



***HyperIP***®  
**IP WAN Optimizer**

**Release 5.5.3-02**

---

**User Guide**

by  
**netex**

---

# Revision Record

Revision	Description
0.06	Pre-release
0.09	Pre-release
0.12	Installation Wizard support
1.0	Manual released
2.0	Corrections and updates for HyperIP release 2.0
3.0	Corrections and updates for HyperIP release 3.0
4.0	Corrections and updates for HyperIP release 4.0
5.1	Corrections and updates for HyperIP release 5.1
5.3	Corrections and updates for HyperIP release 5.3 (added troubleshooting section)
5.4	Corrections and updates for HyperIP release 5.4 (support new hardware model)
5.5	Corrections and updates for HyperIP Release 5.5 (NxN support, support for multiple disk image versions)
5.5.1	Corrections and updates for HyperIP Release 5.5.1 (VMware ESX support)
5.5.1-1	Corrections to netex.com website references; corrections to installation section and miscellaneous typographical errors
5.5.1-2	Correct the hardware platform back panels description
5.5.2	Corrections and Updates for HyperIP release 5.5.2 (smaller disk footprint for VMware)
5.5.3	Added support for new hardware platform; support for VMware tools; new CLI commands for initial configuration
5.5.3-01	Remove broken cross-references in the NRBSStat Error Codes and System Error Codes section.
5.5.3-02	Update key request references, copyrights and logo

© 2006-2011 by Network Executive Software, Inc. Reproduction is prohibited without prior permission of Network Executive Software. Printed in the U.S.A. All rights reserved.

The U.S. Department of Commerce may restrict the distribution of technical information contained in this document when exported outside the U.S. Therefore, careful attention should be given to compliance with all applicable U.S. Export Laws if any part of this document is to be exported.

You may submit written comments using the comment sheet at the back of this manual to:

Network Executive Software, Inc. (NetEx or NESi)  
Publications Department  
6420 Sycamore Lane  
Maple Grove, MN 55369  
USA

Comments may also be submitted over the Internet by addressing e-mail to [pubs@netex.com](mailto:pubs@netex.com), or by visiting our web site at <http://www.netex.com>.

Always include the complete title of the document with your comments.

# Preface

This manual contains reference information for the Network Executive Software (NetEx) HyperIP product. It is intended for installers and users of the product.

This manual can be found on the HyperIP Software CD and is accessible on our website via documentation links on the HOME Page.

## Notice to the Customer

Comments about this manual may be submitted via e-mail to [pubs@netex.com](mailto:pubs@netex.com) or by visiting our website, <http://www.netex.com>. Always include the complete title of the document with your comments.

Information on Network Executive Software's general software support policy (e.g., alternate contact methods, support severity level descriptions, and service status definitions) may be found at <http://www.netex.com/support/product-support/hyperip>.

Details on Network Executive Software's warranty and support policies specific to HyperIP may be found at <http://www.netex.com/support/hyperip-hardware-support-policy>.

## Modifications to HyperIP

HyperIP contains proprietary software. Modifications to the software or NetEx provided hardware platforms that are not specifically authorized by NetEx are prohibited.

Examples of prohibited activities include (but are not limited to) the following items:

- Installing other software on HyperIP
- Modifying the file system (including adding, deleting, or moving files and/or directories, or changing permission levels, ownership, or other attributes of files and/or directories)
- Adding or deleting user accounts
- Starting or stopping system services
- Adding or removing hardware components from NetEx provided hardware platforms.

Any unauthorized modifications to HyperIP may affect its operation and/or obstruct NetEx's ability to diagnose problems and provide corrections. Any work resulting from unauthorized modifications shall be paid by the customer at NetEx's then-current support rates and may result in the immediate termination of warranty/support coverage.

## Notice to the Reader

The material contained in this publication is for informational purposes only and is subject to change without notice. Network Executive Software is not responsible for the use of any product options or a feature not described in this publication, and assumes no responsibility for any errors that may appear in this publication.

Refer to the revision record (at the beginning of this document) to determine the revision level of this publication.

Network Executive Software does not by publication of the descriptions and technical documentation contained herein, grant a license to make, have made, use, sell, sublicense, or lease any equipment or programs designed or constructed in accordance with this information.

## Corporation Trademarks and Products

**Network Executive Software**      **HyperIP®, NetEx®**

**VMware**                              **ESX™, ESXi™**

These references are made for informational purposes only.

# Document Conventions

The following notational conventions are used in this document.

Format	Description
displayed information	Information displayed on a display terminal (or printed) is shown in this font.
<i>user entry</i>	<i>This font</i> is used to indicate the information to be entered by the user.
UPPERCASE	The exact form of a keyword that is not case-sensitive or is issued in uppercase.
MIXedcase	The exact form of a keyword that is not case-sensitive or is issued in uppercase, with the minimum spelling shown in uppercase.
<b>bold</b>	The exact form of a keyword that is case-sensitive and all or part of it must be issued in lowercase.
lowercase	A user-supplied name or string.
value	Underlined parameters or options are defaults.
< <i>label</i> >	The label of a key/button appearing on a keyboard or GUI screen. If “label” is in uppercase, it matches the label on the key (for example: <ENTER>). If “label” is in lowercase, it describes the label on the key (for example: <up-arrow>).
<key1><key2>	Two keys to be pressed simultaneously.
No delimiter	Required keyword/parameter.

# Contents

<b>Revision Record .....</b>	<b>ii</b>
<b>Preface.....</b>	<b>iv</b>
Notice to the Customer .....	iv
Modifications to HyperIP.....	iv
Notice to the Reader.....	v
Corporation Trademarks and Products.....	v
Document Conventions.....	vi
<b>Contents .....</b>	<b>vii</b>
<b>Figures.....</b>	<b>x</b>
<b>Introduction.....</b>	<b>1</b>
<b>Theory of Operation .....</b>	<b>3</b>
Un-optimized Traffic .....	4
<b>Typical Gateway Mode Configuration.....</b>	<b>5</b>
<b>Proxy IP Address Configuration .....</b>	<b>7</b>
<b>Automatic Hot-Standby Configuration .....</b>	<b>9</b>
<b>Multiple Site (NxN) Configuration.....</b>	<b>13</b>
<b>Product Features.....</b>	<b>15</b>
Statistics and Diagnostics.....	15
Idle Traffic Processing .....	15
HyperIP Configuration.....	15
Multiple User Interfaces.....	15
Efficient Bandwidth Management .....	16
SNMP.....	16
Data Compression .....	16
Automatic Hot-Standby .....	17
Two Deployment Modes.....	17
NTP Compatible .....	17
Command Line Interface (CLI) .....	17
<b>Scalability Considerations.....</b>	<b>19</b>
<b>Security Considerations.....</b>	<b>21</b>
Physical Security for NetEx Provided Hardware Appliance .....	21
System Security .....	21
Security of User Data.....	21

Securing Management Access.....	21
<b>HyperIP Command Line Interface .....</b>	<b>23</b>
Overview .....	23
Features.....	23
Restrictions for the CLI.....	23
Command Descriptions .....	24
CLI Command Summary .....	25
<b>Web Browser User Interface .....</b>	<b>35</b>
Browser Considerations.....	35
Home Page.....	35
The Status Bar .....	35
The “-left frame-” Menu .....	37
The “-right frame-” Menu.....	38
The “HyperIP Services” Menu.....	39
HyperIP Web Browser Pages .....	40
HyperIP HOME Page.....	40
Admin Password.....	40
Web Browser Access Password .....	41
Web Browser Certificates.....	41
View Latest Documentation .....	41
Install Commands.....	41
License Key .....	41
Warnings for License Expiration and Automatic Hot-Standby (AHS) Role Changes.....	42
SNMP Configuration.....	42
HyperIP System Config Page.....	44
HyperIP Config Page.....	47
NxN Configuration Page .....	48
Bandwidth Schedule (Rate Limiting) Page .....	50
Proxies and Intercepts Page.....	51
HyperIP Proxies .....	51
HyperIP Intercepts.....	52
Advanced Config Page.....	53
Maintenance Page.....	56
HyperIP Code Updates and Images.....	57
HyperIP Configuration Save/Restore .....	58
Display HyperIP State / Site Status Detail .....	58
Diagnostic Commands Page.....	61
Measure HyperIP Path.....	62
Segment Size Test .....	62
Diagnostic Dump Processing .....	63
TCP Dump Processing .....	64
HTTP File Downloads Page.....	66
Download to your browser workstation .....	66
Upload from your browser workstation.....	67
<b>Operational Procedures .....</b>	<b>69</b>
Initial Configuration via Serial Port (or console for VMware) to Use Web Interface .....	69
Saving HyperIP Configuration to Your Workstation .....	70
Restoring HyperIP Configuration from your Windows Workstation.....	70

Downloading Software Updates (Patches).....	71
Upgrade (Image Restore) Procedure.....	71
Switching Partitions – General Case.....	72
<b>HyperIP Appliance .....</b>	<b>75</b>
Chassis Description.....	75
Power .....	77
Powering Off the Appliance .....	80
Agency Certifications .....	80
<b>Customer Troubleshooting .....</b>	<b>81</b>
Accessing HyperIP.....	81
Statistics .....	81
Informational Logs .....	81
System Dumps .....	81
System Log .....	81
HyperIP Base Log.....	82
Troubleshooting via the Web Browser Interface .....	82
Diagnostic Page/Traceroute .....	82
Advanced Web Page .....	83
System Config Page.....	83
Problem Isolation/Resolution.....	83
Hardware Problem For NetEx Supplied Hardware Platform Only.....	83
Cannot Access HyperIP to Perform Initial Configuration .....	84
Cannot Access HyperIP Web Interface after Initial Configuration .....	84
Cannot communicate between HyperIPs .....	84
Applications Cannot Communicate To or Through HyperIP .....	85
Poor Performance across the Network.....	87
Troubleshooting using the Display HyperIP State Command .....	88
Local System Related Configuration Problems .....	97
<b>Appendix A: NRBSStat Error Codes .....</b>	<b>99</b>
System Log File .....	99
NRBSStat Error Codes.....	99
System Error Codes .....	107
<b>Appendix B: GPL License.....</b>	<b>109</b>

# Figures

- Figure 1: Un-optimized Traffic Disposition Matrix ..... 4
- Figure 2: Typical HyperIP “Gateway” Configuration..... 5
- Figure 3: Typical Proxy IP Address Configuration..... 7
- Figure 4: Typical Automatic Hot-Standby “Gateway” Configuration ..... 9
- Figure 5: HyperIP AHS Roles/State Diagram ..... 10
- Figure 6: NxN HyperIP Configuration..... 13
- Figure 7: Web Browser Page Status Bar Screen Capture..... 36
- Figure 8: Web Browser Page Status Bar Description..... 37
- Figure 9: Web Browser Page “-left frame-“ Menu ..... 37
- Figure 10: Web Browser Page “-right frame-“ Menu..... 38
- Figure 11: Web Browser Page “HyperIP Services Menu..... 39
- Figure 12: Web Browser Home Page ..... 40
- Figure 13: Web Browser Install Page and Install Help ..... 43
- Figure 14: Web Browser System Config Page and Help ..... 45
- Figure 15: Web Browser HyperIP Configure and NxN Config Page ..... 47
- Figure 16: Web Browser Rate Limit Schedule Page..... 50
- Figure 17: Web Browser Proxies and Intercepts Page ..... 51
- Figure 18: Web Browser Advanced Configure Page ..... 53
- Figure 19: Web Browser Show/Set Site Tune Parameters Page ..... 55
- Figure 20: Web Browser Maintenance Page ..... 56
- Figure 21: HyperIP State Display..... 59
- Figure 22: Web Browser Diagnostic Commands Page ..... 61
- Figure 23: Web Browser Diagnostic Page (tcpdump output)..... 65
- Figure 24: Web Browser File Downloads/Uploads Page (Download)..... 66
- Figure 25: HyperIP Hardware Model Differences ..... 75
- Figure 26: Control Button and Status LED Locations..... 76
- Figure 27: Control Button Functions..... 76
- Figure 28: LED Status Indicators ..... 77
- Figure 29: View of Rear Panel for Models 10XY..... 78
- Figure 30: NIC Status LEDs on Ethernet NIC Connectors ..... 78
- Figure 31: Drawing of Rear Panel for Models 11XY, 12XY ..... 79
- Figure 32: Drawing of Rear Panel for Models 13XY, 14XY..... 79

Figure 33: Drawing of Rear Panel for Models 15XY.....	80
Figure 34: Display HyperIP State Command Output, Part 1 .....	89
Figure 35: Display HyperIP State Command Output, Part 2 .....	90
Figure 36: Details for HyperIP State Command Output, Part 2 .....	91
Figure 37: Display HyperIP State Command Output, Part 3 .....	92
Figure 38: Details for HyperIP State Command Output, Part 3 .....	93
Figure 39: Display HyperIP State Command Output, Part 4 .....	94
Figure 40: Details of HyperIP State Command Output, Part 4.....	95
Figure 41: Symptom and Problem Determination Table .....	97



# Introduction

HyperIP improves IP application performance when running over high-speed IP WAN networks. HyperIP provides three primary functions to enhance performance:

- 1) **Application Acceleration over distance** – mitigates the effects of long distance (latency) on TCP/IP traffic.
- 2) **Data Compression** – highly efficient, block level compression (beneficial at speeds exceeding 200Mb/s rates)
- 3) **Shield** from variations in WAN conditions. HyperIP increases the tolerance of TCP applications for variations in WAN conditions that may be occasional but are often disruptive:
  - Latency
  - Jitter
  - Bit Error Rate
  - Distance
  - Bandwidth changes
  - Out of order packets

HyperIP can be valuable as a rate-limiting tool as well. Its time-of-day bandwidth scheduler can be set to rate limit specifically to your site's requirements.



# Theory of Operation

Each of the HyperIPs serves as the endpoint of the TCP connection to the application server (or storage controller) on the LAN segment. An independent connection is maintained over the WAN between the HyperIPs. The flow of data from the application is governed by the generation of TCP acknowledgements from the local HyperIP to the local application server or storage controller. These acknowledgements keep the TCP windows open, so data can continue to be sent by the application. HyperIP shields the application's TCP connection from performance variations due to packet loss and latency on the WAN, since the performance over the WAN is managed by HyperIP.

The HyperIP protocol dynamically adjusts the rate control, latency time, and bandwidth capacity to match the changing conditions of the network. Rate control is established by matching the speed at which the sending HyperIP is sending data, to the speed at which the peer HyperIP is receiving the data. HyperIP dynamically calculates round-trip times, bandwidth capacity, and transmission rates, and uses that information to calculate the capacity of the network.

HyperIP manages multiple LAN packet streams, and aggregates them over the HyperIP network. As new TCP application connections are started, HyperIP is able to accommodate the additional workload by inserting the new packet stream into the HyperIP connection without creating congestion. As TCP applications are stopped, the additional bandwidth capacity is automatically reclaimed by HyperIP for sharing among the remaining connections.

HyperIP also has the ability to compress the aggregated blocks prior to sending them over the WAN. Depending on the compressibility of the data, this usually results in a fewer number of packets traversing the WAN.

A HyperIP deployment may consist of an Automatic Hot-Standby (AHS) configuration, in which case two HyperIPs exist on each end of an IP WAN connection that provide an automatic failover capability; or a HyperIP deployment may consist of a single HyperIP on each end of an IP WAN connection (non-AHS).

For either AHS or non-AHS configurations, HyperIP can be deployed in either *Gateway Mode* or *Proxy Mode*, which are described in later sections.

# Un-optimized Traffic

It is entirely possible that HyperIP could be receiving TCP traffic but not accelerating it. This can happen when connections are established prior to HyperIP being fully operational or when Gateway mode is disabled. Site policies can vary among customers regarding how un-optimized traffic should be handled when received at the HyperIP data interface. The following matrix shows how HyperIP can be configured to handle this traffic under the following circumstances (Bold values are the defaults):

<b>Packet Characteristics</b>	<i>New Connections</i> <b>(Configured in HyperIP)</b>	<i>Current Connections</i> <b>(Configured in HyperIP)</b>	<b>Packet Disposition</b>
TCP connect	Forwarded	Forwarded	Forwarded
TCP connect	<b>Blocked</b>	n/a	Dropped
TCP data	n/a	<b>Forwarded</b>	Forwarded
TCP data	n/a	Blocked	Dropped

**Figure 1: Un-optimized Traffic Disposition Matrix**

HyperIP can also forward connections after it reaches a maximum number of optimized connections. This option requires the Current Connections setting above to be set to Forwarded.

These options are set on the HyperIP Config webpage.

# Typical Gateway Mode Configuration

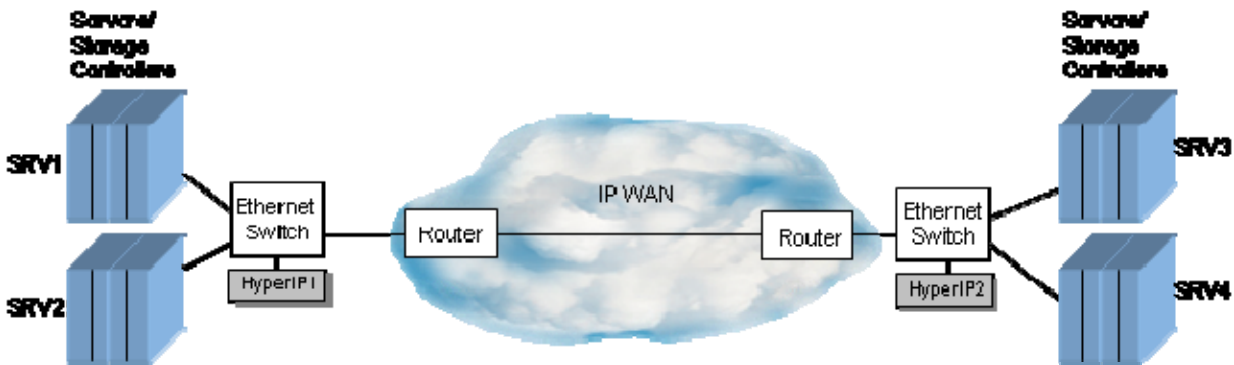


Figure 2: Typical HyperIP “Gateway” Configuration

In order to optimize traffic between applications in the two LAN networks, the application hosts or IP-enabled storage controllers (SRV1, SRV2, etc.) are configured to send the IP traffic to the HyperIP by specifying a static route with the HyperIP as the IP gateway for the destination application host’s IP address. HyperIP determines which packets are to be re-routed and optimized via HyperIP. Non-optimized packets follow standard routing rules in effect, and in the picture above, would typically still be routed over the IP WAN, but would not be optimized.

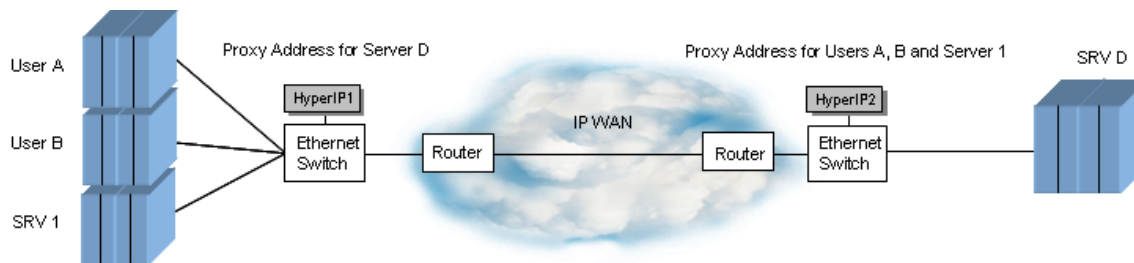
As shown in the picture, there can be an arbitrary number of hosts configured to be rerouted through HyperIP. One or more hosts (or IP-enabled storage controllers) may exist on each side of the WAN “cloud”. However, from an application standpoint, the application connectivity through HyperIP must be peer-to-peer. In other words, TCP applications running on SRV1 and SRV2, communicate with their peer applications on SRV3 and/or SRV4.

Note: In this mode of operation, HyperIP requires at least one intercept defining the source, destination IP addresses and ports to be optimized.



# Proxy IP Address Configuration

Some customer networks/applications may be better suited to employ the feature of Proxy IP Address mode. Proxy IP Address mode allows a customer to deploy the HyperIPs anywhere in the customer network, by configuring a secondary IP address (used as a “proxy” IP address) for each of the remote host IP addresses which require optimized IP WAN services. The “proxy” IP addresses are valid IP addresses on the local subnet. The applications use the local proxy address which is configured in the HyperIPs. The applications’ data is passed between the HyperIPs and subsequently delivered to the “real” host IP address at the remote site. The picture below describes this configuration:



**Figure 3: Typical Proxy IP Address Configuration**

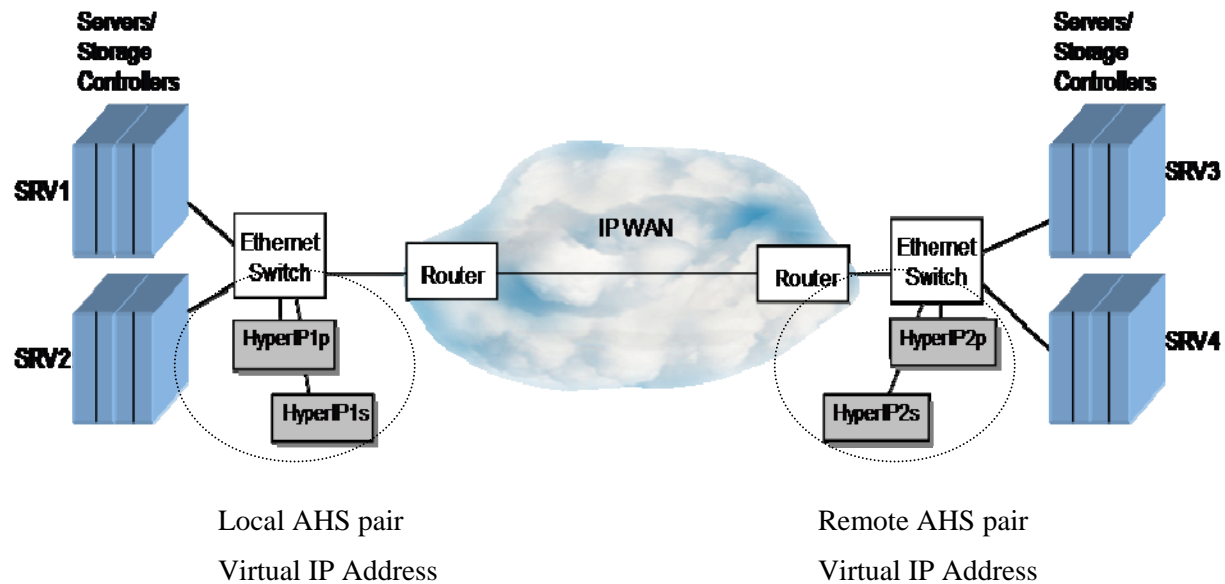
Proxy IP Address mode is used for:

1. Finer granularity of control of applications which can use the HyperIPs
  - This deployment allows a customer to provide optimized IP WAN services to a specific application, server or even an individual instance of an application (as indicated by “User A” and “User B” in Figure 3) at the IP level when configured in the application.
  - Additional security may be achieved due to limiting the TCP connections to the configured “proxy” IP addresses.
2. Ease of deployment.
  - Deployment can be done on any subnet, since this implementation utilizes the existing routing policies.
  - Does not require specific gateway definitions to be set in the network or in the application hosts.

\*Note: Not all applications allow proxy IP addressing.



# Automatic Hot-Standby Configuration



**Figure 4: Typical Automatic Hot-Standby “Gateway” Configuration**

The Automatic Hot-Standby (AHS) feature provides “appliance level” redundancy to the HyperIP configuration. In the above AHS configuration, both sides of the HyperIP network have an AHS pair deployed. The two members of the AHS pair act as a single entity to the application hosts. One member is identified as ‘primary’ and the other as ‘secondary’. There is nothing special about these names; they are just unique terms for identifying each member.

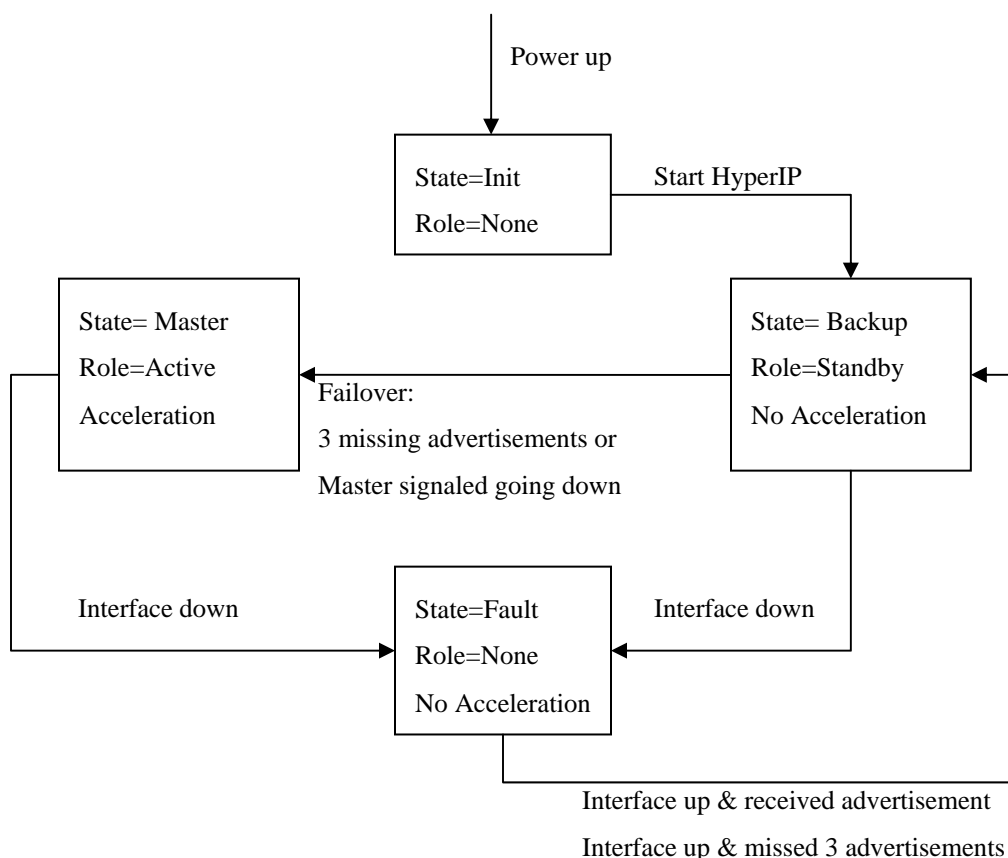
Just like the non-AHS configuration, each HyperIP interface is assigned a unique IP address on the subnet it will reside on. Both members of the AHS pair must be deployed on the same subnet (i.e., have an IP address residing on the same subnet). Additionally, the AHS pair is assigned another IP address on that subnet, known as a virtual IP address. The virtual IP address is shared by the AHS pair, but is ‘owned’ by only one HyperIP at any given time. This virtual IP address is the address known and used by the application servers (as the gateway address) to direct IP traffic to.

At any given time, each AHS member has a specific role. The member currently in use (i.e., owning the virtual IP address and accepting IP traffic on behalf of the virtual IP address) has the ‘Active’ role while the other member has the ‘Standby’ role.

The AHS feature provides for failover capability when the ‘Active’ becomes inoperable. The ‘Standby’ will assume ownership of the virtual IP address and the responsibility of optimizing the IP transported traffic by becoming the ‘Active’. Existing TCP connections will be broken and new (and renewed) TCP sessions will be established, providing applications with optimized IP WAN traffic through the new

‘Active’ HyperIP. When the previously failed HyperIP is once again operational, it will assume the ‘Standby’ role.

The following state diagram illustrates the AHS states and roles the HyperIPs may be operating in, and events which cause state changes:



**Figure 5: HyperIP AHS Roles/State Diagram**

In order to provide high availability, several configuration items must be obtained and setup in the HyperIPs. Each of the members in an AHS pair requires an IP address for the physical Ethernet interface (i.e. data interface). These IP addresses are used by HyperIP to transmit IP packets across the WAN to the remote HyperIP and for AHS pair advertising. The AHS pair also utilizes a virtual IP address. This address is used as the gateway address by the local application hosts. When HyperIP are configured for proxy IP addresses, these too are virtual addresses for the HyperIP.

An implementation of Virtual Routing Redundancy Protocol (VRRP) (IETF RFC 2338) is used to provide the high availability feature. VRRP protocol also requires a “virtual router ID”. The virtual router ID is an 8-bit value that must be unique on the local area network and identifies the unique group participating in the VRRP communication. Other routers or AHS pairs on the same LAN may be running an implementation of VRRP also requiring unique virtual router IDs. See your network administrator for a unique virtual router ID for each AHS pair.

*Note: If a virtual router ID is not unique for the AHS pair on the LAN, the communication between the members may be unpredictable, as it is not known how another vendors' equipment will respond to the messages intended for an AHS HyperIP.*

*Note: The master HyperIP's data interface MAC address is used in response to ARP requests. This varies from the above mentioned RFC.*

If an AHS pair of HyperIP units is connected to an Ethernet switch running spanning tree, the following must be taken into consideration.

