CORE™

CORE on a Wide Area Network (WAN)

Vitech

Vitech Corporation
2270 Kraft Drive, Suite 1600
Blacksburg, Virginia 24060
540.951.3322 FAX: 540.951.8222
Customer Support: support@vitechcorp.com
www.vitechcorp.com

CORE™ is a trademark of Vitech Corporation and refers to all products in the CORE software product family.

Other product names mentioned herein are used for identification purposes only, and may be trademarks of their respective companies.

Publication Date: June 2015

TABLE OF CONTENTS

LIST OF FIGURES

CUSTOMER RESOURCE OPTIONS

Supporting users throughout their entire journey of learning MBSE is central to Vitech's mission. For users looking for additional resources outside of this document, please refer to the links below. Alternatively, all links may be found at www.vitechcorp.com/resources.

Webinars
Webinar archive with over 40 hours of premium industry and tool-specific content.
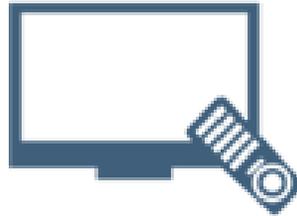
Screencasts
Short videos to guide users through installation and usage of Vitech software.

A Primer for Model-Based Systems Engineering
Our free eBook and our most popular resource for new and experienced practitioners alike.

Help Files
Searchable online access to Vitech software help files.

Technical Papers
Library of technical and white papers for download, authored by Vitech systems engineers.

MySupport
Knowledge Base, Exclusive Webinars and Screencasts, Chat Support, Documents, Download Archive, etc.

Our team has also created resources libraries customized for your experience level:

All Resources	**Advanced**
Beginner	**IT / Sys Admin**
Intermediate	**Student**

THIS PAGE INTENTIONALLY BLANK

INTRODUCTION

This document describes how to use CORE Server in a WAN (wide-area network) environment, including necessary configuration of the CORE server and clients, configuration of domain name servers, and configuration of network firewalls and routers separating the server and clients. When using CORE solely to access a local repository, no special configuration is required. When using CORE to access remote repositories across a WAN, these configuration changes are required.

ALTERNATIVE APPROACHES

Rather than configuring firewalls and routers to natively support CORE, it may be possible to leverage existing network capabilities.

Virtual Private Network (VPN)

If the CORE clients and server are on a common virtual private network (VPN) bridged by the firewalls between them, then no special configuration may be required. However, the firewalls should forward all traffic to the VPN, and firewall rules should not be applied to the VPN. In addition to simplifying configuration of CORE on a WAN, a VPN is also desirable because it provides end-to-end encryption of all CORE data.

Terminal Services

Windows Terminal Services and some other products can allow CORE users who are remote from the CORE Server to run their clients on the server but see the user interface on their own computers. Vitech cannot support this approach, but, if Terminal Services is already used in your organization, you may be able to leverage it. Using CORE via Terminal Services may require considerable resources on the server and may consume a moderate amount of network bandwidth, but performance will be better over high-latency links, especially for performing exports, generating reports, and running simulations.

GENERAL NOTES

The following should be observed throughout these instructions:

Restricted Port Numbers

While the IP ports used for CORE network communications are configurable, you should avoid using lower-numbered ports, many of which are already used by Windows operating systems. Using them in CORE may result in a resource conflict that could cause CORE and/or your operating systems to malfunction. Also avoid using ports required by other software on your network or any commonly used ports.

IP Services Database

The mapping of IP service names to port numbers and protocols is defined in a simple text file named "services." Several ports used by CORE are configured via this file. Because some ISP software installs its own version of the file, a computer may have several of them in different locations. When modifying this mapping, it is best to find and modify all of them. The default location is %SystemRoot%\system32\drivers \etc\services. The actual current location is specified in the Windows registry at:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
\DataBasePath.)

NETWORK LICENSE MANAGER (NLM) NOTES

The following facts may simplify configuring your network to support CORE:

Alternative License Mechanisms

The Network License Manager (NLM) allows a pool of licenses to be shared by all users with access to a common network. However, there are three alternatives to using the NLM for licensing. The preferred way to license CORE clients connected to a remote server is the "Enterprise" license mechanism. This is built into Enterprise server and requires no additional network configuration. However, the Enterprise license mechanism can only license CORE clients logged into the server, whereas the Network License Manager can serve a mix of CORE clients logged in to the server and locally. The "node-locked" license mechanism locks one client licenses directly to the client computer. The disadvantage is that it cannot be shared by multiple installations on different computers. There is also a USB mechanism which can be shared by multiple installations but requires a license USB key be attached to the computer running the software. Different users of the same CORE server can employ a mix of license mechanisms.

