HyperIP®

IP WAN Optimizer

Virtual Appliance

Release 6.1

User Guide

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 NRBStat Error Codes and System Error Codes section.
5.5.3-02	Update key request references, s and logo
6.0.0	Release 6.0.0; support for Microsoft Hyper-V, discontinue NetEx supplied hardware appliances.
6.0.0-01	Correct AltPerm and AltTemp button descriptions for the webpage
6.0.1	Change version; no content change.

Revision	Description
6.1	Updates in login page; additional certificates management; maintenance; more consistent web pages.

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
6450 Wedgwood Road N. Suite 103
Maple Grove, MN 55311
USA

Comments may also be submitted over the Internet by addressing e-mail to support@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 distribution package 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 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.

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

Modifications to HyperIP

HyperIP contains proprietary software. Modifications to the software 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

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™**
Microsoft	**Hyper-V™**

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`.
`user entry`	*`This font`* 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.
bold	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.
<***label***>	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

Revision Record ..... **ii**

Preface ..... **v**
Notice to the Customer v
Modifications to HyperIP v
Notice to the Reader v
Corporation Trademarks and Products vi
Document Conventions vii

Contents ..... **ix**

Figures ..... **xii**

Introduction **1**

Theory of Operation **3**
Un-optimized Traffic 4

Typical Gateway Mode Configuration **5**

Proxy IP Address Configuration **7**

Automatic Hot-Standby Configuration **9**

Multiple HyperIP Sites Configuration **13**

Product Features **15**
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

Scalability Considerations **19**

Security Considerations **21**
System Security 21
Security of User Data 21
Securing Management Access 21

HyperIP Command Line Interface 23
Overview 23
Features 23
Command Descriptions 23
CLI Command Summary 24

Web Browser User Interface 41
Browser Considerations 41
Home Page 41
The Status Bar 41
Top Left Frame 43
The "–select a page–" Menu 43
The "Services" Menu 45
HyperIP Web Browser Pages 47
HyperIP HOME Page 47
Admin Password 47
Links 48
Installation Steps 48
Web Browser Certificates 48
HyperIP SNMP MIBs 48
HyperIP Online Documentation 48
HyperIP Product Key Request 48
Install Commands 49
HELP 49
Product Information 49
License Key 50
License Expiration Warning and SNMP Traps 50
SNMP Server Configuration 50
System Configuration Page 51
HyperIP Configuration Page 53
Site Add / Delete Page 54
Site Edit / Import Page 56
Proxies & Intercepts Page 57
HyperIP Proxies 57
HyperIP Intercepts 58
Bandwidth Schedule (Rate Limiting) Page 59
Advanced Configuration Page 60
Maintenance Commands Page 62
Diagnostic Commands Page 64
File Downloads/Uploads Page 67
Download to your browser workstation 68
Upload from your browser workstation 68
Password Change Page 68
Monitor Password 68

Operational Procedures 71
Initial Configuration via console to Use Web Interface 71
Saving HyperIP Configuration to Your Workstation 72
Restoring HyperIP Configuration from your Windows Workstation 72
Downloading Software Updates (Patches) 72
New Product Version (Image) Install Procedure 73

Switching Partitions – General Case....74
Restoring or Reverting a Virtual Machine from an Operational Snapshot....74

Customer Troubleshooting....75
Accessing HyperIP....75
Statistics....75
Informational Logs....75
System Dumps....75
System Log....75
HyperIP Base Log....76
HyperIP Transport Log....76
Troubleshooting via the Web Browser Interface....76
"Diagnostic Commands" Page....76
Advanced Configuration Page....77
System Configuration Page....77
Problem Isolation/Resolution....77
Hardware Problem....77
Cannot Access HyperIP to Perform Initial Configuration....78
Cannot Access HyperIP Web Interface after Initial Configuration....78
Cannot communicate between HyperIPs....78
Applications Cannot Communicate To or Through HyperIP....79
Poor Performance across the Network....80
Troubleshooting using the Display HyperIP State Command....81
Local System Related Configuration Problems....90

Appendix A: Error Codes....91
System Log File....91
NRBStat Error Codes....91
System Error Codes....99

Appendix B: GPL License....101

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: Multiple HyperIP Sites Configuration 13
Figure 7: Web Browser Page Status Bar Screen Capture 42
Figure 8: Web Browser Page Status Bar Description 43
Figure 9: Web Browser Page “–select a page-“ Menu 44
Figure 10: Web Browser Page “HyperIP Services Menu 46
Figure 11: Web Browser Home Page 47
Figure 12: Install Commands Web Page with Help 49
Figure 13: System Configuration Web Page with Help 52
Figure 14: HyperIP Configuration Web Page with Help 53
Figure 15: Site Add / Delete Web Page 54
Figure 16: Site Edit / Import Web Page 56
Figure 17: Web Browser Proxies and Intercepts Web Page 57
Figure 18: Bandwidth Schedule Web Page 59
Figure 19: Advanced Configure Web Page with Help 60
Figure 20: Tuning Parameters Web Page 61
Figure 21: Maintenance Web Page with Help 63
Figure 22: Diagnostic Commands Web Page with Help 65
Figure 23: Diagnostic Page; tcpdump output sample 66
Figure 24: File Downloads/Uploads Web Page with Help 67
Figure 25: Password Change Web Page with Help 69
Figure 26: Display HyperIP State Command Output, Part 1 81
Figure 27: Display HyperIP State Command Output, Part 2 83
Figure 28: Details for HyperIP State Command Output, Part 2 84
Figure 29: Display HyperIP State Command Output, Part 3 85
Figure 30: Details for HyperIP State Command Output, Part 3 86
Figure 31: Display HyperIP State Command Output, Part 4 87
Figure 32: Details of HyperIP State Command Output, Part 4 88

Figure 33: Symptom and Problem Determination Table 90

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** applications 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
    - Packet loss

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):

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

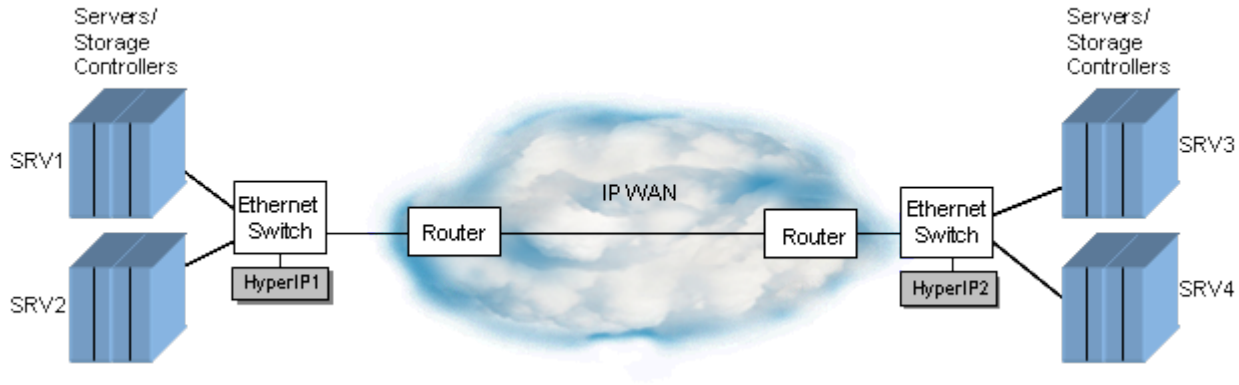

Figure 2: Typical HyperIP "Gateway" Configuration

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:

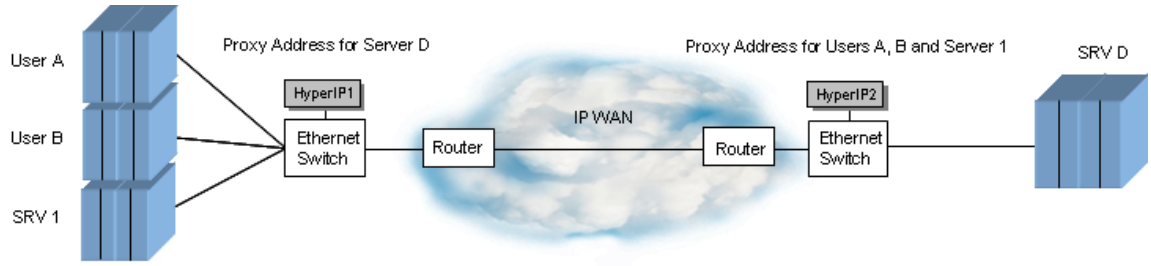

Figure 3: Typical Proxy IP Address Configuration

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

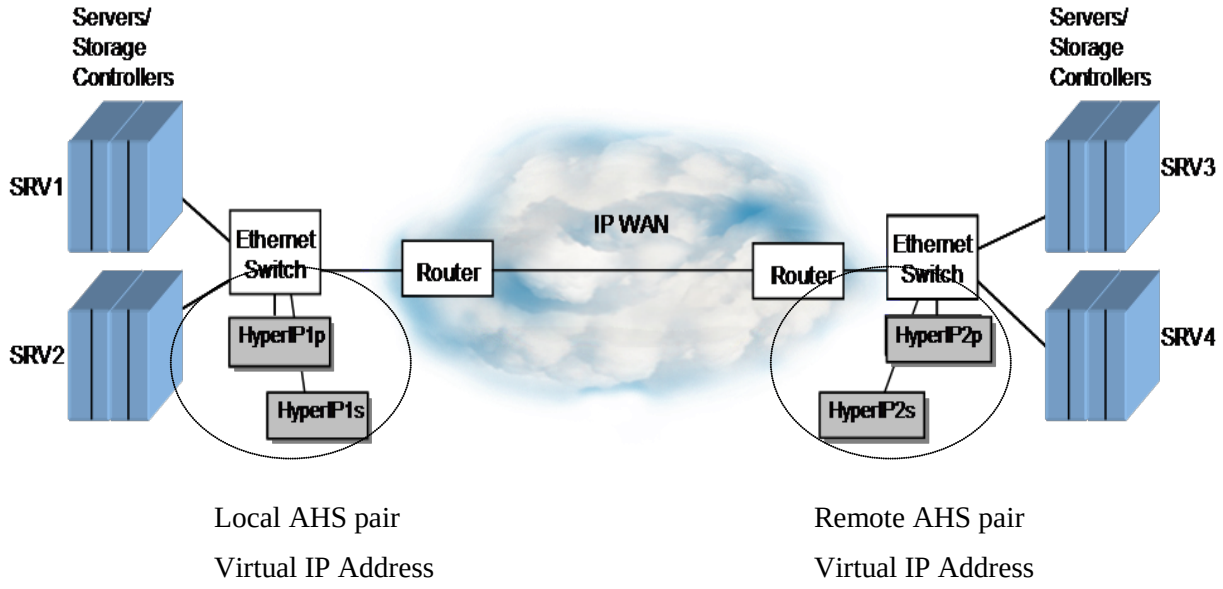

Figure 4: Typical Automatic Hot-Standby "Gateway" Configuration

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 has 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:

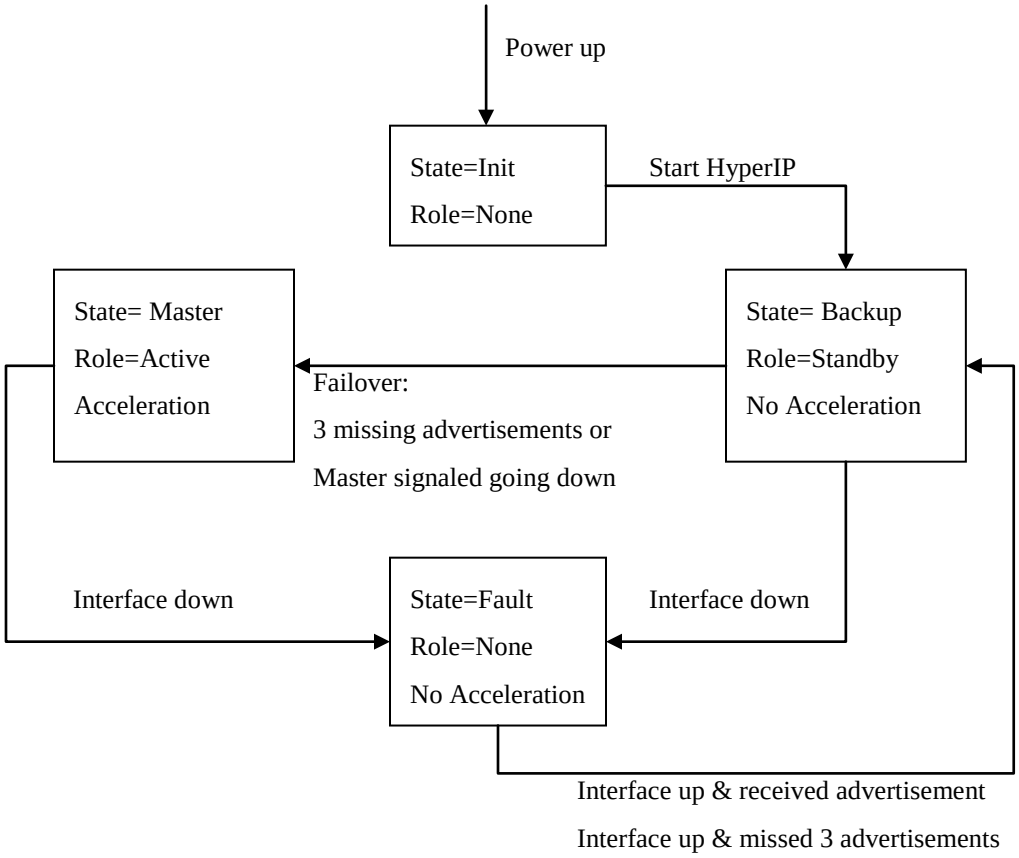

Figure 5: HyperIP AHS Roles/State Diagram

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 Spanning Tree Protocol (STP) 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 HyperIP Sites 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 Site Add / Delete web page allows the setup to be done with a few table entries. The Site Edit / Import web page 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.

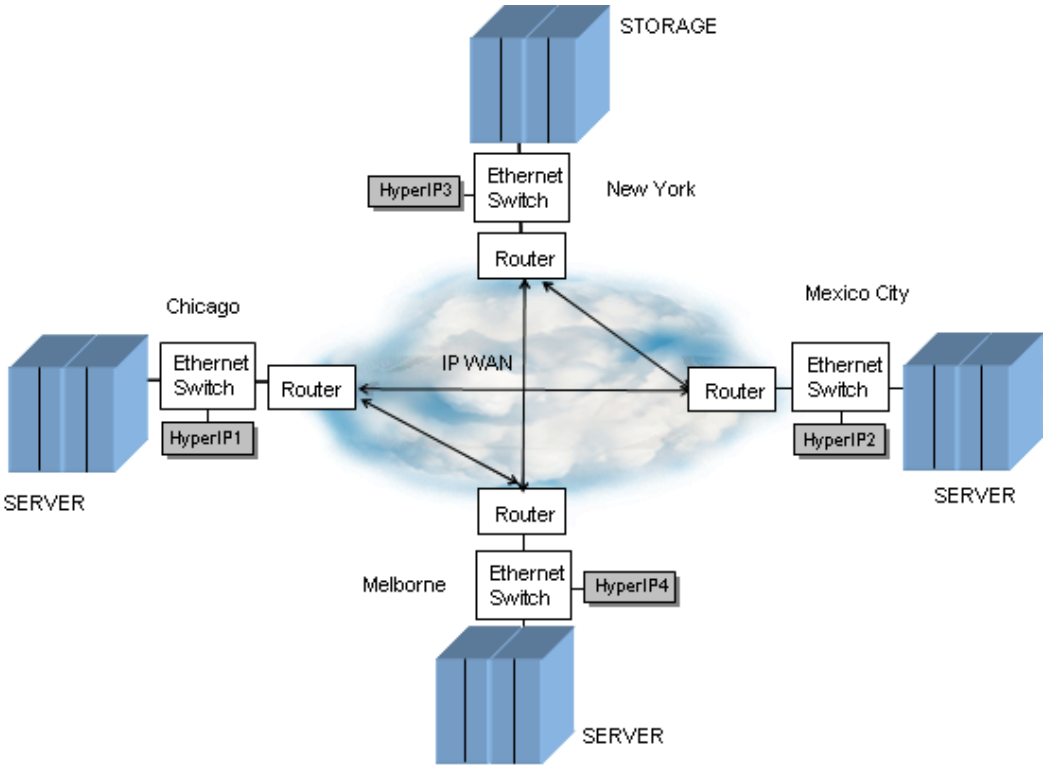

Figure 6: Multiple HyperIP Sites Configuration

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 ‘system’ setup of hostname, 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.

Multiple User Interfaces

An administrator may configure and/or monitor the HyperIP via a web browser such as Netscape or Internet Explorer, or via SSH (or serial port on older NetEx supplied appliance or console for virtual machine 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. Enter a specific NTP server to 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 connects to HyperIP via SSH (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

Depending on the resources dedicated to the VM, a single HyperIP may support 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 resources dedicated to the VM, 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.

With HyperIP running as a virtual machine, 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.

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

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 HyperIP Virtual Appliance can be managed by the console however, 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, 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 virtual appliance can be physically disconnected from the management network.

The following is a list of steps the administrator may take to secure management access to the HyperIP virtual 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 HTTP access on the data interface (defaults to disabled)

5. Disable ping access on the data interface (defaults to disabled)
6. Disable HTTPS access on the data interface (private browser access connection – defaults to disabled)
7. Disable SSH access on the data interface (private connection – defaults to disabled)

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

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

12. 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.

13. 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.

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 SSH or when connected via the console interface.

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.

