger an RLS event and will result in the Ethernet port on the other end being shut down if RLS is enabled.

*** The Redundancy feature and any related redundancy commands are not supported in this release.**

14.1 Determination of Error Rates on Horizon Compact Plus Systems

Horizon Compact Plus systems employ forward error correction to compensate for and correct errors occurring over the RF link. Once these errors are corrected, the user data can flow error-free. The post-correction data error rate is reported as "Rx Block Receive Errors" within the Horizon Compact Plus, accessible through traffic statistics in CLI or through the Performance web page. Rx Block Error Rate is also available and is reported in scientific notation.

The Horizon Compact Plus systems communicate with each other via “Rx Blocks” at all times even if there is no Ethernet traffic. The Rx Blocks are transmitted at a fixed rate and therefore a Rx Block error rate is also available. The incoming Ethernet data stream is treated as a bit stream and sub-divided into Rx Blocks for transmission over the RF link. Rx Blocks are continuously transmitted to the far end modem regardless of whether or not Ethernet traffic exists. The modems transmit approximately 59,000 blocks per second on a 100 Mbps link. In order to determine a Rx Block error rate of 1x10e-6 there would have to be a minimum of 1 million Rx Blocks transmitted. At 59,000 blocks per second, it would take 16.8 seconds to transmit 1 million blocks.

Horizon enhancements to the DragonWave RLS functionality consist of:

- The fade monitor (“soft failure” mode) analyzes the Rx Block error rate over time increments. RLS will trigger when the user-configurable error rate threshold is exceeded. The sample time parameter for both “break” (“break” relates to the shutting down of the link) and “make” (“make” relates to the re-establishment of the link) can be configured independently.

- A “hard failure” mode triggers on a percentage of erred packets on a link. This mode is applicable to link outages or severely degraded data transfer.
    - The default value of error threshold is a loss of 50% of Rx Blocks (packets) over a default sample time of 50 mS. The sample time and error threshold are user-configurable.
    - Advanced Mode provides support for a combined “hard”/”soft” failure mode
        - Fast RLS switch for “hard” failure (severe degradation or link outage)
        - Longer sample time and RLS switch for “soft” failure (high error rate)
- Increased flexibility in setting a larger differential for “break vs. make” error values
- Addition of a Receive Signal Level “RSL” threshold monitor to be optionally used in “make” criteria for link startup

14.2 RLS Configuration – Port Groups

When RLS is enabled there are two options available for determining when RLS should be invoked to shut down the Ethernet ports. These are the basic and advanced modes. The port group configuration determines what port, or ports, the system will monitor and apply the failure algorithms to before a port shutdown takes place. Note that any port that is part of a port group cannot be used for management, regardless of the status of RLS (enabled or not).

14.2.1 Basic Mode

In basic mode, the user can configure the modem Block error rate thresholds under which RLS will be invoked and the Ethernet ports disabled. The user can also set the thresholds for which RLS will be revoked and the Ethernet ports brought back to service. Complete link outages due to loss of Ethernet connectivity, loss of RF path, hardware failure, or power failure will trigger an RLS event and the modem’s Ethernet ports will be shut down until the outage is repaired.

The basic mode relies on the follow situations occurring:

“Soft” failure. This mode monitors the link for data errors either as a steady state error rate or bursts of data errors.

a. The RLS signal degrade settings correspond to “soft” failure mode.
b. Minor modem block errors can be corrected by the modem. This correction is invisible to the user and is not traffic affecting. The Rx Blocks Error counter indicates uncorrectable errors in the modem block stream over the air. Modem blocks may, or may not, contsain user/payload data. The counter is a true representation ov over-the-air data performance, even when there is no user data present.
c. The sample time is user configurable
d. An RLS signal degrade threshold setting in percentage is available to allow shorter sampling times should errors occur on a frequent basis.

14.2.2 Advanced Mode

The advanced mode relies on any of the following situations occurring:

1. “Hard” failure. This mode invokes RLS when the link has deteriorated to a point of a massive amount of data errors being received over the link.
    a. A link outage will trigger an immediate RLS condition.
    b. The RLS signal fault parameters correspond to “hard” failure mode.
    c. The user-configurable error rates vary from 5% to 95%.
    d. The user-configurable sample time ranges from 5 mS to 1000 mS.

Example: Configuring 50% error rate over the link for a 100 mS time period will invoke RLS if the error rate equals, or exceeds, 50% over a period of 100 mS.

2. "Soft" failure. This mode monitors the link for data errors either as a steady state error rate or bursts of data errors.
    a. The RLS signal degrade settings correspond to "soft" failure mode.
    b. Minor modem block errors can be corrected by the modem. This correction is invisible to the user and is not traffic affecting. The Rx Blocks Error counter indicates uncorrectable errors in the modem block stream over the air. Modem blocks may, or may not, contsain user/payload data. The counter is a true representation ov over-the-air data performance, even when there is no user data present.
    c. The sample time is user configurable
    d. An RLS signal degrade threshold setting in percentage is available to allow shorter sampling times should errors occur on a frequent basis.

    While monitoring for a "soft" failure, any "hard failure" will invoke RLS immediately.

Note: When selecting Advanced Mode, both the "hard" failure mode and "soft" failure mode are to be configured.

14.3 Settings for Basic Mode

Basic mode relies on RLS link monitor parameters consisting of errors in data transfer between the modems. It monitors Rx Block errors and the user configures the number of errors and sampling time for those errors for both the invocation and revocation of RLS.

14.3.1 RLS Signal Degrade Settings

These settings correspond to "soft" failure mode.

The following command sets the minimum RSL value that will re-establish, or "make", the link.

set rls make rsl [RSL Threshold (dB)] [Sample Period (sec)]

Example: **set rls make rsl -60.0 100**

When the RSL level is maintained at -60.0 or a higher value (less negative) for the duration of the sample period (100 seconds), the link will be re-established, provided that there are no other existing "soft" or "hard failures"

Setting the RSL sample period to zero (0), the default value, disables this feature.

14.3.2 RLS Link Monitor Parameters

This CLI only command provides a custom method for the configuration on the "soft error" monitor. The method directly configures the sampling period, required repeated consecutive samples and the erred block thresholds per period of the "soft error" monitor. This method allows additional low-level tuning of the "soft error" monitor.

The RLS link monitor parameters are a measure of the number of block errors per designated sampling time period. The user configures the RLS settings for:

- the number of desired block errors required in order to invoke, or revoke, RLS
- the number of samples in which the block errors occur
- the sampling time in milliseconds
- a "quick" sampling time that determines a fail condition if the block error threshold is exceeded before the down sample time period times out

The following command configures the link monitor parameters:

set rls link monitor parameters [dn2up block errors per sample] [up2dn block errors per sample] [dn2up # of samples] [up2dn # of samples] [dn2up sample time in msec] [up2dn sample time in msec] [quick sample time]

Example: **set rls link monitor parameters 2 4 5 2 1000 100 10**

- If there are 4 or more block errors in 100 mS for 2 consecutive samples then invoke RLS ("break")
- If the 4 or more block errors occur within the first 10 mS (quick sample time) of the 100 mS period, count it as a failure and immediately restart the 100 mS sample period.
- If 2 or less block errors occur in 1000 mS period for 5 consecutive samples revoke RLS ("make")

Note that the quick sample time parameter provides a quicker response to block errors if the block error threshold occurs early in the configured sample time period. To disable the quick sample time feature, configure its value the same as the "up2dn" sample time.

14.4 Settings for Advanced Mode

If the user requires a quicker RLS response, the Advanced Mode is recommended.

Note: When selecting Advanced Mode, both the "soft" failure mode (Basic mode parameters) and "hard" failure mode (Advanced mode parameters) are to be configured.

14.4.1 RLS Signal Fault Settings

These settings correspond to "hard" failure mode The RLS signal fault settings are designed to detect and react to brief bursts of extreme Rx Block error rates. The RLS signal fault detection and reaction time is the quickest of the two RLS fault detection methods. RLS signal fault detection works with the RLS signal degrade settings in Advanced Mode.

set rls signal fault parameters [detect time] [percentage erred blocks]

The RLS signal fault parameters command accepts two parameters:

- **[detect time]** is the time, in milliseconds, that the **[percentage erred blocks]** threshold must be met to activate RLS.
- **[percentage erred blocks]** is the percentage of erred Rx Blocks required to invoke RLS. For example, the command **set rls signal fault parameters 1000 50** will activate RLS when 50% or more of the Rx Blocks received in 1000 milliseconds are erred.

14.4.2 Recovery from a Hard Failure

Once a "hard" failure has caused an RLS activation, it uses the "soft" failure - RLS signal degrade parameters – to determine the length of time to wait before reactivating the Ethernet ports.

14.5 RLS Link Control Settings

By default, the disabling and enabling of the data Ethernet port is automatically managed by the Horizon Compact Plus system in response to detected RLS events. It is possible to enable manual control of RLS shutdowns, so that the data Ethernet port remains shutdown until a user explicitly re-enables it. There are two commands that make up RLS link control.

set rls link control [on/off]

To enable manual control of the data Ethernet port link state, set rls link control to **on**. The default setting is **off**, allowing the Horizon Compact Plus to re-enable the data Ethernet port once the RLS condition is cleared.

set rls link enable [on/off]

When **rls link control** is set to **on**, the data Ethernet port remains in a shutdown state after the RLS condition has been cleared. The Ethernet port is manually re-enabled by issuing the **set rls link enable on** command. The **set rls link enable off** command disables the Ethernet port.

Procedure 14-1
Configure Rapid Link Shutdown Options

Perform this procedure to configure the Rapid Link Shutdown Options for the Horizon Compact Plus system. When RLS is used, the Horizon Compact Plus Port 1 will be set to "down" during modem-to-modem communication failure. This feature allows a router to select an alternate path should the modem-to-modem communications fail.

Note: To perform this procedure, you must have NOC user rights.

Required Action	Steps
login	Log in as a NOC user.
View rls	Displays the state of the Rapid Link Shutdown feature. RLS provides the ability to shut down the Horizon Compact Plus Ethernet link (both endpoints) during system outages. The default is "off". Sequence: **get rls** press Enter The system responds: *RLS option is :[off/on].*
View rls status	Displays the detailed status of the RLS configuration. Sequence: **get rls status** press Enter The system responds (Example): *RLS Option: On Advanced* *Rapid Link Shutdown: Activated* *RLS Peer Mismatch: Activated* *Degrade Monitor State: Activated* *Hard Fault Monitor State: Acitvated* *Make RSL Threshold: OK* *Peer RLS State: OK* *Radio Interface State: Up* *Network Interface State: Down* *User Configured Establish FER: 8.82E-07* *Minimum Achievable Establish FER: 3.06E-07* *User Configured Shutdown FER: 1.76E-04* *Minimum Achievable Shutdown FER: 3.06E-06* *User Configured Establish Monitor Time(mSec): 40000* *Actual Establish Monitor Time(mSec): 45517* *User Configured Shutdown Monitor Time(mSec): 3000* *Actual Shutdown Monitor Time(mSec): 4550*

Required Action	Steps
Configure rls [on/off] [basic/advanced]	Turns the Rapid Link Shutdown (RLS) feature on or off. Turning RLS on, with the optional "advanced" feature, enables use of the signal fault monitor as well as the signal degrade monitor. Setting RLS on without issuing the basic or advanced command defaults to RLS on, basic. RLS provides the ability to shut down the Horizon Compact Plus Ethernet ports (Port 1 on both endpoints) during system outages. Note: a save mib and reset system command must be issued in order for the rls setting to take effect. The default is "off". Sequence: **set rls [on/off] [basic/advanced]** press Enter The system responds: *RLS option [on/off][basic/advanced]* *Where* *On means the RLS function is active.* *Off means the RLS function is inactive.*
View rls link control	Displays the state of the Rapid Link Shutdown (RLS) link control feature. RLS provides the ability to shut down the Horizon Compact Plus Ethernet ports (Port 1 on both endpoints) during system outages. The RLS link control feature determines how the system will react when link recovery takes place, either providing automatic recovery of the Ethernet ports by the Horizon Compact Plus system or waiting for the user to manually recover the Ethernet ports through use of the "set rls link enable on" command. The default is "off". Sequence: **get rls link control** press Enter The system responds: *RLS link control option is set to [on/off]* Where On means the user has to re-establish the Ethernet connection by using the "set rls link enable on" command Off means the system will auto-recover the Ethernet connection.

Required Action	Steps
Configure rls link control [on/off]	Determines whether RLS link control performs automatic recovery or requires manual recovery of the Ethernet port. RLS provides the ability to shut down the Horizon Compact Plus Ethernet ports (Port 1 on both endpoints) during system outages. The user can manually recover the Ethernet ports through the use of the "set rls link enable on" command. The default is "off". Sequence: **set rls link control [on/off]** press Enter The system responds: *RLS link control is set to [on/off]* *Where* *On means the user must manually recover the Ethernet port through the use of the "set rls link enable on" command.* *Off means the Horizon Compact Plus system will automatically recover the Ethernet port.*
View rls link enable	Displays the state of the Rapid Link Shutdown (RLS) link enable feature. RLS provides the ability to shut down the Horizon Compact Plus Ethernet ports (Port 1 on both endpoints) during system outages. The default is "off". Sequence: **get rls link enable** press Enter The system responds: *RLS link enable is set to [on/off]* *Where* *On means to re-enable the Ethernet port on the modem* *Off means the Ethernet port is not re-enabled.*
Configure rls link enable [on/off]	Manually enables or disables the Horizon Compact Plus Ethernet link. This feature requires the rls link control feature to be "on". The default is "off". Sequence: **set rls link enable [on/off]** press Enter The system responds: *RLS link enable is set to [on/off]* *Where* *On means to re-enable the Ethernet port on the modem* *Off means the Ethernet port is not re-enabled.*

Required Action	Steps
Configure Port Groups	This command determines what combination of port failures will invoke RLS. Sequence: **get rls port group** press Enter The system responds: *Rls port group configuration* *Ports :P1 P2 P3 P4* *Combination :any* The above response indicates that any one port P1 through P4 needs to fail and RLS will be invoked. **set rls port group [p1[[p2] [p3] [p4] [any|all]** press Enter Example 1: **set rls port group p1 p2 p3 p4 all** press Enter The system responds: *Rls port group configuration* *Ports :P1 P2 P3 P4* *Combination :all* The above response indicates that RLS will only be invoked when all of ports P1 through P4 have failed. Example 2: **set rls port group p3 any** press Enter (“any” or “all” works for this example) The system responds: *Rls port group configuration* *Ports : P3* *Combination :any* If P3 fails RLS will be invoked.
Configure rls make rsl	This is an optional command. This command sets the minimum RSL value required to re-establish, or “make”, the link. Sequence: **set rls make rsl [RSL (dB)] [Duration (sec)]** press Enter The system responds: RLS Make RSL Parameters: [RSL (dB)] [Duration (sec)] Example: **set rls make rsl -60.0 100** When the RSL level is maintain at -60.0 or a higher value (less negative) for the duration of the sample period (100 seconds), the link will be re-established. Setting the RSL sample period to zero (0), the default value, disables this feature.

Required Action	Steps
Configure rls link monitor parameters	This is a custom method for the configuration of the “soft error” monitor. The method directly configures the sampling period, required repeated consecutive samples and the errored block thresholds per period of the “soft error” monitor. This method allows additional low-level tuning of the “soft error” monitor. **Note:** When this command is used, it overrides the **set rls signal degrade parameters** and **set rls signal degrade threshold** commands invoked by CLI, Web or SNMP methods. Sequence: **set rls link monitor parameters [dn2up block errors per sample] [up2dn block errors per sample] [dn2up # of samples] [up2dn # of samples] [dn2up sample time in msec] [up2dn sample reset time in msec]** Please contact DragonWave Customer Support for assistance if the default “soft error” monitor behaviour needs to be tuned for a specific application.
View rls signal fault parameters	The RLS signal fault settings are designed to detect and react to brief bursts of extreme Rx Block error rates or link outages. The RLS signal fault detection and reaction time is the quickest of the two RLS fault detection methods. RLS signal fault detection works with the RLS signal degrade settings in Advanced mode. Sequence: **get rls signal fault parameters** press Enter The system responds: *RLS Signal Fault Parameters: 1000 100*

Required Action	Steps
Configure rls signal fault parameters [fault period msec] [fault threshold]	Sets the RLS signal fault monitor parameters. The RLS signal fault settings are designed to detect and react to brief bursts of extreme Rx Block error rates. The RLS signal fault detection and reaction time is the quickest of the two RLS fault detection methods. RLS signal fault detection works with the RLS signal degrade settings in Advanced mode. Sequence: **set rls signal fault parameters [fault period msec] [fault threshold]** press Enter Where **[fault sample period msec]** is the sample period to apply Fault Threshold ratio **[fault threshold percentage]** is the ratio of 'fault sample period' faulted before the link is shut down. The system responds: *RLS Signal Fault Parameters: 1000 100*
View current status of the eoam RLS message option.	Use this command to view the current status of the eoam message option for RLS events. Note that the eoam function must be enabled before eoam commands will be invoked. See Volume 4 of this manual for more information on eoam. Sequence: **get rls shutdown policy** press Enter The system responds: *RLS shutdown notification policy: eoam-msg*
Change the current status of the eoam RLS message option.	This command enables or disables the option to send out an eoam message when an RLS event is triggered. Note that the eoam function must be enabled before eoam commands will be invoked. See Volume 4 of this manual for more information on eoam. Sequence: **set rls shutdown policy [port-down | eoam-msg]** Example: **set rls shutdown policy port-down** press Enter The system responds: *RLS shutdown notification policy is set to :port-down*
Save changes to mib	Saves the MIB to RAM. Perform this command save setting changes to FLASH. This command does not restart the system and does not put any new settings into effect. A system reset command will cause settings in RAM to be programmed into FLASH and to take effect. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

Required Action	Steps
reset system	Resets the system to save the settings to FLASH and restart the system with the new settings taking effect. Sequence: **reset system** press Enter The system responds: *Are you sure you want to reset? Y(yes) or N(no)* press **Y** Once the system reboots, login and continue with the RLS configuration.

This concludes the steps to configure Rapid Link Shutdown for the Horizon Compact Plus system using the CLI manager.

This page is left blank intentionally

15.0 Configuring the Time Source (SNTP)

The time and date can be entered into the Horizon system. This is maintained for as long as power is applied to the system. If power fails, then all timing information is lost. An accurate clock is necessary for time stamping entries in the events and performance logs.

To maintain the time and date in the system, five network sources of timing information are configurable. Either an Internet time source or an NTP server on your network may be used.

Simple Network Time Protocol (sntp) is used.

Five time sources are configured by default. Each time source is indexed 1 to 5. Indices 1 and 2 are from Industry Canada servers, 3 and 4 are from U.S. Navy servers and 5 is from a Swiss server. Any other time sources can be configured. The timing information is polled every 60 minutes.

Table 15-1 Time Sources

Index	Stratum	Source IP Address	Source
1	2	199.212.17.15	Industry Canada
2	2	199.212.17.20	Industry Canada
3	1	192.5.41.40	U.S. Navy
4	1	192.5.41.209	U.S. Navy
5	2	129.132.2.21	Switzerland

Procedure 15-1
Configuring the Horizon Time and Date

Required Action	Steps
login	Log in as a NOC user.
View date time	Returns the current date and time on the system. Sequence: **get date time** press Enter The system responds: *Date and Time : 28/09/2011 14:17:42*
Configure date time	Sets the system date and time if SNTP is not enabled. Sequence: **set date time [dd/mm/yyyy hh:mm:ss:ms]** press Enter Where dd – day (01 – 31) mm – month (01 – 12) yyyy – year (1970 – 2099) hh – hour (0 – 23) mm – minutes (0 – 59) ss – seconds (0 – 59) ms – milliseconds (0 – 999) The system responds: *Date and Time : [dd/mm/yyyy hh:mm:ss:ms]*
Save changes to mib	Saves the MIB to RAM. Perform this command save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

Procedure 15-2
Configuring the Time Source

Required Action	Steps
login	Log in as a NOC user.
View sntp settings	*Displays the current time settings. This example shows the Horizon Compact Plus system default settings.* *Sequence :* **get sntp** press Enter *The system responds :* *SNTP feature is turned on.* *Current system time: 12/10/2005 15:36:54. Last SNTP synch: 12/10/2005 15:27:41.* *Index | Status | Stratum | Name* *1 Good 2 199.212.17.15* *2 Good 2 199.212.17.20* *3 Good 1 192.5.41.40* *4 Good 1 192.5.41.209* *5 Good 2 129.132.2.21* ***Notes: SNTP servers are polled every 60 minutes.* *Search for SNTP server always starts at index 1, for every poll.* *System time will be set to first server found, every poll period.* *Stratum level supplied by SNTP server. 0 indicates not available.* *You can force a re-synch to all servers by setting SNTP 'on'.* *System will not automatically adjust to Daylight Savings Time.*
View sntp offset	*Displays the number of hours offset from GMT entered into the system.* *Sequence :* *get sntp offset press Enter* *The system responds (example shows an offset of -1.5 hours) :* *System time offset from GMT: -1.5 hours.* ***Notes: System will not automatically adjust to Daylight Savings Time.* *North America requires negative offset from GMT e.g. -5.0 hours*

Required Action	Steps
Configure sntp server	*Allows a new time source server to be entered.* *Sequence :* **set sntp server [index] [ip address]** press Enter *Where [index] is a number 1 to 5 corresponding to the desired time source index to be changed, and [ip address] is the ip address of the server providing the new time source.* *The system responds :* *Success: SNTP server information accepted.*
Configure sntp offset	*Allows the time difference from GMT to be entered, so that local time is available to the system.* *Sequence :* **set sntp offset [offset hours]** press Enter Note that the offset hours can be negative or positive, depending on your location relative to Greenwich, U.K. The maximum offset accepted is ±14 hours The system responds : *System time offset from GMT: [offset hours] hours.* ***Notes: System will not automatically adjust to Daylight Savings Time.* *North America requires negative offset from GMT e.g. -5.0 hours*
Configure sntp default	*Sets the five timing sources to the default values shown in the get sntp command shown at the beginning of this exercise.* *Sequence :* **set sntp default** press Enter *The system responds :* *SNTP default values will now be used.*
Save changes to mib	Saves the MIB to RAM. Perform this command save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

16.0 Adaptive Modulation

The two principal modulation schemes used on the Horizon Compact Plus system are QPSK and xQAM. QPSK (the lowest modulation scheme) is ideal for long distance, but has the lowest throughput capability.

Higher throughputs are achieved by using more complex modulation schemes e.g. 16-QAM, 32-QAM, 64-QAM, 128-QAM, 256-QAM. The higher numbers indicate a progressively more complex scheme and a higher bandwidth (throughput) capability e.g. 256-QAM is more complex than 128-QAM and provides a higher throughput. More complex modulation schemes are susceptible to noise and thus require a stronger signal for the demodulator to accurately decode the data stream. Consequently, the more complex the modulation scheme used, the shorter the distance limitation of the radio link.

