

HyperIP®

by

netex

READ THIS FIRST!

Thank you for your interest in NetEx HyperIP® for VMware

If you have received a distribution from NetEx, it includes HyperIP software and product documentation. If you have downloaded the evaluation zip from NetEx, documentation is also included. Always obtain the latest product documentation from our website at <http://www.netex.com/support/product-support/hyperip>.

Product License Keys are required to operate your new HyperIP and must be obtained from NetEx. Keys are designed to enable the successful operation of a specific HyperIP installation (by an internal serial number) for a specific period of time.

Go to this URL <http://www.netex.com/products/hyperip/key-request> once the HyperIP software has been installed and an internal serial number has been retrieved (refer to the following installation steps). For continuous operation of HyperIP past the License period, a new key must be installed prior to the expiration of the current Key.

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 5.5.3 on VMware®

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. 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 an Evaluation Key must be installed on each HyperIP to function.

Installation for Each HyperIP

1. If you have downloaded the OVF from NetEx, you will need the vSphere Client (formerly VMware Infrastructure Client) installed.
2. Collect your site information on the Configuration Worksheet (at the end of this guide).
3. Refer to the latest documentation, FAQ and Updates at the NESi HyperIP website to get the latest news regarding HyperIP releases: <http://www.netex.com/support/product-support/hyperip>.
4. Installation:
5. Installation:

□ ESX(i) 3.5

Request an ISO image download by sending a request to support@netex.com. Define a virtual machine as a Linux virtual machine (Linux, Other 32-bit), with 2 GHz CPU, 9 G storage, 1 GByte of RAM one virtual switch (two if you require a separate management interface). You will also need to attach the downloaded ISO to the virtual machine to install the image (be sure the CD is connected on boot). (You may need to modify the BIOS setting in this VM to allow booting from the CDRom.) Boot up the virtual machine. Follow the prompts to restore the image. Select the "Restore (VGA Console)" option. Once the software is installed, you may unattach the ISO.

□ Esx(i) 4.0 and above

Download the zip file which contains the OVF. Unzip. Open the vSphere Client and login to your VMware Virtual Center server. From the File menu, select Deploy OVF Template. Choose Deploy from file and click Browse to find the HyperIP.OVF file in the unzipped folder. Follow the prompts to assign the new HyperIP Virtual Machine a unique name, Inventory Location, ESX Host/Cluster, Datastore, and Network Mappings. HyperIP uses the first listed interface as the data network. The second interface is used for management.

HyperIP requires the management and data interfaces to reside on different subnets. For optimum performance the data interface's physical Ethernet interface should be dedicated to this virtual machine.

Upon successful completion, Power On the HyperIP Virtual Machine.

System Configuration for Each HyperIP

6. Use the console to perform initial configuration.
7. Login as user 'hipadmin'. The default password is **hipadmin**.

Connect the management interface to your management network. Use the Command Line Interface (CLI) command 'cfgInterface'.

An example:

```
cfgInterface mgmt 192.168.1.101 255.255.255.0 auto 1500
```

This will configure the management interface with an IP address of 192.168.1.101, with subnet mask 255.255.255.0, auto-negotiation of speed/duplex and an MTU of 1500. For more information about this and all CLI commands, see the User Guide.

You may also need to configure a default route.

An example:

```
cfgDefaultGateway 192.168.1.1
```

8. Now would also be a good time to change your security access settings to allow pinging your management interface.

An example:

```
cfgAccessOn mgmt ping
```

At this point a restart will most likely be required. Use the CLI command 'showRestarts'. Then perform the recommended restart.

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 you will be using only one interface, execute the above commands for the "data" interface.

9. Optional: Install the HyperIP Plugin for Virtual Center. Using the CLI commands 'vCenterConfig' and 'vCenterRegister' you can install the HyperIP Plugin to your Virtual Center, allowing you to launch the HyperIP User Interface directly from your vSphere Client (provided that the HyperIP Virtual Machine's management interface has network access to Virtual Center and the host running the vSphere Client). Add a custom attribute to your HyperIP Virtual Machine as instructed by the 'vCenterRegister' command. Any running vSphere Clients must be restarted after Plugin installation.

