



Best Practices
with
Veeam Backup and Replication



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

HyperIP in a Veeam Backup and Replication Network

Veeam Backup and Replication over WANs utilizing HyperIP have shown LAN-like performance. Veeam replication achieved bandwidth utilization consistently exceeding 90% from distances of hundreds of miles (with high bit error rates on dirty lines) to as far as transcontinental distances.

What this means to end-users

Veeam on native Ethernet TCP/IP fabrics with HyperIP is now the highest possible WAN throughput option. Veeam replication is no longer limited by TCP throughput issues, shortening replication window times.

Implementation of HyperIP and Veeam Backup & Replication

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 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 OVF installation package. HyperIP is keyed and instructions on how to obtain keys are included in the download package.

Installation of VEEAM Backup & Replication software

Veeam software can be downloaded, as a trial, from this URL: <http://www.veeam.com/vmware-esx-backup.html>. Datasheets and documentation can also be found at this link.

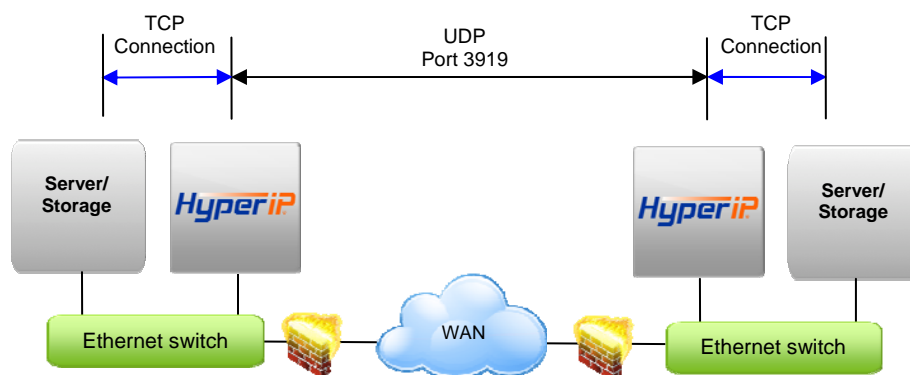
Adding HyperIP into your network

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 or physical appliance footprint
- adaptive lossless block level compression
- time of day rate controls for changing throughput requirements

HyperIP requires at least two appliances (virtual or physical), 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:

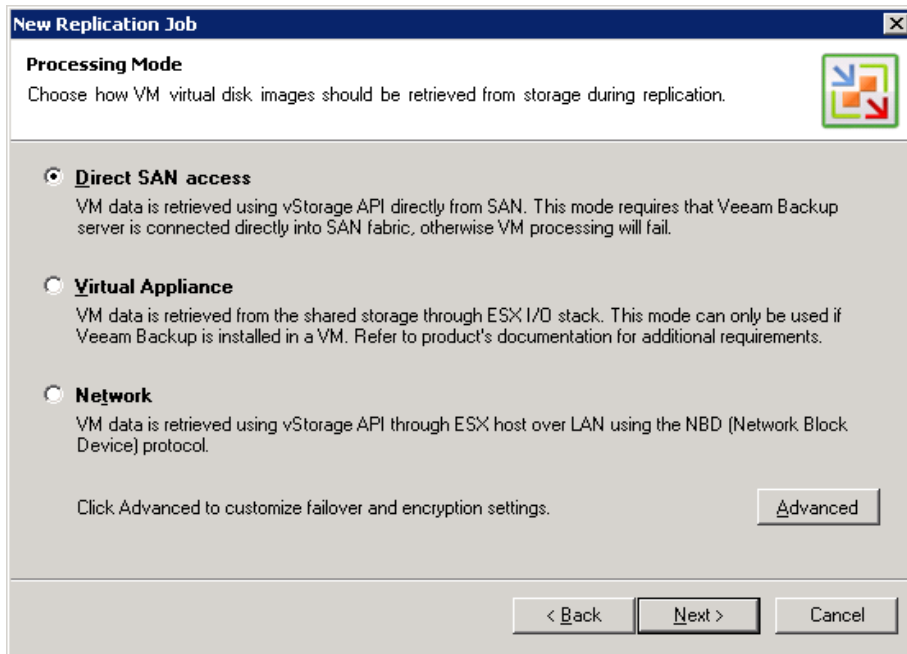
- **Gateway Mode:** User must add route statements in the *data movers (application servers, storage devices, etc.)* defining HyperIP as the IP gateway for the destination IP addresses or networks. Alternatively, these IP route statements or redirect filters, may be configured in a router. Gateway mode **requires users to define HyperIP intercepts** based on IP addresses, TCP ports and/or protocols to determine what traffic to act on.
- **Proxy Mode: (Not supported with Veeam Backup and Replication)** 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>

Veeam 5 Backup and Replication Configuration

The Veeam Backup and Replication jobs retrieve VM data in one of the three processing modes shown in the screenshot below.