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. **cfgAccessOff <*interface*> <*service*>** ***interface*** (data|mgmt) ***service*** service to block (http|https|ping|snmp|ssh)
cfgAccessOn	Modify the security access rules to allow certain services. Allow access to service. **cfgAccessOn <*interface*> <*service*>** ***interface*** (data|mgmt) ***service*** service to allow (http|https|ping|snmp|ssh)
cfgDefaultGateway	Set the system's default gateway to IP_ADDRESS. Configure the default gateway. **cfgDefaultGateway <*ip_address*>** ***ip_address*** IP Address of default gateway (AAA.BBB.CCC.DDD where each part is in the range 0-255)
cfgGlobalParam ??Tab does not give Parameter definition??	Set the specific global parameter for the HyperIP. Configure a global parameter. **cfgGlobalParam <*parameter*> <*value*>** ***parameter*** / ***description*** / ***value*** 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)
cfgHostname	Set the system hostname. Configure the HyperIP IP hostname. **cfgHostname <*hostname*>** ***hostname*** Hostnames are composed of a series of labels concatenated with dots. Each label must be between 1 and 63 characters long, start with a letter and not end with a hyphen. The entire hostname (including the delimiting dots) has a maximum of 255 characters. Allowable characters (A-Z)(a-z)(0-9)(-)(.)

Command	Command Description/Syntax
cfgIntercept	Enable, Disable or Delete an existing intercept. **cfgIntercept <*action*> <*intercept-id*>** ***action*** (delete|enable|disable) ***intercept-id*** existing intercept id (0-99)
cfgInterface	Configure the management or data interface's IP address, netmask, speed and MTU. **cfgInterface <*interface*> <*ip_address*> <*netmask*> <*speed*> <*mtu*>** ***interface*** (data|mgmt) ***ip_address*** IP address (in dotted notation) XX.XX.XX.XX ***netmask*** netmask (in dotted notation) XX.XX.XX.XX ***speed*** interface speed (auto | half10 | full10 | half100 | full100 | full1000) ***mtu*** maximum transmission unit (576-16110) Note: some interfaces do not allow speed settings to be changed. The command can be entered, but the interface driver will error the change.
cfgInterfaceDown	Bring down the data or management interface. **cfgInterfaceDown <*interface*>** ***interface*** interface to configure down (data|mgmt)
cfgInterfaceUp	Bring up the data or management interface. **cfgInterfaceUp <*interface*>** ***interface*** interface to configure up (data|mgmt)
cfgPassword	Set the password for a given userid, enter the password at the prompt. Set the password for a userid. Enter nothing or use 'none' for no password (monitor only). **cfgPassword <*userid*>** ***userid*** userid to set the password for (admin|monitor)
cfgProxy	Enable, Disable or Delete an existing proxy. **cfgProxy <*action*> <*proxy-id*>** ***action*** action to apply (delete|enable|disable) ***proxy-id*** existing proxy id

Command	Command Description/Syntax
cfgSerialPort	Configure the specified serial port as off, for direct connection to/from a PC, or for modem connection in answer mode. (Only valid for machines that have a serial port.) **cfgSerialPort <*speed*> <*config*>** ***speed*** baud rate to set (9600|19200|57400|115200) ***config*** serial configuration (off|dir|ans)
deleteAllIntercepts	Delete ALL configured intercepts.
deleteAllProxies	Delete ALL configured proxies.
deleteAllTuning	Delete ALL site-specific tuning parameters.
deleteConfig	Delete configuration file from disk. **deleteConfig <fname>** ***fname*** existing file name of configuration to delete
deleteImage	Delete a product image file. **deleteImage <*fname*>** ***fname*** existing file name of image to delete
deleteUpdate	Delete a product update file. **deleteUpdate <*fname*>** ***fname*** existing file name of update to delete
exit	Exit this CLI session
help	Display an overview of the CLI syntax
history	Display the current session's command line history OR set the size of the history list (zero means unbounded). **history [*limit*]** ***limit*** size of history list (0 is unlimited).
installImage	Install a product image into the inactive (alternate) partition from the image file. **installImage <*fname*>** ***fname*** existing filename of image to install to the non-running partition.
installImageCD	Install a product image to the alternate (inactive) partition from CD/DVD (for VMs the CD/DVD device must be attached to the VM).

Command	Command Description/Syntax
installKey	Install the HyperIP product license key. (obtain the key from http://www.netex.com/hyperip/hyperip-key-request) You will need to have the machine's fingerprint (serial number) to fill out the request. **installKey <*key*>** ***key*** HyperIP product license key from Network Executive Software, Inc..
installUpdate	Install a product update into the active (current) partition from the update file. **installUpdate <*fname*>** ***fname*** existing filename of update to install to the running partition.
listConfigs	Show the existing saved configurations on the hard drive in the running partition.
listImages	Show a list of existing product image files on the hard drive.
listUpdates	Show a list of existing product update files on the hard drive or show the update information of a specified update file. **listUpdates [*fname*]** ***fname*** existing filename of update to show information about.
logout	Logout of the current CLI session.
newCert	Generate a new SSL certificate

Command	Command Description/Syntax
newIntercept	Add a new intercept to HyperIP. **newIntercept** ***<intercept-id>*** ***<remote-site-name>*** ***<sourceIP>*** ***<sourcePort>*** ***<destinationIP>*** ***<destinationPort>*** ***<protocol>*** ***<forwardAtLimit>*** ***intercept-id*** unique identifier (consisting of 8 alphanumeric characters – case insensitive) naming the intercept ***remote-site-name*** name of remote site to intercept traffic for ***sourceIP*** Criteria to compare in IP header - origin IP address. If the (TCP connect) packet matches all IP criteria, it will be intercepted and HyperIP will tunnel it. ***sourcePort*** Criteria to compare in IP header - origin port(s). If the (TCP connect) packet matches all IP criteria, it will be intercepted and HyperIP will tunnel it. ***destinationIP*** Criteria to compare in IP header - destination IP. If the (TCP connect) packet matches all IP criteria, it will be intercepted and HyperIP will tunnel it. address ***destinationPort*** Criteria to compare in IP header - destination port(s). If the (TCP connect) packet matches all IP criteria, it will be intercepted and HyperIP will tunnel it. ***protocol*** Criteria to compare in IP header - ICMP, UDP, TCP (i|u|t|iu|it|ut|iut). If the (TCP connect) packet matches all IP criteria, it will be intercepted and HyperIP will tunnel it. ***forwardAtLimit*** (yes|no) – When HyperIP has reached the configured connection limit and a connection arrives matching the IP criteria, this setting causes HyperIP to forward the packet or drop it.

Command	Command Description/Syntax
newProxy	Add a new proxy to HyperIP. The proxy IP address/port will be used to tunnel communication to the destination IP address. There must be a reciprocating proxy on the remote HyperIP. **newProxy <*proxy-id*> <*remote-site-name*> <*proxyIP*> <*proxyPort*> <*destinationIP*> <*protocol*>** ***proxy-id*** A unique identifier (consisting of 8 alphanumeric characters – case insensitive) naming the proxy ***remote-site-name*** remote site name which will receive the communication matching this proxy IP/port(s) ***proxyIP*** proxy IP address which is representing the destination IP address/port(s) ***proxyPort*** proxy port(s) which match the incoming packet (along with proxyIP) to be tunneled to the destination IP. ***destinationIP*** destination IP address which is represented by the proxy IP ***protocol*** ICMP,UDP,TCP [i|u|t|iu|it|ut|iut] to be triggered for this proxy IP
ping	Send an ICMP ECHO_REQUEST to the network host. (Enter a Ctrl-c to quit). **ping <*host*>** ***host*** hostname or IP address to send the ICMP echo request to. A simple hostname in the form of: 1-63 characters in length, allowable characters (A-Z)(a-z)(0-9)(-) or a fully qualified hostname in the form of: 5-255 characters in length, allowable characters (A-Z)(a-z)(0-9)(-)(.), systemName.localDomainName or an IP-address in the form of: AAA.BBB.CCC.DDD where each part is in the range 0-255.
quit	Exit this CLI session
reboot	Reboot the HyperIP; controlled restart of the HyperIP machine.

Command	Command Description/Syntax
receiveConfigHttp	Receive a configuration file via HTTP. **receiveConfigHttp <*syst*> <*path*> <*fname*>** ***syst*** hostname or IP address to send the ICMP echo request to. A simple hostname in the form of: 1-63 characters in length, allowable characters (A-Z)(a-z)(0-9)(-) or a fully qualified hostname in the form of: 5-255 characters in length, allowable characters (A-Z)(a-z)(0-9)(-)(.), systemName.localDomainName or an IP-address: in the form of: AAA.BBB.CCC.DDD where each part is in the range 0-255 ***path*** path to configuration file ***fname*** name of configuration file to transfer to the HyperIP.
receiveConfigHttps	Receive a configuration file via HTTPS. **receiveConfigHttps <*syst*> <*path*> <*fname*>** ***syst*** hostname or IP address to send the ICMP echo request to. A simple hostname in the form of: 1-63 characters in length, allowable characters (A-Z)(a-z)(0-9)(-) or a fully qualified hostname in the form of: 5-255 characters in length, allowable characters (A-Z)(a-z)(0-9)(-)(.), systemName.localDomainName or an IP-address: in the form of: AAA.BBB.CCC.DDD where each part is in the range 0-255 ***path*** path to configuration file ***fname*** name of configuration file to transfer to the HyperIP.
receiveImageHttp	Receive a product image via HTTP **receiveImageHttp <*syst*> <*path*> <*fname*>** ***syst*** hostname or IP address to send the ICMP echo request to. A simple hostname in the form of: 1-63 characters in length, allowable characters (A-Z)(a-z)(0-9)(-) or a fully qualified hostname in the form of: 5-255 characters in length, allowable characters (A-Z)(a-z)(0-9)(-)(.), systemName.localDomainName or an IP-address: in the form of: AAA.BBB.CCC.DDD where each part is in the range 0-255 ***path*** path to image file ***fname*** name of image file to transfer to the HyperIP.

Command	Command Description/Syntax
receiveImageHttps	Receive a product image via HTTPS **receiveImageHttps <*syst*> <*path*> <*fname*>** ***syst*** hostname or IP address to send the ICMP echo request to. A simple hostname in the form of: 1-63 characters in length, allowable characters (A-Z)(a-z)(0-9)(-) or a fully qualified hostname in the form of: 5-255 characters in length, allowable characters (A-Z)(a-z)(0-9)(-)(.), systemName.localDomainName or an IP-address: in the form of: AAA.BBB.CCC.DDD where each part is in the range 0-255 ***path*** path to image file ***fname*** name of image file to transfer to the HyperIP.
receiveUpdateHttp	Receive an update or patch file via HTTP. **receiveUpdateHttp <*syst*> <*path*> <*fname*>** ***syst*** hostname or IP address to send the ICMP echo request to. A simple hostname in the form of: 1-63 characters in length, allowable characters (A-Z)(a-z)(0-9)(-) or a fully qualified hostname in the form of: 5-255 characters in length, allowable characters (A-Z)(a-z)(0-9)(-)(.), systemName.localDomainName or an IP-address: in the form of: AAA.BBB.CCC.DDD where each part is in the range 0-255 ***path*** path to patch file ***fname*** name of patch file to transfer to the HyperIP.
receiveUpdateHttps	Receive an update file via HTTPS. **receiveUpdateHttps <*syst*> <*path*> <*fname*>** ***syst*** hostname or IP address to send the ICMP echo request to. A simple hostname in the form of: 1-63 characters in length, allowable characters (A-Z)(a-z)(0-9)(-) or a fully qualified hostname in the form of: 5-255 characters in length, allowable characters (A-Z)(a-z)(0-9)(-)(.), systemName.localDomainName or an IP-address: in the form of: AAA.BBB.CCC.DDD where each part is in the range 0-255 ***path*** path to patch file ***fname*** name of patch file to transfer to the HyperIP.

Command	Command Description/Syntax
remoteCli	Connect to another HyperIP **remoteCli <*uid*> <*name*>** ***uid*** userid (hipadmin|monitor) monitor is only valid if password is setup for that user. ***name*** hostname or IP address to send the ICMP echo request to. A simple hostname in the form of: 1-63 characters in length, allowable characters (A-Z)(a-z)(0-9)(-) or a fully qualified hostname in the form of: 5-255 characters in length, allowable characters (A-Z)(a-z)(0-9)(-)(.), systemName.localDomainName or an IP-address: in the form of: AAA.BBB.CCC.DDD where each part is in the range 0-255
resetToFactory	Reset configuration to factory defaults
restartForce	Restart HyperIP immediately.
restartManagement	Restart management services immediately.
restoreConfig	Restore configuration from a file on the hard disk **saveConfig [*fname*]** ***fname*** filename of the configuration to restore from
saveConfig	Save configuration to a file on the hard disk **saveConfig [*fname*]** ***fname*** filename to save the configuration in
serialnumber	Show serial number. The serial number (or fingerprint) is required to obtain the HyperIP Product License Key from Network Executive Software, Inc.
setBootAlt	Configure for the alternate partition to boot next with a specific configuration. This is typically used following an install of a new version of HyperIP software. **setBootAlt [*fname*]** ***fname*** file name of the configuration file to use with that boot.
setBootCurr	Configure for the current partition to boot. This is typically used to unset the setBootAlt command.

Command	Command Description/Syntax
setConnLimits	Set connection limits **setConnLimits <*tcpLimit*> <*udpLimit*> <*aggLimit*>** ***tcpLimit*** TCP connection limit (0..8192) * ***udpLimit*** UDP connection limit (0..8192) ***aggLimit*** Aggregate connection limit. The absolute maximum number of connections supported (UDP + TCP) is 8192. A value of zero disables connection limit checking. • * Tcplimit controls window sizes in the following manner: Tcplimit set to 1-50 – HyperIP will use 16MB windows Tcplimit set to 51-200 – HyperIP will use 4 MB windows (or system calculated) Tcplimit set to 0 or 200-8192 – HyperIP will use 170KB windows
showAccess	Display secure management access on data and management interfaces
showBoot	Show current System boot options and versions on each partition.
showCert	Display SSL certificate
showConfig	Display the current HyperIP configuration statements; these are internal configuration statements for NESi support personnel.
showConnLimits	Show connection limits (see “setConnLimits”)
showHipStatus	Display the HyperIP state, which includes site connections and throughput as well as ICMP statistics, and TCP/UDP connections and statistics.
showHostname	Display the HyperIP IP hostname (bound to the management interface).
showIfCfg	Displays the settings for the Ethernet interfaces. These may not match the active system. Use ‘showIfState’ to display active settings.
showIfState	Displays the state of the Ethernet interfaces.
showIntercepts	Display all configured intercepts.

Command	Command Description/Syntax
showLog	Display log messages for a given subsystem and instance. Instance number 0 is current; the higher the number the older the log. Type 'q' to quit when in paging mode. **showLog <*subsys*> <*level*>** ***subsys*** Log subsystem name (api/base/boot/conn/ha/sys/tran/web/weba) [base] ***level*** Log instance number [0]
showProxies	Display all configured proxies.
showRestarts	Display which, if any, restarts are pending.
showRoutes	Display kernel IP routing table.
showSerialPort	Shows the current setup of the serial port. (Not all machines support serial ports).
showSiteParms	Show the current user configurable transport tuning parameters to a specific remote site **showSiteParms <*siteNum*>** ***siteNum*** ID of the remote site to see the tuning parameters (1-99)
showSites	Displays the currently defined sites.
showVersion	Display HyperIP product version information, key, platform and serial number.
shutdown	Shutdown the appliance. Open a new CLI session when HyperIP has come back up.

Command	Command Description/Syntax
siteAdd	Add a site definition **siteAdd <*localSiteId*> <localSiteR*ole*> <newS*iteId*> <newSite*Name*> <*ipAddress*> <*segsize*> <*maxrate*> <*initstate*>** ***localSiteId*** site number of the local site (this HyperIP) Range 1-99 ***localSiteRole*** local AHS role (noAHS | primary | secondary) ***newSiteId*** user-selectable unique number used for internal identifiers (must be consistent for each site across HyperIPs) (1-99) ***newSiteName*** user-selectable unique name used for internal identifiers (must be consistent for each sites across HyperIPs) ***ipAddress*** the IP address for HyperIP being added (primary for AHS) ***segsize*** maximum bytes sent from HyperIP to IP per write to this site (100-32768) ***maxrate*** maximum transmit rate in megabits-per-sec for sending to this site (can be limited by rate schedule) ***initstat*** initial state (halt, start)

Command	Command Description/Syntax
siteAddAHS	Add an AHS site definition **siteAddAHS <*localSiteId*> <*localSiteRole*> <*newSiteId*> <newSite-Name> <*primaryIP*> <*virtualIP*> <virtualID> <secondIP> <*segsize*> <*maxrate*> <*initstate*>** ***localSiteId*** site number of the local site (this HyperIP) (1-99) ***localSiteRole*** local AHS role (noAHS | primary | secondary) ***newSiteId*** user-selectable unique number used for internal identifiers (must be consistent for sites across HyperIPs) (1-99) ***newSiteName*** user-selectable unique name used for internal identifiers (must be consistent for sites across HyperIPs) ***primaryIP*** the IP address for HyperIP being added (primary for AHS) (may be this one) ***virtualIP*** the address used by servers as gateway addresses across the HyperIP network. The real & virtual HyperIP addresses on each side of the network must be in the same subnet ***virtualID*** VRRP unique id for AHS communication (0-255) ***secondIP*** the IP address of the secondary AHS HyperIP (may be this one) ***segsize*** maximum bytes sent from HyperIP to IP per write to this site (100-32768) ***maxrate*** maximum transmit rate in megabits-per-sec for sending to this site (can be limited by rate schedule) ***initstat*** initial state (halt, start)
siteDelete	Delete site definition(s) **siteDelete <*localSiteId*> <*localSiteRole*> <*remoteSiteId*>** ***localSiteId*** site number of the local site (1-99) ***localSiteRole*** Local AHS role (noAHS | primary | secondary) ***remoteSiteId*** number of the site being deleted (1-99)
siteDeleteAll	Delete ALL site definitions, hosts, sessions, routes & related definition(s)
siteHalt	Change the operational and configured state of the remote site to Halt . **siteHalt <site*name*>** ***sitename*** remote site name to halt
siteHaltAll	Halt all remote sites.