Network License Manager (NLM) 4.3.7

NLM 4.3.7 uses the UDP protocol. If an NLM client terminates abnormally, there may be a delay (90 minutes, by default) before the license is released. The NetTerm utility may be used to manually release an unused token. NetTerm can release tokens checked out by the computer where it is running. If NetTerm is running on the NLM server, it can release any token.

Network License Manager Location

If the Network License Manager is used, it is often installed on the same computer as the CORE Server software. However, the NLM is a separate product and can be installed on a separate host from the CORE server. (A client can obtain a license from an NLM on one computer and use it to log into a CORE server on another computer.) If possible, the NLM should be installed on the same LAN as the clients.

SERVER-SIDE FIREWALL RULES FOR NETWORK LICENSE MANAGER 4.3.7

The following must be allowed by a server-side firewall to permit CORE clients to obtain licenses from the NLM:

NLM Listening Port for CORE client

Default port: 32000
Protocol: UDP
Direction: Inbound
Server configuration: Customized NLM.Ini.Z file supplied by Vitech.
Client configuration: Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE \Vitech \CORE\9.0\NLM\port.

NLM Reply Port for CORE client

Default port: 32001
Protocol: UDP
Direction: Outbound
Server configuration: Automatic
Client configuration: Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE \Vitech \CORE\9.0\NLM\replyPort.

<u>**NLM Listening Port for NetTerm (Optional)**</u>

Default port: 32000
Protocol: UDP
Direction: Inbound
Server configuration: Customized NLM.Ini.Z file supplied by Vitech.
Client configuration: Options >> Network command on NetTerm console window or Windows
registry at:
HKEY_LOCAL_MACHINE\SOFTWARE \cca\netterm\nlm_port.

<u>**NLM Reply Port for NetTerm (Optional)**</u>

Default port: No default.
Protocol: UDP
Direction: Outbound
Server configuration: Automatic
Client configuration: Not configurable. NetTerm may not work if a server-side firewall restricts
outbound UDP traffic (initiated by the server).

SERVER-SIDE FIREWALL RULES FOR CORE

The following must be allowed by a server-side firewall to permit CORE clients to access the server:

<u>**CORE Server NetLDI Listening Port (Required)**</u>

Default port: 10995
Protocol: TCP
Direction: Inbound
Server configuration: Specified during installation or as "CORE90NetLDI" in the services file.
(See "IP Services Database" above)
Client configuration: Specified during installation or as "CORE90NetLDI" in the services file.
(See "IP Services Database" above)
Purpose: Handles client logins

<u>**Gem Listening Port (Required)**</u>

Default port: 10996
Protocol: TCP
Direction: Inbound
Server configuration: Specified during installation or manually as follows:

Must first stop and uninstall CORE90NetLDI service. At a command
prompt, enter:

netldi delete CORE90NetLDI

Edit   %CORE90Server%\InstallAids\CreateNetLDI.Bat.   Replace
"10996:10996" with desired port range. Run CreateNetLDI.Bat and start
the service.
Client configuration: Automatic
Purpose: A "gem" process is an agent spawned on the CORE application server for
each client.

Broadcast Update Port (Optional)

Default Port:	32971
Protocol:	UDP
Direction:	Outbound
Server configuration:	Specified during installation or as "CORE90Update" in the services file. (See "IP Services Database" above). Must be unique for each CORE server in the subnet.
Client configuration:	Automatic
Purpose:	The broadcast update mechanism is the most efficient way for the server to report repository changes to interested clients.

Backchannel Update Port (Optional)

Default Port:	32972
Protocol:	UDP
Direction:	Outbound
Server configuration:	Specified during installation or as "CORE90Update2" in the services file. (See "IP Services Database" above.)
Client configuration:	Automatic
Purpose:	The backchannel update mechanism is the second most efficient way for the server to report repository changes to interested clients. If a client is unable to use either the broadcast or backchannel update mechanism, it reverts to "standard" mode, which requires no additional ports or configuration.

CORE2net Server NetLDI Listening Port (Optional)

Default port:	10998
Protocol:	TCP
Direction:	Outbound
Server configuration:	Specified as "CORE2net90NetLDI" in the services file. (See "IP Services Database" above.)

SERVER-SIDE FIREWALL RULES FOR CORE2NET

The following must be allowed by a server-side firewall to permit web clients to browse pages served by a CORE2net web server. CORE2net is usually installed on the same host as the CORE server with which it is associated (during CORE2net installation). However, CORE2net is separately licensed and installed and may reside on a system that is remote from the CORE server, in which case an additional port is required:

HTTP Listening Port (Required)

Default port:	80
Protocol:	TCP
Direction:	Inbound
Server configuration:	Specified via Administrative Tools window in CORE client software (using a client that logs in to the CORE server associated with the CORE2net server).
Purpose:	Handles requests from HTTP clients such as web browsers.