The processing modes determine how data will flow between the source ESX(i) host and the Veeam Backup Server. HyperIP resides between the Veeam Backup Server and the remote (across the WAN) ESX(i) or Linux host.

When the Veeam Backup Server is located with the source ESX(i) host, HyperIP will be in the data path between the Veeam Backup Server and the target ESX(i) or Linux host. In this configuration, any of the processing modes can be used.

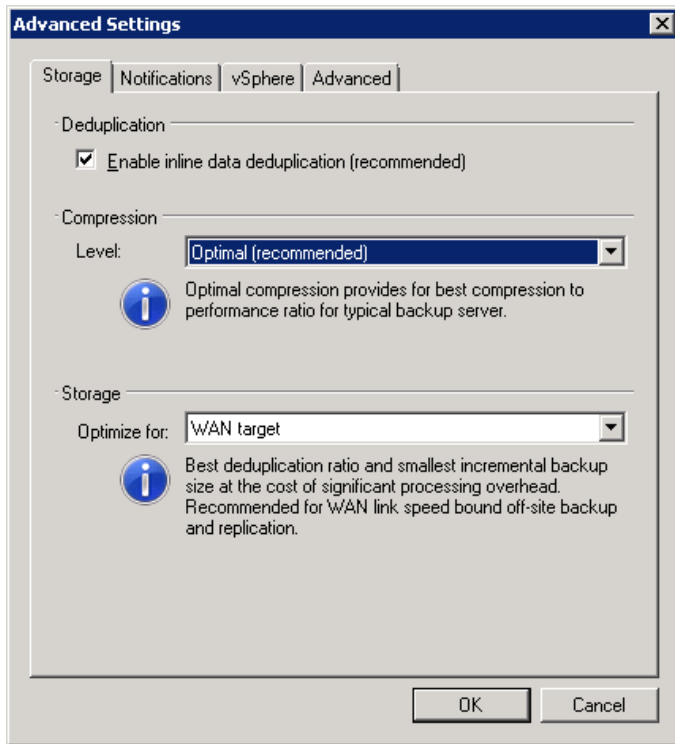
When the Veeam Backup Server is located with the target ESX(i) host, HyperIP will be in the data path between the Veeam Backup Server and the source ESX(i) host. In this configuration, Network, or "Direct SAN access" (if using an iSCSI SAN), processing modes may be used.

To utilize HyperIP in the data path, The Veeam Backup Server and ESX(i) or Linux host routing tables need to be modified to direct traffic to the HyperIP's. Route statements are added to each using the local HyperIP as the IP gateway. You must be logged into the Veeam Backup and ESX(i) servers with authority to make routing changes.

The HyperIPs must be configured to intercept traffic between the Veeam Backup Server and the remote ESX(i) or Linux host (see Appendix A for HyperIP configuration). HyperIP must be on the same subnet and VLAN as the Veeam Backup Server and the ESX(i) or Linux host interface for the gateway statement to be effective. If HyperIP cannot be placed on the same network, contact NetEx support at support@netex.com for other options to direct traffic to HyperIP.

Drawings depicting HyperIP placement in the network and routing changes to implement HyperIP in the data path are described in the following sections.