Command	Command Description/Syntax
siteStart	Change the operational and configured state of the remote site to Start. **siteStart <site*name*>** ***sitename*** remote site name to start
siteStartAll	Start all remote sites.
siteTuneParms	Set the user configurable transport tuning parameters for a remote site (*=default) **siteTuneParms <*sitenum*> <*maxmtowait*> <*minbtosend*> <*compalg*> <*compadapt*> <*compapercnt*> <*userexmitq*> <*rexmwblks*> <*rcvdataqhb*> <*rcvdataqlb*> <*bufolim*> <recvgapq>** ***sitenum*** remote site number or ID for these session tuning parameters (1..99) ***maxmtowait*** maximum milliseconds to wait before sending data, 0-9999 [*] ***minbtosend*** minimum bytes to send when using maxmtowait, 0-65400 [*] ***compalg*** compression algorithm to use: [*] **0** implies “none” or no compression **1** implies “LZO“ or compression on ***compadapt*** use adaptive compression: [*] **0** implies “no” **1** implies “yes“ ***compapercnt*** compress data only if compressed data size will be *<compapercnt>%* less than the original data size. Only used when ***compadapt*** is 1.[*] ***userexmitq*** use a retransmit queue to delay before retransmitting: [*] **0** implies “no” **1** implies “yes“ ***rexmwblks*** retransmit queue depth - # of segments to wait when using ***userexmitq(0..99)[*]*** ***rcvdataqhb*** # of bytes on local receive data queue before HyperIP will start discarding (0..999999999) [*] ***rcvdataqlb*** # of bytes on local receive data queue under which data is accepted after discarding (0..999999999) [*] ***bufolim*** maximum number of write segments allowed to be in progress [*] ***recvgapq*** store packets received out of order - 0:no 1:yes [*]

Command	Command Description/Syntax
siteTuneReset	Reset user configurable transport tuning parameters for remote site to default values **siteTuneReset** <***sitenum***> ***sitenum*** ID number of site for these session tuning parameters (1..99)
tailLog	Display most recent log messages for a given subsystem and instance. Instance number 0 is current, the higher the number the older the log. Type 'q' to quit when in paging mode. **tailLog** [**subsys**] [**level**] [**lines**] ***subsys*** subsystem name of log to be displayed (api | base | boot | conn | sys | tran | web | weba) [base] ***level*** log instance number [0] ***lines*** number of lines to display [0]
tcpdump	tcpdump prints out a description of the contents of packets on a network interface. Host addresses, port numbers and protocols are not converted to names. Use 'CTRL-c' to stop the command. **tcpdump** <**interface**> ***interface*** interface to perform the tcpdump on (data | mgmt)
traceroute	The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking the route one's packets follow (or finding the miscreant gateway that's discarding your packets) can be difficult. traceroute utilizes the IP protocol `time to live' field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to some host. Use 'CTRL-c' to stop the command. **traceroute** <**host**> ***host*** hostname or IP address to send the ICMP echo request to. A simple hostname in the form of: 1-63 characters in length, allowable characters (A-Z)(a-z)(0-9)(-) or a fully qualified hostname in the form of: 5-255 characters in length, allowable characters (A-Z)(a-z)(0-9)(-)(.), systemName.localDomainName or an IP-address: in the form of: AAA.BBB.CCC.DDD where each part is in the range 0-255

Command	Command Description/Syntax
vCenterRegister	Register the HyperIP plugin with VMware Virtual Center server. **vCenterRegister <intf> <server> <userid>** **intf** data or mgmt (data/mgmt) **server** Virtual Center hostname or IP address **userid** Virtual Center userid

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 5.0
- Google Chrome Version 44.0.2403.157

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.

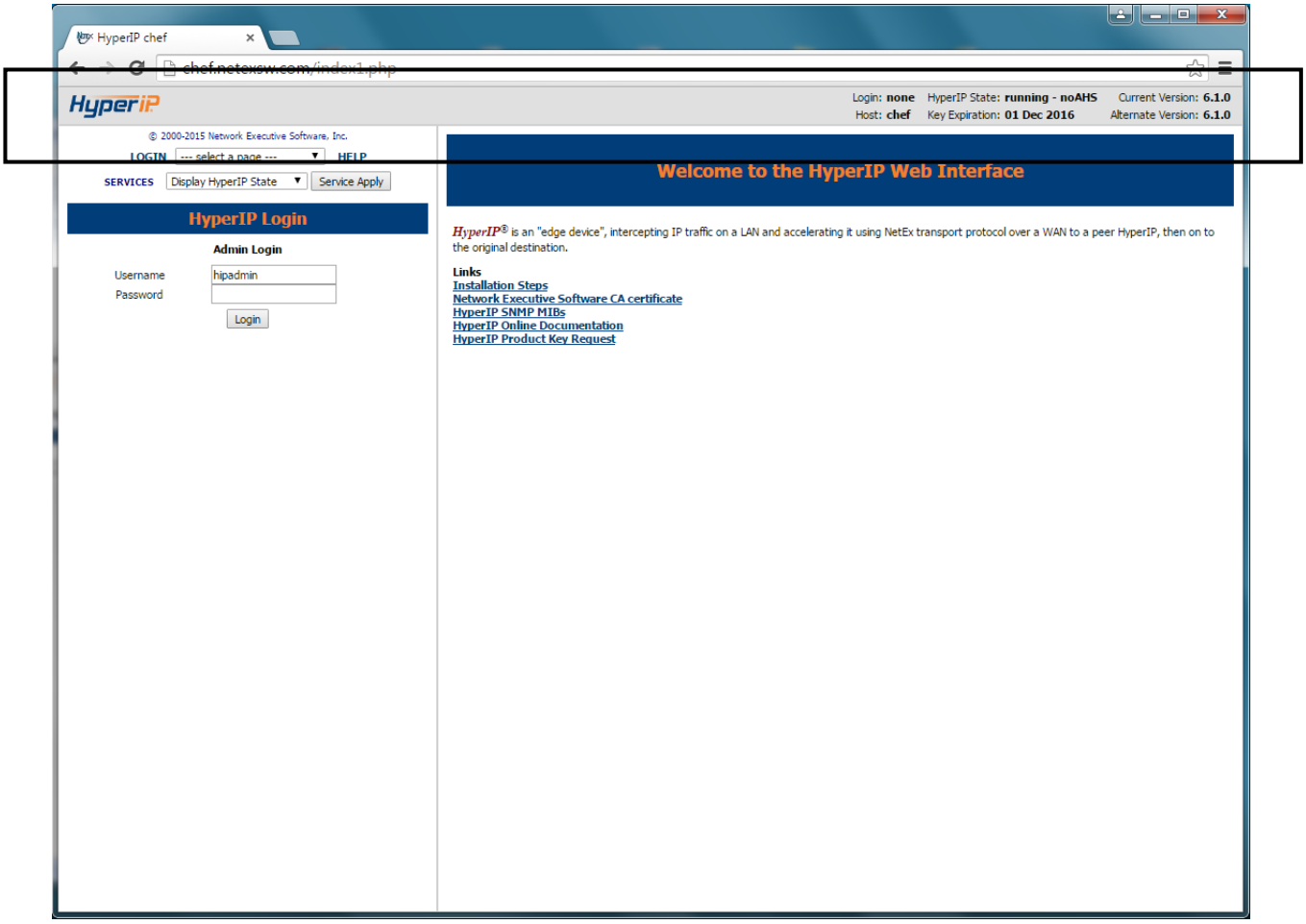

Figure 7: Web Browser Page Status Bar Screen Capture

Status Field	Description
Login [none|*name*]	Logged in name will be hipadmin or none if not logged in. If a monitor password is set, the user must enter the monitor password to view/change the HyperIP.
Host[*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	Describes both the operational state and the state of the AHS. The operational state will be "**running**" when HyperIP is capable of optimizing traffic. If the state is "**down**" then HyperIP is not capable of optimizing traffic (i.e. the license key has not been installed or is expired or otherwise invalid). The AHS state describes what state and role, if any, this HyperIP is in, with respect to AHS. "**noAHS**" means this HyperIP is not configured for AHS. For an AHS configuration, "**Master**" or "**Backup**" is the AHS operational state for this HyperIP and "**Active**" or "**Standby**" is its current AHS role. See the "Hot Standby Configuration" section above for more about AHS.

Status Field	Description
Key Expiration	If a License Key has been installed, the date (MM-DD-YYY) when the license key expires is shown.
Current Version	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 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.
Alternate Version	

Figure 8: Web Browser Page Status Bar Description

Top Left Frame

This frame is persistent on every page and contains functions and navigation that are required frequently.

LOGIN
Login as the admin user (hipadmin) to assign admin authority to the current session. Only available when logged out.

LOGOUT
Logout as the admin user (hipadmin) to remove admin authority from the current session. Only available when logged in.

HELP
Clicking on Help will display a summary of help information for this frame, including a summary of the navigation pages and services.

The "–select a page–" 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 "–select a page-" menu controls access to the panels:

- The **Welcome & Links** bring up the Welcome page and some useful links (in the right frame; initial screen).
- The **Install Commands** links go to the **Installation** page.
- The **System Configuration** link goes to the **System Configuration** page.
- The **HyperIP Configuration** link goes to the **HyperIP Configuration Commands** page.
- The **Site Add/Delete** link goes to the page to **Add or Delete Sites** (in the right frame).
- The **Site Edit/Import** link goes to the page to **Edit or Import Sites** (in the right frame).
- The **Proxies & Intercepts** link goes to the page to **Edit or Import Sites** (in the right frame).
- The **Bandwidth Schedule** link goes to the page to manage the **Bandwidth Schedule** (in the right frame).
- The **Advanced Configuration** link goes to the **Advanced Configuration Commands** page.
- The **Maintenance Commands** link goes to the **Maintenance Commands** page.
- The **Diagnostic Commands** link goes to the **Diagnostic Commands** page.
- The **File Upload/Downloads** link goes to the **File Download/Upload** page.
- The **Password Change** link goes to the **Password Change** page.

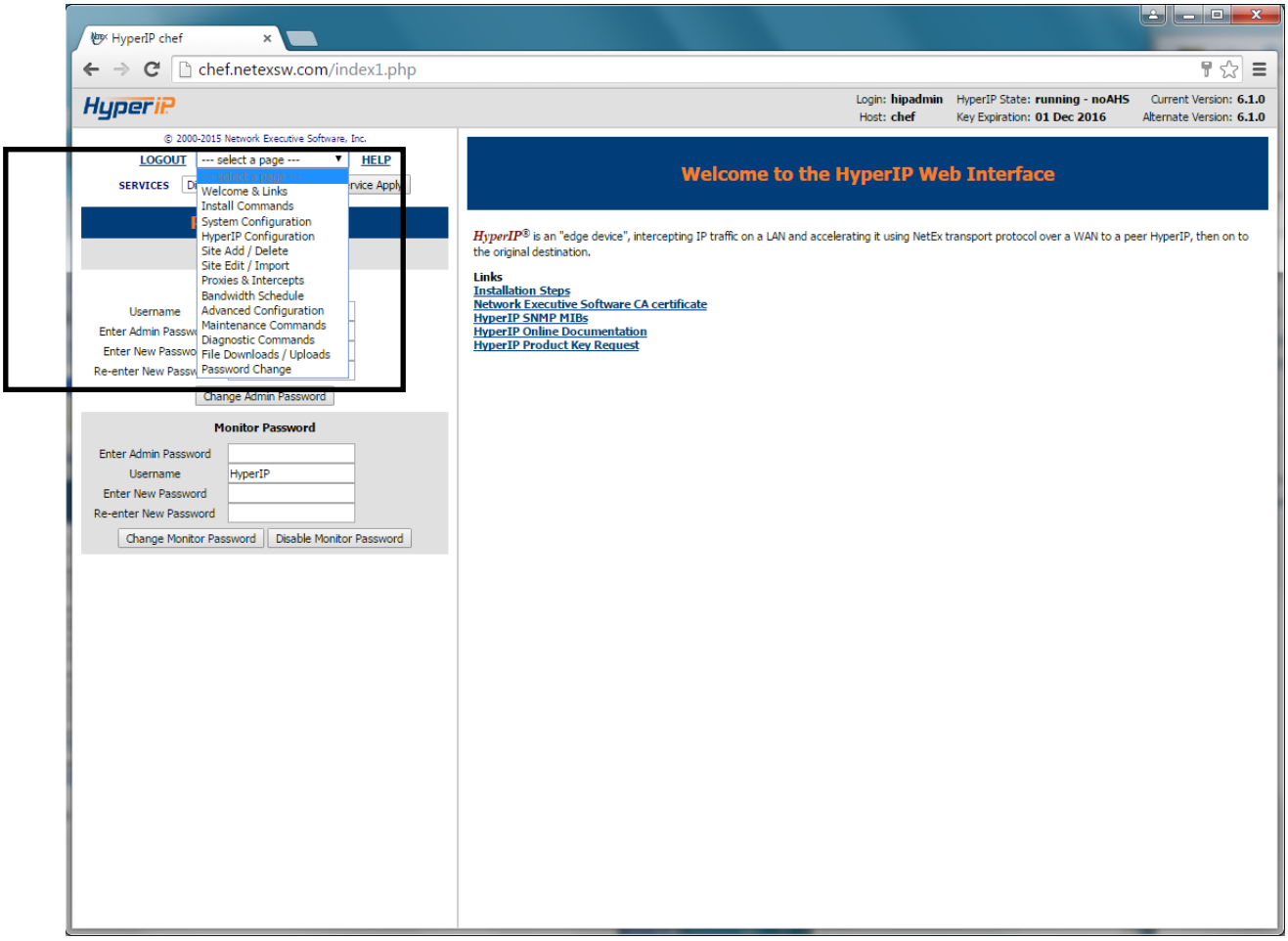

Figure 9: Web Browser Page "–select a page-" Menu

The “Services” Menu

This menu is used to perform service functions that will start, stop, restart, or display the status of the HyperIP service, and reboot or halt the operating system. To perform, select the desired 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).

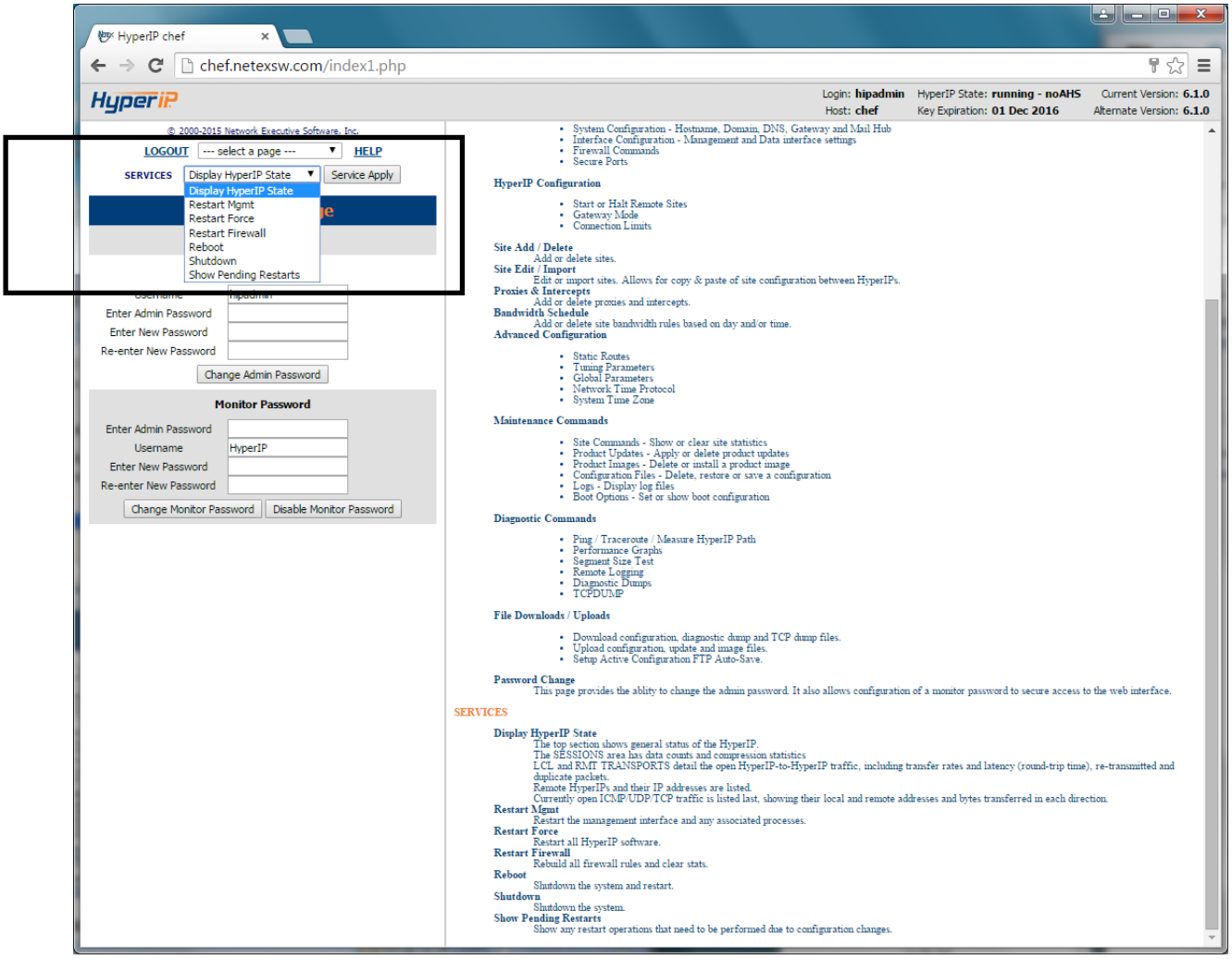

Figure 10: Web Browser Page "HyperIP Services Menu

HyperIP Web Browser Pages

HyperIP HOME Page

This screen is used to enter the password and has links to the NetEx website for the latest documentation, installation steps, SNMP MIB information and a link to the License Key Request page.

