



Best Practices with Tivoli Storage Manager



Link to HyperIP at IBM's PartnerWorld:

<https://www-304.ibm.com/software/brandcatalog/ismlibrary/details?catalog.label=1TW10SM44#>

©2011 NetEx Software
6420 Sycamore Lane N.
Suite 300
Maple Grove, MN 55369
<http://www.netex.com>

HyperIP in a Network with Tivoli Storage Manager (TSM)

Implementation of HyperIP and Tivoli Storage Manager

The addition of HyperIP into the network using gateway mode does not require any changes to the TSM server or Client applications. Changes are necessary to the host routing tables for HyperIP to get inserted in the data path. The routing changes are described later in this document.

Installation of HyperIP

Refer to the latest documentation, FAQ, and Updates at the HyperIP website to get the latest news regarding HyperIP releases: <http://www.netex.com/support/products/hyperip>.

HyperIP is a WAN Optimization Virtual Appliance and can be requested from this URL: <http://www.netex.com/hyperip/evaluation-request>.

Fill out the Evaluation Agreement, accept the terms, and a download link will be sent to you to download the installation package. HyperIP is keyed and instructions on how to obtain keys are included in the installation package.

Video tutorials are available to assist in stepping through the configuration of HyperIP: <http://www.netex.com/support/products/hyperip-screencasts>

Appendix A in this document contains screenshots and information regarding HyperIP configuration.

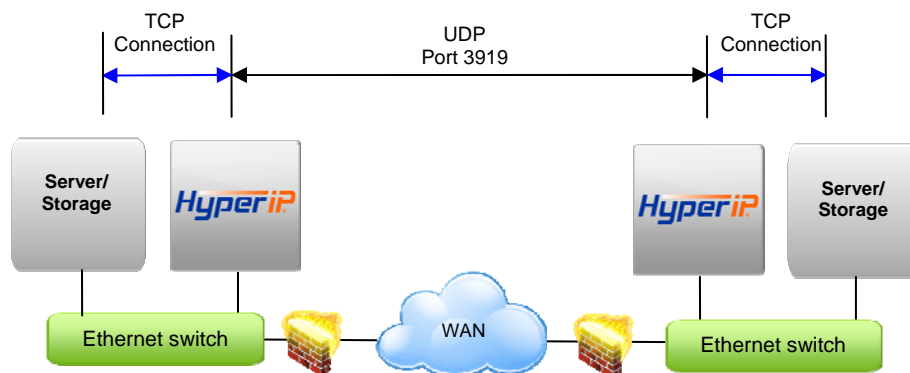
Adding HyperIP into your network

HyperIP improves the performance of backup and replication applications over your IP WAN. **HyperIP does not alter application protocols nor modify any file systems.** It efficiently moves block or file data over the IP WAN under any network conditions.

HyperIP also provides:

- support of WAN speeds scaling from 1-800 Mb/s
- virtual footprint
- adaptive lossless block level compression
- time of day rate controls for changing throughput requirements

HyperIP requires at least two appliances (virtual), one residing on each side of the WAN, as shown in the figure below. Multiple servers and storage at each site can utilize the HyperIP data path. HyperIP can also be deployed in a hub or mesh configuration.



HyperIP terminates TCP connections locally and tunnels the data between HyperIPs using UDP port 3919. **Network devices filtering IP traffic in the data path between the HyperIPs must be configured to allow UDP port 3919.**

HyperIP must be *in* the data path to optimize the movement of data. HyperIP connects to a (virtual) LAN switch with a single Gigabit Ethernet NIC and has two modes of operation to facilitate being inserted into the data path:

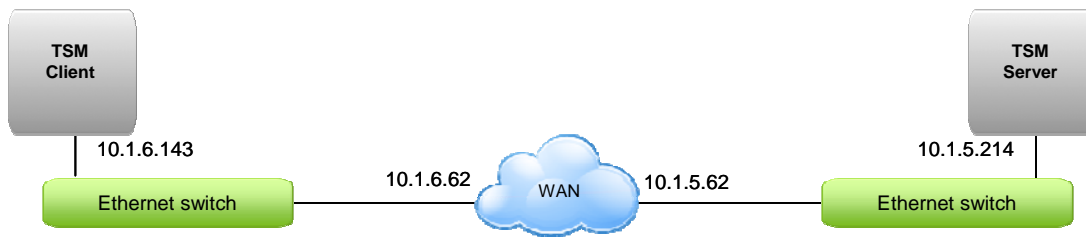
- **Gateway Mode:** User must add route statements in the *data movers (application servers, storage devices, etc.)* defining HyperIP as the IP gateway for the destination IP addresses or networks. Alternatively, these IP route statements or redirect filters, may be configured in a router. Gateway mode **requires users to define HyperIP intercepts** based on IP addresses, TCP ports and/or protocols to determine what traffic to act on.
- **Proxy Mode:** HyperIP requires additional local IP addresses (proxy) which represent remote IP addresses of the application servers or storage devices. This local proxy IP address is then used to communicate with the remote application. HyperIP is configured with a 1:1 mapping in which each destination IP address requires an associated local proxy address. *Applications that do not support Network Address Translation (NAT) must use the HyperIP gateway mode.*

Each HyperIP requires its own key associated with the HyperIP serial number. You must connect to the user interface on each HyperIP to retrieve its serial number and complete the form at: <http://www.netex.com/hyperip/hyperip-key-request> to request the key.

For further explanation on the features/functionality of HyperIP see the HyperIP User guide at: <http://www.netex.com/support/products/hyperip-docs>

Tivoli Storage Manager Configuration Before HyperIP

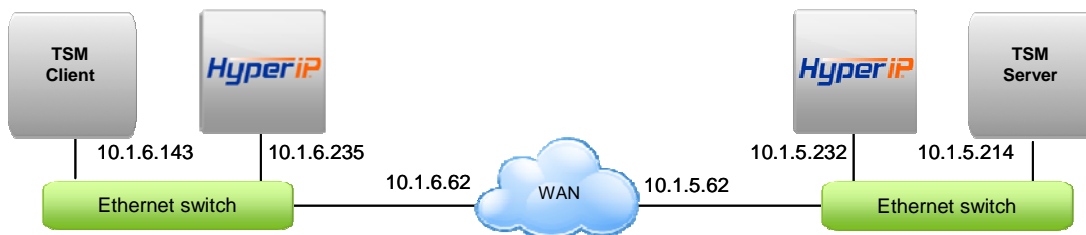
The drawing below shows a TSM configuration before installing HyperIP:



The client host will establish a TCP connection directly with the TSM server.

Tivoli Storage Manager Configuration With HyperIP

The drawing below shows a TSM configuration after installing HyperIP:



When adding HyperIP, as in the drawing above, the TSM Client and Server hosts will use HyperIP as an IP gateway to the remote host. HyperIP tunnels the TSM traffic across the WAN.

The route definitions and specific HyperIP information for the drawing are defined below:

TSM client IP route to TSM server:

Route add 10.1.5.214/32 gateway 10.1.6.235

TSM Server IP route to TSM Client:

Route add 10.1.6.143/32 gateway 10.1.5.232

Client site HyperIP definitions:

NxN Sites:

Itself – 10.1.6.235

Peer HyperIP (Remote Site) – 10.1.5.232

Intercept: Source Address = 10.1.6.143 Destination Address = 10.1.5.214

Server site HyperIP site definition:

Itself – 10.1.5.232

Peer HyperIP (Local Site) – 10.1.6.235

Intercept: Source Address = 10.1.5.214 Destination Address = 10.1.6.143

Appendix A-HyperIP Configuration

The following information is required when configuring HyperIP:

- Interface IP address and network mask.
- Browser Access options for HyperIP (http or https)
- HyperIP hostname
- HyperIP default gateway
- HyperIP Domain name
- DNS IP address
- IP addresses or networks utilizing HyperIP (required to configure intercepts)

Using this information follow the instructions in the HyperIP HyperStart Guide to configure HyperIP for the network: <http://www.netex.com/support/products/hyperip-docs>

Additional information is available at:

<http://www.netex.com/support/hyperip-support-table/hyperip/hyperip>

Example HyperIP browser interface screen shots and configuration tips are included on the following pages.