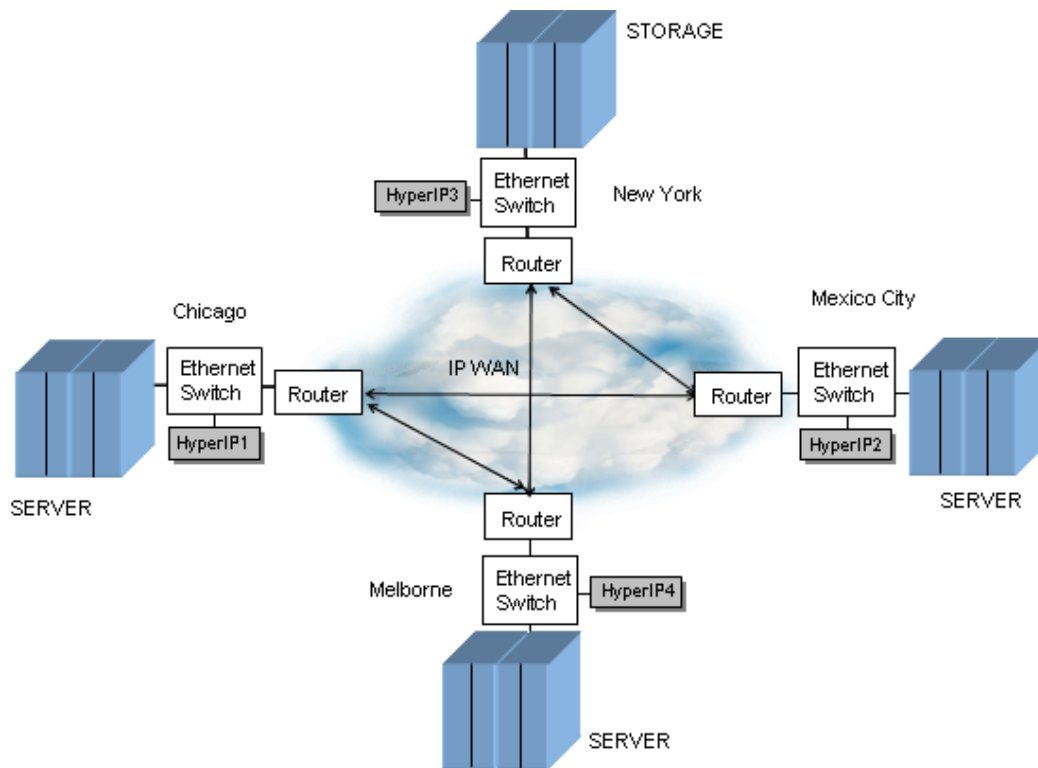
1. VRRP connectivity delays between each AHS pair following link up transition
  - a. Disconnecting and reconnecting the Ethernet cable on either HyperIP in the AHS pair causes a dual master situation since the link down/up event invokes the STP protocol on the switch rendering the link incapable of sending/receiving IP messages for about 30 seconds (varies by site configuration). The switch runs the STP initialization process to determine where this port exists in the spanning tree topology and whether this port is part of a physical loop.
  - b. Once STP initialization begins, the HyperIP unit in the BACKUP VRRP state is unable to receive advertisements from the master. This causes the Backup HyperIP unit to transition to the MASTER VRRP state.
  - c. Once STP initialization is finished, both HyperIP units of the AHS pair will detect the existence of two masters by each seeing the advertisements of the other. The dual master situation is resolved by an algorithm which recognizes the advertisement from the HyperIP with the higher IP Address as the one which should remain the master. The HyperIP unit with the lower IP Address transitions to the BACKUP VRRP state.



# Multiple Site (NxN) Configuration

Multiple sites may be configured (currently up to 10). Each site may be configured with a single HyperIP or an AHS dual-HyperIP. The HyperIP NxN Config web page allows the setup to be done with a few table entries. The page also facilitates copying an established configuration from one HyperIP to another with browser copy-paste commands.

Each site-to-site session can be independently configured to the requirements between those sites.



**Figure 6: NxN HyperIP Configuration**



# Product Features

## Statistics and Diagnostics

A HyperIP session is defined as a connection between two HyperIP nodes. HyperIP provides session-level statistics. Input/Output byte counts, message counts, and session establishment requests are maintained.

Diagnostic aids include the ability to trace the route to specified nodes, monitor various statistics and display status and state of the HyperIP connection. Due to the “tunneling” nature of the HyperIP, doing a “traceroute” through HyperIP (i.e., from one host through the HyperIP “tunnel” to another host) will not show any nodes in the “tunnel”. If troubleshooting the “tunnel” is required, the HyperIP Web Browser interface has a traceroute capability that will show the network nodes within the “tunnel”.

HyperIP maintains several operational logs that may be useful in diagnosing a configuration or operational problem. If your site utilizes a centralized syslog mechanism (e.g., monitor one or syslogd), HyperIP can be configured to send the logs to a remote syslog server.

Additionally, HyperIP provides graphs depicting traffic flow in/out for the previous hour, day, week, and month. These graphs also show compression and retransmissions between HyperIPs. Graphing is only available via the web browser interface.

## Idle Traffic Processing

HyperIP maintains contact with its peer utilizing idle-traffic messages. When user traffic is active between the HyperIP nodes, idle-traffic messages are not transmitted. If there is no user traffic activity, idle-traffic messages will be used to assure that the destination HyperIP is still available. If no response is detected from the destination HyperIP within the session time-out period, the path to that destination HyperIP is assumed to be inoperative and the connection is placed in recovery mode.

## HyperIP Configuration

Initial setup of IP address, netmask and gateway is performed via the Command Line Interface (CLI). Subsequent configuration and maintenance is done via a web browser to HyperIP. After configuration, the HyperIP runs without human intervention; when it powers up and is initialized, it automatically establishes connection with the configured remote HyperIP.

HyperIP can be configured to automatically save configuration data to a customer’s FTP server. When configured this way, HyperIP will FTP configuration data to the FTP server whenever configuration changes are made, providing an automatic backup of the configuration data in case of critical HyperIP failure.

## Multiple User Interfaces

An administrator may configure and/or monitor the HyperIP via a web browser such as Netscape or Internet Explorer, or via a telnet/SSH (or serial port on NetEx supplied appliance or console for VMware deployments) session to the Command Line Interface (CLI). Commands are available to manage the HyperIP, monitor statistics, and display network activity.

HyperIP supports an optional dedicated management interface that can be used strictly for management. Traffic on this interface will not be optimized and routing between the management and data interface will not be allowed.

## Efficient Bandwidth Management

HyperIP network protocol dynamically optimizes network performance, based on factors such as available bandwidth, distance, and workload on the network. Continuous feedback from the receiving side is used to adjust the rate at which data is sent from the sending side. This feature allows HyperIP to share network resources with other IP applications without taking priority.

Additionally, HyperIP can be configured to throttle the bandwidth based on time and day scheduling. This added feature allows a site policy to dictate when HyperIP rate is adjusted for the time applications run and require additional network resources or need to limit the use of the network resources.

## SNMP

SNMP is configured on the HyperIP node to collect MIB-II data for the network interfaces, as well as the HyperIP enterprise MIBs, which allow this data to be collected by an SNMP Monitor. Text files for the supported MIBs can be found on the distribution CD, from a link on the WEB browser interface (on the home page) and on NetEx's website at <http://www.netex.com>.

Additionally, when configured, HyperIP provides the ability to send SNMP traps for the following significant events:

- Product License Key expiration notice
- AHS role change (i.e. became active)
- HyperIP-to-HyperIP connection established
- HyperIP-to-HyperIP communication lost
- HyperIP-to-HyperIP communication restored
- HyperIP-to-HyperIP connection terminated
- HyperIP-to-HyperIP connection lost

*Note: Only one trap server can be set on HyperIP.*

## Data Compression

This feature utilizes a lossless adaptive technique that compresses data (assuming the data is compressible) in order to reduce the 'optimized link' bandwidth usage and increase the effective throughput.

By default the compression threshold is set to less than 80% of the original data; i.e., if the compressed data length is at least one byte less than the threshold size, it will continue to compress the data. If the compressed output length is greater than the threshold size, compression will not be performed for the subsequent data and a delay will be initiated before once again attempting compression. The wait period is logarithmic and is adjusted longer if the data continues to be uncompressible.

## Automatic Hot-Standby

The Automatic Hot-Standby (AHS) feature provides “appliance level” redundancy in the HyperIP configuration. In an AHS configuration, either or both sides of the HyperIP network may have an AHS pair deployed. With AHS deployed, HyperIP is not a single point of failure.

## Two Deployment Modes

HyperIP has two deployment possibilities: gateway mode and proxy IP address mode\*. Both modes can be configured with AHS. Gateway mode requires a static route (with a gateway) to be defined in the hosts which direct IP traffic (to be optimized) to HyperIP. (Gateway mode is available beginning with Release 1, and proxy IP address mode is available beginning with Release 5.) Proxy mode allows the HyperIPs to be deployed anywhere in a customer network without additional static routes to be added between subnets. The end user application then uses the proxy IP address (configured in HyperIP) instead of the real remote application IP address and the IP traffic will be optimized by the HyperIPs.

\*Note: *Not all applications allow proxy IP addressing, and may not work transparently.*

## NTP Compatible

The use of NTP protocol for HyperIP clock synchronization ensures that all log files between various HyperIPs are chronologically correct, as well as ensuring license expiration warnings are in sync with local site time. Various external, pre-defined NTP servers can be selected and/or private local NTP servers(s) can be utilized.

## Command Line Interface (CLI)

HyperIP CLI provides a secondary option for configuration, maintenance and monitoring. This section describes the CLI. Connecting HyperIP to an Ethernet infrastructure or a serial connection enables usage of the CLI to configure and control various operational aspects of HyperIP.

To use the CLI, the administrator either telnets/SSH to HyperIP (or connects a terminal to the serial port/or uses the console). At the login prompt, log in as *hipadmin*. The default password is *hipadmin*. ***(You should change the administrator password to a more secure password at installation time.)***



# Scalability Considerations

A single HyperIP may support up to over 8000 TCP connections from local applications. If a configuration requires more TCP connections, additional HyperIPs can be added to accommodate the additional connections.

HyperIP can be used to throttle traffic in 1K bits per second increments on a link from 1.5 Mb/s to 800Mb/s depending on the hardware model, assuming the Product License Key allows the setting. This feature allows a customer to limit specific traffic from over-subscribing the link. Performance is dependent on the incoming traffic from the local hosts, the available bandwidth on the link to the remote HyperIP, and the traffic to the remote host. Refer to the matrix in section HyperIP Appliance on page 75 for the model specific performance numbers.

With HyperIP running as a virtual machine under VMware's ESX or ESXi, the performance considerations are relative to the capacity of the physical hardware, the assignment of physical resources to the HyperIP VM, and the number of VMs on the physical hardware.

HyperIP contains utilities which will assist in identifying the total and available bandwidth between the local and remote HyperIPs. The utilities should be run without HyperIP optimizing traffic (or on the standby HyperIPs), since the bandwidth calculation algorithm requires dedicated resources to accurately measure packet times and delays. This analysis is a point in time analysis of the link between the HyperIPs. If required, this utility can be re-run at several different times during a day, week, and/or month for a complete depiction of the link usage.

To further "tune" HyperIP for optimum performance in your site, HyperIP provides a utility which can be run to evaluate "segsize". Segsize is a runtime parameter used by the HyperIP transport. The segsize is the amount of data which would be retransmitted if there is a lost packet. This utility should be run at installation time and especially if the link is experiencing high bit error rates.



# Security Considerations

## Physical Security for NetEx Provided Hardware Appliance

In order to aid in securing physical access, the Network Executive Software, Inc. (NetEx) appliance has a locking bezel on the front to prevent unauthorized powering-off and access to the removable devices and/or hard disk drives. The ability to alter the hardware (BIOS) settings is also disabled to minimize the possibility of altering the platform setup of the NetEx supplied appliance.

## System Security

The HyperIP is a custom product that utilizes some standard protocols and services. To ensure compliance and product integrity, Network Executive Software, Inc. continually monitors standards and user group activities to obtain early alerts regarding security vulnerabilities in any of the protocols or services that may impact HyperIP. If Network Executive Software, Inc. determines there is security vulnerability, notices will be sent to customer contacts as soon as any such vulnerability is identified.

## Security of User Data

By default, HyperIP uses UDP port 3919 for transmission of packets. This port number is configurable, and must be the same at both ends of the configuration. The intended deployment of HyperIP is in a secure, trusted environment and typically behind an existing firewall. Check with your firewall administrator to ensure that the HyperIP UDP port traffic will be allowed. HyperIP operation is not affected by firewalls, as long as the firewall does not block the HyperIP UDP port.

HyperIP is only designed to enhance IP application performance; there is no additional checking beyond the usual IP stack checks on the applications' IP packets before being transferred to the remote HyperIP. If the local and remote LANs are not mutually trusted, firewalls may be installed to perform additional security checks between the two LANs.

## Securing Management Access

The NetEx supplied HyperIP Appliance can be managed by the serial interface. For VMware deployments the HyperIP can be managed by the console. The preferred method of management is via the web browser interface. HyperIP optionally supports a dedicated management Ethernet interface for monitoring and maintenance. Although HyperIP may permit management traffic on both interfaces, it internally blocks traffic flow between the data and management Ethernet interfaces and does not optimize data on the management interface.

To minimize unauthorized access to HyperIP, HTTPS and SSH on the management Ethernet interface is the only access enabled when using the factory default settings. (HTTPS supports both SSL v3 and TLS v1.) **No services are enabled by default on the data interface.** Less secure services such as TELNET, HTTP, ping, and SNMP can be enabled on the management interface through the user interface if desired. The user interface can also be used to enable any of these services on the data Ethernet interface.

If the site requires total security of HyperIP, once configuration is complete, the appliance can be physically disconnected from the management network (and the serial connection).

The following is a list of steps the administrator may take to secure management access to the NetEx appliance. The items are listed in order of increasing security, from an open and trusted environment to one that prevents total management access to HyperIP:

1. Change the admin password (admin password is required to perform configuration changes)
2. Set an access password for web browser access (defaults to none)
3. Change SNMP community from 'public' to your site community
4. Disable TELNET access on the data interface (defaults to disabled)
5. Disable HTTP access on the data interface (defaults to disabled)
6. Disable ping access on the data interface (defaults to disabled)
7. Disable HTTPS access on the data interface (private browser access connection – defaults to disabled)
8. Disable SSH access on the data interface (private telnet connection – defaults to disabled)

--- When all the above steps are completed, the appliance's configuration can not be altered via the data interface (RECOMMENDED).

9. Disable TELNET access on the management interface (defaults to disabled)
10. Disable HTTP access on the management interface (defaults to disabled)
11. Disable ping access on the management interface (defaults to disabled)
12. Disable HTTPS access on the management interface (private browser access connection)
13. Disable SSH access on the management interface (private telnet connection)

--- When all the above are done, alterations can only be done from the serial interface/console. No one can alter the configuration from the Ethernet interface.

14. Disable SNMP to the data interface (defaults to disabled)

--- No one can view anything from the data interface - no SNMP monitoring on the data interface.

15. Disable SNMP to the management interface (defaults to disabled)

--- When all the above are done, no one can view anything from either Ethernet interfaces - no SNMP monitoring. The management interface could be disconnected as well.

16. Disconnect the serial interface (for NetEx supplied appliances only)

--- When all the above are done, HyperIP can only optimize the customer's IP traffic (no management access).

# HyperIP Command Line Interface

## Overview

This section describes the HyperIP command line interface (CLI) and the commands that are available to the HyperIP user or administrator. Commands may be executed once logged into HyperIP via Telnet, SSH, or when connected via the serial port.

## Features

The CLI facility offers command completion support through two methods.

- The <TAB> key will perform command completion.
- The <ENTER> key can be used to perform command completion **and** execution of that completed command if the entered characters identify a unique command.

The command completion feature is only available during a CLI session and is not available for commands issued through the web browser. (The CLI is not available via the web browser.)

The list of available commands may be displayed by typing “?”.

Help is available for all commands. Typing the command followed by a “?” will give the command syntax. A second “?” entered will give detailed help for the command.

## Restrictions for the CLI

The following restrictions and limitation exist for the CLI:

1. The special characters # ~ % ! \$ & < > ? \ ` ( ) | ; ‘ / “ and the backspace and space characters are not allowed for specifying the following CLI command fields:
  - Filenames
  - Passwords
  - SNMP community name
2. Some of the CLI commands contain a host path field which specifies how to connect with a remote host in order to receive or send a HyperIP type file. CLI commands use the following syntax to define the host path: `userid@machine:path`  
  
The userid, machine and path fields do not allow the following special characters ! # ~ % @ \$ & < > ? \ ` ( ) | ; ‘ / “ backspace and space characters.
3. The following CLI commands do not support command completion and execution because they incorporate passwords as part of command entry:
  - `receiveImageFTP`
  - `receiveImageFTPNonPassive`

The FTP server used to host files for retrieval by CLI commands that allow access to those files over the network must be running on an “open source” compatible FTP server (UNIX-, Linux-, Windows-based, etc.).

# Command Descriptions

Commands are listed in alphabetical order, with parameters also described. The format of the commands in this section is:

**commandname** <parm1> <parm2> <etc>

**NOTE:** *Help is available for all commands by typing the command followed by a “?”. The list of available commands may be displayed by typing “?”.*

Commands are logged in the system log, time stamped by user issuing the command. See the detailed description of these commands below.

The following table details the available CLI commands, including a description for each and syntax.

## CLI Command Summary

Command	Command Description/Syntax									
cfgAccessOff	Deny access to service. <b>cfgAccessOff</b> < <i>interface</i> > < <i>service</i> > <i>interface</i> (data mgmt) <i>service</i> service to block (http https ping snmp ssh telnet)									
cfgAccessOn	Allow access to service. <b>cfgAccessOn</b> < <i>interface</i> > < <i>service</i> > <i>interface</i> (data mgmt) <i>service</i> service to allow (http https ping snmp ssh telnet)									
cfgDefaultGateway	Configure the default gateway. <b>cfgDefaultGateway</b> < <i>ip_address</i> > <i>ip_address</i> IP Address of default gateway									
cfgGlobalParam	Configure a global parameter. <b>cfgGlobalParam</b> < <i>parameter</i> > < <i>value</i> > <table border="0"> <thead> <tr> <th><i>parameter</i></th> <th><i>description</i></th> <th><i>value</i></th> </tr> </thead> <tbody> <tr> <td>UDPPORT</td> <td>This is the UDP port number used for communication between HyperIP appliances.</td> <td>Any available port. (3919 - default)</td> </tr> <tr> <td>OKTODEC</td> <td>This parameter controls whether or not the transmitting rate will be decreased. You may want to turn this parameter off if you are running traffic on a static network (private link) in which there are periods of time with little traffic.</td> <td>0 (off) or 1 (on – default)</td> </tr> </tbody> </table>	<i>parameter</i>	<i>description</i>	<i>value</i>	UDPPORT	This is the UDP port number used for communication between HyperIP appliances.	Any available port. (3919 - default)	OKTODEC	This parameter controls whether or not the transmitting rate will be decreased. You may want to turn this parameter off if you are running traffic on a static network (private link) in which there are periods of time with little traffic.	0 (off) or 1 (on – default)
<i>parameter</i>	<i>description</i>	<i>value</i>								
UDPPORT	This is the UDP port number used for communication between HyperIP appliances.	Any available port. (3919 - default)								
OKTODEC	This parameter controls whether or not the transmitting rate will be decreased. You may want to turn this parameter off if you are running traffic on a static network (private link) in which there are periods of time with little traffic.	0 (off) or 1 (on – default)								
cfgIntercept	Enable, Disable or Delete an existing intercept. <b>cfgIntercept</b> < <i>action</i> > < <i>intercept-id</i> > <i>action</i> (delete enable disable) <i>intercept-id</i> intercept id									

Command	Command Description/Syntax
cfgInterface	<p>Configure the management or data interface's IP address, netmask, speed and MTU.</p> <p><b>cfgInterface</b> &lt;interface&gt; &lt;ip_address&gt; &lt;netmask&gt; &lt;speed&gt; &lt;mtu&gt;</p> <p><i>interface</i> (data mgmt)</p> <p><i>ip_address</i> IP address XX.XX.XX.XX</p> <p><i>netmask</i> netmask XX.XX.XX.XX</p> <p><i>speed</i> (auto half10 full10 half100 full100 full1000)</p> <p><i>mtu</i> maximum transmission unit (400-16384)</p>
cfgInterfaceDown	<p>Bring down the data or management interface.</p> <p><b>cfgInterfaceDown</b> &lt;interface&gt;</p> <p><i>interface</i> (data mgmt)</p>
cfgInterfaceUp	<p>Bring up the data or management interface.</p> <p><b>cfgInterfaceUP</b> &lt;interface&gt;</p> <p><i>interface</i> (data mgmt)</p>
cfgProxy	<p>Enable, Disable or Delete an existing proxy.</p> <p><b>cfgProxy</b> &lt;action&gt; &lt;proxy-id&gt;</p> <p><i>action</i> (delete enable disable)</p> <p><i>proxy-id</i> proxy id</p>
cfgSerialPort	<p>Configure the serial port. (NetEx supplied hardware appliances only)</p> <p><b>cfgSerialPort</b> &lt;speed&gt; &lt;config&gt;</p> <p><i>speed</i> (9600 19200 57600 115200)</p> <p><i>config</i> (off dir ans)</p> <p><b>off</b> – no serial port connection</p> <p><b>dir</b> – direct connect cable</p> <p><b>ans</b> – modem connected for incoming connection</p>
cleanupImage	<p>Delete/Cleanup a product image.</p> <p><b>cleanupImage</b> &lt;fname&gt;</p> <p><i>fname</i> file name of image to delete</p>
deleteAllIntercepts	Delete ALL configured intercepts.
deleteAllProxies	Delete ALL configured proxies.
deleteAllTuning	Delete ALL site-specific tuning parameters.
exit	Exit this CLI session

<b>Command</b>	<b>Command Description/Syntax</b>
installImage	Restore a product image to the alternate partition from disk. <b>installImage &lt;fname&gt;</b> <i>fname</i> file name of image to restore to the non-running partition.
installImageCD	Restore a product image to the alternate (non-running) partition from CD/DVD
legacyDialog	Run the legacy menus (will be deprecated in future releases)
listConfigs	Show the current saved configurations on the hard drive in the running partition.
listImages	Show a list of product images on the hard drive.
newIntercept	Add a new intercept to HyperIP. <b>newIntercept &lt;intercept-id&gt; &lt;remote-site-name&gt; &lt;sourceIP&gt; &lt;source-Port&gt; &lt;destinationIP&gt; &lt;destinationPort&gt; &lt;protocol&gt; &lt;forwardAtLimit&gt;</b> <i>intercept-id</i> unique intercept ID <i>remote-site-name</i> 2 name of remote site to intercept traffic for <i>sourceIP</i> origin IP address <i>sourcePort</i> origin port(s) <i>destinationIP</i> destination IP address <i>destinationPort</i> destination port(s) <i>protocol</i> ICMP,UDP,TCP (i u t iu it ut iut) <i>forwardAtLimit</i> (yes no)

Command	Command Description/Syntax
newProxy	<p>Add a new proxy to HyperIP.</p> <p><b>newProxy</b> &lt;<i>proxy-id</i>&gt; &lt;<i>remote-site-name</i>&gt; &lt;<i>proxyIP</i>&gt; &lt;<i>proxyPort</i>&gt; &lt;<i>destinationIP</i>&gt; &lt;<i>protocol</i>&gt;</p> <p><i>proxy-id</i>                      unique proxy ID</p> <p><i>remote-site-name</i>            remote site name</p> <p><i>proxyIP</i>                        proxy IP address</p> <p><i>proxyPort</i>                    proxy port(s)</p> <p><i>destinationIP</i>                destination IP address</p> <p><i>protocol</i>                      ICMP,UDP,TCP [i u t iu it ut iut]</p>
quit	Exit this CLI session
reboot	Reboot the HyperIP
receiveConfigHttp	<p>Receive a configuration file via HTTP.</p> <p><b>receiveConfigHttp</b> &lt;<i>syst</i>&gt; &lt;<i>path</i>&gt; &lt;<i>fname</i>&gt;</p> <p><i>syst</i>                            hostname with or without domain extension, or IP address</p> <p><i>path</i>                            path to configuration file</p> <p><i>fname</i>                          name of configuration file</p>
receiveConfigHttps	<p>Receive a configuration file via HTTPS.</p> <p><b>receiveConfigHttps</b> &lt;<i>syst</i>&gt; &lt;<i>path</i>&gt; &lt;<i>fname</i>&gt;</p> <p><i>syst</i>                            hostname with or without domain extension, or IP address</p> <p><i>path</i>                            path to configuration file</p> <p><i>fname</i>                          name of configuration file</p>
receiveImageFtp	<p>Receive a product image via FTP</p> <p><b>receiveImageFtp</b> &lt;<i>uid</i>&gt; &lt;<i>syst</i>&gt; &lt;<i>path</i>&gt; &lt;<i>fname</i>&gt; &lt;<i>pw</i>&gt;</p> <p><i>uid</i>                              userid for FTP</p> <p><i>syst</i>                            host name with or without domain extension, or IP address</p> <p><i>path</i>                            path to image file</p> <p><i>fname</i>                          file name of image</p> <p><i>pw</i>                                password on remote host</p>

<b>Command</b>	<b>Command Description/Syntax</b>
receiveImageFtpNonPassive	<p>Receive a product image via FTP – nonpassive</p> <p><b>receiveImageFtpNonPassive</b> &lt;uid&gt; &lt;syst&gt; &lt;path&gt; &lt;fname&gt; &lt;pw&gt;</p> <p><i>uid</i>               userid for FTP</p> <p><i>syst</i>               host name with or without domain extension, or IP address</p> <p><i>path</i>               path to image file</p> <p><i>fname</i>             file name of image</p> <p><i>pw</i>                 password on remote host</p>
receiveImageHttp	<p>Receive a product image via HTTP</p> <p><b>receiveImageHttp</b> &lt;syst&gt; &lt;path&gt; &lt;fname&gt;</p> <p><i>syst</i>               host name with or without domain extension, or IP address</p> <p><i>path</i>               path to image file</p> <p><i>fname</i>             file name of image</p>
receiveImageHttps	<p>Receive a product image via HTTPS</p> <p><b>receiveImageHttps</b> &lt;syst&gt; &lt;path&gt; &lt;fname&gt;</p> <p><i>syst</i>               host name with or without domain extension, or IP address</p> <p><i>path</i>               path to image file</p> <p><i>fname</i>             file name of image</p>
receiveUpdateHttp	<p>Receive an update file via HTTP.</p> <p><b>receiveUpdateHttp</b> &lt;syst&gt; &lt;path&gt; &lt;fname&gt;</p> <p><i>syst</i>               hostname with or without domain extension, or IP address</p> <p><i>path</i>               path to update file</p> <p><i>fname</i>             name of update file</p>
receiveUpdateHttps	<p>Receive an update file via HTTPS.</p> <p><b>receiveUpdateHttps</b> &lt;syst&gt; &lt;path&gt; &lt;fname&gt;</p> <p><i>syst</i>               hostname with or without domain extension, or IP address</p> <p><i>path</i>               path to update file</p> <p><i>fname</i>             name of update file</p>
remoteCLI	<p>Connect to another HyperIP</p> <p><b>remoteCli</b> &lt;uid&gt; &lt;name&gt;</p> <p><i>uid</i>                userid</p> <p><i>name</i>             hostName.localDomain</p>
restartForce	Restart HyperIP immediately.

<b>Command</b>	<b>Command Description/Syntax</b>
restartManagement	Restart management services immediately.
restartNetwork	Restart network interfaces immediately.
saveConfig	Save configuration to disk <b>saveConfig [fname]</b> <i>fname</i> file name to save the configuration in
serialnumber	Show serial number.
setBootAltTemp	Configure for the alternate partition to boot next with a specific configuration. Once it has booted one time it must be made permanent for subsequent boots ( <i>setBootCurrPerm</i> ). This is typically used following a install of a new version of HyperIP software. <b>setBootAltTemp [fname]</b> <i>fname</i> file name of the configuration file to use with that boot.
setBootCurrPerm	Configure for the current partition permanently. This is typically used after verifying a new version of HyperIP software.
setConnLimits	Set connection limits <b>setConnLimits &lt;tcpLimit&gt; &lt;udpLimit&gt; &lt;aggLimit&gt;</b> <i>tcpLimit</i> TCP connection limit <i>udpLimit</i> UDP connection limit <i>aggLimit</i> Aggregate connection limit. The absolute maximum number of connections supported (UDP + TCP) is 8192. A value of zero disables connection limit checking.
showBoot	Show current System boot options
showConfig	Display the current HyperIP configuration statements
showConnLimits	Show connection limits (see “setConnLimits”)
showHipStatus	Display HyperIP status.
showIntercepts	Display all configured intercepts.
showInterfaces	Display active interface configuration, noting pending changes.
showProxies	Display all configured proxies.
showRestarts	Display pending restarts.
showRoutes	Display routing table.