If a system is using a given modulation scheme and weather conditions cause signal levels to deteriorate below acceptable levels (risking a link failure), changing the modulation scheme to a less complex (lower order) scheme, will allow the link to remain functional, although the throughput will be lower, until weather conditions improve. The modulation scheme can then be returned to the original scheme and the throughput returned to normal levels. Horizon Compact Plus has a Hitless Automatic Adaptive Modulation scheme.

16.1 Hitless Automatic Adaptive Modulation

The Horizon Compact Plus system can be configured to automatically switch to lower modulation schemes if environmental conditions deteriorate to the point where a wireless link may otherwise fail. Compact Plus will do this without causing a “hit” or losing data. This feature is called Hitless Automatic Adaptive Modulation (HAAM).

All radio bands available with the Horizon Compact Plus support HAAM.

Note that HAAM cannot be invoked if RLS, ATPC, or redundancy (not supported in this release) is enabled.
When HAAM is turned on, regardless of the user configured system mode (includes modulation scheme), the system switches to the highest modulation scheme available (system mode) for the radio band being used.

If weather conditions cause the Signal to Noise Ratio (SNR) to drop below the “Down SNR” threshold for the modulation scheme in use (see **Table 16-1**), the current modulation scheme will switch to the next lowest modulation scheme available. If the SNR continues to fall and drops below the “Down SNR” threshold for that modulation scheme, the system will switch again to the next lowest modulation scheme. If the SNR still continues to fall, the system will continue to downshift through all the available modulation schemes until it reaches the lowest order scheme for the radio band in use.

Example: Initial modulation scheme is 256QAM. If the SNR falls below the “Down SNR” threshold for 256QAM, which is 30 dB, the system will switch to 128QAM. The “Down SNR” threshold for 128QAM is 27.17 dB. If the SNR drops below this new threshold, then a modulation downshift will occur again to 64QAM. The system will continue downshifting as the SNR thresholds are encountered until QPSK is reached.

Table 16-1 Modulation Up/Downshift SNR Thresholds

	Regular, 10*-12 performance	
Mode	Up SNR, dB	Down SNR, dB
QPSK	22.84	N/A
16QAM	23.68	18.11
32QAM	26.00	21.42
64QAM	29.02	24.18
128QAM	31.53	27.17
256QAM	N/A	30.00

These values are common to all radio bands and channel bandwidths.

By default, the transmit power will remain the same as that allowed for the 256QAM modulation scheme, regardless of the modulation scheme currently operating. However, a maximum power can be configured so that power levels will not exceed this figure, regardless of the modulation scheme operating.

As conditions improve the SNR will increase. When the “Up SNR” thresholds are exceeded, then modulation upshift will occur. This will occur in steps as the “Up SNR” threshold for each modulation scheme is exceeded and until the 256QAM modulation scheme is reached.

HAAM is supported by all radio bands available to the Horizon Compact Plus, however, some jurisdictions may not allow its use.

There are ten CLI commands associated with HAAM:

- **get haam**
- **get haam status**
- **set haam [on/off]**
- **set haam manual mode [on/off]**
- **diagnose haam [up/down]**
- **get haam system modes***
- **get haam wtr****
- **set haam wtr****
- **get haam eoam option**
- **set haam eoam option**

*Definiton – haam system modes – the modes supported by both haam and the configured radio band.

**Definition - haam wtr - the wait to restore time in seconds is applicable in the lower mode. It is the minimum time the system has to spend in the lower modulation. When the system enters the lower mode the wtr timer is started. If the link improves within this time, the modulation is not shifted to a higher modulation scheme until this time has expired

The CLI commands are demonstrated in the procedure below:

Procedure 16-1
Configuring Hitless Automatic Adaptive Modulation

Required Action	Steps
login	Log in as a NOC user.
Check if haam is on or off	Displays the current on/off condition of Hitless Automatic Adaptive Modulation (HAAM). Sequence: **get haam** press Enter The system responds: *HAAM status: on/off*

Required Action	Steps
View haam status	Displays the current status of the HAAM setting. Note that HAAM cannot be invoked if RLS is enabled. Sequence : **get haam status** press Enter The system responds : *HAAM set to :off* *Configured HAAM modes:* *hy50_91_qpsk hy50_159_16qam hy50_205_32qam* *hy50_250_64qam hy50_296_128qam hy50_364_256qam* *Current running HAAM mode is :hy50_364_256qam* *HAAM manual mode set to :off* *Peer HAAM set to :on.* *Peer configured HAAM modes:* *hy50_91_qpsk hy50_159_16qam hy50_205_32qam* *hy50_250_64qam hy50_296_128qam hy50_364_256qam* Example system modes shown.
Enable haam	This command turns the Hitless Automatic Adaptive Modulation (HAAM) option on or off. Note that HAAM cannot be invoked if RLS, ATPC or redundancy is enabled. Sequence : **set haam [<on/off>]** Example: **set haam on** and press Enter The system responds : *HAAM is set to on!* *Change requires a 'save mib' and 'reset system'* *Would you like to 'savemib' now? Enter Y(yes) or N (no):*Y *Mib saved successfully.* *A 'reset system' is required for the change to take effect.*

Required Action	Steps
Configure the “wait to restore” time (wtr)	This command allows you to enter a time, in seconds, that the system will wait before upshifting the modulation scheme after the link improves. It is only applied when the system has downshifted to the lower available modulation scheme. Sequence: **set haam wtr [seconds]** press Enter Example: **set haam wtr 60** press Enter (sets a wait to restore time of 60 seconds) The system responds: *HAAM wait-to-restore value is is set to 60.* **get haam wtr** press Enter The system responds: *HAAM wait-to-restore value is 60.*
Configure the EOAM option	This command enables (on) or disables (off) the HAAM EOAM option. Sequence: **get haam eoam option** press Enter The system responds: *Eoam option for HAAM is: off.* **set haam eoam option on** press Enter The system responds: *Eoam option for HAAM is set to : on.*
Set the system to support the **diagnose haam [up/down]** command	Use this command to put the system into manual switching mode (on) or automatic switching mode (off). Note that manual mode needs to be enabled at both ends of the link for manual switching to work. This command works together with the **diagnose haam [up/down]** command. Sequence: **set haam manual mode [on/off]** Example: **set haam manual mode on** and press Enter The system responds: *Modem1 manual mode set :Success* *Warning:Please make sure that the peer system has the same configuration!*

Required Action	Steps
Manually change the modulation scheme for operational checking or troubleshooting.	Use this command to switch the modulation scheme up or down manually one modulation step at a time. The command **set haam manual mode on** must be invoked before this will work. Use the command **set haam manual mode off** once diagnostics have been completed. Sequence: **diagnose haam [up/down]** and press Enter Example : **diagnose haam down** press Enter The system responds: *Diagnostic status :Success;* *Previous: hy50_364_256qam;* *Current: hy50_296_128qam.* *HAAM interrupt status register: 0x1100044*
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*
Reset the system to make changes effective.	Resets (restarts) the system to save the settings to FLASH and restarts the system with the new settings taking effect. Sequence: **reset system** press Enter The system responds: *Are you sure you want to reset? Y(yes) or N(no)* press **Y**

This page is left blank intentionally

17.0 System Management

The Horizon Compact Plus system can be fully managed locally or remotely. Horizon Compact Plus supports Telnet access, SNMP management and a Web interface accessible through the IP network. Refer to Volume 1 of this manual for details of enabling Telnet access to the system. The entire Command Line Interface (CLI) command set is available through Telnet. The entire list of system parameters is available through SNMP access. The Web interface provides access to performance parameters and limited system configuration.

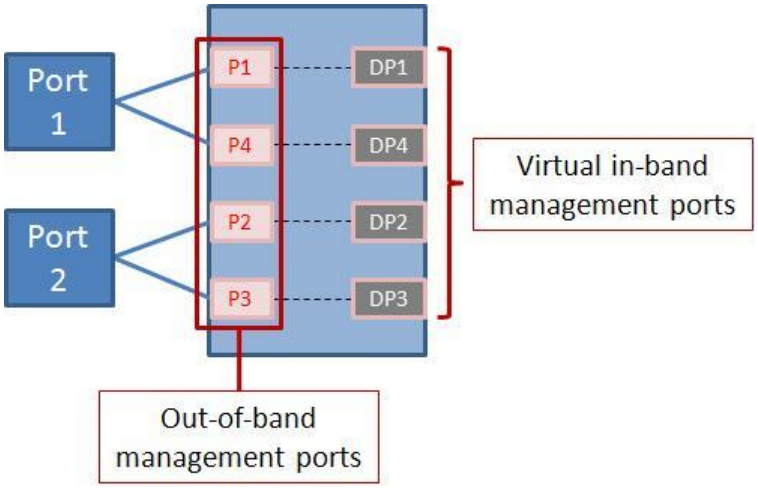
Management traffic can be configured as in-band or out-of-band.

17.1 In-band and Out-of-band Management

The Horizon Compact Plus has two physical 10/100/1000 Base-t (GigE) Ethernet ports, Port 1 and Port 2. Each physical port can also be independently configured as two virtual 10/100 Base-t data ports. Ethernet Port 1 becomes p1 and p4 and Ethernet Port 2 becomes p2 and p3. Associated with ports p1 through p4 are four virtual ports, dp1 through dp4.

Out-of-band management can be carried on any one of port p1 through p4. In-band management can be carried on any one of the virtual ports dp1 through dp4.

Both in-band and out-of-band management allow Telnet, or Web, sessions to be established through one Horizon Compact Plus system, over the radio link to the far end Horizon Compact Plus system. All management traffic must arrive on the configured port, or it will be ignored by the system.



Management traffic includes:

1. Telnet traffic and associated CLI commands
2. SNMP management
3. ping
4. FTP, used for configuration backup and restore and software upgrades.
5. HTTP

All ports may be configured to operate with or without management VLANs (see Section 7.0).

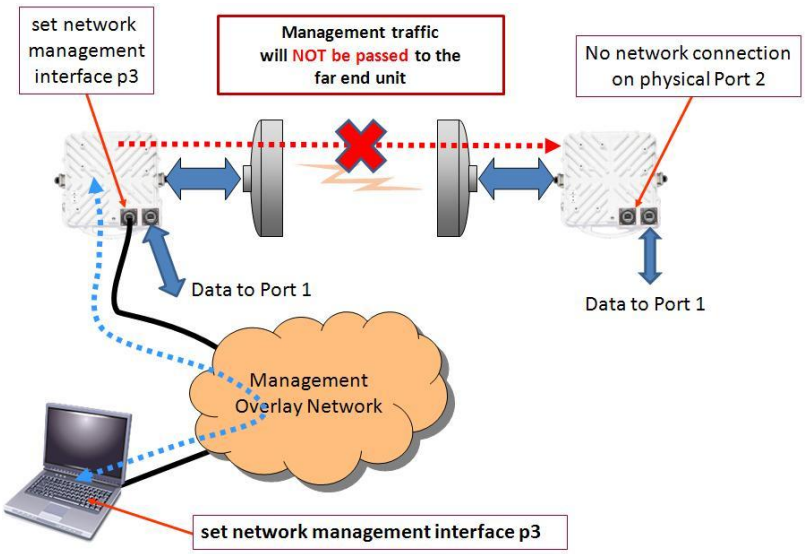
The key points to consider when choosing the system management configuration are as follows:

- Inband management reduces the port count requirement on the sub-tending switch, since no separate management port is required for management.
- Out-of-band management requires a separate switchport in the sub-tending switch to connect.
- Any port that is part of a port group cannot be used for in-band or out-of-band management (see Section 14.2).

To configure the management interface use the following procedure:

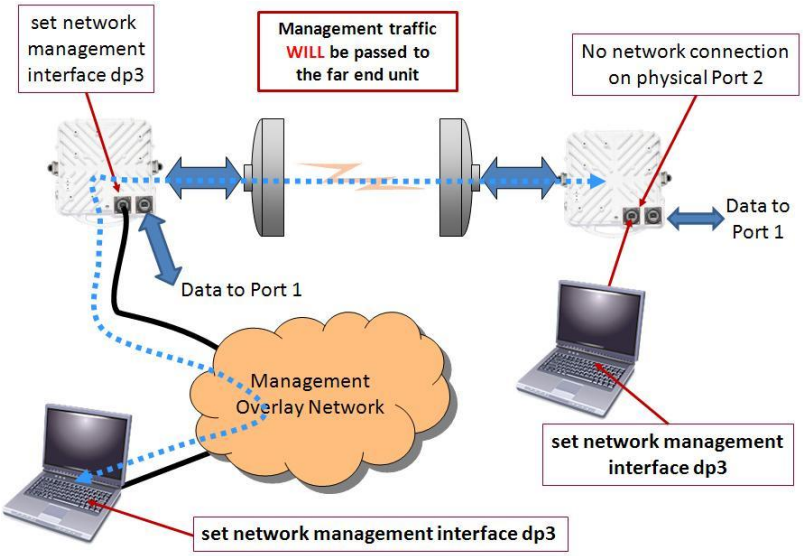
Procedure 17-1
Configuring Network Management Interface

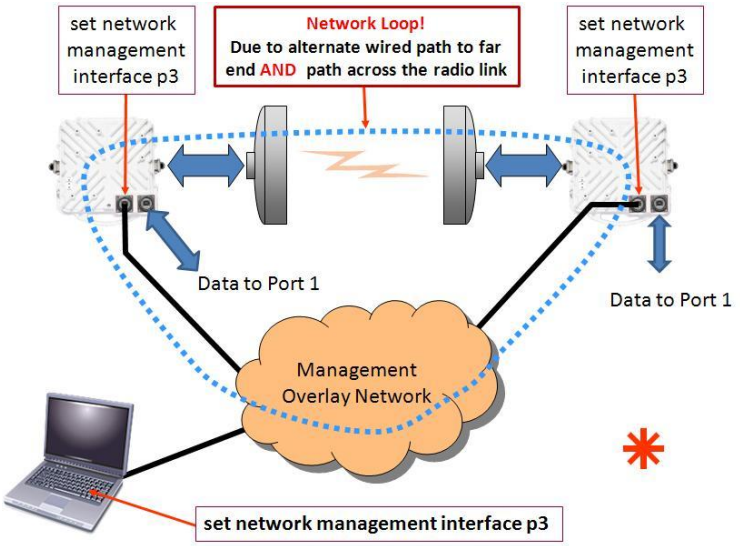
Required Action	Steps
login	Log in as the Super User.
Configure network management interface	This command sets the port on which management traffic will be carried and also the type of network management – in-band, or out-of-band. Select either dp1 through dp4 for in-band management, or p1 through p4 for out-of-band management. The following example changes the network management interface from in-band on dp3 to out-of-band on p1. Ensure that there is an associated physical connection for the port selected. Note that if you change the management port you will need to reconnect your PC to the new active port. Sequence : **set network management interface** press Enter The system responds: *#Press 'Ctrl-X' to exit config process* *#Press 'Enter' to retain previous value* (shown in brackets) *Port Name (dp3) ?* ***p1*** *Would you like to save MIB ? Enter Y(Yes) or N(No):y* *Apply the setting to system immediately.This operation may cause the loss of current connection!* *Continue? Enter Y(Yes) or N(No)y* *Mib saved successfully.Configuring management interface...* *Config Name* *User Config* *Running Config* *Port Name* : ***p1*** ***p1*** **Note: it is recommended that when using out-of-band management that the port payload state of the port concerned is set to "disabled". See Section 4.0 Configuring Ethernet Ports 1 and 2.**



The CLI command **set network management interface p3** (could be p2, p1, or p4 if the management is connected to corresponding port) configures the Horizon Compact Plus to only accept management traffic on p3 of the system connected through the network to the management station (PC). Full management of the near end is possible. Management of the far end unit over the radio link is not possible.

The CLI command **set network management interface dp3** (could be dp2, dp1, or dp3 if the management is connected to p2, p1, or p3 respectivey) applied at both ends of the link**,** configures the system to carry in-band management traffic across the radio link to the far end, allowing full management of both ends of the link. Note that there is no physical connecton to the management overlay network on the far end of the link.





When both the near and far end Horizon Plus units are configured with the same out-of-band management port (p3 in this example) and both are connected to the management overlay network, then a network loop is established, causing network failure.

17.2 Telnet Access

Once correctly configured, the Horizon Compact Plus is accessible through a Telnet session using Super User, NOC and Admin level user accounts. Refer to Volume 1 for details of CLI commands. The Horizon Compact Plus system can be completely configured, tested and managed through a Telnet session. The Telnet function is enabled by default but can be disabled within the Horizon Compact Plus system.

Procedure 17-2
Configuring Telnet Access

Required Action	Steps
login	Log in as the Super User.
View telnet access	Returns the status of Telnet access (on by default) Sequence : **get telnet access** press Enter The system responds: *telnet access is [on/off]*
Configure telnet access	Enables or disables Telnet access. Sequence : **set telnet access [on/off]** press Enter The system responds: *telnet access is [on/off]*
Save changes to mib	Saves the MIB to RAM. Perform this command to save configuration changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

17.3 Secure Shell Access Security

Telnet sessions over a network such as the Internet are not secure. User names and passwords, as well as commands and system responses, are transmitted in clear text during a Telnet session. A secure shell (SSH) protocol can be enabled in the Horizon Compact Plus system to ensure that access to the units is restricted to authorized clients. Horizon Compact Plus uses the Secure Shell SSH2 server programme to create the secure environment for Telnet sessions. SSH2 is a recognised industry standard, encrypting, security, programme. When enabled, SSH encrypts the entire Telnet session, including all usernames, passwords, commands and responses from the system. SSH also verifies that you are talking to the desired server by means of an authentication process using a “fingerprint”. The “fingerprint” is a unique identifier found only on the desired server.

A Secure Shell client programme needs to be installed on any computer which is to be used to manage a Horizon Compact Plus system with SSH enabled. A free SSH client programme (PuTTY) is available on the Web.

Note that both SSH and Telnet can be enabled at the same time. To ensure security, once SSH has been enabled, disable Telnet.

Also note that the Web server must be enabled on the Horizon before SSH can be enabled.

17.4 Configuring Secure Shell (SSH)

Use the following procedure to manage the SSH feature of the Horizon Compact Plus system.

Procedure 17-3
Configuring Secure Shell (SSH)

Required Action	Steps
login	Log in as the Super User.
View ssh server	Returns the status of the Secure Shell SSH2 server. Sequence : **get ssh server** press Enter The system responds: *ssh server is [on/off]*
Configure ssh server	Enables or disables the Secure Shell SSH2 server. Sequence : **set ssh server [on/off]** press Enter The system responds: *ssh server is [on/off]* *Note: The Web server must be ON before the SSH server can be enabled.* *A system reset is required before SSH will be invoked.*

Required Action	Steps
View ssh server fingerprint	Retrieves the fingerprint of the server Sequence : **get ssh server fingerprint** The system respond :
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*
Reset system	A system reset is required to activate this feature. Sequence **reset system** press Enter The system responds: *Are you sure you want to reset? Y(yes) or N(no)* press **Y** The system will proceed to reset. You will have to log on again to regain access.

17.5 Web Interface

This section provides an overview of the Horizon Compact Plus Web interface. To use the Horizon Compact Plus Web-based interface, you need a Desktop computer, laptop or mobile device with a Web browser and IP access to the Horizon Compact Plus system.

The Horizon Compact Plus Web interface is enabled by default. To disable the Web interface login to the system using Telnet and issue the CLI command **set web server off** press Enter.

17.5.1 Features

The following list describes the features of the Horizon Compact Plus Web interface:

- Remote system availability - the Web interface can be used on any computer having IP access to the Horizon Compact Plus system.
- Runs in a standard Web browser - the Web interface is supported on: Firefox 3.5 – Firefox 7.0, MSIE 8 – 9, but will work with most popular browsers such as Chrome, Safari and Opera .
- Requires no local software - the Web interface runs in the browser. All necessary software is stored on the Horizon Compact Plus system.
- Controlled access levels depending upon login type - Super User, NOC and Admin level functions are supported based upon login type.

- Password protected.
- SSL Web server - provides encryption for the Web session and verifies that the Web browser is indeed connecting to a Horizon Compact Plus system.
- Real-time view of the network - the auto-refresh capability allows real-time monitoring of the Horizon Compact Plus link.

17.5.2 Connecting to the Web Interface

You may connect to the system through an IP network, either from a location which is local to the Horizon Compact Plus Ethernet connection, or through a remote connection which has IP access to the Horizon Compact Plus system.

Notes:

User groups may be configured for mandatory use of HTTPS (SSL). If configured, those users (Super User, Noc, Admin) are required to access the Horizon Compact Plus Web interface through SSL. Attempts to access the modem through standard HTTP will result in the user being locked to the login screen.

If HTTPS (SSL) access is not required for the user group, then those users may choose between standard HTTP and HTTPS (SSL) access, as both modes will work.

When the computer is configured and connected, perform the following procedure.

Procedure 17-4
Connecting to the Web Interface

Perform this procedure to monitor and configure the Horizon Compact Plus system.

1. In the **Address** or **URL** bar of the Web browser, type the IP address of the Horizon Compact Plus System to be accessed. Press **Return**.
2. The system will respond and display the login screen.
3. Type your user name (with Super User, NOC, or Admin rights) and password.
4. Press **OK**. The Horizon Compact Plus home Web page launches.
5. Bookmark the page for easy reference later.

A Web browser may be used to configure the Horizon Compact Plus system, provided the IP address of the system is known (default value 192.168.10.100) and you log on as the default Super User. Refer to Volume 1 of this manual for logging on details and basic configuration.

The Horizon Compact Plus Web interface follows standard Web browser conventions:

- A text box allows keyboard input for that parameter
- Drop-down boxes display the list of available options for that parameter.

Notes:

1. the following functions are not supported through the Web interface :

- User account establishment and account management
- Software upload and download, including backup and restore of system configuration and user accounts
- Configure Horizon Compact Plus Type
- Ping

2. Configuration privileges correspond to the login level.

17.5.3 Exiting the Application

To exit the Horizon Compact Plus Web interface application, close the Web browser window. Closing the window will cause the user to be logged out of the system.

17.5.4 Login

The login page appears whenever you connect to the Horizon Compact Plus Web interface. The session will remain active for as long as your browser stays connected to the Horizon Compact. Due to security concerns, if the computer is unattended for any length of time, then it is recommended you disconnect from the Horizon Compact Plus Web interface by closing your browser window.