<u>**CORE Server NetLDI Listening Port (Required)**</u>

Default port: 10995
Protocol: TCP
Direction: Outbound
Server configuration: Specified during installation or as "CORE90NetLDI" in the services file. (See "IP Services Database" above). Must match CORE server configuration.

<u>**Gem Listening Port (Required)**</u>

Default port: 10996 (depends on CORE server configuration as described above)
Protocol: TCP
Direction: Outbound
Server configuration: Automatic

<u>**CORE2net Server NetLDI Listening Port**</u>
(Required if CORE2net server resides on different host from CORE server)

Default port: 10998
Protocol: TCP
Direction: Inbound
Server configuration: Specified as "CORE2net90NetLDI" in the services file. (See "IP Services Database" above.)
Purpose: Listens for requests to start the CORE2net server. The requests are issued from the Administrative Tools window of the CORE client software.

SERVER-SIDE NETWORK ADDRESS TRANSLATION (NAT)

There are two kinds of network address translation (NAT): *dynamic* and *one-to-one*.

<u>**Firewall Configuration for Server-Side NAT**</u>

If a server-side firewall (or router) supports one-to-one NAT, then the device should assign the CORE server, Network License Manager (NLM), and/or CORE2net server unique NAT public addresses. If the firewall or router must employ dynamic NAT (or sufficient public addresses are not available), then it must forward the CORE Server NetLDI listening port and the gem listening port to the CORE server, the NLM listening port to the Network License Manager, and the CORE2net Server NetLDI listening port and the HTTP listening port to the CORE2net server.

<u>**DNS Configuration for Server-Side NAT**</u>

A symbolic name should be registered for the CORE server in DNS (Domain Name Service) servers both inside and outside the firewall or router. The DNS server inside the firewall or router should map the name to the server's actual IP address on its local network. The DNS server outside the firewall or router should map the same name to the server's NAT public address (if the firewall or router uses one-to-one NAT) or to the firewall's or router's WAN address.

CORE Server Configuration for Server-Side NAT

If no DNS is available inside the firewall or router to map the CORE server's symbolic name (as established above) to its private IP address, then the same effect can be achieved by adding the mapping to the "hosts" file on the server. The hosts file is located in the same folder as the "IP Services Database" file (described above).

Client Configuration for Server-Side NAT

If no DNS is available outside the firewall or router to map the CORE server's symbolic name (as established above) to its NAT public address (if the firewall or router uses one-to-one NAT) or to the firewall's or router's WAN address, then the same effect can be achieved by adding the mapping to the "hosts" file on the client. The hosts file is located in the same folder as the "IP Services Database" file (described above).

When prompted for the IP address of the CORE server during client installation, specify the server's symbolic name (as established above). The value can also be set via the CORE client login dialog.

If clients are still unable to log in to the CORE server using DNS servers and/or hosts files as described above, then, when prompted for the IP address of the CORE server during client installation, specify the CORE server's NAT public address in dotted-decimal form (if the firewall or router uses one-to-one NAT) or the firewall's or router's WAN address. The value can also be set via the CORE client login dialog. Set the server location to the actual private IP address of the CORE server as it is known on its local network.

When prompted for the IP address of the NLM during client installation, specify the NLM host's NAT public address (if the firewall or router uses one-to-one NAT) or to the firewall's or router's WAN address. If the client is already installed, set the value from the network license chooser dialog.

CORE2net Configuration for NAT

No special steps are required if the CORE2net server software runs on the same host as the CORE server. If the CORE2net server is separate from the CORE server, then special configuration is required only if network address translation is performed by a device between them on the network.

If NAT is performed on the side of the CORE2net server: when you specify the IP address of the CORE2net server via the Administrative Tools window in the CORE client software, use the CORE2net server's NAT public address (if the firewall or router uses one-to-one NAT) or the firewall's or router's WAN address.

Note that a web browser attempting to access CORE2net may need to specify a different address, depending on its network path to the CORE2net server.

If NAT is performed on the side of the CORE server: if no DNS is available outside the firewall or router to map the CORE server's symbolic name (as established above) to its NAT public address (if the firewall or router uses one-to-one NAT) or to the firewall's or router's WAN address, then the same effect can be achieved by adding the mapping to the "hosts" file on the CORE2net server. The hosts file is located in the same folder as the "IP Services Database" file (described above).

When prompted for the IP address of the CORE server during CORE2net server installation, specify the CORE server's symbolic name (as established above). If the CORE2net server is already installed, set the value in the Windows registry at:
HKEY_LOCAL_MACHINE\SOFTWARE\Vitech\CORE2net Communication Server\9.0\Database \serverName.

If the CORE2net server still fails on startup using DNS servers and/or hosts files as described above, then, when prompted for the IP address of the CORE server during CORE2net server installation, specify the CORE server's NAT public address in dotted-decimal form (if the firewall or router uses one-to-one NAT) or the firewall's or router's WAN address. If the CORE2net server is already installed, set the value in the Windows registry at: HKEY_LOCAL_MACHINE\SOFTWARE\Vitech\CORE2net Communication Server\9.0\Database \serverName. Add the following string value in the Windows registry: HKEY_LOCAL_MACHINE \SOFTWARE\Vitech\CORE2net Communication Server\9.0\Database\gemServerName. Set it to the actual private IP address of the CORE server as it is known on its local network.

CLIENT-SIDE FIREWALL RULES FOR NETWORK LICENSE MANAGER 4.3.7

The following must be allowed by a client-side firewall to permit CORE clients to obtain licenses from Network License Manager (NLM) 4.3.7:

NLM Listening Port for CORE client

Default port:	32000
Protocol:	UDP
Direction:	Outbound
Client configuration:	Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE \Vitech \CORE\9.0\NLM\port. Must match server configuration.

NLM Reply Port for CORE client

Default port:	32001
Protocol:	UDP
Direction:	Inbound
Client configuration:	Windows registry at HKEY_LOCAL_MACHINE\SOFTWARE \Vitech \CORE\9.0\NLM\replyPort.

NetTerm (Optional)

NetTerm will not work with a client-side firewall.

CLIENT-SIDE FIREWALL RULES FOR CORE

The following must be allowed by a client-side firewall to permit CORE clients to access the server:

NetLDI Listening Port (Required)

Default port:	10995
Protocol:	TCP
Direction:	Outbound
Client configuration:	Specified during installation or as "CORE90NetLDI" in the services file. (See "IP Services Database" above). Must match server configuration.

Gem Listening Port (Required)

Default port:	10996 (depends on server configuration as described above)
Protocol:	TCP
Direction:	Outbound
Client configuration:	Automatic

Broadcast Update Port (Optional)

Default Port:	32971 (depends on server configuration as described above)
Protocol:	UDP
Direction:	Inbound
Client configuration:	Automatic

Backchannel Update Port (Optional)

Default Port:	32972 (depends on server configuration as described above)
Protocol:	UDP
Direction:	Inbound
Client configuration:	Automatic

API Login Port (Optional)

Default Port:	32002
Protocol:	TCP
Direction:	Inbound
Client configuration:	Specified via Administrative Tools window in CORE client software. (Must be matched by any application written to use CORE Applications Programming Interface against this client.)
Purpose:	Listens for connections from programs written to use CORE API.

API Data Ports (Optional)

Default Ports:	32003-32050
Protocol:	TCP
Direction:	Inbound
Client configuration:	Specified via Administrative Tools window in CORE client software.
Purpose:	Handle requests from programs in active CORE API sessions.

CLIENT-SIDE NETWORK ADDRESS TRANSLATION (NAT)

There are two kinds of network address translation (NAT): *dynamic* and *one-to-one*.

Firewall Configuration for Client-Side NAT

Special configuration is required if client-side network address translation is applied to a client that needs to obtain a NLM 4.3.7 license, that desires the efficiency of the "broadcast" or "backchannel" update modes, or which will be used as a CORE API server. If the client-side firewall (or router) supports one-to-one NAT, then the device should assign each CORE client a unique NAT public address. If the firewall or router must employ dynamic NAT (or sufficient public addresses are not available), and if only a single client is located behind it, then it must forward the inbound ports listed above to the CORE client.

If multiple clients are behind the firewall or router, and if it must employ dynamic NAT (or sufficient public addresses are not available), then at most one of the clients will be able to use broadcast update mode, and at most one of the clients will be able to use backchannel update mode. (The broadcast update port can be forwarded to one and the backchannel port to the other.) The remaining clients will automatically revert to "standard" update mode, which is less efficient. Each client requiring an NLM license should be assigned a different NLM reply port. Each client which will act as a CORE API server should be assigned a different API login port and a distinct range of API data ports. The firewall or router should forward the appropriate ports to the respective clients.

Client Configuration for Client-Side NAT

If multiple CORE clients are behind a client-side firewall (or router), and if it must employ dynamic NAT (or sufficient public addresses are not available), then it must forward a unique set of inbound ports to each client (as described above). A client's assigned Network License Manager reply port can be specified in the Windows registry at: HKEY_LOCAL_MACHINE\SOFTWARE\Vitech\CORE\9.0\NLM\replyPort. If a client will act as a CORE API server, its assigned API login and data ports can be specified via the Administrative Tools window in the CORE client software.

NetTerm

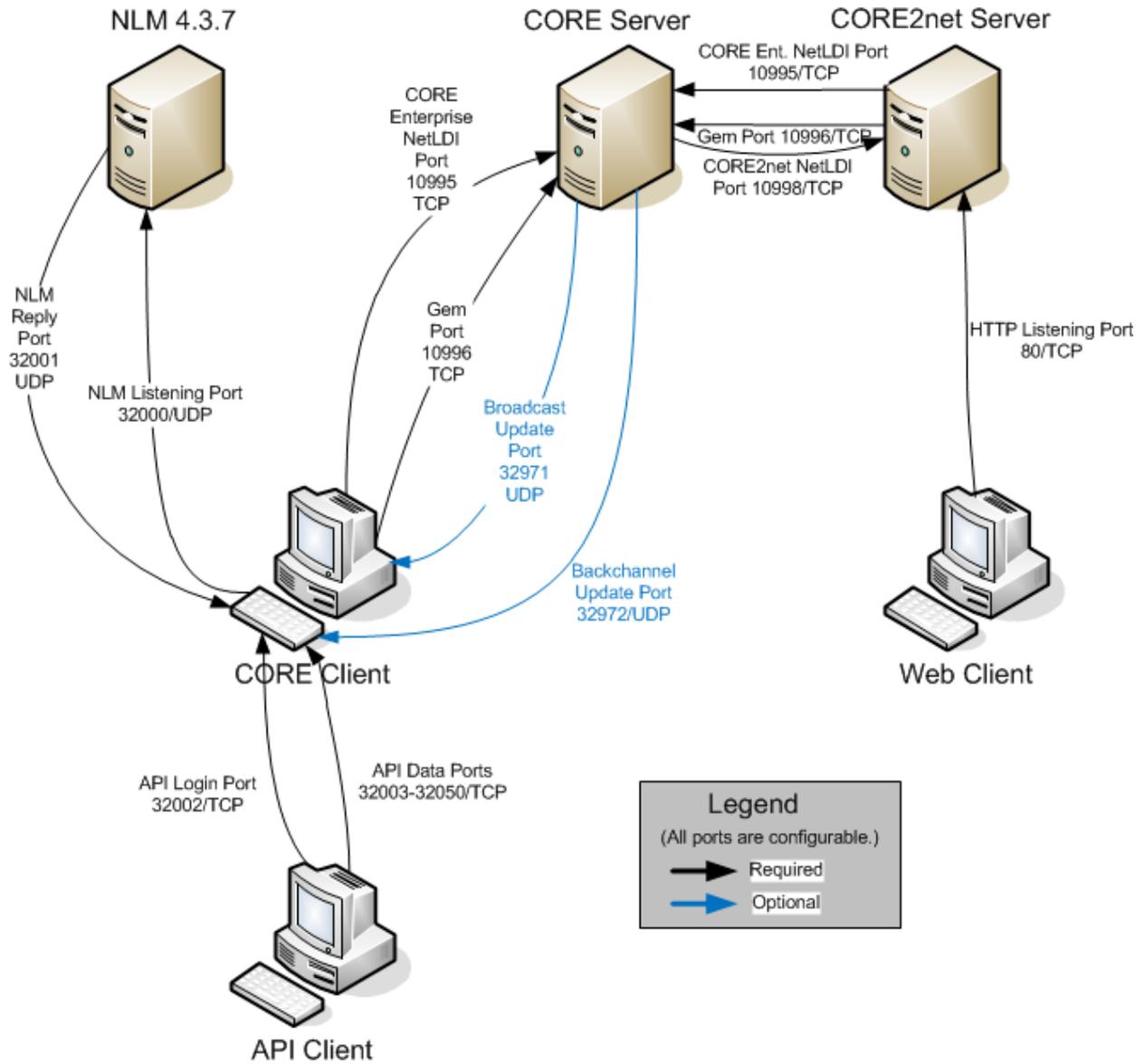NetTerm will not work with client-side NAT.

Figure 1 - Network Diagram

Vitech Corporation

2270 Kraft Drive, Suite 1600
Blacksburg, Virginia 24060
540.951.3322 FAX: 540.951.82222
Customer Support: support@vitechcorp.com
www.vitechcorp.com