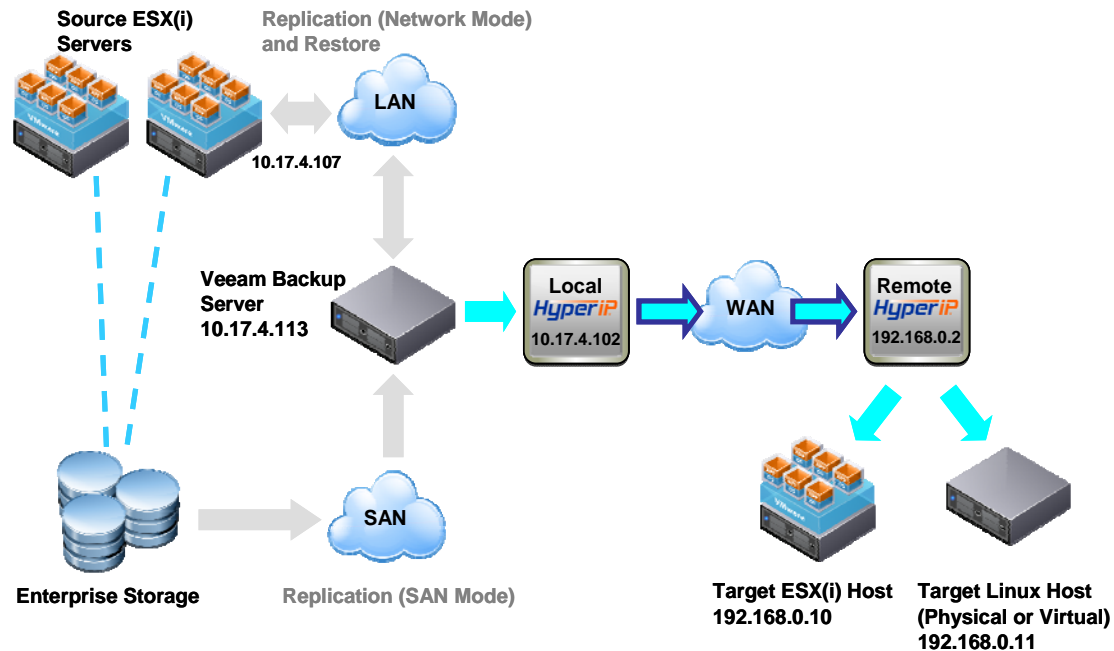
When performing backup or replication across a WAN, optimizing for WAN target in the advanced settings on the replica destination screen is suggested.



Veeam 5 Backup Server located with Source ESX(i) Hosts

The Veeam Backup Server receives data from the source ESX(i) host via the SAN, LAN or the ESX I/O stack, manipulates the traffic as configured (compression, deduplication, etc.) and sends across the WAN to the target remote ESX(i) or Linux host.

When the source host is ESX and the target is ESXi, Veeam suggests using a Linux host as the target or positioning the Veeam Backup Server on the target side of the WAN. The target side configuration is described in the next section.



In the Veeam Backup Server, add a persistent host route to the Target ESX(i) or Linux host with HyperIP as the gateway. An example using the IP addresses in the above drawing:

```
route add 192.168.0.10 mask 255.255.255.255 10.17.4.102 -p
route add 192.168.0.11 mask 255.255.255.255 10.17.4.102 -p
```

ESX(i) configuration

ESX uses the service console (one of the vswif's). ESXi uses the vmkernel NIC. A host route is needed to the remote Veeam Backup Server with HyperIP as the gateway.

ESX

```
route add -host 10.17.4.113/32 gw 192.168.0.2 vswif0
```

Note: The ESX route statements can be made persistent by adding them to the /etc/rc.local file.