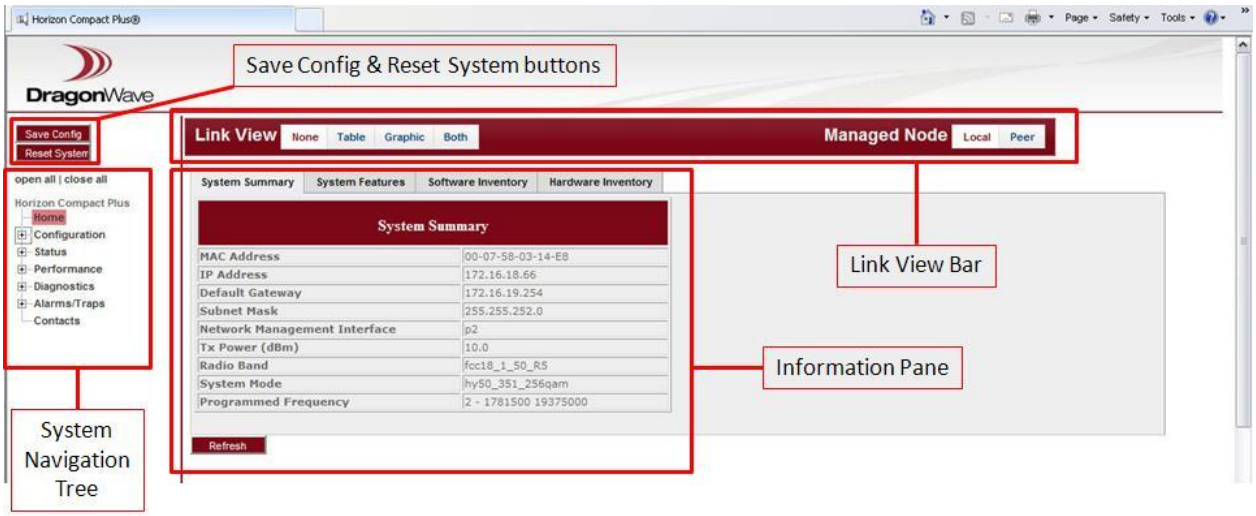
Horizon Compact Plus links (near and far end systems combined) support five simultaneous Web sessions. The five sessions can be comprised of any user account level.

Figure 17-1
Web Interface - Login Screen

17.5.5 Home Screen

The Horizon Compact Plus Web interface runs in a standard Web browser.

Figure 17-2 Web Interface - Home Screen



The **Link View Bar** Managed Node buttons switch management access between the Peer or Local Horizon Compact Plus nodes. In addition, a graphic view of the radio link and a real time status table for both ends of the link can be selected for viewing.

The **Information Pane** displays information related to the node being managed. Selecting either of the System Summary, System Features, Software and Hardware Inventory tabs reveals related information for the node being managed.

The **System Navigation Tree** provides access to all web configurable features for the node being managed.

To ensure that any changes that have been made to the system configuration are properly saved, you will need to click on the **Save Config** button. Some features also need the **Reset System** button to be clicked before changes become effective (this is traffic affecting). For some features that would normally require a Reset System, there is also the option to have any changes take effect immediately (not traffic affecting). Incorrectly applying these changes may result in a failed wireless link. Care must be taken to ensure that communication to the peer link is not broken if management of the peer link is still required to be performed over the wireless link after changes have been made.

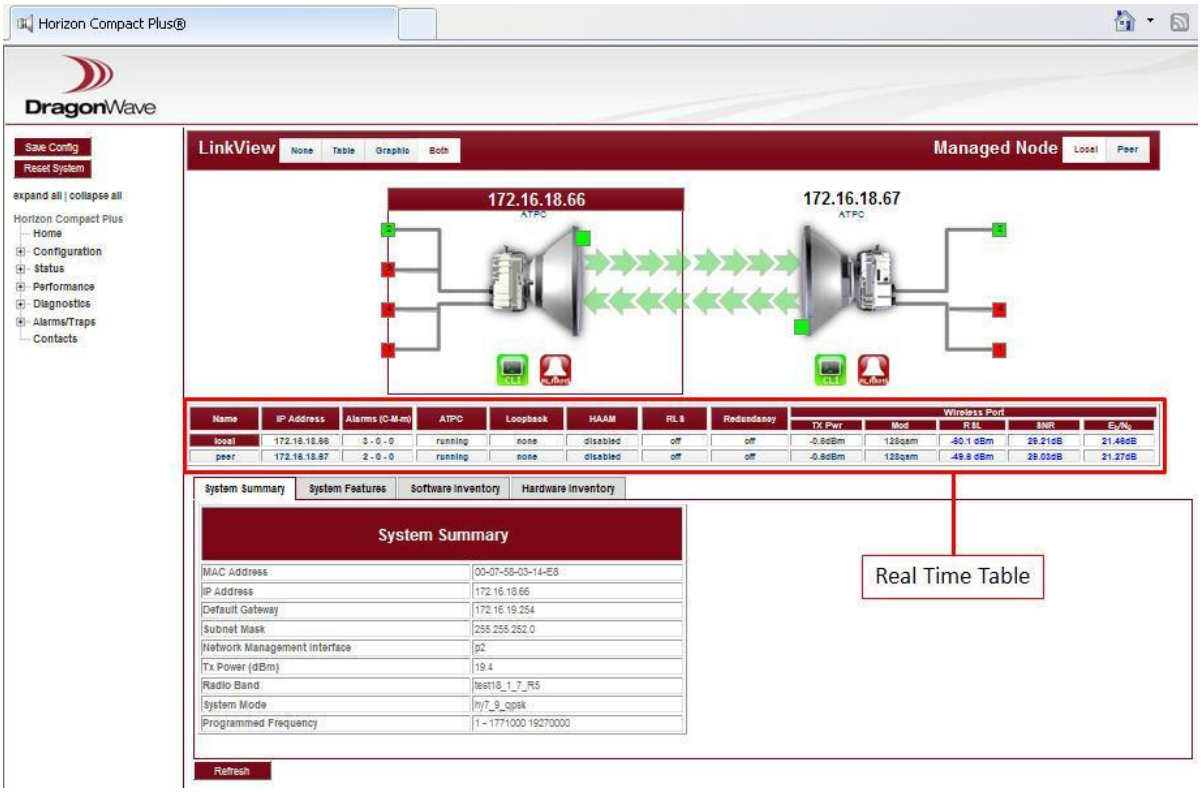
WARNING:

Changing these features may be used to change the radio configuration of an existing working link. If management of the far end Horizon Compact Plus is only via the radio link, then configure the far end radio first. Otherwise, if you configure the near end radio first, you will lose the link to the far end radio and be unable to manage or configure it.

17.5.6 Graphics and Table View

On the **Link View Bar** are the Link View buttons. A real time table of system status is displayed when you click on the **Table** button. The number of rows in the table will reflect the number of systems involved in the link (e.g. 2 rows for a basic link, 4 rows for a fully redundant link). All of the fields in the table are updated dynamically. When a field value changes the text colour changes to blue for a one second period. This draws the user's attention to changing values. The RSL, SNR and Eb/No values are examples of parmeters that may change frequently. Each cell in the table has a clickable hyperlink that displays the relevant configuration detail that manages that component in place of the Information Pane (see Figure 17-2). Clicking on the **Graphic** button shows a graphical representation of the radio link. Clicking on the **Both** button places both the Table and the Graphic features on the screen (see Figure 17-3).

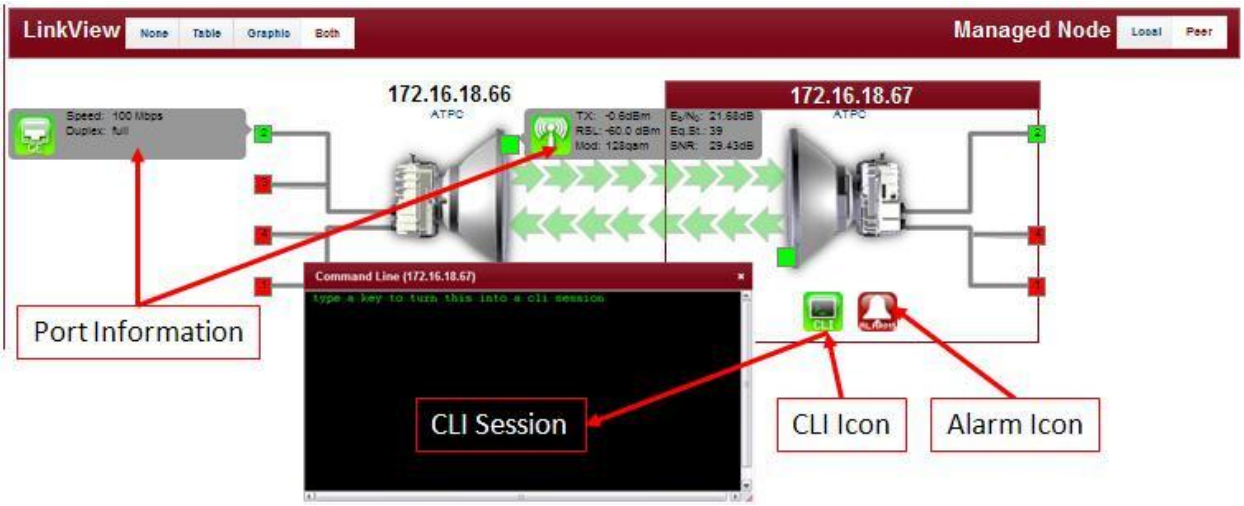
Figure 17-3 Web Interface – Graphics withTable View



Clicking on the **Managed Node** buttons allows you to select the local, or peer, node for management. This is valid for both the graphics view and with no graphics displayed. Also, clicking on the local (left hand) or peer (right hand) node icons selects that node for management. Figure 17-3 shows the left hand node is being managed with the node icon surrounded by a box and the ip address highlighted. The arrows shown ingressing and egressing the node icons indicate the status of connectivity between the nodes. Green arrows indicate that modem blocks are being successfully transmitted/received (sync). Red arrows indicate a failure to transmit/receive modem blocks (no sync).

Hovering the mouse cursor over a port icon (red, or green, square, or “handle”) on the graphic reveals information about that port. A green handle depicts a connected port and a red handle a disconnected port. Both Ethernet and wireless port handles are displayed. Click on a handle while hovering to pin, or un-pin, the information bubble to/from the screen. Clicking on any value shown in the bubble will link you to the relevant configuration detail which displays below the graphic in place of the Information Pane.

Figure 17-4 Web Interface – Graphics Features



When alarms occur, the alarm icon (bell) background colour will change to reflect the severity of the alarm (Red, Amber, Yellow, Green for Critical, Major, Minor and no alarms respectively). When hovering the mouse cursor over the alarm icon the number of Critical, Major and Minor alarms currently present is shown. Clicking on the number of active alarms links you to the related alarms detail which displays below the graphic in place of the Information Pane.

Hovering over the CLI icon reveals a “Web CLI” link. Click on “Web CLI” to open a CLI session with the selected node. Depending on what node you have initially logged onto, you may, or may not, be prompted for user name and password. You may then configure features that are not accessible via the normal web interface (e.g. user accounts). To expand the CLI session window drag the right hand bottom corner to the right and down. To close the CLI window click on the “X” in the top right hand corner of the CLI window.

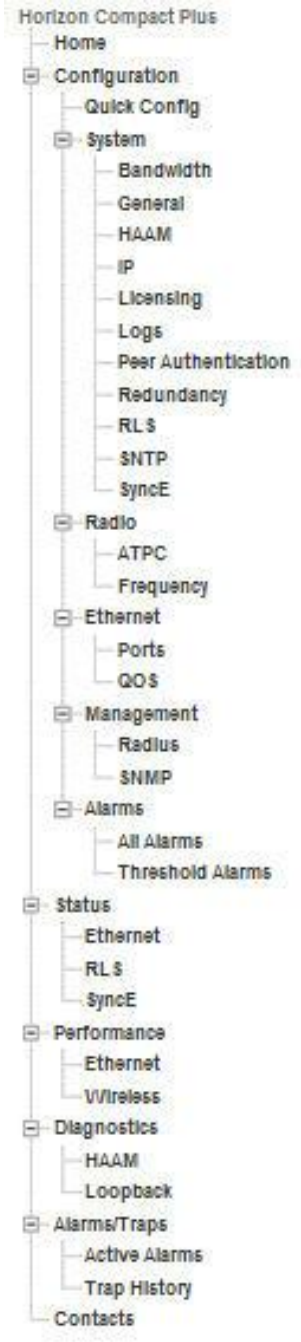
Figure 17-5 Web Interface – Graphics – Loss of Signal

Figure 17-5 shows the graphic display when a system node loses synchronization (down). The arrows are shown in green for the local node egress indicating that the local node is transmitting. The red arrows indicate that the peer node is not transmitting modem blocks and therefore the link is broken. In this instance the cause of the failed node in the figure was a system reset (traffic affecting). The rotating icon in the overlay indicates that the peer node will be trying to reconnect in 10 seconds.

17.5.7 Web Page Tree Diagram

Figure 17-6 maps the information and configurable features available via the Web interface.

Figure 17-6 Web Interface – Tree Diagram



Clicking on any of the features listed in the Tree Diagram results in a feature dedicated display to appear in place of the Information Pane. The features relate to the current node being managed.

Changing the value or status of some configurable radio features, that would normally require a Reset System before they become effective, can be applied immediately without a Reset System being applied.

WARNING:

Changing these features may be used to change the radio configuration of an existing working link. If management of the far end Horizon Compact Plus is only via the radio link, then configure the far end radio first. Otherwise, if you configure the near end radio first, you will lose the link to the far end radio and be unable to manage or configure it.

17.6 Secure Sockets Layer (SSL) Web Server

The Horizon Compact Plus Web server can be configured for Secure Sockets Layer (SSL). The Web server may be configured to operate in standard mode or in SSL mode. Horizon's SSL Web server is HTTP 1.0/1.1 compliant, features full support of HTML 2.0, 3.2, 4.0 and supports SSL 3.0.

Secure Sockets Layer, SSL, is the standard security technology for creating an encrypted link between a Web server and a browser. This link ensures that all data passed between the Web server and browser, remain encrypted. In order to be able to verify it's identity to web clients, a web server requires a valid SSL Certificate.

Once generated, the web server's certificate may be held as a private certificate or it may be registered with a Trusted Certificate Authority such as:

- Microsoft Root Authority
- Thawte Server
- GTE Cybertrust Root
- VeriSign RSA Secure Server

SSL access can be enabled on a per-user group basis. SSL access can be invoked for the Super User, for all NOC accounts, for all Admin accounts, or any combination of the three. Once SSL access has been enabled for the user group then all members of that user group can use SSL to connect to the Horizon Compact Plus Web browser. Even if SSL access is not required for the user group, those users may access the Horizon Compact Plus Web browser through HTTPS (SSL) as a security measure.

17.6.1 What is SSL?

SSL stands for Secure Sockets Layer. The SSL protocol, developed by Netscape, is supported by all popular Web browsers such as Internet Explorer, Netscape, AOL and Opera. An SSL certificate, issued by a Certification Authority (CA), must be installed on the Web server in order for SSL to work. SSL can then be used to encrypt the data transmitted (secure SSL transactions) between a browser and Web server. Browsers indicate an SSL secured session is active by changing the URL from http to https and by displaying a small padlock in the bottom toolbar.

SSL works as follows:

1. A browser requests a secure page (usually through the https:// format within the URL).
2. The Web server sends its public key with its certificate.
3. The browser checks that the certificate was issued by a trusted party (usually a trusted root Certificate Authority), that the certificate is still valid and that the certificate is related to the site contacted. The browser keeps a list of trusted Certificate Authorities. New CA's may be added to the browser by the user.
4. The browser then uses the public key, to encrypt a random symmetric encryption key and sends it to the server with the encrypted URL required as well as other encrypted http data.
5. The Web server decrypts the symmetric encryption key using its private key and uses the symmetric key to decrypt the URL and http data.
6. The Web server sends back the requested html document and http data encrypted with the symmetric key.
7. The browser decrypts the http data and html document using the symmetric key and displays the information.

17.6.2 Generating a Certificate

In order to generate a valid SSL certificate on the Horizon Compact Plus, the user must be logged in as the Super User, and the system time must be accurate. The SSL certificate is tied to the Horizon Compact Plus's IP address. If the IP address is changed, then the SSL certificate should be regenerated. Otherwise the browser SSL session will allow access but it will report that the certificate is invalid. In this situation, it is the browser user's responsibility to verify that the proper Horizon Compact Plus is being accessed and that the invalid certificate is due to an IP address change. Note, the underlying SSL connection between the browser and the Horizon Compact Plus is still encrypted.

Procedure 17-5
Generate SSL Certificate on the Horizon Compact Plus

Perform this procedure to generate an SSL certificate on the Horizon Compact Plus.

Note: To perform this procedure, you must have Super User rights.

Required Action	Steps
login	Log in as the Super User.

Required Action	Steps
View ssl certificate status	Displays the status of the modem's SSL certificate. Sequence: **get ssl certificate status** press Enter The system responds : ---------- *SSL Certificate Information* *Certificate:* *Data:* *Version: 3 (0x2)* *Serial Number: 2 (0x2)* *Signature Algorithm: sha1WithRSAEncryption* *Validity* *Not Before: Apr 15 21:03:15 2010 GMT* *Not After : Jun 14 21:03:15 2010 GMT* *Subject: C=US, O='Default Company Inc', CN=192.168.12.108.* *Certificate IP Address is not valid.*
create ssl certificate	Creates an SSL certificate on the Horizon Compact Plus system. Once created, users may access the Horizon Compact Plus system Web interface through HTTPS (SSL). The SSL certificate is linked to the Horizon Compact Plus IP address. If the Horizon Compact Plus IP address is changed, then the certificate should be regenerated. Make sure the system time on the Horizon Compact Plus is accurate before proceeding further (from CLI use “get date time” to verify this). Sequence: **create ssl certificate [<duration> <country> <company name>]** press Enter Where **<duration>** is the period in days for which the certificate will be valid, **<country>** is a two letter country code and **<company name>** is the nameof your company. Example – **create ssl certificate 730 US ClearWire.** This generates a valid DragonWave-signed certificate that the web server will now use, valid for two years. The system responds: *Certificate generation in progress...please wait a few seconds...* *Certificate Generation was Successful.* *Embedded web server is now using the newly generated certificate.* *Please accept the certificate in your web client when prompted.*

Required Action	Steps
View ssl certificate status	Perform this step to verify the certificate is active. Displays the status of the modem's SSL certificate. Sequence: **get ssl certificate status** press Enter The system responds : --- *SSL Certificate Information* *Certificate:* *Data:* *Version: 3 (0x2)* *Serial Number: 1 (0x1)* *Signature Algorithm: sha1WithRSAEncryption* *Validity* *Not Before: Jun 2 14:47:48 2010 GMT* *Not After : Nov 3 14:47:48 2013 GMT* *Subject: C=US, O=DragonWave Inc., CN=192.168.255.51* *Certificate IP Address is valid.*

This concludes the steps to generate an SSL certificate on the Horizon Compact Plus using the CLI manager.

17.6.3 Installing Certificates on Your Web Browser

Browsers keep a list of trusted Certificate Authorities (CA) in order to verify SSL certificates. A default list of CA's is included with the browser software. New CA's can be added to the browser by the user.

Since the DragonWave certificate does not commonly appear in a browser's list of authorities, you will need to install it yourself. Once you have installed the DragonWave certificate in your browser's database for trusted root authorities, you can securely communicate with devices running the Horizon Compact Plus Secure Web server.

Please refer to your Web browser's documentation for instructions on installation of certificates on your particular browser.

These instructions are provided as an example as to how to install the certificate in Mozilla FireFox version 3.5.6.

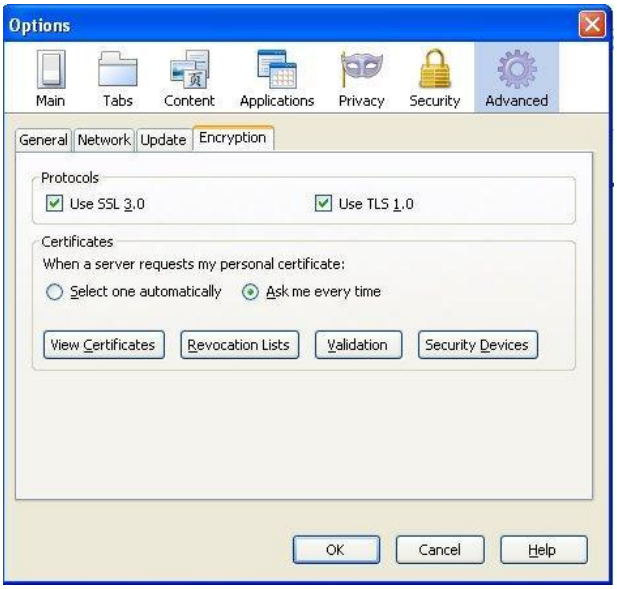
Note 1: As of this release the CLI command "save certificate ftp", as demonstrated in step 1 of Procedure 16-6, is not yet a valid command. Log onto the DragonWave Inc. web site and download the certificate file "dwicacert.pem" and continue Procedure 16-6 starting at step 2.

Procedure 17-6

Install SSL Certificates on Your Web Browser

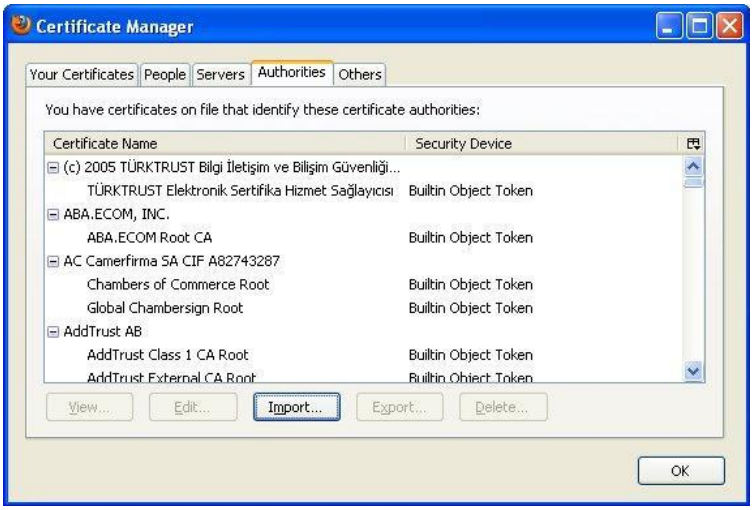
Perform this procedure to install the DragonWave SSL certificate on your Web browser.

1. **See Note 1 above before proceding.** Sign on Download the DragonWave SSL certificate with Super User rights from CLI with the command "save certificate ftp:dwicacert.pem" to a trusted location on a trusted ftp server.

