



READ THIS FIRST!

Congratulations on your purchase of the NetEx HyperIP® WAN Optimizer

The enclosed CD includes HyperIP software and product documentation. If you purchased an appliance from NetEx, the software has been pre-installed at the factory but the HyperDocs CD has a recovery image for disaster recovery purposes only.

Product Keys are required to operate your new HyperIP and must be retrieved from hyperip.com. Product Keys are designed to enable the successful operation of a specific HyperIP (by an internal serial number) up to a specific bandwidth speed for a specific period of time.

A "Ship Key" is made available for each new HyperIP that will provide operation for 90 days. For continuous operation of HyperIP past the initial 90-day "Ship Key" period, a new key that provides operation for the balance of the license term ("Term Key") must be installed prior to the expiration of the "Ship Key". The "Term Key" is available once product payment has been received.

NetEx will make short term Product Keys available which allow unrestricted bandwidth for special circumstances like Recovery on Demand (RoD), Synchronize on Demand (SoD), initial bandwidth requirement evaluation, etc. Contact support@netex.com or at (800) 854-0359 for these requests.

In order to retrieve the Product Keys, NetEx customers must first register on the NetEx Registered Customer Intranet (www.hyperip.com). Customers will need their "Customer Code" to register. Customer Codes are located on the packing list that ships with each HyperIP Product. Once successfully registered, keys (when available) can be accessed at www.hyperip.com and then installed on the HyperIP with the associated HyperIP serial number. (HyperIP on VMware must be installed to obtain this serial number.)

If you cannot locate your Customer Code or your packing list, contact NetEx via telephone at 1-888-604-5573 or 763-694-4300 (Monday – Friday, 8AM – 5PM Central Time) or via e-mail at Nesi-Admin@netex.com.

IMPORTANT NOTE: THE HYPERIP SOFTWARE KEY ALLOWS OPERATION OF THE PRODUCT FOR A DESIGNATED PERIOD OF TIME. IF APPLICABLE FEES ARE NOT PAID IN A TIMELY MANNER OR IF THE LICENSE IS TERMINATED, THE HYPERIP PRODUCT MUST BE REMOVED FROM THE NETWORK, OTHERWISE IT WILL CEASE OPERATION WHICH MAY INTERRUPT DATA TRANSMISSIONS.

HyperStart for HyperIP® Release 5.5.2

This document is a 'Getting Started Guide'. If you have any problems with the installation refer to the HyperIP User Guide for detailed information and troubleshooting tips found on the HyperIP Software CD. Links to FAQs, Updates and the latest documentation for supported versions are also found on our website at <http://www.netex.com/support/product-support/hyperip>.

A configuration process must be performed on each HyperIP and a Product License Key must be installed on each HyperIP to function.

Initial Configuration for Each HyperIP

1. Register at <https://www.hyperip.com> using your Customer code.
2. Collect your site information on the Configuration Worksheet (at the end of this guide).
3. Refer to the latest FAQ and Updates at the NESi HyperIP website to get the latest news regarding HyperIP releases: <http://www.netex.com/support/product-support/hyperip>.

System Configuration for HyperIP on VMware ESX:

Installation via the console:

Define a virtual machine as a Linux virtual machine (Linux, other 32 bit), with 2 GHz CPU, 5 G storage, 1 GByte of RAM one virtual switch (two if you require a separate management interface). HyperIP requires the management and data interfaces to reside on different subnets. For optimum performance the physical Ethernet interface should be dedicated to this virtual machine. You will also need to attach the CDROM drive to the virtual machine to install the image. (You may need to modify the BIOS setting in this VM to allow booting from the CDROM.) Insert the HyperIP Software CD into the CDROM and boot up the virtual machine. Follow the prompts to restore the image. Select the "Restore (VGA Console) option. Once the software is installed, remove the CD.