Command	Command Description/Syntax
showSerialPort	Show current setup of the serial port
showSiteParms	Show the current tuning parameters for sessions to remote site <b>showSiteParms</b> <siteName> <i>siteName</i> name of site to see the tuning parameters for
showVersion	Display HyperIP product version information.
siteAdd	Add a site definition <b>siteAdd</b> <id> <role> <siteid> <sitename> <primaryIP> <segsz> <maxrate> <initstate> <i>id</i> site number of the local site (this HyperIP) <i>role</i> local AHS role (noAHS   primary   secondary) <i>siteid</i> user-selectable unique number used for internal identifiers (must be consistent for each site across HyperIPs) <i>sitename</i> user-selectable unique name used for internal identifiers (must be consistent for each sites across HyperIPs) <i>primaryIP</i> the IP address for HyperIP being added (primary for AHS) <i>segsz</i> maximum bytes sent from HyperIP to IP per write to this site (<64KB) <i>maxrate</i> maximum transmit rate in megabits-per-sec for sending to this site (can be limited by rate schedule) <i>initstat</i> initial state (halt, start)

Command	Command Description/Syntax
siteAddAHS	<p>Add an AHS site definition</p> <p><b>siteAddAHS</b> &lt;<i>id</i>&gt; &lt;<i>role</i>&gt; &lt;<i>siteid</i>&gt; &lt;<i>sitename</i>&gt; &lt;<i>primaryIP</i>&gt; &lt;<i>virtualIP</i>&gt; &lt;<i>virtualID</i>&gt; &lt;<i>secondIP</i>&gt; &lt;<i>segsz</i>&gt; &lt;<i>maxrate</i>&gt; &lt;<i>initstate</i>&gt;</p> <p><i>id</i> site number of the local site (this HyperIP)</p> <p><i>role</i> local AHS role (noAHS   primary   secondary)</p> <p><i>siteid</i> user-selectable unique number used for internal identifiers (must be consistent for sites across HyperIPs)</p> <p><i>sitename</i> user-selectable unique name used for internal identifiers (must be consistent for sites across HyperIPs)</p> <p><i>primaryIP</i> the IP address for HyperIP being added (primary for AHS) (may be this one)</p> <p><i>virtualIP</i> the address used by servers as gateway addresses across the HyperIP network. The real &amp; virtual HyperIP addresses on each side of the network must be in the same subnet</p> <p><i>virtualID</i> VRRP unique id for AHS communication (1-255)</p> <p><i>secondIP</i> the IP address of the secondary AHS HyperIP (may be this one)</p> <p><i>segsz</i> maximum bytes sent from HyperIP to IP per write to this site (&lt;64KB)</p> <p><i>maxrate</i> maximum transmit rate in megabits-per-sec for sending to this site (can be limited by rate schedule)</p> <p><i>initstat</i> initial state (halt, start)</p>
siteDelete	<p>Delete site definition(s)</p> <p><b>siteDelete</b> &lt;<i>siteid</i>&gt; &lt;<i>newrole</i>&gt; &lt;<i>delid</i>&gt;</p> <p><i>siteid</i> site number of the local site</p> <p><i>newrole</i> Local AHS role ( noAHS   primary   secondary)</p> <p><i>delid</i> number of the site being deleted</p>
siteDeleteAll	Delete ALL site & related definition(s)
siteHalt	<p>Halt a remote site</p> <p><b>siteHalt</b> &lt;<i>name</i>&gt;</p> <p><i>name</i> remote site name to halt</p>
siteHaltAll	Halt all remote sites.

Command	Command Description/Syntax
siteStart	Start a remote site <b>siteStart</b> <name> <i>name</i> remote site name to start
siteStartAll	Start all remote sites.
siteTuneParms	Set tuning parameters for a remote site <b>siteTuneParms</b> <sitename> <maxmtowait> <minbtosend> <compalg> <compadapt> <compapercnt> <userexmitq> <rexmwlks> <rcvdataqhb> <rcvdataqlb> <bufolim> <recvgapq> <i>sitename</i> name of site for these session tuning parameters <i>maxmtowait</i> maximum milliseconds to wait before sending data, 0-9999 <i>minbtosend</i> minimum bytes to send when using maxmtowait, 0-65400 <i>compalg</i> compression algorithm to use: <b>0</b> implies “none” or no compression <b>1</b> implies “LZO” or compression on <i>compadapt</i> use adaptive compression: <b>0</b> implies “no” <b>1</b> implies “yes” <i>compapercnt</i> compress data only if compressed data size will be <compapercnt>% less than the original data size. Only used when <i>compadapt</i> is 1. <i>userexmitq</i> use a retransmit queue to delay before retransmitting: <b>0</b> implies “no” <b>1</b> implies “yes” <i>rexmwlks</i> retransmit queue depth - # of segments to wait when using <i>userexmitq</i> <i>rcvdataqhb</i> # of bytes on local receive data queue before HyperIP will start discarding <i>rcvdataqlb</i> # of bytes on local receive data queue under which data is accepted after discarding <i>bufolim</i> maximum number of write segments allowed to be in progress <i>recvgapq</i> store packets received out of order - 0:no 1:yes

Command	Command Description/Syntax
siteTuneReset	Reset tuning parameters for remote site to default values <b>siteTuneReset</b> < <i>sitename</i> > <i>sitename</i> name of site for these session tuning parameters
vCenterConfig	Configure a VMware Virtual Center server location and user-name/password for plugin registration. <b>vCenterConfig</b> < <i>server</i> > < <i>username</i> > < <i>password</i> > <i>server</i> Virtual Center hostname or IP address <i>username</i> Virtual Center user <i>password</i> Virtual Center password
vCenterRegister	Register HyperIP plugin with configured VMware Virtual Center.

# Web Browser User Interface

The web browser UIF is used to configure and monitor various operational aspects of HyperIP.

In general, the frame on the left-side of the page is where input is done and actions are performed. The results and status is usually found in the right-side frame.

## Browser Considerations

The browser can be hosted on any system, as long as that system has network connectivity to HyperIP. The web browser interface has been verified with the following browsers:

- IE 8.0
- Firefox 3.6

Set the destination URL/Address in the browser to the IP Address/Hostname of the HyperIP that is to be configured or monitored. When the browser first connects to HyperIP, the HyperIP home page is displayed.

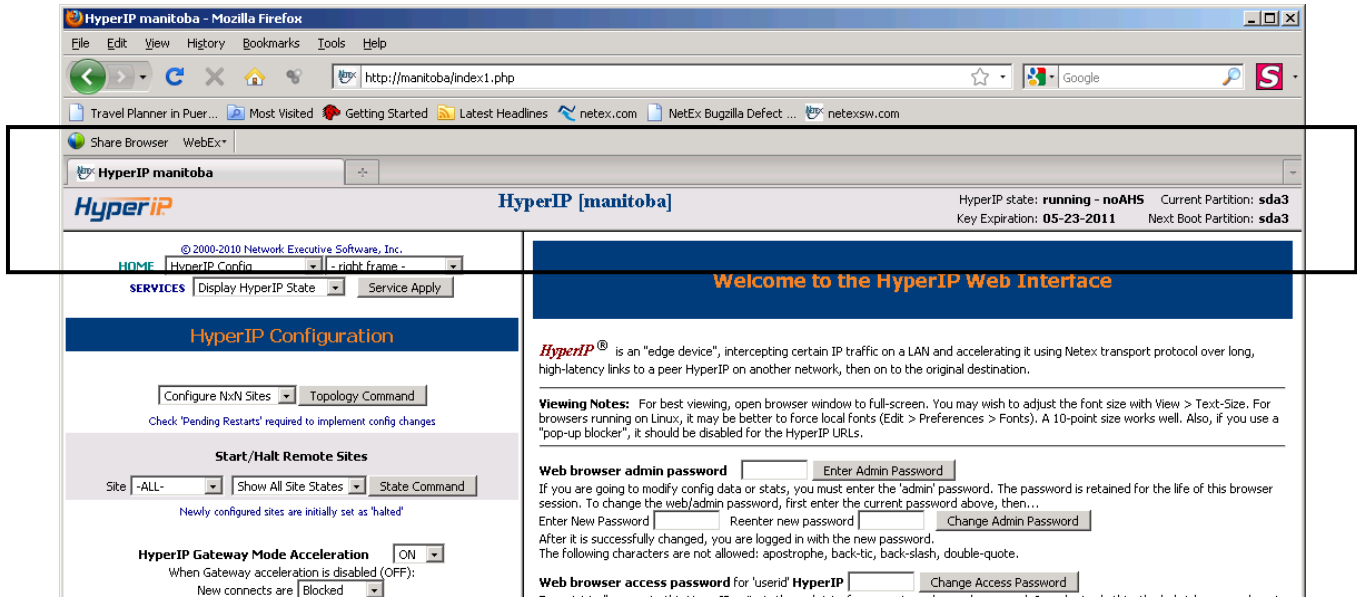
*Note: The default access rules will only allow requests sent via HTTPS (example: <https://10.10.2.2>) on the management port.*

## Home Page

The right frame of the home page allows entry of a password. When the browser session is used to modify configuration data, the HyperIP password must be entered in the password area on the screen. The userid and default password are “hipadmin”. To enter the password, type the password in the display box (it will not be visible), and then click <**Enter Password**>. The left frame of the display will indicate success or failure of the password submission.

## The Status Bar

Across the top of all the pages is a Status Bar. Important status information is maintained in this frame. This information is updated every 60 seconds. The following figures describe the status frame.



**Figure 7: Web Browser Page Status Bar Screen Capture**

Status Field	Description
HyperIP[hostname]	The Local IP Hostname which is configured on the System Config web page. If the hostname is changed, a reboot is required before it will show up in the status frame.
HyperIP State	<p>Describes both the operational state and the state of the AHS. The operational state will be <b>“running”</b> when HyperIP is capable of optimizing traffic. If the state is <b>“down”</b> then HyperIP is not capable of optimizing traffic (i.e. the license key has not been installed or is expired or otherwise invalid).</p> <p>The AHS state describes what state and role, if any, this HyperIP is in, with respect to AHS. <b>“NoAHS”</b> means this HyperIP is not configured for AHS.</p> <p>For an AHS configuration, <b>“Master”</b> or <b>“Backup”</b> is the AHS operational state for this HyperIP and <b>“Active”</b> or <b>“Standby”</b> is its current AHS role. See the <b>“Hot Standby Configuration”</b> section above for more about AHS.</p>
Key Expiration	If a License Key has been installed, the date (MM-DD-YYY) when the license key expires is shown.
Current Partition	HyperIP provides two software systems (of which only one can be operational at any one point in time). These two systems reside on the hard disk in their own partitions ( <b>sda3</b> and <b>sda4</b> ) on the hard disk. This allows an administrator to load a new version of software in the other partition without disturbing the currently running software version.
Next Boot Partition	<p>When the <i>Current Partition</i> is the same as the <i>Next Boot</i> partition, it has been marked permanent and will continue to be the version of software that will be operational on subsequent boots or power on resets (PORs) of this HyperIP.</p> <p>If the Current Partition is different than the Next Boot partition the Current Partition will only be operational until a POR or boot. (This is typical after downloading and booting a new version of the software, but before it is verified and made per-</p>

Status Field	Description
	manent.) Use the Display Product Information command found on the Maintenance webpage to see the version of software on each partition. This command is documented on page 56.

Figure 8: Web Browser Page Status Bar Description

## The “–left frame–” Menu

After the password is entered correctly, use the navigation links at the top of the left frame (in the drop down menu) to go to the various pages. The “–left frame–” menu controls access to the left-side panels:

- The **HOME & Install Commands** links go to the **HyperIP Installation** page (initial screen).
- The **System Config** link goes to the **HyperIP System Configuration** page.
- The **HyperIP Config** link goes to the **HyperIP Configuration Commands** page.
- The **Advanced Config** link goes to the **HyperIP Advanced Configuration Commands** page.
- The **Maintenance Commands** link goes to the **HyperIP Maintenance Commands** page.
- The **Diagnostic Commands** link goes to the **HyperIP Diagnostic Commands** page.
- The **File Upload/Downloads** link goes to the **HyperIP Download/Upload** page.

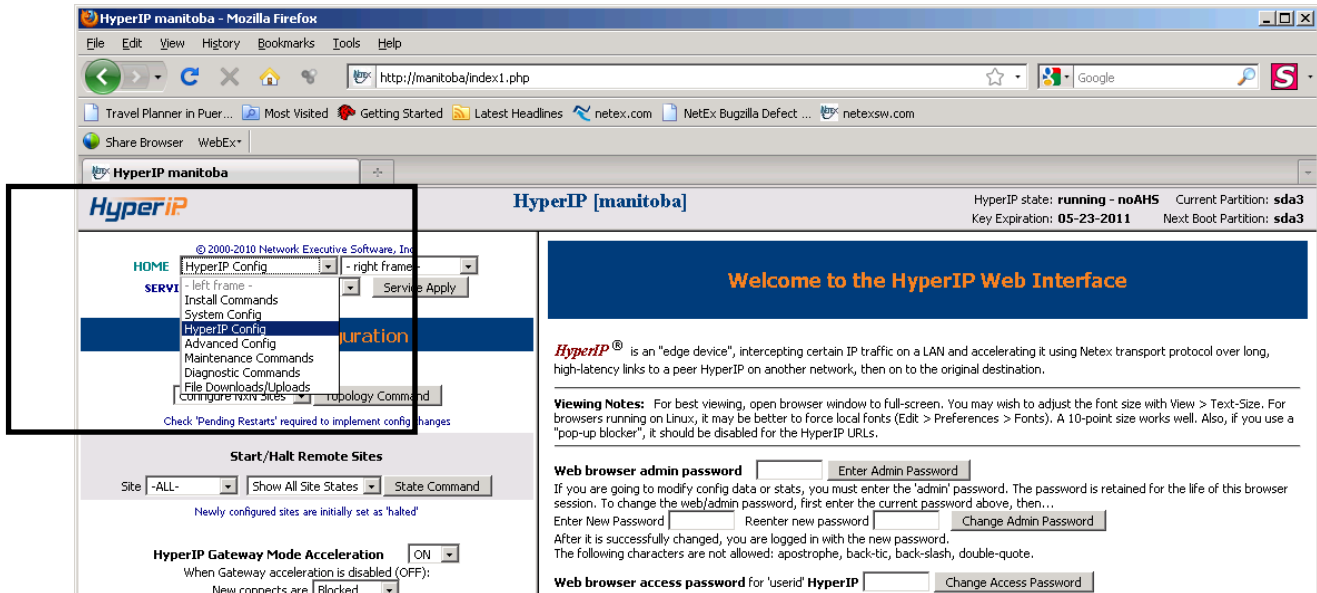


Figure 9: Web Browser Page “–left frame–” Menu

## The “–right frame–” Menu

The “–right frame–” menu controls access to the right-side panels:

- The **Bandwidth Schedule** link goes to the **Bandwidth Schedule** setup page.
- The **Proxies & Intercepts** link goes to the **Proxies and Intercepts** setup page.
- The **NxN Configuration** link goes to the **Topology page for HyperIP Site Configuration** page.
- The **HELP** links are used to obtain ‘help’ information for the other pages.

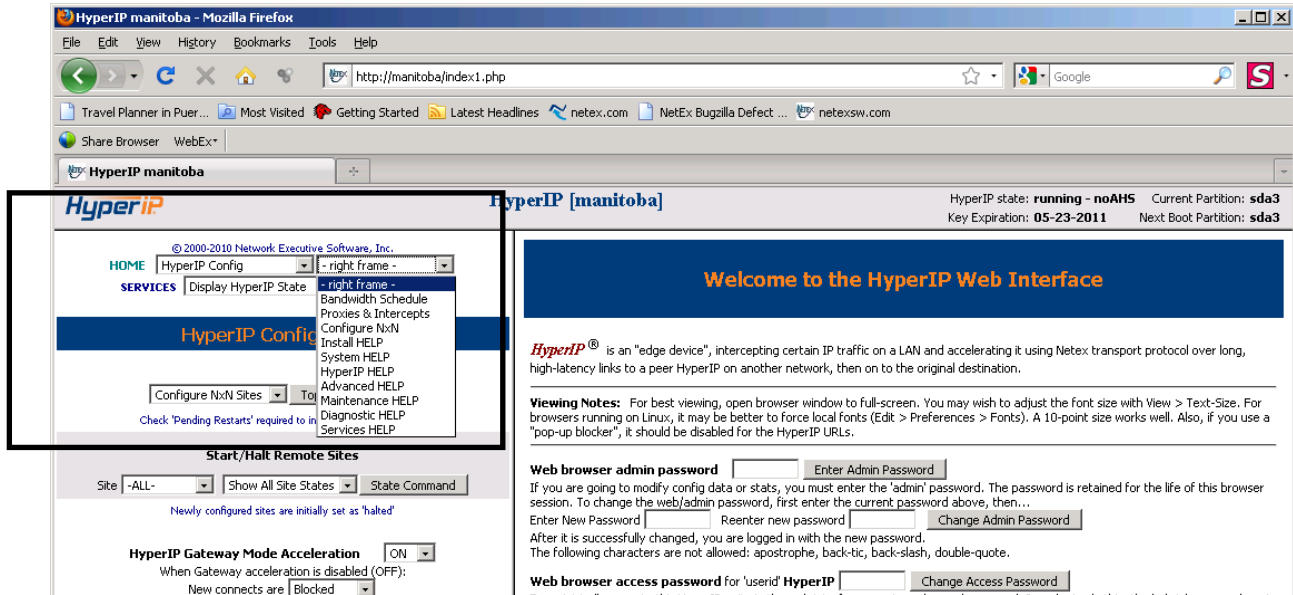


Figure 10: Web Browser Page “–right frame–” Menu

## The “HyperIP Services” Menu

This menu is used to issue commands that will start, stop, restart, or display the status of the HyperIP service, and reboot or halt the operating system. To invoke, select the desired command from the drop down menu and click <*Service Apply*>. The drop down menu includes:

- **Display HyperIP State** displays useful HyperIP monitoring information (in the frame at the right).  
*Note – if the connection between the “local” and “remote” HyperIPs is not functional, this command may require a long period of time to complete.*
- **Restart Mgmt** will perform a ‘stop’ and then a ‘start’ of the HyperIP software related to the management services (i.e. HTTP, SNMP, etc.). This will only affect the management interface.
- **Restart Force** sequentially does a ‘stop’ then a ‘start’ of HyperIP software (except the base operating system). This will cause a ‘soft’ restart of all the software and will affect both the data and the management interfaces.
- **Reboot** is used if a **full** reboot of the HyperIP operating system is needed (this takes 2-4 minutes). This will cause a ‘stop’ and then a ‘start’ of the HyperIP software as well as the base operating system.
- **Shutdown** is used when the system needs to be powered off.
- **Show Pending Restarts** will show what if any action is required to fully implement the configuration changes that have been performed (and are pending).

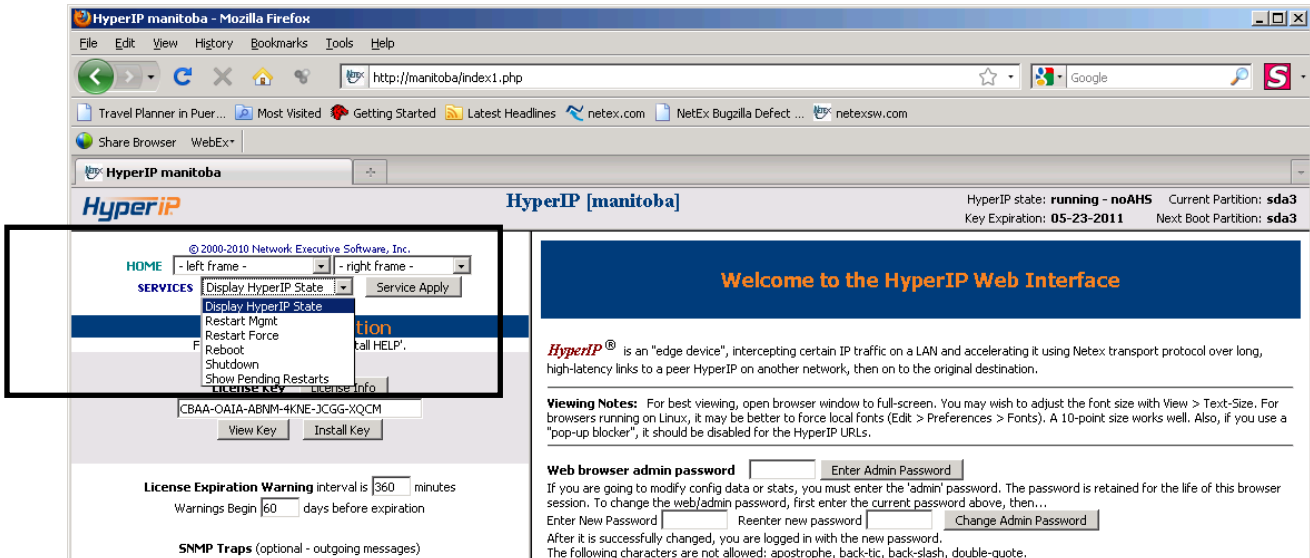


Figure 11: Web Browser Page “HyperIP Services Menu

# HyperIP Web Browser Pages

## HyperIP HOME Page

This screen is used to enter the password, set up license information, and has links to the NetEx website for the latest documentation.

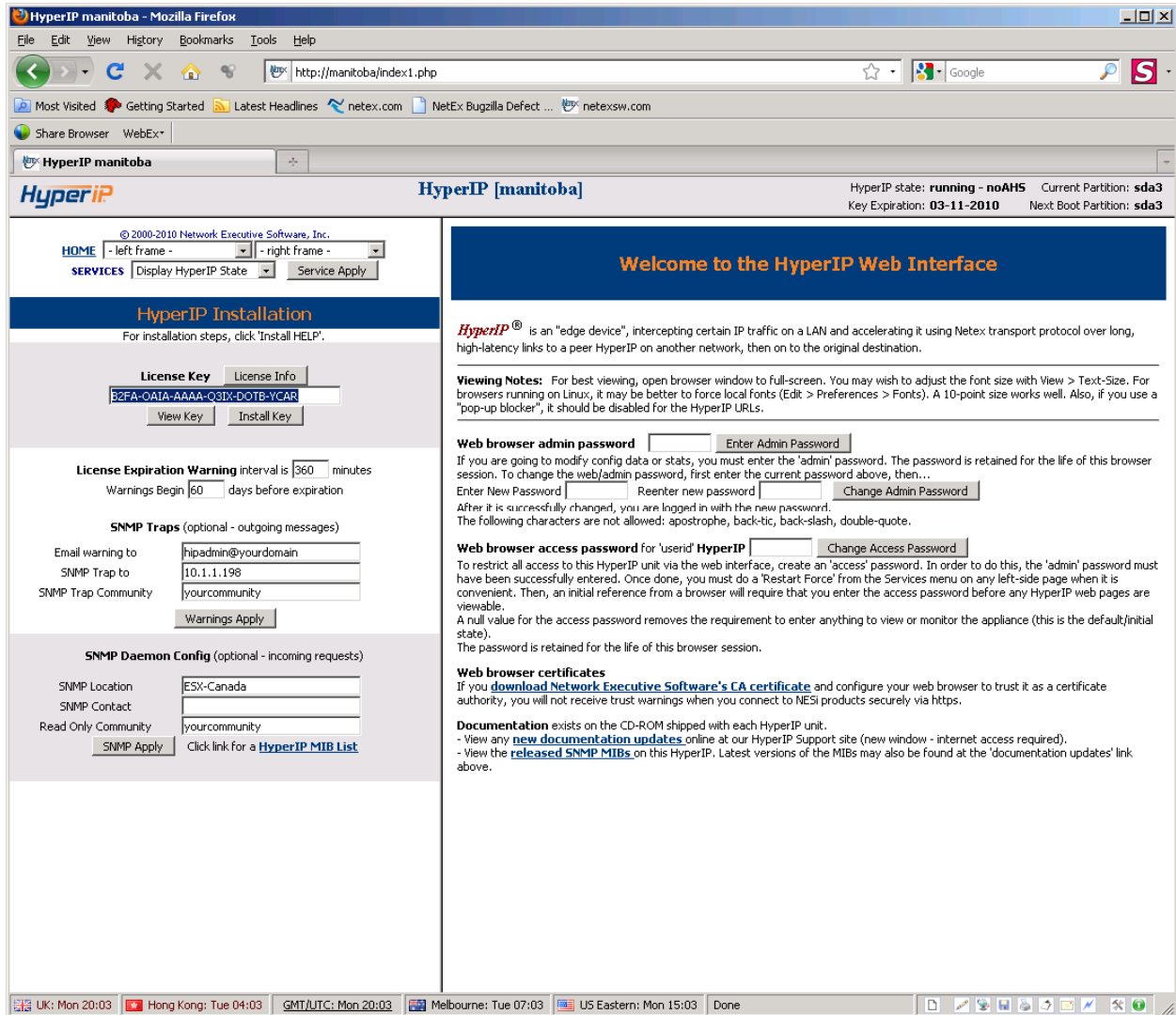


Figure 12: Web Browser Home Page

## Admin Password

HyperIP's web password is stored on the HyperIP and is validated on the home page. The password is required to perform any modifications to the HyperIP configuration. The password is saved when the configuration is saved, and will be restored when the configuration is restored. The password of user '*hipadmin*', is initially set to '*hipadmin*', To change the password, type in the new admin password twice (will not be visible) and click **<Change Admin Password>**.

## Web Browser Access Password

The HyperIP administrator can optionally set up an access password to prevent unauthorized access to HyperIP. When the access password is set, web browser access to the HyperIP can only be gained if the proper password is entered. The access password can only be set/changed by the HyperIP administrator after the 'HyperIP' user password has been validated.

## Web Browser Certificates

The HyperIP Web Interface may be accessed more securely by using HTTPS protocol. Each HyperIP provides a link to the NetEx CA (certificate authority) certificate that digitally signs the site certificates that web browsers automatically obtain from the HyperIP when connecting using HTTPS. If you wish to avoid trust warnings from your web browser, you may download the NetEx CA certificate and configure your web browser to trust it as a certificate authority. To verify that the NetEx CA certificate is authentic, view the certificate and confirm the following information:

Issued To: NetEx Certificate Authority  
\*SHA1 Fingerprint: BE04 BE4B 123A 1164 4678 32AE 298D E04E 67C1 4045

The NetEx CA certificate may also be downloaded online from

[http://www.netex.com/netex\\_ca.crt](http://www.netex.com/netex_ca.crt)

\*Ignore case, colons, and whitespace in this field. Also, some browsers may refer to this as the "Thumbprint".

## View Latest Documentation

At the bottom of the right frame is a **bold** web link to the NetEx support web site where the latest HyperIP documentation is available for viewing and/or download. Clicking the link will bring you to a menu of available documents. External web access from your browser to the Internet is required for this link to work.

By clicking on the link to the **bold** web link, *released SNMP MIBs*, you can view a local copy of the enterprise MIBs supported on HyperIP.

## Install Commands

### License Key

This section of the page is used to install (or re-install) the Product License Key and set the expiration warning parameters. HyperIP software will not initialize until a valid license key has been installed and verified during startup (system reboot or HyperIP service restart.) The Product License Key has an associated expiration date; therefore a new key must be obtained and installed before the prior key's expiration in order to prevent interruptions in the HyperIP's operation.

If a key has already been installed, clicking *<License Info>* will display the HyperIP license information as well as the internal serial number. When a new key is received, copy/paste it into the box provided and click *<View Key>*. This will display the capabilities that are encoded within the key. If these are the correct capabilities, then click *<Install Key>*. If HyperIP is running, the key is immediately read, validated, and activated; otherwise, it will be processed when HyperIP is restarted (Restart Force or Reboot). Then *<License Info>* will show the new license information for HyperIP per the installed key; i.e. compression, bandwidth, etc.

## Warnings for License Expiration and Automatic Hot-Standby (AHS) Role Changes

HyperIP can be configured to issue warning notifications of Product License Key expiration and AHS role changes as well as various HyperIP communication state notices.

Two options exist to warn the administrator that the key expiration date is nearing or when an AHS causes HyperIP to become 'Active':

- Email - To set up an email to notify of key expiration, simply type in the email address (mailid@domain) to which notifications are to be sent
- SNMP - Set the SNMP parameters (IP address to send trap to, and the community name)

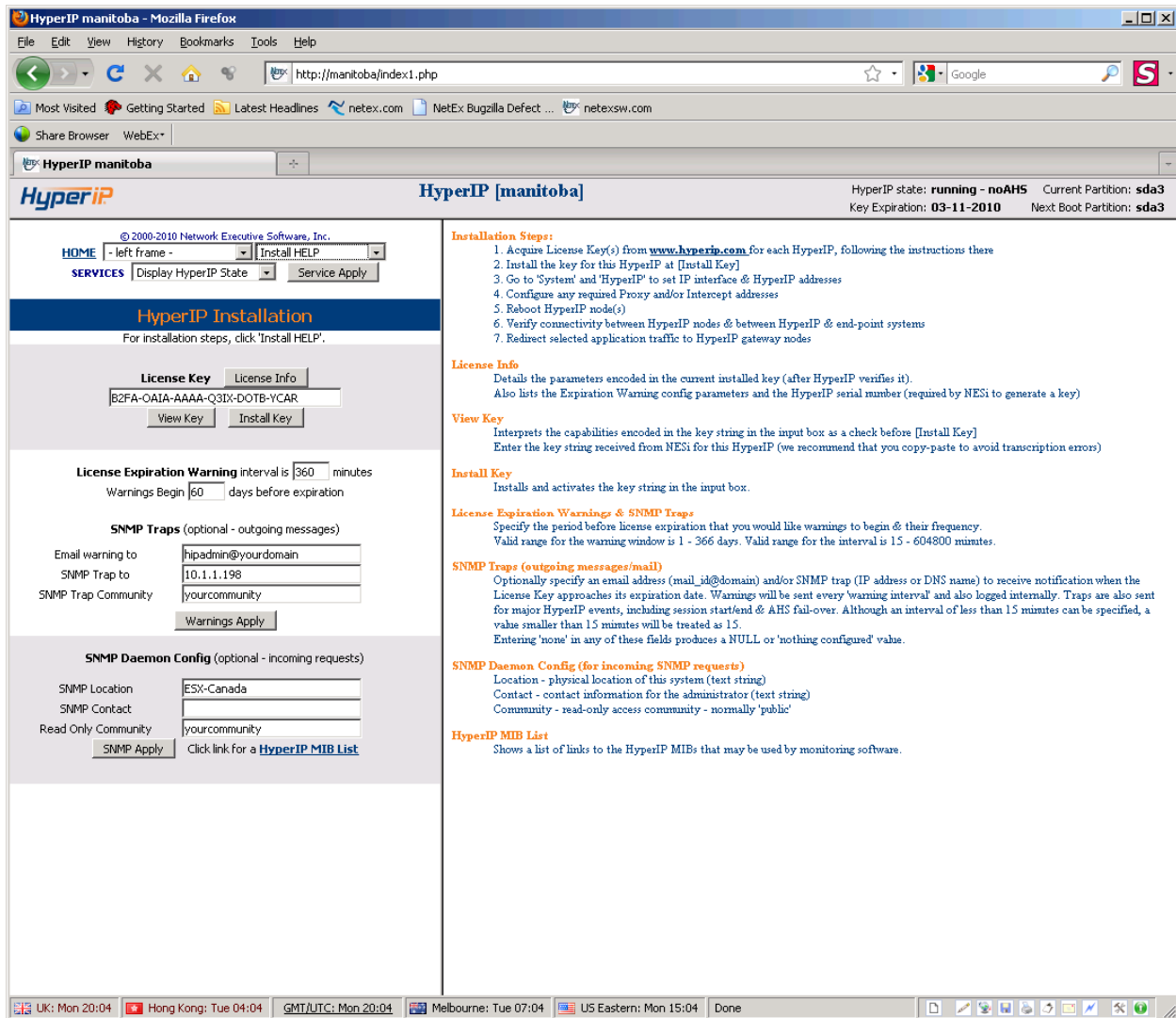
To specify the period before license expiration that you would like warnings to begin and their frequency, enter the number of days in the box provided. Enter the desired frequency (in minutes) at which warnings will be issued. Warnings will be sent every 'warning interval' and also logged internally. Entering 'none' in any of these fields produces a NULL or 'nothing configured' value.

