



GarrettCom[®]

Industrial Networking at Its BestSM

Magnum Network Software – DX

Software Release Notes

Software Revision 3.1.0 RC5

GarrettCom, Inc.

www.GarrettCom.com

www.GarrettCom.com/techsupport

email: support@GarrettCom.com

This document contains Confidential information or Trade Secrets, or both, which are the property of GarrettCom. This document may not be copied, reproduced or transmitted to others in any manner, nor may any use of the information in 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 2010, GarrettCom.

All Rights Reserved

Release 3.1.0 RC5 Release Notes

The following notes describe the many new features and quality enhancements that have been made in MNS-DX version 3.1.0 RC5 (since version 3.0.4 RC4). Please reference the appropriate MNS-DX Software Manual for further details and specifics on new features at <http://www.garrettcom.com/techsupport/index.htm#software> under the Software Technical Manuals option.

1.0 INTRODUCTION

The following notes contain details related to the MNS-DX v3.1.0 RC5 software release. MNS-DX v3.1.0 RC5 includes several enhancements over MNS-DX v3.0.4 RC4 as listed in Sections 2.0 New Features and 3.0 Quality Enhancements.

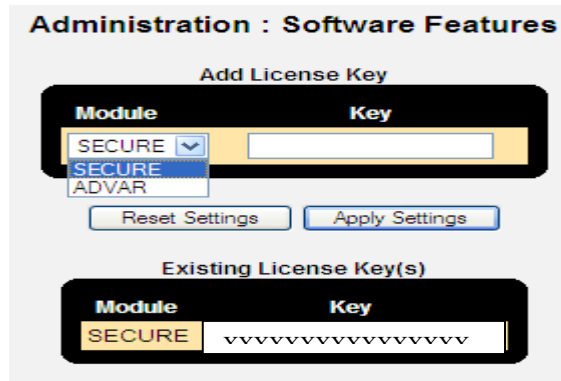
IMPORTANT NOTICE: Please note that LICENSE KEYS are now REQUIRED for certain product features and functionality to be carried forward with this software upgrade. The proper license keys MUST be installed before upgrading the DX unit to 3.1.0 (RC5). If the proper license keys are not installed before you upgrade, you will lose the unit configuration and the product features and functionality that falls under licensing.

To check your license keys, first you MUST be running MNS-DX v3.0 software. You can use the "license show" command from the CLI as shown below:

```
MagnumDX# license show

Feature Key
=====
SECURE XXXXXXXXXXXXXXXXXXXX
```

Or you can use the Web GUI interface page "Administration: Software Features" to view the License Keys that are set (under Existing License Key(s) heading) in the DX unit or add the MNS-DX-SECURE or MNS-DX-ADVAR License Keys as required:



***** If you do not see the keys listed, then they are NOT installed *****

The license keys sets are summarized below:

MNS-DX is the base software license key that comes standard with all DX units and includes capabilities such as:

- Ethernet ports can be configured as switched ports or routed ports or combinations
- Serial ports can be software configurable as RS232 or RS485 ports
- RSTP supports RSTP-2004 (802.1w) & STP (802.1d), provides resilient Ethernet networks
- Routing features support RIP and RIP-II for routed ports
- VRRP – Virtual Router Redundancy Protocol provides router redundancy for Ethernet LAN devices
- DHCP Server and Client – provides DHCP services or queries for IP addresses
- Remote Access for secure administration is via SSH and optionally via telnet
- VLANs (802.1q) supports tagged based VLANs as access VLANs or trunk ports
- SNMP supports v1, v2 and v3 – for managing the device using Network Management Systems
- Event log locally stored provides a log of the most recent events
- SNTP provides time synchronization with NTP/SNTP servers
- Modbus interoperability over Ethernet or serial ports (RS232 or RS485)
- QoS prioritization to traffic using QoS and DiffServ tags across a network, and across a WAN port
- Trouble shooting is made easy with a built in protocol analyzer

MNS-DX-SECURE is an optional license key that can be purchased to add extra security features to the base MNS-DX such as IPSec, VPN, firewall, encryption and authentication needed for industrial cyber security. These extra Security features are unlocked via a licensed software key. MNS-DX-SECURE license key includes:

- IPSec VPN support with proven interoperability and conformance to industry standards
- Firewall provides stateful firewall rules for traffic flows or for IP streams or ports
- RADIUS provides management authentication via a RADIUS Server
- Configurable Login Banner message presented before user login to deter unauthorized users
- Secure Serial SSL connectivity to encrypt data
- Syslog operation enables logs to be collected by syslog servers for analysis
- SSH Port Forwarding allows secure access to less secure devices on the network
- Ethernet port security

MNS-DX-ADVVAR is an optional license key that can be purchased to add the advanced routing options of OSPF and BGP to the base MNS-DX. These Advanced Routing features are unlocked via a licensed software key.