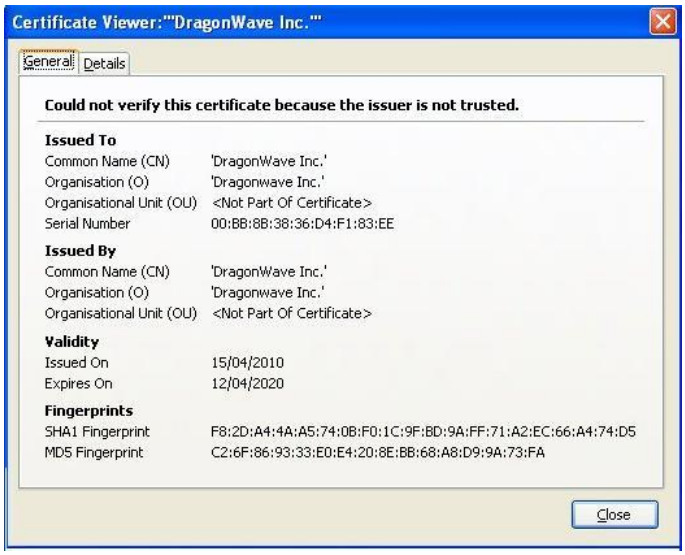


2. From the Firefox web browser, open the Tools Menu, click Options, select the Advanced tab, select the Encryption tab, and the following window should appear:

3. Now click the "View Certificates" button, then on the Certificate Manager window, click the Authorities tab.



4. Click the Import button, and choose the dwicacert.pem file that was downloaded above. Be sure to check mark the "Trust this CA to identify web sites," box, then click the View button, and it should look something like the following:



5. Click Close and click OK, and click OK again on the Certificate Manager window (the new DragonWave certificate should be in the list of CA's).

At this point, you have installed the DragonWave certificate in the list of trusted certificate authorities. Your browser should now silently accept the HTTPS communication being offered by the Horizon Compact Plus Secure Web server.

17.6.4 Enabling SSL per User Group

Web interface access for each user group may be configured so that SSL use is mandatory. If the use of SSL is not mandatory for a user group then that group can choose between standard HTTP access and HTTPS (SSL) access. For example, SSL may be made mandatory for all Noc and Admin level users, but not required for the Super User.

Procedure 17-7
Configure Mandatory SSL Access for Each User Group

Perform this procedure to configure mandatory SSL access to the Horizon Compact Plus modem for each user group.

Note: To perform this procedure, you must have Super User rights.

Required Action	Steps
login	Log in as the Super User.
get http secure access status	Displays the status of the user group's mandatory SSL access to the Horizon's Web interface. If the secure access is not required then users may access the Web interface both through standard HTTP and through HTTPS (SSL). Sequence: **get http secure access [user group]** press Enter where **[user group]** is one of: Super, Noc, Admin Note: **[user group]** is case sensitive. The system responds: *The HTTP Secure access for [user group] users is [not enabled/enabled]* Example: *The HTTP Secure access for Noc users is not enabled.*
set http secure access	Sets the SSL access to mandatory for the selected user group. Once set, the user group must access the Horizon Compact Plus Web interface using HTTPS (SSL). Standard Web access through HTTP will be restricted for that user group. Sequence: **set http secure access [user group] [on/off]** press Enter The system responds: *The HTTP secure access is set successfully.*
save mib	Saves the MIB to RAM. Perform this command save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

This page is left blank intentionally

18.0 Event and Performance Logging

The Horizon Compact Plus system supports two logs, the Events Log and the Performance Log. Each can be used to track the behaviour of the system over time. In addition, a "Syslog" feature can be invoked that sends information stored in the event and performance logs to a remote syslog server, for further analysis.

18.1 Events Log

The Events Log is invoked or disabled by issuing the CLI command **set logging [on/off].** This log records alarm and reset events. Approximately 17,500 events can be captured by the Events log. Once the log is full the oldest entries are overwritten. See Procedure 18-1 for more details.

Procedure 18-1
Events Log

Required Action	Steps
login	Log in as a NOC account
View events log status	This command returns the status of the events log Sequence : **get logging** press Enter The system responds : *Logging has been :[enabled/disabled.]*
View log entries	This command lists all events entries in the log since the log was enabled, or after it was last cleared. Ctrl-c aborts the listing. Sequence : **get log entries** press Enter The system responds : *Start of log ...* *0 10/07/2005 11:31:36 0 225017 477 W Demodulator lost synchronization* *0 10/07/2005 11:31:36 0 225016 476 W Link is down* *0 10/07/2005 11:31:36 0 225015 475 I cold start* *0 10/07/2005 11:31:36 0 225014 474 W auto negotiation duplex mismatch* *0 01/01/1970 00:00:11 0 225013 473 I Initialized Radio Manager* *0 01/01/1970 00:00:02 0 225012 472 I Flash Log is initialized* *<<<<Press any key to continue.....>>>>* *End of log.*
Configure events logging	This command enables and disables events logging Sequence : **set logging [on/off]** press Enter The system responds : *Logging is :[on/off]*

Required Action	Steps
save log	Saves the events log to a specified ftp server. Sequence : **save log ftp:[mylogfile]** press Enter Note: The maximum system log file size for ftp to a server holds about 1200 events (100KB). If more than 1200 events are stored on the system, then multiple files will be created and named as "mylogfile1", "mylogfile2" etc. The system responds (example): *Enter the IP address of FTP server followed by 'Enter' Key :[ip address]* *220 ProFTPD 1.2.5 Server (Dragonwave FTP Site) [support.dragonwaveinc.com]* *UserName :username* *331 Password required for username.* *Password :******* *230 User username logged in.* *Copy log entries to a file? Enter Y(yes) or N (no):y* *Trying to copy the data to mylogfile File. Please wait for a while.* *200 PORT command successful.* *150 Opening ASCII mode data connection for mylogfile.* *226 Transfer complete.* *Data successfully transferred to specified file. 221 Goodbye.*
erase log	Removes all entries from the events log Sequence : **erase log** press Enter The system responds : *Erased log succcessfully.*

18.2 Performance Log

Issuing the CLI command **set performance logging [on/off]** enables or disables the Performance Log. This log collects system performance information at time intervals that are configured using the CLI command **set performance log interval [hh:mm:ss].** See Procedure 18-2 for more details.

Between 6000 and 8000 entries can be logged before the Performance Log memory is full. Once the memory is full, new entries will overwrite the oldest entries. The following table assumes that an average of 7000 entries will occur before memory overflow. If the memory accepts more entries, then the log duration before overflow will be extended.

Procedure 18-2
Performance Log

Required Action	Steps
login using NOC account	Log in as a NOC account
View performance logging	Returns the status of performance logging Sequence : **get performance logging** press Enter The system responds : *Performance Logging has been :[enabled/disabled.]*
Configure performance logging	Allows you to enable or disable performance logging Sequence : **set performance logging [on/off]** press Enter The system responds : *Performance Logging is :[on/off]*
Configure performance log interval	Sets the time interval between performance log updates Sequence : **set performance log interval hh:mm:ss** press Enter Where **hh** is in hours, **mm** is in minutes and **ss** is in seconds. Note that the maximum interval allowed is 24 hours and the minimum is 15 seconds. The default setting is 15 minutes. See for log durations for different intervals. The system responds : *The performance logging interval is set to: hh:mm:ss*
View performance log	This command lists all performance entries in the log since the log was enabled, or after it was last cleared. Ctrl-c aborts the listing. Sequence : **get performance log** press Enter The system responds : *Start of Performance log ...* *SNR Eb/No RSL Temp Avg.BW PeakBW* *1 06/21/2007 13:15:09 0 526172 I 8.71 6.08 -44.88 30.5 68 85* *1 06/21/2007 12:29:56 0 526171 I 8.32 5.69 -44.75 30.6 66 90* *End of Performance log.*
erase performance log	Erases the performance log Sequence : **erase performance log** press Enter The system responds : *Erased log successfully.*

Table 18-1 Performance Log Durations

Logging Interval	Log Duration
15 secs (minimum)	~ 29 hours
1 minute	~ 116 hours (~ 4.8 days)
15 minutes (default)	~ 73 days (~ 2.4 months)
1 hour	~ 292 days (~ 9.7 months)
24 hours (maximum)	7000 days (~ 19.2 years)

18.3 Syslog Feature

Note that events and performance data are always being collected and stored, but only made available for viewing by the user when the logs are enabled. However, these data are always available to the Syslog feature, whether or not the events and/or performance logs are enabled.

The Syslog feature is invoked by configuring the IP address of a remote syslog server on the network using the CLI command **set syslog forwarding host [ip address]** and then turning on log forwarding. (See Procedure 18-3 for more details).

Procedure 18-3
Syslog Feature

Required Action	Steps
login using NOC account	Log in as a NOC account
Configure the IP address of the syslog server	Sets the IP address of the PC on which the Syslog Server is running. Sequence : **set syslog forwarding host [ip address]** press Enter The system responds : *Successfully set syslog forwarding destination IP address to [ip address]* *To turn on forwarding, execute 'set syslog forwarding on'.*
Turn on Syslog forwarding	Turns on syslog forwarding. Sequence : **set syslog forwarding on** press Enter The system responds : *Set forwarding rule 'on'* *Syslog Forwarding Admin Status : on* *Syslog Forwarding Oper Status : off (waiting for first send request)*

Required Action	Steps
Changing the IP address of a Syslog Server	If you want to change a Syslog Server IP address and the current Syslog Server is already running, first turn off syslog forwarding. Sequence : **set syslog forwarding host [new ip address]** press Enter The system responds : *Error : Could not update syslog server IP address because it is currently turned 'on'. Please turn 'off' and then change the IP Address.* **set syslog forwarding off** press Enter The system responds : *Set forwarding rule 'off'* *Syslog Forwarding Admin Status : off* *Syslog Forwarding Oper Status : off (Admin state is 'off')* **set syslog forwarding host [new IP address]** press Enter The system responds : *Successfully set syslog forwarding destination IP address to [new IP address]* *To turn on forwarding, execute 'set syslog forwarding 'on'.* **set syslog forwarding on** press Enter The system responds : *Set forwarding rule 'on'* *Syslog Forwarding Admin Status : on* *Syslog Forwarding Oper Status : off (waiting for first send request)*
View syslog status	This command returns the status of the syslog server. Sequence : **get syslog forwarding status** press Enter The system responds : *Syslog Forwarding Admin Status : on* *Syslog Forwarding Oper Satus : on*
View the IP address of the syslog server	Use the following command to return the current syslog server IP address. Sequence : **get syslog forwarding host** press Enter The system responds : *Syslog Forwarding Host : [IP address]*
Save changes to mib	Saves the MIB to RAM. Perform this command to save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*

This page is left blank intentionally

19.0 Radio and Network Loopback

Horizon supports three types of loopback:

1. Radio
2. Network
3. EOAM – see Volume 4 for more details

Only one of any type can be applied at any one time on any Horizon Compact Plus node.

Note that there is a traffic hit when entering or leaving a loopback mode.

Figure 19-1 shows a graphical representation of the Radio Loopback and the Network Loopback

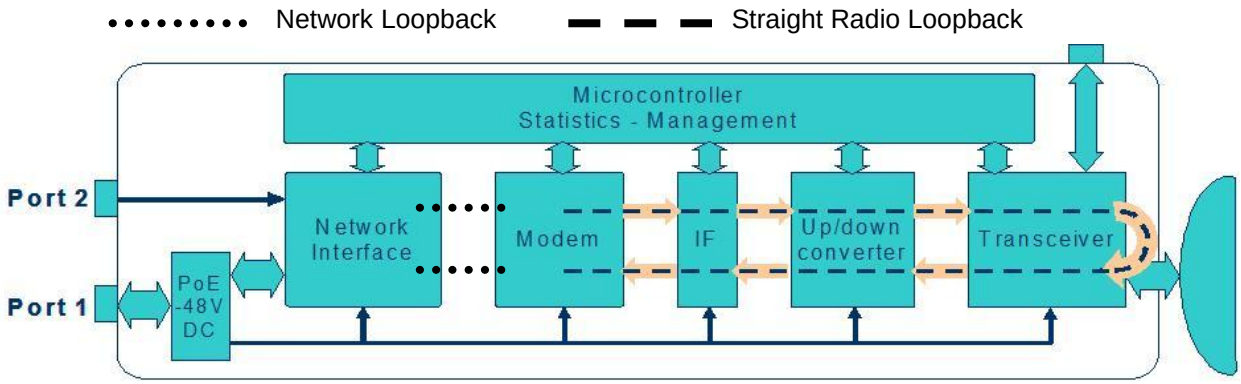


Figure 19-1 Radio/Network Loopback

19.1 Radio Loopback

Horizon provides a radio loopback facility for analysis of transmit or receive path issues. Invoking a radio loopback is service affecting and will stop all data transfer. There are two options:

- Straight radio loopback - Ethernet traffic is not looped back to the network, Ethernet traffic is discarded and the RF portion of the Horizon unit is placed in loopback
- Radio loopback plus network option – Ethernet traffic and the radio are placed in loopback

During the loopback, if the modem transmitter loss of sync alarm is not active, then both the transmitter and receiver of the Horizon unit under test are functioning correctly. A user configurable time limit can be applied to the loopback feature (default is 30 seconds). Once the time limit has expired the loopback will be automatically removed. Note that the far end transmitter should be muted when analysing the near end system using the radio loopback feature.

Procedure 19-1
Radio Loopback

Required Action	Steps
login into **far end system**	Log in as a NOC account

Required Action	Steps
MUTE FAR END TRANSMITTER	This command mutes and unmutes the radio transmitter Sequence: **set radio transmitter state off [yyy]** Where **yyy** is the time in seconds after which the radio will automatically turn back on. Omitting the **yyy** will maintain the radio off indefinitely untill a **set radio transmitter on** command is issued. The system responds: *Radio transmitter state is [on|off]*
login into **near end system**	Log in as a NOC account
View radio loopback status	Returns the status of the radio loopback feature. Sequence: **get radio loopback** press Enter The system responds: *radio loopback is [on/off][time][network]*
Configure radio loopback	Enables and disables the radio loopback option. This feature allows the radio transmitter and receiver system to be tested. In one option the data signal is dropped and the radio signal alone is looped back. In the second option, the data as well as the radio signal is looped back. When in loopback, if no loss of synch alarm is raised, then this indicates that the radio transmit and receive portions of the system are working correctly. Note that this command is service affecting. The default time limit before the loopback is automatically removed is set to 30 seconds. Setting the time parameter to zero (0) maintains the loopback in place indefinitely, until it is turned off. Sequence : **set radio loopback [on/off] [time][network]** press Enter Where **time** is in seconds Option 1 **set radio loopback on** press Enter Radio loopback only with default time limit s**et radio loopback on 45 network** press Enter Radio and network loopback initiated with a timeout period of 45 seconds The system responds (Example) : *This may affect user traffic. Continue? Enter Y (Yes) or N (No)* ***Y*** *Radio loopback is on 45 network* **NOTE: setting the time to zero (0) will maintain the loopback condition on indefinitely. To stop the loopback, issue the following command:** **set loopback off** press Enter

19.2 Network Loopback

The network loopback feature allows network troubleshooting between a Horizon Compact Plus and another network device. The MAC address of the target device is included in the CLI command to invoke the loopback. The source and destination MAC addresses are swapped so that loopback packets may legally navigate a switched Ethernet network. Loopback packets may be directed into any one of the five user QoS queues.

- The queue and the timeout parameters are optional. The default queue is 1 and the default timeout is 30 seconds.
- If a timeout is applied then the loopback is removed when the timeout expires.
- A timeout of 0 means that the loopback needs to be manually removed.
- Network loopback is not saved in the mib and is removed automatically upon reboot.
- A link must be operational in order to enable a far-end loopback.
- If the link goes down then a far-end loopback is terminated.
- Only a single loopback of any type (radio, network, eoam) is allowed at a time on a node.
- If one type (far-end or near-end) of network loopback is active at one end of a link then the same type of network loopback is allowed at the other end of the link however the opposite type of loopback is not permitted. For example, if a near-end loopback is enabled at a node then a far-end network loopback cannot be enabled at the other end of the link, however a near-end network loopback could be.
- Loopback packets must be a multiple of 4 bytes in length, not less than 64 bytes and not more than 500 bytes.
- Live traffic takes priority over network loopback packets, so some network loopback packets may be lost in the presence of a large amount of live traffic.
- The following destination MAC addresses cannot be looped back:
    1. All zeroes 00:00:00:00:00:00
    2. Any broadcast or multicast address
    3. The MAC address of the local node
    4. The MAC address of the peer node

Procedure 19-2
Network Loopback

Required Action	Steps
login into the system.	Log in as a NOC account
View the status of the network loopback feature	Use this command to return the current status of network loopback. Sequence: **get network loopback** press Enter The system responds: *No loopback active*

Required Action	Steps
Invoke a network loopback	Use this command to invoke a near-end or far-end network loopback to a specific MAC address. The system responses are the same for both near-end and far-end loopbacks. Sequence: **set network loopback nearend|farend xx:xx:xx:xx:xx:xx [queue <queue>] [<time>]** Where : **xx:xx:xx:xx:xx:xx** is the destination MAC address of the target device **<queue>** is the number of the target queue (1 to 5) and is optional. Default is queue 1. **<time>** is the time after which the loopback is automatically removed and is optional. Default time is 30 seconds. Example: **set network loopback nearend 60:50:40:30:20:10 queue 2 45** press Enter The system responds: *This may affect user traffic. Continue? Enter Y(Yes) or N(No): y* *Network Loopback is : on* **get network loopback** press Enter *The network loopback is active* *Location : Near end* *Destination MAC : 60:50:40:30:20:10* *User Queue : 2* *The loopback will terminate automatically at 30/06/2010 16:48:27*
Manually terminate a loopback.	A loopback that has been applied with a time parameter of 0 (zero) is maintained indefinitely (except on system reboot). To terminate the loopback, or to terminate before a configured set time has fully elapsed, use the following command: Sequence: **set network loopback off** press Enter The system responds: *This may affect user traffic. Continue? Enter Y(Yes) or N(No) :y* *Network loopback is: off*

19.3 EOAM Loopback

Note that only one type of loopback (Radio, Network or EOAM) can be invoked on a Horizon Compact Plus at any one time. See Volume 4 of this manual for more details about EOAM.

20.0 Network Management

This section describes how to use network management to manage the Horizon Compact Plus units.

20.1 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an application-layer protocol used to exchange management information between network devices. Network management systems contain two primary elements: a manager and an agent. The manager resides on a Network Management Station (NMS). The NMS is a console through which the network administrator performs network management functions. Agents reside on the network devices such as bridges, hubs, routers, or network servers. The Horizon Compact Plus system is a network device that contains an agent.

The SNMP manager uses Management Information Bases (MIBs). MIBs are a collection of definitions of the properties for the managed objects. Every managed device keeps a database of values for each definition written in the MIB. There are several standard MIBs provided in each NMS software package. These MIBs are common parameters for network devices such as unit health and IP traffic statistics. Each manufacturer typically provides an Enterprise MIB. The Enterprise MIB is a collection of definitions that address the particular aspects of the manufacturer's product. These Enterprise MIBs must be loaded onto the NMS, in other words, they must placed in the MIB "database" directory and enabled, in order for the NMS to access the parameters.

SNMP includes a limited set of management commands and responses. The management system issues Get and Set commands and the agent sends a response message in return. The Get command reads a parameter, and the Set command will configure, or assign a value to, a parameter. The managed agent also sends an event notification, called a *trap,* to the management system to identify the occurrence of conditions such as thresholds that have been exceeded.

Each SMNP managed object belongs to a community, or group. The Network Management Station may belong to multiple communities. The community string must be set in the agent device in order for the NMS to access the device.

20.2 Supported SNMP Versions

DragonWave Horizon Compact Plus systems support three versions of SNMP.

- Version 1 (SNMP v1) is the initial implementation of SNMP.
- Version 2 (SNMPv2c) is the second release of SNMP, which has additions and enhancements to data types, counter size and protocol operations.
- Version 3 (SNMPv3) is the most recent version of SNMP. The functionality of SNMPv1 and SNMPv2c remain intact, but SNMPv3 has significant enhancements to administration and security.

SNMPv3 is an interoperable standards-based protocol that provides secure access to devices by authenticating and encrypting packets over the network. The security features provided in SNMPv3 are as follows:

- Message integrity
- Authentication
- Encryption

Procedure 20-1
Setting up SNMP

Perform this procedure to set up SNMP for the Horizon Compact Plus system.

Required Action	Steps
login	Log in as a NOC account for SNMP v1 and v2c, or Super user for SNMP v1, v2c and v3
Configure snmp access mode [v1/v2c/v3/off]	Selects a SNMP access mode. The default mode is SNMP mode v1. Sequence: **set snmp access mode [v1/v2c/v3/off]** press Enter The system responds: *SNMP Mode: [v1 | v2c | v3 | off]*
Configure snmp set request [on/off]	Sets the SNMP access mode to on. This allows SNMP 'set' requests. Sequence: **set snmp set request [on/off]** press Enter The system responds: *SNMP Set Requests are [on/off].*
View snmp set request	Displays SNMP requests state. Displays if SNMP 'set' requests are enabled. The default state is off. Sequence: **get snmp set requests** press Enter The system responds: *SNMP Set Requests are [on | off].*

Required Action	Steps
FOR SNMP v1 or v2c ONLY	
View snmp managers	Displays a list of managers that can access the system via SNMP v1 and v2c only. Sequence: **get snmp managers** press Enter The system responds: *Mgr # IpAddress CommunityString* *1 192.168.1.133 example text1* *2 192.168.1.100 example text2* If there are no managers specified, the system responds: *No managers configured for the system.*
Configure snmp manager [mgr#] [ip address] [enable/disable] [community string]	Specifies the SNMP managers to allow access to the system, v1 and v2c only. Sequence: **set snmp manager [mgr#] [ip address] [enable/disable] [community string]** press Enter The system responds: *Mgr# IpAddress Status CommunityString* *1 192.7.1.1 disabled public* *2 0.0.0.0 disabled public* *3 0.0.0.0 disabled public* *4 0.0.0.0 disabled public* *5 0.0.0.0 disabled public* *6 any disabled public* Notes: 1. Only maximum of 5 managers are allowed. If all the managers are filled in, remove 1 manager by overwriting the particular index. 2. By setting the IP address of last index to 'any' and 'enable', anybody can have access to the system via SNMP**.**

Required Action	Steps
FOR SNMPv3 ONLY	

Configure snmpv3 manager *{1..5}*
 	
This command requires the following prompts to be answered.
 	
user *username*
 	
securityLevel
[noAuthNoPriv
authNoPriv | authPriv]
 	
[**auth** {**md5** | **sha | none**} *auth-password*]
 	
[**priv** {**DES | none**}
priv-password]
	This specifies an snmpv3 external user.
	
	There may be up to 5 external SNMP managers configured in the system. Each user should have unique name. The default security level for the system is noAuthNoPriv.
	
	The user is prompted with the current value for each option. User may choose to keep or modify this entry by selecting y\n. For each prompt, available options are shown.
	