- A. We recommend using the console to perform initial configuration. Login as user 'hipadmin'. The default password is **hipadmin** and should be changed on first login.
- B. One of the commands in the Command Line Interface (CLI) is LegacyDialog; enter LegacyDialog at the CLI prompt and a NESi dialog will start; select the installation wizard and enter your site parameters collected in Step 2, at the prompts. (You need to set the security Access, in the wizard, on the Management and Data Interfaces to allow HTTPS and Pings to perform the tasks described in this document.)
- C. Once access to HyperIP user interface is available, copy the HyperIP Serial Number from one of the following sources:
 - the installation wizard screen or
 - the LegacyDialog/Expert/System/License menu or
 - from the Web Maintenance Commands/Show Product Info.
- D. Email this Serial Number, along with the bandwidth which was purchase for this system and your company code to support@netex.com with the subject line containing: HyperIP Product License Key Request.
After verification, support@netex.com will notify you of your license key availability on www.hyperip.com.
- E. Exit the LegacyDialog and follow the prompts to save/implement. Reboot the HyperIP (under "restart" menu option in the LegacyDialog).

- F. If you are using a dedicated management interface, insure the physical network interface is connected to your network. Connect the management interface to your management network.

If you are using a dedicated management interface, insure the physical network interface is connected to your network.

Once configuration is complete, you should be able to successfully ping the HyperIP management IP address from other network hosts on the management network (if the security access setting allows. ping is disabled by default – to enable, go to the primary menu and select “Expert”. In the expert menu select “Access” and follow the wizard instructions.)

- G. Connect the data interface to your data network. Now you should be able to successfully ping the HyperIP data IP address from other network hosts on the data network (if the security access setting allows. ping is disabled by default – to enable, go to the primary menu and select “Expert”. In the expert menu select “Access” and follow the wizard instructions.)

Now you should be able to successfully ping the HyperIP data IP address from other network hosts on the data network (if the security access setting allows. ping is disabled by default – to enable, go to the primary menu and select “Expert”. In the expert menu select “Access” and follow the wizard instructions.)

- H. Now start a web browser on any host with network access to the HyperIP unit for subsequent monitoring or configuring. Browse (HTTPS is the default service) to the HyperIP (by host name or IP address as the URL); type the ‘hipadmin’ password in the box on the home page and click <Enter Password>. If the default password hasn’t been changed yet, it should be changed at this time. Enter the new password in the right panel and click <Change Admin password>.

- I. Go to **Configure and Start Sites for Each HyperIP**

System Configuration for HyperIP on NetEx (supplied hardware) Appliances

Installation via the Ethernet Port.

These instructions will guide you through initial installation using a web browser to connect to the HyperIP management port. For information regarding initial configuration via SSH or the serial port, refer to the HyperIP User guide. The default IP addresses for the management Port is 10.10.2.2/24. Initially, only the management port is enabled and is accessible via HTTPS or SSH only. By default the data port is not accessible.

- a. Use a workstation with an IP address on the 10.10.2.0/24 network (not 10.10.2.2) and attach to the HyperIP management port via a switch or crossover cable. Browse (HTTPS is the default service) to the HyperIP (IP address (10.10.2.2) as the URL); type the ‘hipadmin’ password in the box on the home page and click <Enter Password>. The default password is **hipadmin** and should be changed on first login. Enter the new password in the right panel and click <Change Admin password>.
- b. Go to the drop-down box at the top of the left panel and select “System Config”. Enter the information from the configuration worksheets filled out in step 2. At the bottom of each section is a “<section Apply>” button, click the <SysConfig Apply> button when the System information is complete. Click the <Interface Apply> button when the interfaces are configured and the <secure Ports> button after selecting the appropriate firewall information for this HyperIP.

If using the fiber GE port click <Convert to Fibre>. This will take a minute to move the Data port configuration from the copper interface to the fiber interface.

- c. In the “Services” drop-down window in the top left panel, select “Show Pending Restarts” and click the <service Apply> button. The right panel will display the level of restart required to implement the changes. Select the appropriate restart (reboot or restart force) in the Services drop-down window and click <Service Apply>. Confirm the action in the right panel by clicking

<confirm> or abort by making necessary changes and executing the command again with confirm.

- d. Connect HyperIP Network Interfaces to switch.

If you are using the dedicated management interface, connect the RJ45 connector (labeled 1) on the back panel to your management network.

The copper data port is the RJ45 connector (labeled 2) on the back panel. The fiber data port is on the NIC in the center of the back panel. Only one data port is active.