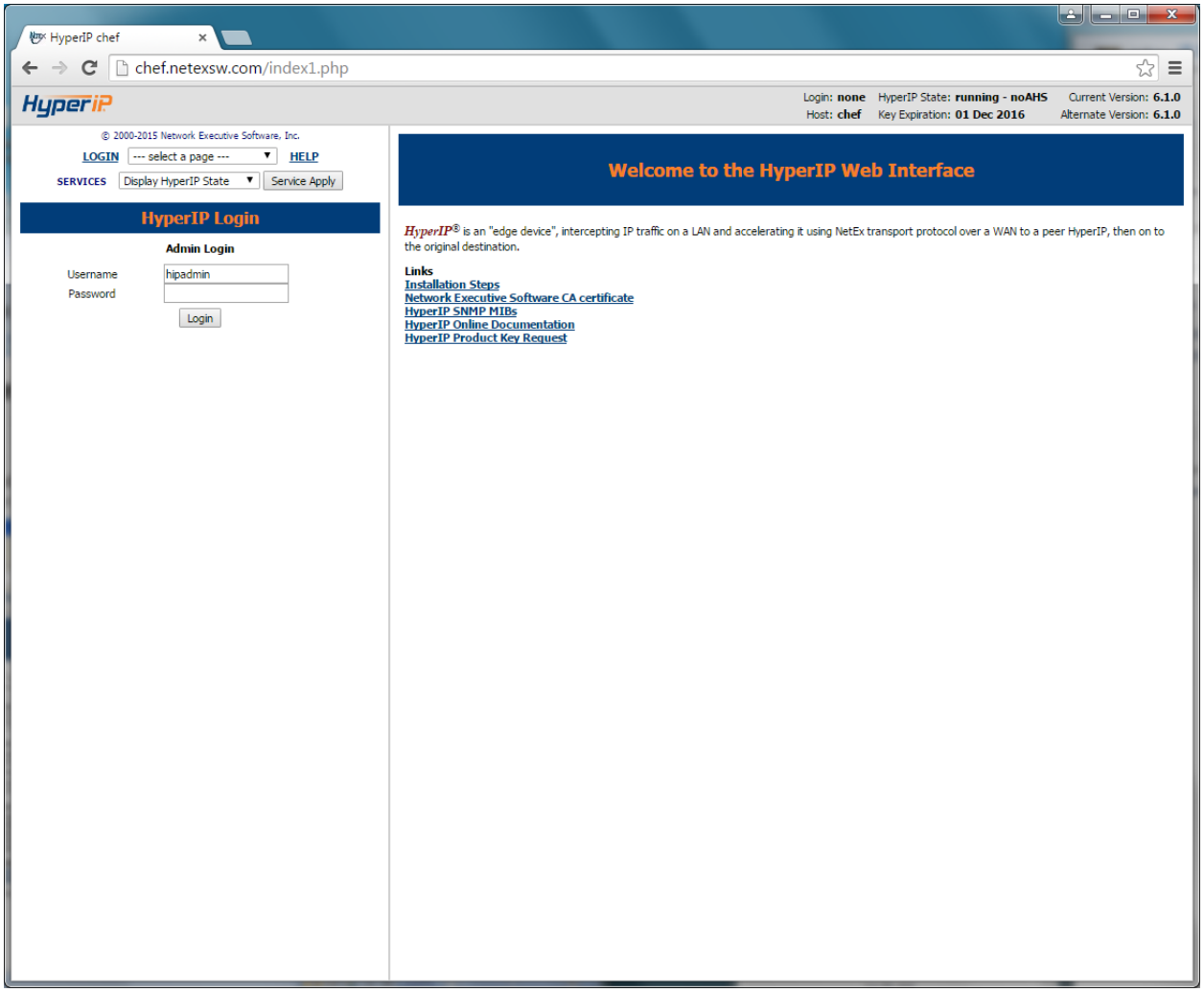

Figure 11: Web Browser Home Page

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, navigate to the **Password Change** page.

Links

Installation Steps

Displays the steps required to install the HyperIP. More detailed steps are located in the User Guide.

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

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

HyperIP SNMP MIBs

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

HyperIP Online Documentation

In 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.

HyperIP Product Key Request

Also in the right frame is a link to the HyperIP Product Key Request Form. Clicking the link will open a new window to the form. External web access from your browser to the Internet is required for this link to work.

Install Commands

The following figure is an example of the display seen when selecting the Install Commands in the <--***select a page***--> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Help under the Install Commands title. This configuration is typically performed only at installation time and when a new license key is to be installed.

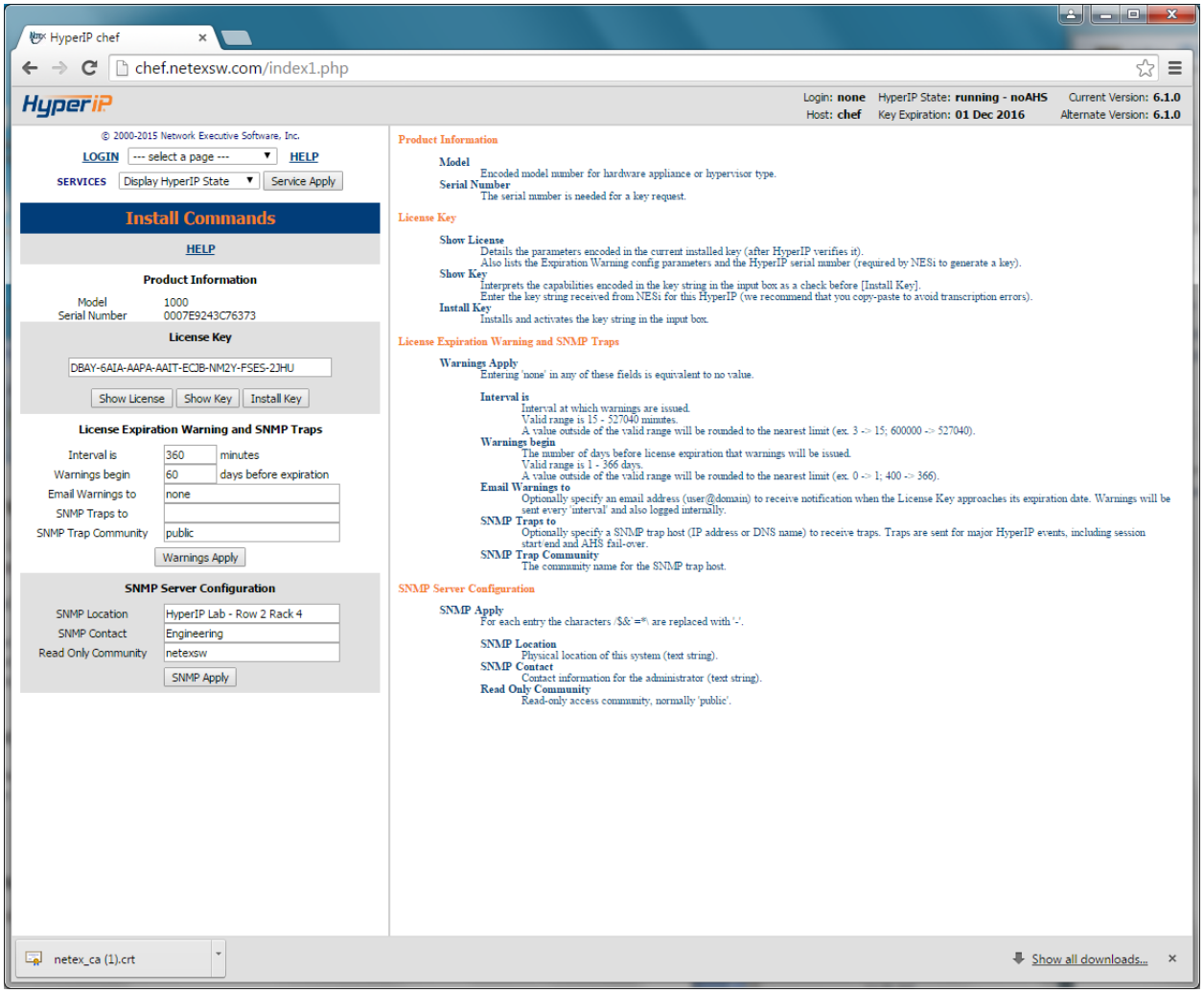

Figure 12: Install Commands Web Page with Help

HELP

Clicking on Help will display a summary of help information for this page (as shown in Figure 12: Install Commands Web Page above).

Product Information

This section contains information regarding the model of the hardware appliance or the hypervisor type and the serial number, which is required when requesting a license key.

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 <***Show License***> 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 <***Show 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 <***Show License***> will show the new license information for HyperIP per the installed key; i.e. compression, bandwidth, etc.

License Expiration Warning and SNMP Traps

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 (mail_id@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, 1 – 366, in the box provided. Enter the desired frequency (in minutes 15 – 527040) 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 Apply)***> 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 Server 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 Apply***> to apply.

System Configuration Page

The following figure is an example of the display seen when selecting the System Configuration in the <-- ***select a page***--> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Help under the System Configuration title. 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 servers on site, such as the name server or mail hub.

Current settings are displayed in the respective boxes. To change a 'Host Configuration' field, enter the updated value in the appropriate box and click <***Host Apply***>.

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).*

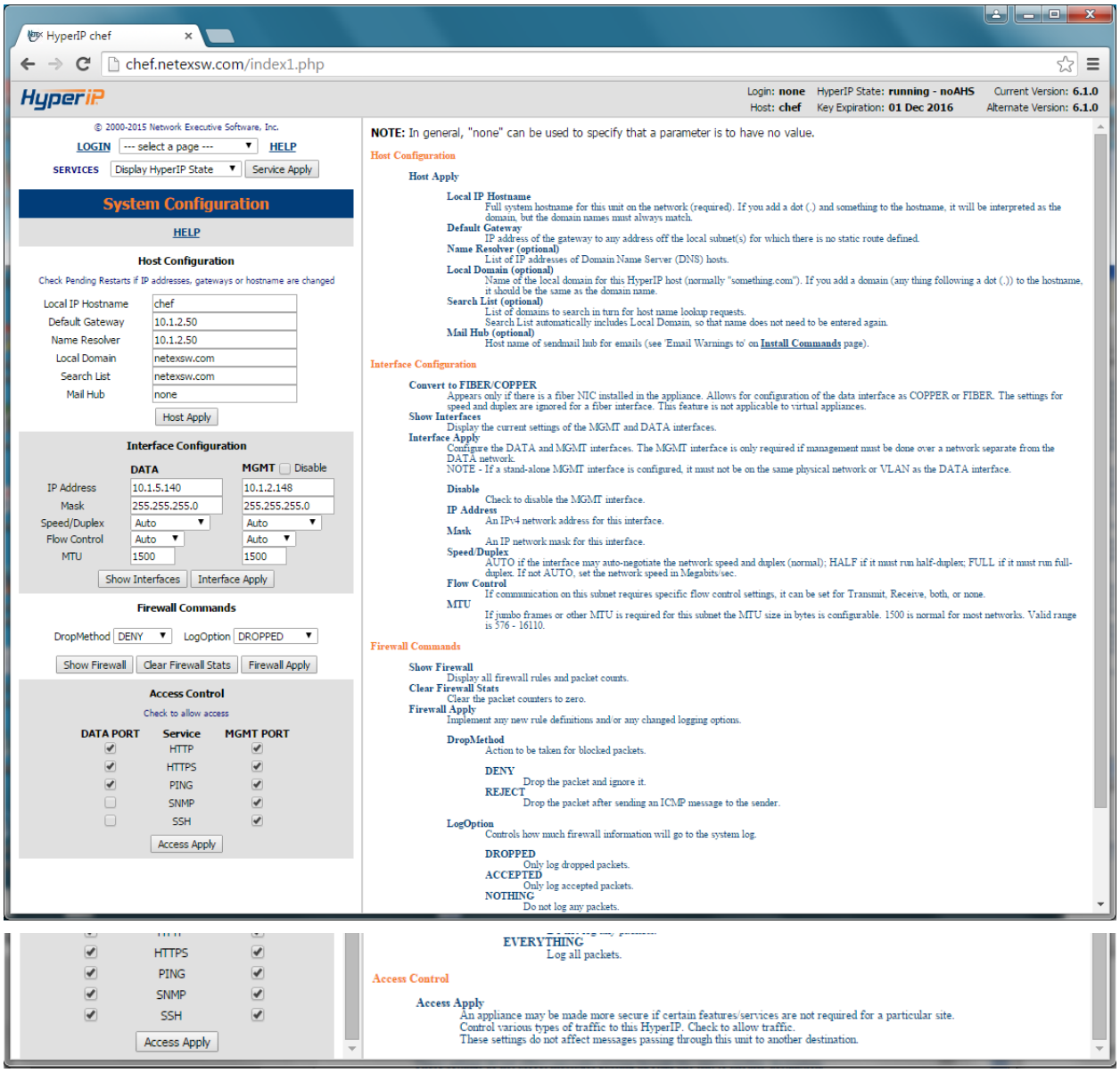

Figure 13: System Configuration Web Page with Help

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

HyperIP Configuration Page

The following figure is an example of the display seen when selecting the "HyperIP Configuration" option in the <***—select a page--***> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Help under the System Configuration title. 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.

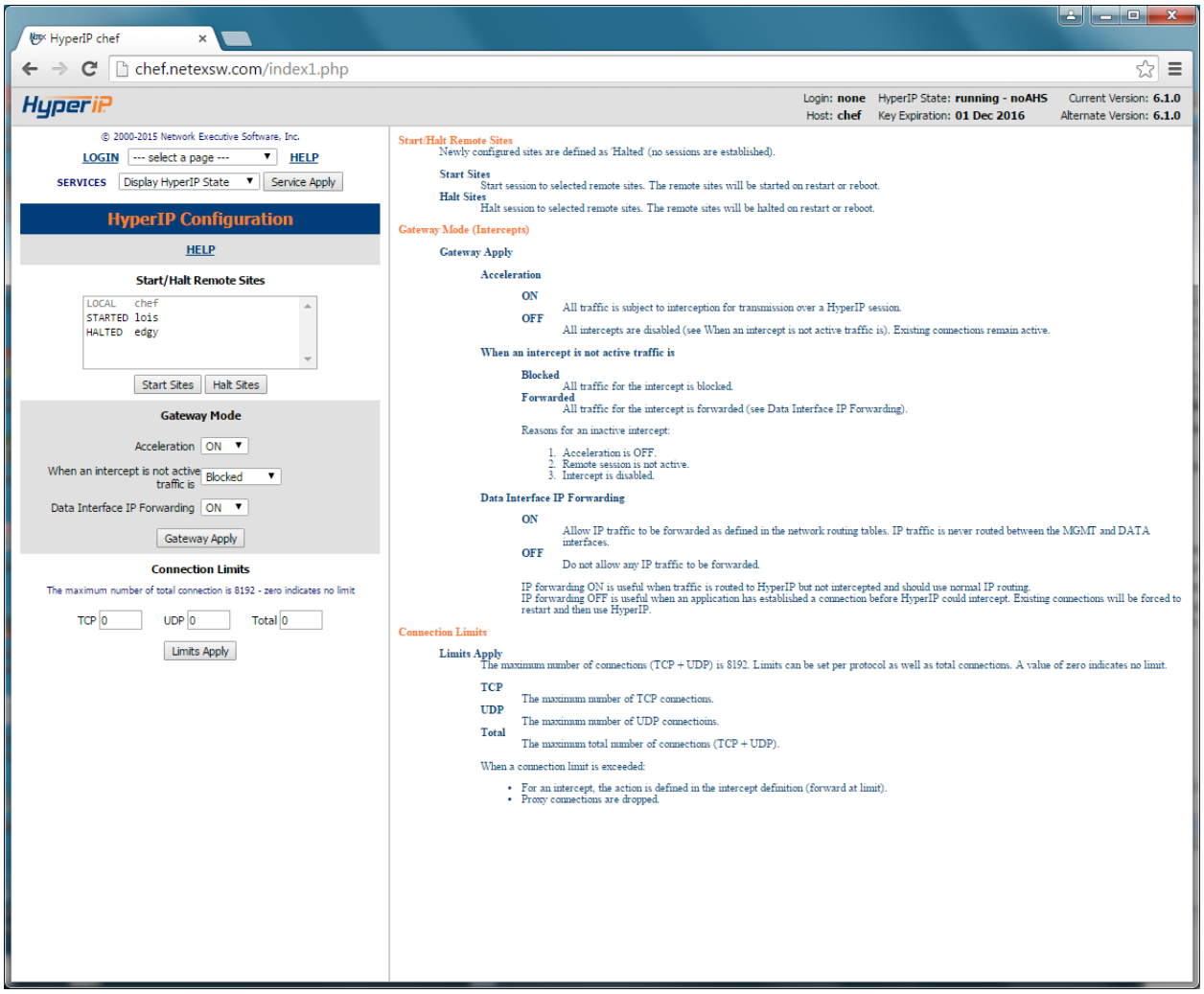

Figure 14: HyperIP Configuration Web Page with Help

Site Add / Delete Page

The following figure is an example of the display seen when selecting the “Site Add/Delete” option in the <***—select a page--***> drop down menu in the top left frame. This information is displayed and entered in the right frame. Site adding/deleting 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.

