



# GarrettCom<sup>®</sup>

## Software Release Notice

### DynaStar 7.7 rc13

This document contains Confidential information or Trade Secrets, or both, which are the property of GarrettCom. This document may not be copied or reproduced or transmitted to others in any manner, nor may any use of the information the document be made, except for the specific purposes for which it is transmitted to the recipient, without the prior written consent of GarrettCom.

Copyright 2009, GarrettCom.  
All Rights Reserved

# VERSION 7.7 rc13 RELEASE NOTES

## 1.1 New Features and Enhancements

This document describes the new features and enhancements that have been added to the **DYNASTAR** products, version 7.7 rc13

- Frame Relay WAN port sub-interface support.
- Serial Port Data Idle timer, changed timer to seconds versus minutes.
- Support for CONITEL 2400 baud option.
- Added unit serial number display.
- Management of IP source address used for Terminal Server, Radius, Syslog etc.
- Firewall Logging
- Quality enhancements.

## 1.2 Frame Relay WAN port sub-interfaces

This feature allows a WAN port (W1 and W2) to support more than one IP interface on a single physical port. This enables a single WAN port to have multiple Frame Relay connections to remote sites, most commonly required when supporting applications where there are multiple Management stations that are configured with different network IP address.

The configuration starts out by defining multiple DLCI's in the Frame Relay DLCI configuration table. Simple define different DLCI's for IP connections (RFC1490) as shown.

\*\*\* Frame Relay DLCI Configuration Table \*\*\*  
Last changed: 4-29-10 9:15:27

Src	Dest	CIR	Frag								
Type	Port	DLCI	Port	DLCI	IP	B	Prty	Kbps	Size	KA	Dest IP Addr
1 RFC 1490	W1	100		Y	1	0	0	N	10.1.1.2		
2 RFC 1490	W1	101		Y	1	0	0	N	11.1.1.2		
3 RFC 1490	W2	200		Y	1	0	0	N	20.1.1.2		
4 RFC 1490	W2	201		Y	1	0	0	N	21.1.1.2		

Once configured you then go to the IP configuration table.

\*\*\* IP Port Information \*\*\*  
Last changed: 4-29-10 9:11:01

Port(s)	Interface	IP Address	IP Mask	[-Use RET to toggle/]	
		x.x.x.x	x.x.x.x	Protocol	Encaps
E0	Ethernet	0.0.0.0	0.0.0.0	RIP	Enet II
W1	CSU/DSU chan 1	0.0.0.0	0.0.0.0	RIP	
W2	CSU/DSU chan 2	0.0.0.0	0.0.0.0	RIP	
E1 - E18	Ether Comm Mod	0.0.0.0	0.0.0.0	RIP	Enet II

Then cursor down to the WAN port of choice (W1 or W2) and enter “CNTRL O” that will take you to a new sub-menu where you can enter different IP networks for each DLCI.

```

*** IP Interface ( W1) CSU/DSU chan 1 ***
      Last changed: 4-29-10 9:11:01
Port(s)  DLCI      IP Address  IP Mask  |-Use RET to toggle|
          x.x.x.x  x.x.x.x    Protocol   Encaps
W1       100       10.1.1.1   255.0.0.0  RIP II
          101       11.1.1.1   255.0.0.0  RIP II

```

### 1.3 Serial Port Data Idle timer

The serial port idle timer used to be based on a value in minutes, this release changes the value to seconds to allow for redundant systems to fail-over faster. The settings are:

0 = disabled  
 1-180 = 1 to 180 seconds, reset by traffic in any direction  
 181-255 = 1 to 75 seconds, reset only by outgoing traffic

### 1.4 Conitel 2400 baud support

Added additional option to run 2400 baud for Conitel transparent protocol

### 1.5 Product serial number

Add the ability to see the DS units serial number to buffer status screen.

```

*** Buffer Pool Status ***

Card Type  Idle Count      Buffers      Max. Pending Queue
           Current Min.  In Use Free  Min.  To Db  From Db
0  Main Proc. 199124 58078   3 32686 32674
           78 in ISR
1  16 Port 319443 243136   1 557 532   1 25
2  ECM    77362 77359   0 5227 5210   3 1

```

**Serial Number: 6b23**  
 DIMM installed: 64 Mbyte

## 1.6 IP source address management

This feature allows the administrator to control which Local IP address is used for various applications. Previously the DynaStar would typically use the local IP address of the interface through which the IP session is established (outgoing). This feature remains as the “best IP address”, however you can now change the source IP address used, to be fixed and match it to any IP interface configured on the unit. This is particularly useful if Firewalls are in use, as previously the actual IP address could change depending upon local influences (IP routing table changes, interfaces go up/down could modify the local IP address being used). Local IP address is selectable for system calls (SNMP, telnet, syslog etc.), terminal server ports and VPNs. Note the DS1500 no longer displays the ROM IP address, which was used for Syslog, SNMP as the IP source address and is no longer needed. Upgrading VPNs will allocate an interface with the same IP address as the previously configured local address, which should result in the same functionality.