- e. Go to **Configure and Start Sites for Each HyperIP**

Configure and Start Sites for Each HyperIP for VMware and NetEx Appliances

4. ***Before continuing, the Product License Key must be installed. Refer to the “Read this First” page to obtain your keys.***

Click on the “Home” link in the top left panel. Enter the license key in the top section and click <Install Key>. Check the right panel information to insure the proper key for this serial number has been entered and has the expected bandwidth.

5. On the HyperIP Config web page, in the HyperIP Configuration frame, select [Configure NxN Sites] from the drop down menu and click <Topology Command>. This will bring up a form to fill in your site definitions.
6. Enter the definitions from your “HyperIP NxN Configuration Worksheet”. Note: the local site must be entered first when configuring each HyperIP.
7. When the sites are all entered in the form, in the area below the table select the site number of this (local) site and select [NoAHS] from the drop down menu. Then click <Apply Config>.

This may take a minute to complete. If errors are displayed above the table, you will need to fix them and repeat step 7. Sites that are successfully configured are displayed above the form.

After the sites are configured, do a “Restart Force”. Select “Restart Force” from the services drop down menu in the top left frame of the web interface and click the “Service Apply” button.

8. Refresh the left frame of your browser. Under the [Start/Halt Remote Sites], select the remote site and select [Start Site] in the drop down menu. Click <State Command>.
9. In the HyperIP Configuration frame, select [Bandwidth Schedule] from the drop down menu and click <Topology Command>. This will bring up a form to fill in your rate limiting schedule.
10. Create a rule after 1, for [Any] day, [Any] month, [Any] date, start time 0000, end time 2400, and enter your assumed bandwidth in Mbits/second. Click <Add Rule>.
11. Complete Installation, System Configuration and Configure and Start Sites on the remote (other) HyperIP.

HyperIP-HyperIP Verification

12. When both HyperIPs are correctly configured and there is network connectivity between them, selecting “Display HyperIP State” from the Services menu in the top left frame, and clicking <Service Apply>, will show a session connection is ‘ACTIVE’. Any other state indicates the HyperIPs are not communicating properly. Refer to the “Customer troubleshooting” section of the HyperIP User Guide or contact NetEx support to resolve this issue.
13. Run test traffic between the HyperIP appliances:

- a. Go to the Diagnostic Page; Segment Size Test (middle of page). Set the parameters to:
 - Start: 1000, End: 1000, Increment: 1000, Megabytes per pass: 1

- Click <StartSegmentTest> button and wait for the test results. This should complete within seconds unless there is something wrong.
 - Verify there are no interface errors by going to the Maintenance Page, in the Miscellaneous drop-down menu, select [Display Interface Stats]
 - b. This will display the interface statistics for all the interfaces on the appliance for several intervals of time (for trend analysis).
 - c. Select [Display Raw Interface Stats] and verify the duplex/speed setting in this display is as expected. (You may wish to check your switch or router for errors, as well.)
 - d. If there are transmit or receive errors on the data interface, it is an indication that the data interface settings (duplex, speed, flow control) may not be compatible with the port switch settings for the port on which HyperIP is connected.
14. If there are interface errors, you may have to re-configure the data interface settings on the System Page (remembering to click <Interface Apply> after changing settings). You will then need to:
 - a. Select [Restart Force] in the Services Command menu; click <Services Apply>.
 - b. Repeat steps 12 and 13 above until the segment size test runs without errors.
 15. Perform steps 12-14 above on the remote HyperIP.
 16. When there are no interface errors, verify the available bandwidth on the link: Go to the Diagnostic page and select the remote HyperIP IP address from the drop down menu next to the <Measure HyperIP Path> button (select verbose or summary preference). Click <Measure HyperIP Path> and wait for results. The information will be the results of sending packets between the HyperIPs and measuring the time between receptions.
 17. From this information the total bandwidth, available bandwidth and the latency at that time is presented. If this is not what is expected, you may wish to employ some other tools or contact the link provider.
 18. Make sure the bandwidth you set in the Bandwidth Schedule is set to 10% less than this available bandwidth.
 19. Next, determine the optimal segment size between the HyperIPs: Go to the Diagnostic page; Set the parameters as follows, click <StartSegmentTest> and wait for the test results. This will take approximately 2 minutes.
 - Start: 1000
 - End: 32000
 - Increment: 4000
 - Megabytes per pass: 1
 20. If this does not complete in 5 minutes, you can kill the test (click <Kill SegTest>) and retrieve the segment size test results (click <Retrieve Seg Results>). Use the last successful segment size as the maximum size.
 21. Now run this test with enough data for each pass to take a minute.