Be sure to click <**Warnings Config**> once the parameters are set.

Note: *The email and SNMP address configured here are also used for traps related to Automatic Hot-Standby (AHS) notices; i.e. AHS switching between Active & Standby HyperIP and various HyperIP communication state notices.*

## SNMP Configuration

This area is used to configure SNMP with information regarding the physical location of this HyperIP, contact information for the administrator, and SNMP read only community (default 'public'). Once the fields have been entered, click <**SNMP Config**> to apply.



**Figure 13: Web Browser Install Page and Install Help**

The following is the information provided in the “Install HELP” display:

### Installation Steps:

1. Obtain the HyperIP serial number (or fingerprint). This is required to request your key.
2. Acquire License Key(s) for evaluations, purchases and renewals go to <http://www.netex.com/request-a-key>.
3. Install the key for this HyperIP at [Install Key]
4. Go to 'System Config' page to set IP interface addresses
5. Configure site(s) on the 'Configure NxN' page.
6. Configure required Proxy and/or Intercept addresses
7. Start site(s)
8. Reboot HyperIP node(s)
9. Verify connectivity between HyperIP nodes & between HyperIP & end-point systems.
10. Redirect selected application traffic to HyperIP gateway nodes if using gateway.

### License Info:

Details the parameters encoded in the current installed key (after HyperIP verifies it).

Also lists the Expiration Warning config parameters and the HyperIP serial number (required by NetEx to generate a key)

### View Key:

Enter the key string received from NetEx for this HyperIP (we recommend that you copy-paste to avoid transcription errors)

Interprets the capabilities encoded in the key string in the input box as a check before [Install Key]

### Install Key

Installs and activates the key string in the input box.

### License Expiration Warnings & SNMP Traps

Specify the period before license expiration that you would like warnings to begin & their frequency.

Optionally specify an email address (mailid@domain) and/or SNMP trap (IP address or DNS name) to receive notification when the License Key approaches its expiration date. Warnings will be sent every 'warning interval' and also logged internally. Traps are also sent for major HyperIP events, including session start/end & AHS fail-over.

Entering 'none' in any of these fields produces a NULL or 'nothing configured' value

### SNMP Daemon Config (for incoming SNMP requests)

Location - physical location of this system (text string)

Contact - contact information for the administrator (text string)

Community - read-only access community - normally 'public'

### HyperIP MIB List

Shows a list of links to the HyperIP MIBs that may be used by monitoring software.

### HyperIP Services

Perform actions to stop, start, or restart the HyperIP processes, restart the network interfaces, reboot or halt the system.

## HyperIP System Config Page

The following figure is an example of the display seen when selecting the System Config in the *<left frame>* drop down menu in the top left frame. The right frame in the following display is the result of selecting the System Help from the *<right frame>* drop down. System configuration is typically performed only at installation time, but may also be required if the network is reconfigured, or if there is a change to the site servers such as the name server or mail hub.

Current settings are displayed in the respective boxes. To change a 'system' field, enter the updated value in the appropriate box and click *<SysConfigApply>*. To change an 'interface' field, enter the updated value in the appropriate field and click *<Interface Apply>*.

Note: *All the fields must be correct when the respective 'apply' button is clicked (i.e. if there is a DNS, the IP address must be entered or it will be **deleted** from the system when the apply configuration button is used).*

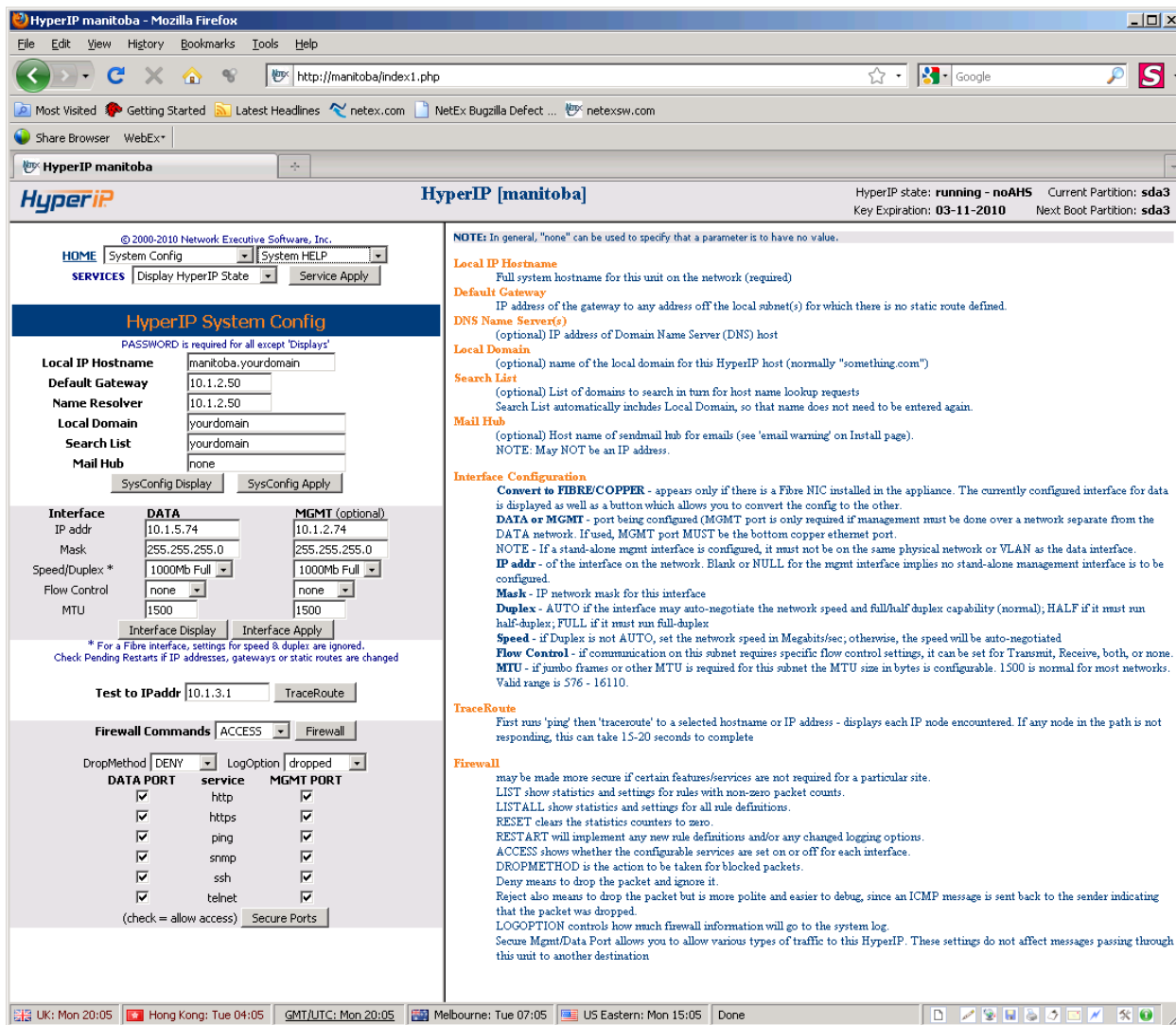


Figure 14: Web Browser System Config Page and Help

The following is the information provided in the “System HELP” display.

**NOTE:** In general, “none” can be used to specify that a parameter is to have no value.

### Local IP Hostname

Full system hostname for this HyperIP on the network (required)

### Default Gateway

IP address of the gateway to any address off the local subnet(s) for which there is no static route defined.

### DNS Name Server(s)

(optional) IP address of Domain Name Server (DNS) host

### Local Domain

Name of the local domain for this HyperIP host (normally “something.com”)

### Search List

(optional) List of domains to search in turn for host name lookup requests

Search List automatically includes Local Domain, so that name does not need to be entered again.

### **Mail Hub**

(optional) Name or IP address of Sendmail hub for email (see 'email warning' on Install page)

### **Interface Configuration**

**Convert to FIBER/COPPER** - appears only if there is a Fiber NIC installed in the NetEx provided appliance hardware. The currently configured interface for data is displayed as well as a button which allows you to convert the config to the other.

**DATA or MGMT** - port being configured (MGMT port is only required if management must be done over a network separate from the DATA network. If used, MGMT port **MUST** be Ethernet port 1.

**IP addr** - of the interface on the network

**Mask** - IP network mask for this interface

**Duplex** - AUTO if the interface may auto-negotiate the network speed and full/half duplex capability (normal); HALF if it must run half-duplex; FULL if it must run full-duplex

**Speed** - if Duplex is not AUTO, set the network speed in Megabits/sec; otherwise, the speed will be auto-negotiated

**Flow Control** - if communication on this subnet requires specific flow control settings, it can be set for Transmit, Receive, both, auto or none.

**MTU** - if jumbo frames or other MTU is required for this subnet the MTU size in bytes is configurable. 1500 is normal for most networks.

### **TraceRoute**

First runs 'ping' then 'traceroute' to a selected hostname or IP address; displays each IP node encountered.

If any node in the path is not responding, this can take 15-20 seconds to complete

### **Firewall**

may be made more secure if certain features/services are not required for a particular site.

LIST show statistics and settings for rules with non-zero packet counts.

LISTALL show statistics and settings for all rule definitions.

RESET clears the statistics counters to zero.

RESTART will implement any new rule definitions and/or any changed logging options.

ACCESS shows whether the configurable services are set on or off for each interface.

DROPMETHOD is the action to be taken for blocked packets.

Deny means to drop the packet and ignore it.

Reject also means to drop the packet but is more polite and easier to debug, since an ICMP message is sent back to the sender indicating that the packet was dropped.

LOGOPTION controls how much firewall information will go to the system log.

Secure Mgmt/Data Port allows you to allow various types of traffic to this HyperIP. These settings do not affect messages passing through this HyperIP to another destination

The `<TraceRoute>` command may be used to test network connectivity to any valid IP address or to verify network configuration changes. TraceRoute is useful to verify network connectivity to the remote HyperIP as well as the local application hosts that will be directing IP traffic to the HyperIP.

## HyperIP Config Page

The following figure is an example of the display seen when selecting the “HyperIP Config” option in the `<left frame>` drop down menu in the top left frame. The right frame in the following display is the result of selecting the Configure NxN from the `<right frame>` drop down. HyperIP configuration is typically performed only at installation time, but may also be required if the HyperIP configuration is changed to/from AHS or when adding/removing HyperIP sites.

The screenshot shows the HyperIP web browser interface. The top navigation bar includes 'HOME', 'HyperIP Config', and 'System HELP'. The main content area is split into two frames. The left frame, titled 'HyperIP Configuration', contains several sections: 'Configure NxN Sites' with a 'Topology Command' button; 'Start/Halt Remote Sites' with a 'State Command' button; 'HyperIP Gateway Mode Acceleration' with a dropdown set to 'ON' and 'Blocked' options for new and current connects; and 'Change HyperIP' with 'ConnectLimits' for TCP, UDP, and total connections. The right frame, titled 'NxN Config [Monday @ 14:06:35]', displays a table of HyperIP sites and an 'Add new Site(s)' table. Below the tables are instructions and a warning about the 'NewConfig' function.

HyperIP Site #	SiteName	primary IPAddr	--- AHS virtual --- IPAddr	secondary ID	secondary IPAddr	SegSize (bytes)	MaxRate (Mbits/s)	del?
33	sonora	10.1.5.177	0	0	0	32768	0	<input type="checkbox"/>
5	mexicali	10.1.5.73	0	0	0	32768	0	<input type="checkbox"/>
2	manitoba	10.1.5.74	0	0	0	32768	0	<input type="checkbox"/>

#	SiteName	primary IPAddr	--- AHS virtual --- IPAddr	secondary ID	secondary IPAddr	SegSize (bytes)	MaxRate (Mbits/s)

```

*** HyperIP site configuration data ***
* N sitename realIP AHSvirtIP VID secondIP SegSize MaxRate
33 sonora 10.1.5.177 0 0 0 32768 0
5 mexicali 10.1.5.73 0 0 0 32768 0
2 manitoba 10.1.5.74 0 0 0 32768 0
  
```

Figure 15: Web Browser HyperIP Configure and NxN Config Page

## Topology Commands

**Configure NxN Sites** – brings up the configuration form in the right-side frame for adding/deleting/modifying the HyperIP sites.

**Bandwidth Schedule** – brings up the Bandwidth Schedule form in the right-side frame for changing the bandwidth (rate limiting) schedule.

**Proxies & Intercepts** – brings up the Proxies and Intercepts form to allow modifications to the proxy and intercept configuration.

*Note: the 3 entries above are the same as selecting these values from the right-side navigation menu.*

## Start/Halt Remote Sites

**Show All Site States** – displays the current state of each configured site: STARTed, HALTed or LOCAL

**Start Site** – changes the selected site's state to STARTed. This initiates connect attempts with the sites remote peer(s)

**Halt Site** – changes the selected site's state to HALTed. This disconnects any sessions to configured remote sites.

**Show Site Config** - displays the configuration file statements related to the selected site.

## Gateway Mode (Intercepts)

When Gateway Mode is ON, all traffic being routed to this HyperIP will be intercepted and resent over a HyperIP session

When Gateway mode is OFF, new application connections can be either discarded (Blocked) or sent to normal IP routing (useful for testing native performance vs. HyperIP optimized performance).

Also, when Gateway Mode is OFF, currently connected TCP/UDP traffic can be blocked or forwarded (useful for forcing an application connection restart).

## Set Connect Limits

The maximum number of TCP, UDP and total connections can be changed. Currently, the total maximum is 8192.

## NxN Configuration Page

The first section of the NxN Config page shows currently configured HyperIP sites (or –none-). Following is a fill-in form in which to configure the information required for session establishment between this HyperIP and all others. Up to 4 sites may be configured at a time in this section. (Refer to Figure 15 above.)

NOTE – the local site must be the first one entered.

### HyperIP Site Number

An arbitrary number (1-99) identifying the HyperIP site. This number must be consistent on all configured HyperIPs.

### HyperIP Site Name

An arbitrary name to identify the HyperIP site. Choose something descriptive for the location or function.

**Primary IP Address**

Enter the real data IP address for the site (primary HyperIP for AHS)

**AHS Virtual IP Address**

(required for AHS, null if non-AHS) Enter the address used by servers as gateway addresses across the HyperIP network.

NOTE: The real & virtual HyperIP addresses on each side of the network must be on the same subnet.

**Virtual Router ID**

(required for AHS only) must be integers < 256 and unique on the subnet.

**Secondary IP Address**

For AHS site, enter the real data IP address for the secondary HyperIP

**SegSize**

The session transmission size in bytes. Only needed if the default value (32 KB) is not appropriate for sessions with this site.

**MaxRate**

The maximum rate to send to this site from any other. The bandwidth schedule may reduce this value but may not exceed it. The sum of the maxrate values for all the sites may not exceed the license rate for the local unit.

**Configure this unit as ...**

Identify the unit being configured by entering its site number and AHS role.

When all data has been entered click the <ApplyConfig> button. If more than 4 sites are to be configured, repeat this process as needed.

To delete all configured sites, select the "Confirm Delete All" box, then click the <DeleteAllSites> button.

For subsequent HyperIPs in the NxN configuration, once one HyperIP is configured you can copy-paste the configuration data from the blue box at the bottom of this page to the corresponding box on an unconfigured unit, enter the site number and AHS role of the new unit and click the <NewConfig> button. This will configure the sites as if they were entered above.

# Bandwidth Schedule (Rate Limiting) Page

Use this form to schedule network rate limits to some or all remote sites for specific times, days or dates. The rate may be reduced from the configured rate for the site, but may not exceed the configured rate.

**HyperIP Configuration**

Bandwidth Schedule | Topology Command

Start/Halt Remote Sites

HyperIP Gateway Mode Acceleration: ON

Change HyperIP: TCP: 0, UDP: 0, total: 0

**Rate Schedule [Monday @ 14:07:31]**

Current Rules: 20 Active Rule#s: 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 License Rate: unlimited Mbps

Rule#	Day	Month	Date	Start Time	End Time	Mbits/s	to Site
1	any	any	any	0000	2400	850	sonora
2	any	any	any	0000	2400	400	mexicali
3	any	any	any	0000	2400	10	mexicali
4	any	any	any	0000	2400	1	mexicali
5	any	any	any	0000	2400	50	mexicali
6	any	any	any	0000	2400	25	mexicali
7	any	any	any	0000	2400	5	mexicali
8	any	any	any	0000	2400	130	sonora
9	any	any	any	0000	2400	135	sonora
10	any	any	any	0000	2400	20	sonora
11	any	any	any	0000	2400	800	mexicali
12	any	any	any	0000	2400	800	sonora
13	any	any	any	0000	2400	155	sonora
14	any	any	any	0000	2400	45	sonora
15	any	any	any	0000	2400	10	sonora
16	any	any	any	0000	2400	155	sonora
17	any	any	any	0000	2400	450	mexicali
18	any	any	any	0000	2400	450	sonora
19	any	any	any	0000	2400	850	sonora
20	any	any	any	0000	2400	950	sonora

**New Rule To Add:**

After #	Day	Month	Date	Start Time	End Time	Mbits/s	to Site
20	any Mo Tu	any Jan Feb	any 01 02	00 00	24 00	950	sonora

Buttons: Add Rule, Delete All Rules, Delete Rule 1

**NOTES:**

- \* the default max transmit bandwidth to each remote site is configured on the 'Configure NIN' page.
- \* the configured rate can be reduced (limited) by this schedule, but not increased.
- \* higher rule number takes precedence for periods where multiple rules overlap for a site.
- \* to force a permanent override rate, add a rule like: 'any any 0000 2400 rate site'. To unset the override, delete the rule.
- \* a rate setting greater than the licensed bandwidth is limited per the license. Zero implies the license limit.

Figure 16: Web Browser Rate Limit Schedule Page

The day/month/date settings are logically 'OR'ed, so that if any of the 3 match with 'now', the rule applies.

Rules are checked when HyperIP is started, when rules are changed, and at every quarter-hour to see which is the current Site highest priority rule, and to set the rate limit accordingly.

## Proxies and Intercepts Page

Use this form to add or delete proxy mode or gateway mode (intercepts) for traffic that is to be optimized via HyperIP. The table allows you to specify source and destination IP addresses, ports and protocols to examine for optimization to a designated remote HyperIP site.

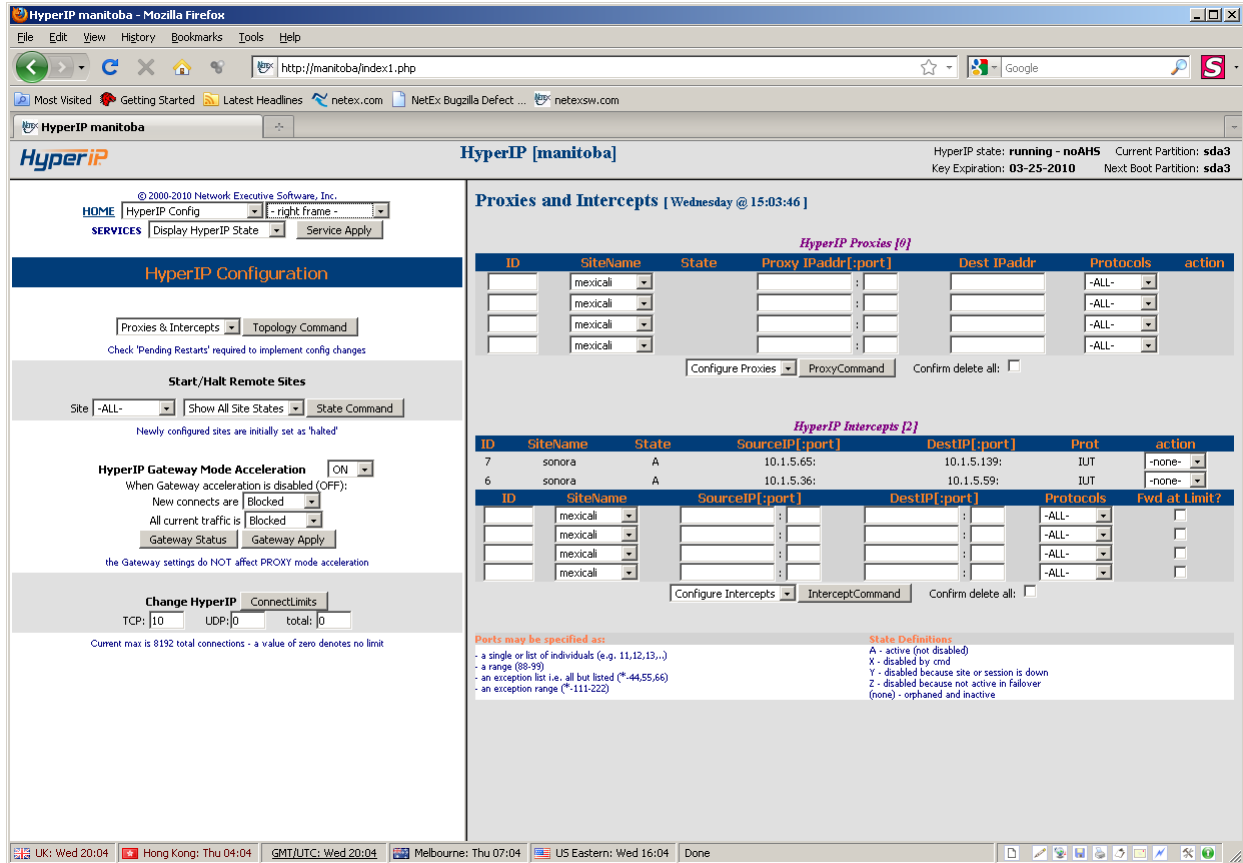


Figure 17: Web Browser Proxies and Intercepts Page

### HyperIP Proxies

#### ID

An arbitrary identifier for the proxy definition

#### SiteName

Destination HyperIP site for traffic matching this proxy IP address

#### Proxy IPaddr:port

Local proxy IP address (virtual IP address)

#### Dest IPaddr

Destination address to redirect to (local proxy IP address represents)

#### Protocols

Select TCP and/or UDP and/or ICMP traffic to optimize

**Action**

For existing entries, delete/disable/enable this proxy

**HyperIP Intercepts****ID**

An arbitrary identifier for the intercept definition

**SiteName**

Destination HyperIP site for traffic matching this intercept

**Source IP:port**

Origination address or addresses to match candidates for optimization. The asterisk (\*) can be used as a wildcard to specify a range of IP addresses (i.e. 10.2.2.\*).

Source port can be specified as a single port, a list of ports, a range of ports, an exception, or an exception range.

**DestIP:port]**

Destination address or addresses to match intercepts candidates for optimization. The asterisk (\*) can be used as a wildcard to specify a range of IP addresses (i.e. 10.2.2.\*).

Destination port can be specified as a single port, a list of ports, a range of ports, an exception, or an exception range.

**Protocols**

Select TCP and/or IP and/or ICMP traffic to optimize

**Action**

For existing entries, delete/disable/enable this proxy or intercept

**Fwd At Limit**

If selected, when the TCP/UDP connection limit is reached, HyperIP will forward the connections un-optimized. If not selected, HyperIP will drop the connection. This also depends on the “all curr traffic” forwarding setting for gateway mode.

## Advanced Config Page

The following figure is an example of the display seen when selecting the Advanced Config in the <left frame> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Advanced Help from the <right frame> drop down.

This is where you may configure <Static Routes> (i.e. from this HyperIP to the remote HyperIP, or to get to an application host on another subnet).

Another selection is used to set the local <TimeZone> for this HyperIP, and to determine whether the system time is to be synchronized with other network hosts <NTP Config>. Advanced configuration is typically NOT required, and usually performed only at installation time, but may be required if the network configuration is changed.

This page also allows you to alter “tuning” parameters for the connections between the HyperIPs.

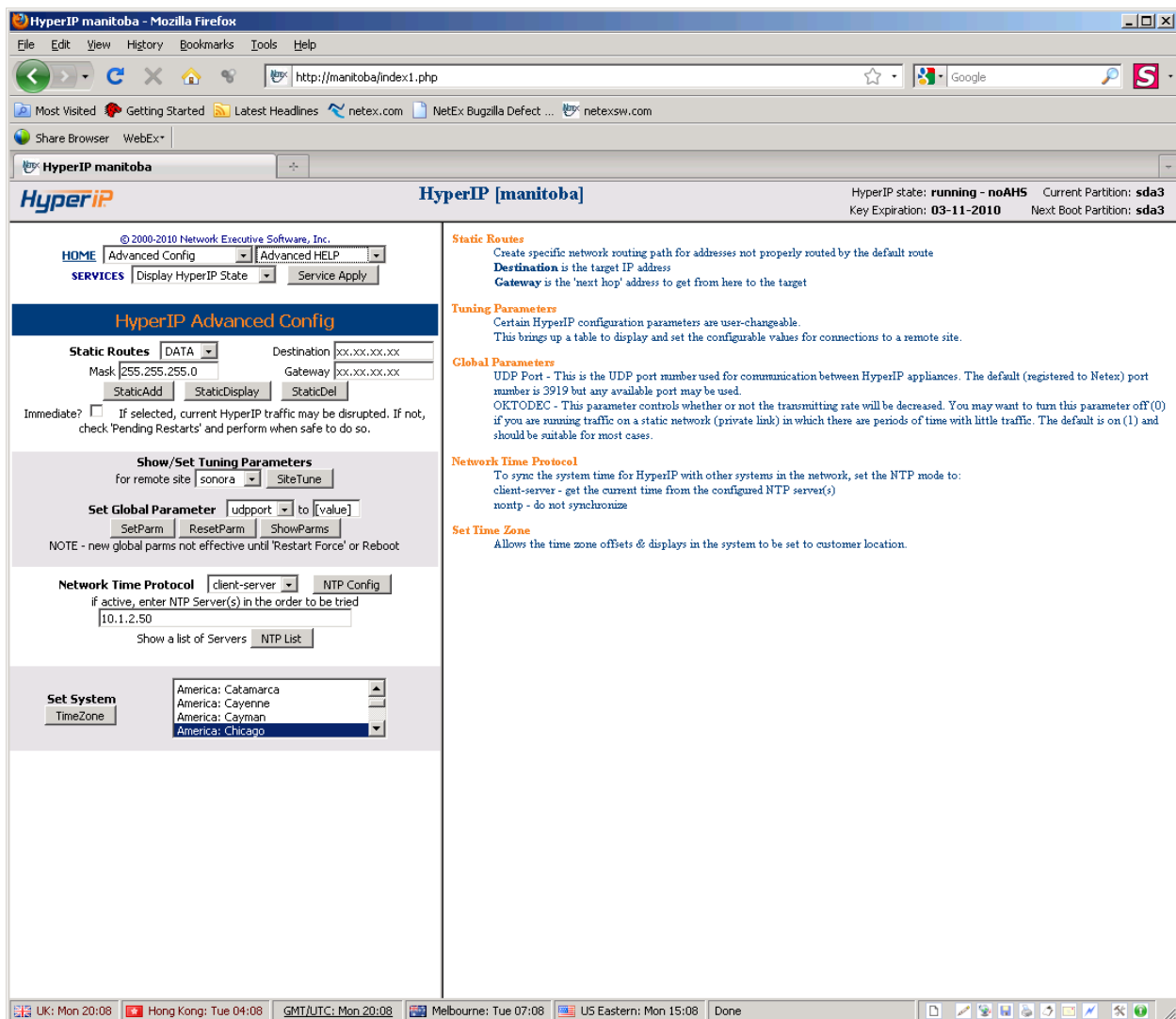


Figure 18: Web Browser Advanced Configure Page

The following information is provided in the “Advanced HELP” display:

## **Static Routes**

Create specific network routing path for addresses not properly routed by the default route

Destination is the target IP address

Gateway is the 'next hop' address to get from here to the target

## **Show/Set Tuning Parameters**

Certain HyperIP configuration parameters are user-changeable.

This brings up a table to display and set the configurable values for connections to a remote site.