	Examples:
	
	`->set snmpv3 manager`
	`Enter the entry number to modify [1-5]: 1`
	
	`Current user Name for Entry [1] is [ ]`
	`Do you accept this user name? [y|n]n`
	`Enter Snmp V3 UserName :user1`
	
	`New user Name for Entry [1] is set to [user1]`
	
	`Current Authentication Protocol for Entry [1] is [NoAuth]`
	`Do you accept this value? [y|n]n`
	`Enter authentication protocol [0=NoAuth | 1=MD5 | 2=SHA]: 1`
	
	`New authtentication protocol for Entry [1] is set to [MD5]`
	
	`Current authentication password for entry [1] is [-]`
	`Do you accept this value? [y|n]n`
	`Enter authentication password: authpass`
	
	`New authtentication password for Entry [1] is set to [authpass]`
	
	`Current privacy Protocol for Entry [1] is [NoPriv]`
	`Do you accept this value? [y|n]n`
	`Enter privacy protocol [0=NoPriv | 1=DES ]: 1`
	
	`New privacy protocol for Entry [1] is set to [DES]`
	
	`Current privacy Password for Entry [1] is [-]`
	`Do you accept this value? [y|n]n`

Required Action	Steps
	Enter privacy password: privpass New privacy password for Entry [1] is set to [privpass] Current status for Entry [1] is [Disabled] Do you accept this value? [y|n]n Do want to activate this entry? [0=disable| 1=enable]: 1 New activate option for Entry [1] is set to [Enabled] index userName authProt authPass privProt privPass status ========== 1 user1 MD5 authpass DES privpass enabled 2 NoAuth - NoPriv - disabled 3 NoAuth - NoPriv - disabled 4 NoAuth - NoPriv - disabled 5 NoAuth - NoPriv - disabled Note: 1.Only maximum of 5 managers are allowed. If all the managers are filled in, remove 1 manager by overwriting the particular index.
View snmpv3 managers	Displays a list of configured SNMPv3 managers. **get snmpv3 managers** press Enter The system responds: ->get snmpv3 managers index userName authProt authPass privProt privPass status ========== 1 NoAuth - NoPriv - disabled 2 NoAuth - NoPriv - disabled 3 NoAuth - NoPriv - disabled 4 NoAuth - NoPriv - disabled 5 NoAuth - NoPriv - disabled Note: 1.Only maximum of 5 managers are allowed. If all the managers are filled in, remove 1 manager by overwriting the particular index.

Required Action	Steps
View snmpv3 trap hosts	Displays a list of configured SNMPv3 trap hosts Note that only the Super user can view the ip addresses of trap hosts. Sequence: **get snmpv3 trap hosts** press Enter The system responds: *# IpAddress UserName Auth Auth Priv Priv TrapHost* *Proto Passwd Proto Passwd Enabled* *= ========== ========== ===== ==========* *1 192.168.4.254 guest None - None - y* *2 0.0.0.0 None - None - n* *3 0.0.0.0 None - None - n* *4 0.0.0.0 None - None - n* *5 0.0.0.0 None - None - n*
Configure snmpv3 trap host ip	To set the trap host ip address to capture v3 traps. This will only set up a trap host destination without authentication or privacy. **NOTE:** You must set a trap host user (see next command) before a configured trap host will function. Only Super user is allowed to set these parameters. Sequence: **set snmpv3 trap host ip <index> <ipAddr>** press Enter where <index> indicates which trap host entry you want to set in the range of 1...5 and <ipAddr> is the ip address of the host on the network. The system responds: *Save mib and reboot Horizon Compact Plus for changes to take effect.*
Configure snmpv3 trap host user	To set the host user name associated with v3 trap hosts. This will only set up a trap host destination without authentication or privacy. **NOTE:** You must set a trap host ip (see previous command) and a host user name before a configured trap host will function. Only Super user is allowed to set these parameters. Sequence: **set snmpv3 trap host user <index> <userName>** press Enter where <index> indicates which trap host ip address entry to which you want to add the host user name in the range of 1…5 The system responds: *Save mib and reboot Horizon Compact Plus for changes to take effect.*

Required Action	Steps
Configure snmpv3 trap host enable	To enable a trap host. **NOTE:** Individual traps need to be enabed before they will be received by an enabled trap host. Only Super user is allowed to set these parameters. Sequence: **set snmpv3 trap host enable <index>** press Enter Where **<index>** is the trap host index you wish to enable in the range 1 to 5 The system responds: *Save mib and reboot Horizon Compact Plus for changes to take effect.*
Configure snmpv3 trap host disable <index>	To disable a trap host. **NOTE:** Only Super user is allowed to set these parameters. Sequence: **set snmpv3 trap host disable <index>** press Enter Where **<index>** is the trap host index you wish to enable in the range 1 to 5 The system responds: *Save mib and reboot Horizon Compact Plus for changes to take effect.*
Configure snmpv3 trap host authentication	Use this command to set up trap host authentication. **NOTE:** Only Super user is allowed to set these parameters. Sequence: **set snmpv3 trap host authentication <index> [none|md5|sha] <authKey>** press Enter Where **<index>** is the trap host index in the range 1 to 5 on which you wish to configure authentication, **[none|md5|sha]** are the protocols available and **<authKey>** is a text string of up to 25 alpha numeric characters. The system responds: *Save mib and reboot Horizon Compact Plus for changes to take effect.*
Configure snmpV3 trap host privacy <index> [none|des] <privKey>	Use this command to set up privacy. **NOTE:** Authentication must be configured before privacy will function. Only Super user is allowed to set these parameters. Sequence: **set snmpV3 trap host privacy <index> [none|des] <privKey>** press Enter Where **<index>** is the trap host index in the range 1 to 5 on which you wish to configure privacy, **[none|des]** are the protocols available and **<privKey>** is a text string of up to 25 alpha numeric characters. The system responds: *Save mib and reboot Horizon Compact Plus for changes to take effect.*

Required Action	Steps
Save changes to mib	Saves the MIB to RAM. Perform this command save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully.*
reset system	Resets the system to save the settings to FLASH and restart the system with the new settings taking effect. Sequence: **reset system** press Enter The system responds: *Are you sure you want to reset? Y(yes) or N(no)* *press **Y*** *The system will proceed to reset. You will have to log on again to regain access.*

This concludes the steps to set up the SNMP for the Horizon Compact Plus system.

20.3 Enterprise Management Information Base (MIB)

A Management Information Base (MIB) contains information about a network device that is managed by SNMP. Horizon Compact Plus supports industry standards MIB I and MIB II. In addition, DragonWave provides an enterprise MIB for Horizon Compact. For a list of objects and their definitions, refer to the Horizon Compact Plus MIB definition file included with the DragonWave Toolkit CD-ROM.

You must load the Horizon Compact Plus MIB onto your own MIB browser or Network Management Station (NMS). HP OpenView is an example of network management software to be used on the NMS. The Horizon Compact Plus Enterprise MIB is provided in a standard MIB format that allows a more direct method of loading the definitions onto the NMS. On some NMS systems, it is as straightforward as placing the Horizon Compact Plus MIB into the proper NMS directory and then enabling it by adding it to the MIB list. Please consult the instructions provided with your NMS for details on loading the Enterprise MIBs.

20.4 SNMP Traps

A trap is a message that reports a problem or a significant event. Traps are defined in the Horizon Compact Plus MIB definition file. A trap destination or trap host is the IP address of a client (network management station) that receives the SNMP traps.

Procedure 20-2
Enable traps

Perform this procedure to enable traps.

Required Action	Steps
login	Log in as a NOC account
View snmp trap hosts	Displays a list of receivers of SNMP traps. Sequence: **get snmp trap hosts** press Enter The system responds: *Host# IpAddress Status CommunityString* *1 0.0.0.0 disabled public* *2 0.0.0.0 disabled public* *3 0.0.0.0 disabled public* *4 0.0.0.0 disabled public* *5 0.0.0.0 disabled public* **Note**: A maximum of 5 hosts is allowed. If all the hosts are filled in, remove 1 host by overwriting the particular index.

Required Action	Steps
Configure snmp trap host [host #] [ipAddress] [enable/disable] [communityString]	Adds an SNMP trap host to the list of receivers of SNMP traps. Specify the IP address where the system sends traps. Sequence: **set snmp trap host [host #] [ipAddress] [enable/disable] [communityString]** press Enter The system responds: *Host# IpAddress Status CommunityString* *1 0.0.0.0 disabled public* *2 0.0.0.0 disabled public* *3 3.3.3.3 enabled new text string here* *4 0.0.0.0 disabled public* *5 0.0.0.0 disabled public* **Note:** A maximum of 5 hosts are allowed. If all the hosts are filled in, remove 1 host by overwriting the particular index.

Required Action	Steps
View snmp traps	Displays the list of traps available in the system and which are enabled/disabled. Sequence: **get snmp traps** press Enter The system responds:

```
 Trap#      TrapName                        Enabled(Yes | No)

    1       Link down                              Yes
    2       Peer authentication failure            Yes
    3       HAAM configuration mismatch            Yes
    4       HAAM operating in lower modulation     Yes
    5       ATPC configuration mismatch            Yes
    6       ATPC auto disabled                     Yes
    7       SNTP server(s) unreachable             Yes
    8       Frequency file invalid                 Yes
    9       Aggregate dropped frame threshold      Yes
   10       Queue dropped frame threshold          Yes
   11       Bandwidth utilization threshold        Yes
   12       Queue depth threshold                  Yes
   13       RLS configuration mismatch             Yes
   14       RLS shutdown activated                 Yes
   15       RLS queue based shutdown               Yes
   16       Modem receiver loss of signal          Yes
   17       Modem SNR below threshold              Yes
   18       Modem equalizer stress above limit     Yes
   19       RSL below threshold                    Yes
   20       Radio synthesizer lost lock            Yes
   21       Radio calibration table unavailable    Yes
   22       Radio current out of limits            Yes
   23       Radio power amplifier                  Yes
   24       Temperature out of limits              Yes
   25       Partner configuration mismatch         Yes
   26       Active on secondary                    Yes
   27       Operating in forced switch mode        Yes
   28       Enet cross link active                 Yes
   29       Active using partner wireless link     Yes
   30       Standby wireless link is in use        Yes
   31       Standby on primary                     Yes
   32       X2 delivering half the capacity        Yes
   33       BNC cable signal not detected          Yes
   34       Ethernet speed reduced                 Yes
   35       SyncE lost lock                        Yes
   36       SyncE secondary source in use          Yes
   37       Invalid system configuration           Yes
   38       MIB change not saved                   Yes
   39       Transmitter loss of sync               Yes
   41       Cold start                             Yes
   42       User session                           Yes
   43       HAAM event                             Yes
```

Required Action	Steps
Configure snmp trap [trapIndex] [enable/disable]	Enables or disables SNMP traps. DragonWave recommends enabling trap 16. This trap indicates loss of communication with the peer Horizon Compact Plus node. Sequence: **set snmp trap [trapIndex] [enable/disable]** Example (enabling trap 16): **set snmp trap 16 enable** press Enter The system responds:

```
 Trap#     TrapName                      Enabled(Yes | No)

   1       Link down                              No
   2       Peer authentication failure            No
   3       HAAM configuration mismatch            No
   4       HAAM operating in lower modulation     No
   5       ATPC configuration mismatch            No
   6       ATPC auto disabled                     No
   7       SNTP server(s) unreachable             No
   8       Frequency file invalid                 No
   9       Aggregate dropped frame threshold      No
  10       Queue dropped frame threshold          No
  11       Bandwidth utilization threshold        No
  12       Queue depth threshold                  No
  13       RLS configuration mismatch             No
  14       RLS shutdown activated                 No
  15       RLS queue based shutdown               No
  16       Modem receiver loss of signal          Yes
  17       Modem SNR below threshold              No
  18       Modem equalizer stress above limit     No
                              ⋮
  25       Partner configuration mismatch         No
  26       Active on secondary                    No
  27       Operating in forced switch mode        No
  28       Enet cross link active                 No
  29       Active using partner wireless link     No
  30       Standby wireless link is in use        No
  31       Standby on primary                     No
  32       X2 delivering half the capacity        No
  33       BNC cable signal not detected          No
  34       Ethernet speed reduced                 No
  35       SyncE lost lock                        No
  36       SyncE secondary source in use          No
  37       Invalid system configuration           No
  38       MIB change not saved                   No
  39       Transmitter loss of sync               No
  41       Cold start                             No
  42       User session                           No
  43       HAAM event                             No
```

Required Action	Steps
Save changes to mib	Saves the MIB to RAM. Perform this command save setting changes to non-volatile memory. Sequence: **save mib** press Enter The system responds: *MIB saved successfully*
reset system	Resets the system to save the settings to FLASH and restart the system with the new settings taking effect. Sequence: **reset system** press Enter The system responds: *Are you sure you want to reset? Y(yes) or N(no)* press **Y** The system will proceed to reset. You will have to log on again to regain access.

This concludes the steps to set SNMP traps using the CLI manager.

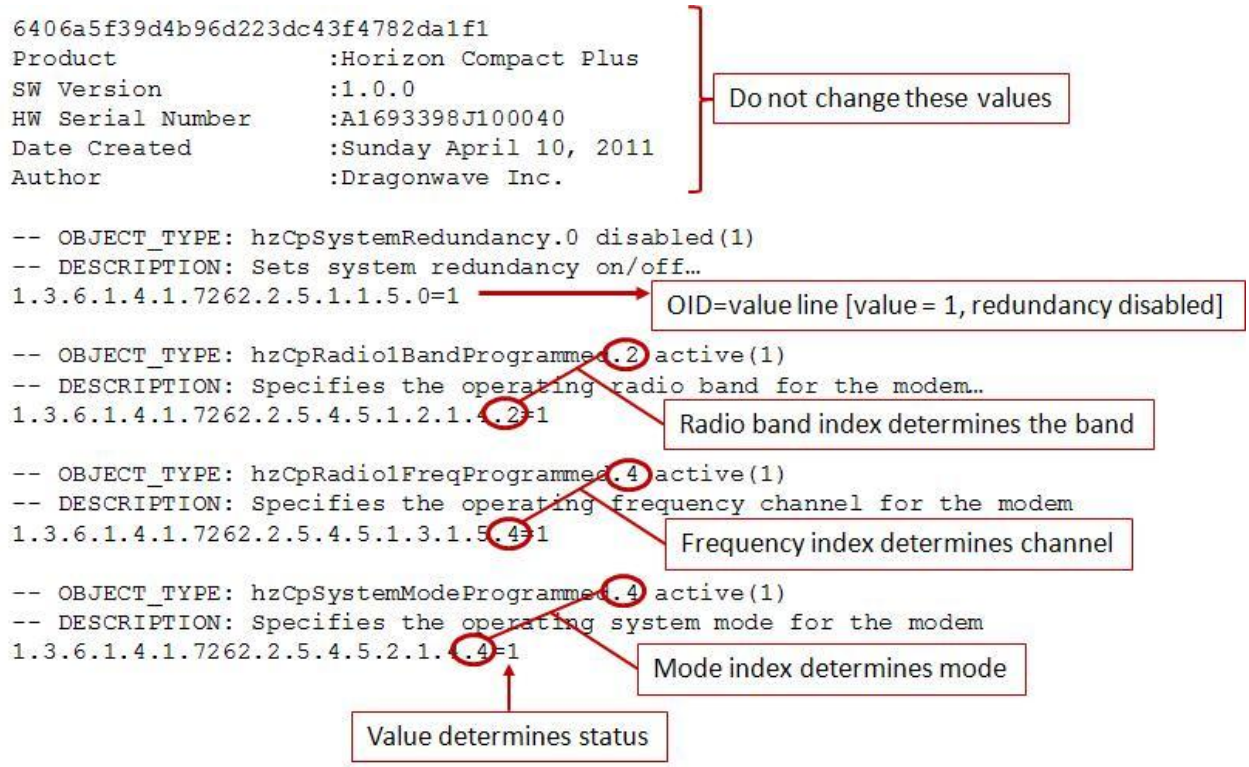
This page left blank intentionally

21.0 Editing System Configuration Files

Volume 1 of this manual describes how to upload and download system configuration files to an ftp server. Downloading a configuration file to a system will allow that system to take on an identical configuration as that of the system from which the configuration file was uploaded.

The configuration file is a text file written in SNMP OID=value format. This file can be edited in order to make changes to the configuration of a system to which the file may be downloaded. Changing the configuration involves changing the OID=value line(s) in the file.

An example of a partial configuration file is shown below:



The first line of the file contains an original hash value of the file and it should not be modified or removed. Also, the header containing product information should not be removed.

The user may modify the OID=value lines in the file to configure a system, and any lines can be commented out with "-- " in front of a line.

If a value contains space(s) the whole OID=value should be within quotes. For example, to configure COS CIR the OID=value should look like this:

```
"1.3.6.1.4.1.7262.2.5.6.6.0=12 12 12 12 12 12 12 16"
```

The index ID's for various parameters can be found in Appendix B – System Configuration OID Indices.

See Volume 1 for the procedure to upload and download configuration files. Only the Super User can upload or download configuration files.

This page is left blank intentionally

Appendix A – Detailed CLI Command List

CLI Command	Description
?	display all commands with their short description.
change password	change current user password.
clear ecfm errors [domain <domain-name(1..20)> | levelid <level-id(0-7)>][switchname <context_name>]	Clear continuity check error conditions logged on a device.
clear ecfm frame delay buffer [switchname <context_name>]	Clear the contents of the Frame Delay rolling buffer
clear ecfm loopback cache [switchname <context_name>]	Clear the contents of the Loopback Reply Cache.
clear ecfm maintenance-points remote [{domain <domain-name(1..20)> | levelid <level-id(0-7)>}][switchname <context_name>]	Clear the contents of continuity check database.
clear ecfm mip-ccm-database [switchname <context_name>]	Clear the contents of MIP CCM Database.
clear ecfm statistics [port <num<1-1>] [level<level-id(0-7)>] [vlan <vlan-id(1-4094)>]] [switchname <context_name>]	Clears ECFM statistics counters
clear ecfm traceroute-cache [switchname <context_name>]	Clear the contents of ECFM traceroute cache.
clear port eoam config [port <num(1-2)>]	Clears ethernet OAM local configuration for all ports/specific port.If the port is not specified, it clears the configuration of both ports.
clear port eoam event-log [port <num(1-2)>]	Clears EOAM event logs.If port num is not specified, it clears the event logs of both ports.
clear port eoam fault-management mib-variable response [port <num(1-2)>]	Clears MIB variable response received from the peer. If port num. is not specified, it clears response on both ports.
clear port eoam statistics [port <num(1-2)>]	Clears ethernet OAM statistics for all ports/specific port. If the port is not specified, it clears the statistics of both ports.
copy [ftp:fileName]	allows the user to download file from remote location. To download user accounts file, filename should startwith 'user' keyword and to download configuration file, filename should start with 'config' keyword.
create ssl certificate	create SSL certificate.
delete ecfmmib [newest|both]	deletes the Ethernet Continuity Fault Management(ECFM) MIB as requested by the user.
delete mib [newest|both]	deletes the MIB as requested by the user.
delete radius server [index]	delete the host and shared key config for a Radius Server.
delete user	delete the admin or noc user.
diagnose aam	enable Automated Adaptive Modulation(aam) diagnostic mode[upspeed|downspeed]

CLI Command	Description
diagnose haam [up/down]	enable Hitless Adaptive Modulation(HAAM) diagnostic mode [up|down]
downgrade system licensed speed	downgrade system licensed speed [speed decrement]
ecfm frame delay [start | stop] type {one-way | two-way }level <level-id(0-7)> [vlan <vlan-id(0-7)>] [port <port-num>] [direction {inward | outward}]{mepid <mpid(1-8191)> | mac <aa:aa:aa:aa:aa:aa>} [count<num_of_observations(1-8192)>] [interval <milliseconds(10-10000)>] [deadline <seconds(1-172800)>] [switchname <context_name>]]	Start or Stop the ECFM delay measurement calculations. Default is to start the measurement.
ecfm ping ethernet mac {<aa:bb:bb:bb:bb:bb> | multicast } {domain <domain-name(1..20)> | level <level-id(0-7)>} [vlan <vlan-id(1-4094)>] [interface <interface-number>] [direction {inward | outward}] [data-pattern <string> | test-pattern null-signal-without-crc | null-signal-with-crc | prbs-without-crc | prbs-with-crc] [size <pdu-size(64-1400)> | variable-bytes][interval <milliseconds(1-600000)>] [count <num_of_msgs(1-8192)>] [deadline <seconds(1-172800)>] [switch <string(32)>]	Send unicast or multicast Loopback messages. The first byte in the unicast address cannot be 0x01 or 0xFF.
ecfm ping ethernet mpid <id> {domain <domain-name(1..20)> | level <level-id(0-7)>} [vlan <vlan-id(1-4094)>] [interface <interface-number>] [direction {inward | outward}] [data-pattern <string> | test-pattern null-signal-without-crc | null-signal-with-crc | prbs-without-crc | prbs-with-crc] [size <pdu-size(64-1400)> | variable-bytes][interval <milliseconds(1-600000)>] [count <num_of_msgs(1-8192)>] [deadline <seconds(1-172800)>] [switch <string(32)>]	Send unicast or multicast Loopback messages.
ecfm traceroute ethernet mac <aa:aa:aa:aa:aa:aa> {domain <domain-name(1..20)> | level <level-id(0-7)>} [vlan <vlan-id(1-4094)>] [time-to-live <ttl-value(1-255)>]	Initiate Linktrace message by providing the MAC Address of the MEP or MIP.
ecfm traceroute ethernet mpid <id> {domain <domain-name(1..20)> | level <level-id(0-7)>} [vlan <vlan-id(1-4094)>] [time-to-live <ttl-value(1-255)>]	Initiate Linktrace message by providing MEPID of the destination MEP of the MEP or MIP.
erase log	erase all of log entries in the flash.
erase performance log	erase all of the performance log entries.
exit	allows the user to exit from Telnet Session.

CLI Command	Description
get aam eoam option	displays eoam msg option for aam.
get aam link monitor parameters	aam link monitor parameters
get aam status	returns Automated Adaptive Modulation(aam) status either on or off. Default is 'off'.
get alarms	returns alarms present in the system.
get alarms counter	returns timestamped alarms present in the system.
get alignment	returns the Horizon alignment status(On|Off).
get antenna diameter	returns the antenna's diameter.
get atpc status	returns the atpc status(On/Off).
get authenticated peer	returns SN with which system has commenced communications with.
get backup ipconfig	returns IP Configuration Parameters stored as backup.
get bandwidth record admin	returns the bandwidth recording admin status as either 'on' or 'off'
get bandwidth record average period	returns the number of seconds configured for computing the running average bandwidth utilization.
get bandwidth record brief	returns the brief contents of all bandwidth records saved in flash.
get bandwidth record current	returns the contents of the active bandwidth record (has not been saved to flash yet).
get bandwidth record instance[0-59]	returns the contents of the specified bandwidth record from flash. If no record is specified, then return all records. 0 is always the newest record and higher record numbers refer to older records.
get bandwidth record logging	returns the bandwidth recording status of logging to flash and syslog as either 'on' or 'off'
get bandwidth record reporting period	returns the number of seconds configured for bandwidth reporting period.
get bandwidth record thresholds	returns ten bandwidth utilizations thresholds used to for counting bandwidth utilization measurements.
get bandwidth record verbose	returns the verbose contents of all bandwidth records saved in flash.
get bandwidth utilization status	returns the current bandwidth utilization and throughput.
get bandwidth utilization threshold	returns the % utilization of bandwidth threshold.
get config commands	displays system configuration commands and their associated values set in the system.
get cos default value	displays the 802.1p priority assigned to untagged packets.
get cos ecfm flow mapping	returns the current status of the ecfm flow mapping [on|off and queue]
get cos expedite queue	get the expedite queue mode.