This page shows currently configured HyperIP sites (or –none-).

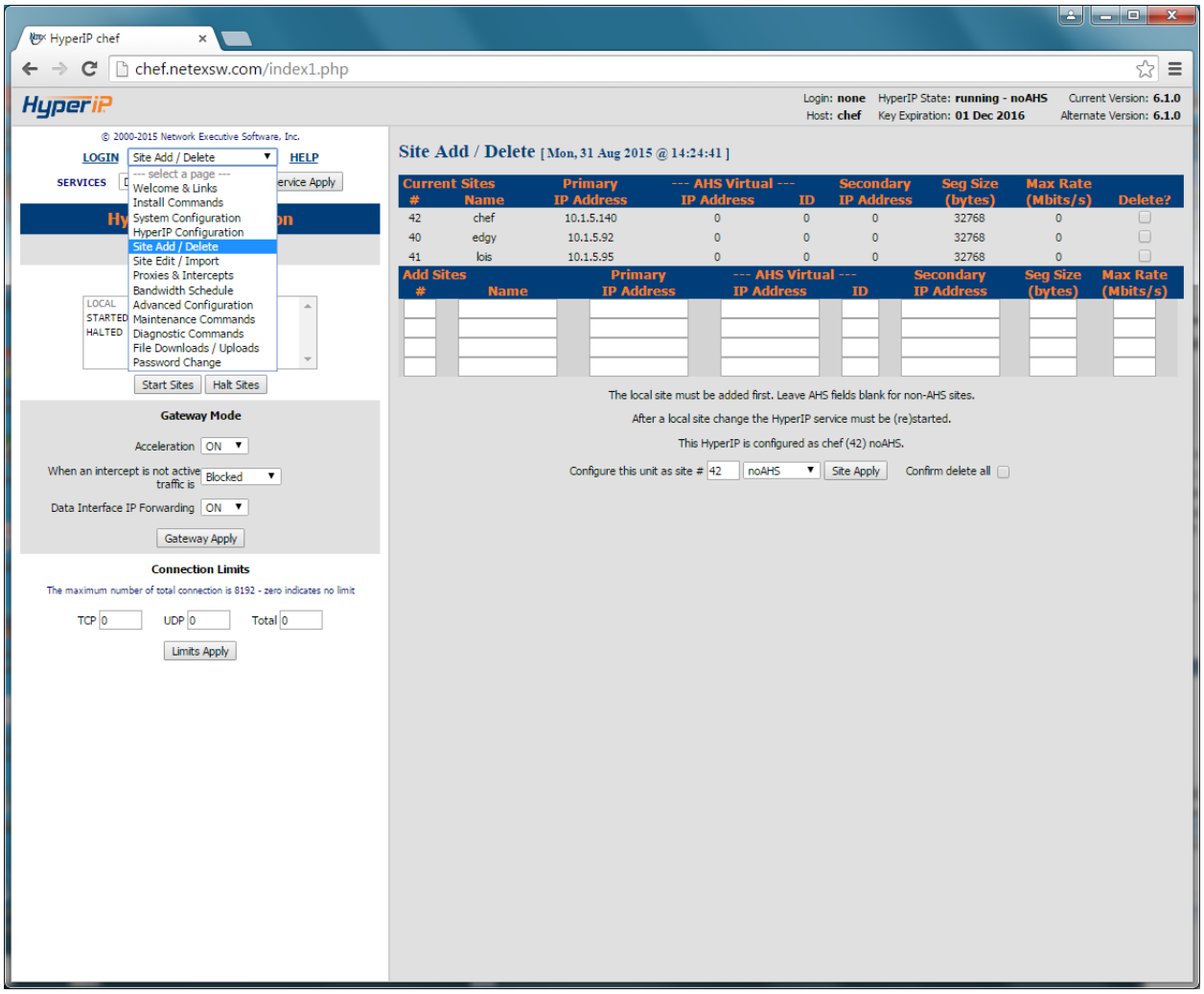

Figure 15: Site Add / Delete Web Page

Following the Current Sites is a fill-in form to configure the information required for session establishment between this HyperIP and all other (HyperIP) sites. Up to four sites may be configured at a time in this section. (Refer to Figure 14 above.)

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

(Site) #

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

(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.

(AHS 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

Seg Size

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

Max Rate

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 <**Site Apply**> button. If more than four sites are to be configured, repeat this process as needed.

To delete all configured sites, select the “Confirm Delete All” box, then click the <**Site Apply**> button.

Site Edit / Import Page

The following figure is an example of the display seen when selecting the “Site Edit / Import” option in the <***—select a page--***> drop down menu in the top left frame. This information is displayed and entered in the right frame. Site adding/deleting 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.

This page shows currently configured HyperIP sites (or –none-).

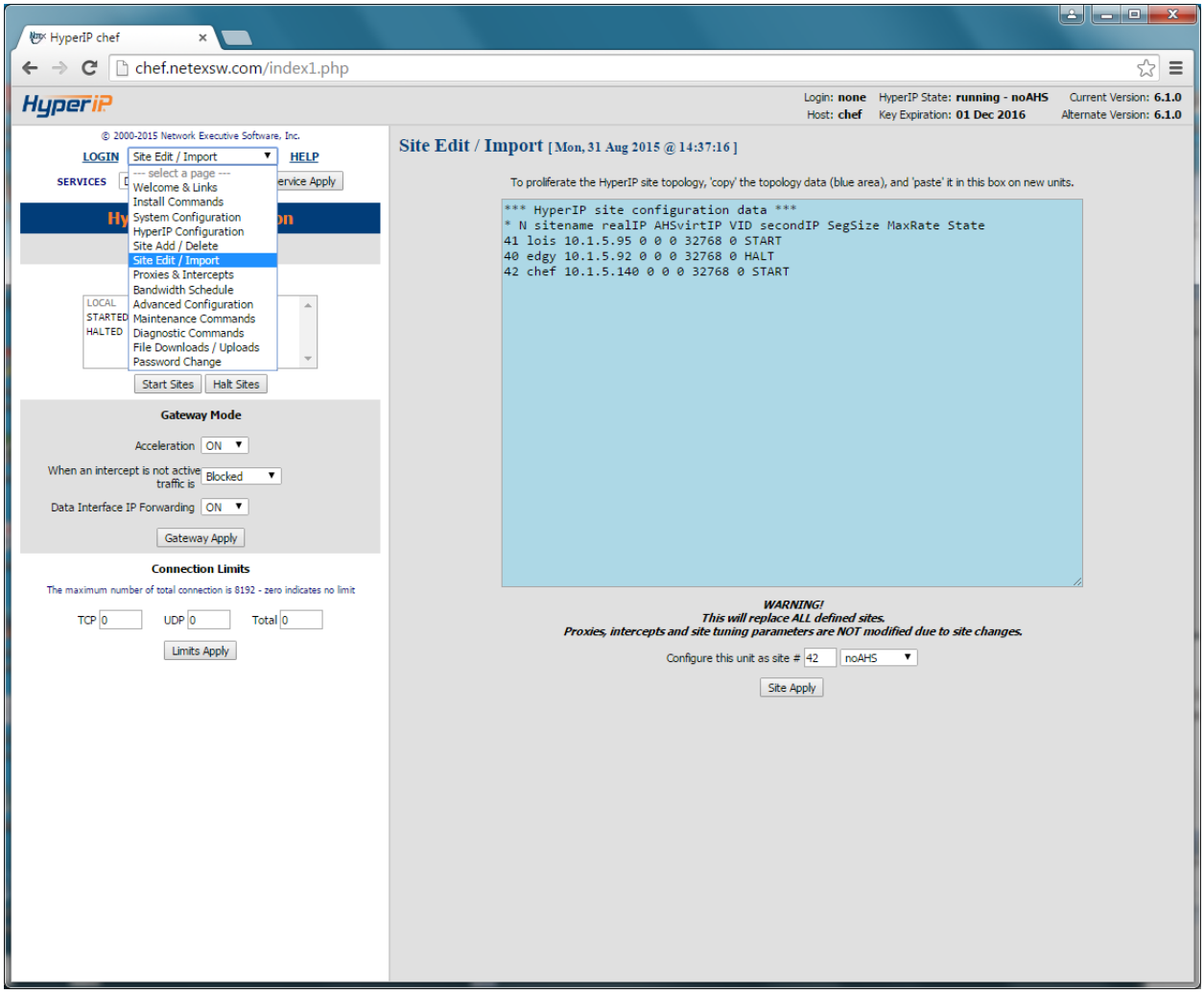

Figure 16: Site Edit / Import Web Page

Once one HyperIP is configured you can copy-paste the configuration data from the blue box on this page to the corresponding box on an unconfigured unit, enter the site number and AHS role of the new unit and click the <**Site Apply**> button. This will configure the sites as if they were entered above.

Modifications to the Sites can be done on this page as well, however, note that all sites are first deleted and then re-added. See definitions in section Site Add / Delete Page on page 54.

Note: There is minimal syntax checking when this is implemented.

Proxies & Intercepts Page

The following figure is an example of the display seen when selecting the “Proxies & Intercepts” option in the <***—select a page--***> drop down menu in the top left frame. This information is displayed and entered in the right frame. Configuring Proxies and Intercepts is typically performed only at installation time, but may also be required if the traffic HyperIP is to tunnel changes, or when adding/removing HyperIP sites.

This page shows currently configured proxies and intercepts (or –none-). 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.

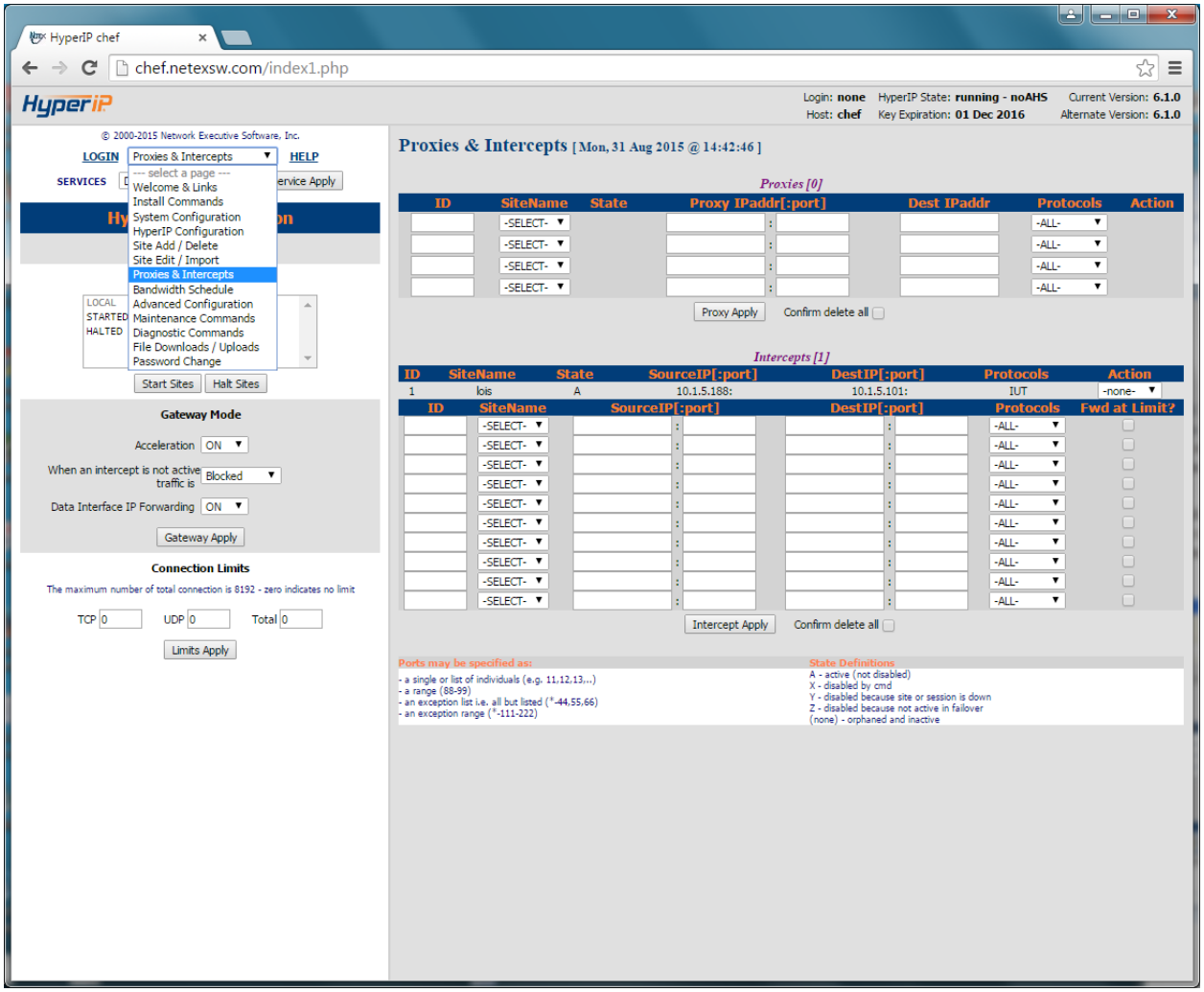

Figure 17: Web Browser Proxies and Intercepts Web Page

HyperIP Proxies

ID A unique identifier (consisting of 8 alphanumeric characters – case insensitive) for the proxy definition

State State of the Proxy as defined: A - active (not disabled) X - disabled by cmd Y - disabled because site or session is down Z - disabled because not active in failover (none) - orphaned and inactive

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 A unique identifier (consisting of 8 alphanumeric characters – case insensitive) for the intercept definition

SiteName Destination HyperIP site for traffic matching this intercept

State State of the Intercept as defined: A - active (not disabled) X - disabled by cmd Y - disabled because site or session is down Z - disabled because not active in failover (none) - orphaned and inactive

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 ‘Data Interface IP Forwarding’ setting for gateway mode.

Bandwidth Schedule (Rate Limiting) Page

The following figure is an example of the display seen when selecting the “Bandwidth Schedule” option in the <***—select a page--***> drop down menu in the top left frame. This information is displayed and entered in the right frame. 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.

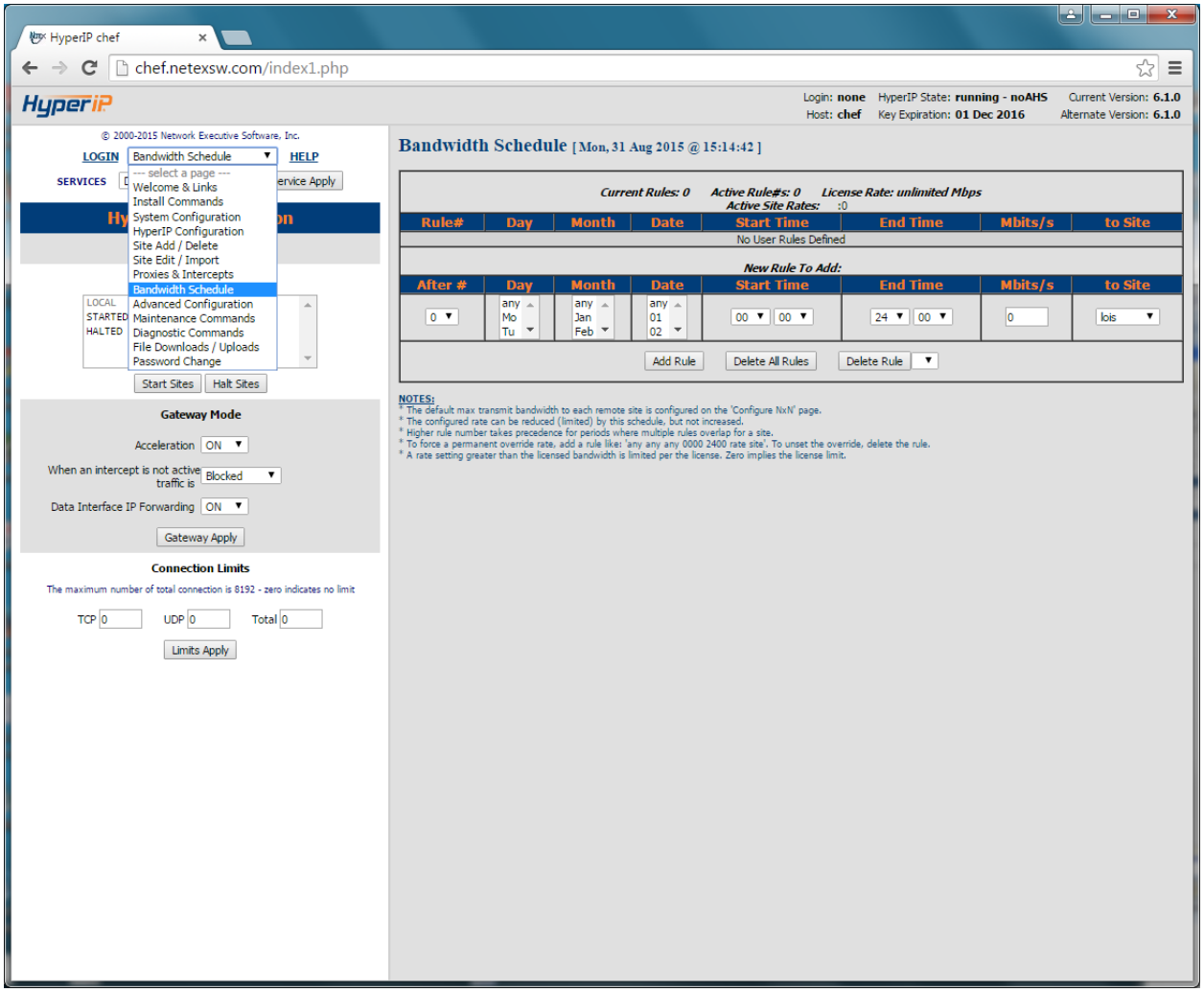

Figure 18: Bandwidth Schedule Web Page

The day/month/date settings are logically ‘OR’ed, so that if any of the 3 match with ‘now’, the rule applies. The rule number is the priority; the higher the number the higher the priority.

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

Advanced Configuration Page

The following figure is an example of the display seen when selecting the Advanced Configuration in the <--***select a page***--> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Help under the Advanced Configuration title.

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

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

Another section is used to set the local time zone for this HyperIP, and to determine whether the system time is to be synchronized with utilizing NTP**.** Advanced configuration is typically NOT required, and usually performed only at installation time, but may be required if the network configuration is changed.

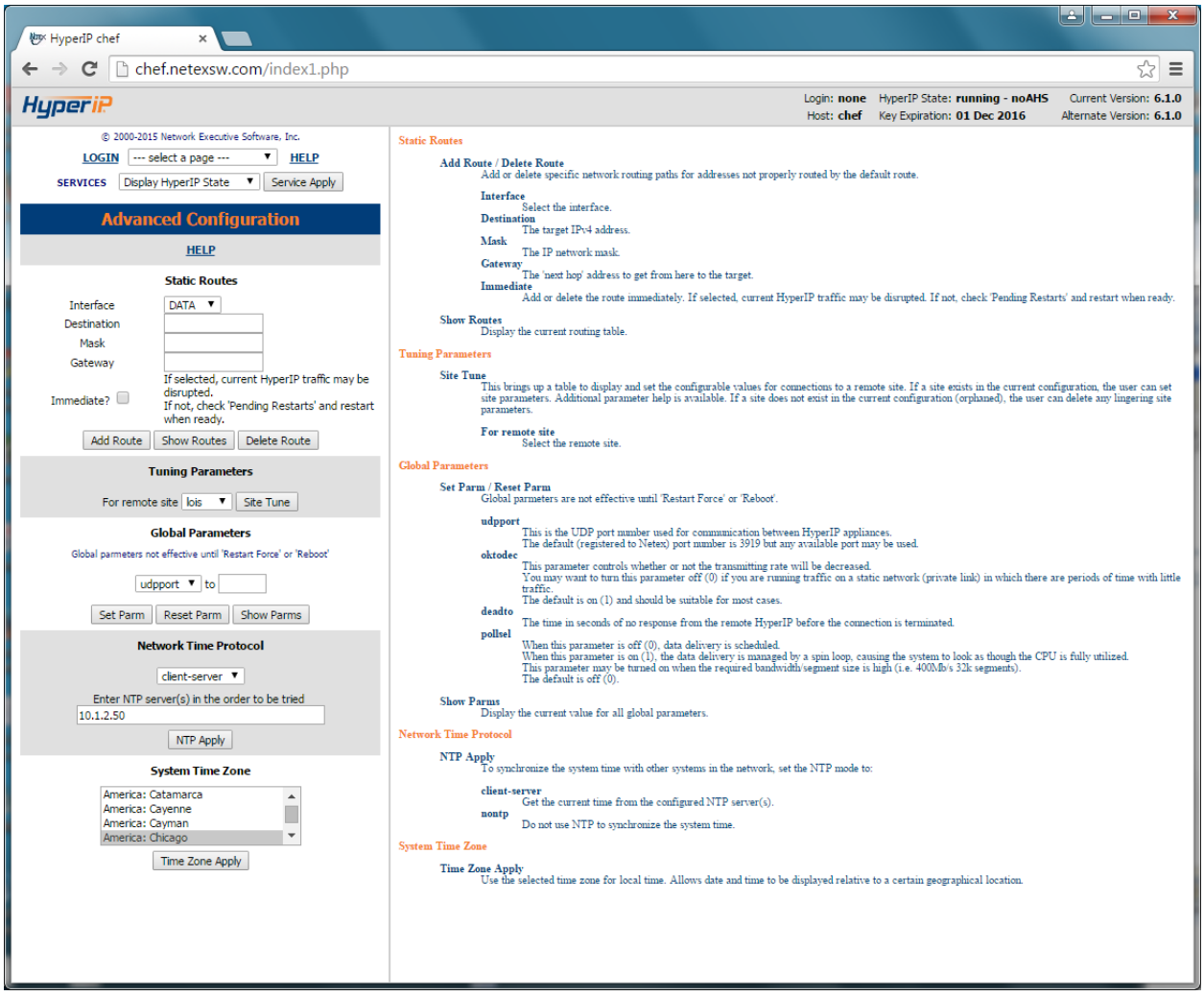

Figure 19: Advanced Configure Web Page with Help

The following is an example of the display seen when selecting remote in the “Tuning Parameters” section and clicking on <Site Tune>.

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***.

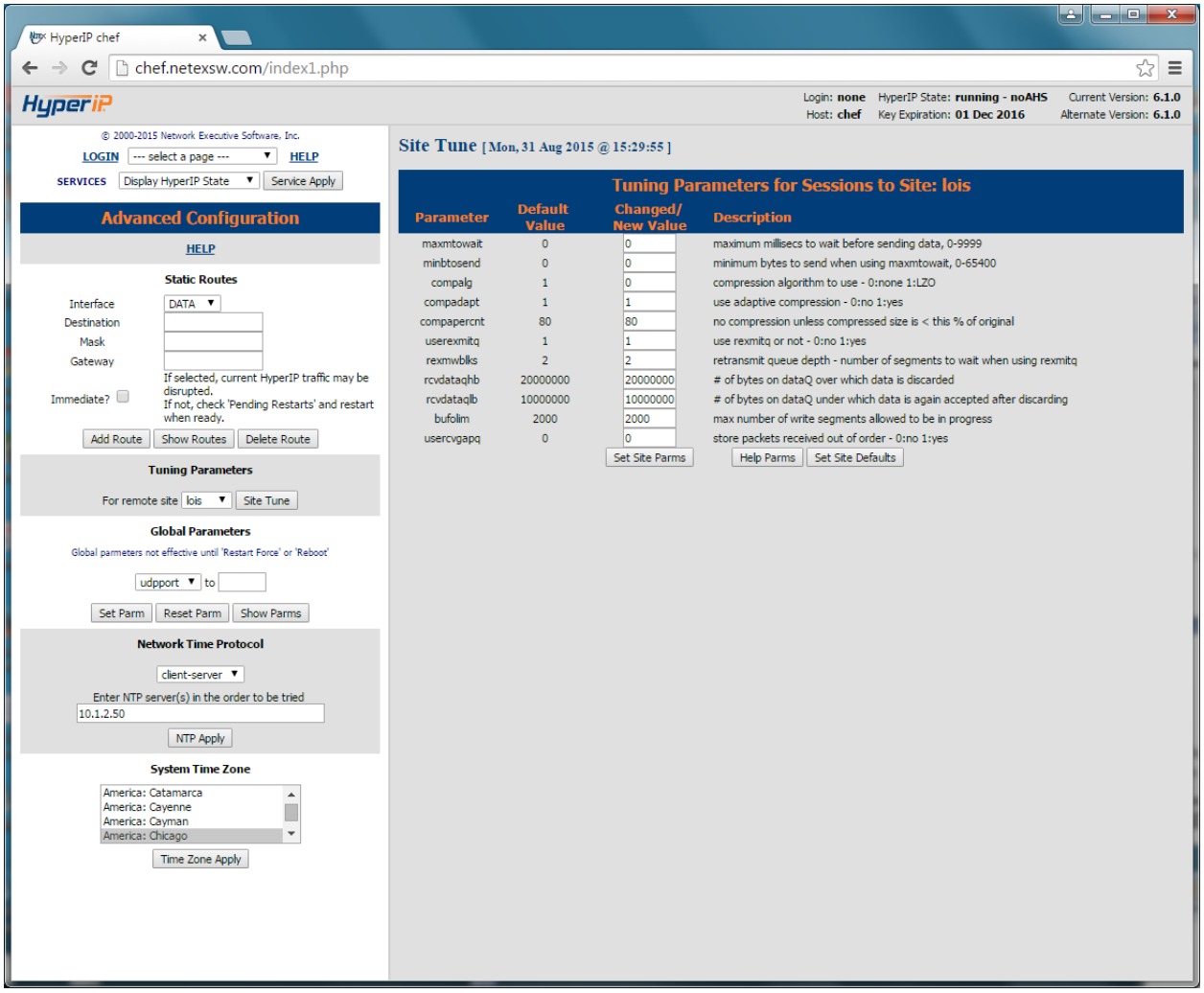

Figure 20: Tuning Parameters Web Page

For details on the Site Tune Parameters, click on the <Help Parms> button in the right frame.

Maintenance Commands Page

The following figure is an example of the display seen when selecting the Maintenance Commands in the <--***select a page***--> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Help under the Maintenance Commands title.

This page is used to perform several maintenance functions for HyperIP; such as saving/restoring configurations, viewing logs and downloading new releases of HyperIP software.

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

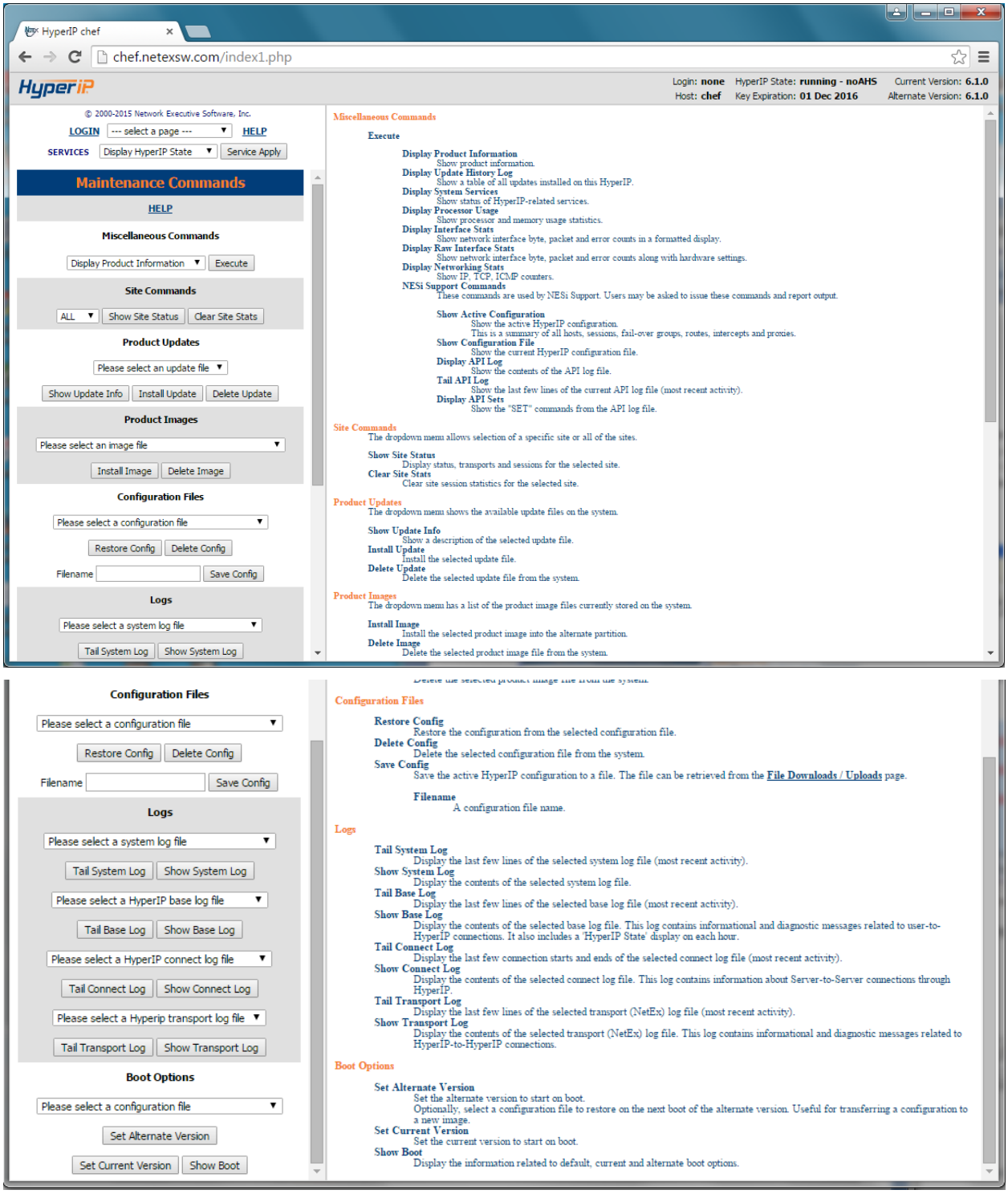

Figure 21: Maintenance Web Page with Help

Diagnostic Commands Page

The following figure is an example of the display seen when selecting the Diagnostic Commands in the <-***-select a page***--> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Help under the Diagnostic Commands title.

This page is used to perform several maintenance functions for HyperIP; from evaluating the connection to dumping diagnostic information to setting up remote logging.

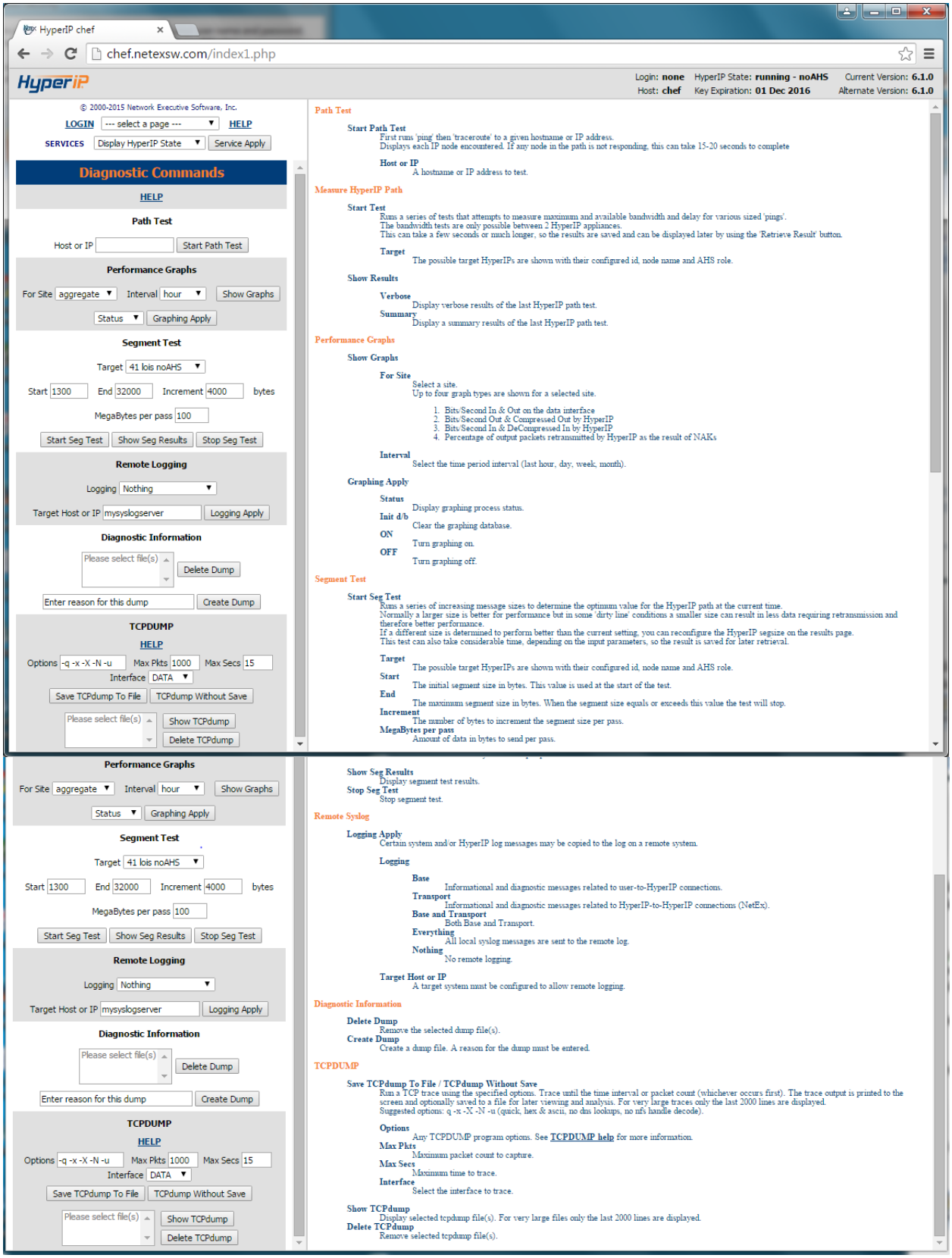

Figure 22: Diagnostic Commands Web Page with Help

The following is an example of the tcpdump output:

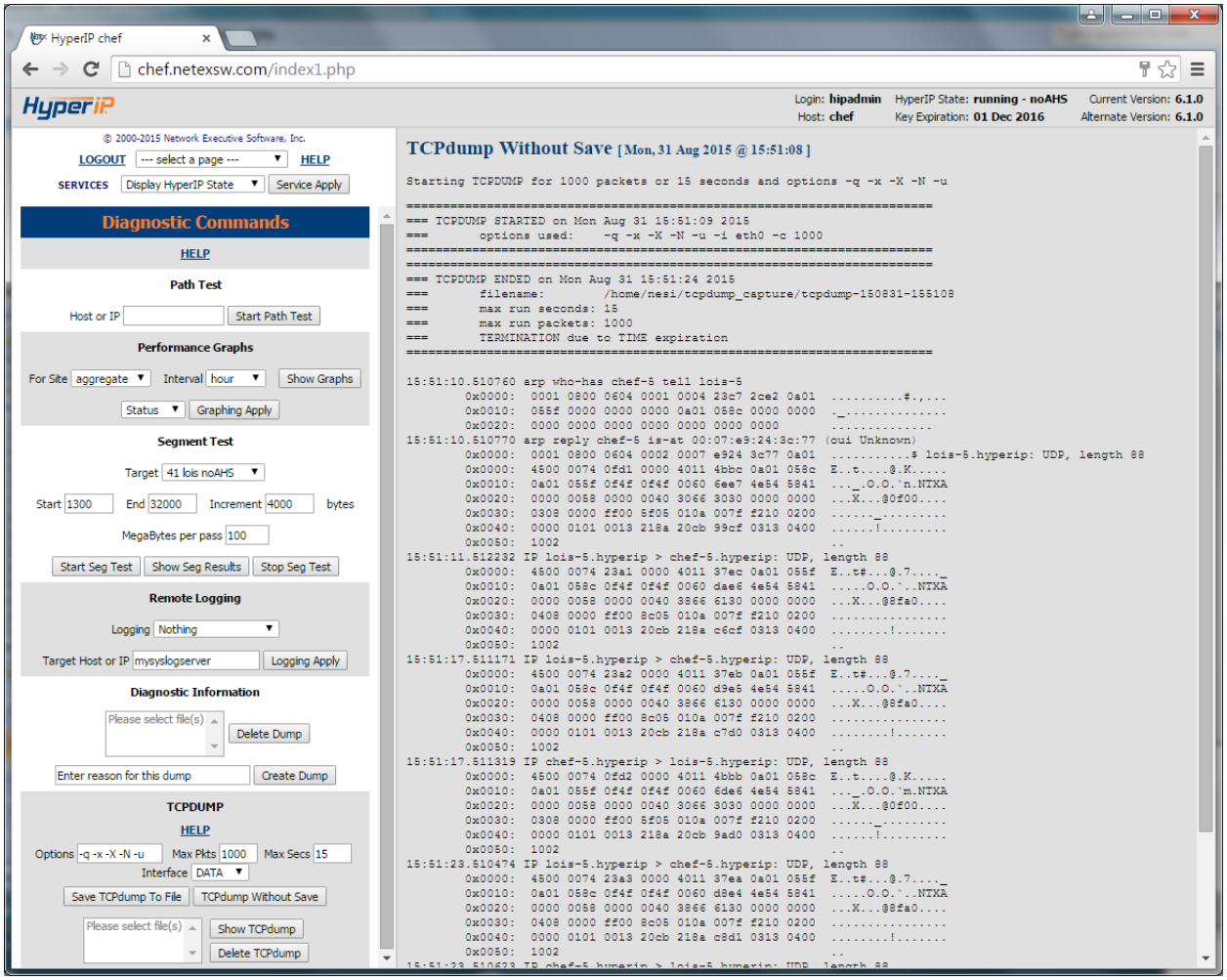

Figure 23: Diagnostic Page; tcpdump output sample

File Downloads/Uploads Page

The following figure is an example of the display seen when selecting the File Downloads / Uploads in the <***--select a page--***> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Help under the File Downloads / Uploads title.

This page is used to perform HTTP or HTTPS downloads of all appropriate maintenance files for HyperIP.

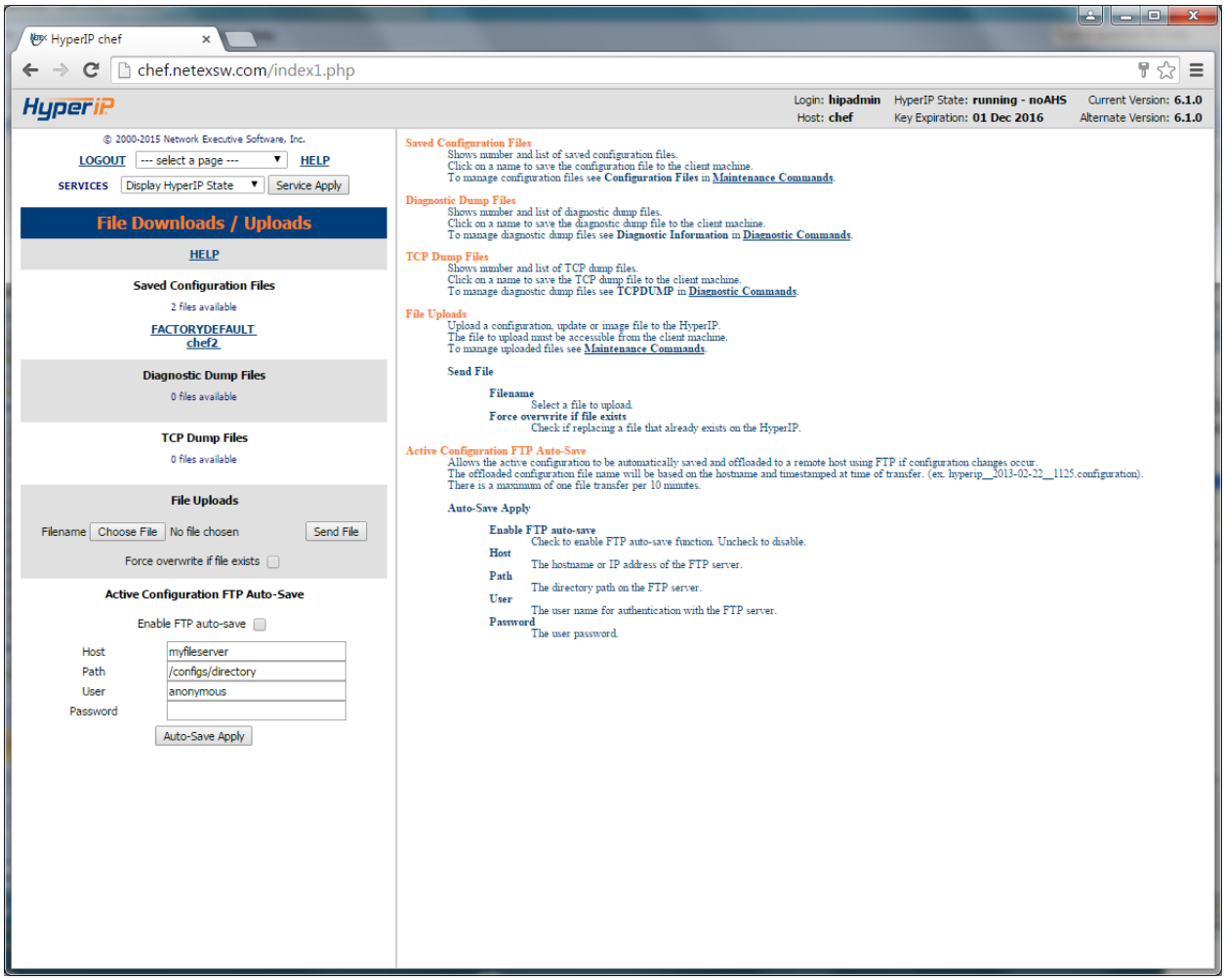

Figure 24: File Downloads/Uploads Web Page with Help

Download to your browser workstation

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

Upload from your browser workstation

To upload a file from your workstation, in the File Uploads section, “Choose File” 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 an update (patch), install a product image (to the alternate partition) or restore a configuration file.

Password Change Page

The following figure is an example of the display seen when selecting the Password Change in the <-- ***select a page***--> drop down menu in the top left frame. The right frame in the following display is the result of selecting the Help under the Password Change title.

Monitor Password

The HyperIP administrator can optionally set up an access password to prevent unauthorized access to HyperIP. When the monitor 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.

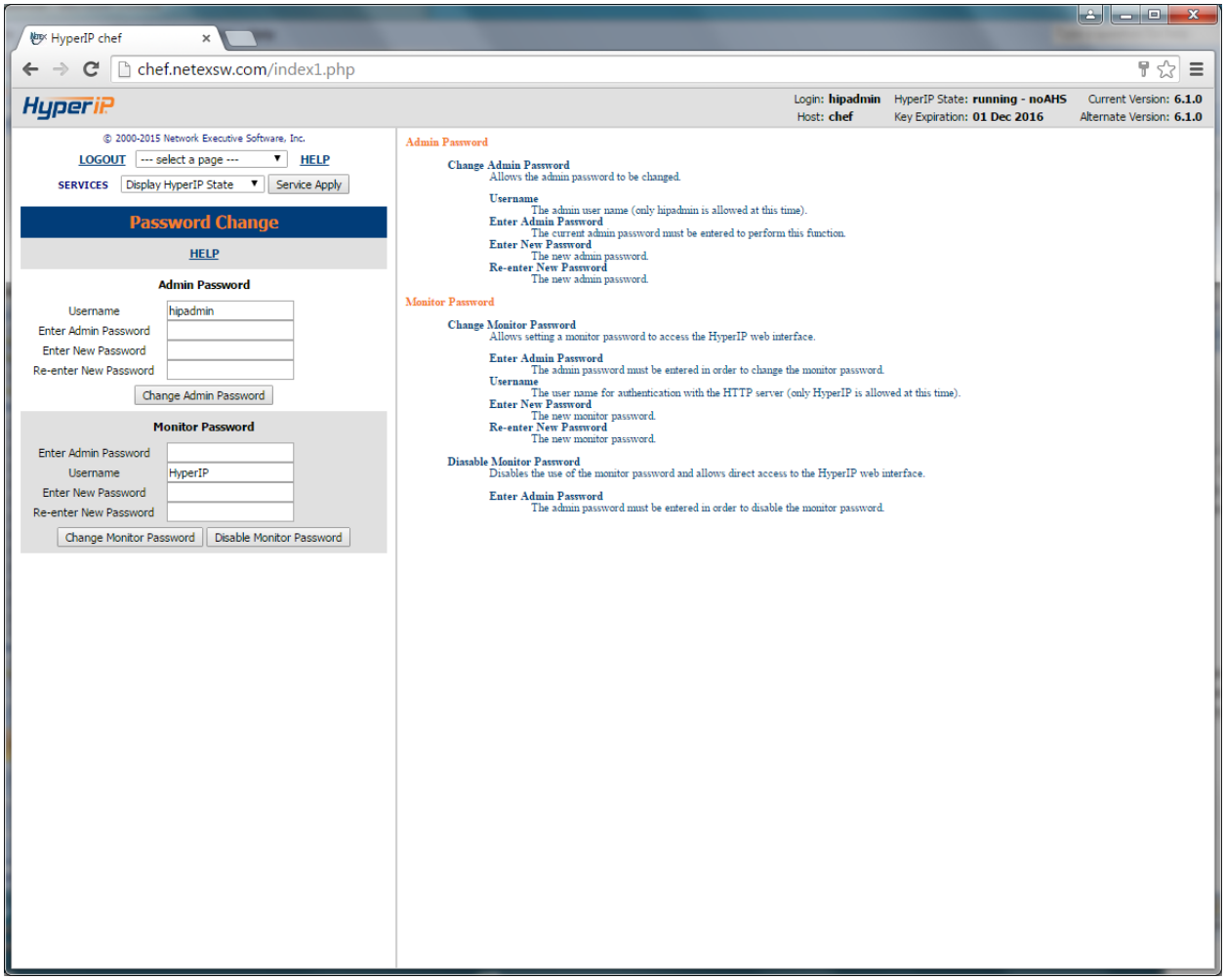

Figure 25: Password Change Web Page with Help

Operational Procedures

Initial Configuration via console to Use Web Interface

The detailed installation can be found in the appropriate HyperStart Guide for your hypervisor (MS Hyper-V or VMware).

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 console, log in as user "*hipadmin*". The default password is *'hipadmin'*.
2. Use the CLI commands to set the hostname, modify the default IP address and the default gateway:

```
cfgHostename <hostname>
 configure IP hostname

  hostname     data or mgmt

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


cfgDefaultGateway <IP_ADDRESS>
 configure the default gateway

  IP_ADDRESS   IP address of default gateway
```

3. Reboot HyperIP by using the following CLI command:

```
reboot
```

4. Be sure the physical network is connected to the management network/switch/hub.
5. Optional: 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. (It will prompt for the VCenter user's password):

```
vCenterRegister <intf> <server> <userid>
 Register the HyperIP plugin with VMware Virtual Center

  intf     data or mgmt (data/mgmt)
  server   Virtual Center hostname or IP address
  userid   Virtual Center userid
```

6. 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. Go to the "Maintenance Commands" page, under "Configuration Files" section.
3. Enter a *useful* filename in the Filename text box (i.e. hostname-date)
4. Click on **<Save Config>** to save the configuration to the HyperIP's hard disk.
5. Now go to the "File Downloads/Uploads" page, under the "Saved Configuration Files" section and select the saved configuration file by the name from Step 3 above. 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 earlier then 5.5.1 are not supported.*

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, under "File Uploads" section. Click <**Choose File**> and enter the filename or select the appropriate configuration file from your workstation. Then click <**Send File**>.
3. On the "Maintenance Commands" page, under the "Configuration Files" section, select the appropriate configuration file and click on **<Restore Config>** to restore the configuration.
4. 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. 6.1.0).
2. It is strongly recommended that the HyperIP's configuration is saved and stored to your workstation. (See the operational procedure "Saving HyperIP Configuration" on page 72 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, under the "File Uploads" section and click <**Choose File**> to find the update file stored on your workstation in Step 3 above. Select <**Send File**>.
6. On the "Maintenance Page", under the "Product Updates" section, select the appropriate patch file in the dropdown list and click **<Install Update>**. The update may take several minutes. The results will be displayed in the right-hand frame when complete.
7. 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.

New Product Version (Image) Install 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 active/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. 6.1.0).
2. Request a download by email to support@netex.com. The response will include a time sensitive link to download the HyperIP image to your workstation. Save the image 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 and then stored to the workstation. (See the operational procedure "Saving HyperIP Configuration" for more details on page 72.)

4. Point your web browser to the (AHS backup/standby) HyperIP, and enter the admin password.
5. Go to the "File Downloads/Uploads" page, under the "File Uploads" section and click <**Choose File**> to find the upgrade (.iso) file stored on your workstation in Step 2 above. Select <**Send File**>.
6. Now, on the "Maintenance Commands" page, under "Product Images" select the image filename (.iso from Step 2) from the drop down menu and click <***Install Image***>. 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 new image running, scroll to the bottom of the "Maintenance Commands" page to the "Boot Options" section and select the configuration file (if appropriate), click <**Set A*lternate Version***>. Now the HyperIP needs to be rebooted. Select the "Reboot" menu item from the "SERVICES" in the top left frame and click on the <***Service Apply***> button. Execute and confirm the appropriate restart. This will take a few minutes. After a few minutes you can reload your browser page.
8. The upgraded HyperIP will now be operational as shown by the Current Version in the top status bar.

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.

- 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.
- The versions are listed in the top status frame.

Use the buttons on the "Maintenance Commands" page, under the "Boot Options" section to change which partition to boot from.

Restoring or Reverting a Virtual Machine from an Operational Snapshot

If you are using a virtual machine management tool to save snapshots and want to restore or revert the virtual machine to a point in time, you will need to perform a Restart Force operation on the virtual HyperIP so the session information is restarted and avoid using stale information.

Customer Troubleshooting

NOTE: The following procedures apply to HyperIP Release 6.1.0 and above.

Accessing HyperIP

Open a browser window, connect to HyperIP using 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 under "SERVICES" in the top left frame on every web page. For more information on the "Display HyperIP State" command, see the section "Troubleshooting using the Display HyperIP State Command" on Page 81.

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

Informational Logs

Several logs are maintained in HyperIP. Each internal component maintains separate logs as well as a system logs. HyperIP's transport maintains **Transport.log** files and the HyperIP application maintains **Base.log** files 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 on the "Maintenance Commands" page, under the "Logs" section. The logs may either be "tailed" or completely displayed.

System Dumps

System dumps can be created by going to the "Diagnostic Commands" page, under the "Diagnostic Information" section. Enter a reason for the dump in the text box and click <**Create Dump**>. Once the dump file is created, it should be moved to your workstation, via the "File Downloads/Uploads" page, under the "Diagnostic Dump Files" section and then to Network Executive Software's FTP server (https://ftp.netex.com/upl). Diagnostic files should be taken from all HyperIPs in question. **IMPORTANT NOTE:** ***If the connection between HyperIP appliances is not operational, creating the diagnostic dump file 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.”

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.). All log files are captured in a diagnostic 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.

As with the system log (the messages file), there may be multiple instances of the HyperIP log (netex.log) (.1, .2, .3, etc.). All log files are captured in a diagnostic dump.

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 Commands” Page

On the “Diagnostic Command” page, under the “Path Test” section a Host or IP address may be entered in the text box and the <**Start Path Test**> clicked. This issues a series of “pings” and “traceroutes” to the Host or IP address entered, and displays the results.

Under the “Performance Graphs” section on this page are selection for viewing various performance graphs. 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

Under the “Segment Test” section on this page is 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.

As noted elsewhere, HyperIP diagnostic dumps are initiated from this page also.

Advanced Configuration 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.

Under the “Tuning Parameters” section is a button <**Site Tune**> to launch a frame to further tune how HyperIP optimizes traffic to specific remote sites. The launched frame contains a <**Help Parms**> button which provides information on setting these parameters.

Under the “Global Parameters” section are global settings (which are not typically altered) for HyperIP’s transport.