## **Global Parameters**

UDP Port - This is the UDP port number used for communication between HyperIPs. The default (registered to NetEx) port number is 3919 but any available port may be used.

oktodec – When this parameter is set to 0 HyperIP will not decrease the transmission when the receiver is not keeping up with the sender. When this is set to 1 (default), HyperIP will attempt to decrease the transmission rate when the receiver is not keeping up with the sender.

## **Network Time Protocol**

To sync the system time for HyperIP with other systems in the network, set the NTP mode to:

client-server - get the current time from the configured NTP server(s)

nntp - do not synchronize

## **Set Time Zone**

Allows the time zone offsets & displays in the system to be set to customer location.

The following is an example of the display seen when selecting a site from the “Show/Set Tuning Parameters” and clicking on the <Site Tune> button in the middle section of the left frame.

**Warning: These parameters should be set under the direction of Network Executive Software, Inc. support personnel; incorrect settings can adversely affect the performance of HyperIP.**

The screenshot shows a Mozilla Firefox browser window displaying the HyperIP configuration interface. The page title is "HyperIP [manitoba]". The interface is divided into several sections:

- Navigation:** HOME, Advanced Config, Advanced HELP, SERVICES, Display HyperIP State, Service Apply.
- HyperIP Advanced Config:** Static Routes (DATA), Mask (255.255.255.0), Destination (jx.xx.xx.xx), Gateway (jx.xx.xx.xx). Buttons: StaticAdd, StaticDisplay, StaticDel.
- Show/Set Tuning Parameters:** for remote site 'sonora', SiteTune button.
- Set Global Parameter:** udpport [ ] to [value]. Buttons: SetParm, ResetParm, ShowParms.
- Network Time Protocol:** client-server, NTP Config. If active, enter NTP Server(s) in the order to be tried: 10.1.2.50. Button: Show a list of Servers NTP List.
- Set System:** America: Catamarca, America: Cayenne, America: Cayman, America: Chicago. Button: TimeZone.
- Session Tuning [Monday @ 14:09:31]:**
  - maxmtowait/minbtosend:** Used to delay when data blocks are handed off to the compression engine, potentially improving the compression ratio.
  - compalg/compadpt/compapercent:** These work together to configure HyperIP compression usage.
  - userxmitq/rexmwbkls:** Work together on the transmitting side when packets are being delivered out of order to prevent unnecessary retransmits.
  - rcvdataqhb/rcvdatalb:** Work together at the receiving side when packets are being delivered out of order to prevent unnecessary retransmits.
  - bufolimit:** When HyperIP sends small blocks (i.e. highly compressed data), this limit may need to be increased to keep the data flowing as fast as possible.
  - usercvgapq:** When the receiving HyperIP is receiving dups at a rate consistent with the transmitting HyperIP's retransmits, this parameter should be turned on.
- Tuning Parameters for Sessions to Site: sonora:**

PARAM	Default Value	Changed/New Value	Description
maxmtowait	0	0	maximum millisecs to wait before sending data, 0-9999
minbtosend	0	0	minimum bytes to send when using maxmtowait, 0-65400
compalg	1	0	compression algorithm to use - 0:none 1:LZO
compadpt	1	1	use adaptive compression - 0:no 1:yes
compapercent	80	80	no compression unless compressed size is < this % of original
userxmitq	1	1	use rexitmq or not - 0:no 1:yes
rexmwbkls	2	2	retransmit queue depth - number of segments to wait when using rexitmq
rcvdataqhb	20000000	20000000	# of bytes on dataQ over which data is discarded
rcvdatalb	10000000	10000000	# of bytes on dataQ under which data is again accepted after discarding
bufolim	2000	2000	max number of write segments allowed to be in progress
usercvgapq	0	0	store packets received out of order - 0:no 1:yes

Figure 19: Web Browser Show/Set Site Tune Parameters Page

# Maintenance Page

The following figure is an example of the display seen when selecting the Maintenance Commands in the <left frame> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Maintenance Help from the <right frame> drop down. This page is used to perform several maintenance functions for HyperIP; such as dumping diagnostic information, saving/restoring configurations, and downloading new releases of HyperIP software.

The *admin* password is required for any entry from this window, except displays.

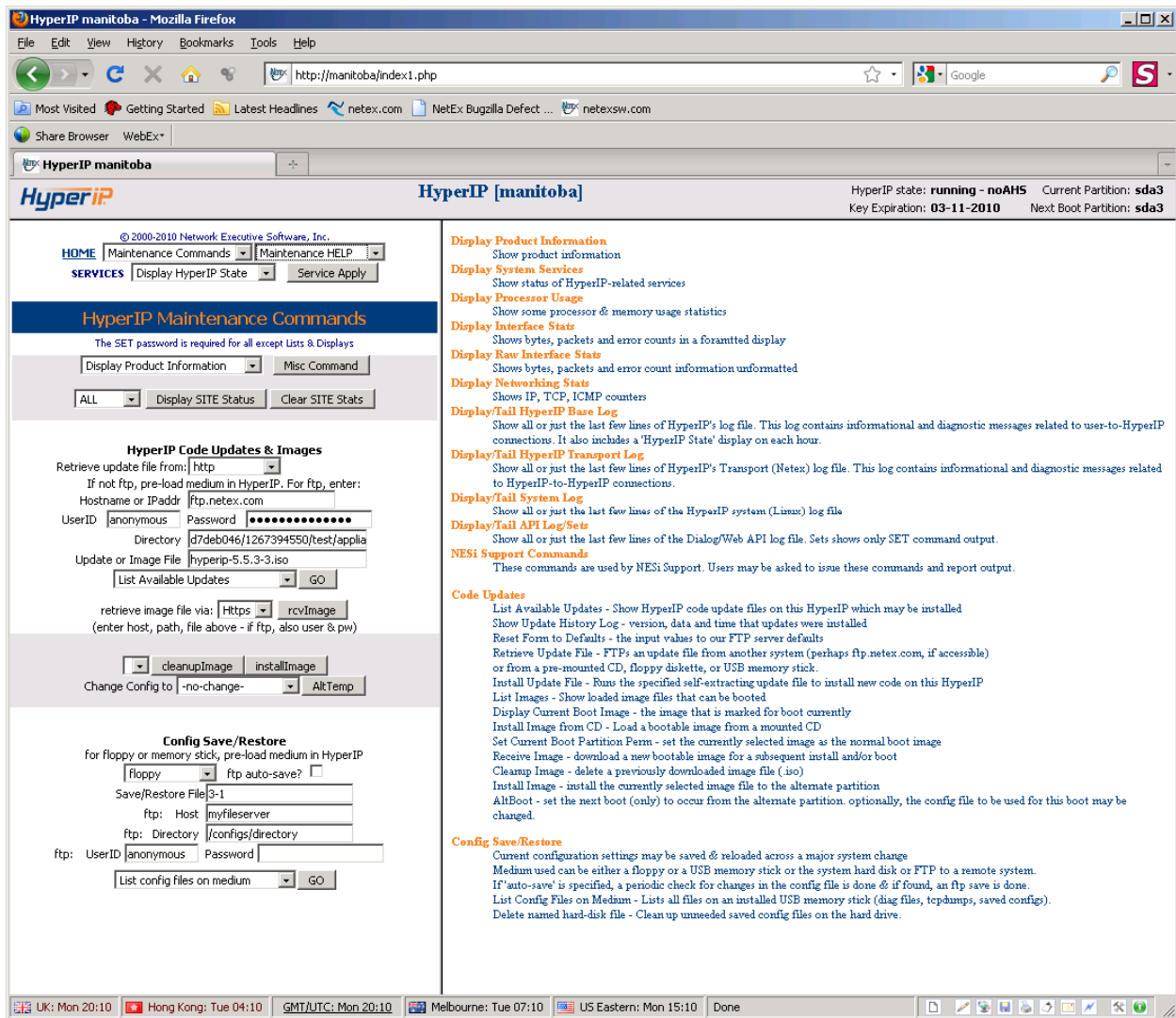


Figure 20: Web Browser Maintenance Page

Most of the following information is provided by the “Maintenance HELP” display.

<Misc Command> (Select command from the adjacent drop down menu)

## Display Product Information

Show Product Information and Boot Partition Information

## Display System Services

Show status of HyperIP-related services

### **Display Processor Usage**

Show some processor & memory usage statistics

### **Display Interface Stats**

Shows bytes, packets and error counts in a formatted display

### **Display Raw Interface Stats**

Shows bytes, packets and error count information unformatted

### **Display Networking Stats**

Shows IP, TCP, ICMP counters

### **Display/Tail HyperIP Base Log**

Show all or just the last few lines of HyperIP's log file. This log contains informational and diagnostic messages related to user-to-HyperIP connections. It also includes a 'HyperIP State' display on each hour.

Note: If HyperIP software isn't starting the last few lines in this log will indicate why.

### **Display/Tail HyperIP Transport Log**

Show all or just the last few lines of HyperIP's Transport (Netex) log file. This log contains informational and diagnostic messages related to HyperIP-to-HyperIP connections.

### **Display/Tail System Log**

Show all or just the last few lines of the HyperIP system log file. This log contains both the Base and the Transport logs too.

### **Display/Tail API Log/Sets**

Show all or just the last few lines of the Dialog/Web API log file. Sets shows only SET command output.

**Show Active Config** – displays the currently running configuration information for this unit.

**Show Configuration File** - shows the current HyperIP configuration file.

*<Display Site State>* shows the status of the connection with the selected site or all connected sites (see the hipstatus output below)

*<Clear Site Stats>* resets the accumulated statistics for the selected site connection(s).

## **HyperIP Code Updates and Images**

HyperIP provides a simple interface to process software updates. Updates can be loaded on the HyperIP via a floppy disk, CD or from an FTP server, by clicking the appropriate button. Default parameters suggest how to move the file directly from NetEx's FTP server (if there is connectivity via the internet).

**When loading from a CD or floppy and there is no directory structure, set the directory to '/**

*<List Available Updates>* displays the names of update files currently stored on the HyperIP.

*<Reset Form to Defaults>* sets values to the default settings.

<*Show Update History Log*> gives a history of updates that have been applied.

<*Show Info for Selected Update*> displays a description of the update file indicated in the “*Update or Image File*” text box.

<*Retrieve Update*> retrieves the update file indicated in the “*Update or Image File*” text box for the media indicated in the “*Retrieve update file from:*” text box and stores it appropriately on the HyperIP.

<*InstallUpdate*> will apply the update indicated in the “*Update or Image File*” text box.

Complete software versions (image files) may also be downloaded via FTP or from a CD to the alternate system partition. (Use the Display Product Information command found on the Maintenance webpage to see the version of software on each partition. This command is documented on page 56.) You will need to use the <*AltTemp*> command to boot the new software version when appropriate. Once the new software version has been booted and verified, use the <*Set Curr Boot Partition Perm*> command to make it permanent. The following commands pertain to retrieving and installing new software versions.

<*List Images*> displays the names of image files currently stored on the HyperIP.

<*InstallImageFromCD*> will install an image from a pre-mounted CD.

<*Set Curr Boot Partition Perm*> sets the currently selected image as the permanent boot image.

The <*rcvImage*> button allows downloading of a new image via ftp, http, or https. Once downloaded, an image may be deleted or installed via the <*cleanUpImage*> or <*InstallImage*> buttons.

<*AltTemp*> sets a selected image file as the partition to next boot (this is temporary until it is made permanent).

## HyperIP Configuration Save/Restore

HyperIP supports several medias to save and restore configuration parameters to/from. The configuration can be saved on the HyperIP hard disk, on any removable media supported by the HyperIP, or to an FTP server, by clicking the appropriate button.

**NOTE:** *When saving to a floppy and there is no directory structure, set the directory to ‘/’.*

If using a floppy or memory stick, place the medium in the drive *before* clicking the button. For a Restore, remove the medium before rebooting, or the system may attempt to use that as the boot device.

Selecting the <*ftp-auto*> causes the HyperIP to automatically save configuration data to the configured FTP server after configuration changes are been made.

**NOTE:** *Configurations saved from HyperIP versions 5.4.6 or earlier will undergo a one-time conversion when restored on version 5.5. Version 5.5 configurations can be saved/restored across HyperIPs running version 5.5 or later, but cannot be restored on previous HyperIP versions.*

## Display HyperIP State / Site Status Detail

The following example shows the selection of *Display HyperIP State* on the **Services** menu in the top left frame or *Display Site Status* on the **Maintenance Commands** page (same information for a single site).

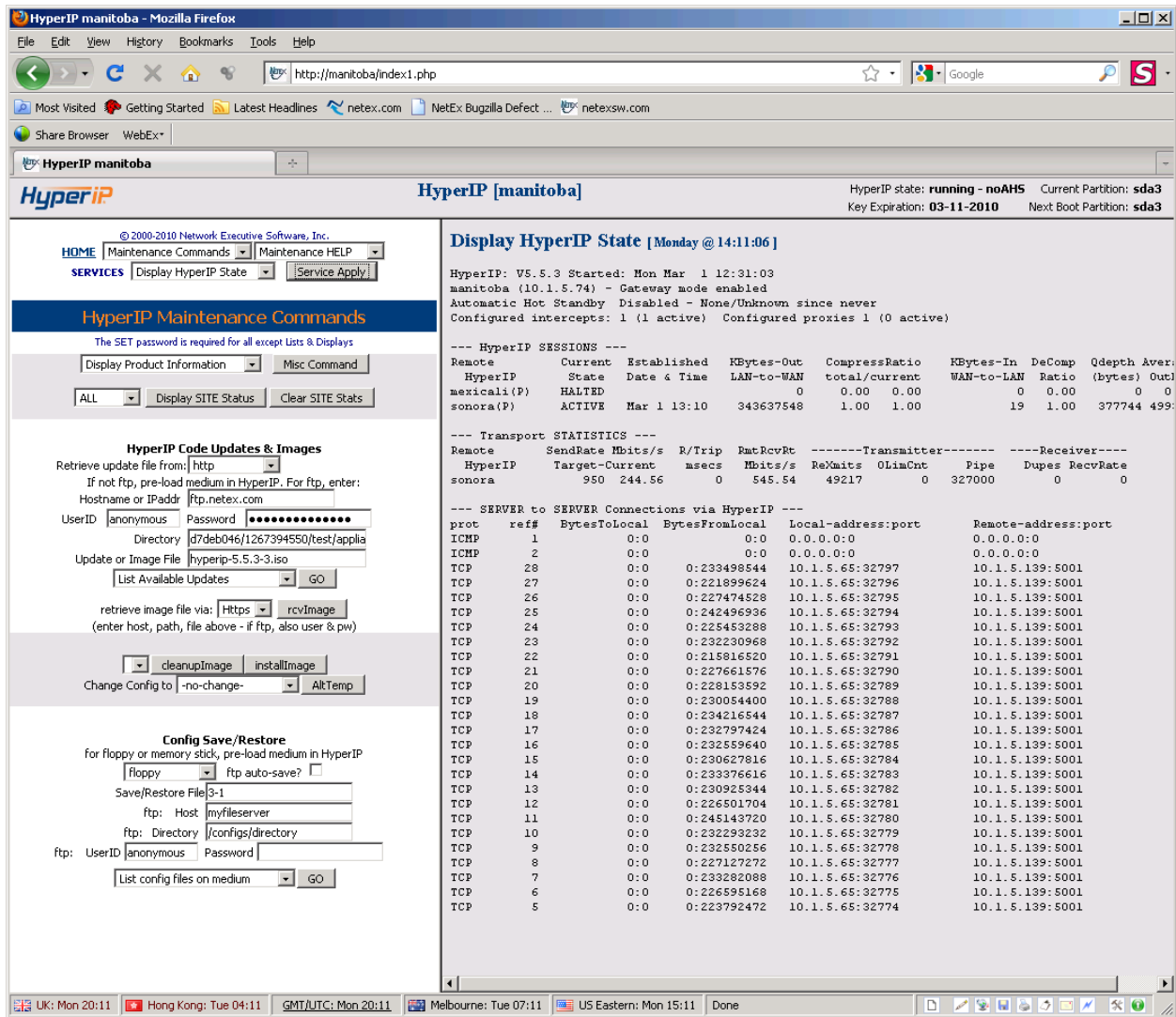


Figure 21: HyperIP State Display

In the previous display, at the bottom, *local-addresses* refer to the hosts that are using this HyperIP as their IP gateway. The *remote-addresses* are on the other side of the HyperIP link.

The Current State in the HyperIP Connections refers to the current condition of the session between the HyperIPs. The possible states include:

- ACTIVE**            The session is active; normal, running mode.
- OFFER**            Session is offered. Typically seen when only one end of the HyperIP link is up and running.
- OFFERW**          The previous offer failed, and the session is waiting for a timeout to re-offer
- CONNECT**        Session has issued a connect.
- CONNW**            The previous connect failed, and the session is waiting for a timeout to re-issue a connect
- CONFIRM**        Session has issued a confirm.
- RCONFIRM**      Session is waiting to read a confirm.

<b>CLOSE</b>	Session has issued a close.
<b>DSCPND</b>	A disconnect is pending on the session.
<b>DISC</b>	Session has issued a disconnect.
<b>WAIT</b>	The remote system sent a “resources low” message, and normal messages may not be sent on this session until the remote system sends a “resource OK” message.
<b>INIT</b>	Session in initialize state.
<b>INITPND</b>	Session initialize pending.
<b>HALTED</b>	Session halted by HyperIP user.
<b>HALTPND</b>	Halt pending on this session.
<b>PACED</b>	Session received a pace (slowdown) notification from the remote HyperIP.
<b>DOWN</b>	Session received a SHUTDOWN notification from the remote HyperIP.

## Diagnostic Commands Page

The following figure is an example of the display seen when selecting the Diagnostic Commands in the <left frame> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Diagnostic Help from the <right frame> drop down. This page is used to perform several maintenance functions for HyperIP; from evaluating the WAN connection to dumping diagnostic information to setting up remote logging.

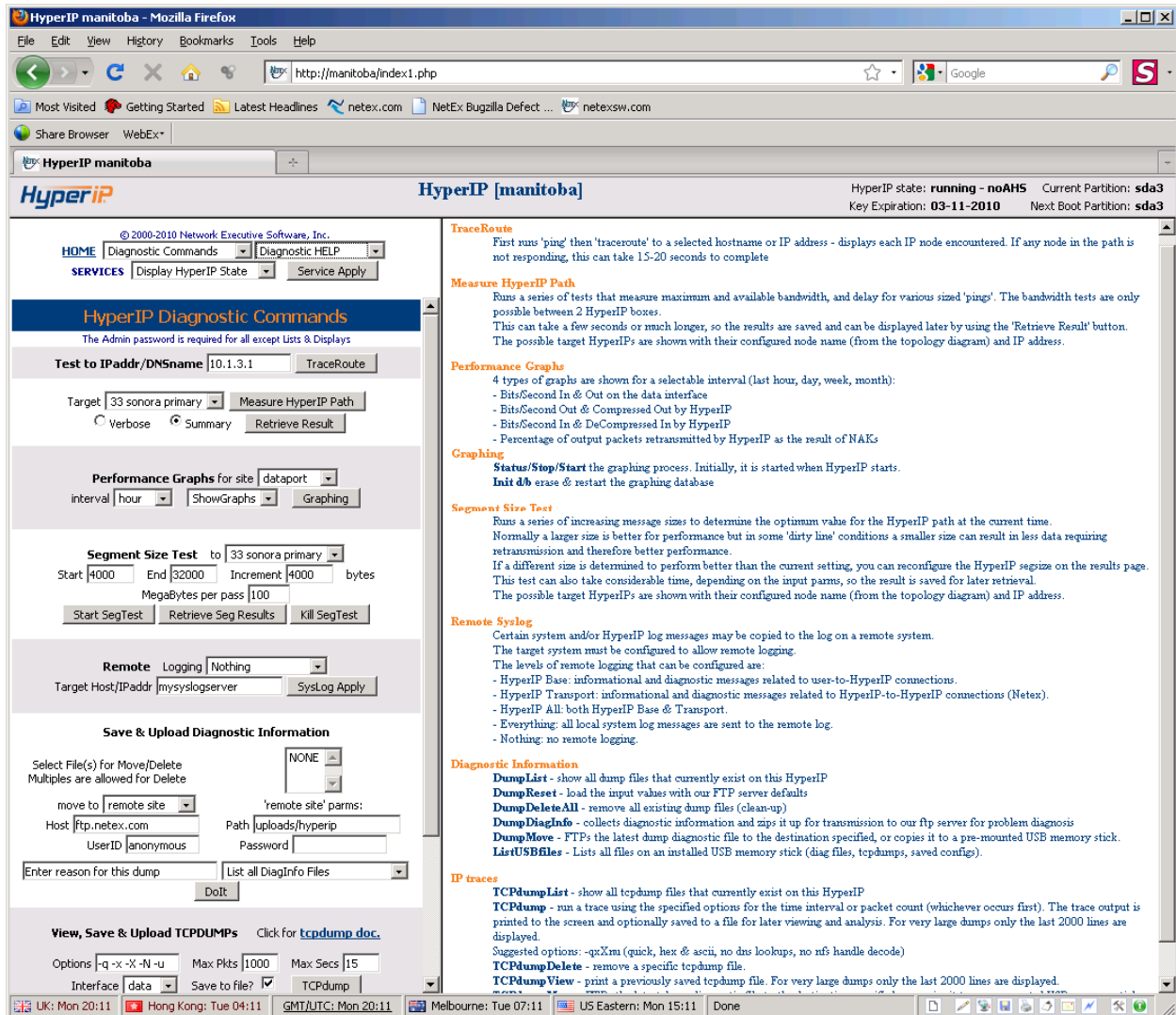


Figure 22: Web Browser Diagnostic Commands Page

Some of the following is the information provided in the “Diagnostic HELP” display.

### TraceRoute

First runs ‘ping’ then ‘traceroute’ to a selected hostname or IP address - displays each IP node encountered. If any node in the path is not responding, this can take 15-20 seconds to complete

## Measure HyperIP Path

The <*Measure HyperIP Path*> button runs a utility that will analyze and evaluate the path between configured HyperIPs. It runs a series of tests that measure maximum and available bandwidth, and delay for various sized 'pings'. These bandwidth tests are only possible between two HyperIP boxes.

This can take a few seconds or much longer, so the results are saved and can be displayed later by using the 'Retrieve Result' button.

The possible target HyperIPs are shown with their configured node name (from the topology diagram) and IP address.

**NOTE:** This utility should be run during installation between quiesced HyperIPs in order to get accurate results.

## Performance Graphs

HyperIP provides four types of graphs to analyze the optimization operation to/from the configured sites: in/out on the data interface, optimized out, optimized in and retransmit percentage. These graphs can be displayed for four intervals as well: last hour, day, week or month.

Be sure the graphing is turned on. To disable the graphing select **OFF** from the center drop down menu and click the <*Graphing*> button. This setting is persistent.

Select the *dataport*, *aggregate* or the appropriate site from the *site* dropdown menu, next select the appropriate graph interval to display (last hour, day, week, and month) from the *interval* dropdown menu and then select ShowGraphs from the center dropdown and click the <*Graphing*> button.

**Site:**

*dataport* - graphs the Bits/Second In & Out on this HyperIP's data interface

site selected - Bits/Second Out & Compressed Out by HyperIP to the site selected from the menu.

Bits/Second In & DeCompressed In by HyperIP from the site selected from the menu.

Percentage of output packets retransmitted by HyperIP as the result of negative acknowledgements.

*aggregate* – displays all of the above graphs for all configured sites

The center dropdown menu has five selections:

**ShowGraphs** – display the selected graphs

**Status** – show the status of the graphing facility

**Init d/b** – initialize the database

**ON** – turn on the collection of the graphing data

**OFF** – turn off the collection of the graphing data

## Segment Size Test

The <*Segment Size Test*> button runs a utility that will analyze the transfer rate between HyperIPs using various segment (HyperIP data block) sizes. If there is a significant improvement using a size other than that currently set, the new size may be set for use on all subsequent HyperIP session connections. A **Restart Force** is required to implement a new segment size.

This runs a series of increasing message sizes to determine the optimum value for the HyperIP path at the current time. If a different size is determined to perform better than the current setting, you can reconfigure the remote site segsize on the 'Configure NxN' page.

Normally a larger size is better for performance but in some 'dirty line' conditions a smaller size can result in less data requiring retransmission and therefore better performance.

This test can also take considerable time, depending on the input parameters, so the result is saved for later retrieval.

The possible target HyperIPs are shown with their configured node name (from the topology diagram) and IP address.

## Remote Logging

Certain system and/or HyperIP log messages may be copied to the log on a remote system. The target system must support and be configured to allow remote logging.

The levels of remote logging that can be configured are:

- **HyperIP Base:** informational and diagnostic messages related to user-to-HyperIP connections.
- **HyperIP Transport:** informational and diagnostic messages related to HyperIP-to-HyperIP connections (Netex).
- **HyperIP All:** both HyperIP Base & Transport.
- **Everything:** all local system log messages are sent to the remote log.
- **Nothing:** no remote logging.

## Diagnostic Dump Processing

HyperIP provides a utility that will collect and save essential data from HyperIP to a file that may be sent to, and analyzed by NetEx support personnel.

**NOTE:** If connectivity between HyperIPs is lost, this command may require several minutes (or longer) to complete.

Select one of the following commands from the drop down menu and click on the adjacent **<DoIt>** button to execute.

**List All DiagInfo Files** - show all diagnostic dump files that currently exist on this HyperIP

**List All Files on Memory Stick** - show all diagnostic dump, configuration and tcpdump files that currently exist on a USB memory device plugged into HyperIP (only if USB is supported on the HyperIP platform).

**Delete All DiagInfo Files** - remove all existing dump files (clean-up)

**Delete Selected DiagInfo File(s)** – remove the DiagInfo File(s) selected in the list displayed (use shift or ctrl keys while mouse clicking to select multiple files).

**Move Selected DiagInfo File** – move the DiagInfo File(s) selected in the list displayed (use shift or ctrl keys while mouse clicking to select multiple files) to the media selected by the “**move to**” drop down menu (memory stick or ftp; FTP site indicated by the “**Host**” text box; requires “**Path**”, **UserID** and “**Password**” text boxes to have valid information entered).

**Create DiagInfo File** - collects diagnostic information and compresses it for subsequent analysis by NetEx Support Personnel. Enter the reason for the dump creation in the “Enter reason for dump” text box, which is included in the dump. The created DiagInfo file must be delivered to NetEx support.

**Move ConnStats History Files** – allows the connection statistics to be offloaded to another server for analysis.

## TCP Dump Processing

HyperIP provides the utility TCPDUMP which is a useful utility to analyze traffic on the HyperIP’s network interfaces. It has a great many options and parameters which can be seen by clicking the [<tcpdump doc>](#) link.

**NOTE:** If no traffic is occurring on the HyperIP interface, this command may require several minutes (or longer) to complete.

Select one of the following commands from the drop down menu and click on the adjacent **<DoIt>** button to execute.

**TCPdump** - run a trace using the specified “*Options*” for the time interval (*Max Secs*) or packet count (*Max Pkts*) (whichever occurs first). The trace output is displayed on the screen and optionally saved to a file for later viewing, analysis or offloading. For very large dumps only the last 2000 lines are displayed.

Suggested options: -qxXnu (quick, hex & ASCII, no DNS lookups, no NFS handle decode)

**List All TCPdump Files** - show all TCP dump files that currently exist on this HyperIP

**List All Files on Memory Stick** - show all diagnostic dump, configuration and tcpdump files that currently exist on a USB memory device plugged into HyperIP (only if USB is supported on the HyperIP platform).

**Display Selected TCPdump File** – display a previously saved tcpdump file. For very large dumps only the last 2000 lines are displayed.

**Delete Selected TCPdump File(s)** – remove the TCP dump file(s) selected in the list displayed (use shift or ctrl keys while mouse clicking to select multiple files).

**Move Selected TCPdump File** – move the TCP dump file(s) selected in the list displayed (use shift or ctrl keys while mouse clicking to select multiple files) to the media selected by the “*move to*” drop down menu (memory stick or ftp; FTP site indicated by the “*Host*” text box; requires “*Path*”, *UserID* and “*Password*” text boxes to have valid information entered).

The following is an example of the tcpdump output.

The screenshot shows a Mozilla Firefox browser window displaying the HyperIP [manitoba] diagnostic page. The page title is "HyperIP [manitoba]" and the URL is "http://manitoba/index1.php". The browser's address bar shows the URL and search engines like Google. The page content includes a navigation menu with "HOME", "Diagnostic Commands", and "Diagnostic HELP". There are several sections for configuration and diagnostics:

- Performance Wraps:** Includes options for "interval" (hour), "ShowGraphs", and "Graphing".
- Segment Size Test:** Allows setting "Start" (4000), "End" (32000), and "Increment" (4000) bytes. It includes buttons for "Start SegTest", "Retrieve Seg Results", and "Kill SegTest".
- Remote Logging:** Includes a "Logging" dropdown (set to "Nothing") and a "Target Host/IPaddr" field (set to "mysyslogserver").
- Save & Upload Diagnostic Information:** Includes a "NONE" dropdown for file selection, a "move to" dropdown (set to "remote site"), and fields for "Host" (ftp.netex.com), "Path" (uploads/hyperip), "UserID" (anonymous), and "Password".
- View, Save & Upload TCPDUMPS:** Includes a "Click for tcpdump doc." link, "Options" (-q -x -X -N -u), "Max Pkts" (5), "Max Secs" (15), and "Interface" (data). It also has a "Save to file?" checkbox and a "TCPdump" button. Below this, there are fields for "File to Delete, View, or Move" (tcpdump-100301-141231) and another set of "Move to" and "remote site" parameters.