To calculate the number of Mbytes needed to run each pass at least 1 minute, enter 7.5 times your available bandwidth for the Megabytes per pass.

E.g., if your available bandwidth is 10Mb/s, enter 7.5*10Mb or 75 Mbytes

 - Start: 1000
 - End: your max successful segment size
 - Increment: 4000 (or less if a smaller segment is used for End)
 - Megabytes per pass: 7.5*Available bandwidth

22. When the passes complete, select the recommended segment size and enter this in your site definition if it is different than 32000.
23. Perform steps 16-22 above on the remote HyperIP.

Entering Proxy IP Addresses and Intercepts

24. On the HyperIP Config web page, in the HyperIP Configuration frame, select [Proxies & Intercepts] from the drop down menu and click <Topology Command>. This will bring up a form to fill in your proxy and intercept definitions.
25. Enter the definitions from your "HyperIP Proxy IP Address Configuration Worksheet".
26. When the Proxies are all entered in the form, in the area below the table select [Configure Proxies] from the drop down menu. Then click <Proxy Command>.

This may take a minute to complete. If errors are displayed above the table, you will need to fix them and repeat step 25. Intercepts that are successfully configured are displayed above the Intercept form.

Note: If more than four proxies need to be entered, the above commands can be repeated until all proxies are configured.

27. Enter the definitions from your "HyperIP Intercept Configuration Worksheet".
28. When the intercepts are all entered in the form, in the area below the table select [Configure Intercepts] from the drop down menu. Then click <Intercept Command>.

This may take a minute to complete. If errors are displayed above the table, you will need to fix them and repeat step 27. Intercepts that are successfully configured are displayed above the Intercept form.

Note: If more than four intercepts need to be entered, the above commands can be repeated until all intercepts are configured.

29. We recommend that configurations be saved on remote or removable media and stored in a secure place, in case of an appliance failure. See User Guide procedures for saving configurations.

Direct IP Traffic to the HyperIPs

30. If deploying using Proxy IP address mode only, you will not have to do step 31, the applications must use the proxy IP address to reach the remote application. Refer to the User Guide for more information on Gateway mode vs. Proxy IP address mode.
31. If you plan to deploy this in gateway mode, you will need to direct your IP traffic to the HyperIP. So, on your local and remote application servers, direct your IP traffic destined for the remote location to use this HyperIP unit as the IP gateway (i.e. a static route in the host or in the router if the hosts are on another subnet).

Configuration Worksheets

This worksheet is used to gather the necessary information for a site HyperIP configuration.

*Only Required for Automatic Hot-Standby

<i>HyperIP System Configuration Worksheet</i>	Site _____ Config	
	Primary	*Secondary
HyperIP Serial Number The HyperIP serial number is required to obtain and validate the Product License Key issued by Network Executive Software, Inc. It must be retrieved from the dialog screen or from the Web interface.		
Data Interface – F=Fiber/C=Copper (NetEx supplied hardware appliance only)		
HyperIP Host name – REQUIRED This is a unique name which may be associated with the HyperIP Data I/F IP address in a name server, and identifies the HyperIP.		
Name Server – REQUIRED if using Mail notices This is the Domain Name Server (DNS) at your site which can resolve IP hostnames		
Domain name – REQUIRED This is your site domain name.		
Domain search path This path includes your domain name and could include others.		
Timezone/NTP Server (passive, active) –Network Time Protocol Select your timezone from the list; Select a specific (private) or the best public NTP server from a list		
Mail hub This is the IP address or hostname of the mail server (i.e. SMTP) server at your site. The HyperIP can be setup to issue Product License Key expiration, AHS changes or HyperIP to HyperIP communication change email warnings to an administrator.		
Email address of administrator This is the email address to send Product License Key expiration, AHS changes, and HyperIP to HyperIP communication change email warnings to.		

