



READ THIS FIRST!

Congratulations on your purchase of the NetEx HyperIP® Transport Optimizer

The enclosed CD includes HyperIP software and product documentation. Although, the software has been pre-installed at the factory the HyperDocs CD has a recovery image for disaster recovery purposes only.

Product Keys are required to operate your new HyperIP appliance. They have NOT been pre-installed and must be retrieved from hyperip.com. Product Keys are designed to enable the successful operation of a specific HyperIP unit (by serial number) up to a specific bandwidth speed for a specific period of time.

A "Ship Key" is available for each new HyperIP unit that will provide operation for 90 days. For continuous operation of the HyperIP unit 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 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 unit. Once successfully registered, keys (when available) can be accessed at www.hyperip.com and then installed on the respective HyperIP unit (based on 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. You will need the HyperIP serial number to receive your Customer Code.

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

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 and on our website at <http://www.netex.com/services/selfhelp/hyperip-docs.html>.

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

Initial Configuration for Each HyperIP

1. Collect your site information on the Configuration Worksheet (at the end of this guide).
2. If you already have the product license key, or it has already been installed, go to Step 3. Otherwise, obtain a product license key as directed above.
3. Record the HyperIP serial number from the label on the top, front of each unit. The serial number of each unit is used as the default password for system administration, and will be needed later in the installation process. On some units the label ends with the letters "IMWE". These letters are not part of the serial number, and should be ignored.
4. Refer to the latest HyperFlash at the NESi HyperIP website to get the latest news regarding HyperIP releases: <http://www.netex.com/services/selfhelp/HyperFlash.html>
5. **Installation wizard via the Serial Port:** Use a null modem cable and connect a VT-100 compatible terminal (or PC* with emulation) to the serial port on the back panel (marked with "|O|O|"). (Configure the VT-100 terminal for 19200 baud, 8 bits, 1 stop bit, No parity.) Once connected, hit the enter key to obtain a login prompt.

*If the PC is running Windows, HyperTerminal can be used as the VT100 emulator; it comes standard on all modern Windows machines. Some of the display screens from the dialog may not appear as intended due to some idiosyncrasies. There are other terminal emulators available (some free) which do not have these idiosyncrasies, such as NetTerm available at <http://securenetterm.com/html/netterm.html>.

Installation wizard via the Ethernet Port: The factory default for port access is *secure* by default. By default the data port is not accessible and the management port is accessible only by using https/ssh. If only using the data port, the initial installation must be made using the installation wizard via the serial port as detailed above in step 4. The default IP address for the management (Port 1) port is 10.10.2.2/24.

6. Login as user 'hipadmin'. The default password is the serial number for the appliance recorded in step 3. 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 1, at the prompts. If the management IP address is changed, the connection will be lost when the network is restarted. (We strongly recommend changing the default password)
7. If using the dedicated management interface, connect the RJ45 connector (labeled 1) on the back panel to your management network. Now 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.)
8. Connect the appliance to your data 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. 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.)

9. If the security access is set to allow http/https, you can 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>.
10. When this and *other* HyperIP units are correctly configured, clicking on [Display HyperIP State] <Service Apply> will show a session connection is 'ACTIVE'.
11. If you plan to deploy this in gateway mode, you will need to direct your IP traffic to the HyperIP appliances. So, on your local and remote hosts, 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). (If deploying using Proxy IP address mode only, you will not have to do this step, but 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.
12. 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.

Post-Configuration Verification via Browser Interface

- A. Run traffic between the HyperIP appliances:
 - a. Go to the Diag Page; Segment Size Test (middle of page), Set the parameters to:
 - Start: 4000, End: 8000, Increment: 4000, Megabytes per pass: 10
 - b. Click <StartSegmentTest> button and wait for the test results. This will take approximately 30 seconds depending on the link.
- B. Verify there are no interface errors:
 - a. Go to the Maint Page, Miscellaneous drop-down menu, select Display Interface Stats
 - b. This will display the interface statistics for all the interfaces installed 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 the 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.
- C. If there are interface errors, you may have to re-configure the data interface settings then:
 - a. on the System Page, click the <Interface Apply> button,
 - b. Select [Restart Force] in the Services Command menu; click <Services Apply>.
 - c. Repeat steps A and B above until the segment size test runs without errors.
- D. Perform steps A-C on the remote HyperIP unit.
- E. When there are no interface errors, determine the optimal segment size between the HyperIP appliances: Diag page; Set the parameters as follows, click <StartSegmentTest> and wait for the test results. This will take approximately 2 minutes.
 - Start: 4000, End: 32000, Increment: 4000, Megabytes per pass: 10
- F. Verify the available bandwidth on the link: Go to the Diag page and select the remote HyperIP IP address from the drop down menu next to the <Measure HyperIP Path> button (select verbose or summary to preference). Click <Measure HyperIP Path> and wait for results. The information will be results of sending packets between the HyperIPs and measuring the time between receptions. 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.

THIS PAGE LEFT INTENTIONALLY BLANK

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 is located on the top, front, right corner of the appliance, from the dialog screen or from the Web interface. | | |
| Data Interface – F=Fiber/C=Copper | | |
| 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 appliance. | | |
| 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 the 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 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).

Proxy IP Address (Proxy IPAddr)

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.)

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 is the source IP address pattern used to match with incoming connections for intercepting traffic.

Destination IP address is the destination IP address 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).

