

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, except for Evaluation and DR keys) 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 6.0.0 on VMware ESX®

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. Video tutorials, 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 Key must be installed on each HyperIP to function. The HyperIP virtual appliance (VA) needs to be created to retrieve the serial number for the key request. The steps to request a key are defined during the process below.

Prerequisites for Installation

- a) vSphere Client (formerly VMware Infrastructure Client)
- b) Collect your site information on the Configuration Worksheet (at the end of this guide)

Installation for Each HyperIP

1. 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 one 2 GHz CPU, 9 GBytes storage, 1 GBytes 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 VMWare" option. Once the software is installed, you may detach the ISO image from the CD/DVD.

□ ESX(i) 4.0 and above

Request an OVA image download by sending a request to support@netex.com. Download the zip file which contains the OVA (an archived OVF directory structure and files). 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.OVA file. 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.

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

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

The HyperIP data port is required for operation and can be used for management as well. A separate management port is available if desired. **HyperIP requires the management and data interfaces to reside on different subnets.**

Perform initial configuration of the data interface and connect the data interface to your data network. Use the following Command Line Interface (CLI) commands listed in the example. (For more information about this and all CLI commands, see the User Guide.)

Configure the IP hostname:

```
cfgHostname MYHOST
```

Then configure the data interface with an IP address on your data network, with subnet mask, interface speed/duplex and MTU.

An example:

```
cfgInterface data 192.168.1.101 255.255.255.0 auto 1500
```

If using the management interface, execute the command for the mgmt interface making sure that it is on a different subnet.

Configure a default route.

An example:

```
cfgDefaultGateway 192.168.1.1
```

Change your security access settings to allow browser access and ping to the interface being used for management.

An example:

```
cfgAccessOn data https
cfgAccessOn data ping
```

Use the CLI command 'showRestarts'. Then perform the recommended restart.

Once configuration is complete, you should be able to successfully ping the HyperIP IP address being used for management from other network hosts on the network.

3. Browse (HTTPS is the configured 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>**.

4. Copy the HyperIP Serial Number and obtain a license key: Go to the Maintenance Commands page by selecting **[Maintenance Commands]** in the upper-left (navigation) drop down menu. Select **[Display Product Information]** from the **<Misc Command>** drop down menu and click the **<Misc Command>** button.

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 download instructions email, enter it along with your email address and click **<RetrieveMyInfo>** and the form will be filled out for you. Otherwise, fill in all the required fields and paste the serial numbers into the appropriate box (you will require two (2) serial numbers - one for each end of your link) and submit the form by clicking **<Accept>**. Once the request is processed and approved, you will receive an email containing a key for each serial number submitted.

Navigate to the "Install Commands" page. Paste the key into the window under License Key and click the **<Install Key>** button.

5. Go to the "System Config" page. Enter any additional System Configuration information on this page and apply by clicking the **<SysConfig Apply>** button at the bottom of the section.
6. Check for any restarts required by selecting "Show Pending Restarts" in the services drop down menu and clicking the **<Service Apply>** button. Execute and confirm the appropriate restart.

Configure and Start Sites for Each HyperIP

7. 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.

Enter the definitions from your “HyperIP NxN Configuration Worksheet”. *Note: the local site must always be entered first when configuring each HyperIP. Make sure that the same ID number is used to identify this site across the HyperIPs.*

The segment size defaults to 32768, and for smaller bandwidths (45Mb/s or less) the recommended size is 1300. Configure this on the NxN as you input the *remote* site information. If bandwidth is over 45 Mb/s, leave segsize at default and continue.

When the sites have all been entered into 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 this step. Sites that are successfully configured are displayed above the form.

After the sites are configured, check for, and execute, any pending restarts.

8. In the HyperIP Configuration frame, under the Start/Halt Remote Sites section, select the remote site and select [**Start Site**] in the drop down menu. Click **<State Command>**.
9. Static routes could be required if the default gateway on the “System Config” page services the mgmt port. This will require that the data port have a default gateway different than that of the mgmt port. On the “Advanced Config” web page, insert destination IP address, subnet mask, and gateway IP address into the Static Routes form and push the **<StaticAdd>** button. Static routes can also be used if the data port default gateway cannot route to the remote HyperIP.
10. On the “HyperIP Config” page, 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.
Create a rule and select the remote site, 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 to resolve this issue.
13. Refer to the Segment Size Test section on the “Diagnostic Commands” page.

This testing will help you determine the appropriate segment size for each remote site.

For network bandwidth larger than 45Mb/s do not configure a segment size of 1300. Leave it at the default of 32768 and run the segment size test to determine the correct size to use.

If you configured the segment size to 1300 go to step 14.

Next, determine which segment size is appropriate for your network.

Set the parameters as follows and then click **<Start SegTest>**.

After about a minute, click **<Retrieve Seg Results>** to obtain the segment test results.

- Start: 1300
- End: 32000
- Increment: 4000

Megabytes per pass: 1

If all passes complete, rerun the test to determine which segment size is appropriate.

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 10 times your available bandwidth for the Megabytes per pass, i.e., if your available bandwidth is 20Mb/s, enter 20*10 or 200 Mbytes per pass.

- Start: 1300
- End: 32000
- Increment: 4000
- Megabytes per pass: 10*Available bandwidth

Run the segment size tests the other direction on the remote HyperIP.

When the passes complete, select the recommended segment size and enter it into your site definition (on the "Configure NxN" page) if it is under 32000. To make the change, edit the remote site definition in the "blue box", changing "32768" to the new value and click the <**NewConfig**> button. You will need to start the site and perform the appropriate restart for the new segment size to be implemented. Verify the sites are active after the changes and restarts are complete.

14. Refer to the Segment Size Test section on the "Diagnostic Commands" page.

Next, determine the optimal segment size between the HyperIPs: Set the parameters as follows and then click <**Start SegTest**>. This will take approximately two minutes. Click <**Retrieve Seg Results**> to obtain the segment test results.

- Start: 32000
- End: 32000
- Increment: 4000
- Megabytes per pass: 100

Select [**Display HyperIP State**] from the SERVICES menu in the top left frame, and click <**Service Apply**>. This will show a second transport session which will display what throughput segment test can achieve and whether retransmits are occurring.

Configure Intercepts

15. 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 or intercept definitions..

Enter the intercept definitions from your "HyperIP Intercept Configuration Worksheet".

NOTE: The source address/network is always on the same side of the WAN as the HyperIP being configured. The destination is always on the remote side of the WAN.

When the Intercepts are all entered into the form, in the area below the table select [**Configure Intercepts**] from the drop down menu. Click <**InterceptCommand**>.

This may take a minute to complete. If errors are displayed above the table, you will need to fix them and repeat this step. 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.

You can now begin to evaluate your application performance.

To deploy in gateway mode (as in the process defined above) you will need to direct your IP traffic to the HyperIP. 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).

If deploying using Proxy IP address mode, 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.

We recommend that configurations be saved remotely and stored in a secure place, in case of an appliance failure. See User Guide procedures for saving configurations.

Configuration Worksheets

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

*Only Required for Automatic Hot-Standby

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 CLI 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 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>		

*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 –Network Time Protocol Select your timezone from the list; If enabling, Enter a specific NTP server.		
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 This is the SNMP community which a SNMP monitor uses to retrieve MIB information from this 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/Firewall/Secure ports Allow access to manage HyperIP on the management and data interface: http, https, ssh, snmp, ping If protocol is not allowed, packets should be: rejected/denied Logging of packets: accepted only, dropped only, everything, nothing		
Gateway Mode 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 specific ports 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.