<i>HyperIP System Configuration Worksheet</i>	Site _____ Config	
	Primary	*Secondary
Default gateway – REQUIRED if other communication via other networks The default IP address (or Hostname) to send traffic which fails any other routing policies.		
HyperIP Data Network Interface: IP address/mask – REQUIRED The data interface must have a physical IP address assigned by your network administrator. The IP address and network mask together identify the HyperIP data interface.		
HyperIP Data I/F options: auto, speed, duplex, MTU, flow control Some switches/routers or interfaces do not auto-negotiate. If the switch or router port does not auto-negotiate, the HyperIP parameters (speed and duplex) must match the switch or router port settings. (Fiber ports ignore speed and duplex)		
Dedicated HyperIP Mgmt Interface IP address/mask If your site requires a dedicated management network interface, set the IP address for this interface. No traffic will be routed between the management network and the data network within HyperIP.		
Dedicated HyperIP Mgmt I/F options: auto, speed, duplex, MTU, flow control If your site requires a dedicated management network interface, the connection of the management interface may require the options to be set to half-duplex, full-duplex, 10Mbps, or 100Mbps speed if the switch doesn't support auto-negotiation.		
Static Routes for Data I/F Depending on your site, you may need to setup static (permanent) routes for specific destination addresses (i.e. specify the WAN router's IP address for the other HyperIP destination address)		
Static Routes for Dedicated Mgmt I/F Depending on your site, you may need to set up static (permanent) routes for specific destination addresses (i.e. specify a particular router to get to a management workstation from this appliance)		
Product License Key - REQUIRED This key is obtained from Network Executive Software, Inc. and is required by the appliance for operation. <i>This key has an expiration date and you must obtain and install a new key before the previous key expires for continued operation</i>		
Key Expiration Warning in Days Number of days prior to key expiration for email warnings to be issued		
Key Expiration Warning Interval Number of minutes between email warnings		

<i>HyperIP System Configuration Worksheet</i>	Site _____ Config	
	Primary	*Secondary
Physical location and contact information for SNMP HyperIP appliance physical location, contact information to be inserted in the SNMP MIBs/traps		
SNMP community The community HyperIP belongs to send SNMP Traps.		
Physical location and contact information for SNMP HyperIP appliance physical location, contact information to be inserted in the SNMP MIBs/traps		
SNMP read only community SNMP community which the SNMP monitor uses to retrieve MIB information from HyperIP.		
SNMP trap/server IP address or IP hostname This is the address of the server which the HyperIP will send SNMP traps to.		
Management and Data Access Settings Allow access to manage HyperIP on the management and data interface: http, https, telnet, ssh, snmp, ping If protocol is not allowed, packets should be: rejected/denied Logging of packets: accepted only, dropped only, everything, nothing		
Gateway Mode (Can only be set via the Web Browser Interface) Gateway Mode: On/Off New and Existing Connections Blocked/Forward (See User Guide for more information on Gateway.)		

HyperIP NxN Configuration Worksheet

The following terms are defined and utilized in the HyperIP NxN configuration on the following page.

Site Number

The site number is a unique identifier of a site within the NxN configuration. Once set, this number is identified with the same site name consistently throughout the entire NxN configuration (i.e. site #1 is Mpls, site #2 is Miami in the Minneapolis HyperIP as well as in the Miami HyperIP.)

Site Name

The site name is a unique string description within the NxN configuration. Once set, this string is identified with the same site number consistently throughout the entire NxN configuration.

Primary IP Address/Mask

The Primary IP Address is an IP address assigned to the data interface of one of the AHS HyperIPs at the site. (There is no order or priority associated with Primary vs. Secondary.) The Primary IP Address must be the same in both AHS HyperIPs at the site.

Virtual IP Address/Virtual ID

The Virtual IP Address and Virtual ID are used when the HyperIPs are configured in an Automatic Hot-Standby configuration (AHS), where only one unit is actively optimizing traffic at a site, and the other is operating in a standby role, ready to take over if the active appliance ceases to advertise its operational state. The Virtual IP address is the IP address assigned and used by the applications for optimization and is shared by both the HyperIPs at the site in AHS. The Virtual ID is a part of the VRRP protocol used by AHS and must be unique in its multicast domain.