CLI Command	Description
get cos qinq itag	returns the protocol id of dot1q Q_in_Q inner tag.
get cos qinq otag	returns the protocol id of dot1q Q_in_Q outer tag.
get cos queue cbs	returns the committed burst size of the cos queues.
get cos queue cir	displays the CIR(Committed Information Rate) for user traffic queues
get cos queue mapping	the table in the response to this command indicates the assignment of dot1p cos value to user queue.
get cos type	returns the cos type.
get cos wfq weight	returns the cos wfq weight.
get date time	displays current Date and Time to the user.
get default gateway	gets the system default gateway.
get default ipconfig	displays default IP Configuration of the system.
get dropped frames threshold	returns the dropped frames threshold set by the user in %.
get dw access	displays the DW access.
get dynamic config change	returns the status (on/off) of the dynamic config change feature.
get ecfm configuration-errors [vlan <vlan-id(1-4094)>] [interface <interface-id>] [switchname <context_name>]	Displays the ECFM configuration-related errors (CFM leak, Conflicting VlanIds, Excessive Levels, etc).
get ecfm default-domain [switchname <context_name>]	Displays the global Default-domain parameters along with the modified parameters corresponding to a VLAN.
get ecfm domain [brief | domain-number(1-32)] [switchname <context_name>]	Display information about the Ecfm maintenance domain.
get ecfm error-log [domain <domain-name(1..20)> | levelid<level-id(0-7)>] [unaware | vlan <vlan-id(1-4094)>] [switchname <context_name>]	Displays the Error Log containing the information about the errors encountered on the MEP.
get ecfm errors [domain <domain-name(1..20)> | levelid <level-id(0-7)>] [switchname <context_name>]	Display continuity check error conditions logged on a device since it was last cleared.
get ecfm frame delay buffer [brief] [one-way | two-way] [level <level-id(0-7)>][unaware | vlan <vlan-id(1-4094)>] [interface <interface-number>][mac <peer-mac-address>]	Display the contents of the rolling buffer maintained for Frame delaycalculations measured at various times.
get ecfm global information[switchname <context_name>]	Displays ethernet CFM global information.
get ecfm loopback cache [brief] [level <level-id(0-7)>][unaware | vlan <vlan-id(1-4094)>]	Displays the Loopback transactions related information.

CLI Command	Description
get ecfm maintenance-point local [mep | mip] [interface [<interface-number>] | domain <domain_name> | level<id(0-7)>]	Displays the brief information about maintenance points configured on a device.
get ecfm maintenance-points local detail {mpid<mepid(1-8092)> | mac <aa:aa:aa:aa:aa:aa>} [domain <domain_name> | level<level-id(0-7)>] [unaware | vlan <integer(1-4094)>]	Displays the detailed information about the maintenance end points(MEP) locally configured on the device. The information includes thevarious MEPs capabilities, states, threshold values, etc.
get ecfm maintenance-points remote [domain <domain-name(1..20)> | levelid <level-id(0-7)>]	Display brief information about remote MEPs
get ecfm maintenance-points remote crosscheck [mpid <id>] [domain <domain-name(1..20)> | level <level-id(0-7)>] [unaware | vlan<integer(1-8191)>][{domain <string(20)> | level <integer(0-7)>}][{unaware | vlan<integer(1-4094)>}] [switch <string (32)>]	Display details about the maintenance points configured statically in a List of MEPIDs (cross check list) of Service (Maintenance Association) - unaware keyword is applicable for VLAN unaware maintenance points.
get ecfm maintenance-points remote detail {mpid id | mac <aa:aa:aa:aa:aa:aa> }[domain <domain-name(1..20)> | level <level-id(0-7)> [unaware | vlan<vlan-id(1-4094)>]] [switchname <context_name>]	Display details about remote MEPs - unaware keyword is applicable for VLAN unaware maintenance points.
get ecfm mip-ccm-database [vlanid <vlan-id(1-4094)>] [macaddress <aa:aa:aa:aa:aa:aa>] [port <port-id>]	Displays the ECFM MIP CCM Database
get ecfm port [{port <port-number>}] [switchname <context_name>]	Displays the ethernet CFM port-specific parameters.
get ecfm service [brief | service-number(1-32)] [switchname <context_name>]	Display information about ethernet CFM Service (Maintenance Association).
get ecfm statistics [port <port-number> [level <level-id(0-7)>][<vlan-id(1-4094)>]] [switchname <context_name>]	Displays ECFM statistics.
get ecfm traceroute-cache	Display details about traceroute cache (Traceroute cache displays LTR replies corresponding to each LTM transaction).
get enet address	gets the ethernet MAC address.
get enet config	returns configuration parameters for ethernet Port1 and Port2.
get enet speed	returns current speed configuration for ethernet Port1 and Port2.
get enet speed alarm enable port1|port2	returns the status of the enet speed alarm for either port 1 or port 2 [on|off]
get enet status	returns status of ethernet Port1 and Port2.
get eoam dwi-msg mode	displays eoam DWI specific msg mode.

CLI Command	Description
get eoam fault-management global information	Displays fault-management global information.
get eoam global information	Displays ethernet OAM global information.
get frequency bank	displays Frequency Banks available in the System.
get frequency file status	displays the status of the frequency file.
get haam	returns the configured Hitless Adaptive Modulation(HAAM) on/off status.
get haam eoam option	returns the status of the haam eoam option
get haam status	returns the local/peer Hitless Adaptive Modulation(HAAM) information.
get haam system modes	returns the modes available for use with Hitless Adaptive Modulation.
get haam wtr	Gets the duration in seconds that Hitless Adaptive Modulation (HAAM) waits before shifting to a higher rate mode.
get health	returns operational condition of resources in the system.
get http secure access [Admin|Noc|Super]	returns the HTTPS access for a specific group of users.
get hw inventory	displays HW inventory.
get install type	gets the system installation type (ODU or IDU/ODU split).
get ip address	gets the system ip address.
get ip config	returns all ip configuration parameters
get leds	displays system LEDS with On/Off values.
get licensed speed count	returns licensed speed count for upgrading and downgrading.
get licensed speed downgrade information	returns the last time's downgrade information.
get log entries	get all of log entries in the flash
get logging	displays logging is enabled or not.
get maximum frame size	returns the maximum frame size
get modem modulation	returns modem modulation type.
get modem statistics	returns modem statistics in the system.
get network loopback	gets the network loopback status.
get network management interface	returns the port used for managing the system. p1 – p4 out-of-band. dp1 – dp4 in-band.
get omni file crc	displays Omni File CRC's of executing and backup software files.
get optical transmitter state	displays the current state of the optical transmitter as 'on' or 'off'.
get pause state	displays PAUSE state (on/off).

CLI Command	Description
get peer authentication failure action	returns action taken by the system on peer authentication failure.
get peer authentication group key	returns group authentication key.
get peer authentication status	returns status of Authentication in the system.
get peer authentication type	returns the type of authentication used to authenticate the peer.
get peer authentication unique key	returns serial number (as entered in the set command) of peer system with which system communicates within UNIQUE authentication mode.
get performance log	gets the performance log
get performance log interval	gets the performance logging interval.
get performance logging	displays performance logging is enabled or not.
get port eoam event-log [port <1-2>]	Displays EOAM event logs.
get port eoam event-notifications [port <1-2>]	Displays EOAM event notifications.
get port eoam fault-management config port <1-2>	Displays EOAM link event actions and max desciptors per variable request.
get port eoam fault-management mib-variable response port <1-2>	Displays MIB variable response.
get port eoam fault-management remote-loopback [port <1-2>] [current-session | last-session] [detail]	Displays EOAM loopback statistics.
get port eoam local information [port <1-2>]	Displays ethernet OAM local information.
get port eoam loopback capability[port <1-2>]	Display EOAM Looback capabilities.
get port eoam neighbour information [port <1-2>]	Displays EOAM neighbour information.
get port eoam statistics [port <1-2>]	Displays EOAM statistics counter.
get programmed frequency	returns RX IF, RX RF, TX IF,and TX RF frequencies after setting the programmed frequency.
get qos	return value indicates whether the dot1p qos is 'on' or 'off'.
get qos policy	return the qos policy [strict_priority or wfq].
get queue utilization threshold	returns the thresholds for the Queue Depth trap
get radio band	gets the radio frequency band in use in the system.
get radio config	returns a list of radio configuration parameters
get radio loopback	gets the radio loopback status [on | off].
get radio statistics	returns radio statistics in the system.
get radio status	returns the radio alarms and synthesizer status.

CLI Command	Description
get radio transmitter state	returns the state of the radio transmitter.
get radius server deadtime	display how long we will try talking to an unresponsive Radius Server before declaring it dead.
get radius server retransmit	display maximum number of time the Radius Client will retransmit per server.
get radius server timeout	display Radius Client timeout period when talking to server.
get radius servers	display all active and configured Radius Servers.
get radius super user authentication	display authentication strict mode. OFF: Super User can login using flash password. ON: No one can login without Radius
get redundancy link monitor parameters	gets redundancy link monitor parameter (both hsb_1wire and hsb_2wire).
get redundancy link switch parameters	gets redundancy link hard error monitor parameter for link establishing.
get redundancy mode	displays the system redundancy mode
get redundancy override	returns the redundancy override status.
get redundancy partner information	returns partner's information.
get redundancy standby enet state	gets programmed state of primary_hsb_2wire or secondary_hsb_2wire port1 in standby state.
get redundancy status	returns the redundancy status.
get rls	returns rls option in the system as on/off.
get rls link control	returns RLS user control for re-enabling failed link. If on, then user has to explicitly enable the link.
get rls link enable	returns RLS global link enable status as on or off.
get rls link monitor parameters	returns RLS modem link monitor parameters.
get rls make rsl	displays RLS make RSL parameters.
get rls port groups	displays which port or ports are to fail before RLS is invoked.
get rls shutdown policy	displays RLS shutdown policy.
get rls signal fault parameters	displays RLS signal fault monitor parameters. The link is faulted for any period that the error threshold is exceeded.
get rls status	display RLS status.
get rsl threshold	returns the RSL threshold set by the user.
get sessions	returns information on current Network Management sessions.
get snmp access mode	specifies whether SNMP 'v1' and 'v2c' requests are enabled.
get snmp managers	returns a list of managers that may access the system via SNMP.

CLI Command	Description
get snmp set request	specifies whether SNMP 'v1' and 'v2c' 'Set' requests are enabled.
get snmp trap hosts	returns the list of receivers of snmp traps.
get snmp traps	returns list of traps that are available in the system.
get snmpv3 managers	returns a list of managers that may access the system via SNMP Version 3.
get snmpv3 trap hosts	returns the list of receivers of snmp traps in V3 mode.
get snr threshold	returns the SNR threshold.
get sntp	returns the SNTP status: whether it is on|off and the list of SNTP servers
get sntp offset	returns the SNTP time offset in hours: the regional time minus Greenwich Mean Time; used to calculate and set the system time
get ssh server	returns the status of the SSH server.
get ssh server fingerprint	returns the SSH server fingerprint.
get ssl certificate status	returns if the SSL certificate has been created and if it's valid for this IP address.
get subnet mask	gets the system subnet mask.
get super user	returns the Super Username and Password stored in the system.
get sw inventory	displays Omni File inventory, stored in FLASH memory; shows primary and backup software in FLASH.
get sw version	displays SW versions in the system.
get synce config	Returns the synchronous Ethernet configuration details
get synce status	Returns the status of synchronous Ethernet
get syslog forwarding host	displays the syslog forwarding host IP Address.
get syslog forwarding status	displays the syslog forwarding status. If 'on' then syslogs are being sent to the specified host
get system mode	displays the system mode
get system speed	returns the speeds of system.
get system summary	displays system summary information
get telnet access	displays whether the Telnet Access is enabled or disabled.
get traffic statistics	returns traffic statistics in the system.
get transmit power	returns the configured and actrual transmit power level for the system.
get user accounts	displays both Admin and NOC user accounts to the user.
get user session	displays the LogIn status of the user.

CLI Command	Description
get vlan tag	gets the vlan tag set in the system.
get vlan tagging	gets the state of vlan tagging.
get web server	gets the web server on or off.
kill ssh sessions	terminates all the active ssh sessions.
list [ftp:file/directory/empty]	displays list of files/directories residing in the FTP Server. If no parameters are specified, displays the user's default/current working directory contents.
lo	terminates the user's session with the system.
ping [-w timeout][-n count][-t] abc.def.ghi.jkl	A basic ping utility -t Ping the specified host until stopped. To stop - type Control-C. -n count Number of echo requests to send. -w timeout Timeout in milliseconds to wait for each reply.
remove frequency indextable	clears the freq index table from system config.
reset [resource id]	resets an individual resource,or the entire system. [resource id] is one of the following: system, modem
save config [ftp:fileName]	saves the configuration commands to user specified file in the FTP server.
save ecfmmib	saves ecfm mib to the flash.
save log [ftp:fileName]	saves the event logs to user specified file in the FTP server.
save mib	saves mib to the flash.
save performance log [ftp:fileName]	saves the performance logs to user specified file in the FTP server.
save users [ftp:fileName]	saves the user account information to user specified file and stores in the FTP server.
set aam [state <on/off>][inter mode <on/off>][max Tx-Pwr <on/off>]	set Automated Adaptive Modulation(aam) to 'on' or 'off'
set aam eoam option [state <on/off>]	set eaom msg option for amm to 'on' or 'off'
set aam link monitor parameters	sets aam link monitor parameter
set aam mode [system mode name/default]	set Automated Adaptive Modulation(aam) intermediate mode
set aam time [time in mseconds]	The time wait on modulation down shifting when system has 50% packet loss
set admin user	allows the user to set up Admin Accounts.(Max of 50 accounts are allowed)
set alarms counter [0]	clears alarms counter.
set alignment [On | Off]	sets the Horizon alignment mode On or Off.
set antenna diameter [index of diameter]	sets the programmed antenna diameter. For use with unlicenced radio bands.

CLI Command	Description
set atpc[on|off] [on|off] [0-10]	sets the atpc(on/off) coordinated power option(on/off) and coordinated power offset value
set bandwidth record logging[on | off]	Set bandwidth logging to both flash and syslog 'on' or 'off'
set bandwidth record thresholds[thresh] [thresh] [thresh] [thresh] [thresh] [thresh] [thresh] [thresh] [thresh] [thresh]	set the integer percent utilization thresholds for ten bandwidth utilization counters. When a bandwidth utilization sample equals or exceeds the threshold then each of the associated counters are incremented.
set bandwidth utilization threshold [threshold] [time limit]	sets the % utilization of bandwidth Threshold. The time that the threshold must be crossed in order for itbe considered an alarmable/trappable event is specified by the user. The default time limit is 10 secs.
set cos default value [0 - 7]	sets the 802.1p priority for untagged packets.
set cos ecfm flow mapping [off|{on QC|Q1|Q2|Q3|Q4|Q5}]	sets the ECFM flow mapping feature on or off and directs ECFM packets to the desired queue.
set cos expedite queue [on | off]	Sets the expedite queue to on or off
set cos qinq itag [protocol id]	set the protocol id of dot1q Q_in_Q inner tag.
set cos qinq otag [protocol id]	set the protocol id of dot1q Q_in_Q outer tag.
set cos queue cbs [committed burst size]	sets the committed burst size of the cos queues. Value ranges from 1% to 100% of total memory.
set cos queue cir [0 - 100, 0 - 100, 0 - 100, 0 - 100]	sets the CIRs for user traffic queues
set cos queue mapping [1/2], ...	assigns the user queue to cos value. Maximum 8 assignments are allowed in a command, one for each dot1p value.
set cos type [cos_vlan | cos_qinq_itag | cos_qinq_otag | cos_dscp_ip_v4 | cos_dscp_ip_v6 | cos_mplsexp]	set the cos type.
set cos wfq weight [weight]	set the cos wfq weight.
set date time [dd/mm/yyyy hh:mm:ss:ms]	sets the calendar date and time on the system. where dd - day (01 to 31) mm - month (01 - 12) yy - year (1970 - 2099) hh - hour (0 - 23) mm - minute (0 - 59) ss - second (0 - 59) ms - millisec (0 - 999)
set default gateway [abc.def.ghi.jkl]	sets the system default gateway.
set dropped frames threshold [threshold] [time limit]	sets the threshold limit (in %) for dropped frames. The time that the threshold must be crossed in order for itbe considered an alarmable/trappable event is specified by the user. The default time limit is 10 secs.
set dw access[on | off]	set dragonwave access in secure password environment.
set dynamic config change	enables the system to allow “on-the-fly” changes of certain parameters without having to reset the system. set radio config, set ip config, set network management interface, set van tag.

CLI Command	Description
set ecfm [on | off | start]	on / off : Enables or disables connectivity fault management (CFM) processing globally on this device. Start : Start the Ethernet CFM Module globally on the ODU.
set ecfm associate vlan-id {vlan-id | vlan-list} primary-vlan-id <vlan-id(1-4094)>	Associate a list of Vlan-Ids to a Primary Vlan.
set ecfm cc enable level [disable] {levelid | level-list} [vlan {vlanid | vlan-list}]	Enables or disables the transmission of continuity check messages (CCMs).The level ID and Vlan ID identifies the Maintenance End Points (MEPs)to which the configuration applies.-Vlan if not specified, enables the transmission of CCMs at specifiedlevels for Vlan unaware MEPs only.
set ecfm cc level {<level-id(0-7)> | level-list} {<default [interval] [role]> | [vlan {<vlan-id(1-4094)> | vlan-list}] [interval {ten-sec | one-min | ten-min}]}	Sets parameter (CCM Interval) for continuity check messages (CCMs).The level ID and Vlan ID identifies the Service (Maintenance Association) to which the configuration applies. - Vlan if not specified, sets (CCM) interval at specified levels for Vlan unaware services (Maintenance Association) only. - default resets to default values. - default role resets only the role to default. - default resets only the interval to the default.
set ecfm ccm-unicast-mac <aa:aa:aa:aa:aa:aa>	Sets the destination mac-address for ECFM unicast Continuity Check Messages. a unicast mac cannot start with 00: or FF: .
set ecfm default-domain global levelid <(0-7)>	Defines or deletes a connectivity fault management (CFM) Maintenance Domain (MD) at a particular maintenance level and puts the device in Ethernet CFM configuration mode, where parameters specific to the maintenance domain can be set.
set ecfm default-domain vlan <integer(1-4094)> ([level<integer(0-7)>][mip-creation-criteria {none | explicit | defer | default}][sender-id-permission {none |chassis | manage | chassis-mgt-address | defer }])	Sets the parameters of default Maintenace Domain (MD) Level, to control MHF creation at the VLAN Ids which are not attached to any Service (Maintenance Association) and SenderID TLV transmission by those MHFs.
set ecfm disassociate vlan-id {vlan-id | vlan-list} primary-vlan-id <vlan-id(1-4094)>	Dis-Associate a list of Vlan-Ids to a Primary Vlan.
set ecfm domain <domain-name(1..20)> level <level-id(0-7)> [delete]	Sets the global default Maintenance Domain (MD)parameters to control MIP creation and SenderID TLV transmission by MHFs.
set ecfm error-log [on | off] [size <entries(1-4096)>]	Enables or disables the logging of Continuity Check errors that occurred on the device in the Error Log table and also sets the maximum size of the table.
set ecfm mep archive-hold-time { <minutes(100-65535) | default }	Sets the amount of in minutes time such that information from a MEP is kept in the CC database before they are purged. Defaults sets to 100 minutes.

CLI Command	Description
set ecfm mep crosscheck {on | off} levelid <level-id | levellist> [vlan <vlan-id | vlanlist>] [switchname <context_name>]	ON/OFF - Enables/Disables the cross-checking functionality between the MEPs configured in the cross-check list. defaults to ON. - Vlan if not specified, enables or disables the cross-checking functionality between the vlan unaware MEPs
set ecfm mep crosscheck mpid <integer(1-8191)> [delete|define] [vlan <integer(1-4094)>]	Statically defines maintenace end point(MEP) . (MEP is defined in a list of MEPIDs of a service associated with a provided VLAN) delete - Disables Linktrace replies (LTR) caching. define - Enables Linktrace replies caching. If neither 'delete' nor 'define' is specified, defaults to 'define'.
set ecfm mep crosscheck start-delay {default}|{start-delay<3-100>}	To configure the number of CCMs to be missed, for which a device waits for the remote maintenance end points(MEPs) to come up. default: the number is reset to the default value of 3.
set ecfm mep level [<0-7> [delete] [inward] mpid <id(1-8191)> [vlan<vlan-id(1-4094)>] [active]	Configures or deletes a Maintenance end point (MEP) (Sets an port as a domain boundary (edge)by defining it as a MEP), and sets direction for the MEP.) - a VLAN unaware MEP can be configured by not specifying the vlan parameter. - Active keyword defines the operational status of MEP, by default a MEP is operationally active. - MEP direction, if not specified would be outward(down).
set ecfm mep-capability level {<level-id(0-7)> | level-list} [on|off] [vlan {<vlan-id(1-4094)> | vlan-list}]([ping] [muliticast-ping] [one-way-frame-delay] [multicast-test] [turnaround-delay][ais] [rdi])	Enable (on) or disable (off) the capabilities of all the MEPs in a MA at the level and vlan. Defaults to enable if on/off not specified.
set ecfm mip ccm-database caching {enable | disable}	Enable or disable Ethernet CFM MIP-CCM database caching
set ecfm mip ccm-database hold-time [<hours>(24-48)]	Sets the hold time for the ecfm ccm-database, in hours. If not specified, the default is 24 hours
set ecfm mip ccm-database size [<entries(1000-10000)>]	Sets the number of entries in the ecfm ccm-database, in hours. If not specified, the default is 1000 entries
set ecfm mip dynamic evaluation {enable|disable}	Enables or Disables the implicit evaluation and creation of a MIP.
set ecfm mip level [delete] <level-id(0-7)> vlan <vlan-id(1-4094)> [active]	Configures a Maintenance intermediate point (MIP) at the specified level and vlan on an interface. active - makes MIP operationally active, by default MIP is configured as operationally active. delete - Deletes the specified Maintenance Intermediate Point (MIP). active keyword sets MIP to operationally inactive.
set ecfm mip-creation-criteria {none | default | explicit}	Sets MIP creation criteria for the MIPs to be associated with the Maintenance Domain.
set ecfm oui {<aa:aa:aa> | default}	Configure the Organization Unit Identifier (OUI). Default sets the OUI to the Switch Base Mac address).
set ecfm port port<1-1> {on|off}	Sets the port number that subsequent ECFM commands will apply to.