ESXi

```
esxcfg-route -a 10.17.4.113 255.255.255.255 192.168.0.2
```

Linux Target

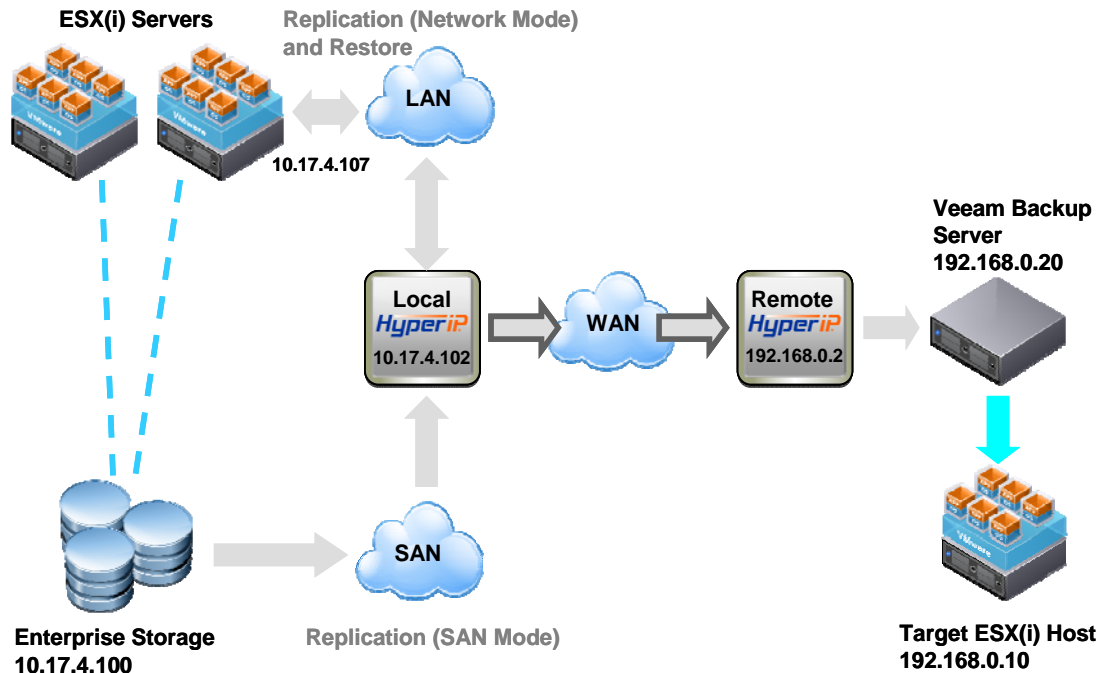
See your particular Linux OS documentation for information on adding routes.

The intercepts for the drawing HyperIPs:

	ID	SiteName	SourceIP	DestIP	Protocol
Local HyperIP:	1	Remote	10.17.4.113	192.168.0.10	All
Local HyperIP:	2	Remote	10.17.4.113	192.168.0.11	All
Remote HyperIP:	1	Local	192.168.0.10	10.17.4.113	All
Remote HyperIP:	2	Local	192.168.0.11	10.17.4.113	All

Veeam 5 Backup Server located with Target ESX(i) Hosts configuration

The Veeam Backup Server receives data from the source ESX(i) host via the SAN (iSCSI) or LAN across the WAN and sends to the target ESX(i) host.



In The Veeam Backup Server, add a persistent host route to the remote ESX(i) host with HyperIP as the gateway. An example using the IP addresses in the above drawing:

```
route add 10.17.4.107 mask 255.255.255.255 192.168.0.2 -p
```

ESX(i) configuration

ESX uses the service console (one of the vswif's). ESXi uses the vmkernel NIC. A host route is needed to the remote Veeam Backup Server with HyperIP as the gateway.

ESX

```
route add -host 192.168.0.20/32 gw 10.17.4.102 vswif0
```

Note: The ESX route statements can be made persistent by adding them to the /etc/rc.local file.

ESXi

```
esxcfg-route -a 192.168.0.20 255.255.255.255 10.17.4.102
```

Storage (if using an iSCSI SAN)

Some form of route add dependent of storage array operating system.

```
route add -host 192.168.0.20/32 gw 10.17.4.102
```

Intercepts for the drawing HyperIPs:

	ID	SiteName	SourceIP	DestIP	Protocol
Local HyperIP:	1	Remote	10.17.4.107	192.168.0.20	All
	2	Remote	10.17.4.100	192.168.0.20	All
Remote HyperIP:	1	Local	192.168.0.20	10.17.4.107	All
	2	Local	192.168.0.20	10.17.4.100	All

Veeam 4 Replication Configuration

Placement of HyperIP in the Veeam data path depends on the replication or backup job settings. Drawings and routing changes to implement HyperIP for “VMware vStorage API” and “Network Replication” are described on the following pages.

New Replication Job

Replication Mode
Choose how VM data should be retrieved during replication. VCB option is only available if Veeam Backup console is installed on the VCB proxy server.

VMware vStorage API
Mode: SAN with failover (recommended) Network traffic encryption
VM data is retrieved using vStorage API directly from SAN, or through ESX host over LAN (if direct storage connection becomes unavailable).