An example:

```
vCenterConfig 109.168.1.98 myUID myPassword  
vCenterRegister
```

10. If you installed the HyperIP Plugin, on the new 'HyperIP' tab there will be a link to launch the HyperIP User Interface (the HyperIP Virtual Machine must be selected for this button to appear). Alternatively, start a web browser on any host with network access to the HyperIP unit. Browse (HTTPS is the default service) to the HyperIP (by IP address as the URL).

Following the previous example, the address would be <https://192.168.1.101/>

The default password is **hipadmin**. The default password should be changed at this time. Enter the new password in the right panel and click <Change Admin password> .

11. Once access to HyperIP user interface is available, copy the HyperIP Serial Number from the Maintenance Commands page, select "Display Product Information" from the <Misc Commands> dropdown menu.

Go to this URL: <http://www.netex.com/products/hyperip/key-request> to request your Product License Key. If you have a reference number from the the download instructions email, you can enter it along with your email address then click <RetrieveMyInfo> and the form will be filled out for you. Otherwise, fill in all the required fields and paste the serial numbers (you will require two (2) serial numbers one for each end of your link) and submit the form. Once the request is processed and approved, you will receive an email containing a key for each serial number submitted.

12. Configure your System Configuration parameters collected in Step 2. After configuration, Reboot the HyperIP (under "Services" menu option in the upper-left navigation pane).
13. Be sure the data interface is connected to your data network. Now you should be able to successfully ping HyperIP's data IP address from other network hosts on the data network. (Note:

ping is disabled by default – to enable, go to the bottom of the System Config page and insure the ping checkbox is selected and click Secure Ports).

Configure and Start Sites for Each HyperIP

14. Before continuing, the Product License Key must be installed. Refer to Step 11 to obtain your keys.
15. 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.
16. Enter the definitions from your “HyperIP NxN Configuration Worksheet”. Note: the local site must be entered first when configuring each HyperIP.
17. 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 17. 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.
18. In the HyperIP Configuration frame, under the [Start/Halt Remote Sites], select the remote site and select [Start Site] in the drop down menu. Click <State Command>.
19. 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.
20. 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>.
21. Complete Installation, System Configuration and Configure and Start Sites on the remote (other) HyperIP.

HyperIP-HyperIP Verification

22. 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 to resolve this issue.
23. 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.
24. 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 review this with your network administrator.
25. Make sure the bandwidth you set in the Bandwidth Schedule is set to at or less than this available bandwidth.
26. 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
27. 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.
 28. 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.
i.e 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
 29. When the passes complete, select the recommended segment size and enter this in your site definition if it is different than 32000.
 30. Perform steps 23-29 above on the remote HyperIP.

Configure Intercepts and Proxies

31. 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.
32. Enter the definitions from your “HyperIP Proxy IP Address Configuration Worksheet”.
33. 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 32. 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.
34. Enter the definitions from your “HyperIP Intercept Configuration Worksheet”.
35. 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 34. 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.
36. 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.

You can now begin to evaluate your application performance.

37. If deploying using Proxy IP address mode only, you will not have to do step 38, 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.
38. If you plan to deploy this in gateway mode, you will not have to do step 37, 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.

Site _____ Config		
<i>HyperIP System Configuration Worksheet</i>	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.		
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.		
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.		
Product License Key - REQUIRED This key is obtained from Network Executive Software, Inc. and is require 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>		

*Only Required for Automatic Hot-Standby

HyperIP System Configuration Worksheet OPTIONAL INFORMATION	Site _____ Config	
	Primary	*Secondary
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.		
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.		
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)		

HyperIP System Configuration Worksheet OPTIONAL INFORMATION (cont.)	Site _____ Config	
	Primary	*Secondary
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		
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 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. At least one Proxy or one Intercept must be defined for each site.

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.

Proxies (For Proxy 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 (For Intercept Worksheet)

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).

© 2011 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.