CLI Command	Description
set ecfm service <{[config] <service_name> [{icc <icc_code> umc <umc_code>] [vlan <vlan-id(1-4094)>] [mip-creation-criteria {none | default | explicit | defer}] [sender-id-permission {none | chassis | manage | chassis-mgt-address | defer}]}>| <{delete <service_name>	Configures the provided Service (Maintenance Association) at the specified vlan. User can configure ICC and UMC when Y.1731 is enabled.
set ecfm traceroute cache [on|off | { holdtime { default | <integer(1-65535)} }	on - Enables Linktrace replies (LTR) caching, by default it is disabled. off - Disables Linktrace replies (LTR) caching. Traceroute cache (LTR Table) should be empty before it can be disabled. holdtime - Sets Linktrace replies (LTR Table) maximum age. holdtime default - resets the age to 100 minutes. - Traceroute caching should be enabled. Traceroute caching should be enabled and cache should be empty.
set ecfm y1731 [on | off]	Enables(on) or disables(off) Y.1731 processing globally on a device. For Y.1731 to be enabled, ECFM should be enabled.
set enet config	Configures the characteristics of the specified Ethernet port. This is an interactive command
set enet speed port[port1 | port2] speed[10|100|1000|auto] AutoNeg[auto]	Sets the ethernet speed for the specified port. Last argument AutoNeg is optional
set enet speed alarm enable port1|port2 on|off	Enables or disables the enet speed alarm for either port 1 or port 2.
set eoam [on | off]	Enable or disable EOAM on the system.
set eoam dwi-msg mode [eoam | bypass-eoam]	Set the DWI specific msg type for eoam .
set eoam fault-management [on | off | start]	Enable/Disable fault management on the system.
set eoam link-monitor event-resend [count(1-10)]	Specify resend count of OAM PDUs to send for event notification. Default count for OAM PDUs is 10.
set eoam oui [<aa:aa:aa> | default]	Configure the Organization Unit Identifier (OUI). Default sets the OUI to the Switch Base Mac address.
set haam[on/off]	Set Hitless Adaptive Modulation(HAAM) on or off.
set haam eoam option	enables the system to send eoam messages when haam changes modulation schemes.
set haam manual mode[on|off]	Set Hitless Automatic Adaptive Modulation(haam) manual mode on or off.
set haam wtr[duration]	Set the duration in seconds that Hitless Adaptive Modulation (HAAM) waits before shifting to a higher rate mode.
set http secure access [Admin|Noc|Super] [on/off]	Set the HTTP Secure access to a group of users on or off.
set ip address [abc.def.ghi.jkl]	sets the system ip address.

CLI Command	Description
set ip config	Leads you through the steps to configure the ip parameters
set lo nulling [on/off]	sets LO nulling params [on|off ,delay, step size, loop size].
set logging [on/off]	sets logging on [enabled] or off [disabled].
set maximum frame size [1600-9600]	sets the size of the maximum frame, range from 1600 to 9600
set network loopback [nearend | farend | off] mac-address <queue N> <timeout>	sets the network loop back to near-end, far-end or off. Ethernet packets destined for the specified MAC address are looped back. The destination MAC (format aa:aa:aa:aa:aa:aa) is required when enabling the loopback. A user queue may be specified for use when QOS is enabled.
set network management interface [p1, p2, p3, p4, dp1, dp2, dp3, dp4]	sets the port used for managing the system. p1 – p4 out-of-band. dp1 – dp4 in-band.
set noc user	allows the user to set up NOC account. Username and Password cannot be empty.(Max 5 NOC accounts are allowed).
set optical transmitter state [on/off]	sets the state of the optical transmitter as 'on' or 'off'.
set pause state [on/off]	sets PAUSE (frames) on or off
set peer authentication failure action [action]	configures the action to take on peer authentication failure. [action] is either block_traffic or pass_traffic.
set peer authentication group key [key]	writes a group authentication key. [key] is a 32 character alpha numeric.
set peer authentication type [authentication type]	sets the authentication type of the air interface. [authentication type] is one of the following: none, unique, group
set peer authentication unique key [key]	stores serial number of peer system that the system will be communicating with.
set performance log interval [hr:min:sec]	sets the performance log interval.
set performance logging	sets the performance logging on[enabled] or off [disabled].
set port eoam [port <1-2>] [on | off]	Enable EOAM on port.
set port eoam fault indication [port <1-2>] [critical-event | dying-gasp] [on | off]	Enabling/disabling critical event or dying gasp fault indication.
set port eoam fault-management action [port <1-2>] [critical-event | dying-gasp | link-fault] [none | warning]	Specifying the action for the critical events received from local.
set port eoam fault-management link-monitor action [port <1-2>] [frame | frame-period | frame-sec-summary] [none | warning]	Specifying the action for the link monitoring threshold crossing events received from local.
set port eoam fault-management mib-request [port <1-2>] <branchleaf:branchleaf:...>	Send MIB variable request to peer.

CLI Command	Description
set port eoam fault-management mib-variable count [port <1-2>] <count(1-100)>	Sets the maximum MIB variables that can be sent in one OAM variable request pdu.
set port eoam fault-management remote-loopback [port <1-2>] [test] [count <no of packets(1-1000)>] [packet <size(64-1500)>] [pattern <hex_string(8)>] [wait-time <integer(1-10)>]	Specify number of packets and packet size for EOAM loopback test. This command also triggers the loop back test.
set port eoam link-monitor [port <1-2>] [frame | frame-period | frame-sec-summary] [on | off]	Enabling or disabling link events for EOAM monitoring.
set port eoam link-monitor default [port <1-2>] [frame | frame-period | frame-sec-summary] [threshold | window]	Sets the link monitoring parameters threshold and window to the default value.
set port eoam link-monitor frame-sec-summary threshold [port <1-2>] [<count(0-900)>]	Threshold error count for frame seconds summary should be lesser than window size.
set port eoam link-monitor frame-sec-summary window [port <1-2>] [<size(100 - 9000)>]	Specifying the window size for frame second summary.Window size should be greater than threshold count.
set port eoam link-monitor threshold [port <1-2>] [frame |frame-period] [<count(1234..)>]	Specifying the threshold error count for link monitoring events.Threshold count should be lesser than window size for frame-period.
set port eoam link-monitor window [port <1-2>] [frame <size(10 - 600)> | frame-period <size(1100000 - 89000000)>]	Specifying the window size for link events for ethernet OAM link monitoring. Frame-period window size should be greater than threshold count.
set port eoam mode [port <1-2>] [active | passive]	Specify eoam mode as active or passive.
set port eoam remote-loopback [port <1-2>] [on | off | deny | permit]	Allows the user to enable or disable EOAM remote loopback. and to deny or permit EOAM remote loopback feature request from its neighbour.
set programmed frequency [IndexID]	sets the frequency of the TX IF and RF stage [Index ID] is the index of frequency list specified in 'get available frequency' command. Before using this command, first set the available Frequency.
set qos [on/off]	enables or disables the dot1p qos. Setting 'on' enables the dot1p qos.
set qos policy [strict priority / wfq]	sets the qos policy [strict prioirty or wfq].
set queue utilization threshold [qid] [depth] [time]	sets the threshold for the Queue Depth trap
set radio band [radioBandName]	set the radio frequency band to be used in the system. Radio bands supported by the system can be obtained using'get radio band' command.
set radio config	Leads you through the steps to configure the radio

CLI Command	Description
set radio loopback [on | off] <timeout> <network>	sets the radio loop back[on|off]. If the user doesn't supply the optional parameter [network], then the modem data path will be disabled.
set radio transmitter state [on | off] [mute time (seconds)]	allows user to mute/unmute the radio transmitter. [transmitter state] is enabled or disabled.
set radius server host [index] [server addr]	sets the host address for server specified by [index].
set radius server key [index] [key]	sets the shared key for server specified by [index].
set radius super user authentication [On|Off]	sets the Radius Authentication Strictness mode. OFF: Super User can login using flash password. ON: No one can login without Radius.
set redundancy link monitor parameters	sets redundancy link monitor parameter (both hsb_1wire and hsb_2wire).
set redundancy link switch parameters	sets redundancy hard error monitor parameter for link establishing.
set redundancy mode	allows the user to set system redundancy [primary_hsb_1wire | secondary_hsb_1wire | primary_hsb_2wire | secondary_hsb_2wire | primary_x2 | secondary_x2 | normal].
set redundancy override [primary | secondary | manual | auto]	
set redundancy standby enet state	allows the user to set required action on port1 of primary_hsb_2wire or secondary_hsb_2wire node when it enters standby state. Allowed actions are 'on', 'off' or 'pulse'.
set redundancy state switch	allows the user to force a change in the redundancy state when the override mode is 'auto' or 'manual'. The user input is not stored in the system and set to off after the state change.
set rls [on/off] | [basic|advanced]	sets the RLS mode on|off and optionally basic|advanced.
set rls link control [on/off]	sets the RLS user link enable option. When this is set to 'On' the user has to explicitly enable the link after it recovers from a fault
set rls link enable [on/off]	sets the RLS global link enable status, if on and no link error exists the link will be enabled.
set rls link monitor parameters [mk erred blks] [brk erred blks] [mk samples] [brk samples] [mk sample time] [brk sample time] [brk sample rst time]	sets the RLS link monitor low-level parameters
set rls make rsl [make rsl threshold] [rsl mk sample time sec]	sets the RLS make RSL threshold and sample period, where: [make rsl threshold] : the minimum rsl threshold to establish the link [make rsl sample period]: the time the link rsl must be above the threshold to establish the link.
set rls port group	enables the user to configure which port or ports are to be monitored and shut down when an RLS event occurs.

CLI Command	Description
set rls shutdown policy [port-down/eoam-msg]	sets the RLS shutdown notification policy to either EOAM messages or port shutdown.
set rls signal fault parameters [fault period msec] [fault threshold]	sets the RLS signal fault monitor parameters, where [fault sample period msec] : sample period to apply Fault Threshold ratio [fault threshold percentage]: ratio of 'fault sample period' faulted before link is shut down.
set rsl threshold [threshold] [time limit]	sets the RSL threshold for the system. The time that the threshold must be crossed in order for itbe considered an alarmable/trappable event is specified by the user. The default time limit is 10 secs.
set snmp access mode [v1|v2c|off]	specifies whether SNMP v1 and v2c requests are enabled.
set snmp manager [Mgr Index] [ipAddress] [enable|disable] [communityString]	adds a SNMP manager to the list of allowed SNMP managers of the system.
set snmp set request [on|off]	allows SNMP 'set' requests.
set snmp trap [trap#] [enable|disable]	enables or disables particular SNMP trap in the system.
set snmp trap host [host#] [ipAddress] [enable|disable] [communityString]	adds an SNMP trap host to the list of receivers of snmp traps.
set snmpv3 manager	adds a SNMP v3 manager to the list of allowed SNMP v3 managers of the system.
set snmpv3 trap host authentication [index] [none|md5|sha] [passwd]	set the authentication protocol and password for an snmpV3 trap host
set snmpv3 trap host disable [index]	disable an snmpV3 trap host.
set snmpv3 trap host enable [index]	enable an snmpV3 trap host.
set snmpv3 trap host ip [index] [ipAddress]	set the IP address of an snmpV3 trap host.
set snmpv3 trap host privacy [index] [none|des]	set the privacy protocol and password for an snmpV3 trap host
set snmpv3 trap host user [index] [userName]	set the user name of an snmpV3 trap host.
set snr threshold [SnrThreshold]	configures the SNR threshold. SNR Threshold is an integer.
set sntp [on|off]	turns SNTP on or off
set sntp default	sets SNTP to default settings: SNTP is on, factory set default SNTP servers are used, 10 minute polling. SNTP time offset is not altered.
set sntp offset	sets the SNTP time offset in hours: the regional time minus Greenwich Mean Time; used to calculate and set the system time
set sntp server	writes one SNTP server, based on the index selected
set ssh server	turns the SSH server on or off.
set subnet mask [abc.def.ghi.jkl]	sets the system subnet mask.

CLI Command	Description
set super user	allows the user to change the Super Username and Password. Username and Password cannot be empty.
set synce forced holdover	This is a user troubleshooting command which forces the system into holdover mode for a configurable timeout value (**time**) in seconds. The default timout is 30 seconds. Values can be 0 to 300 seconds. 0 keeps the holdover on indefinitely.
set synce member port [p3-p8|wp1|wp2|freerun]	This command allows you to add all the ports that are required to handle SynchE into the member port group. Note that in order to configure the ports that are to be the primary and secondary clock sources, the ports must first be made part of the member port group.
set synce mode [off|manual|auto]	Use this command to enable SyncE. Select manual when you want the system to go into holdover when the primary clock source fails. If the primary source recovers, the system will automatically switch back to the primary source. Select auto if you want the system to switch to the secondary clock source if the primary clock source fails. In auto the system will not switch back to the primary if the primary clock recovers, unless set synce revertive is enabled.
set synce primary source [p3-p8|wp1|wp2|freerun]	This command allows you to select which port is to be the primary clock source. Note that the port must be configured as a GigE port (1000 Mbps). Note, also, that ports p1 and p2, being SFP ports cannot be used as a clock source.
set synce revertive [on|off] [time]	This command allows you to enable or disable the revertive mode. On a primary clock source failure and provided that the SyncE mode is configured for auto, when revertive mode is enabled (on), it allows the system to automatically revert back from the secondary to the primary clock source, once the primary clock source has recovered and remains stable for a selected time in seconds. The default time is 10 seconds.
set synce secondary source [p3-p8|wp1|wp2|freerun]	This command allows you to select the port that will provide the secondary clock source. It will take over from the primary clock source if the primary clock source fails. Note that unless the revertive feature is enabled (set synce revertive on), if, after a switch to the secondary clock source, the primary clock source recovers, the system will not automatically switch back from secondary to the primary clock source.
set synce wander filter [option1|option2]	This command allows the user to select either Ethernet Equipment Clock filter Option 1, or Option 2. Option 1 would be used in the E1 TDM hierarchy and Option 2 in the T1 TDM hierarchy.
set syslog forwarding [on|off]	set syslog forwarding on or off. Syslog will start forwarding messages to specified host when turned 'on'
set syslog forwarding host [ipAddress]	set the syslog forwarding host IP Address.
set system current speed [speed]	sets the current speed in Mbps.
set system mode [system mode name]	sets the system mode.
set telnet [on|off]	enables or disables the Telnet Access to the user. (Access: Only through Serial Port)
set traffic statistics [0]	clears all traffic statistics, including extended statistics to 0. Only parameter accepted is '0'.

CLI Command	Description
set transmit power [powerLevel]	sets the transmit power level for the system.
set vlan tag [vlan ID(0 - 4095)] [vlan priority(0 - 7)]	sets the vlan tag in the system.
set vlan tagging [on|off]	sets the state of vlan tagging.
set web server [on|off]	set the embedded web server on or off. This applies to both HTTP and SSL.
upgrade system licensed speed [speed increment] [key]	allows the user to upgrade the licensed speed.

This page is left blank intentionally

Appendix B – System Configuration OID Indices

Frequency File Version: 1.00.00

Diplexer Type: 74-000291-01

Radio Band: fcc18_1_10_R5 (Index 1)

Frequency Index	Low Program Channel
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10
10	11
11	12
12	13
13	14
14	15
15	16
16	17
17	18
18	19
19	20
20	21
21	22
22	23
23	24
24	25
25	26
26	27
27	28
28	29
29	30
30	31
31	32
32	33
33	34
34	35
35	36
36	37
37	38
38	39
39	40

```
Frequency High Program
Index          Channel
0                      1'
1                      2'
2                      3
3                      4'
4                      5'
5                      6'
6                      7'
7                      8'
8                      9'
9                      10'
10                     11'
11                     12'
12                     13'
13                     14'
14                     15'
15                     16'
16                     17'
17                     18'
18                     19'
19                     20'
20                     21'
21                     22'
22                     23'
23                     24'
24                     25'
25                     26'
26                     27'
27                     28'
28                     29'
29                     30'
30                     31'
31                     32'
32                     33'
33                     34'
34                     35'
35                     36'
36                     37'
37                     38'
38                     39'
39                     40'

Normal Mode
Index          System Mode
0                      cw_test
1                      hy10_12_qpsk
2                      hy10_28_16qam
3                      hy10_36_32qam
4                      hy10_44_64qam
5                      hy10_52_128qam
6                      hy10_60_256qam
7                      hy10_64_256qam

HAAM Mode
Index                  System Mode
0                      hy10_12_qpsk
1                      hy10_28_16qam
2                      hy10_36_32qam
3                      hy10_44_64qam
4                      hy10_52_128qam
5                      hy10_64_256qam
```

Radio Band: fcc18_1_20_R5 (Index 2)

Frequency Low Program

Index	Channel
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10
10	11
11	12
12	13
13	14
14	15
15	16
16	17
17	18
18	19
19	20

Frequency High Program

Index	Channel
0	1'
1	2'
2	3
3	4'
4	5'
5	6'
6	7'
7	8'
8	9'
9	10'
10	11'
11	12'
12	13'
13	14'
14	15'
15	16'
16	17'
17	18'
18	19'
19	20'

Normal Mode

Index	System Mode
0	cw_test
1	hy20_26_qpsk
2	hy20_60_16qam
3	hy20_77_32qam
4	hy20_94_64qam
5	hy20_112_128qam
6	hy20_129_256qam
7	hy20_137_256qam

HAAM Mode

Index	System Mode
0	hy20_26_qpsk
1	hy20_60_16qam
2	hy20_77_32qam
3	hy20_94_64qam
4	hy20_112_128qam
5	hy20_137_256qam

```
Radio Band:    fcc18_1_30_R5 (Index 3)

        Frequency Low Program
        Index          Channel
        0                      1
        1                      2
        2                      3
        3                      4
        4                      5
        5                      6
        6                      7
        7                      8
        8                      9
        9                      10
        10                     11
        11                     12
        12                     13

        Frequency High Program
        Index          Channel
        0                      1'
        1                      2'
        2                      3
        3                      4'
        4                      5'
        5                      6'
        6                      7'
        7                      8'
        8                      9'
        9                      10'
        10                     11'
        11                     12'
        12                     13'

        Normal Mode
        Index          System Mode
        0                      cw_test
        1                      hy30_39_qpsk
        2                      hy30_92_16qam
        3                      hy30_118_32qam
        4                      hy30_144_64qam
        5                      hy30_170_128qam
        6                      hy30_196_256qam
        7                      hy30_209_256qam

        HAAM Mode
        Index          System Mode
        0                      hy30_39_qpsk
        1                      hy30_92_16qam
        2                      hy30_118_32qam
        3                      hy30_144_64qam
        4                      hy30_170_128qam
        5                      hy30_209_256qam

Radio Band:    fcc18_1_40_R5 (Index 4)

        Frequency Low Program
        Index          Channel
        0                      1
        1                      2
        2                      3
        3                      4
        4                      5
        5                      6
        6                      7
        7                      8
        8                      9
        9                      10
        10                     11
```

```
        Frequency High Program
        Index           Channel
        0                       1'
        1                       2'
        2                       3
        3                       4'
        4                       5'
        5                       6'
        6                       7'
        7                       8'
        8                       9'
        9                       10'
        10                      11'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy40_52_qpsk
        2                       hy40_122_16qam
        3                       hy40_157_32qam
        4                       hy40_192_64qam
        5                       hy40_227_128qam
        6                       hy40_262_256qam
        7                       hy40_279_256qam

        HAAM Mode
        Index           System Mode
        0                       hy40_52_qpsk
        1                       hy40_122_16qam
        2                       hy40_157_32qam
        3                       hy40_192_64qam
        4                       hy40_227_128qam
        5                       hy40_279_256qam

Radio Band:    fcc18_1_50_R5 (Index 5)

        Frequency Low Program
        Index           Channel
        0                       1
        1                       2
        2                       3
        3                       4
        4                       5
        5                       6
        6                       7
        7                       8

        Frequency High Program
        Index           Channel
        0                       1'
        1                       2'
        2                       3'
        3                       4'
        4                       5'
        5                       6'
        6                       7'
        7                       8'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy50_66_qpsk
        2                       hy50_154_16qam
        3                       hy50_198_32qam
        4                       hy50_241_64qam
        5                       hy50_285_128qam
        6                       hy50_329_256qam
        7                       hy50_351_256qam
```

```
        HAAM Mode
        Index           System Mode
        0                       hy50_66_qpsk
        1                       hy50_154_16qam
        2                       hy50_198_32qam
        3                       hy50_241_64qam
        4                       hy50_285_128qam
        5                       hy50_351_256qam

Radio Band:    test18_1_7_R5 (Index 6)

        Frequency Low Program
        Index           Channel
        0                       1
        1                       30
        2                       31
        3                       32
        4                       62

        Frequency High Program
        Index           Channel
        0                       1'
        1                       30'
        2                       31'
        3                       32'
        4                       62'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy7_9_qpsk
        2                       hy7_22_16qam
        3                       hy7_28_32qam
        4                       hy7_34_64qam
        5                       hy7_40_128qam
        6                       hy7_47_256qam
        7                       hy7_50_256qam

        HAAM Mode
        Index           System Mode
        0                       hy7_9_qpsk
        1                       hy7_22_16qam
        2                       hy7_28_32qam
        3                       hy7_34_64qam
        4                       hy7_40_128qam

Radio Band:    braz18_1_14_R5 (Index 7)

        Frequency Low Program
        Index           Channel
        0                       1
        1                       2
        2                       3
        3                       4
        4                       5
        5                       6
        6                       7
        7                       8
        8                       9
        9                       10
        10                      11
        11                      12
        12                      13
        13                      14
        14                      15
        15                      16
        16                      17
        17                      18
        18                      19
        19                      20
        20                      21
```

```
21                      22
22                      23
23                      24
24                      25
25                      26
26                      27
27                      28
28                      29
29                      30
30                      31

Frequency High Program
Index          Channel
0                       1'
1                       2'
2                       3
3                       4'
4                       5'
5                       6'
6                       7'
7                       8'
8                       9'
9                       10'
10                      11'
11                      12'
12                      13'
13                      14'
14                      15'
15                      16'
16                      17'
17                      18'
18                      19'
19                      20'
20                      21'
21                      22'
22                      23'
23                      24'
24                      25'
25                      26'
26                      27'
27                      28'
28                      29'
29                      30'
30                      31'

Normal Mode
Index          System Mode
0                       cw_test
1                       hy14_19_qpsk
2                       hy14_43_16qam
3                       hy14_56_32qam
4                       hy14_68_64qam
5                       hy14_80_128qam
6                       hy14_93_256qam
7                       hy14_99_256qam

HAAM Mode
Index          System Mode
0                       hy14_19_qpsk
1                       hy14_43_16qam
2                       hy14_56_32qam
3                       hy14_68_64qam
4                       hy14_80_128qam
5                       hy14_99_256qam
```

Radio Band: braz18_1_28_R5 (Index 8)

Frequency Low Program

Index	Channel
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10
10	11
11	12
12	13
13	14
14	15