Network Time Protocol settings are also located on this page.

System Configuration Page

From the ”System Configuration” page, the system name, domain, mail hub and name server is configured, the Ethernet interface configuration may be altered and examined, and HyperIP’s managed access options can be configured. Adjustments to the firewall and restarting the system’s firewall are performed here as well.

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 81.

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

1. Hardware problem (on the physical machine)
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

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.

The following is a short list of things to check to determine if the older hardware appliance 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 physical hardware 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 ssh request from a locally attached PC. Attach a terminal to the serial port, and use the hypervisor's CLI commands to ensure the Ethernet ports are properly configured and active. (Faulty Ethernet interface, cable and or switch port).
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, follow your hardware vendor's return process

Cannot Access HyperIP to Perform Initial Configuration

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

- Hardware and hypervisor is powered up.
- Physical 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.

Cannot Access HyperIP Web Interface after Initial Configuration

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

Login to HyperIP (via 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.

Cannot communicate between HyperIPs

Each HyperIP 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 application 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 hardware and hypervisor 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.

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 the section Cannot communicate between HyperIPs on page 78. 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.
- 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.

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 "Diagnostic Commands" page contains tests to evaluate the network between HyperIPs. 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) "Path Test" executes a series of pings and traceroutes. This may help determine if there are unexpected delays in the path to the remote HyperIP site.
            (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 appropriately. Some switches do not auto-negotiate well, and so interfaces 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 the interface is connected.
   b) View Raw Interface Stats on the hypervisor or switch for errors and negotiated speed and duplex states.
   c) Verify end-to-end connectivity, and round trip delay times, by issuing pings and/or traceroute/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.)

- ***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:

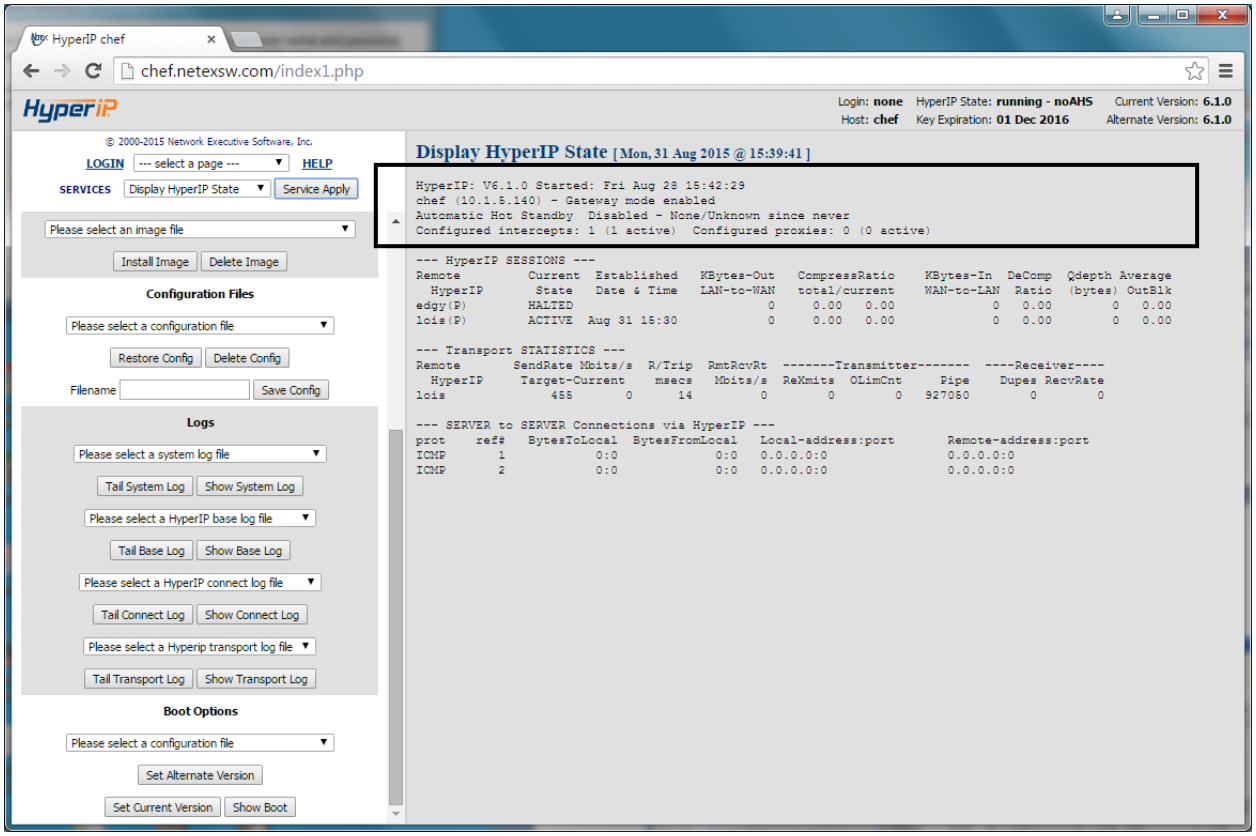

Figure 26: Display HyperIP State Command Output, Part 1

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.

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.
CLOSE	Session has issued a close.
DSCPND	A disconnect is pending on the session.
DISC	Session has issued a disconnect.
WAIT	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.
INIT	Session in initialize state.
INITPND	Session initialize pending.
HALTED	Session halted by HyperIP user.
HALTPND	Halt pending on this session.

PACED Session received a pace (slowdown) notification from the remote HyperIP.

DOWN Session received a SHUTDOWN notification from the remote HyperIP.

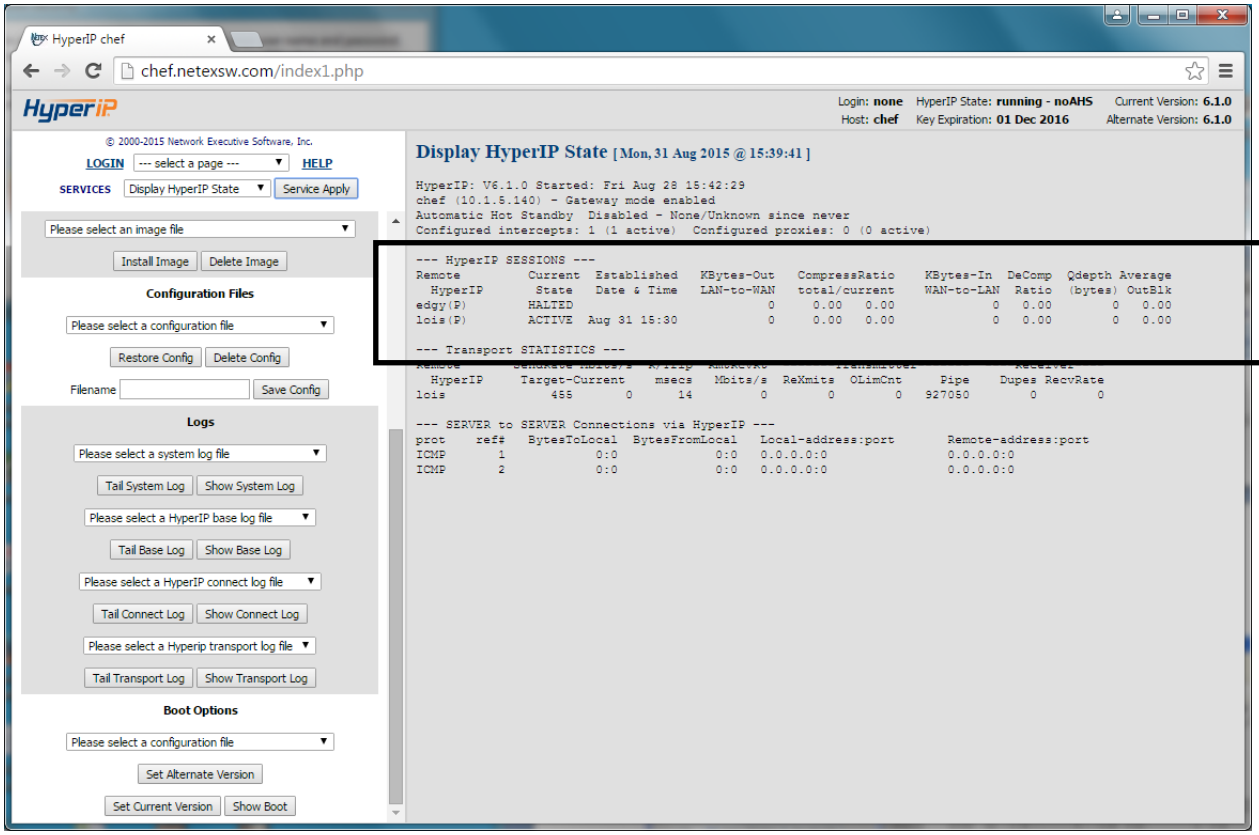

Figure 27: Display HyperIP State Command Output, Part 2

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 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

Title	Definition or Details
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 28: Details for HyperIP State Command Output, Part 2

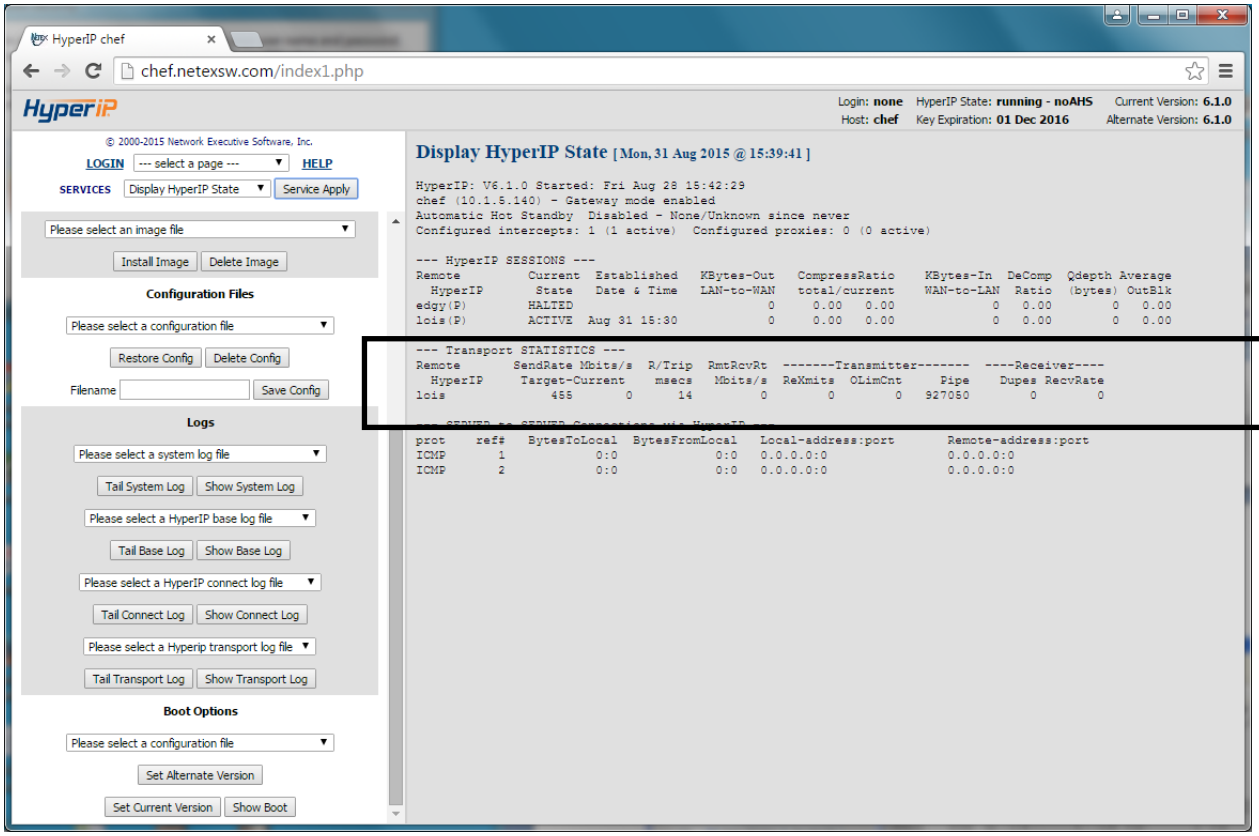

Figure 29: Display HyperIP State Command Output, Part 3

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 by the *MaxRate* 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.

Title	Definition or Details
R/Trip msecs	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 rage 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 30: Details for HyperIP State Command Output, Part 3

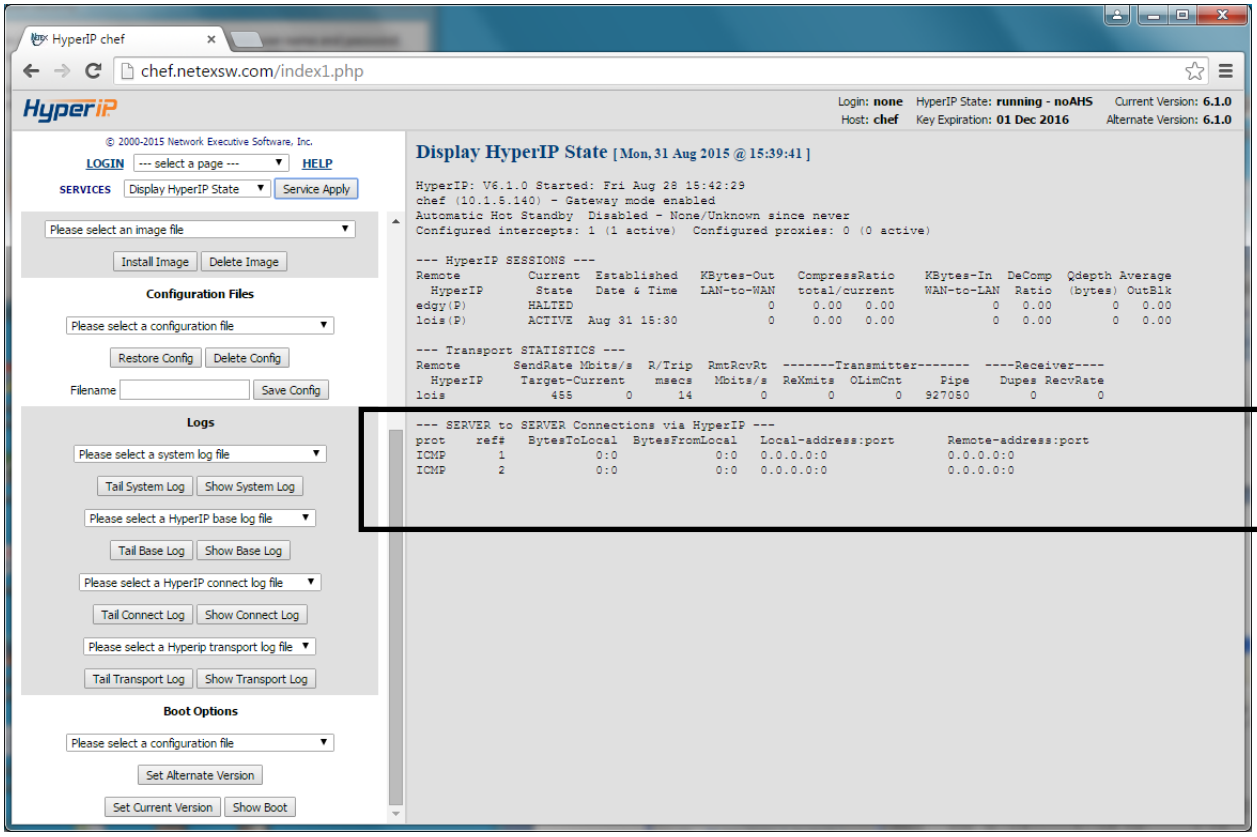

Figure 31: Display HyperIP State Command Output, Part 4

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 32: 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 Path" facility on the browser "Diagnostic Commands" 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 Path" facility on the browser "Diagnostic Commands" 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	Look in message log for Sendmail messages:
	1. If no Sendmail messages – Mail hub or administrator email address not setup
	2. If message log entry looks like:
	`Nov 5 10:19:37 HYPERIP sendmail[21491]: iA5GJaH21487: iA5GJbG21491: DSN: Host unknown (Name server: YOURMAILHUB.com: host not found)`
	Configured Mail hub cannot be resolved by your nameserver
	3. If message log entry looks like:
	`Nov 5 10:25:25 HYPERIP sendmail[30567]: iA5GPPF30567: to=ADMIN@ADMINDOMAIN.com, delay=00:00:00, xdelay=00:00:00, mailer=relay, pri=30399, relay=YOURMAILHUB.com. [10.1.3.1], dsn=5.1.1, stat=User unknown`
	Configured administrator email user is not correct for the Mail hub

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 33: Symptom and Problem Determination Table

Appendix A: Error Codes

System Log File

System messages are found in the system log file, which may be viewed by using the browser on the "Maintenance Commands" page, under the "Logs" section. 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, NRBLEN exceeds NRBBLKO	3
TNONMAX	2008	During a non-segmented write, NRBLEN 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, NRBLEN 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
SRBUSY	3307	A SREAD request has been issued to a session connection that is in the process of servicing a remote caller or NETEX initiated Disconnect. A Disconnect Indication is pending from NETEX	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

Name	NRBStat	Meaning	Action
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
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

Name	NRBStat	Meaning	Action
NRBUSY	4307	An NREAD was issued to a connection that is servicing a disconnect	1
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

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
EOVERFLOW	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 in the tutorials and the appropriate HyperStart Guide.
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:

CentOS 5

PHP

LZO Compression

KeepAlive

Watchdog

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

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

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.

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.

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:

You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

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.

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 of 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.

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:

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,

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,

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.

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.

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.

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.

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.

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.

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.

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

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.

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