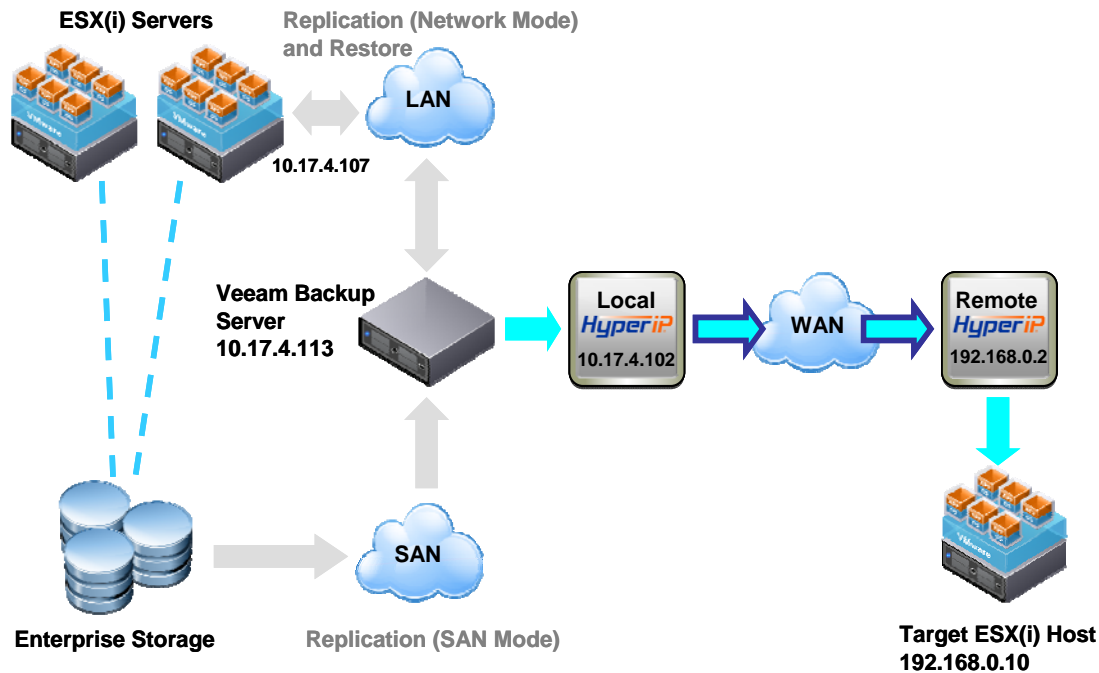
VMware Consolidated Backup
Mode: SAN (recommended) Network traffic encryption
VM data is retrieved by VCB framework directly from the storage, and then processed by Veeam Backup. This mode requires that VCB proxy server is connected directly into SAN fabric.

Network replication
VM data is retrieved over LAN using proprietary Veeam methods. If enabled, service console agent is leveraged to reduce the amount of data transferred and to allow for direct-to-target operation.

< Back Next > Cancel

VMware vStorage API configuration

When "VMware vStorage API" is selected, the Veeam Backup Server receives data via the SAN or LAN, manipulates the traffic as configured (compression, deduplication, etc.) and sends to the remote ESX(i) host.



In The Veeam Backup Server, add a persistent host route to the remote ESX(i) host with HyperIP as the gateway. An example using the IP addresses in the above drawing:

```
route add 192.168.0.10 mask 255.255.255.255 10.17.4.102 -p
```

ESX(i) target configuration

ESX uses the service console (one of the vswif's). ESXi uses the vmkernel NIC. A host route is needed to the remote Veeam Backup Server with HyperIP as the gateway. Examples for ESX and ESXi:

ESX

```
route add -host 10.17.4.113/32 gw 192.168.0.2 vswif0
```

Note: The route statements will be lost after a reboot and can be made persistent by adding them to the /etc/rc.local file.