## 1.7 MIB II statistics

There were a number of problems reading various Ethernet interface statistics, predominately for the DS1500 platform, changes involved snmp code changes in the image, and no changes have been made to the mib itself. The values that were being returned were either zero or blank for some Ethernet controllers. ( in/out counters, mtu, speed, etc.)

## 1.8 Firewall Logging

### Feature Summary

- Track up to 1000 simultaneous “connections” through the Dynastar.
- The user will have the option of logging to the security log, sending to syslog or sending traps for a number of events.
- This implementation will use the IP filters to determine what is blocked or allowed.
- Logging will be enabled on a per filter basis.
- One assumption is that only routed traffic will be monitored

### Feature Detail

#### *Logging*

Up to 1000 sessions may be tracked.

Any sessions, which have not received a packet for a certain amount of time, will be placed into a dormant state. In the event of there being no sessions available, these dormant sessions will be reused first.

Sessions will be hashed with protocol, source and destination ports and IP addresses for faster lookup.

If the sessions are all in use, a log message will be generated but the session will not be tracked.

The first packet on a session will result in a log being sent if enabled in the filter table.

If the packet is denied, additional packets on the same connection will be counted and a record will be sent based on a configurable timer, default 30 seconds.

If the packet is allowed, an additional record will be generated when the TCP session completes (SYN, SYN-ACK, ACK). A further record will be sent when the session is cleared, reset or declared dead due to inactivity.

Records will be sent based on the configurable timer with packet counts.

If there are no available session records, a log will be generated and sent no more frequently than the configurable timer (default 30 seconds).

## ***Record Format***

The record format of logged firewall events will be as follows (S.S.S.S = Source Address, D.D.D.D = Destination Address, SP = Source Port, DP = Destination Port, T = ICMP Type, X = Hit Count, Y = Hit Rate Interval, N = Max Flow Count):

Permitted TCP Session Start:  
TCP S.S.S.S (SP) -> D.D.D.D (DP), Session started  
Permitted TCP Session Established:  
TCP S.S.S.S (SP) -> D.D.D.D (DP), Session established  
Permitted TCP Session Update:  
TCP Update S.S.S.S (SP) -> D.D.D.D (DP), X packets  
Permitted TCP Session End:  
TCP S.S.S.S (SP) -> D.D.D.D (DP), Session closed  
Permitted UDP Session Start:  
UDP Start S.S.S.S (SP) -> D.D.D.D (DP), Session started  
Permitted UDP Session Update:  
UDP Start S.S.S.S (SP) -> D.D.D.D (DP), X packets  
Permitted ICMP Session Start:  
ICMP Start S.S.S.S (T) -> D.D.D.D, Session started  
Permitted ICMP Session Update:  
ICMP Start S.S.S.S (T) -> D.D.D.D, X packets  
Denied TCP, First Hit:  
TCP Denied S.S.S.S (SP) -> D.D.D.D (DP), First packet  
Denied TCP, Hit Rate:  
TCP Denied S.S.S.S (SP) -> D.D.D.D (DP), X packets in Y-second interval  
Denied UDP, First Hit:  
UDP Denied S.S.S.S (SP) -> D.D.D.D (DP), First packet  
Denied UDP, Hit Rate:  
UDP Denied S.S.S.S (SP) -> D.D.D.D (DP), X packets in Y-second interval  
Denied ICMP, First Hit:  
ICMP Denied S.S.S.S (T) -> D.D.D.D, First packet  
Denied ICMP, Hit Rate:  
ICMP Denied S.S.S.S (T) -> D.D.D.D, X packets in Y-second interval  
Permitted Cache Full TCP/UDP/ICMP rule:  
Warning: Maximum permitted flows (N) are being tracked  
Denied Cache Full:  
Warning: Maximum denied flows (N) are being tracked

## **ICMP**

The first permitted ICMP packet between two IP hosts will be logged. An ICMP packet between a given two IP devices is counted as a session. An ICMP session will be timed out after 100 seconds.

No syslog or trap will be sent when the session times out.

## **UDP**

The first permitted UDP packet will be logged. A UDP packet between a given two IP devices is counted as a session. A UDP session will be timed out after 100 seconds.

No syslog or trap will be sent when the session times out.

## **TCP**

The first permitted TCP packet will be logged. A valid session is one that begins with a valid 3-way handshake (Syn, Syn-Ack, Ack). A log event will be generated when the connection is completed.

Denial of service attacks can be identified because multiple initial packets will be received but connection completed events will not be seen.

Valid sessions will be tracked and a syslog or trap will be sent periodically with packet counts and when the session terminates.

## **Debug**

Filter debug added using hidden command 52

## **Configuration**

New screens include enabling logging destinations.

*\*\*\* Security Logging Configuration \*\*\*  
Last changed: 4-29-10 9:11:01*

<i>Event Type</i>	<i>Log</i>	<i>Alarm</i>	<i>Syslog</i>
		<i>Severity</i>	
<i>Valid Console Logins</i>	<i>Y</i>	<i>N</i>	<i>N</i>
<i>Console Logouts</i>	<i>N</i>	<i>N</i>	<i>N</i>
<i>Failed Password</i>	<i>Y</i>	<i>N</i>	<i>N</i>
<i>Max Failed Password</i>	<i>Y</i>	<i>Y</i>	<i>N</i>
<i>Failed User ID</i>	<i>Y</i>	<i>N</i>	<i>N</i>
<i>Max Failed UID</i>	<i>Y</i>	<i>Y</i>	<i>N</i>
<i>Port Status Change</i>	<i>N</i>	<i>N</i>	<i>N</i>
<i>Ethernet Security</i>	<i>Y</i>	<i>Y</i>	<i>N</i>
<i>Config Change</i>	<i>N</i>	<i>N</i>	<i>N</i>
<i>RADIUS Logins</i>	<i>Y</i>	<i>N</i>	<i>N</i>
<i>RADIUS Logouts</i>	<i>Y</i>	<i>N</i>	<i>N</i>
<i>RADIUS Rejects</i>	<i>Y</i>	<i>Y</i>	<i>N</i>
<i>RADIUS Timeouts</i>	<i>Y</i>	<i>N</i>	<i>N</i>

<i>RADIUS Timeout Logs</i>	<i>Y</i>	<i>N</i>	<i>N</i>
<b><i>Firewall Records</i></b>	<i>N</i>	<i>N</i>	<i>N</i>

Enabling logging per IP Filter entry

\*\*\* IP Filter Table \*\*\*

Last changed: 4-29-10 10:59:06

Type	Source IP (Tog)	Source IP (Address)	Mask (Bits)	Destination IP (Address)	Mask (Bits)	VPN (Tog)	Protocol Filter Ctrl O to config
1	Src	100.1.1.1					Forward
2	Def						Block

\*\*\* UDP/TCP Filter Table \*\*\*

Last changed: 4-29-10 10:59:06

Protocol (Toggle)	Socket Name	Action (Toggle)	Log Interval ((1-600 sec., 0=OFF))	Max MTU (128-1536)	Diff Serv (Toggle)
1	ICMP	Forward	<b>30</b>	1536	None

## 1.9 Quality Enhancements.

- Checked in changes for security logging of password changes. This change effects SRAM to be sure to use cnfgload.cmp during upgrades.
- Logging out from the console application was generating 2 TRAP/SYSLOG messages, this has been fixed so only 1 message is generated.
- VPN stopped working after firewall logging was added, switch IP addresses for incoming VPN check.
- XOT HDLC state problem fixes for Siemens LIRR app  
Blocks not releasing, not resolving collision if call outstanding  
Added hidden commands 72 to dump XOT states for first 20 blocks  
and 158 to toggle XOT debugging. 72 only works if XOT debugging is on.
- XOT sessions not clearing down completely when cleared by remote.
- Make BPDU on non-bridge port message only occur infrequently
- Add port monitor support missing for PAD over Ether on RX.
- Fixed Snmp dynastar time since last status change and mac address.
- BGP: Add logError message to help determine why neighbor net count exceeds RIB count
- BGP: Add initialization of net parameters involved in net count exceeds RIB count
- BGP: processing 0.0.0.0, for default route.
- Stop IP to TRANS ports attempting to call.
- B Block FTP and SFTP incompatible files (alfload.bin, download.bin)
- Bug 2184 - Frame Relay, packet tx'd out wrong interface
- Bug 2188 - VPN / IP filters broken
- Bug 2189 - Can't edit field in supervisor
- Bug 2190 - Siemens XOT / DTR modifications