Frequency High Program

Index	Channel
0	1'
1	2'
2	3'
3	4'
4	5'
5	6'
6	7'
7	8'
8	9'
9	10'
10	11'
11	12'
12	13'
13	14'
14	15'

Normal Mode

Index	System Mode
0	cw_test
1	hy28_38_qpsk
2	hy28_88_16qam
3	hy28_113_32qam
4	hy28_138_64qam
5	hy28_163_128qam
6	hy28_188_256qam
7	hy28_201_256qam

HAAM Mode

Index	System Mode
0	hy28_38_qpsk
1	hy28_88_16qam
2	hy28_113_32qam
3	hy28_138_64qam
4	hy28_163_128qam
5	hy28_201_256qam

Radio Band: braz18_1_56_R5 (Index 9)

Frequency Low Program

Index	Channel
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

```
        Frequency High Program
        Index           Channel
        0                       1'
        1                       2'
        2                       3'
        3                       4'
        4                       5'
        5                       6'
        6                       7'
        7                       8'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy56_71_qpsk
        2                       hy56_166_16qam
        3                       hy56_214_32qam
        4                       hy56_261_64qam
        5                       hy56_308_128qam
        6                       hy56_356_256qam
        7                       hy56_380_256qam

        HAAM Mode
        Index           System Mode
        0                       hy56_71_qpsk
        1                       hy56_166_16qam
        2                       hy56_214_32qam
        3                       hy56_261_64qam
        4                       hy56_308_128qam
        5                       hy56_380_256qam

Diplexer Type: 74-000291-02

Radio Band:    etsi18_2_28 (Index 1)

        Frequency Low Program
        Index           Channel
        0                       1
        1                       2
        2                       3
        3                       4
        4                       5
        5                       6
        6                       7
        7                       8
        8                       9

        Frequency High Program
        Index           Channel
        0                       1'
        1                       2'
        2                       3'
        3                       4'
        4                       5'
        5                       6'
        6                       7'
        7                       8'
        8                       9'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy28_38_qpsk
        2                       hy28_88_16qam
        3                       hy28_113_32qam
        4                       hy28_138_64qam
        5                       hy28_163_128qam
        6                       hy28_188_256qam
        7                       hy28_201_256qam
```

```
        HAAM Mode
        Index           System Mode
        0                       hy28_38_qpsk
        1                       hy28_88_16qam
        2                       hy28_113_32qam
        3                       hy28_138_64qam
        4                       hy28_163_128qam
        5                       hy28_201_256qam

Radio Band:    etsi18_2_56 (Index 2)

        Frequency Low Program
        Index           Channel
        0                       1
        1                       2
        2                       3
        3                       4

        Frequency High Program
        Index           Channel
        0                       1'
        1                       2'
        2                       3'
        3                       4'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy56_71_qpsk
        2                       hy56_166_16qam
        3                       hy56_214_32qam
        4                       hy56_261_64qam
        5                       hy56_308_128qam
        6                       hy56_356_256qam
        7                       hy56_380_256qam

        HAAM Mode
        Index           System Mode
        0                       hy56_71_qpsk
        1                       hy56_166_16qam
        2                       hy56_214_32qam
        3                       hy56_261_64qam
        4                       hy56_308_128qam
        5                       hy56_380_256qam

Diplexer Type: 74-000305-01

Radio Band:    esp13_1_56_R5 (Index 1)

        Frequency Low Program
        Index           Channel
        0                       1
        1                       2
        2                       3
        3                       4
        4                       5

        Frequency High Program
        Index           Channel
        0                       1'
        1                       2'
        2                       3'
        3                       4'
        4                       5'
```

```
        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy56_71_qpsk
        2                       hy56_166_16qam
        3                       hy56_214_32qam
        4                       hy56_261_64qam
        5                       hy56_308_128qam
        6                       hy56_356_256qam
        7                       hy56_380_256qam

        HAAM Mode
        Index           System Mode
        0                       hy56_71_qpsk
        1                       hy56_166_16qam
        2                       hy56_214_32qam
        3                       hy56_261_64qam
        4                       hy56_308_128qam
        5                       hy56_380_256qam

Radio Band:    esp13_1_28_R5 (Index 2)

        Frequency Low Program
        Index           Channel
        0                       1
        1                       2
        2                       3

        Frequency High Program
        Index           Channel
        0                       1'
        1                       2'
        2                       3'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy28_38_qpsk
        2                       hy28_88_16qam
        3                       hy28_113_32qam
        4                       hy28_138_64qam
        5                       hy28_163_128qam
        6                       hy28_188_256qam
        7                       hy28_201_256qam

        HAAM Mode
        Index           System Mode
        0                       hy28_38_qpsk
        1                       hy28_88_16qam
        2                       hy28_113_32qam
        3                       hy28_138_64qam
        4                       hy28_163_128qam
        5                       hy28_201_256qam

Radio Band:    etsi13_1_28_R5 (Index 3)

        Frequency Low Program
        Index           Channel
        0                       1
        1                       2
        2                       3
        3                       4

        Frequency High Program
        Index           Channel
        0                       1'
        1                       2'
        2                       3'
        3                       4'
```

```
        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy28_38_qpsk
        2                       hy28_88_16qam
        3                       hy28_113_32qam
        4                       hy28_138_64qam
        5                       hy28_163_128qam
        6                       hy28_188_256qam
        7                       hy28_201_256qam

        HAAM Mode
        Index           System Mode
        0                       hy28_38_qpsk
        1                       hy28_88_16qam
        2                       hy28_113_32qam
        3                       hy28_138_64qam
        4                       hy28_163_128qam
        5                       hy28_201_256qam

Radio Band:    etsi13_1_14_R5 (Index 4)

        Frequency Low Program
        Index           Channel
        0                       1
        1                       2
        2                       3
        3                       4
        4                       5
        5                       6
        6                       7
        7                       8

        Frequency High Program
        Index           Channel
        0                       1'
        1                       2'
        2                       3'
        3                       4'
        4                       5'
        5                       6'
        6                       7'
        7                       8'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy14_19_qpsk
        2                       hy14_43_16qam
        3                       hy14_56_32qam
        4                       hy14_68_64qam
        5                       hy14_80_128qam
        6                       hy14_93_256qam
        7                       hy14_99_256qam

        HAAM Mode
        Index           System Mode
        0                       hy14_19_qpsk
        1                       hy14_43_16qam
        2                       hy14_56_32qam
        3                       hy14_68_64qam
        4                       hy14_80_128qam
        5                       hy14_99_256qam
```

```
Radio Band:    etsi13_1_7_R5 (Index 5)

        Frequency Low Program
        Index          Channel
        0                      1
        1                      2
        2                      3
        3                      4
        4                      5
        5                      6
        6                      7
        7                      8
        8                      9
        9                      10
        10                     11
        11                     12
        12                     13
        13                     14
        14                     15
        15                     16

        Frequency High Program
        Index          Channel
        0                      1'
        1                      2'
        2                      3'
        3                      4'
        4                      5'
        5                      6'
        6                      7'
        7                      8'
        8                      9'
        9                      10'
        10                     11'
        11                     12'
        12                     13'
        13                     14'
        14                     15'
        15                     16'

        Normal Mode
        Index          System Mode
        0                      cw_test
        1                      hy7_9_qpsk
        2                      hy7_22_16qam
        3                      hy7_28_32qam
        4                      hy7_34_64qam
        5                      hy7_40_128qam
        6                      hy7_47_256qam
        7                      hy7_50_256qam

        HAAM Mode
        Index          System Mode
        0                      hy7_9_qpsk
        1                      hy7_22_16qam
        2                      hy7_28_32qam
        3                      hy7_34_64qam
        4                      hy7_40_128qam

Diplexer Type: 74-000305-02

Radio Band:    esp13_2_56_R5 (Index 1)

        Frequency Low Program
        Index          Channel
        0                      6
        1                      7
        2                      8
        3                      9
        4                      10
```

```
        Frequency High Program
        Index           Channel
        0                       6'
        1                       7'
        2                       8'
        3                       9'
        4                       10'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy56_71_qpsk
        2                       hy56_166_16qam
        3                       hy56_214_32qam
        4                       hy56_261_64qam
        5                       hy56_308_128qam
        6                       hy56_356_256qam
        7                       hy56_380_256qam

        HAAM Mode
        Index           System Mode
        0                       hy56_71_qpsk
        1                       hy56_166_16qam
        2                       hy56_214_32qam
        3                       hy56_261_64qam
        4                       hy56_308_128qam
        5                       hy56_380_256qam

Radio Band:    esp13_2_28_R5 (Index 2)

        Frequency Low Program
        Index           Channel
        0                       4
        1                       5
        2                       6

        Frequency High Program
        Index           Channel
        0                       4'
        1                       5'
        2                       6'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy28_38_qpsk
        2                       hy28_88_16qam
        3                       hy28_113_32qam
        4                       hy28_138_64qam
        5                       hy28_163_128qam
        6                       hy28_188_256qam
        7                       hy28_201_256qam

        HAAM Mode
        Index           System Mode
        0                       hy28_38_qpsk
        1                       hy28_88_16qam
        2                       hy28_113_32qam
        3                       hy28_138_64qam
        4                       hy28_163_128qam
        5                       hy28_201_256qam

Radio Band:    etsi13_2_28_R5 (Index 3)

        Frequency Low Program
        Index           Channel
        0                       5
        1                       6
        2                       7
        3                       8
```

```
        Frequency High Program
        Index           Channel
        0                       5'
        1                       6'
        2                       7'
        3                       8'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy28_38_qpsk
        2                       hy28_88_16qam
        3                       hy28_113_32qam
        4                       hy28_138_64qam
        5                       hy28_163_128qam
        6                       hy28_188_256qam
        7                       hy28_201_256qam

        HAAM Mode
        Index           System Mode
        0                       hy28_38_qpsk
        1                       hy28_88_16qam
        2                       hy28_113_32qam
        3                       hy28_138_64qam
        4                       hy28_163_128qam
        5                       hy28_201_256qam

Radio Band:    etsi13_2_14_R5 (Index 4)

        Frequency Low Program
        Index           Channel
        0                       9
        1                       10
        2                       11
        3                       12
        4                       13
        5                       14
        6                       15
        7                       16

        Frequency High Program
        Index           Channel
        0                       9'
        1                       10'
        2                       11'
        3                       12'
        4                       13'
        5                       14'
        6                       15'
        7                       16'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy14_19_qpsk
        2                       hy14_43_16qam
        3                       hy14_56_32qam
        4                       hy14_68_64qam
        5                       hy14_80_128qam
        6                       hy14_93_256qam
        7                       hy14_99_256qam

        HAAM Mode
        Index           System Mode
        0                       hy14_19_qpsk
        1                       hy14_43_16qam
        2                       hy14_56_32qam
        3                       hy14_68_64qam
        4                       hy14_80_128qam
        5                       hy14_99_256qam
```

Radio Band: etsi13_2_7_R5 (Index 5)

Frequency Low Program

Index	Channel
0	17
1	18
2	19
3	20
4	21
5	22
6	23
7	24
8	25
9	26
10	27
11	28
12	29
13	30
14	31
15	32

Frequency High Program

Index	Channel
0	17'
1	18'
2	19'
3	20'
4	21'
5	22'
6	23'
7	24'
8	25'
9	26'
10	27'
11	28'
12	29'
13	30'
14	31'
15	32'

Normal Mode

Index	System Mode
0	cw_test
1	hy7_9_qpsk
2	hy7_22_16qam
3	hy7_28_32qam
4	hy7_34_64qam
5	hy7_40_128qam
6	hy7_47_256qam
7	hy7_50_256qam

HAAM Mode

Index	System Mode
0	hy7_9_qpsk
1	hy7_22_16qam
2	hy7_28_32qam
3	hy7_34_64qam
4	hy7_40_128qam

Diplexer Type: 74-000306-01

Radio Band: itu15_1_28_490_R5 (Index 1)

Frequency Low Program

Index	Channel
0	1
1	2
2	3
3	4
4	5
5	6

```
        Frequency High Program
        Index           Channel
        0                       1'
        1                       2'
        2                       3'
        3                       4'
        4                       5'
        5                       6'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy28_38_qpsk
        2                       hy28_88_16qam
        3                       hy28_113_32qam
        4                       hy28_138_64qam
        5                       hy28_163_128qam
        6                       hy28_188_256qam
        7                       hy28_201_256qam

        HAAM Mode
        Index           System Mode
        0                       hy28_38_qpsk
        1                       hy28_88_16qam
        2                       hy28_113_32qam
        3                       hy28_138_64qam
        4                       hy28_163_128qam
        5                       hy28_201_256qam

Diplexer Type: 74-000306-02

Radio Band:    itu15_2_28_490_R5 (Index 1)

        Frequency Low Program
        Index           Channel
        0                       7
        1                       8
        2                       9
        3                       10
        4                       11
        5                       12

        Frequency High Program
        Index           Channel
        0                       7'
        1                       8'
        2                       9'
        3                       10'
        4                       11'
        5                       12'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy28_38_qpsk
        2                       hy28_88_16qam
        3                       hy28_113_32qam
        4                       hy28_138_64qam
        5                       hy28_163_128qam
        6                       hy28_188_256qam
        7                       hy28_201_256qam

        HAAM Mode
        Index           System Mode
        0                       hy28_38_qpsk
        1                       hy28_88_16qam
        2                       hy28_113_32qam
        3                       hy28_138_64qam
        4                       hy28_163_128qam
        5                       hy28_201_256qam
```

Diplexer Type: 74-000306-03

Radio Band: etsi56_1_56_R5 (Index 1)

Frequency Low Program

Index	Channel
0	C1
1	C2
2	C3
3	C4

Frequency High Program

Index	Channel
0	C1'
1	C2'
2	C3'
3	C4'

Normal Mode

Index	System Mode
0	cw_test
1	hy56_71_qpsk
2	hy56_166_16qam
3	hy56_214_32qam
4	hy56_261_64qam
5	hy56_308_128qam
6	hy56_356_256qam
7	hy56_380_256qam

HAAM Mode

Index	System Mode
0	hy56_71_qpsk
1	hy56_166_16qam
2	hy56_214_32qam
3	hy56_261_64qam
4	hy56_308_128qam
5	hy56_380_256qam

Radio Band: etsi56_1_28_R5 (Index 2)

Frequency Low Program

Index	Channel
0	C1
1	C2
2	C3
3	C4
4	C5
5	C6
6	C7
7	C8

Frequency High Program

Index	Channel
0	C1'
1	C2'
2	C3'
3	C4'
4	C5'
5	C6'
6	C7'
7	C8'

```
        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy28_38_qpsk
        2                       hy28_88_16qam
        3                       hy28_113_32qam
        4                       hy28_138_64qam
        5                       hy28_163_128qam
        6                       hy28_188_256qam
        7                       hy28_201_256qam

        HAAM Mode
        Index           System Mode
        0                       hy28_38_qpsk
        1                       hy28_88_16qam
        2                       hy28_113_32qam
        3                       hy28_138_64qam
        4                       hy28_163_128qam
        5                       hy28_201_256qam

Diplexer Type: 74-000317-02

Radio Band:    etsi56_2_56_R5 (Index 1)

        Frequency Low Program
        Index           Channel
        0                       C5
        1                       C6
        2                       C7
        3                       C8
        4                       C9

        Frequency High Program
        Index           Channel
        0                       C5'
        1                       C6'
        2                       C7'
        3                       C8'
        4                       C9'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy56_71_qpsk
        2                       hy56_166_16qam
        3                       hy56_214_32qam
        4                       hy56_261_64qam
        5                       hy56_308_128qam
        6                       hy56_356_256qam
        7                       hy56_380_256qam

        HAAM Mode
        Index           System Mode
        0                       hy56_71_qpsk
        1                       hy56_166_16qam
        2                       hy56_214_32qam
        3                       hy56_261_64qam
        4                       hy56_308_128qam
        5                       hy56_380_256qam
```

```
Radio Band:    etsi56_2_28_R5 (Index 2)

        Frequency Low Program
        Index           Channel
        0                       C9
        1                       C10
        2                       C11
        3                       C12
        4                       C13
        5                       C14
        6                       C15
        7                       C16
        8                       C17
        9                       C18

        Frequency High Program
        Index           Channel
        0                       C9'
        1                       C10'
        2                       C11'
        3                       C12'
        4                       C13'
        5                       C14'
        6                       C15'
        7                       C16'
        8                       C17'
        9                       C18'

        Normal Mode
        Index           System Mode
        0                       cw_test
        1                       hy28_38_qpsk
        2                       hy28_88_16qam
        3                       hy28_113_32qam
        4                       hy28_138_64qam
        5                       hy28_163_128qam
        6                       hy28_188_256qam
        7                       hy28_201_256qam

        HAAM Mode
        Index           System Mode
        0                       hy28_38_qpsk
        1                       hy28_88_16qam
        2                       hy28_113_32qam
        3                       hy28_138_64qam
        4                       hy28_163_128qam
        5                       hy28_201_256qam

Diplexer Type: 74-000317-03 Diplexer Type:   74-000317-03
```

This page is left blank intentionally

Appendix C – Site Survey Information

Planning

When installing a microwave link, proper planning is required. Items to be addressed for proper planning include:

- RF path planning
- site preparation, including power and LAN connections
- installation issues for outdoor units including modem and Radio
- Governing body licensing issues (FCC, etc)
- Check local, regional, and national building and electrical codes
- lightning and ground protection
- surge protection
- use of outdoor cabling
- other radio system at the same frequency

Site Survey

A site visit must be done prior to installation to ensure proper line of sight path clearance exists and that proper facilities exist at the site according to the details listed below.

Line–of–Sight and Path Clearance. Determine optimum location for the radio. Radio and antenna location are important to ensure optimum radio range and throughput:

- Install the antenna as high as possible to maximize the range of a building-to-building connection
- Maintain a clear line–of–sight between Horizon Compact Plus antennas. Obstructions can impede performance or limit ability to transmit or receive data. Reduced signal strength could affect performance; and
- Maintain maximum path clearance at both ends for the directional antennas.

When determining maximum path clearance, be aware of objects that restrict performance such as:

- Buildings
- Trees
- Rooftop objects such as a/c units
- Conductive metal surfaces
- standing pools of water
- edges of the roof (parapet) of the building on which the Horizon Compact Plus is to be mounted.

Site Preparation

When you visit the site, be sure to record all installation requirements. You will need to determine the following:

- Other equipment in the area which can potentially interfere with the DragonWave Radios
- Ability to install the Horizon Compact Plus units.
- Facilities exist on which to mount the unit? (3" – 4" diameter pole/mast mount, tower mount, wall mount);
- A mast or tower mount exists and is there sufficient room (clearance) to install the Horizon Compact Plus unit;
- The mast or tower has the ability to withstand wind load due to mounting of the Horizon Compact Plus units;
- Permits that may be required;
- Documentation required by building or site owner/landlord.
- Obstructions, such as tree growth or new buildings, that may be a problem in the future

If the Outdoor Unit (ODU) is being installed, the all-in-one cable will likely have to transit the outside wall and terminate on equipment located inside the building. If the Indoor Unit (Rack mount IDU) is being installed, the IF cable from the radio will likely have to transit the outside wall and terminate at the IDU. Determine the following:

- Cable distance between Horizon Compact Plus and network equipment and the distance to the power source. DragonWave offers 3 lengths (30m, 60m, 90m).
- Location of building penetration point (drainage or service openings, elevator service sheds, other rooftop openings, or penetration through an outside wall).
- Size (diameter) of hole at the building access point. Check for other cables and clearance for Horizon Compact Plus cables.
- Location of the nearest appropriate power outlet
- Location of the nearest ground bar or ground plane bus
- Power backup, such as Uninterruptible Power Supply (UPS)
- Location and ease of access to wiring closets
- Location and ease of access of network equipment (switch, router, etc)
- Grounding points for lightning arrestors and cable shields at building entry point
- Locations and grounding points for surge protectors.
- Check local electrical codes for requirements for lightning rods.
- If possible, ensure that Horizon Compact Plus installations will be lower in height than existing lightning rods

Note: Record all installation requirements, including cable lengths, GPS co-ordinates (height, Lat., Long) and distance between the sites.

Appendix E - 802.1P Priority Tagging Overview

IEEE 802.1P The Institute of Electrical and Electronics Engineering (IEEE) 802.1P signaling method is used for traffic prioritization at OSI Reference Model Layer 2. 802.1p is a spin-off of the 802.1Q (Vlans) standard. Network adapters and switches route traffic based on the priority level for best-effort Quality of Service (QoS).

The 802.1Q VLAN standard specifies a VLAN tag that appends to a MAC frame. The VLAN tag has two parts: The VLAN ID (12-bit) and Prioritization (3-bit). The prioritization field was not defined in the VLAN standard and the 802.1P implementation defines this prioritization field.

To be compliant with 802.1p, Layer 2 switches must be capable of grouping incoming LAN packets into separate traffic classes.

Eight classes are defined by 802.1p. Although network managers must determine actual mappings, IEEE has made broad recommendations. The highest priority is seven, which might go to network-critical traffic such as interactive video and voice. Data classes four through one range from controlled-load applications such as streaming multimedia and business-critical traffic - carrying voice traffic, for instance - down to "loss eligible" traffic. The zero value is used as a best-effort default, invoked automatically when no other value has been set.

IP protocols can efficiently transport various data types over the same network resources. IP traffic is “bursty” in nature and requires flow control, buffering, and other mechanisms to deal with this “bursty” traffic when networks are heavily loaded. The performance attributes of time-sensitive traffic streams, such as voice and video conferencing, are of particular concern when implementing IP networks. The majority of time-sensitive traffic streams (VoIP, TDM over Ethernet, etc) do not have control protocols to negotiate speeds or re-transmits. Traffic is sent assuming delivery and ordering is unchanged.

Ethernet-based architectures require buffering capacity to absorb typical IP bursty traffic and to prevent packet loss to maintain Service Level Agreements (SLAs).

802.1P COS/QOS is used to accommodate bursty IP traffic

CoS vs QoS

What Is Quality of Service?

Quality of Service (QoS) is a traffic management scheme that allows you to create differentiated services for network traffic, thereby providing better service for selected network traffic.

QoS works by slowing down unimportant packets, or discarding those packets under high load. It therefore delivers the important packets, but at the expense of the unimportant packets.

QoS primarily comes into play when the amount of traffic through an interface is greater than the interface’s bandwidth.

When the traffic through an interface exceeds the bandwidth, packets from one or more Queues from which the device selects the next packet to send. By setting the queuing property on a device or interface, you can control how the Queues are serviced, thus determining the priority of the traffic.

What is Class of Service?

Class of Service (CoS) is an algorithm that tags packets then classifies those packets in order to assign them to Queues of differing priority. Unlike Quality of Service (QoS) traffic management, CoS does not ensure network performance or guarantee priority in delivering packets.

In summary: CoS = assigning priority values to data streams

QoS = traffic engineering to process data according to the priority values

Horizon Compact Plus™ Product Manual, 83-000095-01-01-01

Visit us on the Internet at: http://www.dragonwaveinc.com/