Important Note: It is critical that customers install the appropriate license keys once they have upgraded to v3.0.1 and before upgrading to this software release, 3.1.0 RC5, or

the unit will lose all configuration and product features and functionality related to the above listed license keys.

Please contact your GarrettCom representative to obtain details on receiving the required License Keys. The proper License Keys can be installed via the CLI or Web interfaces.

Once you have your license keys, you can install them using the "license add" CLI command or through the "Administration : Software Features" web page.

***** You MUST reboot your DX after installing the license key(s) for the key(s) to take effect *****

2.0 NEW FEATURES

2.1 3G Cellular Modem

MNS-DX 3.1.0 RC5 software supports the added capability of a cellular modem on the DX940 platform and provides support for CDMA operation on the Verizon Wireless cellular network. The cellular interface provides IP connectivity via a data connection to the internet. There is no support for voice calls.

In order to make data connections on the cellular wireless network, the wireless modem must be activated by the service provider (i.e. Verizon Wireless). Only manual activation via a voice call to customer service is supported. Once activated, over-the-air service provisioning (OTASP) must be manually started by the user and successfully completed before the modem is ready for use. OTASP can be performed using the DX940 software.

When the modem connects to the network, it is automatically assigned a local IP address and default gateway.

2.2 PPP over Frame Relay

The MNS-DX software now supports the ability to establish a PPP connection over a Frame Relay DLCI. The encapsulation of PPP in the frame relay packet will use the techniques described in RFC 1973.

PPP data packets will be placed in the Frame Relay transmit queues according to the settings in the QoS : Diffserv page.

PPP control packets (LCP, IPCP, etc) will be placed in a strict high priority queue which is handled ahead of all data traffic. This is the queue Frame Relay uses for LMI.

2.3 Multilink PPP

The MNS-DX software has been enhanced to support up to four Multilink PPP bundles, and up to four links per bundle. For each bundle, the following parameters must be configured:

- **BID** : A bundle ID (1-4) used to identify this bundle for administrative purposes. Bundle N will correspond to IP interface "BunN". For example, bundle 2 will be IP interface Bun2.
- **Authentication**: None, CHAP, PAP, or CH/PAP
- **Username and Password**: These are used for CHAP or PAP. It is the username and password required to authenticate to us. It's also the username and password we'll try to authenticate with remotely if we are required to do so by the LCP negotiation process.
- **LCP echo interval**: The LCP keep alive time to be used by LCP on the member ports.
- **Fragmentation size**: Maximum size packet that can be transmitted over this bundle. Larger packets will be fragmented using the MLPPP fragmentation procedure.
- **MRRU**: "Maximum received reconstructed unit". The largest packet this bundle will re-assemble.
- **Header Compression**: The type of IP compression to use on this bundle. The options are None, VJC and IPHC.
- **Member ports**: The ports that comprise the bundle.
- **LFI**: If this option is used, packets marked as Expedited Forward (DSCP 46) will not be encapsulated with an MLPPP header, just a normal PPP header. These packets will not be subject to MLPPP fragmentation.

The IP address of the MLPPP interface must be configured in the system IP address table after the bundle is created. The bundle member ports will not begin PPP until this is complete.

Bundle member ports may be serial ports, but these ports cannot be attached to a modem.

Bundles cannot be configured to use IPCP to assign an IP to the other end of the bundle. Packets sent over a PPP bundle will have an MLPPP header as described by RFC 1990 unless special handling is required (such as Link Fragmentation and Interleaving).

MLPPP has the capability to fragment packets; however only a single packet can be fragmented and reassembled at a time, so multiple fragmented packets cannot be interleaved. To prevent MLPPP packet reassembly issues, most MLPPP traffic is assigned a priority of 2 regardless of any QOS settings. The exception to this pertains to the LFI feature described in Section 2.4.