The main content area displays the output of a TCPdump command. The title is "TCPdump [Monday @ 14:12:31]". The output shows the start and end of the capture, options used (-q -x -X -N -u -i eth0 -c 5), and a list of captured packets. The packets are shown in hexadecimal and ASCII, with source and destination IP addresses and ports. The output ends with "5 packets captured", "2923 packets received by filter", and "2586 packets dropped by kernel".

Figure 23: Web Browser Diagnostic Page (tcpdump output)

## HTTP File Downloads Page

The following figure is an example of the display seen when selecting the Http File Downloads in the <left frame> drop down menu in the top left frame. This page is used to perform HTTP or HTTPS downloads of several maintenance files for HyperIP.

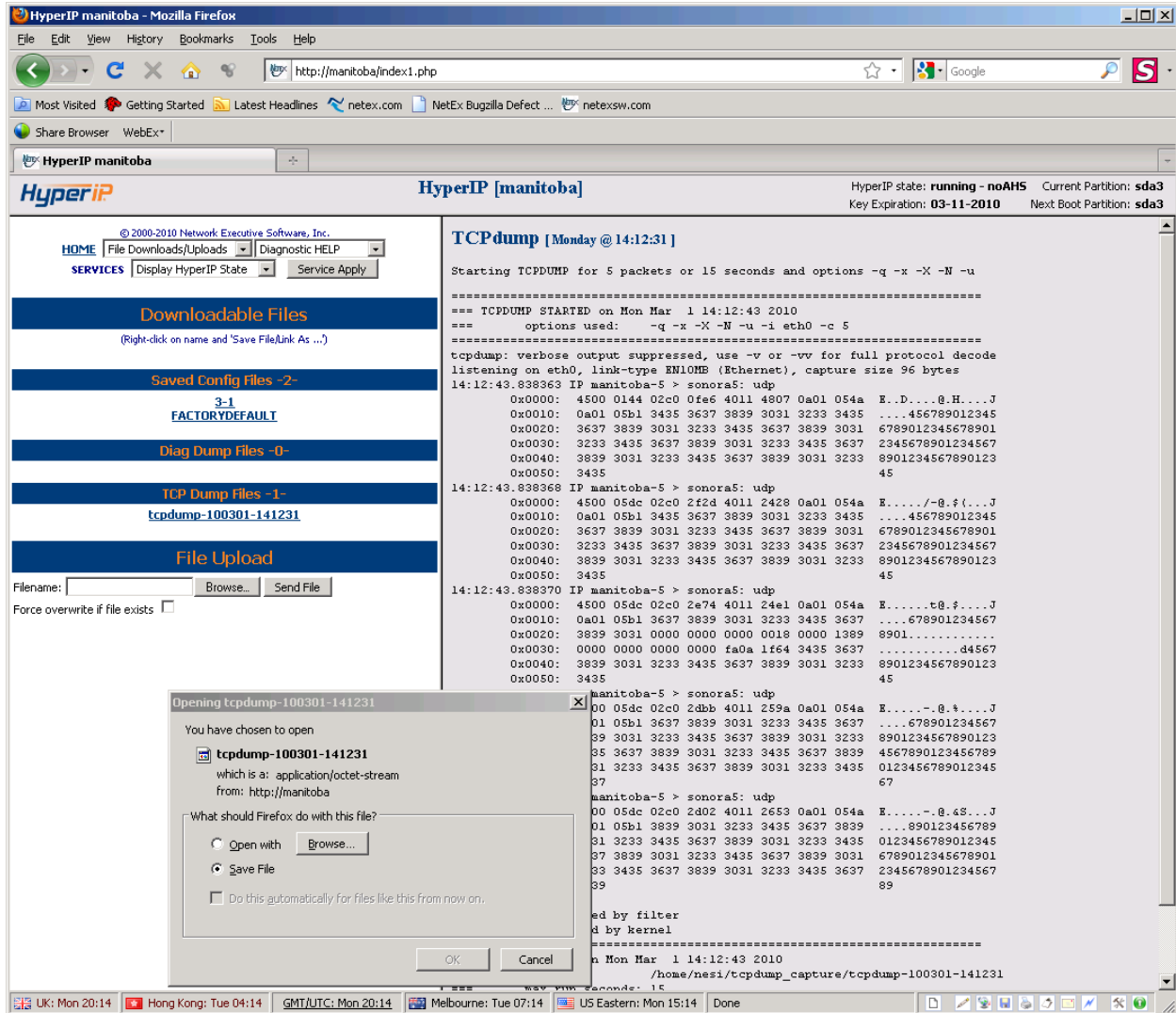


Figure 24: Web Browser File Downloads/Uploads Page (Download)

### Download to your browser workstation

To download a file from the HyperIP to your browser workstation, right click on the selected file and the “Save file...”. These files are files which have been saved on the HyperIP hard drive from the Maintenance Commands Page.

## **Upload from your browser workstation**

To upload a file from your workstation, “Browse” to look for the file on your workstation or type in the complete path/filename in the textbox. If the file is successfully transferred, the right frame will indicate that the file is valid and was successfully updated. Use the facilities on the Maintenance Commands Page to install this update (patch), upgrade (to the alternate partition) or restore this appropriate configuration file.



# Operational Procedures

## Initial Configuration via Serial Port (or console for VMware) to Use Web Interface

The following procedure describes the minimum required steps to configure a new HyperIP to use the management Ethernet port when the default IP address (10.10.2.2) cannot be used.

1. Using the serial port connection for appliance or console for VMware installations and log in as user “*hipadmin*”. The default password is ‘*hipadmin*’.
2. Use the CLI command to modify the default IP address:

```
cfgInterface <interface> <ip_address> <netmask> <speed> <mtu>
configure network interface

interface      data or mgmt
ip_address    IP address XX.XX.XX.XX
netmask       netmask XX.XX.XX.XX
speed         interface speed
mtu           mtu
```

3. Set the appropriate default gateway to get to local management servers (i.e., management workstation, FTP, etc.), as required by using the following CLI command:

```
cfgDefaultGateway <IP_ADDRESS>
configure the default gateway

IP_ADDRESS    IP address of default gateway
```

4. Reboot HyperIP by using the following CLI command:

```
reboot
```

5. For VMware deployments using VCenter management, you will need to log back in to HyperIP and use the following CLI commands to register with VCenter (You will need to use the IP address of the VCenter server at this point, since DNS is not configured yet.) This will register a plugin which adds a HyperIP tab with helpful links and a link to launch the browser to finish configuring and managing the HyperIP:

```
vCenterConfig <server> <username> <password>
configure a VMware Virtual Center for plugin registration

server        Virtual Center hostname or IP address
username      Virtual Center user
password      Virtual Center password

vCenterRegister register HyperIP plugin with configured VMware Virtual
Center

manitoba CLI> vCenterRegister
```

```
manitoba CLI> cfgDefaultGateway
```

6. Connect the management port to the appropriate LAN switch/hub.
7. You can now utilize the web interface (https).

## Saving HyperIP Configuration to Your Workstation

The following procedure documents the steps to save a HyperIP's configuration. It is strongly recommended that the HyperIP's configuration be saved off of the HyperIP appliance (i.e. on a workstation or removable media) in case a hard failure occurs and the HyperIP must be replaced with a spare. This procedure assumes your workstation has management access to the HyperIP via a web browser.

1. Use the HyperIP's DNS name or the IP address as the URL in your web browser and enter the password for the HyperIP.
2. From the "Maintenance" page, find the "Config Save/Restore" section.
3. Select the "**hard disk**" from the first drop down menu and enter a *useful* filename in the "**Save/Restore File**" field (i.e. HyperIP name and date)
4. Select "**Save Config to File**" from the second drop down menu and Click on <Go> to save the configuration to the HyperIP's hard disk.
5. Now go to the "File Downloads/Uploads" page, select the configuration file by the name from Step 3 above from the Saved Config Files section. Select "**Save File**" in the popup window and Click <ok> to save it to your workstation.

## Restoring HyperIP Configuration from your Windows Workstation

The following procedure documents the steps to restore a HyperIP appliance's configuration from a previously saved configuration. (Assumes the new HyperIP has been configured to use your Windows workstation via the Web Interface.) This procedure assumes the HyperIP and the site policies allow it network access to the workstation.

**NOTE:** *Configurations saved from HyperIP versions 5.4.6 or earlier will undergo a one-time conversion when restored on version 5.5 or later. Version 5.5 configurations can be saved/restored across HyperIPs running version 5.5 or later, but cannot be restored on previous HyperIP versions.*

1. From a Windows workstation, direct your web browser to the IP address you set on the HyperIP management port.
2. Enter the admin password then go to the "File Downloads/Uploads" page enter the configuration filename or click <Browse> to select the appropriate configuration file from your workstation. Then click <Send File>.
3. Now, go to the "Maintenance" page. On the "Maintenance" page, find the "Config Save/Restore" section.
4. Select "**hard disk**" from the first drop down box.
5. Enter the file name of the saved configuration to restore in the "**Save/Restore File**" field.
6. Select "**Restore Config from File**" and click on <Go> to restore the configuration.

7. Check the results in the right frame and follow the instructions to complete the restore. (Typically a reboot is required.)

## Downloading Software Updates (Patches)

The following steps document the procedure to update HyperIP with a software patch (Patchxxxx.nex) from Network Executive Software, Inc.'s website. This procedure assumes the workstation which manages the HyperIP has Internet access.

In general, configuration should be saved, the update file is staged on a local workstation, and the backup/standby HyperIPs are updated, (and rebooted if necessary). Then, the active/master HyperIPs can be restarted to force a failover to the standby HyperIPs so they can be updated (and rebooted if necessary).

1. Review the appropriate Release Notices and Updates for information regarding the update before downloading the update to set the proper expectations for the update by going to <http://www.netex.com> and following the Support tab to Products and then to HyperIP. Choose the Updates link for the appropriate release of HyperIP (i.e. 5.5.3).
2. It is strongly recommended that the HyperIP's configuration is saved on removable media or the HyperIP hard disk and then moved to the workstation. (See the operational procedure "Saving HyperIP Configuration" on page 70 for more details.)
3. Select the Update to expand the description and pre-requisites. Click on the update link or copy and paste the URL into your browser; be sure it starts with *https://* and ends with *.nex*. Save this file on your workstation (and remember the location it is stored).
4. Now point your web browser to the backup/standby HyperIP, and enter the admin password.
5. Go to the "File Downloads/Uploads" page and click <Browse> to find the update file stored on your workstation in Step 3 above. Select Send file.
6. Go to the "Maintenance Page", in the "HyperIP Code Updates and Images" section, select "**List Available Updates**" and click the <Go> button. The update file which was retrieved should be listed in the right frame.
7. To install the code update, set the "**Update or Image file**" to the name of the update to install (i.e. Patch-xxxx.nex).
8. Select "**Install Update File**" from the drop down menu and click on the <Go>. The update may take several minutes. The results will be displayed in the right-hand frame when complete.
9. Once you receive confirmation that the update has been completed, follow the update instructions related to this update (i.e. may require a restart or even a full REBOOT of the HyperIP). Then follow the directions at the beginning of this procedure to update the AHS master HyperIP at this site, if appropriate.

## Upgrade (Image Restore) Procedure

The following steps document the process to install a new software version (system image) from Network Executive Software, Inc. on the HyperIPs. This procedure assumes the workstation which manages the HyperIP has Internet access.

In general, configuration should be saved, the image is staged on your workstation, the AHS backup/standby HyperIPs have the upgrade installed, and rebooted first. (This insures the new image that was installed starts (boots) up successfully before installing on the active/master HyperIPs.) Then, the ac-

tive/master HyperIPs can be restarted to force a failover to the standby HyperIPs so these can then have the new image installed and rebooted.

The following show the steps involved to retrieve the image and install them on a HyperIP from your workstation:

1. Review the appropriate Release Announcement and FAQs for information regarding the new install image before downloading the image to set the proper expectations for the update by going to <http://www.netex.com> and following the Support tab to Products and then to HyperIP. Choose the Docs link for the appropriate release of HyperIP (i.e. 5.5.3).
2. Request a download by email to [support@netex.com](mailto:support@netex.com). The response will include a time sensitive link to download the HyperIP image to your workstation. Save the upgrade file (.iso) on your workstation (and remember the location it is stored at).
3. It is strongly recommended that the HyperIP's configuration is saved on removable media or the HyperIP hard drive and then moved to the workstation. (See the operational procedure "Saving HyperIP Configuration" for more details on page 70.)
4. Point your web browser to the (AHS backup/standby) HyperIP, and enter the admin password.
5. Go to the "File Downloads/Uploads" page and click <Browse> to find the upgrade (.iso) file stored on your workstation in Step 2 above. Select Send File.
6. Now, go to the "Maintenance Page", select the upgrade filename (.iso from Step 2) from the drop down menu next to <cleanupImage> and click <installImage>. This will install the upgrade image on the 'other' partition, (not overwrite the currently running partition) and may take several minutes. The results will be displayed in the right-hand frame when complete.
7. In order to have this upgrade be running, the HyperIP needs to be configured to start/boot from the 'other' partition with a Configuration file. (This start/boot setting is only temporary so you can verify the successful startup on the other partition.) Select the Config ID of the configuration file you wish to use (i.e the one you saved before the upgrade) on the 'other' partition. Click on the <AltTemp> button.
8. When ready to restart/reboot to test your new image, select the "Reboot" menu item from the SERVICES on the top left frame and click on the <Service Apply> button. This will take a few minutes. After a few minutes you can reload your browser page.
9. The upgraded HyperIP will now be operational. When you are satisfied with the new image, you need to make this the images that will always startup when the HyperIP is rebooted or restarted. Go to the HyperIP Maintenance Commands page, to the HyperIP Code Updates & Images section in the middle of the left frame. Select "**Set Curr Boot Partition Perm**" in the drop down menu next to the <GO> and click on the <GO> button. This makes the current partition the startup partition.

## Switching Partitions – General Case

If you are testing a new software image and would like to switch back to the other partition, the following are general definitions and command line interface commands to perform these tasks. The current partitions are named sda3 and sda4.

- The "Current" partition is always the partition that you are running now.

- The “Alternate” partition is always the partition that you are NOT running from.
- setBootAltTemp, without a configuration name, will always setup the partition that you are NOT running to be booted the next time and will use the configuration that was last running (Factory Defaults if not prior operation).
- setBootAltTemp, with a configuration name, will always setup the partition that you are NOT running to be booted the next time and will use the configuration data from the file specified.
- setBootCurrPerm will always set the partition that you are running now as the permanent boot partition.
- Use the Display Product Information command found on the Maintenance webpage to see the version of software on each partition. This command is documented on page 56.



# HyperIP Appliance

## Chassis Description

To date, HyperIP has been distributed in the following hardware models. All models are a 1U rack-mountable chassis with slide rails.

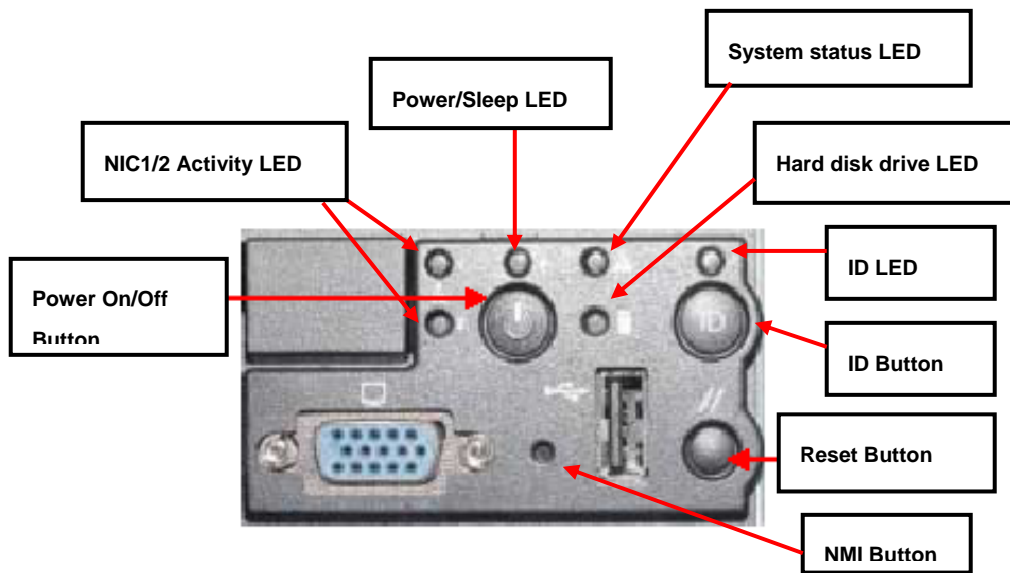
Model Number	Maximum Throughput	Power supply	Floppy/CD/DVD available	Rail Kit
<b>10XY</b> 1000, 1001, 1002, 1003, 1010, 1011, 1012, 1013	455Mb/s	350w 100-127 volts 50-60 Hz 4.96 amps 200-240 volts 50/60 Hz 2.48 amps	Floppy and CD only	Fits only these models
<b>11XY &amp; 12XY</b> 1112, 1110, 1212, 1210	550Mb/s	500w 100-127 volts 50/60 Hz; 4.96 amps 200-240 volts 50/60 Hz 2.48 amps	CD only	Fits only these models
<b>13XY &amp; 14XY</b> 1310, 1312, 1410, 1412	800Mb/s	650w 100-127 volts 50-60 Hz 4.96 amps 200-240 volts 50/60 Hz 2.48 amps	CD/DVD only	
<b>15XY</b> 1520, 1522	800Mb/s	600w 100-127/200- 240 Vac 50/60 Hz 5.5/2.5 A amps	CD/DVD only	

**Figure 25: HyperIP Hardware Model Differences**

To install the bezel on the front panel of the appliance, place the bezel between the chassis handles and push it toward the front of the chassis until it snaps into place. To lock the bezel, insert the key into the

lock. Turn the key clockwise until it stops (about a quarter turn). The bezel is now locked and cannot be opened.

Figure 25 illustrates the locations of the indicators and controls on the right side, front panel of the appliance. To prevent unauthorized access to the system's peripherals and control panel, a key locks the bezel to the front panel. To unlock the bezel, insert the key into the lock and turn the key counter-clockwise until it stops (about a quarter turn). The bezel is now unlocked and can be opened.



**Figure 26: Control Button and Status LED Locations**

The following figures define the usage and meaning of the indicators and buttons on the front panel of the HyperIP appliance.

Button	Description
Power On/Off	Toggle system power on/off
ID Button	Toggles front panel ID LED and baseboard ID on the rear of the chassis (may be controlled by software)
Reset Button	Reboots and initializes the system
NMI Button	When pressing the recessed button with a pin or paper clip, issues a non-maskable interrupt and puts the system into a halt state.

**Figure 27: Control Button Functions**

LED	Description
Power/Sleep LED	Continuous green indicates the system has power applied. Blinking green light* indicates the system is sleeping. No light indicates system does not have power (other than 5V standby)
Hard disk drive status LED	Random blinking green light indicates hard disk drive activity. Continuous amber light indicates hard disk drive fault. No light** indicates no hard disk drive activity or fault.
System status LED	Continuous green light indicates system is operating normally. Blinking green light indicates the system is operating in a degraded condition Continuous amber light*** indicates the system is operating in a critical or non-recoverable condition. Blinking amber light*** indicates the system is in a non-critical condition. No light indicates POST/system stop.
ID LED	Continuous blue light indicates ID button is depressed or light turned on by software. No light indicates button is not depressed.
NIC 1 Activity LED NIC 2 Activity LED	Continuous green light indicates a link between the system and the network to which it is connected. Blinking green light indicates network activity.

\* The power LED is maintained on standby (by chipset). If system is powered down without going through BIOS, the LED state in effect at the time of power off will be restored when the system is powered on until the BIOS clears it. If the system is not powered off normally, it is possible that the Power LED will be blinking at the same time as the System status LED due to a failure or configuration change that prevents the BIOS from running.

\*\* Also off when Power is off or in sleep mode.

\*\*\* The amber status takes precedence over the green status. When the amber LED is on/blinking the green LED is off.

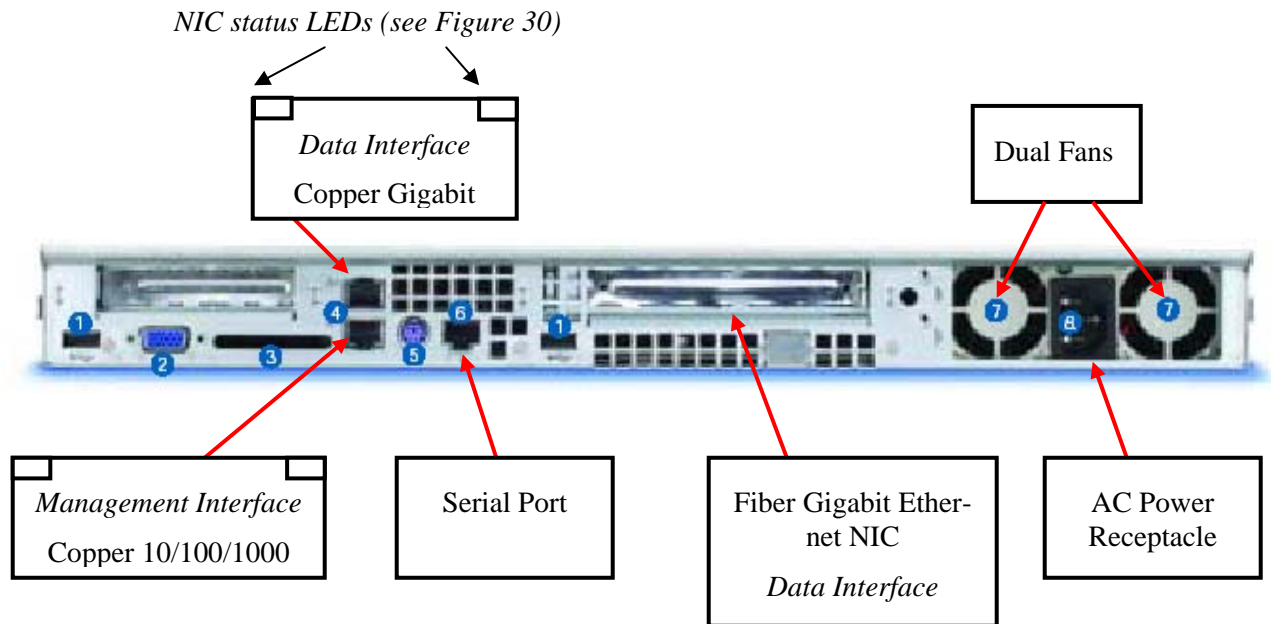
**Figure 28: LED Status Indicators**

## Power

- **WARNING: The button on the front panel does not turn off AC power. To totally remove power from the appliance you must unplug the AC power cord from the wall outlet or the chassis.**
- **Do not attempt to modify or use the supplied AC power cord if it is not the exact type required.**
- **The power supply cord is the main disconnect to AC power. The socket outlet must be installed near the equipment and readily accessible.**

If the power cord supplied with the system is not compatible with the AC wall outlet in your region, one that meets the following criteria must be obtained:

- The cord must be rated for the available AC voltage and have a current rating that is at least 125 percent of the current rating of the appliance.
- The plug on the power cord that connects to the power receptacle must be a grounding-type male plug designed for use in your region. The plug must have certification marks showing certification by an agency acceptable in your region.
- The connector that plugs into the AC receptacle on the power supply must be an IEC 320, sheet C13-type female connector.
- In Europe, the cord must be less than 4.5 meters (14.76 feet) long, and it must be flexible <HAR> (harmonized) or VDE certified cordage to comply with the chassis' safety certifications.

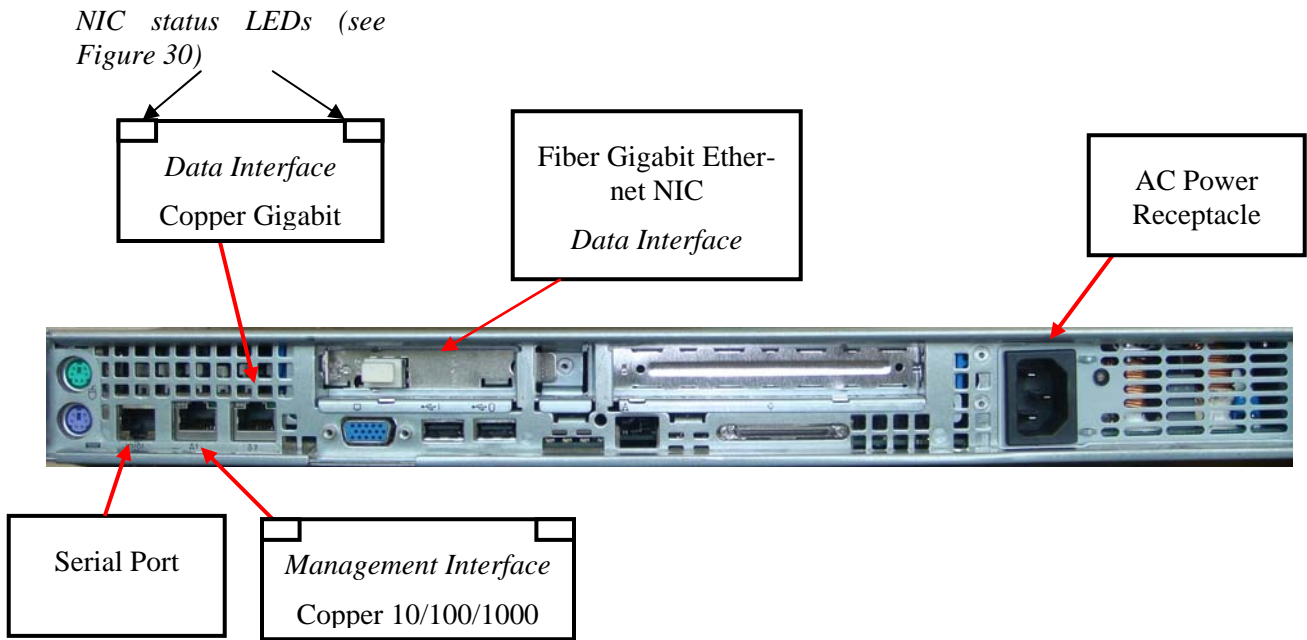


Connectors 1, 2, 3, and 5 are not used for HyperIP operation or maintenance.