This System webpage is used to configure or verify the basic system information and access settings:

HyperIP hostname
HyperIP default gateway
Data port IP address and network mask (required)
Mgmt port IP address and network mask (optional)

HyperIP arsenal - Mozilla Firefox

File Edit View History Bookmarks Tools Help

HyperIP arsenal

HyperIP [arsenal]

HyperIP Status: running - noMMS Current Version: 5.5.4 (Build 11) (r3002) Key Expiration: 00-22-2012 Alternate Version: 5.5.4 (Build 9) (r3022)

Welcome to the HyperIP Web Interface

HyperIP[®] is an "edge device", intercepting certain IP traffic on a LAN and accelerating it using NetS transport protocol over long, high-latency links to a peer HyperIP on another network, then on to the original destination.

Viewing Notes: For best viewing, open browser window to full-screen. You may wish to adjust the font size with View > Text-Size. For browsers running on Linux, it may be better to force local fonts (Edit > Preferences > Fonts). A 10-point size works well. Also, if you use a "pop-up blocker", it should be disabled for the HyperIP URLs.

Web browser admin password ***** [Enter Admin Password]
If you are going to modify config data or status, you must enter the 'admin' password. The password is retained for the life of this browser session. To change the web/admin password, first enter the current password above, then...
Enter New Password: [Enter New Password] [Reenter new password] [Change Admin Password]
After it is successfully changed, you are logged in with the new password.
The following characters are not allowed: apostrophe, back-tic, back-slash, double-quote.

Web browser access password for 'local HyperIP' ***** [Change Access Password]
To restrict all access to the HyperIP unit via the web interface, create an 'access' password. In order to do this, the 'admin' password must have been successfully entered. Once done, you must do a 'Restart Force' from the Services menu on any left-side page when it is convenient. Then, an initial reference from a browser will require that you enter the access password before any HyperIP web pages are viewable.
A null value for the access password removes the requirement to enter anything to view or monitor the appliance (this is the default/initial state).
The password is retained for the life of this browser session.

Web browser certificates
If you download Network Executive Software's CA certificate and configure your web browser to trust it as a certificate authority, you will not receive trust warnings when you connect to NES products securely via https.
Documentation exists on the CD-ROM shipped with each HyperIP unit.
- View our [new documentation](#) (updates) or view our [HyperIP Support](#) site (new window - internet access required).
- View the [published SNMP MIBs](#) on the HyperIP. Latest versions of the MIBs may also be found at the 'documentation updates' link above.

System Configuration
Check Pending Features if IP addresses, passwords or hostname are changed

Local IP Hostname: arsenal
Default Gateway: 10.1.6.50
Name Resolver: none
Local Domain: netexec.com
Search List: netexec.com
Mail Hub: none
[Sync Config Apply]

Interface Configuration

IP addr: 10.1.6.228
Mask: 255.255.255.0
Speed/Duplex: Auto
Flow Control: Auto
MTU: 1500
MGMT: ☒ Enable
[Interface Display] [Interface Apply]

Firewall Commands
Drop Method: DENY Log Option: DROPPED
[Firewall List] [Firewall Reset] [Firewall Restart]

Secure Ports
Check to allow access

DATA PORT	Service	MGMT PORT
<input type="checkbox"/>	HTTP	<input type="checkbox"/>
<input checked="" type="checkbox"/>	HTTPS	<input type="checkbox"/>
<input checked="" type="checkbox"/>	PING	<input type="checkbox"/>
<input type="checkbox"/>	SNMP	<input type="checkbox"/>
<input checked="" type="checkbox"/>	SSH	<input type="checkbox"/>

[Secure Ports]

Find: [] [Next] [Previous] [Highlight] [Match case]

If there is only one interface available to the HyperIP, configure only the Data port.
To remove the mgmt port from use, delete the IP address in the MGMT IP addr window.
Be sure to allow user access through the data port if using only one interface.