ESXi

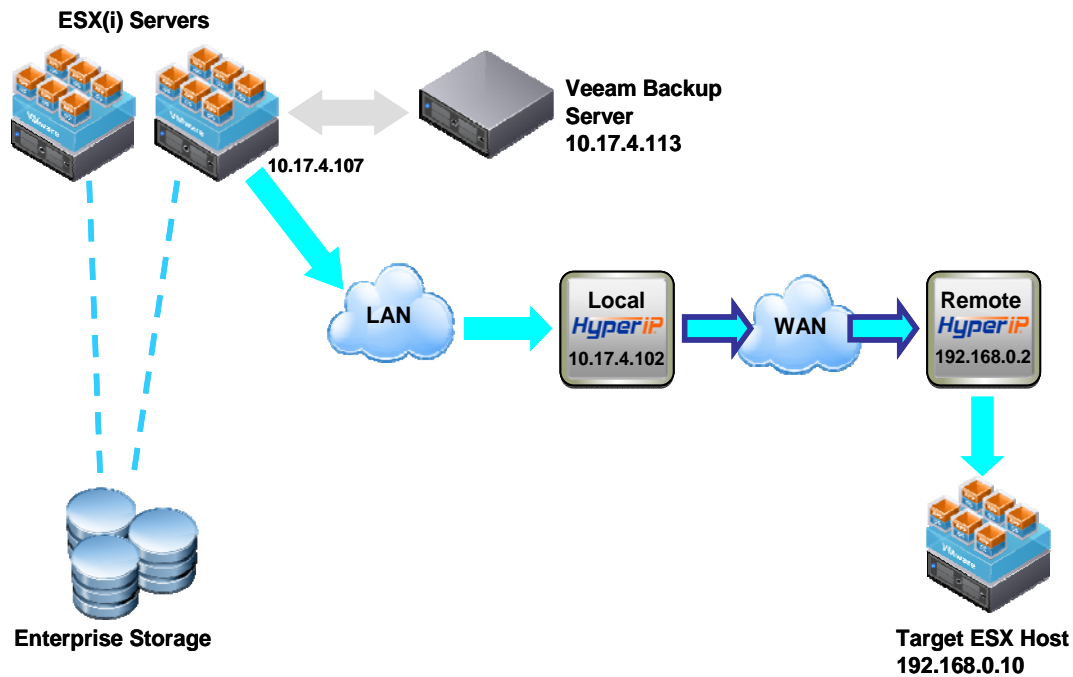
```
esxcfg-route -a 10.17.4.113 255.255.255.255 192.168.0.2
```

Proxies are not supported with Veeam backup and Replication. The intercepts for the drawing HyperIPs:

	ID	SiteName	SourceIP	DestIP	Protocol
Local HyperIP:	1	Remote	10.17.4.113	192.168.0.10	All
Remote HyperIP:	1	Local	192.168.0.10	10.17.4.113	All

Network backup or Replication

If “Network Replication” or “Network Backup” is selected, traffic flows between the ESX hosts without passing through the Veeam Backup Server.



ESX

```
route add -host 10.17.4.107/32 gw 192.168.0.2 vswif0
```

```
route add -host 192.168.0.10/32 gw 10.17.4.102 vswif0
```

Note: The route statements will be lost after a reboot and can be made persistent by adding them to the /etc/rc.local file.

ESXi

```
esxcfg-route -a 10.17.4.107/32 255.255.255.255 192.168.0.2
```

```
esxcfg-route -a 192.168.0.10 255.255.255.255 10.17.4.102
```

Proxies are not supported with Veeam Backup and Replication. The intercepts for the drawing HyperIPs:

	ID	SiteName	SourceIP	DestIP	Protocol
Local HyperIP:	1	Remote	10.17.4.107	192.168.0.10	All
Remote HyperIP:	1	Local	192.168.0.10	10.17.4.107	All

Appendix A-HyperIP Configuration

HyperIP may reside on its own internal switch and traffic sent outside the ESX server, through an external switch and back to the HyperIP or HyperIP could reside on the same virtual switch as the VMkernel and/or Service Console NIC. For unrestricted performance, HyperIP should be configured with a dedicated network interface.

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>

There are also videos on "You Tube" created to assist users with HyperIP installations. If you have difficulty seeing the text, increase to high definition and maximize the screen. When visiting these following links, please click "play all videos" found on the middle right.

Installation: http://www.youtube.com/view_play_list?p=E76DF2AAB28F2559
Configuration: http://www.youtube.com/view_play_list?p=3E44BCA6E69E1FED
Verification: http://www.youtube.com/view_play_list?p=855150D24C4B930B