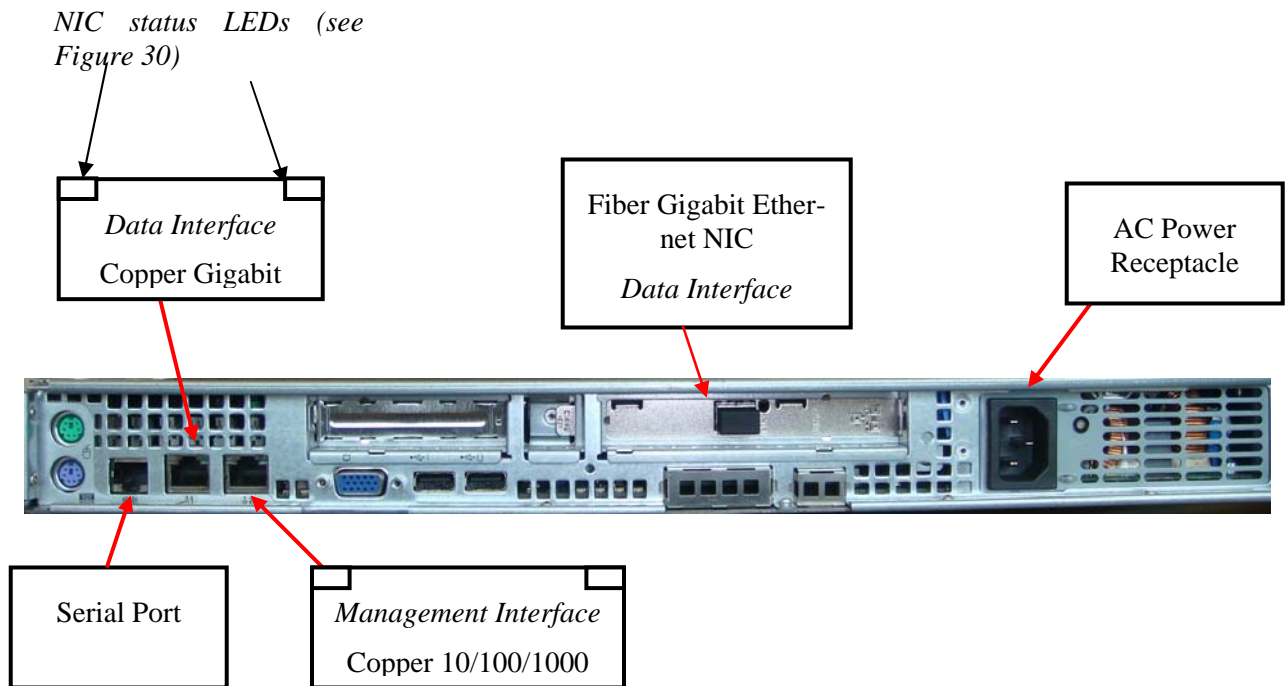
**Figure 29: View of Rear Panel for Models 10XY**

LED Color	LED State	NIC State
Green/Amber (Left)	Off	10 Mb/sec
	Green	100 Mb/sec
	Amber	1000 Mb/sec
Green (Right)	On	Active Connection
	Blinking	Transmit/Receive Activity

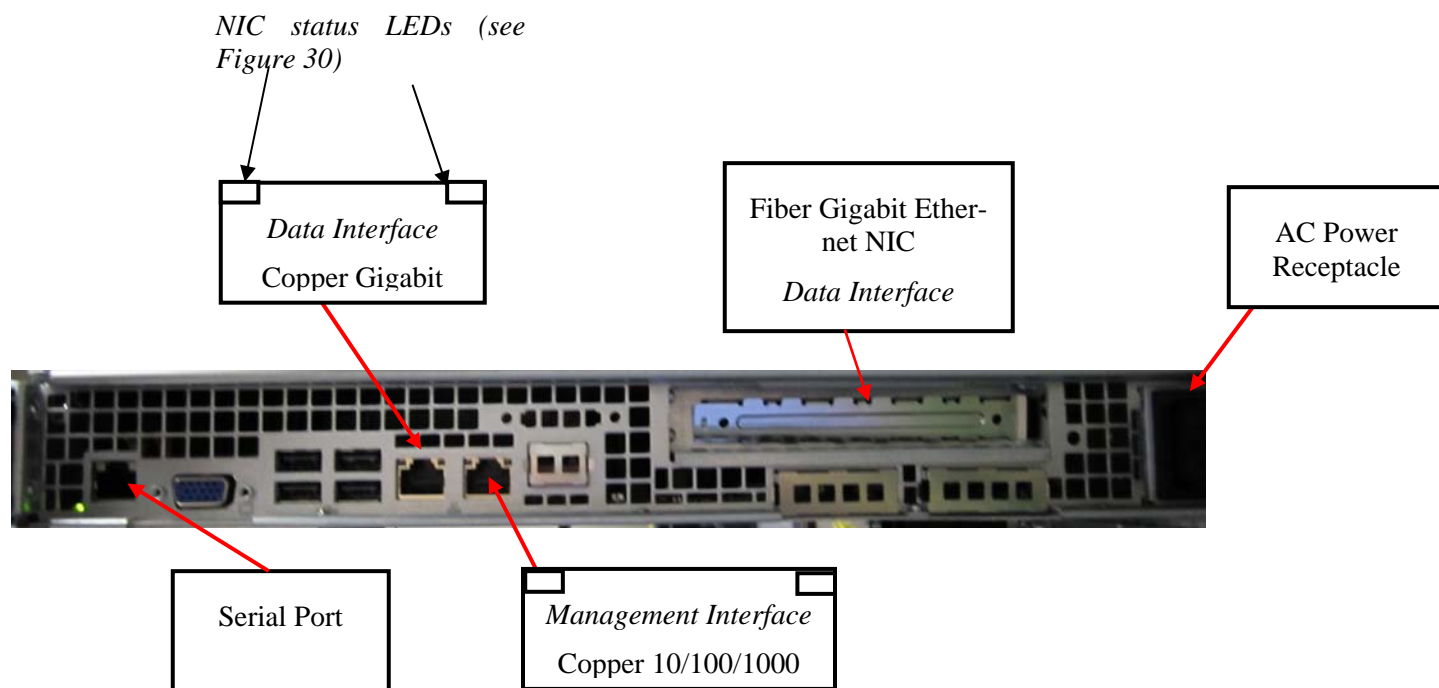
**Figure 30: NIC Status LEDs on Ethernet NIC Connectors**



**Figure 31: Drawing of Rear Panel for Models 11XY, 12XY**



**Figure 32: Drawing of Rear Panel for Models 13XY, 14XY**



**Figure 33: Drawing of Rear Panel for Models 15XY**

## Powering Off the Appliance

When the system has been “quiesced” through the legacy dialog or <*Shutdown*> from the web browser interface, power can be turned off by depressing the Power On/Off button. Refer to the diagram Figure 26, for the location of the buttons on the front panel (under the security faceplate).

## Agency Certifications

Contact [support@netex.com](mailto:support@netex.com) for agency certifications for all HyperIP Models.

# Customer Troubleshooting

**NOTE:** The following procedures apply to HyperIP Release 5.5 and above.

## Accessing HyperIP

Open a browser window, connect to HyperIP using HTTP or HTTPS, and enter the hipadmin password. The default password is *hipadmin*.

**NOTE:** During the course of troubleshooting, if it becomes necessary to reset the HyperIP appliance, the browser sessions will obviously be disconnected.

The following features and HyperIP components may prove useful in trouble shooting problems.

## Statistics

HyperIP provides session-level statistics. Input/Output character counts and message counts are maintained. Statistics may be gathered while HyperIP is running by issuing the command “Display HyperIP State” which is available on the Maintenance Commands Page. For more information on the “Display HyperIP State” command, see the section “Troubleshooting using the Display HyperIP State Command” on Page 88.

HyperIP also provides performance graphs with hourly, daily, weekly and monthly displays.

## Informational Logs

Several logs are maintained in HyperIP. Each internal component maintains a separate log as well as a system log. HyperIP’s transport maintains a **Transport.log** file and the HyperIP application maintains a **Base.log** file to record related events. These logs can be instrumental in diagnosing a problem. The system, transport and base logs are accessible via the HyperIP web browser interface from the Maintenance page (Misc commands). The logs may either be “tailed” or completely displayed.

## System Dumps

System dumps are created by the “diagInfo” utilities selection in the drop down menu in the Save and Upload Diagnostic Information on HyperIP’s “Diagnostic” browser screen. Once the dump is taken, it should be moved to your workstation, via the File Downloads/Uploads page and then to Network Executive Software’s ftp server (<https://ftp.netex.com/upl>). Diagnostic dumps should be taken from all HyperIPs in question. **IMPORTANT NOTE:** *If the connection between HyperIP appliances is not operational, the dumpdiaginfo command may require several minutes to complete.*

## System Log

The system logs events in a file named messages. These events may indicate errors or merely normal events. This log should be scanned to determine if there are unusual events logged, or missing events. Messages indicating driver events, logins, interface changes, and service changes are logged here. It is helpful to become familiar with this file on a normal, operational HyperIP in order to determine differences when HyperIP is not working.

In order to find the last time the system was restarted, go to the bottom and scroll up until “restart” is located. That will be the last restart, and new events follow the restart.

The system log file is aged out when full, i.e., when the log is full (or by operator command), the name is changed to “messages.1” and a new “messages” file is opened. If “messages.1” already exists, it is renamed “messages.2” etc, until “messages.5” is discarded and “messages.4” is renamed “messages.5.” Only the current system log (messages) file is viewable via the browser, although all messages log (system log) files are captured in a system dump.

## HyperIP Base Log

The HyperIP application logs events in **HyperIP base log**. As in the system log, these events may indicate errors or merely normal events. When there is a problem, this log should also be scanned to determine if there are unusual events logged, or typical events missing. Events such as HyperIP startup and shutdown, TCP connections, configuration changes, and license changes are logged here. It is helpful to become familiar with HyperIP’s **base.log** file on a normal, operational HyperIP in order to determine differences when HyperIP is not working.

If the HyperIP has stopped working, the last lines in this file will typically show why.

As with the system log (the messages file), there may be multiple instances of the HyperIP log (.1, .2, .3, etc.). Up to 31 log files are saved in HyperIP. Only the current instance of hyperip.log is viewable via the browser, although all log files are captured in a system dump.

### HyperIP Transport Log

This log contains information regarding HyperIP’s transport. Messages in this log are specific to events on the network connecting the HyperIP appliances.

## Troubleshooting via the Web Browser Interface

The Help buttons for each page provide more detail regarding the items available on that page. The descriptions in this section are specific to displays available for troubleshooting. On the panels which include configuration information, such information should be verified when troubleshooting.

### Diagnostic Page/Traceroute

On the diagnostic page, an IP address may be entered and the traceroute button clicked. This command issues a series of “pings” and “traceroutes” to the IP address entered, and displays the results.

Also available for diagnosing configuration issues, is a utility which measures the available capacity of the WAN connection between the HyperIPs.

Performance graphs are available on the diagnostic page. The SNMP data is sampled every minute. They are automatically aggregated into the number of intervals that fit in the graph size:

- 60 intervals for the last hour,
- 120 intervals for the last day,
- 140 intervals for the last week,

- 155 intervals for the last month

This page has another utility which is useful at initial installation and assists in determining the optimum *segsize* for HyperIP transport. This segment is the largest amount of data to be retransmitted in the case of a packet lost in the WAN.

HyperIP dumps are initiated and uploaded to a server accessible to HyperIP from this page also.

## Advanced Web Page

From this page, static IP routes may be examined. Routes need to be set such that the HyperIP appliances can communicate with each other and with the local hosts they are optimizing traffic for.

This page contains a button <SiteTune> to launch a frame to further tune how HyperIP optimizes traffic to specific remote sites. The launched frame contains a <helpParms> button which provides information on setting these parameters.

## System Config Page

From the "System Config" page, traceroute commands may be executed, the interface configuration may be examined (or altered), and HyperIP's managed access options can be configured.

## Problem Isolation/Resolution

This section of the Reference Manual is intended to provide general guidelines for troubleshooting HyperIP problems. It is NOT an exhaustive, "catch-all" that will definitively determine the resolution to every problem encountered, but hopefully, will provide suggestions and recommendations useful in resolving issues. Also refer to the section "Troubleshooting using the Display HyperIP State Command" on page 88.

Due to the nature of the HyperIP product, it is likely problems will fall in one of the following areas:

1. Hardware problem (for NetEx supplied Hardware)
2. Cannot Access HyperIP to Perform Initial Configuration
3. Cannot Access HyperIP Web Interface after Initial Configuration
4. Cannot communicate between HyperIPs
5. Applications cannot communicate to or through HyperIP
6. Performance between the peer applications is not as expected, or has suddenly deteriorated.

Each of these potential problem areas is discussed in the following sections.

### Hardware Problem For NetEx Supplied Hardware Platform Only

The HyperIP hardware platform supplied by NetEx is a 1U appliance with a hard drive mainly used for software storage and logging. It has a single power supply and fan assembly, with two 10/100/1000 copper Ethernet ports on the motherboard. (One is used only as a management interface.) A gigabit fiber Ethernet NIC is also part of the configuration, and may be optionally configured for use as the data port.

In many instances it may be possible to determine that the hardware platform is defective. Some examples are: power supply failure, hard drive crash, or Ethernet interface inoperable. HyperIP hardware failure service policy is return to factory warranty replacement; *the entire appliance is the ONLY Field Replaceable Unit (FRU)*.

The following is a short list of things to check to determine if the NetEx supplied hardware platform is operational or not. If the system exhibits any of these behaviors, the appliance most likely has a hardware problem and should be returned.

1. Although the appliance is plugged in and has power, no lights can be seen from the front or the rear of the appliance. Note: *that the network lights are not an indicator.* (Faulty power supply)
2. The system does not boot up or display a logon prompt when a terminal is connected to the serial port. (Faulty hard drive and/or system).
3. System boots up, but the network interface is not responding, isn't found, or does not respond to a ping or telnet request from a locally attached PC. Attach a terminal to the serial port, and use the CLI showInterface and showRoute commands to ensure the Ethernet ports are properly configured and active. (Faulty Ethernet interface, cable and or switch port).

NOTE: Failure to respond to a ping or telnet request can also be caused by HyperIP's maintenance access settings blocking the packets (configuration issue).

4. Red warning indicator LED's may be illuminated. These LED's can be seen through the air flow slots on the rear panel of the machine. (Faulty system, hard drive, and/or power supply)
5. In all cases of hardware failure, the appliance must be replaced. Before returning the hardware, an RMA number must be obtained. Call, or contact via email, Network Executive Software, Inc. support and request an RMA number..

## Cannot Access HyperIP to Perform Initial Configuration

If you cannot get to the HyperIP to perform the initial configuration steps, verify the following:

- HyperIP is powered up.
- HyperIP network interfaces are connected to the LAN switch.
- Your management workstation's network interface settings are appropriate to communicate to HyperIP.
- Your management workstation's network routes.

If you still are having problems performing the initial configuration contact [support@netex.com](mailto:support@netex.com).

## Cannot Access HyperIP Web Interface after Initial Configuration

Verify the network is connected and that the HyperIP is powered up. Be sure to use HTTPS for your browser.

Login to HyperIP (via serial port or VM console). Using the CLI:

- showRestarts – if there are perform pending restarts
- showInterface – to verify the Interface settings are correct
- showRoutes – to verify the network routes are correct

If you still are having problems contact [support@netex.com](mailto:support@netex.com).

## Cannot communicate between HyperIPs

Each HyperIPs must be properly configured in order to optimize IP traffic. Basically, each appliance must have an IP addresses assigned, the appliances must "know" the IP addresses of its peer, and the applica-

tion servers must be configured to direct traffic to HyperIP. Consult the configuration sections beginning on page 5 for detailed information on HyperIP configuration

ON EACH HyperIP:

HyperIP network(s) interfaces are connected and the HyperIP is powered up. Then via the web interface, verify the following:

Display HyperIP State to verify the HyperIP software is started. If not, verify HyperIP License Key is installed and valid.

The Display HyperIP State should show the current state as ACTIVE for each configured and started remote site.

Verify sites are configured and started. If not started, start them.

Verify your network allows UDP port 3919 traffic.

Verify the network routes are correct.

If any changes have been made, check for pending restarts.

If you still are having problems contact [support@netex.com](mailto:support@netex.com).

## Applications Cannot Communicate To or Through HyperIP

Each HyperIP must be properly configured in order to optimize IP traffic. If the HyperIPs are not communicating with each other refer to xxxxx. Once you have verified the HyperIPs can communicate with each other, follow these steps to diagnose a problem with the applications not communicating to or through HyperIP.

- Use traceroute utility on the HyperIPs and in the local nodes to test access between HyperIPs and local IP nodes.
  - If traceroute fails, ensure the HyperIP Access Settings permit ping on the data interface. Verify route settings allow access between local IP nodes.
  - If changes are made in the HyperIPs, check for pending restarts.
- In the HyperIPs verify intercepts and/or proxies are correct. If not, make the corrections and check for pending restarts.
- Run <Measure HyperIP Path> on each of the HyperIPs independently. This utility is launched from the Diagnostic Commands Page. (Note: this may not run on links below 2Mb/s)
- Check Bandwidth Schedule on each HyperIP to ensure adequate bandwidth is scheduled for this site at this time.
- Run <Start SegTest> on each of the HyperIPs, independently. This utility is launched from the Diagnostic Commands Page. Set the parameters as follows: start 1000 end 32000 increment 4000 1MB per pass.
  - If necessary, change the segsize for this site to the recommended value, by deleting and then re-adding the site with the new segment size.
- If you are running in an AHS configuration, verify that only one HyperIP at each site has the Master Role. If a site shows more than one as Master, reboot one of the HyperIPs.
- Check each HyperIP Connect Log to see that expected IP connections are being logged.

- Check each HyperIP System Log for TCP errors.
- Use HyperIPs TCPdump utility to view the connection activity to HyperIP.

If you still are having problems contact [support@netex.com](mailto:support@netex.com).

## Poor Performance across the Network

Once connections have been established, other problems could arise which can result in less than expected performance between the host applications which are to be optimized.

- 1) HyperIP retransmits due to:
  - a) Over-estimation of the available bandwidth,
    - i) HyperIP calculates the available bandwidth by attempting to send as much data as possible, increasing the send rate until errors are detected. When errors are detected, the send rate is decreased until there are no errors, then increased to just under the error threshold. The current send rate may be displayed by:
      - (1) **NOTE:** This check is best accomplished via the browser interface. From the browser Maintenance panel, issue the command “Display HyperIP State.” The throughput rate is in the Mbits/s Current and is displayed in megabits per second. The throughput rate should closely match the bandwidth available between appliances.
      - (2) The send rate is adjusted lower due to circuit conditions such as; errors on the link, jitter (variations in round trip delay time), and congestion. When these conditions are present, performance may be degraded slightly.
      - (3) The HyperIP “Diagnostics” page contains tests to evaluate the network between HyperIPs. Both of the following tests should be run when performance issues occur. The HyperIPs should not be running any user traffic when these tests are run.
        - (a) “Measure HyperIP Path” is used to calculate the total and available bandwidth between HyperIPs. This test can validate the bandwidth available between HyperIPs and how much of that bandwidth is available for new application.
        - (b) “Segment Size Test” determines throughput rates for various-sized UDP packets and is useful to determine the appropriate HyperIP segment to be used for this link.
  - b) limited buffers in intermediate nodes,
    - i) Some network nodes may have limited buffer space which could severely restrict HyperIP performance due to dropped packets. If this is the case, HyperIP can be tuned to prevent overdriving such nodes. Tuning could consist of limiting the size of the data “pipe” between the appliances. Size of the pipe is tuned by use of the “bufolimit” and “maxkbitspersec” parameters described below. Run the diagnostic tools to tune HyperIP to the network.
    - ii) Switch or router buffers may be increased; refer to specific vendor information.
  - c) Rate limiting equipment, such as ATM switches with fixed CBR or UBR (committed bit rate, or uncommitted bit rate) etc.
- 2) Incorrect Network Configurations such as Half/Full duplex mismatches in the network.
  - a) Make sure attached network equipment is able to support the speed and duplex settings in HyperIP. HyperIP’s default is auto-negotiate but this setting may be changed during configuration of the appliance. Some switches do not auto-negotiate well, and so HyperIP should be set to full-duplex, 100 (or 1000) mbps. On copper Ethernet interfaces, improper setting of auto-negotiate will cause framing and/or CRC errors on the segment on which HyperIP is connected.
  - b) View Raw Interface Stats on the Maintenance Commands web page for errors and negotiated speed and duplex states.

- c) Verify end-to-end connectivity, and round trip delay times, by issuing pings and/or trace-route/tracert without, then with HyperIP in the path.
- d) Issue pings with data sizes greater than the default. Consult the documentation on the particular server being used to issue the pings, for example on RedHat Linux, the ping command with 4Kbytes of data is “ping 10.1.2.50 -s 4096.”
- e) Ensure all network segments are able to run at the configured speed. i.e., if HyperIP is configured as 1000 Mbps (gigabit Ethernet) all segments in the path must be capable of supporting gigabit speeds. i.e., the total speed of the network will not be faster than that of the slowest segment.
- f) If the fiber interface is being used, and there is a speed mismatch, the fiber “active” indicator will not illuminate. (Note: Auto-negotiate is not an option for a fiber interface.)
  - o **NOTE:** Several HyperIP transport parameters that may affect throughput are customer configurable. These parameters are changed from the browser, on the Advanced Configuration page, then Site Tuning Parameters. See the section on the site tuning parameters for definitions.

**Important Note:** When troubleshooting HyperIP problems such as performance, it may be worthwhile checking the site tuning parameters to ensure they are not set in such a manner that will degrade, or even prevent, HyperIP communications.

## Troubleshooting using the Display HyperIP State Command

The “Display HyperIP State” command provides information regarding the HyperIP transport, application connections, throughput, and the general state of the link between HyperIP appliances. The following screen shot provides a sample output of this command:

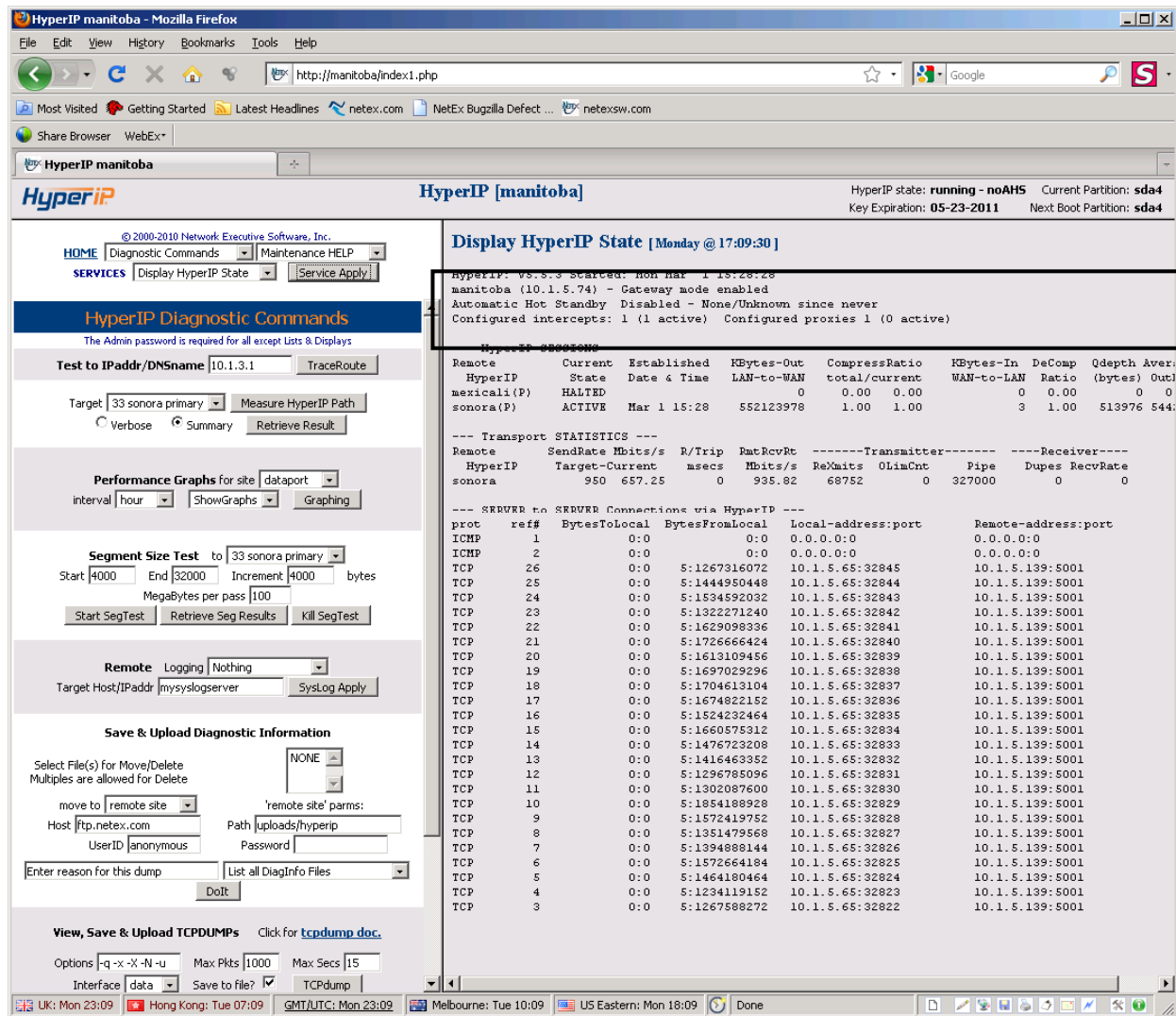


Figure 34: Display HyperIP State Command Output, Part 1

An explanation of the fields in the **outlined** section follows:

The first line of the display indicates the version of the HyperIP software currently running and the date that HyperIP was last started.

*Viewing this line is useful when verifying a code update has taken effect and to determine the up-time of the HyperIP software.*

The second line is the HyperIP data interface IP address and indicator whether Gateway mode is enabled or not.

The third line shows the state of this HyperIP appliance when running Automatic Hot Standby (AHS). When running AHS, there should always be one HyperIP as active/master and one standby/backup on each side of the WAN. If the time this appliance has been active/master or backup/standby is not close to the uptime indicated by the “started” line, there has been an AHS failover event. A failover occurs because the standby appliance lost communication with the active appliance and took over the active function. Failover may be caused by a HyperIP restart or due to a switch or HyperIP failure.

The fourth line indicates the number of configured and currently-active intercepts and proxies.

Multiple HyperIP appliances in an active/master state is an indication of either a configuration error resulting in a mismatch in the virtual router identifier (VRID), or a loss of communication, between the two appliances.

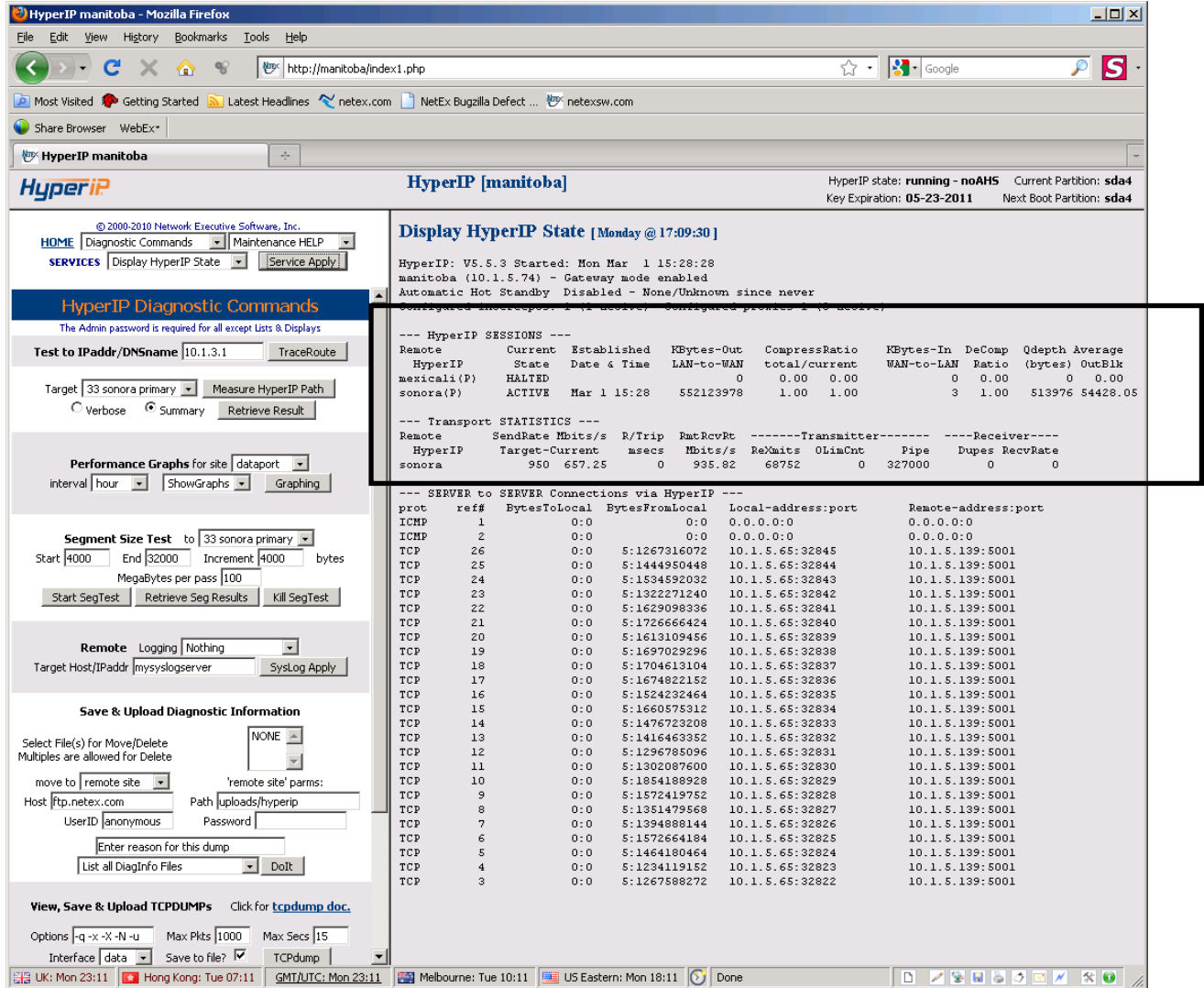


Figure 35: Display HyperIP State Command Output, Part 2

In above figure, the outlined section provides operational status and statistical information for the connections between the HyperIP appliances. Each line represents a connection to a remote HyperIP appliance. If the HyperIP is configured for AHS, there will be two lines since the appliance will establish connections to both remote appliances. If not configured for AHS, there will be a single connection. The following describes the items in the highlighted section:

Title	Definition or Details
Remote HyperIP	The HyperIP appliance, as defined in the configuration, where this connection

Title	Definition or Details
	terminates.
Current State	Current State of this connection. Active state indicates that the connection is established. Any state other than active indicates that the connection is not yet functional.
Established Date & Time	When the connection between HyperIPs was established
Kbytes Out LAN to WAN	Data sent by this HyperIP over each connection from all locally-attached servers
Compressed Ratio Total	Compression ratio for the data sent to the remote HyperIP appliance during the lifetime of this connection. It is useful to view this information when determining an overall data transfer compression ratio.
Compressed Ratio Current	The compression ratio obtained in the last six seconds. The information in this display is used to get the compression ratio of the data being sent now.
Kbytes In WAN to LAN	Data received from the remote HyperIP to be passed on to locally-attached servers.
Decompression Ratio	The compression ratio of the data received from the remote HyperIP appliance during the lifetime of this connection. It is useful to view this information when determining an overall data transfer compression ratio. When viewed with comp_out, the user can get a quick view of the compression ratio of all traffic passing between HyperIP appliances.
Qdepth	Data bytes from locally-attached servers waiting to be sent to the HyperIP transport and then to the WAN.
Average Outblock	The average amount of data per block that the HyperIP is sending to the transport.