2.4 Real-time Queue and Link Fragmentation and Interleaving

Operation has been enhanced to support Link Fragmentation and Interleaving (LFI) over a PPP Bundle that is compatible with Cisco routers. This functionality is primarily for sharing a low-speed WAN link between low-priority data and real-time traffic such as VoIP.

LFI in MNS-DX will be an optional queuing discipline that may be configured for a PPP Multilink Bundle. To enable LFI, the user should choose an appropriate fragment size when configuring a bundle and enable the “LFI” option for the bundle.

When LFI is enabled, packets marked for Expedited Forwarding (DSCP 46) will be handled as follows:

- No MLPPP fragmentation
- No MLPPP header/encapsulation
- If member port is a DLCI, the packet is placed in a high priority transmit queue (priority 4) regardless of the setting in QoS : DiffServ page

The Frame Relay Transmit queue mode (TxQ Mode) should be configured appropriately (see section 2.5).

2.5 Frame Relay Priority Queues

For each WAN port, the user may select a frame relay queuing discipline. The options are as follows:

- **8421** 8-4-2-1 weighted fair queue
- **S421** Strict queue for the highest priority traffic, lower priority traffic gets remaining bandwidth based on a 4-2-1 WFQ scheme
- **T421** Strict queue for the highest priority traffic with a token bucket policer that limits the total bandwidth that can be consumed by the highest priority traffic. Lower priority traffic gets remaining bandwidth based on a 4-2-1 WFQ scheme.

For **T421**, the total bandwidth allocated to high priority traffic can be configured by the user by setting the **Token Q Pct** value. This is the sustained percentage of bandwidth that high priority traffic can consume. If high priority traffic is using less than **Token Q Pct** of the link, the token bucket will continue to fill until it reaches a max of two seconds of link bandwidth. At that point, if the policed traffic is sent at line rate, it will be allowed to consume all the link bandwidth for a minimum of two seconds before being limited to the **Token Q Pct** value.

2.6 DNS Support

Functionality is added to allow a user to configure host names in applicable areas of the system. Host names are resolved (i.e., an IP address is determined for the host name) in two

ways: either in the statically configured host table or by dynamically resolving them using the Domain Name System.

A host name or IP address may be configured for certain configuration items. When a host name is configured, the system will first look for the host name in the static host configuration and if it is not found will attempt to resolve it using DNS.

Dynamic DNS Updating (DDNS Updating) is also supported and will update DNS Servers when an interface becomes operational (up and with an IP address assigned to it.) Only the HTTP update method is supported.

3.0 QUALITY ENHANCEMENTS (Previous issues resolved and minor enhancements)

- 3.1** Protocol monitor does not work for W2 interface on DX1000. (#2295)
- 3.2** Port forwarding to a nonexistent device causes the SSH session to be logged out. With this change, the system now logs errors to the port forwarding window, the SSH tunnel window, and PuTTY log file, and closes down the port forwarding session and its related window after a small delay to allow the user to read the error message. (#2263)
- 3.3** Port forwarding telnet session cross posts key strokes. Session IDs that were supposed to be unique were incorrectly re-used causing old session data to be posted to new sessions. (#2315)
- 3.4** Output from "vpn trace high" CLI command is missing information. (#2298)
- 3.5** VPN incorrectly logs "Dead Peer Detected" event when DPD is negotiated with a peer. This event should be logged when a dead peer is actually detected via the keepalive mechanism. (#2299)
- 3.6** PSK for VPN tunnels have maximum key length of 20. Key length is increased to a maximum of 128. Now accepts all alphanumeric characters as well as the '?' character. (#2303)
- 3.7** Added a one year password aging option for user accounts. (#2146)
- 3.8** Added an optional parameter that allows administrator passwords to expire and force a password change. (#2162)
- 3.9** Resolved web page error that occurs after a user with an expired password tries to log in. (#2296)