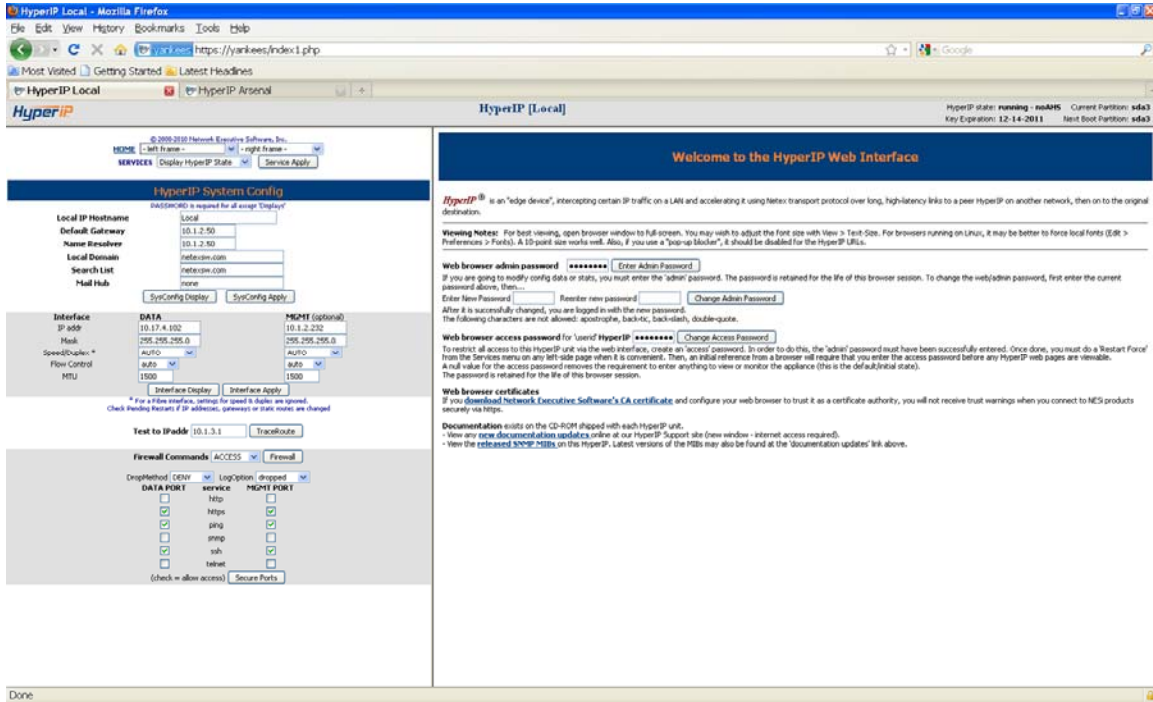
Additional information is available at:

<http://www.netex.com/support/hyperip-support-tablehyperip/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
- HyperIP Domain name
- DNS IP address
- Data port IP address and network mask (required)
- Mgmt port IP address and network mask (optional)