Secondary IP Address

The Secondary IP Address is an IP address assigned to the data interface of one of the AHS HyperIPs at the site. (There is no order or priority associated with Primary vs. Secondary.) The Secondary IP Address must be the same in both AHS HyperIPs at the site.

Segment Size (Segsize)

This is the maximum HyperIP data segment size to be used at this site.

Maximum Rate (MaxRate)

The Maximum Rate is the maximum rate that data can be transferred by this site. The sum of all the sites MaxRates cannot exceed the license rate. Specific sessions can be reduced by the use of the bandwidth schedule.

HyperIP NxN Configuration Worksheet

<i>Site Number</i>	<i>Site Name</i>	<i>Primary IP Address</i>	<i>Virtual IP Address/Virtual ID</i>	<i>Secondary IP Address</i>	<i>Segment Size (Segsize in bytes)</i>	<i>Maximum Rate (MaxRate in Mbits/sec)</i>

© 2009 Network Executive Software, Inc. All rights reserved. NetEx and HyperIP are registered trademarks of Network Executive Software, Inc. All other brand and product names are trademarks or registered trademarks of their respective owners. All intellectual property belongs to its respective owners.

HyperIP Proxy IP Address Configuration Worksheet

Traffic is handled by the HyperIP when the packet matches the Proxy IP address or 'intercept' definitions. The following terms are defined and utilized in the HyperIP Proxy IP Address and Intercept Configuration on the following page.

Identifier (ID)

Each definition must have an ID reference (up to 8 characters).

Site Name

Each definition belongs to the pre-defined Site Name from the NxN configuration worksheet

Proxy IP Address (Proxy IPaddr:Port)

The Proxy IPaddr is an IP address on HyperIP's data subnet that will be used by the application to send traffic to (vs. the real destination address.) If a specific port(s) are required, they are only specified here.

Proxy's Destination IP Address (Proxy Dest IPaddr)

This is the actual destination IP address on the remote network which maps to this proxy IP address.

Intercepts

An 'intercept' is the set of IP connection criteria which HyperIP would like to process or intercept.

Source IP address:port is the source IP address (and port) pattern used to match with incoming connections for intercepting traffic.

Destination IP address:port is the destination IP address (and port) pattern used to match with incoming connections for intercepting traffic.

Protocol

The protocol used to match with the incoming connections for intercepts and proxy IP addresses. Valid protocols are ICMP, UDP and TCP.

Connection Limit Action

HyperIP has a limit to the number of local connections (TCP/UDP) it can support (can be configured less). When this limit is reached, HyperIP can be configured to forward or drop the traffic. Selecting **Fwd at Limit** of Yes will cause HyperIP to forward traffic that matches this definition when the connection limit is reached. (Note: This is for intercepts only - new connects via proxy are always dropped at the connection limit).

HyperIP Proxy IP Address Configuration Worksheet

<i>Identifier (ID)</i>	<i>Site Name</i>	<i>Proxy IP Address (Proxy IPaddr:port)</i>	<i>Proxy's Destination IP Address (Proxy Dest IPaddr)</i>	<i>Protocol ICMP/UDP/ TCP</i>	<i>Connection Limit Action Fwd at Limit?</i>

HyperIP Intercept Configuration Worksheet

<i>Identifier (ID)</i>	<i>Site Name</i>	<i>Source IP Address (Source IPaddr:port)</i>	<i>Destination IP Address (Dest IPaddr:port)</i>	<i>Protocol ICMP/UDP/ TCP</i>	<i>Connection Limit Action Fwd at Limit?</i>

© 2009 Network Executive Software, Inc. All rights reserved. NetEx and HyperIP are registered trademarks of Network Executive Software, Inc. All other brand and product names are trademarks or registered trademarks of their respective owners. All intellectual property belongs to its respective owners.

© 2009 Network Executive Software, Inc. All rights reserved. NetEx and HyperIP are registered trademarks of Network Executive Software, Inc. All other brand and product names are trademarks or registered trademarks of their respective owners. All intellectual property belongs to its respective owners.