The HyperIP “Configure NxN” frame is launched from the HyperIP Configuration webpage and is used to add information about the sites:

Local HyperIP data port IP address

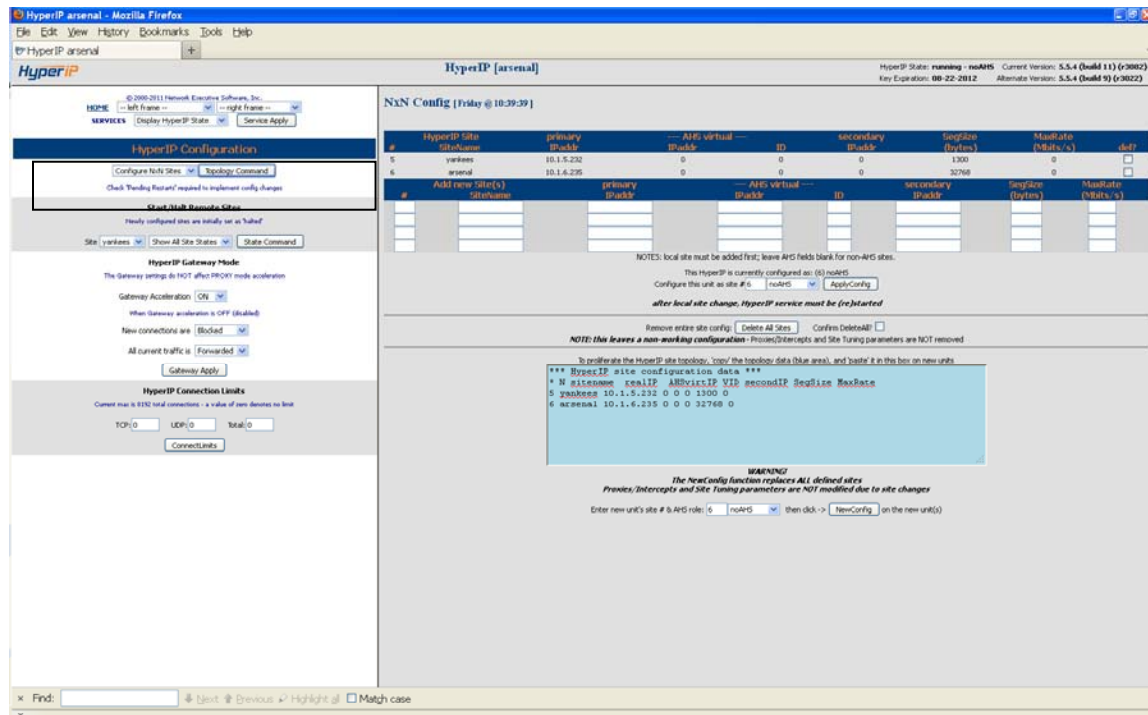
Remote HyperIP data port IP address (External NAT address)

site number/site name (user-defined and unique within the HyperIP environment)

MaxRate (required if there are multiple remote HyperIPs configured)

Segsize (default: 32768 – May be changed after setup tests have been run)

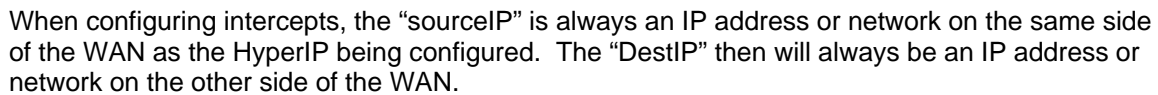
NOTE: Use 1300 on lower-speed links (under 45 Mb/s) or networks where fragmentation will cause a performance hit due to packet loss or overhead. An example would be where a PIX firewall is being used.



When configuring sites, it is important that the site defining the HyperIP being configured is entered first and site numbers remain the same across all HyperIPs. In the example above, when we configure the “Remote” HyperIP, site “remote” will be entered first using site #5 and site “local” will use site # 3.

The site name only needs to be unique to the configured HyperIP and is suggested to remain consistent across all configurations as well.

IP addresses or networks utilizing HyperIP



HyperIP with Tivoli Storage Manager