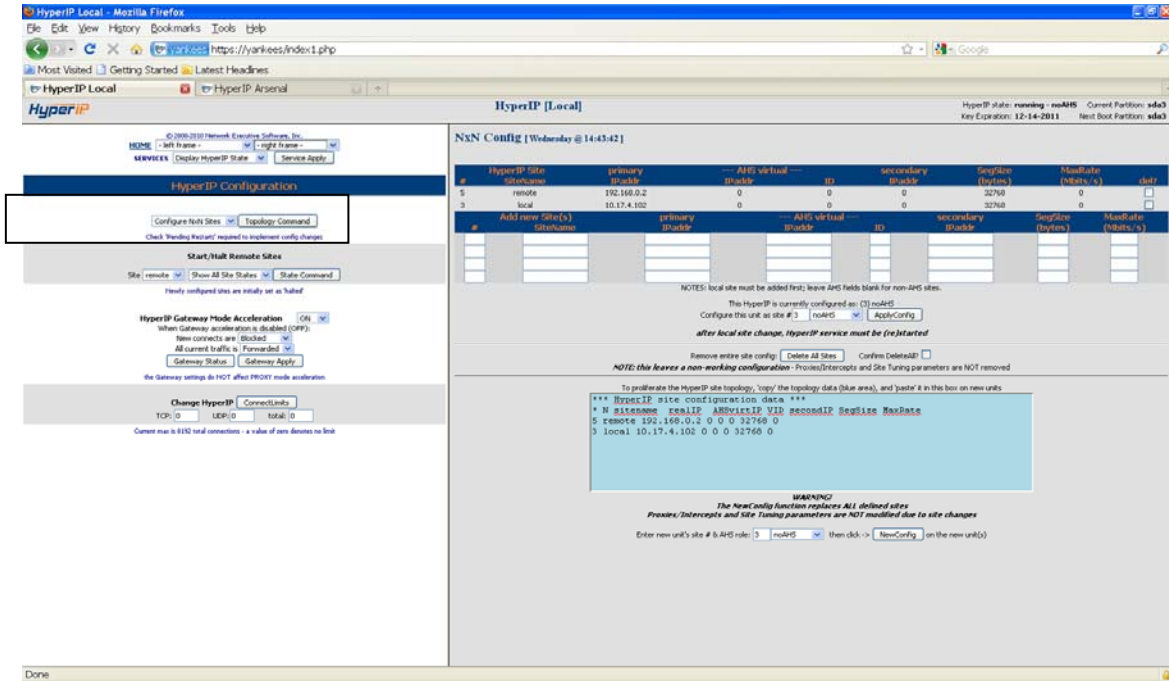


If there is only one interface available to the HyperIP, configure only the Data port.
To remove the mgmt port from use, enter "none" (without quotes) in the IP addr window.

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

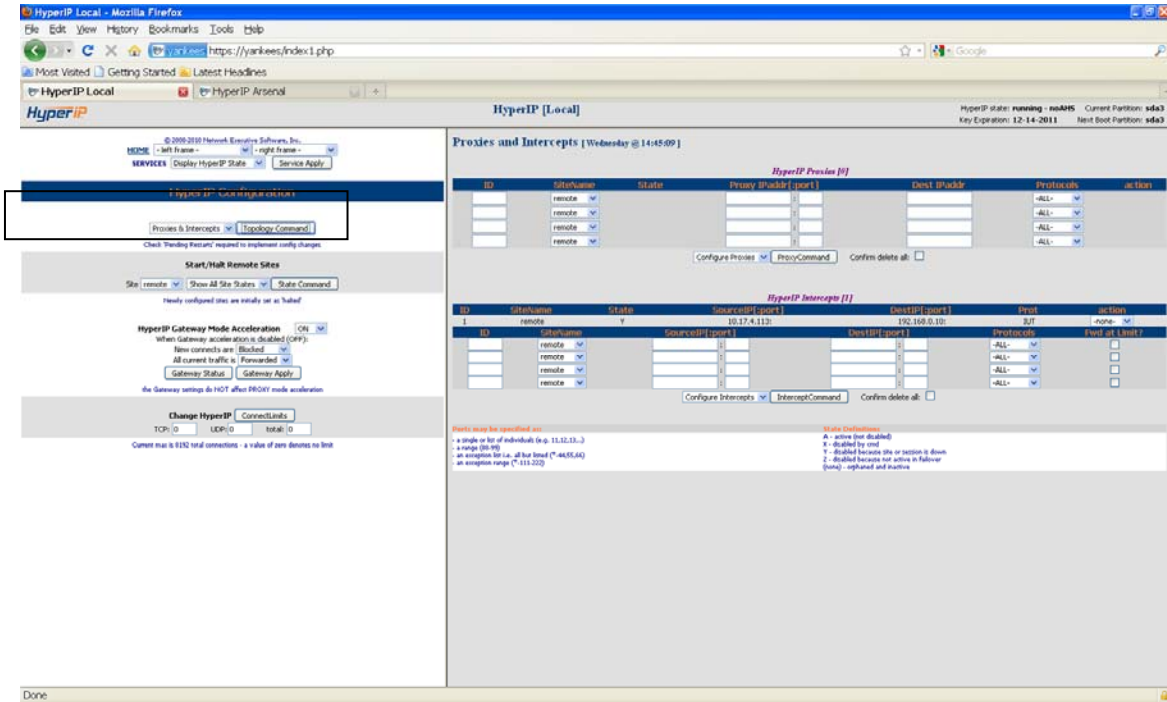
- Local HyperIP IP address
- Remote HyperIP IP address
- site number/site name (user-defined and unique within the HyperIP environment)
- MaxRate (required if there are multiple remote HyperIPs configured)
- Segsize (default: 32768 – May be changed after setup tests have been run)

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.

The HyperIP “Proxies & Intercepts” frame is launched from the HyperIP Configuration webpage and is used to configure what traffic the HyperIPs will intercept on behalf of the remote sites:
IP addresses or networks utilizing HyperIP



When configuring intercepts, the “sourceIP” is always an IP address or network on the same side of the WAN as the HyperIP being configured. The “DestIP” then will always be an IP address or network on the other side of the WAN.

Note: Intercepts networks may be defined on a byte boundary by using an asterisk wildcard. (Using 10.1.5.* will match IP addresses 10.1.5.0-10.1.5.255)