- 3.10** When a user password expires, the CLI did not allow the user to change their password. This capability has been added. (#2304)
- 3.11** OSPF/RIP interfaces should be disabled by default. (#2272)
- 3.12** The CLI command "snmp add trap-station" had an undocumented keyword so resolved the command. (#2285)
- 3.13** Static NAT table allows duplicate entries. Changed so that duplicate entries cause an error to be reported. (#2289)
- 3.14** Changed text on system information screen from "License: None" to "License: MNS-DX". (#2291)
- 3.15** Software should not allow installation of multiple licenses of the same type. Installing duplicate licenses now causes an error to be reported. (#2300)
- 3.16** Resolved issue of serial port S7 on the DX1000 has signal DCD always 'On' no matter the actual hardware state. (#2308)
- 3.17** Increased the Login Banner size to a maximum of 1000 characters. (#2309)
- 3.18** When an Inactive User Expiration is Set the users should expire without having to login first. (#2311)
- 3.19** Outbound firewall is ineffective when a packet is being tunneled through a VPN. (#2290)
- 3.20** Fixed problem where IP traffic is always routed through a VPN tunnel if one exists, even if there is a lower cost route available. (2277)
- 3.21** Fixed problem where Linux/Cygwin SFTP client hangs after "quit" when connecting to DX. (#2274)
- 3.22** Resolved issue where an Async PPP link will not come up between DX and Cisco router. (#2335)
- 3.23** Fixed issue where downloaded files are truncated when using PuTTY PSFTP client. (#2324)
- 3.24** Inter-VLAN routing not functioning properly on DX940. All untagged VLAN traffic was being assigned to VLAN 1. (#2342)
- 3.25** Changed software so that new events are saved to the persistent memory log files once every 180 seconds. (#2339)

- 3.26** Changed software so that installed license keys are not deleted when the system is returned to factory defaults. (#2348)
- 3.27** Change Ethernet histogram counter display for DX940 also, counter values are now a sum of Rx and Tx. There is a hardware limitation that does not allow Rx and Tx to be counted separately. (#2345)
- 3.28** Add CLI command 'fr clear statistics'. (#2367)
- 3.29** Static routes that point to next hops out a PPP link were deleted when IP addresses are changed. This has been resolved. (#2369)
- 3.30** DX940 shows RJ45s instead of fiber ports on virtual front panel display. (#2358)
- 3.31** Increased maximum number of terminal server channels per port to 32. (#2354)
- 3.32** Under certain rare situations, utilizing the ping command could send cpu utilization to 100%. This has been resolved. (#2370)
- 3.33** VPN as backup route doesn't work when traffic is destined to a DX private IP address. (#2379)
- 3.34** In some cases, traffic is not passed over VPN as it is expected to be routed. (#2380)
- 3.35** The PPP crash that could sometimes occur when the connection is reset under load has been resolved. (2383)
- 3.36** Increased the maximum number of firewall rules to 100 rules. (#2387)
- 3.37** If the user attempts to load or boot a pre 2.1.0 image on a DX40 with an incompatible flash type, the following message is displayed and the boot fails:

"Failure: Version x.y.z does not support flash device." (#2374)
- 3.38** Fixed E1 CAS operation (no time slot 16). (#2388)
- 3.39** Add "fr clear fragmentation" to the CLI. (#2390)
- 3.40** Display an error when the user tries to upload a duplicate filename in the "Administration : Software Upgrade" page. (#2366)
- 3.41** RFC1490 DLCI's always show as "UP" initially in "Routing : IP Addresses" even if DLCI is inactive. (#2389)
- 3.42** Previously could not set PPP authentication to CHAP/PAP through the CLI. (#2397)
- 3.43** All PPP connections would be reset when a profile is reset. Now only those connections using the specific profile will be reset. (#2398)

- 3.44 Setting VJC compression over a PPP link could cause a system crash. (#2399)
- 3.45 CLI help displays a valid username of up to 32 characters but only accepts up to 31. (#2401)
- 3.46 System will now properly display profile names longer than 16 chars in CLI. (#2394)
- 3.47 Add 'ppp clear statistics' command in CLI. (#2395)
- 3.48 Cleaned up superfluous messages in CLI when working with PPP. (#2400)
- 3.49 PPP over serial doesn't detect a physical link down status. (#2396)
- 3.50 Frame Relay monitor swaps "FrameNum" and "DLCI". (#2407)
- 3.51 Add unit serial number to the system info page available through CLI or Web GUI. (#2409)
- 3.52 Fixed an IPsec interoperability issue with Cisco 2800 router. This was a regression in 3.0. Tunnel cycles from up to down periodically. (#2432)
- 3.53 When the target of a port forwarding connection takes too much time to respond to a connect request, the SSH server times out the TCP write too quickly, with the result that the port forwarding connection is closed down before the handshake can proceed. (#2441)
- 3.54 If a configuration has 1 or more non-IP DLCI's, switching configurations will fail after a few configuration switches. (#2440)