**Figure 36: Details for HyperIP State Command Output, Part 2**

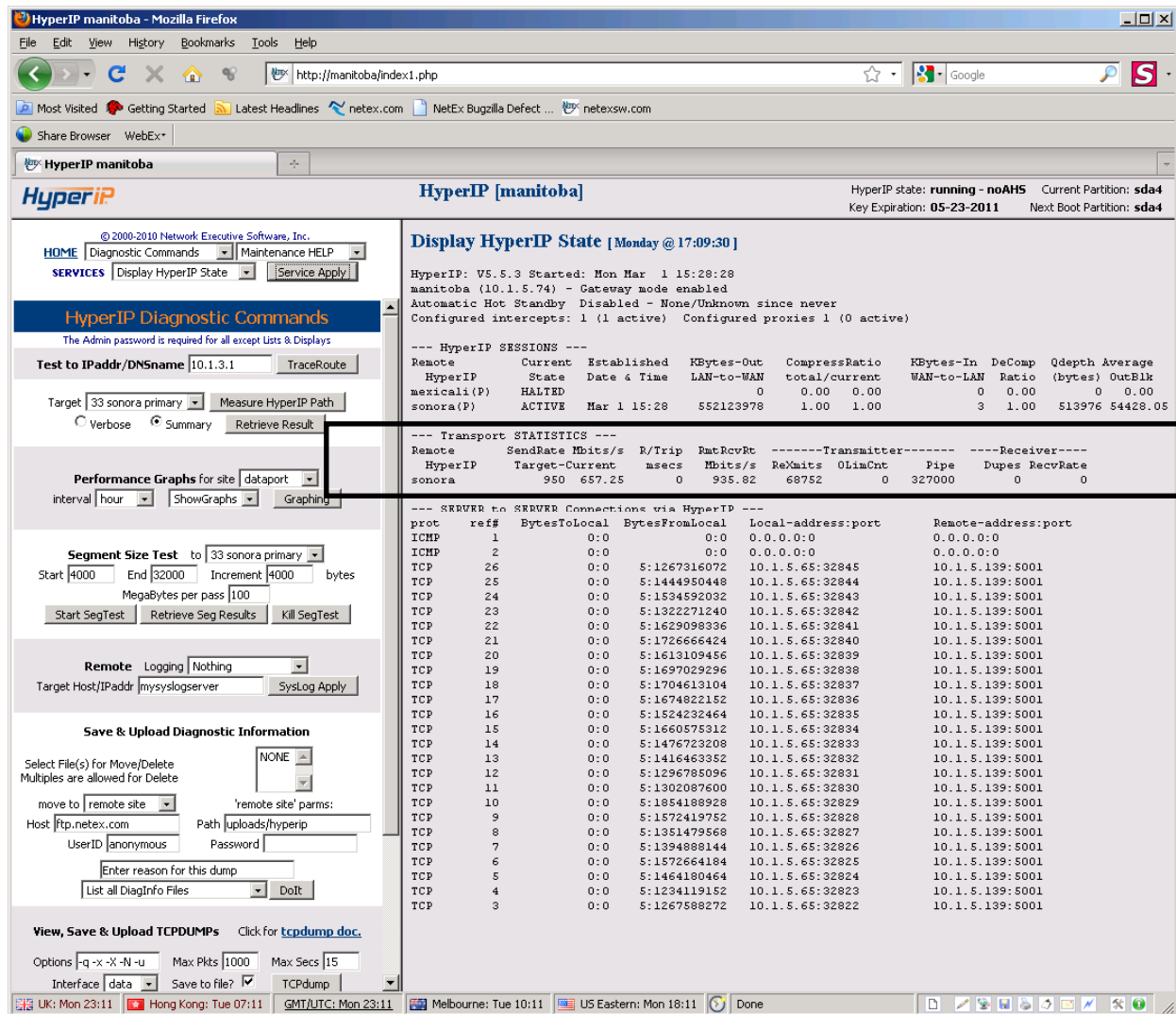


Figure 37: Display HyperIP State Command Output, Part 3

The lines highlighted in previous figure detail the statistics from this HyperIP's perspective for each connected remote HyperIP.

*Note: There should be two lines if this is an AHS configuration, and one line if not.*

This is a good place to look to determine the status of the HyperIP connections, what type of throughput they are achieving and whether the connection is seeing any dropped or out of order packets. Only the active connection will be passing traffic at any given time.

Title	Definition or Details
To HyperIP	The remote HyperIP appliance, as defined in the configuration, where this connection terminates.
Send Rate Target	The data transfer rate which this HyperIP connection is attempting to achieve, in Megabits per second. If the HyperIP transfer is not throttled, this number will usually be above the link bandwidth available. If the HyperIP is throttled

Title	Definition or Details
	by the <i>MaxRate</i> parameter or the bandwidth scheduler, the highest number seen here will be the throttle rate.
Send Rate Current	The rate at which this HyperIP is currently sending data, in Megabits per second.
R/Trip msec	The current round trip time as observed by the HyperIP software in milliseconds.
RmtRcvRt	Megabits per second the remote HyperIP has been able to receive from the WAN and forward to its local LAN. This information is used to determine if this HyperIP connection needs to adjust the send rate up due to bandwidth available or down to avoid overrunning the WAN or the remote HyperIP.
Rexmits	Transmitter Retransmits – The number of HyperIP protocol packets which have been resent due to a negative acknowledgment. Observing whether the retransmit count is increasing over time will indicate if lost packets could be affecting performance.
OlimCnt	The number of times this HyperIP has needed to delay sending data due to the number of outstanding blocks.
Pipe	The Pipe is the calculated amount of data the network can hold between the HyperIPs based on the target send rate and the round trip time (msec)
Dupes	Received Duplicates – The number of HyperIP protocol packets that has been received twice, as reported by this HyperIP. These numbers typically increment because a packet arrived from the network out of order and this HyperIP has already sent a negative acknowledgement for the packet to the remote HyperIP.
RecvRate	The rate at which this HyperIP is receiving data.

**Figure 38: Details for HyperIP State Command Output, Part 3**

The screenshot shows the HyperIP [manitoba] web interface. The main content area displays the output of the 'Display HyperIP State' command. A black box highlights the 'SERVER to SERVER Connections via HyperIP' section, which contains a table of connections.

**HyperIP State Output:**

```

HyperIP: V5.5.3 Started: Mon Mar 1 15:28:28
manitoba (10.1.5.74) - Gateway mode enabled
Automatic Hot Standby Disabled - None/Unknown since never
Configured intercepts: 1 (1 active) Configured proxies 1 (0 active)

--- HyperIP SESSIONS ---
Remote   Current   Established   KBytes-Out   CompressRatio   KBytes-In   DeComp   Qdepth   Average
HyperIP  State     Date & Time  LAN-to-WAN   total/current   WAN-to-LAN  Ratio   (bytes)  OutBlk
mexicali(P)  HALTED   0           0           0.00  0.00           0  0.00           0  0.00
sonora(P)    ACTIVE   Mar 1 15:28  552123978   1.00  1.00           3  1.00           513976  54428.05

--- Transport STATISTICS ---
Remote   SendRate  Mbits/s   R/Trip   RmtRcvRt   -----Transmitter-----   -----Receiver-----
HyperIP  Target-Current  msecs   Mbits/s   ReMbits   OLimCnt   Pipe   Dupes   RecvRate
sonora   950  657.25     0         935.82    68752     0      327000  0        0

--- SERVER to SERVER Connections via HyperIP ---
prot  ref#  BytesToLocal  BytesFromLocal  Local-address:port  Remote-address:port
ICMP  1     0:0           0:0             0.0.0.0:0           0.0.0.0:0
ICMP  2     0:0           0:0             0.0.0.0:0           0.0.0.0:0
TCP   26    0:0           5:1267316072    10.1.5.65:32845     10.1.5.139:5001
TCP   25    0:0           5:1444950448    10.1.5.65:32844     10.1.5.139:5001
TCP   24    0:0           5:1534592032    10.1.5.65:32843     10.1.5.139:5001
TCP   23    0:0           5:1322271240    10.1.5.65:32842     10.1.5.139:5001
TCP   22    0:0           5:1629098336    10.1.5.65:32841     10.1.5.139:5001
TCP   21    0:0           5:1726666424    10.1.5.65:32840     10.1.5.139:5001
TCP   20    0:0           5:1613109456    10.1.5.65:32839     10.1.5.139:5001
TCP   19    0:0           5:1697029296    10.1.5.65:32838     10.1.5.139:5001
TCP   18    0:0           5:1704613104    10.1.5.65:32837     10.1.5.139:5001
TCP   17    0:0           5:1674822152    10.1.5.65:32836     10.1.5.139:5001
TCP   16    0:0           5:1524232464    10.1.5.65:32835     10.1.5.139:5001
TCP   15    0:0           5:1660575312    10.1.5.65:32834     10.1.5.139:5001
TCP   14    0:0           5:1476723208    10.1.5.65:32833     10.1.5.139:5001
TCP   13    0:0           5:1416463352    10.1.5.65:32832     10.1.5.139:5001
TCP   12    0:0           5:1296785096    10.1.5.65:32831     10.1.5.139:5001
TCP   11    0:0           5:1302087600    10.1.5.65:32830     10.1.5.139:5001
TCP   10    0:0           5:1854188928    10.1.5.65:32829     10.1.5.139:5001
TCP   9     0:0           5:1572419752    10.1.5.65:32828     10.1.5.139:5001
TCP   8     0:0           5:1351479568    10.1.5.65:32827     10.1.5.139:5001
TCP   7     0:0           5:1394888144    10.1.5.65:32826     10.1.5.139:5001
TCP   6     0:0           5:1572664184    10.1.5.65:32825     10.1.5.139:5001
TCP   5     0:0           5:1464180464    10.1.5.65:32824     10.1.5.139:5001
TCP   4     0:0           5:1234119152    10.1.5.65:32823     10.1.5.139:5001
TCP   3     0:0           5:1267588272    10.1.5.65:32822     10.1.5.139:5001

```

Figure 39: Display HyperIP State Command Output, Part 4

The previous figure highlights the local packet statistics for which HyperIP is accelerating.

There are always two ICMP entries representing statistics for (ref #1) only messages coming in on the local network, and (ref #2) is only messages received from the WAN and sent out the local network. All ICMP messages optimized by HyperIP will be indicated in these two entries.

Following the ICMP entries are the UDP and TCP data statistics. If there is no UDP or TCP traffic being optimized by HyperIP, the message “No Current Connections” will be displayed.

Information for the TCP/UDP connections is defined in the following table.

Title	Definition or Details
prot	Protocol – Whether this connection is using UDP or TCP.
ref	Reference – An internal HyperIP identifier used to track this specific source IP address, port and destination IP address, port connection.
Bytes to local	Bytes sent by this HyperIP to the local host
Bytes from local	Bytes received by the HyperIP from the local host
Local address and port	The IP address on the local LAN with which this HyperIP appliance is communicating. The local reference does not indicate which IP address initiated the connection or in which direction traffic is flowing. Port – Identifies the UDP or TCP port used with the local IP address for this connection.
Remote address and port	The IP address on the remote LAN with which the remote HyperIP appliance is communicating. The local reference does not indicate which IP address initiated the connection or in which direction traffic is flowing. Port – Identifies the UDP or TCP port used with the remote IP address for this connection.

**Figure 40: Details of HyperIP State Command Output, Part 4**

The user can use this portion of the display to verify there are connections established, whether they are expected connections and that the connections are moving data by determining that the byte counts are incrementing. When viewing the display output, it is a good idea to validate that the same connections exist on both of the active HyperIPs.

When monitoring HyperIP, the user is typically verifying that everything is working as desired. Determining answers to the following questions will provide a quick look at whether HyperIP is working properly. Troubleshooting performance issues or outages begins by looking at the same data:

**What is the operational state of this HyperIP?**

View the top of the display to determine that the HyperIP is active or passive.

If the HyperIP is standby, view the time that it has been in this state. Under normal operating conditions, AHS failover will not occur. Checking this time against the active appliance can provide information about a temporary outage and where the outage occurred. Whether the HyperIP is active or standby, HyperIP connections should be established, see below for more information on determining the state of HyperIP connections.

If this HyperIP state is active, view additional information in this display answering the questions below.

**Are my HyperIP connections established?**

Examine the information in the middle of the page and verify all HyperIP connections are in the “ACTIVE” state. There should be one connection listed under local statistics for each HyperIP connection. (There will be only one if AHS is not configured. If AHS is configured, there should be two connections displayed under the local statistics.)

If all connections are not in ACTIVE state or expected HyperIP connections are missing, the HyperIP appliances are having difficulty communicating.

If this is the case, log on to all HyperIP appliances and verify the system IP address, static routes and routing tables.

Verify the HyperIP appliances can communicate by using the “Test to IPaddr” facility on the browser “Diag” page.

Validate that the HyperIP configuration contains the proper IP addresses for each HyperIP appliance. Refer to the pertinent sections of this User’s Guide for more information on configuring HyperIP. If no configuration or operational error can be found, contact NetEx support.

If all expected connections are in ACTIVE state, HyperIP appliances are connected and ready to move traffic.

### **Are my HyperIP connections moving data?**

Verify that blocks in and/or block out counts are incrementing for the session which connects to the remote active HyperIP.

If the counts are incrementing, HyperIP is moving data.

If counts are not incrementing, either HyperIP is unable to send data across the WAN, or there are no active connections attempting to send data.

Look at the bottom of the page and verify that the expected connections are displayed and that the byte counts are incrementing.

If connections are shown, and byte counts are incrementing there may be an issue communicating between the two HyperIP appliances or HyperIP may be having trouble communicating across the WAN.

Verify the HyperIP appliances can communicate by using the “Test to IPaddr” facility on the browser “Diag” page.

Compare the number of blocks\_out with the number of retransmits (**Note:** You will have to execute the Display HyperIP State command multiple times for the comparison.) If retransmits/duplicates are counting up, there is a problem on the link (WAN) between HyperIP appliances.

### **At what speed are the HyperIP appliances communicating?**

The rcvrates provide a measure of how much data is being successfully transferred between two HyperIP appliances.

### **What is my compression ratio?**

View the compression ratio entry in the sessions display to determine the compression ratio of all data sent.

### **Are all the TCP and UDP connections I expect established?**

Connections are displayed at the bottom of the page.

If they are not, refer to the troubleshooting section of this document.

## Local System Related Configuration Problems

The following table is a short list of symptoms which could be the result of obscure management system configuration problems.

Symptom	Problem Determination
Email notices are not being received when expected	<p>Look in message log for Sendmail messages:</p> <ol style="list-style-type: none"> <li>If no Sendmail messages – Mail hub or administrator email address not setup</li> <li>If message log entry looks like: <pre>Nov 5 10:19:37 HYPERIP sendmail[21491]: iA5GJaH21487: iA5GJbG21491: DSN: Host unknown (Name server: YOURMAILHUB.com: host not found)</pre> <p>Configured Mail hub cannot be resolved by your nameserver</p> </li> <li>If message log entry looks like: <pre>Nov 5 10:25:25 HYPERIP sendmail[30567]: iA5GPPF30567: to=ADMIN@ADMINDOMAIN.com, delay=00:00:00, xdelay=00:00:00, mai- ler=relay, pri=30399, relay=YOURMAILHUB.com. [10.1.3.1], dsn=5.1.1, stat=User unknown</pre> <p>Configured administrator email user is not correct for the Mail hub</p> </li> </ol>
SNMP Traps are not being received when expected	Trap server cannot be found. DNS server not configured.
AHS failover bouncing between Master & Backup	If your network is running spanning tree routing protocol, you should configure the port where HyperIP appliances are connected to 'PortFast' to avoid failover bouncing due to the lack of communication between the AHS pairs.

**Figure 41: Symptom and Problem Determination Table**



# Appendix A: NRBStat Error Codes

## System Log File

System messages are found in the system log file, which may be viewed by using the browser Maintenance panel, under Miscellaneous Commands. The file can be either “tailed” or viewed completely. Some of the more common error messages and/or codes are detailed in the tables that follow.

## NRBStat Error Codes

The HyperIP transport utilizes a data structure called the NRB (Network Request Block) to pass control and other information within the protocol. If an error occurs, an NRB status code (NRBStat) is generated that describes the error. The following table lists the more common NRBStat codes, with potential actions to take if these error codes are encountered.

Name	NRBStat	Meaning	Action
SUCCESS	0	Normal completion	4
PBUFOVFL	1	Pdata buffer too small to hold data	1
PBUFADDR	2	NRBBUF not entirely within user's memory	1
UBITGTWD	3	NRBUBIT bigger than machine's word size	1
NRBREQBAD	4	NRBREQ invalid	1
BUFGTMAX	5	Buffer size exceeds an implementation-defined maximum.	1
OBUFOVFL	11	Odata buffer too small to hold data	1
OBUFADDR	12	Odata buffer not entirely within user's memory	1
BBUFOVFL	21	Both pdata and odata buffers too small	1
NREFBAD	100	NRBNREF in NRB does not refer to a connection currently in use by the application.	1
ERODMAX	103	Odata is greater than the system maximum	1
NRBINUSE	310	User attempted to reuse NRB before previous request issued with that NRB completed.	1
NETXDOWN	500	HyperIP transport not running on local computer	3

Name	NRBStat	Meaning	Action
UCONNMAX	503	Number of connections requested exceeds implementation-defined limit.	1
NOTAUTH	504	User program not authorized to use HyperIP transport	1
DRAIN	505	HyperIP transport being drained before shutdown	1
SYSCONMAX	511	Number of connections requested exceeds total allowable system wide connections.	1
ABORT	512	HyperIP transport aborting due to error or operator	1
NOBUFSPC	513	No space to allocate data buffers (level2)	1
NOLICIP	600	No license for IP HyperIP transport	5
NOLICHC	601	license for HYPERchannel HyperIP transport	4
NOLICHCP4	602	No license for protocol 4 over HYPERchannel	1
HY_INTR	666	Internal only: is a HYPERchannel interface	1
DPNOTHRD	700	Could not create a thread	
DPNOLCL	701	no local host defined yet	3
DPDUPLCL	702	lcl host already defined	1
DPDUP	703	host already defined	1
DPNHOST	704	mod/del host not found	1
DPNUMINTR	705	Num interfaces invalid	1
DPNOTIMP	706	Not activated in ntx_default	3
DPHOSTMEM	707	Unable to allocate host entry	1
DPINTRFMEM	708	Unable to allocate interface entry	1
DPBADINTRF	709	Bad interface type	3
DPDNSERR	710	DNS lookup failure	3
DPNOTLAST	711	Delete local host before remotes	1
NONRBSPC	913	No space to allocate nrbs (level2)	1

Name	NRBStat	Meaning	Action
NOPAMSPC	914	No space to allocate pams	1
DMAXOUTB	1005	data_length > max out on DWTIRE request	1
DMAXINB	1006	data_length > max in of DREAD request	1
DREFBAD	1100	DREF specified by NRBNREF is not in use or is not owned by this application program.	1
DDATMOD	1101	Datamode invalid or assembly/disassembly cannot be done.	1
ASSDATBD	1102	Associated data bit value does not match presence or absence of data.	1
MSGPLEN	1103	Message proper length not 8-64 bytes	1
DRVPERM	1200	Hardware problem with adapter (it's off, not operational, etc.)	6
DRVTEMP	1201	Adapter reported an error	6
DRVDFREE	1202	I/O halted by DFREE or Adapter release	1
DRVDOWN	1204	Adapter connection lost (DOWN)	6
DREADTO	1300	DREAD or DCONNECT timed out before any data received on the network.	2
DWRITMAX	1304	The number of DWRITE requests outstanding for a single connection exceeds maximum.	1
DREADMAX	1305	The number of DREAD requests outstanding for a single connection exceeds maximum.	1
DDISCED	1306	DREAD or DWRITE when the connection is in disconnect mode	1
ASDGONE	1310	Device service discarded associated data because no DREAD issued in time.	2
MSGPLOST	1311	Message proper(s) lost due to excess demand for driver's resources.	1
DPRIV	1312	User not authorized to request privileged driver services	1
DREFINUSE	1501	A specific DREF is already in use or all driver paths are in use.	1

Name	NRBStat	Meaning	Action
DCONNMAX	1503	The maximum number of user driver attaches allowed has been exceeded.	1
DUNAVAIL	1504	Driver service not directly available to applications programs.	1
DDRAIN	1505	HyperIP transport currently being drained by operator.	1
NODREF	1506	DREF requested does not exist on local host	1
ADPDRAIN	1507	HyperIP transport has been drained - adapter cannot accept requests.	1
DBLKOMAX	1509	NRBBLKO value exceeds maximum allowed.	3
DBLKIMAX	1510	NRBBLKI value exceeds maximum allowed.	3
TBUFMAX	2005	During a WRITE, NRBLLEN exceeds NRBBLKO	3
TNONMAX	2008	During a non-segmented write, NRBLLEN exceeds the segment size	3
TREFBAD	2100	TREF specified by NRBNREF is not in use or is not owned by this application.	1
TDATMOD	2101	DATAMODE field in the NRB not valid for the local host.	1
TODATMAX	2103	The quantity of Odata provided exceeds implementation-defined maximum.	1
TREADTO	2300	TREAD timed out before any data received from corresponding application.	2
TCONACTV	2301	TCONNECT, TOFFER or TCONFIRM issued for a connection that is already established.	1
TREPLY	2302	Reply to a connect indication was neither TCONFIRM nor TDISCONNECT, hence invalid.	1
TREADEXP	2303	TREAD to read confirm or disconnect was expected, but some other request was made	1
TWRITMAX	2304	Number of TWRITE requests outstanding exceeds maximum allowed	1
TREADMAX	2305	Number of TREAD requests outstanding exceeds maximum allowed	1

Name	NRBStat	Meaning	Action
TWBUSY	2306	A TWRITE was issued to a connection that is servicing a remote caller or disconnect	1
TRBUSY	2307	A TREAD was issued to a connection that is servicing a remote caller or disconnect	1
TCONCLOS	2308	A write request was issued against a connection that already accepted a TCLOSE	1
TNORESP	2400	No response received from remote HyperIP transport for DEADTO seconds - connection terminated	2
TRREADTO	2402	Remote application failed to issue TREAD within READTO seconds	2
TREMEXIT	2403	Remote application exited without doing explicit disconnect	1
TCONTO	2500	A connect message was sent repeatedly to remote host, but no response for CONTO sec	2
TCONNMAX	2503	Maximum number of transport connections exceeded	1
TUNAVAIL	2504	Transport service not directly available to applications programs	1
TDRAIN	2505	HyperIP transport currently being drained by operator	1
TPAMBAD	2506	PAM passed to transport not valid	1
TBLKOMAX	2509	Specified value of NRBBLKO exceeds maximum	3
TBLKIMAX	2510	Specified value of NRBBLKI exceeds maximum	3
TCLASSBD	2511	Specified class of service not implemented	1
SBUFMAX	3005	During a WRITE, NRBLLEN exceeds NRBBLKO	3
SREFBAD	3100	SREF specified by NRBNREF is not in use or is not owned by this application.	1
SDATMOD	3101	DATAMODE specified not supported for internal communications	1
SODATMAX	3103	The quantity of Odata provided exceeds implementation-defined maximum.	1
SREADTO	3300	SREAD timed out before any data received from corresponding application.	2

Name	NRBStat	Meaning	Action
SCONACTV	3301	SCONNECT, SOFFER or SCONFIRM issued for a connection that is already established.	1
SREPLY	3302	Reply to a connect indication was neither SCONFIRM nor SDISCONNECT, hence invalid.	1
SREADEXP	3303	SREAD to read confirm or disconnect was expected, but some other request was made	1
SWRITMAX	3304	Number of SWRITE requests outstanding exceeds maximum allowed	1
SREADMAX	3305	Number of SREAD requests outstanding exceeds maximum allowed	1
SWBUSY	3306	An SWRITE was issued to a connection that is servicing a remote caller or disconnect	1
SCONCLOS	3308	A write request was issued against a connection that already accepted an SCLOSE	1
SRREADTO	3402	Remote application failed to issue SREAD within READTO seconds	2
SREMEXIT	3403	Remote application exited without doing explicit disconnect	1
SHALTSREF	3422	A HALT SREF operator command was issued against this session	1
SCONTO	3500	A connect message was sent repeatedly to remote host, but no response for CONTO sec	2
NOPNAME	3501	The PNAME specified is not OFFERed on host specified during SCONNECT	1
PNAMBUSY	3502	PNAME exists but is busy right now	1
SCONNMAX	3503	Maximum number of session connections exceeded	1
SUNAVAIL	3504	Session service not directly available to applications programs	1
SDRAIN	3505	HyperIP transport currently being drained by operator	1
NOHOST	3506	The HOST specified in SCONNECT does not exist on network	1
HOSTUNAV	3507	The HOST exists, but no session level connections currently allowed	1

Name	NRBStat	Meaning	Action
NOPATH	3508	The HOST exists, but no communications path exists between local host and it	1
SBLKOMAX	3509	Specified value of NRBBLKO exceeds maximum	3
SBLKIMAX	3510	Specified value of NRBBLKI exceeds maximum	3
SCLASSBD	3511	Specified class of service not implemented	1
SDRAIN2	3522	offer terminated due to services drained	1
SDRAIN3	3523	remote connect rejected due to services drained	1
NNREFBAD	4100	NREF specified by NRBNREF is not in use or is not owned by this application.	1
NDATMODE	4101	Datamode requested on NWRITE is not supported for intra-host communications. The block will be sent using bit-stream transmission (DATAMODE=0).	1
CHKSUM	4104	The checksum on an incoming driver level message is not correct	2
PDATALEN	4105	The length of Pdata was less than or very different from specified length in message proper	2
NREADTO	4300	NREAD timed out before any data received from corresponding application.	2
NCONACTV	4301	NCONNECT or NOFFER issued for a connection that is already established.	1
NINVCONF	4303	Only the offering side may confirm.	1
NWRITMAX	4304	Number of NWRITE requests outstanding exceeds maximum allowed	1
NREADMAX	4305	Number of NREAD requests outstanding exceeds maximum allowed	1
NWBUSY	4306	An NWRITE was issued to a connection that is servicing a disconnect	1
NRBUSY	4307	An NREAD was issued to a connection that is servicing a disconnect	1

Name	NRBStat	Meaning	Action
NOVCIRC	4403	When processing an NWRITE request, network service found that a virtual circuit between the two applications no longer exists	2
NREFINUSE	4501	The NREF requested is already in use	1
NCONNMAX	4503	Maximum number of network connections exceeded	1
NUNAVAIL	4504	Network service not directly available to applications programs	1
NDRAIN	4505	HyperIP transport currently being drained by operator	1
NPAMBAD	4506	The PAM passed to network for a connection is not valid.	1
NBLKOMAX	4509	Specified value of NRBBLKO exceeds maximum	3
NBLKIMAX	4510	Specified value of NRBBLKI exceeds maximum	3
NCLASSBD	4511	Specified class of service not implemented	1
VCPHYS	4512	During attempt to establish a virtual circuit, a network component physically did not respond	2
VCBUSY	4513	During attempt to establish a virtual circuit, circuit facilities were busy	2
VCEQUIP	4514	During an attempt to establish a virtual circuit, a network component could not honor the request due to equipment failure	2
USERDIED	9001	indication that user process died	1

#### Actions

1. Contact Network Executive Software support.
2. Check the network connection between HyperIP appliances. Insure the physical connections show connectivity, IP addresses are correct, and any firewalls are allowing these IP addresses and UDP port 3919 traffic through.
3. Check HyperIP's configuration. Configuration instructions begin on page 5
4. No action necessary
5. Check for valid license; refer to License Key on page 41 for details on viewing the license.
6. Check the appliance hardware for error conditions.

# System Error Codes

The following table details various system error codes that may be entered in the system log file. The system log can be either “tailed” or viewed completely. Some of the more common error messages and/or codes are detailed in the table that follows.

Name	Code	Meaning	Action
EINTR	4	Interrupted system call	1
EIO	5	I/O Error	1
EAGAIN	11	Try again	1
ENOMEM	12	Out of memory	1
EACCES	13	Permission denied	1
EBUSY	16	Device or resource busy	1
EEXIST	17	File exists	1
ENODEV	19	No such device	1
ENOTDIR	20	Not a directory	1
EISDIR	21	Is a directory	1
EINVAL	22	Invalid argument	1
EFBIG	27	File too large	1
ENOSPC	28	No space left on device	1
ENAMETOOLONG	36	File name too long	1
EPROTO	71	Protocol error	1
E_OVERFLOW	75	Value too large for defined data type	1
ENOTUNIQ	76	Name not unique on network	2
EREMCHG	78	Remote address changed	2
ESTRPIPE	86	Streams pipe error	1
EADDRINUSE	98	Address already in use	1
EADDRNOTAVAIL	99	Cannot assign the requested address	1

Name	Code	Meaning	Action
ENETDOWN	100	Network is down	3
ENETUNREACH	101	Network is unreachable	3
ENETRESET	102	Network dropped connection because of reset	3
ECONNABORTED	103	Software caused connection abort	1
ECONNRESET	104	Connection reset by peer	1
ENOBUFS	105	No buffer space available	1
EISCONN	106	Transport endpoint is already connected	1
ENOTCONN	107	Transport endpoint is not connected	3
ESHUTDOWN	108	Cannot send after transport endpoint shutdown	3
ETIMEDOUT	110	Connection timed out	3
ECONNREFUSED	111	Connection refused	3
EHOSTDOWN	112	Host is down	3
EHOSTUNREACH	113	No route to host	2
EALREADY	114	Operation is already in progress	1
EINPROGRESS	115	Operation now in progress	1

#### Actions

1. Contact Network Executive Software support
2. Check the network configuration. Network and HyperIP configuration is explained beginning on page 5.
3. The connection between the source and destination seems to be inoperative. Use ping and traceroute utilities to verify the connections between the source IP and the HyperIP, and the remote HyperIP and the destination IP.

# Appendix B: GPL License

The following packages are GPL licensed code and are used in HyperIP. The source or links to the source for these can be made available from Network Executive Software, Inc. by request to [support@netex.com](mailto:support@netex.com):

Red Hat Distribution 7.2

Streams

PHP

LZO Compression

KeepAlive

Watchdog

## GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.  
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA  
Everyone is permitted to copy and distribute verbatim copies  
of this license document, but changing it is not allowed.

### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

## GNU GENERAL PUBLIC LICENSE

### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
  - b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
  - c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
  - a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
  - b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
  - c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

7. You are not responsible for enforcing compliance by third parties to this License. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE

LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS