TIBCO Messaging Appliance™ P-7500

Operations Guide

Software Release 8.7
revised November 2012

Two-Second Advantage®

Important Information

Contents

Figures

Preface

This document describes how to perform a variety of tasks associated with managing the operation of TIBCO Messaging Appliance P-7500 systems. The software procedures show you how to perform tasks using the P-7500 Command Line Interface (CLI).

Topics

Audience

This document is intended for use as a reference by system administrators and experienced users who are familiar with IP network configuration.

TIBCO assumes that:

- you have a functioning IP network
- you and your TIBCO Sales representative have determined the correct number and placement of P-7500 systems required
- that these P-7500 systems have been or will be installed in an equipment rack and at least minimally configured by network administrators who are responsible for installing and setting up network equipment

Related Documentation

This section lists documentation resources you may find useful.

TIBCO Messaging Appliance P-7500 Documentation

In addition to this book, the following documents form the TIBCO Messaging Appliance P-7500 documentation set:

- *TIBCO Messaging Appliance P-7500 Hardware Installation*
- *TIBCO Messaging Appliance P-7500 Getting Started*
- *TIBCO Messaging Appliance P-7500 Concepts*
- *TIBCO Messaging Appliance P-7500 Maintenance and Troubleshooting*
- *TIBCO Messaging Appliance P-7500 Administration Interface Reference*
- *TIBCO Messaging Appliance P-7500 Release Notes*

  If the information in the latest *TIBCO Messaging Appliance P-7500 Release Notes* differs from the information in this document, always follow the release notes.

Typographical Conventions

The following typographical conventions are used in this manual.

Table 1 General Typographical Conventions

Convention	Use
`code font`	Code font identifies commands, code examples, filenames, pathnames, and output displayed in a command window. For example: Use `MyCommand` to start the foo process.
`bold code font`	Bold code font is used in the following ways: • In procedures, to indicate what a user types. For example: Type **`admin`**. • In large code samples, to indicate the parts of the sample that are of particular interest. • In command syntax, to indicate the default parameter for a command. For example, if no parameter is specified, `MyCommand` is enabled: MyCommand [**`enable`** | disable]
italic font	Italic font is used in the following ways: • To indicate a document title. For example: See *TIBCO BusinessWorks Concepts*. • To introduce new terms For example: A portal page may contain several portlets. *Portlets* are mini-applications that run in a portal. • To indicate a variable in a command or code syntax that you must replace. For example: `MyCommand` *pathname*
Key combinations	Key name separated by a plus sign indicate keys pressed simultaneously. For example: Ctrl+C. Key names separated by a comma and space indicate keys pressed one after the other. For example: Esc, Ctrl+Q.

Table 2 Syntax Typographical Conventions

Convention	Use
`[ ]`	An optional item in a command or code syntax. For example: `MyCommand [optional_parameter] required_parameter`
`|`	A logical 'OR' that separates multiple items of which only one may be chosen. For example, you can select only one of the following parameters: `MyCommand para1 | param2 | param3`

`{ }`	A logical group of items in a command. Other syntax notations may appear within each logical group.
	For example, the following command requires two parameters, which can be either the pair `param1` and `param2`, or the pair `param3` and `param4`.
	`MyCommand {param1 param2} | {param3 param4}`
	In the next example, the command requires two parameters. The first parameter can be either `param1` or `param2` and the second can be either `param3` or `param4`:
	`MyCommand {param1 | param2} {param3 | param4}`
	In the next example, the command can accept either two or three parameters. The first parameter must be `param1`. You can optionally include `param2` as the second parameter. And the last parameter is either `param3` or `param4`.
	`MyCommand param1 [param2] {param3 | param4}`

How to Contact TIBCO Support

For comments or problems with this manual or the software it addresses, please contact TIBCO Support as follows.

- For an overview of TIBCO Support, and information about getting started with TIBCO Support, visit this site:

  http://www.tibco.com/services/support

- If you already have a valid maintenance or support contract, visit this site:

  https://support.tibco.com

  Entry to this site requires a user name and password. If you do not have a user name, you can request one.

Chapter 1 General Administration Tasks

This chapter describes a variety of tasks associated with managing the TIBCO Messaging Appliance P-7500 system. Each section in the chapter covers a different topic.

Topics

Displaying the Software Version

The TIBCO Messaging Appliance P-7500 system software consists of these major components:

- Command Line Interface (CLI)
- Data Plane Manager
- Control Plane
- Management Plane

The user can determine the version of all components using the show version CLI command:

```
tibco> show version

Process              Release          Build date
-------------------- ---------------- -------------------------------------
CLI                  8.3.0.0100       Jan  8  2009 14:24:17 EST
DataplaneMgr         8.3.0.0100       Jan  8  2009 14:24:17 EST
Controlplane         8.3.0.0100       Jan  8  2009 14:24:17 EST
Managementplane      8.3.0.0100       Jan  8  2009 14:24:17 EST

RVGD Version: 8.3.0 V8 1/22/2009

Current load is: 8.3.0.0100
Backout load is: 8.2.0.0100

Loads available on the router:
Load 1: 7.0.2
Load 2: 7.2.0
Load 3: 8.1.2
Load 4: 8.2.0
Load 5: 8.3.0

System uptime: 10d 2h 38m 38s

 tibco>
```

NOTICE

NOTICE: The TIBCO Messaging Appliance P-7500 systems do not currently support upgrades or patches to an individual system software component, so in a properly installed system all of the software components display the same release number.

Configuring Network Parameters

You are able to quickly configure the behavior of the networking stack from the CLI using the setup Privileged EXEC command to configure network parameters. For details on how to use the setup Privileged EXEC command, refer to *TIBCO Messaging Appliance P-7500 Getting Started*.

You specify network information using the setup Privileged EXEC command in the CLI. You enter the setup command and it prompts you for this information:

Table 3 setup Privileged EXEC Command Prompts

Parameter	Description
Hostname	the host name of the Rendezvous P-7500
Link Aggregation Group (LAG)	a set of multiple physical Ethernet ports combined (that is, aggregated) into one high-speed virtual workgroup or logical port, as defined by the IEEE 802.3ad standard
IP Address / subnet mask	the static IP address and subnet mask (default gateway) for the management interface eth1 and messaging interface lag1
NTP server	the IP address of the Network Time Protocol (NTP) server
DNS server	the IP address of the Domain Name System (DNS) server
Default Gateway	the IP address of the Default Gateway
Clock	the local time in the format hh:mm:ss for the system clock
Time Zone	the local time zone and number of hours and minutes offset from Coordinated Universal Time (UTC) for the system time zone

Managing User Accounts

NOTICE

NOTICE: There is a limit of eight concurrent CLI user sessions per TIBCO Messaging Appliance P-7500 system, not including the always available serial console port located on the rear of the P-7500. This limit does not apply to SFTP user accounts.

Creating User Accounts

The system administrator can assign CLI or SFTP user accounts to multiple individuals within an organization. Create new user accounts or change user account passwords using the username Global CONFIG command:

tibco(config)# username *name* password *password* [cli | sftp]

where:

name	is the user name to be assigned to the user account. An account user name can contain up to 32 alphanumeric characters, and must be unique among all created user accounts, whether CLI or SFTP.
password	is the password to be assigned to the user account. An account password can contain up to 128 alphanumeric characters, and can be used with all created user accounts, CLI or SFTP.
cli	specifies a CLI user account. It is the default and creates a standard CLI account.
sftp	specifies an SFTP user account. SFTP accounts are used to retrieve log files from the P-7500.

Use the no username Global CONFIG command to delete existing user accounts:

tibco(config)#no username *name*

where the *name* parameter is identical to the username command.

Both the username and no username commands must be run in Global Configuration mode.

For example, to create a new CLI user:

tibco> enable

```
tibco# configure
tibco(config)# username bob01 password tibpub1
tibco(config)#
```

Changing the CLI Inactivity Timeout Setting

When a CLI user fails to log out or leaves an open CLI session connected to the P-7500 indefinitely, the CLI session connection is automatically closed after a period of inactivity.

Changing Timeout Globally

The default global timeout setting that a CLI session can wait without activity before it times out is five minutes. Global CLI inactivity timeout settings apply across all CLI user sessions.

To change on a global basis the CLI inactivity timeout setting for all CLI user sessions on the TIBCO Messaging Appliance P-7500 system, enter the console Global CONFIG command:

tibco(config)# console timeout *idle-timeout*

where *idle-timeout* is the integer value specifying the inactivity timeout value in minutes. Valid range is 0 to 43200. To disable the timer, enter 0.

Changing Timeout Session-by-Session

You can change the CLI timeout setting on a session-by-session basis. The per session setting overrides the global timeout setting, but only for the specified CLI user session.

To change the CLI inactivity timeout setting for your current CLI user session on the TIBCO Messaging Appliance P-7500 system, enter the session Privileged EXEC command:

tibco# session timeout *idle-timeout*

where *idle-timeout* is the integer value specifying the inactivity timeout value in minutes. Valid range is 0 to 43200. To disable the timer, enter 0.

Displaying Inactivity Timeout Settings

To show the global inactivity timeout configuration for all CLI user sessions on the TIBCO Messaging Appliance P-7500 system, enter the show console User EXEC command:

```
tibco> show console
Inactivity timeout: <disabled>
```

To show the inactivity timeout configuration for all current CLI user sessions on the TIBCO Messaging Appliance P-7500 system, enter the show session User EXEC command:

```
tibco> show session
```

Example:

```
tibco(config)# session timeout 90
tibco> show session
session   user          from            login                idle          timeout
  1       tibco1   192.168.1.213   2008-09-09 10:56:23   0d 0h 1m 52s      0
* 2       tibco2   192.168.1.213   2008-09-09 11:47:43    0d 0h 0m 0s      90
* indicates current session
```

Disconnecting a CLI User Session

To forcibly disconnect a CLI user session from the TIBCO Messaging Appliance P-7500 system, and thereby allow access to the system for other CLI users, enter the disconnect Privileged EXEC command:

```
tibco# disconnect sessionid session-id
```

where *session-id* is the integer value correlating to an existing session number, as displayed by the show session User EXEC command. The *session-id* identifies which session to disconnect. Valid range is 1 to 8 (corresponding to the eight possible CLI user sessions).

Note: Users cannot disconnect their own session. A disconnect command that specifies the current session is ignored.

Example

```
tibco> show session
session    user          from                  login          idle    timeout
* 1       tibco1  192.168.1.35   2008-11-28  16:31:10   0d 0h 0m 0s        90
  2       tibco2  192.168.1.246  2008-11-28  16:43:49   0d 0h 1m 52s        0
* indicates current session
tibco> enable
tibco# disconnect sessionid 2
```

When user session 2 is disconnected, this message is displayed to tibco2:

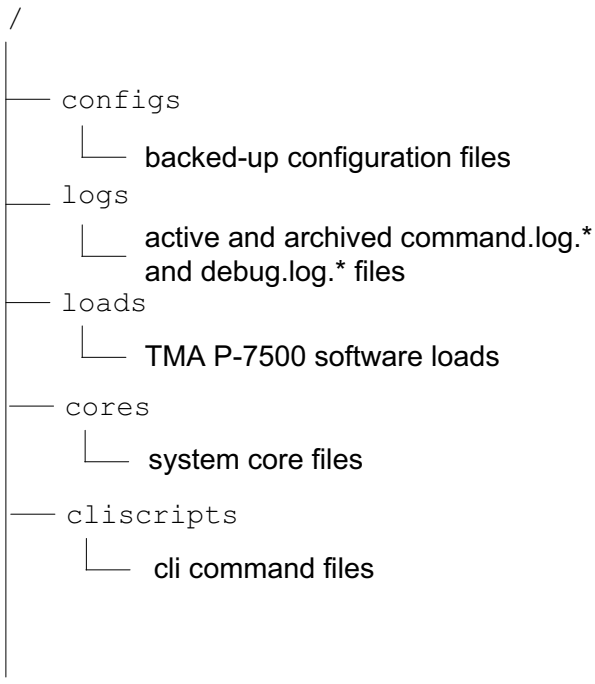
```
Exiting due to disconnect from tibco1, session 1, from 192.168.1.35
```

Adding or Removing System Files

The user has access to a restricted part of the file system on the TIBCO Messaging Appliance P-7500 system and has various CLI commands available to manipulate this file system.

All files which you can add or remove from the TIBCO Messaging Appliance P-7500 system exist under the / root directory. The root directory structure is shown in Figure 1, along with the names of the subdirectories and a brief description of what they contain.

Figure 1 Root Directory Structure



Note: The debug log record files contained in the directory /logs are for use by TIBCO support staff only.

Running these CLI commands allows you to operate on, read, and generate P-7500 files in the / root directory:

cd

To change the present working directory, enter the cd User EXEC command:

tibco> cd [*directory*]

where *directory* is the directory to change to. If none is specified, the working directory is changed to the / root directory.

copy

Used to either:

- copy current configuration locally within the TIBCO Messaging Appliance P-7500 system
- back up a configuration database file to an SFTP server from the /configs subdirectory on a TIBCO Messaging Appliance P-7500 system
- restore a configuration database file from a SFTP server to the /configs subdirectory on a TIBCO Messaging Appliance P-7500 system
- download new software from a SFTP server to the /loads subdirectory on a TIBCO Messaging Appliance P-7500 system for software upgrade

To copy the current configuration locally within the TIBCO Messaging Appliance P-7500 system, enter this copy Privileged EXEC command:

tibco# copy current-config *destination*

where *destination* is the location in the system / root directory to put the configuration copy. Valid file name formats are described in Table 4.

Refer to TIBCO Messaging Appliance P-7500 *Maintenance and Troubleshooting* for more information on the copy Privileged EXEC command and its use.

Table 4 Valid File Name Formats for copy Privileged EXEC Command

Format	Syntax	Description
current-config	current-config	The current persistent-state of the TIBCO Messaging Appliance P-7500 system.
SFTP	sftp://[*username@*]*ip-addr*/ *remote-pathname*	A remotely available file accessible through the SFTP protocol. In a copy operation only one of either *source* or *destination* can be specified as an SFTP file, but not both. Copying of files through the Secure Copy (SCP) protocol is not supported by the TIBCO Messaging Appliance P-7500 system.
pathname	[/][*directory*/]*filename*	Absolute or relative name of a regular file stored in the / root directory. Internally, an absolute name is always relative to the / root directory, while relative names are always evaluated relative to the present working directory (displayable through the pwd User EXEC command).

To delete a file from the TIBCO Messaging Appliance P-7500 system, enter the delete Privileged EXEC command:

tibco# delete *filename*

where *filename* is the name of the local file to delete which might include a pathname. Only local-pathname formats can be used. * and ? characters can be used to match multiple files.

dir

To list the contents of a directory, enter the dir User EXEC command:

tibco> dir [*pattern*]

where *pattern* is the name of the file or directory to display. * and ? characters can be used to match multiple files. If not specified, all the files in the present working directory are displayed.

more

To display the contents of a text file in a directory, enter the more User EXEC command:

tibco> more *pattern*

where *pattern* is the name of the text file to display. * and ? characters can be used to match multiple text files. If not specified, all the text files in the present working directory are displayed.

Note: Binary files cannot be displayed.

pwd

To display the present working directory (pwd), enter the pwd User EXEC command. For example:

tibco> pwd

The present working directory is displayed.

rename

To rename a P-7500 file within one of the / root subdirectories listed in Figure 1, enter the rename Privileged EXEC command:

tibco# rename *old-name new-name*

where:

old-name is the current name of the Pathname file to be renamed. Only local-pathname formats can be used.

new-name is the new name for the Pathname file specified by *old-name*. Only local-pathname formats can be used.

Configuring DNS Servers

The DNS server is configured and managed by an administrator. Refer to your third-party DNS server documentation for information on choosing a host machine and installing the server software.

To successfully enable a DNS server, you must have previously configured a DNS server on a host machine, and configured the DNS server settings on your P-7500.

Overview

A Domain Name System (DNS) server resolves server hostnames to the correct IP address. Residing on a separate host machine accessible by the TMA P-7500, the DNS server allows you to assign hostnames for network object IP addresses. Once configured, CLI commands that use the hostname parameter are directed to the configured DNS server for IP address resolution.

DNS Server CLI Commands

name-server

To provision a primary DNS server to resolve host names for the TMA P-7500, enter the name-server Global CONFIG command:

tibco(config)# name-server *ip-addr*

where *ip-addr* is the IP address for the DNS server, specified in the dotted decimal notation form *nnn.nnn.nnn.nnn*.

ALERT! The name-server Global CONFIG command causes a disruption in customer service because it restarts the P-7500.

NOTICE

NOTICE: Ensure that the DNS server IP address is reachable from the TMA P-7500 management interface.

no name-server

To de-provision an existing DNS server and delete all associated configuration values, enter the no name-server Global CONFIG command:

```
tibco(config)# no name-server
```

show name-server

To query the currently provisioned DNS server, enter the show name-server Global CONFIG command:

```
tibco(config)# show name-server
```

DNS Server Configuration Example

A sample session to provision a DNS server with an IP address of “192.120.1.1” is:

```
tibco(config)# name-server 192.120.1.1
WARNING: This will cause a reboot of the system
Do you want to continue (y/n)? y
tibco(config)#
```

A sample session to query the provisioned DNS server is:

```
tibco> show name-server
Name server: 192.120.1.1
```

Configuring 802.3ad Link Aggregation

Overview

Link aggregation, defined in IEEE standard 802.3ad, is a standard for aggregating multiple Ethernet ports into one virtual interface. The aggregated ports appear as a single IP address to your P-7500 and applications, which means no application changes are required.

Used by the Network Acceleration Blade (NAB), 802.3ad link aggregation provides these advantages:

- increased network bandwidth –

  The capacity of multiple links is combined into one logical link.

- increased availability –

  With link aggregation, traffic on a failed link can be redirected to one of the other links in the LAG (that is, the logical port transparently continues to function over the remaining physical ports). This allows for larger client loads per P-7500 system with a longer meantime between failures.

- more efficient bandwidth utilization –

  All traffic to or from the logical port is transparently load shared among all of the available physical ports.

Since 802.3ad link aggregation is an open standard for the construction of aggregated links between multiple vendors' devices, it allows for the interconnection of multiple vendors' equipment.

NOTICE

NOTICE: The use of 802.3ad link aggregation is restricted as follows:

- only point-to-point links between two devices can be aggregated. Multipoint aggregations among more than two devices is not supported.
- link aggregation is supported only on point-to-point links with MACs operating in full duplex mode
- all links in a LAG must operate at the same data rate: 1000 Mb/s

Using link aggregation, network traffic is dynamically distributed across ports, so administration of what data actually flows across a given port is taken care of automatically within the aggregated link.

Note: The NAB configures 802.3ad link aggregation on TIBCO Messaging Appliance P-7500 systems as Active mode only. Thus, third-party switches that support 802.3ad link aggregation can be configured as either Active or Passive mode when connected to the TIBCO Messaging Appliance P-7500 system.

The link aggregation standard provides inherent, automatic redundancy on point-to-point links. In other words, if one of the multiple ports used in a link fails, network traffic is dynamically redirected to flow across the remaining good ports in the link. The redirection is fast and triggered when a switch detects the physical failure. The switch then sends the data to the new port location, and the network continues to operate with virtually no interruption.

Link Aggregation Tasks

By default through the setup Privileged EXEC command, the physical interfaces on the NAB are all configured as 'lag1' upon completing the initial software configuration procedure described in *TIBCO Messaging Appliance P-7500 Getting Started*.

The NAB of a P-7500 system also supports multiple IP Addresses on an interface in addition to 802.3ad link aggregation. To assign independent IP addresses to every port of the NAB (that is, have no LAG configured), or have a mixture of some NAB ethernet ports grouped into a single LAG and the remaining ports independently addressed, refer to Chapter 8, Configuring IP Interfaces and Addresses, on page 123.

Turning Off Power to the System

To turn off power to the P-7500 system, on a system by system basis, enter the power-down Privileged EXEC command:

```
tibco# power-down
```

ALERT

ALERT! Notify the appropriate personnel to ensure that all traffic to and from P-7500 systems is stopped before issuing the power-down Privileged EXEC command Otherwise, the power-down command causes a disruption in customer service.

Use the power-down Privileged EXEC command when, for example, you have to pack up and move the P-7500 system.

After issuing the power-down Privileged EXEC command, use a paper clip to press the 1/0 button on the front panel of the P-7500 system to turn power back on (refer to *TIBCO Messaging Appliance P-7500 Hardware Installation* for location and details on the 1/0 button).

Note: The P-7500 system does not restart automatically after this command is run.

Managing Command Logging

For network monitoring (for example, identifying the user who caused a security violation, or identifying when a security violation occurred on the network), it is useful for the system administrator to be able to retrieve a log of all user command actions attempted on the P-7500 system through the CLI, web, and SEMP interfaces.

The command logging facility is used to capture information about all P-7500 system commands issued by users through either the P-7500 CLI, web, or SEMP interface.

Command Log Record Data

The information contained in each command log record includes, in order:

- log date and time, for example, Oct 20 12:15:51
- syslog destination and level, for example, <local1.info>
- host name of the P-7500 system, for example, tibco1
- local user name with local process identifier number or pid in square brackets, for example, bob[7703]
- type of P-7500 system interface making the command attempt, for example, CLI, web, or SEMP
- IP address of host of source of command attempt, for example, 192.168.1.215
- user name assigned to the CLI, web, or SEMP user account
- time when command attempt was started, for example, 12:15:51
- time when command attempt finished, for example, 12:15:51
- description of result, that is: ok, command action status, or reason for failure
- command operation attempted

Note: All CLI, web, and SEMP configuration command attempts made on P-7500 systems are logged by default.

Naming Convention

Command log record files are uncompressed text files with the name command.log.[*x*], where *x* is an integer from 1 to 20 identifying the archived file number, and the active file is named command.log.

Logging Capacity

The active command log record file is closed once the file size exceeds 50MB. Upon closing, a new file is opened, and this cycle repeats. The command log record file is in the directory /logs and is available for retrieval from P-7500 systems. There are up to 21 command log record text files available for viewing at any one time, including the currently active log file.

Directory Maintenance

Directory maintenance is not required for command log record files because the files are rotated.

Configuring Command Logging

To configure the command logging feature on a P-7500 system, switch to the logging configuration mode:

```
tibco(config)# logging
```

You are now in the logging configuration mode:

```
tibco(config-logging)#
```

Enter the command Logging CONFIG command:

```
tibco(config-logging)# command {cli | semp-mgmt | web | all} mode {shutdown | config-cmds | all-cmds}
```

where:

cli, semp-mgmt, web, or all	specifies which P-7500 interface to be logged.
shutdown	turns off the command logging facility for the specified P-7500 interface (cli, semp-mgmt, web, or all).
config-cmds	log configuration commands only (not show commands) for the specified P-7500 interface (cli, semp-mgmt, web, or all). This is the default.
all-cmds	log all commands except for help (help commands are never logged) for the specified P-7500 interface (cli, semp-mgmt, web, or all).

Note: The no version of this command (no command {cli | semp-mgmt | web | all}) reverts logging back to the default mode of config-cmds for the specified P-7500 interface.

Viewing Command Logging Configuration

To view the configuration of the command logging facility on the P-7500, enter the show logging command User EXEC command:

```
tibco> show logging command
```

Example:

```
tibco> show logging command

Cmd Interface      Logging Mode
-----------------------------------------------
CLI                all
SEMP/mgmt          config
web                config
```

Retrieving Command Log Record Files

Command log record files are stored locally on the P-7500 in subdirectory /logs as uncompressed text files, for retrieval and viewing by the system administrator on a regular basis.

Retrieval and viewing of command log record files can be done by using either the copy or more command.

The copy Privileged EXEC command transfers a text file from the /logs subdirectory to an external SFTP server from the P-7500 for viewing:

tibco# copy [/][logs/]*filename* sftp://[*username@*]*ip-addr*/*remote-pathname*

Where:

filename	is the name of the command log record file (that is, command.log.[*x*]).
username@ *ip-addr* *remote-pathname*	point to the location where the command log record file is to be copied onto the SFTP server.

Note: Ensure that you have an SFTP server on the P-7500 network to which you have IP connectivity.

The more User EXEC command directly displays the contents of a text file from the /logs subdirectory on the P-7500 for viewing:

tibco> more /logs/*pattern*

where *pattern* is the name of the command log record file (that is, command.log.[*x*]) to display. * and ? characters can be used to match multiple text files.

Displaying System Alarms

To enable the display of P-7500 system alarms in the current CLI session, on a session-by-session basis, enter the alarm-display User EXEC command:

```
tibco> alarm-display
```

To disable the display of P-7500 system alarms in the current CLI session, on a session-by-session basis, enter the no alarm-display User EXEC command:

```
tibco> no alarm-display
```

Example:

```
tibco> alarm-display

## ATTENTION: Critical System Alarms. Enter "show alarm" to view. ##

tibco> show alarm

Alarm display is enabled.

Source        | Slot | Alarm
--------------+------+-----------------------------------------------
Chassis Fan 2 |      | Failed
```

Note: The display of P-7500 system alarms is enabled by default.

Recovering Lost Passwords

Contact TIBCO for technical support to recover lost passwords from P-7500 systems.

Chapter 2 Managing TIBCO Rendezvous Tasks

This chapter describes the tasks associated with managing TIBCO Rendezvous operations on the TIBCO Messaging Appliance P-7500 system, including:

- client parameters
- the Command Line Interface (CLI) commands used to manage the range of Rendezvous client services supported by P-7500 systems

Rendezvous clients are entities to which P-7500 systems offer service. Through these entities P-7500 systems provide various access control capabilities that the network administrator can manage on a per client basis, or on a group of clients using profiles.

Profiles allow common configurations to be applied to groups of clients, which makes provisioning users from the CLI easier.

Topics

Overview

Clients

Clients send content into the network and also receive traffic from the network. They access the network by establishing a TCP connection to their P-7500 system.

Clients are created automatically by the P-7500 system, and are identified by the IP address and TCP port used by the P-7500 system to reach them. The network administrator can view status and statistics on a per-client basis, to help in network monitoring and troubleshooting.

Client Profiles

A profile is a set of characteristics that can be distinctly assigned to one or more clients. You can manage a large number of clients efficiently by creating a profile with a specific set of common characteristics and assigning it to all users who share these characteristics. For example, all users in the same department could share a common profile. When a parameter in the profile is changed by the network administrator, this change is made automatically by the P-7500 system to all clients using this profile.

There is one default profile, which must be named default, and it is assigned automatically to each client. The default profile cannot be deleted from the P-7500 system.

Rendezvous Service Provisioning Tasks

To configure Rendezvous service on the TIBCO Messaging Appliance P-7500 system:

1. Enter the rv Global CONFIG command:

```
tibco(config-rv)#
```

   Entering the rv Global CONFIG command moves you to the Rendezvous CONFIG level within the CLI for configuring Rendezvous service parameters.

2. (Optional) If not using the default listen port (Port 7500), specify the TCP port number that Rendezvous clients use for Rendezvous services when connecting to the P-7500 system:

```
tibco(config-rv)# listen-port port [backup]
```

   For more information, refer to listen-port on page 27.

3. (Optional) Configure mappings from the network parameter passed in the client initialization handshake to a new network parameter that is to be associated with the client instead:

```
tibco(config-rv)# network-mapping from-network to-network
```

   For example:

```
tibco(config-rv)# network-mapping ;239.1.1.1 ;239.1.1.2

tibco(config-rv)# show rv network-mapping
Original network    Mapped network
---------------------- ------------------------
;225.9.9.9             ;225.10.10.10
;239.1.1.1             ;239.1.1.2
```

   For more information, refer to network-mapping on page 27.

4. (Optional) Configure mappings from the service parameter passed in the client initialization handshake to an actual integral service port number that is used to uniquely identify the service in the P-7500 system:

```
tibco(config-rv)# service-mapping service-name service-port
```

   For example:

```
tibco(config-rv)# service-mapping http 80

tibco(config-rv)# show rv service-mapping
Original service      Mapped service
----------------------  ------------------------
equities                 7800
```

   For more information, refer to service-mapping on page 28.

5. Leave this command level, and go to the Global CONFIG command level:

```
tibco(config-rv)# exit
```

6. An RV Interface is required for the RVGD to connect to the P-7500 and to uniquely identify the system to connecting clients. Enter the Virtual Router CONFIG level, and assign the primary virtual router an RV interface:

```
tibco(config)# virtual-router primary
tibco(config-virtual-router)# rv-interface <ip-interface>
```

   where <*ip-interface*> is an ASCII string specifying an ethernet interface port or LAG on the NAB.

7. Leave this command level, and go to the Rendezvous CONFIG command level:

```
tibco(config-virtual-router)# exit
tibco(config)# rv
```

8. By default, Rendezvous Service is disabled (that is, not running) on the P-7500 system. Start the Rendezvous service:

```
tibco(config-rv)# no shutdown
```

   For more information, refer to shutdown on page 28.

You have completed this procedure.

(Optional) To start Rendezvous Gateway services on the TIBCO Messaging Appliance P-7500 system:

NOTICE

NOTICE: Rendezvous clients communicate with the TIBCO Messaging Appliance P-7500 system through the lag1 interface, while the Rendezvous Gateway communicates with other Rendezvous entities in the network through the Ethernet 2 (eth2) interface on the system (once Rendezvous Gateway services are started). To facilitate low latency communications between the Rendezvous Gateway and TIBCO Messaging Appliance P-7500 system, configure the lag1 and eth2 interfaces in the same IP subnet and connect the interfaces to the same Layer 2 network.

1. Enter the VRF IP CONFIG command level:

```
tibco# configure
tibco(config)#ip vrf management
```

2. Configure the primary eth2 interface.

```
tibco(config-ip-vrf)# interface eth2:1
tibco(config-ip-vrf-interface)# ip-address <ip-addr>
```

where <*ip-addr*> is an IP address in CIDR form: n.n.n.n (n is 0-255).

For Example:

```
tibco(config-ip-vrf)# interface eth2:1
tibco(config-ip-vrf-interface)# ip-address 192.168.162.80/19
```

3. Exit the VRF IP CONFIG command level, then move to the Rendezvous CONFIG level to start the Rendezvous service:

```
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# exit
tibco(config-ip)# exit
tibco(config)# rv
tibco(config-rv)# no shutdown
```

4. Start Rendezvous Gateway services:

```
tibco(config-rv)# gateway
tibco(config-rv-gateway)# no shutdown
```

For more information, refer to gateway on page 26.

You have completed this procedure.

Configuring Rendezvous Services

To configure TIBCO Rendezvous services on a P-7500 system, enter the rv Global CONFIG command:

```
tibco (config)# rv
```

Entering the rv Global CONFIG command moves you to the Rendezvous CONFIG level within the CLI for configuring Rendezvous service parameters:

```
tibco (config-rv)#
```

From here you can configure the P-7500 system for Rendezvous service using these Rendezvous CONFIG commands:

- gateway on page 26
- listen-port on page 27
- network-mapping on page 27
- service-mapping on page 28
- shutdown on page 28

gateway

To configure Rendezvous Gateway services, enter the gateway Rendezvous CONFIG command:

```
tibco# configure
tibco(config)# rv
tibco(config-rv)# gateway
tibco(config-rv-gateway)#
```

The CLI is now at the Rendezvous Gateway CONFIG level for configuring the Rendezvous Gateway on the P-7500 system. From here you can configure the Rendezvous Gateway service parameter shutdown.

shutdown

To stop Rendezvous Gateway services on the P-7500 system, enter the shutdown Rendezvous Gateway CONFIG command:

```
tibco(config-rv)# gateway
tibco(config-rv-gateway)# shutdown
```

By default, Rendezvous Gateway services are disabled (that is, not running) on the P-7500 system. However, Rendezvous Gateway services can still be configured through the TIBCO Rendezvous Gateway Web interface even when disabled. The no version of this command (no shutdown) starts Rendezvous Gateway services on the P-7500 system.

Note: Before entering the no shutdown Rendezvous Gateway CONFIG command, you must:

1. Stop Rendezvous services (if running) through the shutdown Rendezvous CONFIG command.
2. Configure an IP address for the eth2:1 IP interface through the VRF IP CONFIG level.
3. Start Rendezvous services through the no shutdown Rendezvous CONFIG command.

Otherwise, an error message is received.

listen-port

To specify the TCP port number that clients use for Rendezvous services when connecting to the P-7500 system, enter the listen-port Rendezvous CONFIG command:

tibco(config-rv)# listen-port *port* [backup]

Where:

port is the TCP port used by clients for Rendezvous services, specified as a decimal value from 0 to 65,535. Port 7500 is used as the default.

backup configures the specified listen port as the backup (that is, backup virtual router) for the system redundancy model supported by the P-7500 system.

Note: Rendezvous services must be in shutdown state before entering the listen-port Rendezvous CONFIG command, otherwise an error message is received.

network-mapping

To configure mappings from the network parameter passed in the client initialization handshake to a new network parameter that is to be associated with the client instead, enter the network-mapping Rendezvous CONFIG command:

tibco(config-rv)# network-mapping *from-network to-network*

Where:

from-network is the name of the original network parameter

to-network is the name of the new network parameter

Note: When the network-mapping Rendezvous CONFIG command is entered, the new network-mapping will not take affect for clients that are already connected to the network.

If an exact match is found between the original network parameter specified in a mapping and the network string passed in a client's RV initialization handshake, the passed network string is replaced by the new mapped network parameter.

The no version of this command (no network-mapping [*from-network*]) deletes the network mapping.

service-mapping

To configure mappings from the service parameter passed in the client initialization handshake to an actual integral service port number that is used to uniquely identify the service in the P-7500 system, enter the service-mapping Rendezvous CONFIG command:

tibco(config-rv)# service-mapping *original-service mapped-service*

Where:

original-service is the name of the Rendezvous service

mapped-service is the port number for the Rendezvous service, specified as a decimal value from 0 to 65,535.

Note: The no version of this command (no service-mapping [*original-service*]) deletes the service mapping.

shutdown

ALERT! The shutdown Rendezvous CONFIG command causes a disruption in customer service because it disconnects all Rendezvous client connections. Plan to stop Rendezvous services when minimal impact to the Rendezvous clients on

To stop Rendezvous services and disconnect all Rendezvous client connections on the P-7500 system, enter the shutdown Rendezvous CONFIG command:

tibco(config-rv)# shutdown

By default, Rendezvous service is disabled (that is, not running) on the P-7500 system. The `no shutdown` version of this command starts Rendezvous service on the system.

Monitoring Rendezvous Services

You can use several show commands to monitor and validate Rendezvous service configurations and status on TIBCO Messaging Appliance P-7500 systems:

show client

To view the current Rendezvous client information on the P-7500 system, enter the show client User EXEC command:

show client [*ip-and-port*] [service *service-id*] [stats [congestion | queues] | subscriptions | connections [wide]] [primary | backup]

where:

ip-and-port	is the IP address and port or IP address and network mask of the client in Classless Inter-Domain Routing (CIDR) form: *n.n.n.n:x or n.n.n.n/y* (*n* is 0-255, *x* is 1-65535, *y* is 0-32). Entering the wildcard character * in place of the IP address specifies all clients.
service	filters the command output to display system information only for clients associated with the specified *service-id.*
service-id	is the port number or name identifying the service. Entering the wildcard character * in place of a specific client service name specifies all client services.
stats	asks to show client traffic statistics.
congestion	asks to show congestion discards statistics in descending order.
queues	asks to show client queue information.
subscriptions	asks to show client subscription information.
connections	asks to show client TCP connection information.

connections wide	asks to show the client TCP connection information in a widescreen computer display format (300+ character width).
primary	asks to show information only for primary clients.
backup	asks to show information only for backup clients.

Example:

```
tibco> show client 192.168.1.219:35582 stats
Service:           7500
Original Service:  7500
Network:           ;225.0.0.1
Client Address:    192.168.1.219:35582
User:              user1
Description:       sys_overnightS0001
URL:
Uptime:            0d 0h 4m 3s
Identifier:        C0A8A497.4E4C48C53EF681510F8
Version:           8.1.1
Type:              Primary
No Echo:           Disabled
Hidden Client:     No
Profile:           default
Client Id:         0
Subscriptions:     6
Pid:               20044

                              Received                Sent
                          --------------------   --------------------
Rv Control Messages                          0                      0
Rv Data Messages                             0                 242652
Rv Total Messages                            0                 242652

Rv Control Bytes                             0                      0
Rv Data Bytes                                0               45618576
Rv Total Bytes                               0               45618576

                           Ingress (msg/sec)       Egress (msg/sec)
                          --------------------   --------------------
Current Rate (1 sec sample)                  0                   1000
Avg. Rate (60 sec interval)                  0                   1000

************************** Ingress Discards ***************************
   No Subscription Match                                             0
   Subject Parse Error                                               0
   Internal Error                                                    0
   RV Header Parse Error                                             0

************************** Egress Discards ****************************
   Transmit Congestion - Slow Consumer                               0
```

show client-profile

To view the current Rendezvous client profile information on the P-7500 system, enter the show client-profile User EXEC command:

tibco> show client-profile *name*

where *name* is the name of the client profile configured on the system.

Note: Currently, only one profile named default is supported and it is assigned automatically to each client. The default profile cannot be deleted from the P-7500 system.

Example:

```
tibco> show client-profile default
Profile Name : default
  Queue Max Depths
      Egress                  : 100000 work units
  Queue Min Burst
      Egress                  : 4      work units
```

Note: A work unit represents 2048 bytes of a message.

show rv config

To view the Rendezvous configuration information on the P-7500 system, enter the show rv config User EXEC command:

tibco> show rv config

```
RV Configuration Status:          Enabled
RV-Gateway:                       Disabled

                        Primary             Backup
                        ------------------- -------------------
RV Listen Port          7500                7500
RV-Gateway Status       Up                  Up
```

show rv network-mapping

To view the Rendezvous network mapping configuration on the P-7500 system, enter the show rv network-mapping User EXEC command:

tibco> show rv network-mapping

Example:

```
tibco> show rv network-mapping
Original network    Mapped network
```

```
---------------------- ------------------------
;225.9.9.9          ;225.10.10.10
;239.1.1.1          ;239.1.1.2
```

show rv service

To view the Rendezvous service information on the P-7500 system, enter the show rv service User EXEC command:

```
tibco> show rv service service [stats | subscriptions] [primary | backup]
```

where:

service	is the port number or name identifying the Rendezvous service. Entering the wildcard character * in place of a specific Rendezvous service name specifies all Rendezvous services.
stats	asks to show statistics on the Rendezvous service subscriptions.
subscriptions	asks to show Rendezvous service subscription information.
primary	asks to show Rendezvous service information only for clients associated with the primary virtual system.
backup	asks to show Rendezvous service information only for clients associated with the backup virtual system.

Example:

```
tibco> show rv service 9999
Primary Virtual Router (10.10.2.78):
  Service:       9999
  Uptime:        0d 0h 2m 34s
  Clients:       1000
  Subscriptions:  1003

Network                          Clients
-----------------------------------      -------
;224.3.4.5                       1000

Backup Virtual Router (N/A):
```

show rv service-mapping

To view the Rendezvous service mapping configuration on the P-7500 system, enter the show rv service-mapping User EXEC command:

```
tibco> show rv service-mapping
```

Example:

```
tibco(config-rv)# show rv service-mapping
Original service  Mapped service
---------------------- ------------------------
```

```
equities        7800
```

show stats client

To view aggregate Rendezvous client statistics information for all clients on the P-7500 system, enter the show stats client User EXEC command:

```
tibco> show stats client

                                Received                    Sent
                          --------------------   --------------------
RV Control  Messages                       5                      1
RV Data Messages                         125                  79321
RV Total Messages                        130                  79322

RV Control Bytes                        8323                    480
RV Data Bytes                          12540                 807239
RV Total Bytes                         20863                 807719

                           Ingress (msg/sec)       Egress (msg/sec)
                          --------------------   --------------------
Current Rate (1 sec sample)                0                      0
Avg. Rate (60 sec interval)                0                    100


******************** Ingress Discards ***************************
   No Subscription Match                                        0
   Subject Parse Error                                          0
   Internal Error                                             N/A
    RV Header Parse Error                                       0

********************* Egress Discards ***************************
   Transmit Congestion - Slow Consumer                          5
```

To clear the statistics for one or more clients on the P-7500 system, run the clear client stats command from the Privileged EXEC level:

tibco> enable
tibco# clear client *ip-and-port* [service*service*] [primary|backup] stats

where:

ip-and-port	is the IP address and port in the form n.n.n.n:x to clear one client, or IP address and mask combination in the form *n.n.n.n/y* to clear several clients matching the criteria. Entering the wildcard character * in place of the IP address and port or mask specifies clear the statistics for all clients.
service *service*	is the port number or name identifying a Rendezvous subscription service. Omit this parameter to clear client statistics regardless of service.
primary	asks to clear statistics only for primary clients.
backup	asks to clear statistics only for backup clients.

show subscriptions

To view Rendezvous client subscription information on the P-7500 system, enter the show subscriptions User EXEC command:

tibco> show subscriptions [service *service*] [{subject *subject*} | {subject-starts *subject-starts*} | following-seq-num *sequence-num* summary] [count *number*][primary | backup]

where:

service *service*	filters the command output to display subscriptions associated only with the service port number or name specified by *service*. Entering the wildcard character * in place of a specific Rendezvous client subscription service name specifies all Rendezvous subscription services.
subject *subject*	asks to show Rendezvous client subscription subject information where *subject* is the subscription subject in the form a.b.c
subject-starts *subject-starts*	asks to show all Rendezvous client subscription subjects that start with the string specified in *subject-starts*.
following-seq-num *sequence-num*	asks to show subscriptions starting from the sequence number specified by *sequence-num*. Can be used in combination with count to iterate over a large number of subscriptions. If you set *sequence-num* to -1, all subscriptions are displayed. -1 is the default.
summary	asks to show the number of Rendezvous client subscriptions for each client.
count *number*	asks to show a certain number of Rendezvous client subscriptions. If you set *number* to -1, all subscriptions are displayed. -1 is the default.
primary	asks to show information only for primary clients.
backup	asks to show information only for backup clients.

If either count or following-seq-num are specified, subscriptions are listed in sequence number order and the sequence numbers are displayed. Otherwise the sequence numbers are not displayed and subscriptions are listed in service/IP address order.

To clear the service-level statistics for one or more Rendezvous subscription services on the P-7500 system, run the clear rv service stats command from the Privileged EXEC level:

```
tibco> enable
tibco# clear rv service service stats [primary|backup]
```

where:

service *service*	is the port number or name identifying the Rendezvous subscription service. Entering the wildcard character * in place of the port number or name asks to clear the service-level statistics for all Rendezvous subscription services.
primary	asks to clear service-level statistics only for primary clients.
backup	asks to clear service-level statistics only for backup clients.

Chapter 3 Managing Access Control Lists

TIBCO provides basic traffic filtering capabilities through the Access Control List (ACL) feature as part of a security solution to prevent certain traffic from entering or exiting a network. You can configure ACLs on your TIBCO Messaging Appliance P-7500 system to control access to a network.

The ACL feature provides the following controls:

- Connection controls – prevents clients from being able to connect to the router.
- Subject-based publisher controls – restricts what subjects clients are allowed to publish on.
- Subject-based subscription controls – restricts what subjects clients are allowed to subscribe to.

Note: The ACL feature is by default locked, and can only be unlocked through a product key provided by TIBCO. It must be unlocked through the product-key Admin EXEC command to have any effect on the system. If locked, access controls are unavailable and there are no system restrictions on either connecting or subject-based publishing or subscribing.

Topics

Overview

ACLs filter network traffic by controlling whether a client can connect to a service on the P-7500 system, and if a client is permitted a connection, what routed messages are forwarded or blocked at the P-7500 system interfaces.

When creating an ACL, you define criteria which are applied to each message or subscription that is processed by the P-7500 system; the system then decides whether to forward or block each message or subscription based on whether or not the message or subscription matches the criteria. If the message is denied, the software discards the message.

Your P-7500 system examines each message to determine whether to forward it or drop it based on the criteria you specify within the ACL configuration through the client connection access controls and subject access controls described on page 38 and page 39, respectively.

Product Key Feature Locking

The product key may be used to enable ACLs on any P-7500 system. If a product key is removed, then a system restart is triggered and all configuration related to the features unlocked by that key is lost.

When the ACL feature is locked, no aspect of it is configurable or displayable. The CLI commands relating to the feature are still visible in the P-7500 CLI, but when run, they fail and return an applicable error message indicating the feature is locked, and take no further action.

Client Connection Access Controls

Client connection access control enables you to choose which clients are allowed to connect to the P-7500 system.

The default setting for a client connection attempt can either be Allow or Disallow. When the default action is set to Allow, there are no restrictions on a client connection attempt. When it is set to Disallow, a client attempting to connect is immediately disconnected from the P-7500 system.

After you have set the default client connection action, you can create a list of clients that you want to act as exceptions to the default action. For example, if the default client connection action is Allow, when a client on the Exceptions list attempts to connect to the P-7500 system, the client is immediately disconnected from the P-7500 system. If the default client connection action is Disallow, the client on the Exceptions list is connected with no restrictions.

Changing the default client connect action, or removing clients from the Exceptions list, does not affect clients that already have an established connection to the P-7500 system. They remain connected.

Exceptions to the default action are configured as a list of ip/mask pairs expressed in CIDR form. Any client whose address falls into any of the ip/mask in this list gets the opposite behavior to the configured default action. There is a limit of 250 exceptions supported.

A global statistic is incremented for every denied connection attempt. In addition, a circular log is also maintained capturing:

- the current timestamp
- the ip/port of the denied client
- the username of the denied client
- the reason the client connection was denied

Changing the setting of client-connect from *allow* to *disallow* or changing the exception list has no effect on already connected clients, they remain connected. The initial value for action is *disallow*.

Subject Access Controls and ACL Profiles

Each client is associated with a single named ACL profile which determines what subject-based access controls are imposed on it. There can be up to 6000 ACL profiles created, including the preconfigured ACL profile named "default". Names must be unique across all ACL profiles. The rules governing what subjects a client can publish and subscribe to are applied when a client is mapped to an ACL profile through the profile-mapping CONFIG command.

Clients that are are not mapped to specific ACL profiles are denied access to the P-7500 system when the ACL feature is unlocked through the product key.

The profile mapping assigns a client to an ACL profile according to their username and service. The username and service can either be explicitly specified in the profile mapping, or left unspecified, thereby implying the mapping applies to any username or service. If either the username or service are not specified in the profile mapping, then the system maps clients to an ACL profile and prioritizes them according to the most restrictive and applicable mapping rule. The mapping rules in order of priority are:

1. "exact username and exact service"
2. "exact username any service"
3. "any username exact service"
4. "any username any service"

For example, consider the following set of ACL profile mappings:

Username	Service	Profile
Bob	Unspecified	profile1
Unspecified	6000	profile2
Bob	7000	profile3
Unspecified	Unspecified	profile4

The following clients connecting with the above parameters are prioritized and mapped as follows to the ACL profiles, in accordance with the most restrictive and applicable mapping rule:

Username	Service	Profile	Mapping Rule
Bob	7000	profile3	1. "exact username and exact service"
Bob	4444	profile1	2. "exact username any service"
Mary	6000	profile2	3. "any username exact service"
Hans	1234	profile4	4. "any username any service"

When you create an ACL profile, you can configure whether you want the default action to be to allow or disallow clients assigned to the ACL profile from publishing on or subscribing to subjects. You can also list specific subjects that you want to be excepted from the default action. Through ACL profiles, subject access controls enable you to specify which subjects clients are permitted to publish on and subscribe to.

Subscriptions are either fully accepted or completely rejected depending on whether they match the configured subject access controls. Special rules are employed when handling subscriptions containing wildcards to ensure configured ACLs are effective in blocking the traffic they have been configured to disallow.

Wildcard subscriptions that match an ACL profile's exceptions are disallowed if the ACL profile's default rule is to allow all subscriptions. For example, if an ACL profile has been configured to allow all subscriptions except FRUIT.APPLES, a subscription to FRUIT.> (covering FRUIT.APPLES) is disallowed. If FRUIT.> were accepted, then messages published to FRUIT.APPLES would match FRUIT.> and be delivered to the client. This would contradict the intention of the ACL.

If the ACL profile's default rule disallows all subscriptions, wildcard characters in the subscription are not given any special treatment when establishing matching exception rules. For example, if an ACL profile has been configured to disallow all subscriptions except FRUIT.BANANAS, a subscription request to FRUIT.> would be disallowed given that the '>' would not be treated as a wildcard character and therefore not cover the exception rule of FRUIT.BANANA. In suppressing the subscription, which requested everything below FRUIT, the ACL profile's intention of only allowing access to FRUIT.BANANA is enforced.

There is no limit to the number of publishing or subscription subject exceptions per ACL profile. However, there is a maximum of 10,000 subject exceptions (publish and subscribe combined) allowed amongst all profiles. Also keep in mind that the more exceptions you have, the more difficult it is to comprehend and manage your subject access control configuration.

Each P-7500 system has a preconfigured ACL profile named "default". The initial configuration of the "default" ACL profile is:

- allow for publish-subject, with no exceptions.
- allow for subscribe-subject, with no exceptions.

Although you can modify the configuration of the "default" ACL profile, it cannot be deleted.

If you change the default action for an ACL profile, any existing subjects that are listed as exceptions are maintained as exceptions, but their behavior becomes the opposite of what it was.

A global statistic is incremented for every denied publish or subscribe subject attempt. In addition, a circular log is also maintained capturing:

- the current timestamp
- the username of the denied client
- the subject that was denied
- the ACL profile name that triggered the denial (shown only when the wide parameter option is entered with the `show log acl` User EXEC command)

Configuring Access Control Lists

There are many reasons to configure ACLs:

- restrict subjects that a client can subscribe to
- restrict subjects that a client can publish on
- restrict which clients are allowed to connect to your network
- provide security for your network

Use of ACLs to provide a basic level of security for accessing your network is recommended. If you do not configure ACLs on your system clients can connect from any host and all messages being published into your network could be received by all clients connecting to your network.

Access Control List Configuration Commands

This section describes the commands you use to specify settings and configuration for the ACL facility.

product-key

When no product key is enabled, only the default features of the P-7500 system are available. To enable a product key on a system to unlock extra feature content such as ACLs, enter the product-key Admin EXEC command:

```
tibco# admin
tibco(admin)# product-key key-value
```

Where:

key-value is the product key provided by TIBCO. Product keys can contain up to 40 alphanumeric characters, and are specific for the P-7500 system and set of features they unlock. If the provided key value does not match the P-7500 system, then there is no effect.

The no version of this command (no product-key *key-value*) removes the named product key and restarts the P-7500 system.

profile-mapping

The Profile Mapping CONFIG level allows you to associate the username and mapped service of a client to a configured ACL profile. You reach this level by entering:

```
tibco(config)# create profile-mapping {[username name] [service mapped-service] | default}
```

Or

tibco(config)# profile-mapping {[username *name*] [service *mapped-service*] | default}

Where:

The create version of the command creates a profile mapping for a username and a mapped service that did not already exist.

name is the username of the client. User names ids are case sensitive. If the username parameter is unspecified, the profile mapping applies to any username.

mapped-service is the Rendezvous Service, specified as a decimal value from 0 to 65,535. If the service parameter is left unspecified, the profile mapping applies to any service.

default asks to map all usernames and mapped services to the profile mapping

The no version of the command removes the named profile mapping from the P-7500 system.

acl-profile

To assign a client's configured ACL profile to the profile mapping, enter the acl-profile Profile Mapping CONFIG command:

tibco(config-profile-mapping)# acl-profile *name*

Where:

name is the name of the specified ACL profile.

The no version of this command (no acl-profile) deletes the ACL profile from the profile mapping.

acl client-connect

To configure client connection access control parameters default-action and exception for the TIBCO Messaging Appliance P-7500 system, enter the client-connect Access Control List CONFIG command:

tibco(config)# acl client-connect

Entering the client-connect Access Control List CONFIG command moves you to the ACL Client Connect CONFIG level:

tibco(config-acl-cc)#

default-action

To set the default action for client connection access attempts, enter the default-action ACL Client Connect CONFIG command:

```
tibco(config-acl-cc)# default-action {allow | disallow}
```

Where:

allow configures the client connection access to allow connections

disallow configures the client connection access to block connections (system default)

exception

To set the exceptions to the default action for client connection access attempts, enter the exception ACL Client Connect CONFIG command:

```
tibco(config-acl-cc)# exception cidr-addr
```

Where:

cidr-addr is the IP address and network mask combination of the excepted client in Classless Inter-Domain Routing (CIDR) form: nnn.nnn.nnn.nnn/dd (where nnn is 0-255, dd is 0-32)

acl profile

To configure ACL client profiles for publishing and subscription subject access control on the TIBCO Messaging Appliance P-7500 system, enter the profile Access Control List CONFIG command:

```
tibco(config)# acl
tibco(config-acl)# create profile name
```

Or

```
tibco(config-acl)#  profile name
```

Where:

The create version of the command creates a new ACL profile that did not already exist.

name is the name of the specified ACL profile.

The no version of this command (no profile *name*) deletes the specified ACL profile from the P-7500 system.

Entering the profile Access Control List CONFIG command moves you to the ACL Profile CONFIG level within the CLI for configuring publishing and subscription subject access control parameters:

```
tibco(config-acl-profile)#
```

acl profile publish-subject

To configure the publishing subject access control parameters default-action and exception for ACL profiles, enter the publish-subject ACL Profile CONFIG command:

```
tibco(config-acl-profle)# publish-subject
```

Entering the publish-subject ACL Profile CONFIG command moves you to the ACL Profile Publish Subject CONFIG level:

```
tibco(config-acl-profile-publish-subject)#
```

default-action

To set the default action for publishing subject access attempts, enter the default-action ACL Profile Publish Subject CONFIG command:

```
tibco(config-acl-profile-publish-subject)# default-action {allow | disallow}
```

Where:

allow configures the publishing subject access to allow the publishing of subjects (system default)

disallow configures the publishing subject access to block the publishing of subjects

exception

To set the exceptions to the default action for publishing subject access attempts, enter the exception ACL Profile Publish Subject CONFIG command:

```
tibco(config-acl-profile-publish-subject)# exception subject
```

Where:

subject is the name of the publishing subject to be excepted in the form a.b.c

acl profile subscribe-subject

To configure the subscription subject access control parameters default-action and exception for ACL profiles, enter the publish-subject ACL Profile CONFIG command:

```
tibco(config-acl-profle)# subscribe-subject
```

Entering the subscribe-subject ACL Profile CONFIG command moves you to the ACL Profile Subscribe Subject CONFIG level:

```
tibco(config-acl-profile-subscribe-subject)#
```

default-action

To set the default action for subscription subject access attempts, enter the default-action ACL Profile Subscribe Subject CONFIG command:

```
tibco(config-acl-profile-subscribe-subject)# default-action {allow | disallow}
```

Where:

allow configures the subscription subject access to allow the subscribing to subjects (system default)

disallow configures the subscription subject access to block the subscribing to subjects

exception

To set the exceptions to the default action for subscription subject access attempts, enter the exception ACL Profile Subscribe Subject CONFIG command:

```
tibco(config-acl-profile-subscribe-subject)# exception subject
```

Where:

subject is the name of the subscription subject to be excepted in the form a.b.c

Steps to Configure Access Control Lists

To configure ACLs on your P-7500 system, use the following basic procedures. The exact steps required may vary depending on your network conditions and preferred configuration.

Before attempting to configure the ACL feature, verify that it is unlocked by entering the show product-key User EXEC command. If locked, enter the product-key ADMIN Exec command to unlock the ACL feature:

```
tibco(admin)# product-key key-value
```

For more information, refer to “product-key” on page 43.

The following example configures ACLs such that:

- Clients on IP subnet 10.10.0.0/16 cannot connect; clients connecting from other IP subnets are allowed
- Clients on service 7000 cannot publish to the subject “FRUIT.BANANAS”; all other subjects are allowed.
- Clients on service 7000 cannot subscribe to the subject “FRUIT.APPLES”; all other subjects are allowed.

Controlling Which Clients Can Connect to the P-7500 System

To control which clients can connect to the P-7500 system:

1. Enter the client-connect Access Control List CONFIG command:

```
tibco(config)# acl client-connect
tibco(config-acl-cc)#
```

2. Set the default action for client connection access attempts:

```
tibco(config-acl-cc)# default-action allow
```

3. Set exceptions to the default action for client connection access attempts:

```
tibco(config-acl-cc)# default-action exception 10.10.0.0/16
```

For more information, refer to “acl client-connect” on page 44.

4. Validate the client-connect ACL rule is correct by entering the show acl client-connect User Exec command. The output should be similar to this:

```
tibco(config-acl-cc)# show acl client-connect

Client Connect Default Action : allow
 Exceptions : 1
  10.10.0.0/16
```

You have completed this procedure.

Controlling Which Subjects a Client May Publish and Subscribe To

To control which subjects a client on the P-7500 system may publish and subscribe to, on a client by client basis:

1. Create an ACL profile:

```
tibco(config)# create acl profile fruit
tibco(config-acl-profile)#
```

For more information, refer to “acl profile” on page 45.

2. Set the default action for publishing subject attempts:

```
tibco(config-acl-profile)# publish-subject
tibco(config-acl-profile-publish-subject)# default-action allow
```

3. Set exceptions to the default action for publishing subject attempts:

```
tibco(config-acl-profile-publish-subject)# exception FRUIT.BANANAS
```

For more information, refer to “acl profile publish-subject” on page 46.

4. Set the default action for subscription subject attempts:

```
tibco(config-acl-profile)# subscribe-subject
tibco(config-acl-profile-subscribe-subject)# default-action allow
```

5. Set exceptions to the default action for subscription subject attempts:

```
tibco(config-acl-profile-subscribe-subject)# exception FRUIT.APPLES
```

For more information, refer to “acl profile subscribe-subject” on page 46.

6. Validate the ACL profile is correct by entering the show acl profile User Exec command. The output should be similar to this:

```
tibco(config-acl-profile)# show acl profile fruit

Profile Name : fruit
 Publish Subject Default Action   : allow
   Exceptions : 1
     FRUIT.BANANAS
 Subscribe Subject Default Action   : allow
   Exceptions : 1
     FRUIT.APPLES
```

For more information, refer to “show acl profile” on page 51.

7. Create a profile map for the clients. In this example, the profile map applies to all usernames in the service (thus the username parameter is left unspecified to mean "any username"):

```
tibco(config)# create profile-mapping service 7000
```

8. Assign the ACL profile to the profile map:

```
tibco(config-profile-mapping)# acl-profile fruit
```

For more information, refer to “profile-mapping” on page 43.

9. Validate the profile mapping is correct by entering the show profile-mapping User Exec command.

```
(config-profile-mapping)# show profile-mapping

Username :
Service :
 ACL Profile :  default

Username :
Service :       7000
 ACL Profile :  fruit
```

You have completed this procedure.

Monitoring Access Control

You can use several show commands to monitor access control configuration and status.

show product-key

To view the system product keys and features that they unlock, enter the show product-key User EXEC command:

```
tibco> show product-key
```

Example:

```
tibco> show product-key

Product Key : LLLLLLLLLLL-LLLLLLLLLLL-LLLLLLLLLLL-HHHH
 Unlocked Features : 1
  Access Control Lists (ACLs)
```

show profile-mapping

To view the configuration of mapping profiles on the P-7500 system, enter the show profile-mapping User EXEC command:

```
tibco> show  profile-mapping [username <name>] [service <mapped-service>] [default]*
```

Where:

name is the user name of the client. User names are case sensitive.

mapped-service is the Rendezvous Service, specified as a decimal value from 0 to 65,535.

default asks to the profile mapping named default

Entering no username or service displays all profile mappings.

Example:

```
tibco> show profile-mapping

Username :
Service :
 ACL Profile :  default

Username :      bob
Service :
 ACL Profile :  default
```

show acl client-connect

To view the current client connection control access configuration, enter the show acl client-connect User EXEC command:

```
tibco> show acl client-connect
```

Example:

```
tibco> show acl client-connect

Client Connect Default Action : allow
  Exceptions : 3
    123.123.123.123/32
    123.123.123.0/24
    123.123.122.0/24
```

show acl profile

To view the current ACL profile configurations, enter the show acl profile User EXEC command:

```
tibco> show acl profile name [detail]
```

Where:

name is the name of the specified ACL profile. Entering the wildcard character * for the name displays all ACL profiles.

detail asks to show detailed ACL profile information

Examples:

```
tibco> show acl profile *

                                 Publish          Subscribe
Profile Name                   Allow/#Except    Allow/#Except
-------------------------------------------------------------------------------------------
another-acl-profile-name          yes / 1          yes / 0
default                          no / 0           no / 1
other-acl-profile-name           yes / 2          no / 2
some-acl-profile-name            yes / 1          yes / 123


tibco> show acl profile other-acl-profile-name

Profile Name : other-acl-profile-name
  Publish Subject Default Action   : allow
    Exceptions : 2
      a.specific.subject.that.is.not.allowed
      a.wildcard.subject.that.is.not.allowed.>
  Subscribe Subject Default Action : disallow
    Exceptions : 2
      a.specific.subject.that.is.allowed
      a.wildcard.subject.that.is.allowed.>
```

show log acl

To view the ACL log for the last 1000 most recent service denials regarding client connections, publishing subjects, or subscription subjects, enter the show log acl User EXEC command:

```
tibco> show log acl [client-connect | publish-subject | subscribe-subject] [wide]
```

Where:

client-connect asks to show service denial logs relating only to client connection ACLs

publish-subject asks to show service denial logs relating only to publishing subject ACLs

subscribe-subject asks to show service denial logs relating only to subscription subject ACLs

wide asks to show ACL log information in a wide screen computer display format (300+ character width)

Note: Entering no command parameters displays service denial log information for all ACLs.

Examples:

```
tibco> show log acl client-connect wide

Most recent ACL client-connect denials (max 1000):
Timestamp                 Client                    Username
-------------------------------------------------------------------------------
2008-07-29T16:50:46-0400 123.123.456.456:12345   johndoe
2008-07-29T16:50:48-0400 123.123.456.456:21345   johndoe
2008-07-29T16:50:50-0400 123.123.456.456:32245   janedoe
2008-07-29T16:50:52-0400 123.123.456.456:42335   janedoe


tibco> show log acl publish-subject

Most recent ACL publish-subject denials (max 1000):
Timestamp                 Username            Subject
2008-07-29T16:50:46-0400 johndoe123456789$ a100.b100.c100.d100.e100.f100.g100.$
2008-07-29T16:50:48-0400 johndoe            a100.b100
2008-07-29T16:50:50-0400 janedoe            b100.c100
2008-07-29T16:50:52-0400 fallguy            d100.e100
```

To clear the global statistics information on ACLs, run the clear stats acl command from the Privileged EXEC level:

```
tibco> enable
tibco# clear stats acl
```

To clear the ACL log either globally, or individually for client connections, publishing subjects, or subscription subjects, run the clear log acl command from the Privileged EXEC level:

```
tibco> enable
tibco# clear log acl [client-connect | publish-subject | subscribe-subject]
```

Where:

client-connect asks to clear service denial logs relating only to client connection ACLs

publish-subject asks to clear service denial logs relating only to publishing subject ACLs

subscribe-subject asks to clear service denial logs relating only to subscription subject ACLs

Note: Entering no command parameters clears service denial log information for all ACLs.

show stats acl

To view global statistics information on ACLs, enter the show stats acl User EXEC command:

```
tibco> show stats acl
```

Example:

```
tibco> show stats acl

Reason                  # Denials
-------------------------------------------------------------------------
Client Connect          123
Publish Subject         987
Subscribe Subject       456
```

To clear the global statistics information on ACLs, run the clear stats acl command from the Privileged EXEC level:

```
tibco> enable
tibco# clear stats acl
```

Chapter 4 Configuring Access Control Lists Using the Browser Administration Interface

You can use the Browser Administration Interface to manage client access to the TIBCO Messaging Appliance P-7500 system, as well as which subjects they are permitted to publish and subscribe to.

The ACL feature is by default locked, and can only be unlocked through a product key provided by TIBCO. If locked, all access controls are shared, and there are no restrictions on client connections, publishing, or subscription. Refer to Chapter 3, Managing Access Control Lists for more information.

Topics

Configuring Client Connections

The Client Connection Information page of the Browser Administration Interface enables you to set which clients are allowed to connect to the P-7500 system.

The default setting for a client connection attempt can either be Allow or Disallow. When the default action is set to Allow, there are no restrictions on a client connection attempt. When it is set to Disallow, a client attempting to connect is immediately disconnected from the P-7500 system.

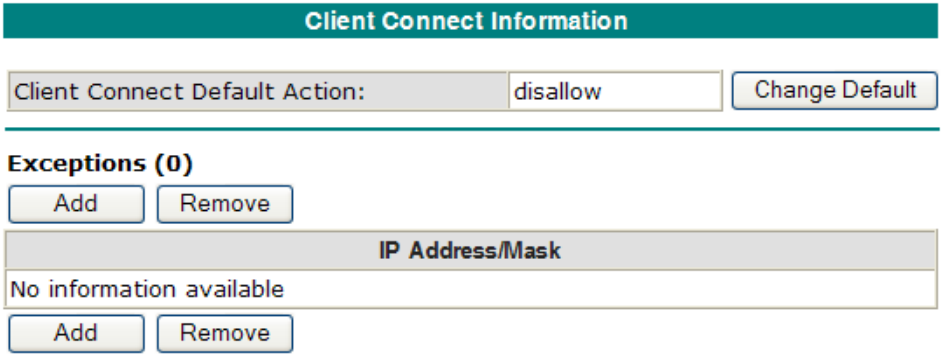
After you have set the default client connection action, you can create a list of clients that you want to act as exceptions to the default action. For example, if the default client connection action is Allow, when a client on the Exceptions list attempts to connect to the P-7500 system the client is immediately disconnected from the P-7500 system, or if the default client connection action is Disallow, the client is connected with no restrictions.

Changing the default client connect action, or removing clients from the Exceptions list, does not affect clients that already have an established connection to the P-7500 system. They remain connected.

Configuring Default Client Connection Access and Exceptions

To configure the default client connection action, and any exceptions to that default:

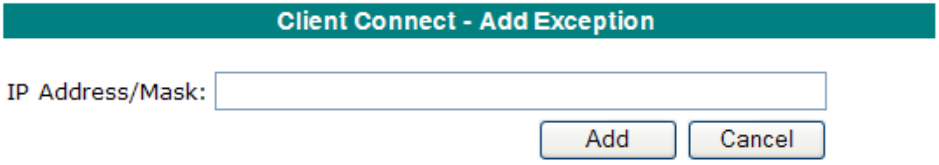
1. Click **Client Connect** in the left margin of the Browser Administration Interface.
2. The Client Connect Information page appears, and the current client connect default action is listed in the Client Connect Default Action field. If you want to change the current client connect default action, click **Change Default**.



The new default action now appears in the Client Connect Default Action field.

If the default client connection action is changed, any clients that are listed as exceptions are maintained as exceptions, but their connection behavior becomes the opposite of what it was.

3. If you want a client to be excepted from the client connect default action, click **Add**.
4. The Client Connect - Add Exception page appears. In the **IP Address/Mask** box, type the IP address and network mask of the client in Classless Inter-Domain Routing (CIDR) form: n.n.n.n/x (where n is 0-255, x is 1-32), and click **Add**.



The IP address for the client appears in the Exceptions list.

5. If you want to remove a client from the Exceptions list, select the check box beside the client's IP address, and click **Remove**.

You have completed this procedure.

Configuring ACL Profiles

You can use the Browser Administration Interface to configure ACL profiles for clients. ACL profiles specify which subjects clients are permitted to publish on and subscribe to.

Clients that are are not mapped to specific ACL profiles are denied access to the P-7500 system when the ACL feature is unlocked through the product key.

When you create an ACL profile, you can configure whether you want the default action to be to allow or disallow clients assigned to the ACL profile from publishing on or subscribing to subjects. You can also list specific subjects that you want to be excepted from the default action.

The rules governing what subjects a client can publish and subscribe to are applied when the ACL profile is mapped to the client. See “Configuring Username Service Mappings” on page 62.

Each P-7500 system has a preconfigured ACL profile named "default". The initial configuration of the "default" ACL profile is:

- allow for publish-subject, with no exceptions.
- allow for subscribe-subject, with no exceptions.

Although you can modify the configuration of the "default" ACL profile, it cannot be deleted.

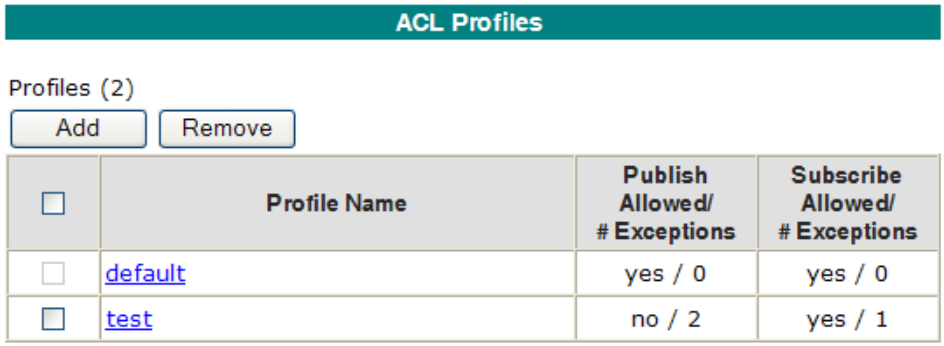
If you change the default action for a custom ACL profile, any existing subjects that are listed as exceptions are maintained as exceptions, but their behavior becomes the opposite of what it was.

Adding ACL Profiles

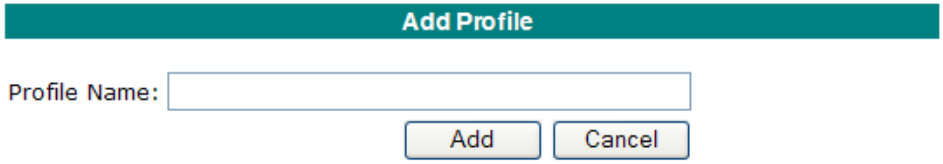
To add ACL profiles:

1. Click **ACL Profiles** in the left margin of the Browser Administration Interface.

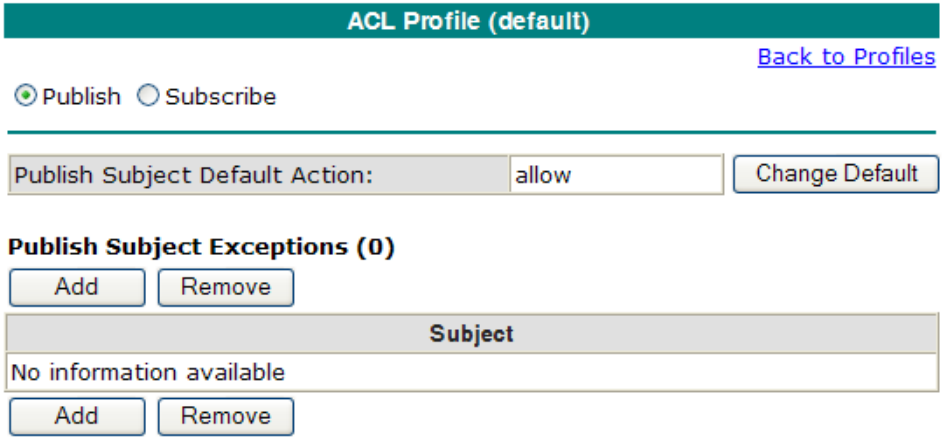
2. The ACL Profiles page appears. Click **Add**.



3. The Add Profile page appears. Type a name for the ACL profile in the **Profile Name** box, and click **Add**.



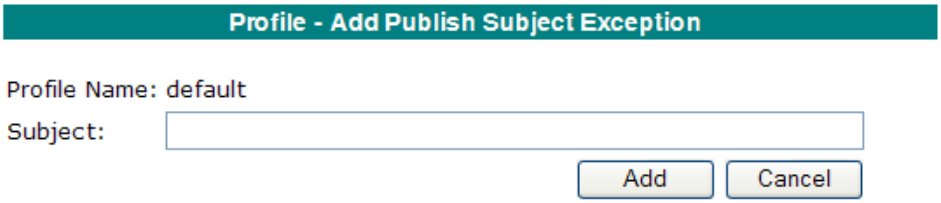
4. The new ACL profile is listed in the ACL Profiles page. In the **Profile Name** column, click the ACL profile.
5. The ACL Profile page for the new ACL profile appears. Click **Publish** to configure the ACL profile for publishing subjects.



6. The current default action is listed in the Publish Subject Default Action field. To configure the default action for publishing subjects, click **Change Default**. The following default actions are possible:

Default Action	Description
Allow	Allow clients that use this ACL profile to publish subjects.
Disallow	Deny clients that use this ACL profile from publishing subjects.

7. If you want a subject to be excepted from the default publish action, click **Add**.
8. The Profile - Add Publish Subject Exception page appears. Type a name for the subject exception in the **Subject** box, and click **Add**.



9. The ACL Profile page for the current ACL profile appears. Click **Subscribe** to configure the ACL profile for subscribing to subjects.
10. The current default action is listed in the Subscribe Subject Default Action field. To configure the default action for subscribing to subjects, click **Change Default**. The following default actions are possible:

Default Action	Description
Allow	Allow clients that use this ACL profile to subscribe to subjects.
Disallow	Deny clients that use this ACL profile from subscribing to subjects.

11. If you want a subject to be excepted from the default subscribe subject action, click **Add**.
12. The Profile - Add Subscribe Subject Exception page appears. Type a name for the publish exception in the **Subject** box, and click **Add**.

13. The ACL Profile page for the current ACL profile appears. The ACL profile is now configured for both publishing on and subscribing to subjects. Click **Back to Profiles** to return to the ACL Profiles page.

    You have completed this procedure.

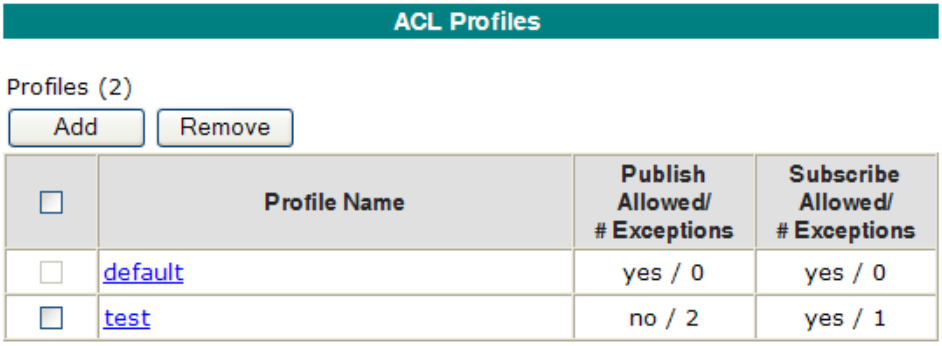
Removing ACL Profiles

You can use the Browser Administration Interface to remove any ACL profile except the default.

When an ACL profile is removed, any username service mappings for the ACL profile are assigned to the default ACL profile. If a connected client mapped to the profile that is removed, the client's connection is maintained, but the publish and subscribe permissions for the default ACL profile are immediately applied to the client.

To remove ACL profiles, follow these steps.

1. Click **ACL Profiles** in the left margin of the Browser Administration Interface.
2. The ACL Profiles page appears. Select the check box beside the ACL profile you want to remove, and click **Remove**.



3. A confirmation dialog box appears. Click **OK** to remove the ACL profile.

    You have completed this procedure.

Configuring Username Service Mappings

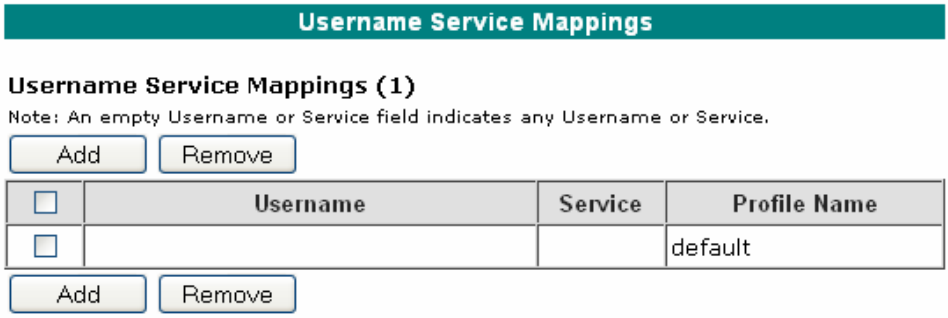
You can use the Browser Administration Interface to map a client's username and the network service that it uses with a specific ACL profile.

All clients must be mapped to an ACL profile to establish a connection to the p-7500 system.

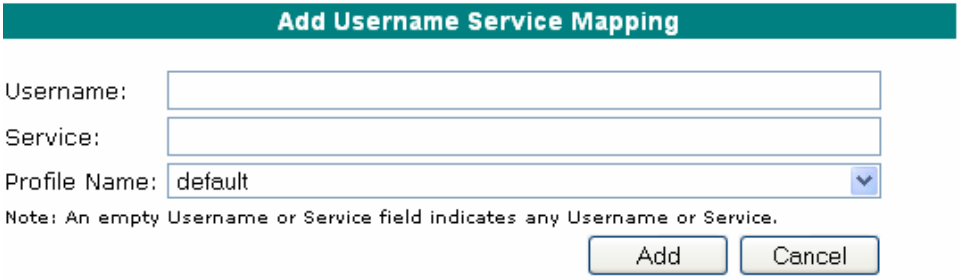
Configuring Username Service Mappings

To map clients' usernames and the network services that they use with specific ACL profiles:

1. Click **Username Service Mappings** in the left margin of the Browser Administration Interface.
2. The Username Service Mappings page appears. Click **Add**.



3. The Add Username Service Mapping page appears. In the **Username** box, type the client username, or leave the field empty to indicate all client usernames.



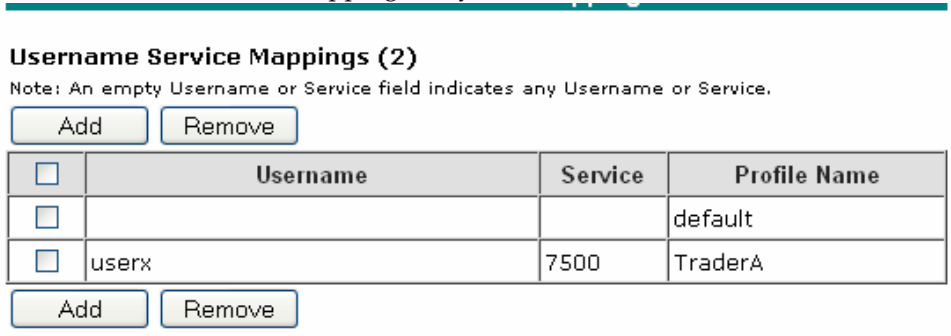
4. In the **Service** box, type the Rendezvous Service used by the client (valid range is 0 to 65535), or leave the field empty to indicate all mapped network services.
5. From the **Profile Name** list, select an ACL profile.
6. Click **Add**.

You have completed this procedure.

Removing Username Mappings

To remove existing username mappings:

1. Click **Username Service Mappings** in the left margin of the Browser Administration Interface.
2. The Username Service Mappings page appears. Select the check box beside the username service mapping that you want to remove, and click **Remove**.



The username is removed from the Username Service Mappings list.

You have completed this procedure.

Subject String Syntax

The TIBCO Messaging Appliance P-7500 system supports the use of subjects for both publishing and subscribing.

Subject strings are NULL-terminated UTF-8 strings where the string of characters is composed of one or more levels (also called elements), separated by a "." delimiter, in the format "a.b.c".

The maximum total character length of subjects (including dot separators) is 196 characters. The maximum element length is 127 characters.

All characters except the NULL character are valid within a subject string, although '_', '*', and '>' have special semantics to the P-7500 system. Refer to Table 5. Characters in subject strings are case sensitive.

Characters with Special Semantics

Table 5 Characters with Special Semantics

Character	Character Name	Special Meaning
_	Underscore	Subject names beginning with underscore are reserved. It is illegal for applications to send to subjects with underscore as the first character of the first element, except _INBOX and _LOCAL. It is legal to use underscore elsewhere in subject names.
.	Dot	Separates elements within a subject name. It is illegal to incorporate the dot character into an element by using an escape sequence.
>	Greater Than	Wildcard element: Matches one or more trailing elements.
*	Asterisk	Wildcard character: Matches one element.

Chapter 5 Managing System Operations Using SEMP

This chapter describes the SEMP Request Over HTTP transport service.

SEMP is a request/response protocol which includes:

- An XML schema which identifies all managed objects available in the router. Any object available through CLI is also available through SEMP
- A simple request/reply paradigm for sending XML-encoded requests to the router, and receiving an XML-encoded response

The SEMP interface is used by application software to manage and monitor a P-7500 system. This interface consists of commands and replies in XML format that are wrapped in HTTP requests and responses and sent over a TCP connection. The commands and replies parallel the commands and replies in the TIBCO Messaging Appliance P-7500 Command Line Interface (CLI).

SEMP Request Over HTTP

A management application uses the SEMP interface to communicate with the P-7500 system as follows:

1. A management application opens a TCP connection to port 80 on the TMA P-7500.
2. The management application then sends HTTP POST messages to issue SEMP commands to the P-7500 system.

   The management application must wait for the reply to each command before issuing the next command.
3. The P-7500 system sends an HTTP response back for each HTTP POST request, containing the SEMP reply.

At this point, the management application can close the connection, or keep the connection open for future HTTP POST requests.

The P-7500 system supports a maximum of 500 concurrent SEMP request over HTTP sessions.

HTTP Request Format

The following is an example of an HTTP request from a management application to issue a SEMP command to the P-7500 system:

```
POST /SEMP HTTP/1.1
Authorization: Basic <usernameAndPassword>
Content-Length:<length>
<SEMP command>
```

Where:

`<usernameAndPassword>` is the username and password for the user. The username and password must be encoded as described in RFC 2617: Section 2: Basic Authentication Scheme. Only basic HTTP authentication is supported.

`<length>` indicates the length (in bytes) of the SEMP command that follows the HTTP header

`<SEMP command>` is the contents of the SEMP command being sent (see “SEMP Command Format” on page 67). The application can only send one SEMP command for each HTTP POST request.

HTTP Response Format

The following is an example of a P-7500 system HTTP response to a management application's SEMP command:

```
HTTP/1.1 200 OK
Content-Length: <length>
<SEMP reply>
```

Where:

`<length>` indicates the length (in bytes) of the SEMP reply that follows the HTTP header

`<SEMP reply>` is the contents of the SEMP reply being returned from the router (see "SEMP Reply Format" on page 68)

An HTTP response of "200 OK" is returned if the command was accepted by the P-7500 (even if it was not successfully executed). If there is an authentication failure, the following response is returned:

```
401 Unauthorized
Basic Realm="CLI"
```

Otherwise, a response of "400 ERROR" is returned.

SEMP Command Format

The format of SEMP commands within HTTP POST requests is modeled after the P-7500 system CLI. Each SEMP command is the equivalent of either a single CLI command, or, in some cases, the equivalent of a CLI command to enter into a mode and a single CLI command.

SEMP commands are formatted in XML, following the schema in the **semp-rpc-tma.xsd** file provided with the TIBCO software release bundle. White space (including line-end characters) is optional in the SEMP command. The top-level element is `<rpc>`, and the next-level element corresponds to the command being issued. Inside the `<rpc>` element are the keywords and parameters of the command.

For example:

```
POST HTTP://192.168.1.180:80/SEMP
Authorization: Basic <base64 uname/passwd>

<rpc semp-version='tma/1_1'>
    <show>
        <client>
            <ip-and-port>*</ip-and-port>
        </client>
    </show>
</rpc>
```

SEMP does not provide a concept of command modes. All commands are issued at the top level of the command mode hierarchy. In particular, the enable and configure commands are not required or supported in SEMP.

SEMP Reply Format

The SEMP interface replies indicate the success or failure of a SEMP command, in addition to the reason code for any failure. SEMP replies are formatted in XML, following the schema in the **semp-rpc-reply-tma.xsd** file.

White space, including line-end characters, is optional in the SEMP reply.

The following is an example of a successful reply of the command described in "SEMP Command Format" on page 67:

```
HTTP/1.1 200 OK
Content-Length: 941
Content-Type: text/xml; charset=utf-8
Client-Date: Thu, 24 Mar 2011 15:31:33 GMT
Client-Peer: 192.168.1.180:15150
Client-Response-Num: 1

<rpc-reply semp-version="tma/1_1">
  <rpc>
    <show>
      <client>
        <primary-virtual-router>
          <client>
            <service>1000</service>
            <client-address>192.168.164.129:44427</client-address>
            <user>root</user>
            <description>./tibrvlisten</description>
            <identifier>C0A8A4B6.31C34D6EB5AB89B5A90</identifier>
            <subscriptions>4</subscriptions>
          </client>
        </primary-virtual-router>
      </client>
    </show>
  </rpc>
<execute-result code="ok"/>
</rpc-reply>
</responses>
```

As shown in the example above, a successfully parsed SEMP command always generates `<rpc-reply>` and `<execute-result>` element tags. As shown in the example above, in the case of SEMP show commands, a number of element tags detailing the command name (without parameters) and output are also generated.

The format of <execute-result> element is:

```
<xs:element name="execute-result">
   <xs:complexType>
      <xs:attribute name="code" use="required">
         <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="ok"/>
                <xs:enumeration value="fail"/>
            </xs:restriction>
         </xs:simpleType>
      </xs:attribute>
      <xs:attribute name="reason" type="xs:string" use="optional"/>
      <xs:attribute name="reasonCode" type="xs:int" use="optional"/>
   </xs:complexType>
</xs:element>
```

The execute-result code has either a value of “ok”, or “fail”. In case of failure, the reason (represented by a string) and reason code (represented by an integer) are also provided.

Chapter 6 SNMPv2c and SNMPv3

The Simple Network Management Protocol (SNMP) enables the monitoring of network elements from a central location. This chapter describes SNMP and how to use the TIBCO Messaging Appliance P-7500 Command Line Interface (CLI) to configure it on TIBCO Messaging Appliance P-7500 systems.

TIBCO Messaging Appliance P-7500 provides the following SNMP implementation:

- Standard SNMPv2c MIB support for services and interfaces as defined by the Internet Engineering Task Force (IETF)
- TIBCO enterprise-specific MIB, defining both the environmental and routing data included as MIB objects for P-7500 systems and their components; refer to *Appendix A TIBCO Enterprise-specific MIB* in *TIBCO Messaging Appliance P-7500 Maintenance and Troubleshooting* for details
- TIBCO enterprise-specific traps
- Enhanced security and management features supported in SNMPv3

Topics

Overview

SNMP is an application-level protocol that manages network elements, such as TIBCO Messaging Appliance P-7500 systems. The goal of SNMP is to simplify network management by defining a single management protocol that can be used by clients to manage any network element from any vendor.

The SNMP protocol comprises the following three elements:

- An SNMP client. The SNMP client runs on a network host and communicates with one or more SNMP servers on other network elements, such as routers, to configure and monitor the operation of those network elements.
- An SNMP server. The SNMP server operates on a network element, such as a router, switch, or computer. It responds to SNMP requests received from SNMP clients and generates trap messages to alert the clients about state changes in the network element.
- A Management Information Base (MIB). A MIB specifies the format of managed information for a network element function. The goal of a MIB is to provide a common and consistent management representation for that function across network elements within the network.
- A standard MIB is defined by a body such as the IETF and fosters consistency of management information representation across many vendors' networking products. An enterprise MIB is defined by a single vendor.
- The TIBCO Enterprise-specific MIB defines both the environmental and routing data included as MIB objects for P-7500 systems and their components. Refer to *Appendix A TIBCO Enterprise-specific MIB* in *TIBCO Messaging Appliance P-7500 Maintenance and Troubleshooting* for details.

SNMP defines a client-server model in which a client obtains information from the server through two mechanisms:

- A request/response protocol by which the client configures and monitors the server. In this instance, the information is solicited.
- Asynchronous reports by which the server, on its own initiative, reports notable changes in the system's status to the client. In this instance, the information is unsolicited.

SNMPv3 is an extensible SNMP framework that supplements the SNMPv2c framework by supporting security for messages based on the User-based Security Model (USM) defined in Request for Comments (RFC) 3414.

SNMP Terminology

Refer to Table 6 for a list of general SNMP terms. Refer to Table 7 for a list of basic SNMPv3 terms.

Table 6 SNMP Terminology

Term	Definition
client	A device that executes network management applications that monitor and control network elements
community	A logical group of SNMP-managed devices and clients in the same administrative domain. Each community is associated with a group.
event	A condition or state change that may cause the generation of a trap message
group	A set of users with the same access privileges to the system
managed object	A characteristic of something that can be managed in a network element
network element	A hardware device, such as a router or computer; also called a managed device
server	A software application that provides management of a network element; also called an agent.
trap	Message sent by an SNMP server to a client to indicate the occurrence of a status change (that is, event), most often errors or failures. Network elements use traps to asynchronously report certain events to clients.

Table 7 SNMPv3 Terminology

Term	Definition
notification	Message sent by an SNMPv3 server to a client to indicate the occurrence of a status change (that is, event), most often errors or failures. Like traps, network elements use SNMPv3 notifications to asynchronously report certain events to clients. Notifications differ from traps in that they are acknowledged by the client.

Table 7 SNMPv3 Terminology

Term	Definition
user	An individual who requires access to the system. The system may provide authentication and privacy for the user through SNMPv3 security features. Each user is associated with a group.
view	Definition of the type of management information that is available on the server to a group: • read • write • trap/notification TIBCO Messaging Appliance P-7500 supports one predefined SNMPv3 view for each group: everything. It includes all MIBs associated with the system.

Supported SNMP Versions

TIBCO Messaging Appliance P-7500 supports:

- SNMPv2c (Community-based SNMPv2, defined in RFC 3416)
- SNMPv3 (compliant with RFC 3410 through RFC 3418)

The server encodes SNMP responses using the same SNMP version received in the corresponding request and encodes traps using the SNMP version configured for the trap recipient.

Supported SNMP Standards

The Request for Comments (RFC) standards documents listed in Table 8 define SNMP and the standard MIBs supported by TIBCO Messaging Appliance P-7500.

Table 8 Supported IETF SNMP Standards Documents[1]

Number	Document Title
RFC 1157	A Simple Network Management Protocol (SNMP)
RFC 1213	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 2863	The Interfaces Group MIB

Table 8 Supported IETF SNMP Standards Documents[1]

Number	Document Title
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

1 For details, refer to the "Request for Comments" home page on the IETF Web site, at http://www.ietf.org/rfc.html.

Technical Description

The SNMP server exchanges network management information with SNMP client software running on a network management host. The server responds to requests for information and actions from the client. The server also controls access to the server's Management Information Base (MIB), the collection of objects that can be viewed or changed by the SNMP client.

The SNMP client collects information on network connectivity, activity, and events by polling network elements. Communication between the SNMP server and client occurs through Protocol Data Unit (PDU) messages in one of the following forms:

- Get, GetBulk, and GetNext requests—The client requests information from the server; the server returns the information in a Get response PDU message.
- Set requests—The client changes the value of a MIB object controlled by the server; the server indicates status in a Set response PDU message.
- Traps notification—The server sends notification PDUs to notify the client of significant events that occur on the network element.

SNMP has six types of Protocol Data Unit (PDU) messages. These are defined in Table 9.

Table 9 SNMP PDU Message Types

PDU Message	Definition
Get Bulk	Transmitted by the client to the server to obtain the identifiers and the values of a group or collection of variables rather than one variable at a time.
Get Next Request	Transmitted by the client to the server to obtain the identifiers and the values of variables located after the designated variables.
Get Request	Transmitted by the client to the server to obtain the values of designated variables.
Get Response	Transmitted by the server to the client in response to a Get request, a Get Next request, or a Set request.
Set Request	Transmitted by the client to the server to modify the values of designated variables.
Notification/Trap	Transmitted by the server, on its own initiative, to inform the client of an event noted on a network element.

SNMPv2c Management Information Base

A MIB is a hierarchy of information used to define managed objects in a network element. These sets represent a resource, event, or activity that occurs in the network element.

MIBs are either standard or enterprise-specific. Standard MIBs are created by the IETF and documented in various RFCs. Refer to "SNMPv2c Traps" for a list of supported MIBS.

Enterprise-specific MIBs are developed and supported by a specific vendor for proprietary functions and features not addressed by standard MIBs. They provide consistency of management data representation across a vendor's product line. If your network contains network elements that have enterprise-specific MIBs, you must obtain them from the vendor and compile them into your network management software.

The TIBCO enterprise-specific MIB defines both the environmental and routing data included as MIB objects for TIBCO Messaging Appliance P-7500 systems and their components. Refer to *Appendix A TIBCO Enterprise-specific MIB* in *TIBCO Messaging Appliance P-7500 Maintenance and Troubleshooting* for details.

SNMPv2c Traps

A trap reports status changes occurring on a network element, most often errors or failures.

SNMP traps are defined in either standard or enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. The standard traps are compiled into the network management software. You can also download the standard traps from the IETF Web site, at http://www.ietf.org.

Enterprise-specific traps are developed and supported by a specific equipment manufacturer. If your network contains network elements that have enterprise-specific traps, you must obtain them from the manufacturer and compile them into your network management software.

SNMPv2c traps supported by the TIBCO Messaging Appliance P-7500 system software include:

- SNMPv2-MIB::coldStart – generated when the agent process starts up
- NET-SNMP-AGENT-MIB::nsNotifyRestart – generated when the agent process rereads its configuration file
- NET-SNMP-AGENT-MIB::nsNotifyShutdown – generated as the agent process is shutting down

For trap descriptions or to download, refer to the RFC Index on IETF Web site, at http://www.rfc-editor.org/rfc-index2.html.

Refer to “Configuring Enterprise-specific Traps” for the traps developed and supported by TIBCO for TIBCO Messaging Appliance P-7500.

Note: SNMPv3 uses notifications in place of traps. Notifications differ from traps only in that they are acknowledged by the client.

SNMPv3 Security Improvements

SNMPv2c provides only password protection for the name of the groups querying the server, through the community name and IP address. In contrast, SNMPv3 supports both authentication and encryption for the name of the groups querying the server.

With SNMPv3, only authorized users can communicate with each other. Based on the concept of applying security levels to the name of the groups querying the server, the server decides whether the group is allowed to view or change specific MIBs. Consequently, an SNMPv3 client can interact with a network element only if the administrator configured the network element to allow the interaction.

SNMPv3 authenticates users through the HMAC-MD5-96 protocol, while CBC-DES is the encryption protocol (for privacy). TIBCO Messaging Appliance P-7500 recognizes up to 16 groups for SNMP access that can have any of the following predefined SNMPv3 security levels:

- Authentication only (auth)
- No authentication and no privacy (no auth)
- Authentication and privacy (priv)

TIBCO Messaging Appliance P-7500 supports one predefined SNMPv3 view: everything. This view includes all MIBs associated with the system.

SNMPv3 uses the User-based Security Model (USM) for message security. USM specifies authentication and encryption, and uses the concept of a user for which security parameters such as authentication are configured for both the server and the client. Consequently, messages sent using USM are better protected than messages sent with SNMPv2c community strings, where passwords (that is, community names) are sent openly. SNMPv3 can be used to secure the network element from the following threats:

- unauthorized entity masquerading as an authorized entity
- unauthorized message stream modification
- unauthorized modification or disclosure of information

In contrast, when an SNMPv2c server receives a message request, the server extracts the client's community name. The SNMPv2c community table is searched for a matching community name. If a match is found, the IP address is accepted. An unmatched community name causes an SNMP authentication error. Each entry in the community table identifies:

- An SNMP community name
- An SNMP view name
- A user's privilege level:
  - Read-only (ro)
  - Read-write (rw)
  - Administrator (admin)
- An IP access list name

Setting Thresholds and Alarms

Trap thresholds are the upper and lower limits that you set for the network conditions and events that you are monitoring with SNMP. When these limits are exceeded, the TIBCO Messaging Appliance P-7500 systems report that a threshold has been exceeded. Alarms add to this reporting functionality by allowing you to configure an action to be taken if the threshold is exceeded.

Alarms that are configured correctly can prevent inconvenient or even catastrophic network failures. The main advantage of alarms is that you can specify at exactly which point an action should take place, and you can tailor them to suit the normal operating conditions of your network.

You can set a rising threshold and a falling threshold through the TIBCO Messaging Appliance P-7500 CLI for some of the enterprise-specific traps (refer to “Configuring Enterprise-specific Traps” on page 94 for details). The rising threshold triggers a status severity change when the threshold is exceeded. The falling threshold causes a status severity change when the excessive activity or abnormal condition has returned to normal.

Note: TIBCO recommends that you initially use the default threshold settings with TIBCO Messaging Appliance P-7500 systems to see how they apply to your network. After you assess your network's normal behavior, you can adjust the threshold and alarm settings on systems to make them more useful for your particular network.

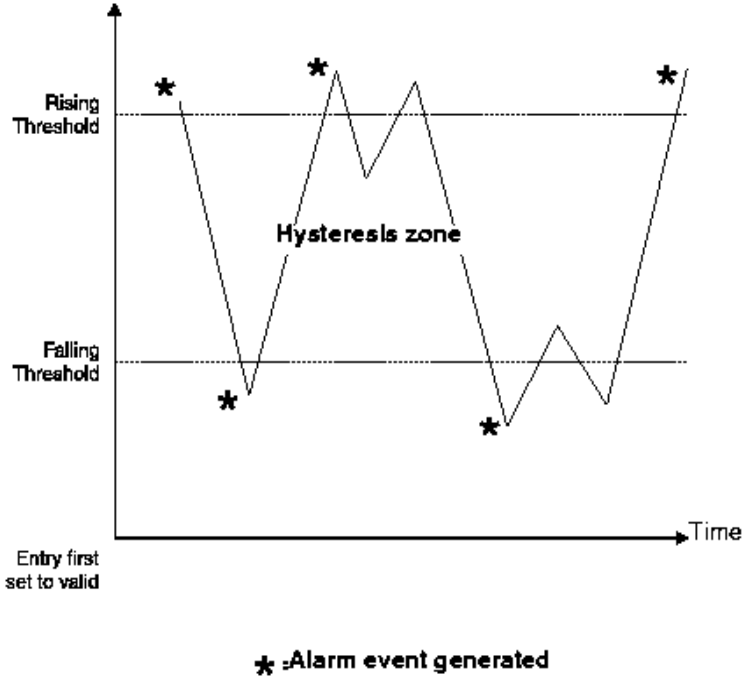
When determining the baseline for conditions that trigger an alarm on your network, observe these guidelines, as applicable:

- Set alarms for any peaks in network utilization. Pick a baseline value that covers most of your network traffic, ignoring any obvious one-time-only peaks. For example, as users log on at the start of the day, you see a large peak in network utilization. The alarm is triggered whenever such peaks occur.
- Set alarms for exceptional peaks in network utilization. Pick a baseline value that covers the highest possible peak seen when service was still provided. The alarm is triggered at levels higher than this peak, alerting you to the most serious utilization on your network.
- When you choose the baseline for error alarms, pick the lowest possible baseline so that the alarm is triggered by any peaks.

For more exact monitoring and control over conditions that trigger an alarm on your network, TIBCO recommends you determine the hysteresis zone for each of the specified alarm values when determining the baseline for normal activity on your network. The hysteresis zone ensures that alarms are not triggered due to small fluctuations around the threshold value. Figure 2 shows an example of this alarm trigger mechanism.

The hysteresis zone is the area where a value has fallen below the upper threshold (also called the rising threshold) but has not yet reached a lower threshold (also called the falling threshold). After a rising threshold generates an alarm, the value must fall below the falling threshold before another alarm is generated. For alarms that are set on falling thresholds, the rule is reversed.

Figure 2 Alarm Trigger Mechanism Using Hysteresis Zone



SNMP Tasks

Server

Perform the required tasks and any of the optional tasks that you need for your SNMP server configuration.

1. Enter the snmp-server Global CONFIG command:

```
tibco(config)# snmp-server
```

Entering the snmp-server Global CONFIG command moves you to the SNMP CONFIG level within the CLI for configuring SNMP parameters:

```
tibco(config-snmp-server)#
```

2. Configure at least one authorized SNMP community (SNMPv2c) or user (SNMPv3), which provides SNMP client access.

```
tibco(config-snmp-server)# community ontario group california
tibco(config-snmp-server)# user ontario group california password version3
```

Note: You can only configure SNMPv3 users when the SNMP server is not running.

3. Create at least one SNMP group:

```
tibco(config-snmp-server)# group california v2c
tibco(config-snmp-server)# group california v3 priv
```

4. (Optional) Set the server parameters, contact and location:

```
tibco(config-snmp-server)# contact “Bob Smith”
tibco(config-snmp-server)# location “10009 Highway 83”
```

5. Designate an SNMP trap host as a recipient for SNMP trap notifications by entering the host SNMP server CONFIG command:

```
tibco(config-snmp-server)# host 126.197.10.5 traps v3 priv user ontario port 165
```

6. Start the SNMP server:

```
tibco(config-snmp-server)# no shutdown
```

Note: By default the SNMP server is not running on the TIBCO Messaging Appliance P-7500 system.

7. (Optional) View the configuration and status of the SNMP server on your TIBCO Messaging Appliance P-7500 system:

```
tibco> show snmp
```

You have completed this procedure.

Trap

Perform the required tasks and any of the optional tasks that you need for your SNMP trap configuration.

1. (Optional) Configure enterprise-specific SNMP traps.
   a. Enter the snmp-server trap Global CONFIG command:

```
tibco(config)# snmp-server
tibco(config-snmp-server)# trap
```

Entering the snmp-server trap Global CONFIG command moves you to the SNMP Trap CONFIG level within the CLI:

```
tibco(config-snmp-server-trap)#
```

   b. Configure the enterprise-specific trap parameters needed for your SNMP trap configuration:

Note: All of the following SNMP Trap CONFIG commands are independent of each other, and optional.

```
tibco(config-snmp-server-trap)# connections
tibco(config-snmp-server-trap)# disk-utilization
tibco(config-snmp-server-trap)# egress-msg-rate
tibco(config-snmp-server-trap)# fan-speed
tibco(config-snmp-server-trap)# ingress-msg-rate
tibco(config-snmp-server-trap)# power-status
tibco(config-snmp-server-trap)# subscriptions
tibco(config-snmp-server-trap)# temperature
tibco(config-snmp-server-trap)# voltage
```

2. Start SNMP trap generation:

```
tibco(config-snmp-server-trap)# no shutdown
```

3. (Optional) View the configuration and status of the SNMP traps on your TIBCO Messaging Appliance P-7500 system:

```
tibco> show snmp trap
```

You have completed this procedure.

Configuring SNMP

NOTICE

NOTICE: Before you configure SNMP on a TIBCO Messaging Appliance P-7500 system, make sure the management IP address is configured. Refer to "Configuring Network Parameters" on page 3 for details.

You should also have the necessary configuration information for:

- IP addresses of SNMP trap recipients
- SNMPv2c communities and their assigned privileges (where applicable)
- SNMPv3 users (where applicable)

To configure SNMP on a TIBCO Messaging Appliance P-7500 system, enter the snmp-server Global CONFIG command:

```
tibco(config)# snmp-server
```

Entering the snmp-server Global CONFIG command moves you to the SNMP CONFIG level within the CLI for configuring SNMP parameters.

```
tibco(config-snmp-server)#
```

From here you can configure the system for SNMPv2c or SNMPv3 using the following SNMP Server CONFIG commands:

- "community" (SNMPv2c only)
- "contact"
- "group"
- "host"
- "location"
- "user" (SNMPv3 only)

Configuring SNMPv2c Communities

For SNMPv2c, access to an SNMP server by an SNMP client is governed by a proprietary SNMP community table that identifies those communities that have read-only, read-write, or administrative privileges to access the SNMP MIBs stored on an SNMP server.

When an SNMP server receives a request, the server extracts the client's community name. The SNMP community table is searched for a matching community. If a match is found, the IP address is accepted. A nonmatching community results in an SNMP authentication error.

Each entry in the community table identifies:

- An SNMP community name
- A user's privilege level
- An SNMP access group

SNMPv2c has three privilege levels:

- Read-only – Read-only access to the entire MIB
- Read-write – Read-write access to the entire MIB except for SNMP configuration objects
- Admin – Read-write access to the entire MIB

Note: TIBCO Messaging Appliance P-7500 only permits read-only access.

community

To configure an authorized SNMPv2c community for read-only access to the SNMP server MIBs, associate SNMPv2c communities with SNMP MIB views, and create and modify the SNMPv2c community table, enter the community SNMP Server CONFIG command:

```
tibco(config-snmp-server)# community <name> group <group>
```

Where:

<name> is the name of the SNMPv2c community

Note: SNMPv2c community names can contain up to 31 alphanumeric characters, and must be unique among all created communities.

<group> is the name of the group to associate with the SNMPv2c community

Note:

- The community name acts as a password and is used to authenticate messages sent between an SNMP client and a TIBCO Messaging Appliance P-7500 system containing an SNMP server.

- The community name is sent in every packet between the client and the server.
- The maximum number of communities in each system is 10.
- By default, SolOS Version 4.3 only permits read-only access.
- The no version deletes a community from the SNMP community table.

group

The TIBCO Messaging Appliance P-7500 system recognizes up to 16 groups for SNMP access. To create or modify an SNMPv2c group, enter the group SNMP Server CONFIG command:

```
tibco(config-snmp-server)# group <name> v2c
```

Where:

<name> is the name of the group

Note: SNMPv2c group names can contain up to 31 alphanumeric characters, and must be unique among all created communities.

v2c is the version of the SNMP protocol to be used to access the group. SNMPv2c is used as a default if no version is specified.

Configuring SNMPv3 Users and Groups

Security features of SNMPv3 allow you to specify who will receive traps and to define MIB views that users in different groups can access. Refer to “SNMPv3 Security Improvements” on page 78 for details.

user

To create or modify SNMPv3 users, enter the user SNMP Server CONFIG command:

```
tibco(config-snmp-server)# user <name> group <group> password <password>
```

Where:

<name> is the name of the SNMPv3 user

Note: SNMPv3 user names can contain up to 31 alphanumeric characters, and must be unique among all created communities.

<group> is the name of the group to associate with the user

<password> is the password assigned for the user

Note: An SNMP user password can contain 8 to 128 alphanumeric characters, and can be used with all created users, whether v2c or v3.

Note:

- If the SNMPv3 user already exists, the user's group is changed to the given group. Otherwise, the user is created and added to the group.
- The no version deletes the given user from the associated group.
- Up to 16 users can be configured.
- You can only configure SNMPv3 users when the SNMP server is not running.
- The MD5 authentication protocol is automatically assigned when an SNMPv3 user is created.
- TIBCO Messaging Appliance P-7500 does not support the SHA authentication protocol for SNMPv3 users.

group

The TIBCO Messaging Appliance P-7500 system recognizes up to 16 groups for SNMP access. To create or modify an SNMPv3 group, enter the group SNMP Server CONFIG command:

```
tibco(config-snmp-server)# group <name> v3 {auth | noauth | priv}}
```

Where:

<name> is the name of the group

Note: SNMPv3 group names can contain up to 31 alphanumeric characters, and must be unique among all created communities.

v3 is the version of the SNMP protocol to be used to access the group.

auth | noauth | priv is the minimum level of security needed to access the group. This applies to SNMPv3 users only.

Note: The no version deletes the specified group.

Setting System Parameters

Setting the contact person and location parameters on TIBCO Messaging Appliance P-7500 systems provides helpful identifiers for the system. These identifiers are arbitrary and do not affect the system's function, but they are useful to have.

contact

To configure the contact person for the TIBCO Messaging Appliance P-7500 system, enter the contact SNMP Server CONFIG command:

```
tibco(config-snmp-server)# contact <name>
```

Where:

<name> is the name of the person who manages the TIBCO Messaging Appliance P-7500 system (0 to 255 characters). Use quotes around the name when it is two or more terms.

location

To configure the location for the TIBCO Messaging Appliance P-7500 system, enter the location SNMP Server CONFIG command:

```
tibco(config-snmp-server)# location <name>
```

Where:

<name> is the name of the server's physical location (0 to 255 characters). Use quotes around the name when it is two or more terms.

Example:

```
tibco(config)# snmp-server contact "Bob Smith"
tibco(config)# snmp-server location "10009 Highway 83"
```

Note: The no version of these commands clears the contact or location identifier from the SNMP configuration.

Configuring SNMP Trap Hosts

Traps are sent to SNMP trap hosts. These hosts are configured in a proprietary trap host table maintained by the SNMP server on the TIBCO Messaging Appliance P-7500 system. Each entry in the table contains:

- IP address of the trap destination
- user name (v3 only) to send in the trap message
- Types of traps enabled to be sent to that destination

host

NOTICE

NOTICE: Traps are not generated until the no shutdown SNMP Trap CONFIG command has been entered. The traps enabled are listed in the "Trap Categories" section.

By default no SNMP trap hosts (that is, clients) are notified of SNMP traps. To designate an SNMP trap host as a recipient for SNMP trap notifications, enter the host SNMP Server CONFIG command:

```
tibco(config-snmp-server)# host <ip-addr> traps [ {v2c | v3 {{auth | noauth | priv} user <name>}}] [port <port>]
```

Where:

host <ip-addr> is the IP address of the SNMP trap host, specified in the dotted decimal notation form nnn.nnn.nnn.nnn

v2c | v3 is the version of the SNMP protocol to be used. SNMPv2c traps are generated as a default if no version is specified.

auth | noauth | priv is the authentication level of the trap. This applies to SNMPv3 traps only. The parameter noauth is used as a default if this parameter is not provided.

user <name> is the name of the user to be used. This applies to SNMPv3 traps only.

port <port> is the UDP port on the host where notifications are to be sent, specified as a decimal value from 0 to 65,535. Port 162 is used as a default if this parameter is not provided.

Note:

- A trap destination is the IP address of an SNMP client that receives the SNMP traps.
- You can configure up to three SNMP trap hosts on each system.
- All traps generated are sent to all configured hosts.
- The no version removes the specified host from the list of recipients for SNMP trap notifications.

Starting and Stopping the SNMP Server

By default the SNMP server is disabled (that is, not running) on TIBCO Messaging Appliance P-7500 systems.

no shutdown

To start the SNMP server, enter the no shutdown SNMP Server CONFIG command:

```
tibco(config-snmp-server)# no shutdown
```

shutdown

To stop the SNMP server once started, enter the shutdown SNMP Server CONFIG command:

```
tibco(config-snmp-server)# shutdown
```

Viewing SNMP Server Status

To view the configuration and status of the SNMP server on your TIBCO Messaging Appliance P-7500 system, enter the show snmp User EXEC command:

```
tibco> show snmp
```

For example:

```
tibco# show snmp
SNMP agent status: enabled
Contact: Bob Smith
Location: 10009 Highway 83
Traps disabled.
Communities:
 public group Gpublic
Groups:
 Gnoauth v3 noauth
 Gpublic v2c
Hosts:
 1.2.3.4 version v2c port 162
SNMPv3 users:
 marge group Gnoauth

Engine ID: 800007e58077be2774ff68a341

Packets in:              119      Packets out:             109
 Get-requests:             1       Get responses:           109
 Get-nexts:              106       Traps:                     0
 Set-requests:             0

Total req. vars:          769      Total set vars:            0

Errors:
 Invalid message:          0       Wrong SNMP version:        0
 Unsupp. sec. level:       0       Bad community name:        0
 Unknown USM user:         0       Bad community use:         0
 Wrong USM digest:         0       ASN parse error:           0
 Decryption error:         0       Unknown context:           0
```

Output Field Descriptions

Refer to Table 10 for descriptions of the show snmp User EXEC command output fields.

Table 10 show snmp Command -- Output Fields

Field	Description
Contact	System's contact person

Table 10 show snmp Command -- Output Fields

Field	Description
Location	System's location
Traps	Indicates whether traps are enabled or disabled
Communities	System's SNMPv2c communities
Groups	System's SNMP groups and version of SNMP used to access the groups (v2c or v3)
Hosts	System's hosts configured to receive SNMP notifications/traps
SNMPv3 users	System's SNMPv3 users
Packets in	Total number of SNMP packets transmitted by the client to the SNMP server • Get-requests– number of get-request SNMP Protocol Data Units (PDUs) processed • Get-nexts – number of get-next SNMP PDUs processed • Set-requests – number of set-request SNMP PDUs processed
Packets out	Total number of SNMP packets transmitted by the SNMP server to the client • Get-responses – number of responses sent to requests from get-request, get-next, and set-request SNMP PDUs • Traps – number of notification/trap SNMP PDUs generated by the SNMP server

Error Message Definitions

Refer to Table 11 for a list of show snmp command SNMP error messages and their definitions.

Table 11 show snmp Command -- SNMP Error Messages

Field	Description
Invalid message	The agent received a malformed SNMP packet
Unsupported security level	The agent received a packet that specified a USM security level it does not support

Table 11 show snmp Command -- SNMP Error Messages

Field	Description
Unknown USM user	The user specified in an SNMP packet was not configured on the agent
Wrong USM digest	The sender of a packet with security level authNoPriv or priv failed authentication
Decryption error	An encrypted packet could not be decrypted
Wrong SNMP version	The agent received a packet with an SNMP version number it does not support
Bad community name	A received packet contained a community name not configured on the agent
Bad community use	Access was requested to an object not in view for the particular community
ASN parse error	The agent was unable to parse a received SNMP packet
Unknown context	A received packet specified a context not configured on the agent

Configuring Traps

Traps are unsolicited messages or notifications sent from an SNMP server to an SNMP client (that is, trap host).

This section provides information for enabling trap generation. The TIBCO Messaging Appliance P-7500 systems generate SNMP traps according to operating specifications defined in supported MIBs.

Trap Categories

The TIBCO Messaging Appliance P-7500 system supports the following trap categories:

- SNMPv2-MIB::coldStart – generated when the server process starts up
- NET-SNMP-AGENT-MIB::nsNotifyRestart – generated when the server process re-reads its configuration file
- NET-SNMP-AGENT-MIB::nsNotifyShutdown – generated as the server process is shutting down
- TIBCO enterprise-specific traps

To enable global trap categories, use the `no shutdown` SNMP Trap CONFIG command. To enable all trap categories for a specific host, use the `host` SNMP Server CONFIG command then the `no shutdown` SNMP Trap CONFIG command.

Configuring Enterprise-specific Traps

NOTICE

NOTICE: For enterprise-specific traps to be effective, their threshold settings must be high enough so that they do not generate false alarms. However, high threshold settings also mean that small amounts of errors can escape detection. Thus, a very small error rate that regularly occurs (such as four per minute) may cause problems with network protocols due to retry delays. Refer to “Setting Thresholds and Alarms” on page 80 for information on refining trap threshold settings.

To configure enterprise-specific SNMP traps on a TIBCO Messaging Appliance P-7500 system, enter the `snmp-server trap` Global CONFIG command:

```
tibco(config)# snmp-server
tibco(config-snmp-server)# trap
```

Entering the snmp-server trap Global CONFIG command moves you to the SNMP Trap CONFIG level within the CLI:

```
tibco(config-snmp-server-trap)#
```

From here you can configure enterprise-specific trap parameters on the system using the following SNMP Trap CONFIG commands:

- "connections"
- "disk-utilization"
- "egress-msg-rate"
- "fan-speed"
- "ingress-msg-rate"
- "power-status"
- "subscriptions"
- "temperature"
- "voltage"

Note: The no version resets all configured traps to their default thresholds

connections

To configure an SNMP trap with a high threshold value for TCP connections on a TIBCO Messaging Appliance P-7500 system, where the value polled is the same as that shown for Active Connections in the output of the show dataplane stats CLI command, enter the connections SNMP Trap CONFIG command:

```
tibco(config-snmp-server-trap)# connections [set-value <set-value> clear-value <clear-value>]
```

Where:

<set-value> is the high trap set threshold value from 1 to 9999. An event is triggered each time the trap value rises above this threshold. Default is 6000.

<clear-value> is the low trap clear threshold value from 1 to 9999. An event is cleared each time the trap value falls below this threshold. Default is 5750.

Note: The no version disables SNMP trap generation for connections on TIBCO Messaging Appliance P-7500 systems, and reverts the threshold values back to default.

disk-utilization

To configure an SNMP trap with a high threshold value for disk space utilization on a TIBCO Messaging Appliance P-7500 system, enter the disk-utilization SNMP Trap CONFIG command:

```
tibco(config-snmp-server-trap)# disk-utilization [set-value <set-value> clear-value <clear-value>]
```

Where:

<set-value> is the high trap set threshold value from 1 to 99. An event is triggered each time the trap value rises above this threshold. Default is 75.

<clear-value> is the low trap clear threshold value from 1 to 99. An event is cleared each time the trap value falls below this threshold. Default is 70.

Note: The no version disables SNMP trap generation for disk space utilization on TIBCO Messaging Appliance P-7500 systems, and reverts the threshold values back to default.

egress-msg-rate

To configure an SNMP trap for aggregate egress message rates in messages/second, whereby a trap is sent when the configured aggregate egress message rate is exceeded, enter the egress-msg-rate SNMP Trap CONFIG command:

```
tibco(config-snmp-server-trap)# egress-msg-rate [set-value <set-value> clear-value <clear-value>]
```

Where:

<set-value> is the high trap set threshold value from 1 to 2147483647. An event is triggered each time the trap value rises above this threshold. Default is 4000000.

<clear-value> is the low trap clear threshold value from 1 to 2147483647. An event is cleared each time the trap value falls below this threshold. Default is 3900000.

Note: The no version disables SNMP trap generation for aggregate ingress message rates on TIBCO Messaging Appliance P-7500 systems, and reverts the threshold values back to default.

fan-speed

To configure an SNMP trap with a default high and low threshold value for case fan speed on a TIBCO Messaging Appliance P-7500 system, where the value polled is the speed of the fan with a unit of revolution per minute (RPM), enter the fan-speed SNMP Trap CONFIG command:

```
tibco(config-snmp-server-trap)# fan-speed
```

Note: The no version disables SNMP trap generation for power supply fan speed on TIBCO Messaging Appliance P-7500 systems.

ingress-msg-rate

To configure an SNMP trap for aggregate ingress message rates in messages/second, whereby a trap is sent when the configured aggregate ingress message rate is exceeded, enter the ingress-msg-rate SNMP Trap CONFIG command:

```
tibco(config-snmp-server-trap)# ingress-msg-rate [set-value <set-value> clear-value <clear-value>]
```

Where:

<set-value> is the high trap set threshold value from 1 to 2147483647. An event is triggered each time the trap value rises above this threshold. Default is 4000000.

<clear-value> is the low trap clear threshold value from 1 to 2147483647. An event is cleared each time the trap value falls below this threshold. Default is 3900000.

Note: The no version disables SNMP trap generation for aggregate ingress message rates on TIBCO Messaging Appliance P-7500 systems, and reverts the threshold values back to default.

power-status

To configure a binary SNMP trap for power status on a TIBCO Messaging Appliance P-7500 system, whereby an event is triggered if a power supply fails, enter the power-status SNMP Trap CONFIG command:

Note: The value polled is status information of the power supplies: 1 indicates a failure of one of the power supplies; 0 indicates no failure.

```
tibco(config-snmp-server-trap)# power-status
```

Note: The no version disables SNMP trap generation for power status on TIBCO Messaging Appliance P-7500 systems.

subscriptions

To configure an SNMP trap with a high threshold for number of subscriptions on a TIBCO Messaging Appliance P-7500 system, where the value polled is a total of all subscriptions and filters, enter the subscriptions SNMP Trap CONFIG command:

```
tibco(config-snmp-server-trap)# subscriptions [set-value <set-value> clear-value <clear-value>]
```

Where:

<set-value> is the high trap set threshold value from 1 to 1999999. An event is triggered each time the trap value rises above this threshold. Default is 5000000.

<clear-value> is the low trap clear threshold value from 1 to 1999999. An event is cleared each time the trap value falls below this threshold. Default is 4750000.

Note: The no version disables SNMP trap generation for number of subscriptions on TIBCO Messaging Appliance P-7500 systems, and reverts the threshold values back to default.

temperature

To configure an SNMP trap with a default high and low threshold value for temperature on the TIBCO Messaging Appliance P-7500 system and blades, where the values polled are CPU1 Core Temp, CPU2 Core Temp, and Chip1 Ambient and Chip2 Ambient for each installed blade, enter the temperature SNMP Trap CONFIG command:

```
tibco(config-snmp-server-trap)# temperature
```

Note: The no version disables SNMP trap generation for temperature on TIBCO Messaging Appliance P-7500 systems and blades.

voltage

To configure an SNMP trap with a default high and low threshold value for voltage on a TIBCO Messaging Appliance P-7500 system, where the voltage sensors configured are BB +1.5V, BB +12V, BB +3.3V, BB +5V, BB -12V, CPU1 12V, CPU1 Vccp, CPU2 12V, CPU2 Vccp, FSB Vtt, Memory Voltage, STBY +3.3V, STBY +5V, and an event is triggered if voltage rises above or falls below factory default thresholds, enter the voltage SNMP Trap CONFIG command:

```
tibco(config-snmp-server-trap)# voltage
```

Note: The no version disables SNMP trap generation for voltage on TIBCO Messaging Appliance P-7500 systems.

Starting and Stopping SNMP Trap Generation

By default SNMP trap generation is disabled on TIBCO Messaging Appliance P-7500 systems.

Note: SNMP trap notifications are not received by any SNMP trap hosts until the host SNMP Server CONFIG command is used to designate and configure the hosts. You can configure up to three SNMP trap hosts on each system.

no shutdown

To start SNMP trap generation, enter the no shutdown SNMP Trap CONFIG command:

```
tibco(config-snmp-server-trap)# no shutdown
```

The traps started are listed in the "Trap Categories" section. All categories are enabled.

shutdown

To stop SNMP trap generation once started, enter the shutdown SNMP Trap CONFIG command:

```
tibco(config-snmp-server-trap)# shutdown
```

Example

This CLI command sequence starts the generation of standard and configured enterprise-specific SNMP traps for power status and subscriptions traps, and disables disk utilization traps:

```
tibco> enable
tibco# configure
tibco(config)# snmp-server trap
tibco(config-snmp-server-trap)# power-status
tibco(config-snmp-server-trap)# subscriptions set-value 350000 clear-value 300000
tibco(config-snmp-server-trap)# no disk-utilization
tibco(config-snmp-server-trap)# no shutdown
```

Viewing SNMP Trap Status

To view the configuration of the SNMP traps and their threshold values on your TIBCO Messaging Appliance P-7500 system, enter the show snmp trap User EXEC command:

Note: To monitor and troubleshoot the status of your TIBCO Messaging Appliance P-7500 system, refer to Chapter 3, TIBCO Messaging Appliance P-7500 Monitoring and Troubleshooting in *TIBCO Messaging Appliance P-7500 Maintenance and Troubleshooting*.

```
tibco> show snmp trap [<name>]]
```

Where:

<name> is the name of the SNMP trap. Entering no name displays all traps.

For example:

```
tibco> show snmp trap

Trap Type                Configured      Set Value      Clear Value
disk-utilization            Yes          75             70
connections                 Yes          6000           5750
subscriptions               Yes          5000000        4750000
voltage
   BB +1.5V high            Yes          1677 mV        1625 mV
   BB +1.5V low             Yes          1325 mV        1365 mV
   BB +1.5V AUX high        Yes          1669 mV        1622 mV
   BB +1.5V AUX low         Yes          1333 mV        1372 mV
   BB +1.5V ESB high        Yes          1638 mV        1591 mV
   BB +1.5V ESB low         Yes          1357 mV        1404 mV
   BB +1.8V high            Yes          1987 mV        1926 mV
   BB +1.8V low             Yes          1637 mV        1689 mV
   BB +12V AUX high         Yes          13578 mV       13144 mV
   BB +12V AUX low          Yes          10416 mV       10725 mV
   BB +3.3V high            Yes          3680 mV        3577 mV
   BB +3.3V low             Yes          2941 mV        3027 mV
   BB +3.3V STB high        Yes          3611 mV        3508 mV
   BB +3.3V STB low         Yes          3027 mV        3113 mV
   BB +5V high              Yes          5564 mV        5407 mV
   BB +5V low               Yes          4446 mV        4576 mV
temperature
   Chassis Temp. high       Yes          45 C           40 C
   NPU Core Temp high       Yes          110 C          90 C
fan-speed
   Chassis Fan 1 low        Yes          2657 RPM       5000 RPM
   Chassis Fan 2 low        Yes          2657 RPM       5000 RPM
   Chassis Fan 3 low        Yes          2657 RPM       5000 RPM
   Chassis Fan 4 low        Yes          2657 RPM       5000 RPM
   Chassis Fan 5 low        Yes          2657 RPM       5000 RPM
   Chassis Fan 6 low        Yes          2657 RPM       5000 RPM
power-status                Yes          0              1
```

```
ingress-msg-rate          Yes     4000000         3900000
egress-msg-rate           Yes     4000000         3900000
redundant-disk            Yes     0               1

tibco>
```

Chapter 7 TIBCO syslog

This chapter describes:

- the TIBCO syslog message format and components
- the TIBCO Messaging Appliance P-7500 Command Line Interface (CLI) commands used to configure syslog on TIBCO Messaging Appliance P-7500 systems for forwarding of messages to a remote syslog message host

Topics

Overview

The TIBCO Messaging Appliance P-7500 system software generates syslog messages, as defined in RFC 3164, to record events such as the following that occur on the routing platform:

- Routine operations, such as change of command modes

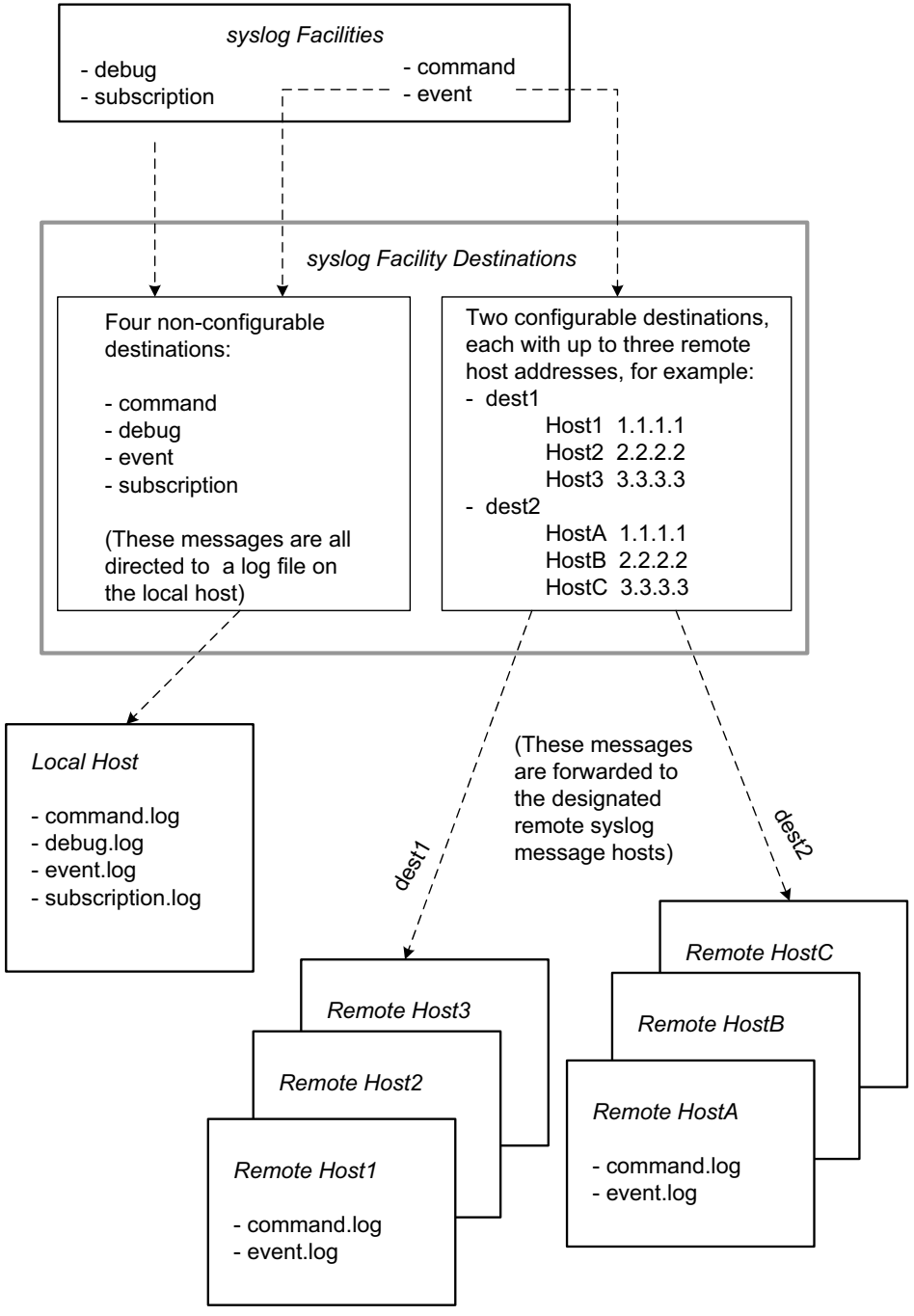
Note: Show command operations are not recorded by TIBCO syslog messages.

- Failure and error conditions, such as voltage levels falling below set threshold values
- Emergency or critical conditions, such as a system blade taken offline due to excessive temperature

Each syslog message identifies the TIBCO Messaging Appliance P-7500 system software process or subsystem that generated the message, and briefly describes the operation or error that occurred.

As shown in Figure 3, the TIBCO syslog system offers both local logging of syslog event messages to local files on TIBCO Messaging Appliance P-7500 systems, as well as forwarding of syslog event messages over the network through standard protocols to remote hosts.

Figure 3 TIBCO syslog Message Flow



Format and Components

Every TIBCO syslog message is created and logged in the form of a plain text ASCII string. Messages are then directed through TIBCO Messaging Appliance P-7500 systems, written to log (ordinary) files, and displayed to users using standard ASCII string handling operations. The logged message is the ASCII string that is written to a log file or to a user at a terminal. This is the string the system administrator or an ordinary user will actually see.

A TIBCO syslog message ASCII string consists of :

- a message priority (facility and severity)
- a header (timestamp and host)
- the message string

Each TIBCO syslog message belongs to a facility, which is a group of messages that are either generated by the same software process, or concern a similar TIBCO Messaging Appliance P-7500 subsystem condition or activity (such as debugging attempts).

Four non-configurable facility destinations are defined and reserved on the TIBCO Messaging Appliance P-7500 system for grouping together related messages from a facility to a log file: command, debug, event, and subscription (refer to Table 12). Syslog message files from the four non-configurable destinations are all directed to a file on the local syslog message host.

In addition, two configurable facility destinations are available for configuration by users for grouping together related messages from a facility to a log file for forwarding to a remote syslog message host.

Table 12 TIBCO syslog Facilities

Facility	Type of Event or Error
command	Actions performed or errors encountered by commands issued at the TIBCO Messaging Appliance P-7500 Command Line Interface (CLI) prompt or by CLI script files
debug	Actions performed or errors encountered by debug processes
event	Actions performed or errors encountered by system processes, for example, system events related to clients, system events related to physical links/LAGs, system events related to routing protocols, system events related to physical hardware
subscription	Actions performed or errors encountered by subscription processes

Each TIBCO syslog message is also preassigned a severity level, which indicates how seriously the triggering event affects routing platform functions. These message event severity levels are defined as an ordered list. Table 13 defines the message severity levels, from highest level to lowest.

Table 13 TIBCO syslog Message Severity Levels

Event Level	Severity Code	Description
LOG_EMERG	0	system is unusable
LOG_ALERT	1	condition needing immediate attention
LOG_CRIT	2	critical conditions
LOG_ERR	3	error conditions
LOG_WARNING	4	warning messages
LOG_NOTICE	5	normal but significant conditions
LOG_INFO	6	informational messages
LOG_DEBUG	7	debug level messages

The associated facility and severity level of a syslog message are together referred to as its priority. By default, priority information is not included in syslog messages.

Chassis syslog Messages

This section describes TIBCO syslog messages related to physical hardware events on the TIBCO Messaging Appliance P-7500 system.

Note: The default thresholds for some TIBCO syslog message events (for example, the Chassis syslog message DISK_UTILIZATION) can be configured through the CLI using the parallel SNMP Trap CONFIG level command (for example, the **disk-utilization** SNMP Trap CONFIG command). There are no Syslog CONFIG level commands for configuring such event threshold values. For information on refining thresholds, refer to "Setting Thresholds and Alarms" on page 80. For further details on the default event threshold values and how to configure them (optional), refer to "Configuring Enterprise-specific Traps" on page 94.

BOOT_DISK_FAIL

Description

This message is sent when the flash bootable disk fails to start.

Event Level Severity

CRITICAL

DISK_DOWN

Description

This message is sent when the disks are not fully redundant, due to disk shutdown, disk failure, or incomplete RAID synchronization.

Event Level Severity

WARNING

DISK_UP

Description

This message is sent when the disks change state from non-redundant to redundant.

Event Level Severity

INFO

DISK_UTILIZATION_HIGH

Description

This message is sent when the disk-utilization value rises above the set threshold value (default is 75).

Event Level Severity

WARNING

DISK_UTILIZATION_HIGH_CLEAR

Description

This message is sent when the disk-utilization value returns to a level below the clear threshold value (default is 70).

Event Level Severity

INFO

FAN_HIGH

Description

This message is sent when the fan speed rises above the upper set threshold value (not configurable).

Event Level Severity

INFO

FAN_HIGH_CLEAR

Description

This message is sent when the fan speed returns to normal operational values.

Event Level Severity

INFO

FAN_LOW

Description

This message is sent when the fan speed falls below the lower set threshold value (not configurable).

Event Level Severity

WARNING

FAN_LOW_CLEAR

Description

This message is sent when the fan speed returns to normal operational values.

Event Level Severity

INFO

POWER_MODULE_UP

Description

This message is sent when one of the power modules return to normal operation.

Event Level Severity

INFO

POWER_MODULE_DOWN

Description

This message is sent one of the power modules fails.

Event Level Severity

WARNING

TEMPERATURE_HIGH

Description

This message is sent when the temperature level rises above the upper set threshold value (not configurable).

Event Level Severity

WARNING

TEMPERATURE_HIGH_CLEAR

Description

This message is sent when the temperature level returns to normal levels.

Event Level Severity

INFO

TEMPERATURE_LOW

Description

This message is sent when the temperature level falls below the lower set threshold value (not configurable).

Event Level Severity

WARNING

TEMPERATURE_LOW_CLEAR

Description

This message is sent when the temperature level returns to normal levels.

Event Level Severity

INFO

VOLTAGE_HIGH

Description

This message is sent when the voltage level rises above the upper set threshold value (not configurable).

Event Level Severity

WARNING

VOLTAGE_HIGH_CLEAR

Description

This message is sent when the voltage level returns to normal levels.

Event Level Severity

INFO

VOLTAGE_LOW

Description

This message is sent when the voltage level falls below the lower set threshold value (not configurable).

Event Level Severity

WARNING

VOLTAGE_LOW_CLEAR

Description

This message is sent when the voltage level returns to normal levels.

Event Level Severity

INFO

Client syslog Messages

This section describes TIBCO syslog messages related to client events on the TIBCO Messaging Appliance P-7500 system.

Note: The default thresholds for some TIBCO syslog message events (for example, the Client syslog message CONNECTIONS_HIGH) can be configured through the CLI using the parallel SNMP Trap CONFIG level command (for example, the **connections** SNMP Trap CONFIG command). There are no Syslog CONFIG level commands for configuring such event threshold values. For information on refining thresholds, refer to "Setting Thresholds and Alarms" on page 80. For further details on the default event threshold values and how to configure them (optional), refer to "Configuring Enterprise-specific Traps" on page 94.

ACL_CONNECT_DENIAL

Description

This message is sent whenever a denial to a client connection request occurs due to the configuration of the client connection access control on the P-7500 system. Refer to "Configuring Access Control Lists" on page 43 for further details.

Event Level Severity

INFO

ACL_PUBLISH_DENIAL

Description

This message is sent whenever a denial to a publishing subject request occurs due to the configuration of the publishing subject access control on the P-7500 system. Refer to "Configuring Access Control Lists" on page 43 for further details.

Event Level Severity

INFO

ACL_SUBSCRIBE_DENIAL

Description

This message is sent whenever a denial to a subscription subject request occurs due to the configuration of the subscription subject access control on the P-7500 system. Refer to “Configuring Access Control Lists” on page 43 for further details.

Event Level Severity

INFO

CONNECT_AUTH_FAIL

Description

This message is sent whenever client authentication fails on the system.

Event Level Severity

INFO

CONNECT_FAIL

Description

This message is sent whenever a client fails to connect to the system.

Event Level Severity

INFO

CONNECTIONS_HIGH

Description

This message is sent when the number of TCP connections rise above the set threshold value (default is 6000).

Event Level Severity

NOTICE

CONNECTIONS_HIGH_CLEAR

Description

This message is sent when the number of TCP connections fall below the clear threshold value (default is 5750).

Event Level Severity

INFO

EG_MSG_RATE_HIGH

Description

This message is sent when the aggregate egress message rate exceeds the set threshold value (default is 4000000).

Event Level Severity

NOTICE

EG_MSG_RATE_HIGH_CLEAR

Description

This message is sent when the aggregate egress message rate falls below the clear threshold value (default is 3900000).

Event Level Severity

INFO

ING_MSG_RATE_HIGH

Description

This message is sent when the aggregate ingress message rate exceeds the set threshold value (default is 4000000).

Event Level Severity

NOTICE

ING_MSG_RATE_HIGH_CLEAR

Description

This message is sent when the aggregate ingress message rate falls below the clear threshold value (default is 3900000).

Event Level Severity

INFO

SUBSCRIPTIONS_HIGH

Description

This message is sent when the number of subscriptions and filters rise above the set threshold value (default is 5000000).

Event Level Severity

NOTICE

SUBSCRIPTIONS_HIGH_CLEAR

Description

This message is sent when the number of subscriptions and filters fall below the clear threshold value (default is 4750000).

Event Level Severity

INFO

Configuring syslog to Forward Messages

To configure a syslog facility destination on a TIBCO Messaging Appliance P-7500 system for grouping together related messages from a facility to a log file for forwarding to a remote syslog message host, enter the create syslog Global CONFIG command (or just syslog if the syslog destination already exists):

```
tibco(config)# create syslog <name>
```

where:

<name> is the name of the user configured syslog destination. The syslog name can contain up to 31 alphanumeric characters, and must be unique among all created syslog destinations.

Note: A maximum of two user configured syslog destinations are permitted per system. The no version removes the user configured syslog destination from the system.

Entering the syslog Global CONFIG command moves you to the Syslog CONFIG level within the CLI for configuring syslog facility and remote host parameters for user configured syslog destinations.

```
tibco(config-syslog)#
```

From here you can configure syslog parameters on the system using the following Syslog CONFIG commands:

- "group"
- "host"

NOTICE

NOTICE: Syslog message files from a user configured destination are not received by remote syslog message hosts (that is, clients) until the host Syslog CONFIG command is used to designate and configure the hosts. You can configure up to three syslog message hosts per user configured syslog destination.

facility

To add the command or event syslog facility to a user configured syslog destination, enter the facility Syslog CONFIG command:

```
tibco(config-syslog)# facility {command | event}
```

Where:

command asks to add the command syslog facility to the user configured destination

event asks to add the event syslog facility to the user configured destination

Note: The no version deletes the specified facility from the user configured destination.

host

NOTICE

NOTICE: Syslog message files from a user configured destination are not received by remote syslog message hosts (that is, clients) until the host Syslog CONFIG command is used to designate and configure the hosts. You can configure up to three syslog message hosts per user configured syslog destination.

To designate a remote syslog message host as a recipient for syslog files, enter the host Syslog CONFIG command:

```
tibco(config-syslog)# host <hostname-or-address> [transport {tcp | udp}]
```

Where:

host <hostname-or-address> is either the name of the remote host, or the IP address with optional port number, specified in the dotted decimal notation form nnn.nnn.nnn.nnn[:nnn]. TCP port 514 is used as a default if the port number is not provided.

transport {tcp | udp} sets the transport mode used for forwading the syslog file to the remote host to either TCP or UDP, respectively. TCP is used as a default if this parameter is not provided.

Note: The no version removes the specified host from the user configured destination.

syslog Configuration Example

This CLI command sequence example configures the syslog facility destination named scott, adds the command and event facilities to this user configured syslog destination, and designates and configures two syslog message hosts for receipt of the forwarded syslog message file.

```
tibco> enable
tibco# configure
tibco (config)# create syslog scott
tibco (config-syslog)# facility command
tibco (config-syslog)# facility event
tibco (config-syslog)# host 192.168.1.12 transport tcp
tibco (config-syslog)# host 192.168.1.13 transport tcp
```

To remove the syslog destination named scott once configured, enter:

```
tibco (config)# no syslog scott
```

Viewing syslog Status

To view the configuration of syslog on your TIBCO Messaging Appliance P-7500 system, enter the show syslog User EXEC command:

Note: To monitor and troubleshoot the status of your TIBCO Messaging Appliance P-7500 system, refer to Chapter 3, TIBCO Messaging Appliance P-7500 Monitoring and Troubleshooting in *TIBCO Messaging Appliance P-7500 Maintenance and Troubleshooting*.

```
tibco> show syslog [<name>]]
```

Where:

<name> is the name of the syslog facility destination. Entering no name displays all destinations.

For example:

```
tibco> show syslog scott
--------------------------------------------------
Name: scott
Facilities: event command
Files
Hosts                    Transport
  192.168.1.12             TCP
  192.168.1.13             TCP

tibco> show syslog
--------------------------------------------------
Name: command
Facilities: command
Files
  command.log
Hosts                    Transport

--------------------------------------------------
Name: debug
Facilities: debug
Files
  debug.log
Hosts                    Transport

--------------------------------------------------
Name: event
Facilities: event
Files
  event.log
Hosts                    Transport

--------------------------------------------------
Name: subscription
Facilities: subscription
```

```
Files
  subscription.log
Hosts                   Transport

--------------------------------------------------
Name: scott
Facilities: event command
Files
Hosts                   Transport
  192.168.1.12            TCP
  192.168.1.13            TCP

tibco>
```

Chapter 8 Configuring IP Interfaces and Addresses

IP addresses are assigned to network interfaces on the TIBCO Messaging Appliance P-7500 system to enable communication with other clients in the network.

This chapter describes:

- the TIBCO P-7500 IP interfaces and options for configuring them
- the TIBCO Messaging Appliance P-7500 Command Line Interface (CLI) commands used to configure, manage, and monitor the IP interfaces supported by P-7500 systems

Refer to Chapter 9, System Redundancy for details on configuring IP interfaces for P-7500 system redundancy.

Note: All functional diagrams and configuration examples in this chapter use the 8-port GigE Network Acceleration Blade (NAB-0801ET) for the purpose of explanation. However, the configuration of IP interfaces and addresses on the 2-port 10GigE NAB (NAB-0210EM) is performed the same, but on two available ports instead of eight.

Topics

Overview

The P-7500 system supports the following options for configuring the network interfaces on the NAB:

- Group the NAB ports into a single Link Aggregation Group (LAG), as shown in Figure 4
- Assign independent IP addresses to NAB to each and every port (that is, no LAG configured), as shown in Figure 5
- A mixture of both, that is, have some of the ethernet ports grouped into a single LAG, and the remaining ports independently addressed, as shown in Figure 6

As described in "Configuring 802.3ad Link Aggregation" on page 13, the P-7500 system supports the concept of a LAG which bundles multiple physical interfaces together to form a single virtual interface. A single LAG is supported on the P-7500 system, which may contain any combination of physical NAB ethernet ports. To applications, the LAG appears as a single IP interface, but inside the LAG, packets are transmitted and received on the bundled physical ports.

By default through the setup Privileged EXEC command, the physical interfaces on the NAB are all configured as 'lag1' upon completing the initial software configuration procedure described in *TIBCO Messaging Appliance P-7500 Getting Started*. Thus, it is common to see only a single IP address associated with P-7500 NAB interface through lag1.

NOTICE

NOTICE: When configuring mated P-7500 systems for system redundancy as described in Chapter 9, System Redundancy, both P-7500 systems in the active/active pair must be configured identically; the only exception is identifying whether a client's configuration is considered to be backup. For example, configuring independent IP interfaces for the eight NAB ports on the primary system and pairing it with a single LAG interface for the NAB ports on the mate system results in unpredictable behavior. This requirement is not currently enforced by the P-7500 system, but operation is unpredictable if the redundant configuration is mismatched on mated P-7500 systems.

Figure 4 Functional Diagram--All NAB Port IP Interfaces Grouped Together into a Single LAG Interface

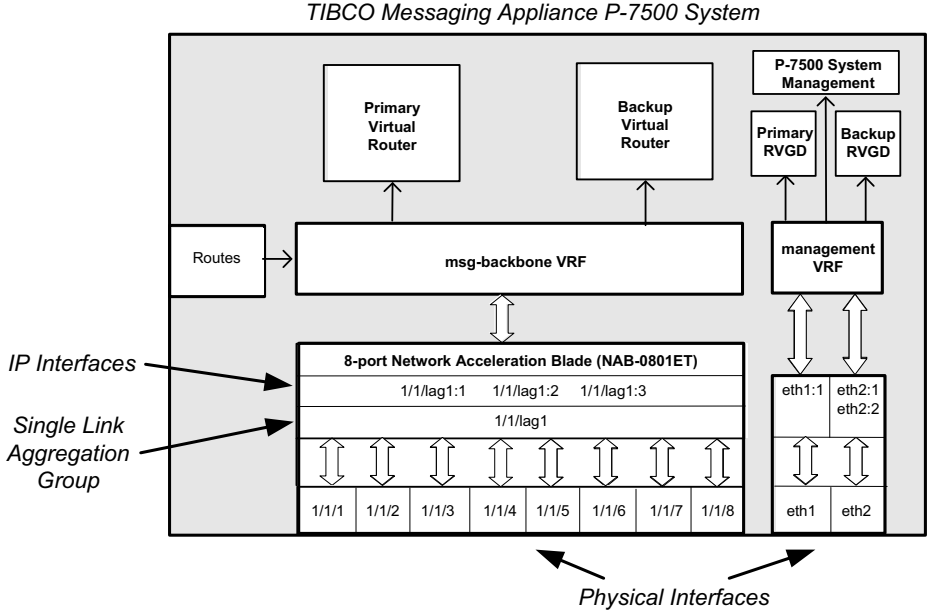


Figure 5 Functional Diagram--All NAB Port IP Interfaces Assigned Independent IP Addresses (No LAG)

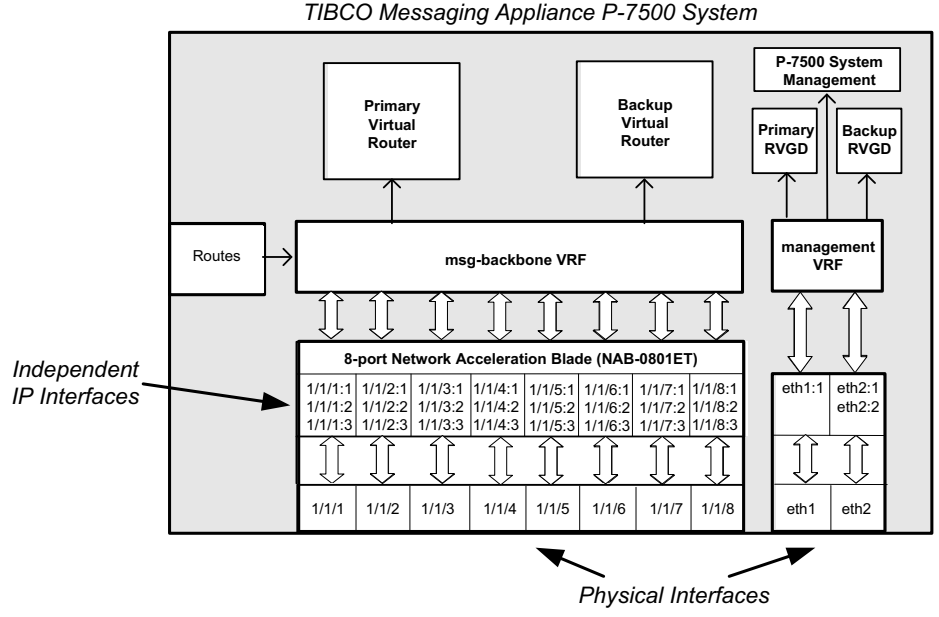
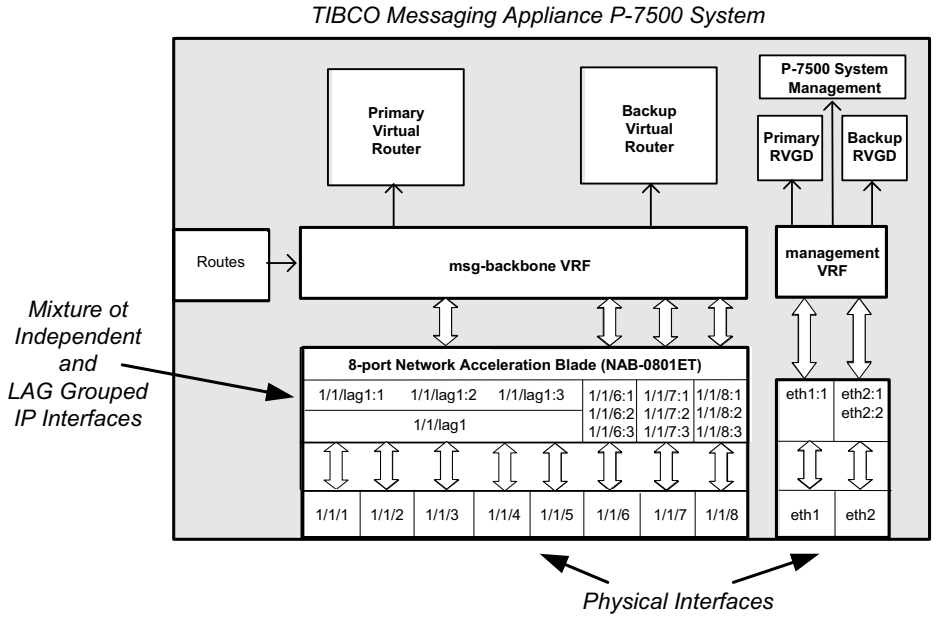


Figure 6 Functional Diagram--Mixture of LAG Grouped and Independently Addressed NAB Port IP Interfaces



Functional Description

As shown in Figure 4 through Figure 6, each physical P-7500 system provides both a primary and backup virtual router to support system redundancy (as described in Chapter 9, “System Redundancy”). Once configured, the primary IP interfaces are active only if the primary virtual router is active (not idle). Likewise, once configured, the backup IP interfaces are active only if the backup virtual router is locally active (not idle). However, unless you are configuring the P-7500 system for redundant operation, configuring the backup virtual router on a P-7500 system is optional since for non-redundant system operation the primary virtual router is always active, and the backup virtual router is always idle.

Note: The primary and backup virtual routers always exist on the physical P-7500 system. They cannot be created nor deleted.

An IP interface is identified by the physical interface it is associated with and an interface type index, numbered 1 to 3. For example, 1/1/5:1 can identify the primary IP interface on physical interface 1/1/5 (however, 1/1/5:1 can be assigned any of the interface types, that is, primary, backup, or static).

Shutting down the physical interface also disables any associated IP interfaces. However, the IP interfaces can be individually configured to be shutdown separate from their associated physical interface.

Physical Interfaces

The physical interfaces identified as eth1 and eth2 are located on the rear of the P-7500 system. The physical interfaces located on the NAB are identified as 1/1/1 through 1/1/8 for NAB-0801ET, and 1/1/1 through 1/1/2 for NAB-0210EM.

Physical interfaces are configured through the Interface CONFIG CLI commands, and their system configuration can be viewed through the show interface User EXEC command.

IP Interfaces

An IP interface is created for each LAG configured on the NAB. An IP interface is also created for each ethernet port on the NAB which is not part of a LAG. Each IP interface may have up to three virtual IP addresses associated with it:

- A static IP address, used primarily for pinging the interface to verify it is physically connected and functional, and for use by the P-7500 system routing

protocols. Clients can connect using this address if the system is not configured for redundancy.

- A primary IP address (required for system redundancy). Clients can connect using this address whenever the router is active for the primary system's IP address in an active/active redundancy deployment
- A backup IP address (required for system redundancy). Clients can connect using this address whenever the system is active for the backup system's IP address in an active/active redundancy deployment

From an IP routing standpoint, the primary and backup IP interface states go in and out of activity depending on the configuration and state of the virtual routers. In contrast, the static IP interface states are always active. They are intended as a diagnostic tool to determine IP reachability to the physical ports. Once configured and enabled, the static IP interfaces are always reachable provided link layer connectivity is intact.

Virtual Routing and Forwarding Objects

Virtual Routing and Forwarding (VRF) is a technology used in networks that allows multiple instances of a routing table to coexist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.

The P-7500 system contains by default two VRF objects called the Management VRF and Message Backbone VRF, respectively. These two VRFs are used by the system to keep management activities, message delivery activities, and routing tables separate.

IP interfaces contained within a VRF are configured through the VRF IP CONFIG CLI commands, and their system configuration can be viewed through the `show interface` User EXEC command.

Management VRF

Through physical interface eth1 (and associated static IP interface eth1:1) , the Management VRF handles the following types of traffic for the P-7500 system:

- CLI or SSH sessions
- SFTP
- SEMP
- SNMP

Through physical interface eth2 (and associated primary and backup IP interfaces eth2:1 and eth2:2) , the Management VRF handles RV Gateway traffic for the P-7500 system.

Message Backbone VRF

The primary and backup virtual routers are served by the Message Backbone VRF. Through the physical interfaces located on the NAB, the Message Backbone VRF handles the client channel traffic (including subject subscriptions) for the virtual routers.

The Message Backbone VRF maintains separate routing information from the Management VRF.

IP Configuration Commands

This section describes the commands you can use to specify address settings and configurations for the IP interfaces on the P-7500 system.

interface

To configure ethernet or LAG parameters for physical interfaces on P-7500 systems, on an interface by interface basis, you must first go to the Interface CONFIG level. You reach this level by entering create interface <phy-interface> at the Global CONFIG level to create the physical interface instance (or interface <phy-interface> if it already exists), where:

<phy-interface> is an ASCII string specifying the ethernet interface port or LAG to be configured. Valid values are eth<port> (for example, eth2); <cartridge>/<slot>/<port> (for example, 1/1/8); <cartridge>/<slot>/lag<N> (for example, 1/1/lag1). There is no default value.

Note: Only a single LAG numbered 1 is supported. A LAG can not be deleted if IP interfaces reference it, and a LAG can not be created on a slot which does not contain a NAB.

Example:

```
tibco# configure
tibco(config)# create interface 1/1/lag1
tibco(config-interface)#
```

The CLI is now at the Interface CONFIG level for LAG 1 on a P-7500 system, and you can use these CLI commands to configure port parameters for this physical interface:

- “member” on page 130
- “shutdown” on page 131

member

To add physical interface members (that is, NAB ports) to a LAG on a member by member basis, enter the member Interface CONFIG command:

```
tibco(config-interface)# member <phy-interface>
```

Where:

<phy-interface> is an ASCII string specifying the physical interface port on the NAB. Valid values are <cartridge>/<slot>/<port> (for example, 1/1/8). There is no default value.

The no version removes a member port from a LAG.

ALERT

ALERT! The no member Interface CONFIG command may cause a short disruption in customer service to the NAB when run. CLI and management sessions are unaffected.

shutdown

To stop a given ethernet or LAG interface on the P-7500 system, enter the shutdown Interface CONFIG command:

```
tibco(config-interface)# shutdown
```

The no version starts a given ethernet or LAG interface on the P-7500 system.

ip vrf

To configure the Management and Message Backbone VRFs on a P-7500 system, enter ip vrf <name> at the Global CONFIG level, where <name> is the name of the specified VRF object, either management for Management VRF, or msg-backbone for Message Backbone VRF.

Example:

```
tibco(config)# ip vrf msg-backbone
tibco(config-ip-vrf)#
```

The CLI is now at the VRF IP CONFIG level for the Message Backbone VRF. From here you can use the following commands to add or delete IP addresses or IP routes:

- “interface” on page 131
- “route” on page 133

interface

To create and configure IP interfaces for VRF objects on an interface by interface basis, enter the create interface VRF IP CONFIG command:

```
tibco(config-ip-vrf)# create interface <ip-interface> [primary | backup | static]
```

To configure existing IP interfaces for VRF objects on an interface by interface basis, enter the interface VRF IP CONFIG command:

tibco(config-ip-vrf)# interface <ip-interface> [*primary* | *backup* | *static*]

Where:

<ip-interface> is an ASCII string in the form of <phy-interface>:<ip> that specifies the IP interface to be associated with the physical interface port. <ip> is a number from 1 to 3 that uniquely identifies this IP interface on the associated physical interface, and it can be associated with any one of the interface types (that is, either primary, backup, or static) .

Valid values are:

eth<port>:<ip> (for example, eth2:1)

<cartridge>/<slot>/<port>:<ip> (for example, 1/1/8:3)

<cartridge>/<slot>/lag1:<ip> (for example, 1/1/lag1:2)

primary specifies that this interface is for the primary virtual router, and is the default if no parameter is entered. It is only active when both the primary virtual router is locally active, and the IP interface on the VRF is running (through the no shutdown VRF IP Interface command)

backup specifies that this interface is for the backup virtual router. It is only active when both the backup virtual router is locally active, and the IP interface on the VRF is running (through the no shutdown VRF IP Interface command)

static specifies that this is the static interface for the physical P-7500 system. It is always active irrespective of the virtual router activity. Clients cannot connect to the static interface if system redundancy is enabled.

Note: The no version of the interface command deletes the specified IP interface from the VRF object.

NOTICE

NOTICE:

- An IP interface can not be deleted if it is referenced for services such as Virtual Router Redundancy Protocol (VRRP).
- There can only be at most one of each IP interface type (that is, primary, backup, or static) bound to any physical interface on the P-7500 system. For example, you can not configure two primary IP interfaces on physical interface 1/1/5.

Entering the interface VRF IP CONFIG command moves you to the VRF IP Interface CONFIG level:

```
tibco(config-ip-vrf-interface)#
```

ip-address

To configure the IP address and network mask for the IP interface on the VRF, enter the ip-address VRF IP Interface command:

```
tibco(config-ip-vrf-interface)# ip-address <cidr-addr>
```

Where:

<cidr-addr> is the IP address/Netmask combination in Classless Inter-Domain Routing (CIDR) form:

nnn.nnn.nnn.nnn/dd

Note: The no version (no ip-address) deletes the IP address and network mask configuration from the IP interface on the VRF.

shutdown

To stop the IP interface on the VRF from running, enter the shutdown VRF IP Interface command:

```
tibco(config-ip-vrf-interface)# shutdown
```

Note: The no version starts the IP interface on the VRF. IP interfaces on the Message Backbone VRF are turned off by default.

route

To configure IP routes on a VRF object, enter the route VRF IP CONFIG command:

```
tibco(config-ip-vrf)#  route {default | <cidr-addr>} <ip-addr> [<ip-interface>]
```

Where:

default specifies the default IP route

<cidr-addr> specifies the IP/Netmask address of the IP route in CIDR form (nnn.nnn.nnn.nnn/dd)

<ip-addr> is the IP address of the IP route in the dotted decimal notation form nnn.nnn.nnn.nnn

<ip-interface> is an optional ASCII string in the form of <phy-interface>:<ip> that specifies the IP interface to be associated with the route. <ip> is a number from 1 to 3 that uniquely identifies this IP interface on the associated physical interface. Valid values are eth<port>:<ip> (for example, eth2:1).

Note: The no version deletes the specified IP route from the VRF object.

virtual-router

Note: The primary and backup virtual routers always exist on the physical P-7500 system. They cannot be created nor deleted. Further, unless you are configuring the P-7500 system for redundant operation as described in Chapter 9, “System Redundancy”, configuring the backup virtual router or Virtual Router Redundancy Protocol (VRRP) parameters on a P-7500 system is optional since for non-redundant system operation it is the primary virtual router that is always active, and the backup virtual router is always idle.

To configure the VRRP and IP interface parameters for the primary and backup virtual routers on each physical P-7500 system, enter virtual-router at the Global CONFIG level:

```
tibco(config# virtual-router {primary | backup}
```

Where:

primary specifies the primary virtual router

backup specifies the backup virtual router

Example:

```
tibco(config)# virtual-router primary
tibco(config-virtual-router)#
```

The CLI is now at the Virtual Router CONFIG level for the primary virtual router. From here you can use the following commands to configure the IP interface parameters for use by VRRP and TIBCO Rendezvous (RV) services:

- “rv-interface” on page 135
- “vrrp-interface” on page 135
- “vrrp-vrid” on page 136

rv-interface

To configure the IP interface that is used both:

- by the Rendezvous Gateway Daemon (RVGD) to communicate with the P-7500 system, and
- for generating client _INBOX subscriptions

enter the rv-interface Virtual Router CONFIG command:

```
tibco(config-virtual-router)# rv-interface <ip-interface>
```

Where:

<ip-interface> is an ASCII string in the form of <phy-interface>:<ip> that specifies the IP interface to be used as the RV interface. <ip> is a number from 1 to 3 that uniquely identifies this IP interface on the associated physical interface.

Note: There is no system default for the IP interface to be used as the RV interface. Further, the RV service cannot be enabled without configuring the RV IP interface beforehand.

Valid values are:

<cartridge>/<slot>/<port>:<ip> (for example, 1/1/8:3)

<cartridge>/<slot>/lag<N>:<ip> (for example, 1/1/lag1:2)

Note: The no version deletes the IP interface specified for use by RV services from the virtual router.

vrrp-interface

To configure the IP interface for use by VRRP, enter the vrrp-interface Virtual Router CONFIG command:

```
tibco(config-virtual-router)# vrrp-interface <ip-interface>
```

Where:

<ip-interface> is an ASCII string in the form of <phy-interface>:<ip> that specifies the IP interface to use for VRRP. <ip> is a number from 1 to 3 that uniquely identifies this IP interface on the associated physical interface.

Note: There is no system default for the IP interface to be used by VRRP. While configuring the VRRP IP interface is optional for non-redundant system operation, is is mandatory for enabling the active/active system redundancy feature described in Chapter 9, System Redundancy.

Valid values are:

<cartridge>/<slot>/<port>:<ip> (for example, 1/1/8:3)

<cartridge>/<slot>/lag<N>:<ip> (for example, 1/1/lag1:2)

Note: The no version deletes the IP interface specified for use by VRRP from the virtual router.

vrrp-vrid

To configure the virtual router identifier (VRID) used by VRRP, enter the vrrp-vrid Virtual Router CONFIG command:

```
tibco(config-virtual-router)# vrrp-vrid <vrid>
```

Where:

<vrid> is a value between 1 and 255 (this value must be different from the VRRP VRIDs being used by anything else on the local subnet). There is no default value.

Note: The no version (no vrrp-vrid) deletes the VRID from the virtual router.

Configuring IP

NOTICE

NOTICE: Rendezvous clients communicate with the TIBCO Messaging Appliance P-7500 system through interfaces on the NAB, while the Rendezvous Gateway communicates with other Rendezvous entities in the network through the Ethernet 2 (eth2) interface on the system (once Rendezvous Gateway services are started). To facilitate low latency communications between the Rendezvous Gateway and TIBCO Messaging Appliance P-7500 system, configure the NAB and eth2 interfaces in the same IP subnet and connect the interfaces to the same Layer 2 network.

Upon completing the initial software configuration procedure described in *TIBCO Messaging Appliance P-7500 Getting Started*, the physical interfaces on the NAB are all configured as lag1 by default through the setup Privileged EXEC command.

Configuring Independent IP Interfaces for all NAB Ports

To configure independent IP interfaces for all NAB ports on NAB-0801ET:

1. Decommission all NAB ports from lag1 on a port by port basis:

```
tibco(config)# interface 1/1/lag1
tibco(config-interface)# no member 1/1/1
tibco(config-interface)# no member 1/1/2
tibco(config-interface)# no member 1/1/3
tibco(config-interface)# no member 1/1/4
tibco(config-interface)# no member 1/1/5
tibco(config-interface)# no member 1/1/6
tibco(config-interface)# no member 1/1/7
tibco(config-interface)# no member 1/1/8
tibco(config-interface)# exit
```

2. Create and configure independent IP interfaces (primary, backup, and static) for all the NAB ports under the Message Backbone VRF (as shown in Figure 5 on page 125):

```
tibco(config)# ip vrf msg-backbone

tibco(config-ip-vrf)# create interface 1/1/1:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.181.110/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/1:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.171.133/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/1:3 static
```

```
tibco(config-ip-vrf-interface)# ip-address 10.10.2.1
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit

tibco(config-ip-vrf)# create interface 1/1/2:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.182.110/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/2:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.172.133/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/2:3 static
tibco(config-ip-vrf-interface)# ip-address 10.10.2.2
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit

tibco(config-ip-vrf)# create interface 1/1/3:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.183.110/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/3:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.173.133/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/3:3 static
tibco(config-ip-vrf-interface)# ip-address 10.10.2.3
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit

tibco(config-ip-vrf)# create interface 1/1/4:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.184.110/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/4:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.174.133/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/4:3 static
tibco(config-ip-vrf-interface)# ip-address 10.10.2.4
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit

tibco(config-ip-vrf)# create interface 1/1/5:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.185.110/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/5:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.175.133/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/5:3 static
tibco(config-ip-vrf-interface)# ip-address 10.10.2.5
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit

tibco(config-ip-vrf)# create interface 1/1/6:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.186.110/19
```

```
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/6:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.176.133/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/6:3 static
tibco(config-ip-vrf-interface)# ip-address 10.10.2.6
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit

tibco(config-ip-vrf)# create interface 1/1/7:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.187.110/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/7:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.177.133/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/7:3 static
tibco(config-ip-vrf-interface)# ip-address 10.10.2.7
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit

tibco(config-ip-vrf)# create interface 1/1/8:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.188.110/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/8:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.178.133/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/8:3 static
tibco(config-ip-vrf-interface)# ip-address 10.10.2.8
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
```

3. (Optional) If required for your network, configure the default IP route for the Message Backbone VRF:

```
tibco(config-ip-vrf)# route default 192.168.160.11
tibco(config-ip-vrf)# exit
tibco(config-ip)# exit
```

You have completed this procedure.

Configuring a Mixture of Independent and LAG grouped IP Interfaces

To configure a mixture of independent and LAG grouped IP interfaces on NAB-0801ET, whereby NAB ports 1/1/6 and 1/1/8 are decommissioned from lag1:

1. Decommission NAB ports 1/1/6 and 1/1/8 from lag1:

```
tibco(config)# interface 1/1/lag1
tibco(config-interface)# no member 1/1/6
```

```
tibco(config-interface)# no member 1/1/8
tibco(config-interface)# exit
```

2. Create and configure independent IP interfaces (primary, backup, and static) for NAB ports 1/1/6 and 1/1/8 under the Message Backbone VRF:

```
tibco(config)# ip vrf msg-backbone

tibco(config-ip-vrf)# create interface 1/1/6:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.186.110/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/6:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.176.133/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/6:3 static
tibco(config-ip-vrf-interface)# ip-address 10.10.2.6
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit

tibco(config-ip-vrf)# create interface 1/1/8:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.188.110/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/8:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.178.133/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/8:3 static
tibco(config-ip-vrf-interface)# ip-address 10.10.2.8
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
```

3. (Optional) If required for your network, configure the default IP route for the Message Backbone VRF:

```
tibco(config-ip-vrf)# route default 192.168.160.11
tibco(config-ip-vrf)# exit
tibco(config-ip)# exit
```

You have completed this procedure.

To commission NAB ports 1/1/6 and 1/1/8 back to lag1 on NAB-0801ET after decommissioning them:

1. Shut down and delete the independent IP interfaces (primary, backup, and static) for NAB ports 1/1/6 and 1/1/8 under the Message Backbone VRF:

```
tibco(config)# ip vrf msg-backbone

tibco(config-ip-vrf)# interface 1/1/6:1 primary
tibco(config-ip-vrf-interface)# shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# no interface 1/1/6:1 primary
tibco(config-ip-vrf)# interface 1/1/6:1 backup
tibco(config-ip-vrf-interface)# shutdown
tibco(config-ip-vrf-interface)# exit
```

```
tibco(config-ip-vrf)# no interface 1/1/6:1 backup
tibco(config-ip-vrf)# interface 1/1/6:1 static
tibco(config-ip-vrf-interface)# shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# no interface 1/1/6:1 static

tibco(config-ip-vrf)# interface 1/1/8:1 primary
tibco(config-ip-vrf-interface)# shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# no interface 1/1/8:1 primary
tibco(config-ip-vrf)# interface 1/1/8:1 backup
tibco(config-ip-vrf-interface)# shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# no interface 1/1/8:1 backup
tibco(config-ip-vrf)# interface 1/1/8:1 static
tibco(config-ip-vrf-interface)# shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# no interface 1/1/8:1 static
```

2. Commission NAB ports 1/1/6 and 1/1/8 back to lag1:

```
tibco(config)# interface 1/1/lag1
tibco(config-interface)#  member 1/1/6
tibco(config-interface)#  member 1/1/8
tibco(config-interface)# exit
```

You have completed this procedure.

Configuring VRRP and IP Interface Parameters for Virtual Routers

To configure the VRRP and IP interface parameters for the primary and backup virtual routers (required for system redundancy, otherwise optional):

1. Configure the VRRP and IP interface parameters for the primary virtual router:

```
tibco(config)# virtual-router primary
tibco(config-virtual-router)# vrrp-interface 1/1/lag1:1
tibco(config-virtual-router)# rv-interface 1/1/lag1:1
tibco(config-virtual-router)# vrrp-vrid 110
tibco(config-virtual-router)# exit
```

2. Configure the VRRP and IP interface parameters for the backup virtual router:

```
tibco(config)# virtual-router backup
tibco(config-virtual-router)# vrrp-interface 1/1/lag1:2
tibco(config-virtual-router)# rv-interface 1/1/lag1:2
tibco(config-virtual-router)# vrrp-vrid 133
tibco(config-virtual-router)# exit
```

You have completed this procedure.

Monitoring IP

You can use several show commands to monitor and validate IP interface configurations and status on TIBCO Messaging Appliance P-7500 systems:

- "show interface" on page 142
- "show ip vrf" on page 143
- "show virtual-router" on page 145

show interface

To view the current configuration parameters and traffic statistics for the physical interfaces on the P-7500 system, enter the show interface User EXEC command:

```
tibco> show interface [<phy-interface>]
```

Where:

<phy-interface> is an ASCII string specifying the physical ethernet interface port or LAG to be displayed. Valid values are eth<port> (for example, eth2); <cartridge>/<slot>/<port> (for example, 1/1/8); <cartridge>/<slot>/lag<N> (for example, 1/1/lag1). There is no default value.

Note: Only a single LAG numbered 1 is supported.

Example from P-7500 system with NAB-0801ET:

```
tibco> show interface 1/1/lag1
Interface: 1/1/lag1
 MAC address: 00:50:c2:44:b0:24
 Enabled: yes
 Rx pkts:       25763843      Rx bytes:      3032103187
 Tx pkts:       228708        Tx bytes:      78771246
 Configured members: 1/1/1, 1/1/2, 1/1/3, 1/1/4, 1/1/5, 1/1/6, 1/1/7, 1/1/8
 Operational members: 1/1/2
```

Example from P-7500 system with NAB-0210EM:

Note: To determine the type of SFP+ modules installed in a NAB-0210EM, observe the displayed "Media type" value returned for the physical interfaces 1/1/1 and 1/1/2. A value of 10GE SR represents the 10GBase-SR SFP+ module.

```
tibco> show interface

Interface: 1/1/lag1

  MAC address: 00:50:c2:44:c0:68
  Enabled: yes
  Rx pkts: 3277876 Rx bytes: 3305443359
  Tx pkts: 3126847 Tx bytes: 2857929026
  Configured members: 1/1/1, 1/1/2
  Operational members: 1/1/1, 1/1/2

Interface: eth1

  MAC address: 00:15:17:4d:2b:4c
  Enabled: yes
  Rx pkts: 22555 Rx bytes: 1899197
  Tx pkts: 10538 Tx bytes: 4330267
  Link detected: yes
  Media type: N/A

Interface: eth2

  MAC address: 00:15:17:4d:2b:4d
  Enabled: yes
  Rx pkts: 0 Rx bytes: 0
  Tx pkts: 0 Tx bytes: 0
  Link detected: no
  Media type: N/A

Interface: 1/1/1

  MAC address: 00:50:c2:44:c0:68
  Enabled: yes
  Rx pkts: 1198305 Rx bytes: 1167525582
  Tx pkts: 3126185 Tx bytes: 2857855874
  Link detected: yes
  Media type: 10GE SR

Interface: 1/1/2

  MAC address: 00:50:c2:44:c0:69
  Enabled: yes
  Rx pkts: 2079571 Rx bytes: 2137917777
  Tx pkts: 662 Tx bytes: 73152
  Link detected: yes
  Media type: 10GE SR
```

show ip vrf

To view the configuration and status of VRF objects within the P-7500 system, enter the show ip vrf User EXEC command:

```
tibco> show ip vrf [<name> [route]]
```

Where:

<name> is the name of the VRF object, either management or msg-backbone. Entering no name displays all VRF objects configured on the system.

route asks to show detailed IP routing information for the specified VRF object.

Note: When no parameters are entered, one line of output for each VRF object configured on the system is displayed. Each line contains the VRF object name and the number of interfaces currently attached to the VRF object. When a specific VRF object name is specified, the output displayed is the IP routing table for that interface and the list of interfaces currently attached to that VRF object.

Examples:

tibco> **show ip vrf**

```
VRF              Interfaces    Routes
---------------------------------------------------
management       3             1
msg-backbone     1             1
```

tibco> **show ip vrf management**

```
VRF: management
Number of interfaces: 3

Interface          V Router       IP Address            Status
--------------     ------------   ----------------------  -------
eth2:1             primary        0.0.0.0/0             disabled
eth2:2             backup         0.0.0.0/0             disabled
eth1:1             primary        192.168.128.77/20     enabled

Number of routes: 1

Destination      Gateway          Network Mask       Interface
----------------  ----------------  ------------------  ---------
default          192.168.128.1    0.0.0.0            eth1:1
```

tibco> **show ip vrf msg-backbone**

```
VRF: msg-backbone
Number of interfaces: 1

Interface       V Router    IP Address               Status   #Conn   #Frag
--------------   ------------  -------------------------  --------  ----------  -----
1/1/lag1:1      primary     192.168.160.77/19        enabled  1       0

Number of routes: 1

Destination      Gateway            Network Mask     Interface
------------------  --------------------  ------------------  ---------
default          192.168.160.1      0.0.0.0          1/1/lag1:1
```

show virtual-router

To view the current configuration of the two virtual routers on the physical P-7500 system, enter the show virtual-router User EXEC command:

```
tibco> show virtual-router

Primary Virtual Router:
  virtual router id:    192.168.160.147
  vrrp vrid:            147
  vrrp ip interface id: 1/1/lag1:1
  rv ip interface id:   1/1/lag1:1

Backup Virtual Router:
  virtual router id:    192.168.160.148
  vrrp vrid:            148
  vrrp ip interface id: 1/1/lag1:2
  rv ip interface id:   1/1/lag1:2
```

Note: The Virtual Router Id is not explicitly configured on the virtual routers, but implicitly determined by the IP address of the interface selected for the VRRP IP interface.

Chapter 9 System Redundancy

TIBCO Messaging Appliance P-7500 active/active system redundancy is a feature that provides system pairing to increase overall service availability.

The two paired systems in an active/active redundancy pair can both actively service clients, but on the failure of one of the systems, its mate takes over the task of providing service to all of those clients. This chapter describes:

- the system redundancy facility
- configuring a redundant system pair
- monitoring redundancy

Topics

Overview

System redundancy eliminates the potential for a single point of failure in a message routing network by allowing the network administrator to define two P-7500 systems as a redundant pair. The TIBCO Messaging Appliance P-7500 offers active/active redundancy, whereby both systems can be active and simultaneously provide service to clients. This allows for load-sharing while both systems are functional. However, if one of the systems is taken out of service or fails, the other system automatically takes over responsibility for the clients typically served by the failed system. Both of these paired systems must be located on the same broadcast subnetwork.

The active/active redundancy feature is largely transparent to clients, RV services, and other P-7500 systems in the network. Only the two systems that are paired as mates require explicit configuration to take advantage of the feature.

Similarly, there is no configuration needed on client host computers to take advantage of the P-7500 redundancy facility. The only visible impact to clients during a redundancy failover is non-delivery of messages for a short period of time, as the clients are forced to reconnect.

Note: Only a one-to-one redundancy pairing is supported at this time. Many-to-1, 1-to-many, and many-to-many groupings are not supported.

Functional Description

Each P-7500 system in an active/active redundancy pair can serve clients and send and receive RV messages during normal operating conditions. However, should one of the systems fail, the active system can provide the service ordinarily provided by both of the systems individually. This model differs from an active/standby model where a primary system provides service to clients and sends and receives data, and the backup system waits in standby mode but only provides service should the primary system fail.

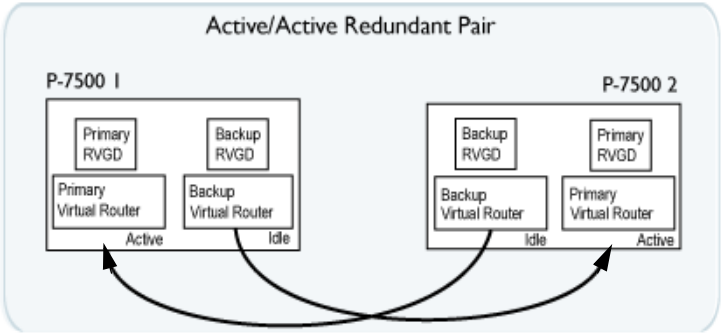
Primary and Virtual Routers

To support active/active redundancy, each P-7500 system uses a primary and backup virtual router. When both systems are active, the primary virtual routers on both systems are active, but the backup virtual routers are idle. If one of the systems in the redundant pair goes out of service, the backup virtual router of the active system changes to an active state, and it provides service for clients and handles the RV messages that typically use the primary virtual router of the system that is out of service.

To enable the backup virtual router of one system to assume the role of its mate's primary virtual router when a system failure occurs, the configuration of the virtual routers on each system must mirror one another. That is, the backup virtual routers on both systems must have the same configuration as the primary virtual routers they backup.

Figure 7 illustrates the relationship between the virtual routers of a redundant pair.

Figure 7 Supporting Relationships Between Virtual Routers



P-7500 1 Backup Virtual Router	supports...	P-7500 2 Primary Virtual Router
P-7500 2 Backup Virtual Router	supports...	P-7500 1 Primary Virtual Router

Use of RV Gateway services is not mandatory for system redundancy; you can configure a redundant pair of P-7500 systems without it. However, if you do need to use RV Gateway services with a redundant P-7500 system pair, then primary and backup Rendezvous Gateway Daemons (RVGDs) are required on each system. For more information on configuring RV Gateway services, refer to Chapter 2, "Managing TIBCO Rendezvous Tasks".

Primary and Backup IP Interfaces

For each P-7500 system, physical interfaces on the Network Acceleration Blade (NAB) must be bound to distinct IP interfaces, each identified by an IP address and subnet mask. It is these IP interfaces that clients connect to.

To enable active/active redundancy, primary and backup instances of the IP interfaces are created for each system in a redundant pair. The same IP interfaces are used by each system, but they are assigned as primary on one and as backup on the other. Therefore, if one system goes out of service, a backup IP interface can still be accessed by the client on the active system.

These primary and backup IP interfaces are associated with the primary and backup virtual routers on each system in the redundant pair.

Figure 8 illustrates a simplified example of the primary and backup IP interfaces and virtual routers used by a redundant pair. Figure 9 illustrates the same redundant pair in a failover situation.

- On P-7500 2, the physical interface 1/6/1 contains two IP interfaces. 1/6/1:1 is configured as the primary IP interface with IP address 192.168.171.133/19,

and 1/6/1:2 is configured as the backup IP interface with IP address 192.168.181.110/19.

- To maintain service if P-7500 2 goes down, the mate system, P-7500 1, also contains the IP interfaces 1/6/1:1 and 1/6/1:2. However the IP addresses assigned to these IP interfaces are reversed. For P-7500 1, the primary IP interface 1/6/1:1 is configured with IP address 192.168.181.110/19, and the backup IP interface 1/6/1:2 is configured with IP address 1192.168.171.133/19.

An ip number from 1 to 3 indicates the type of IP interface (primary, backup, or static). A typical association is 1 for primary, 2 for backup, and 3 for static. However, this is not enforced.

Figure 8 Simplified Active and Backup Configuration

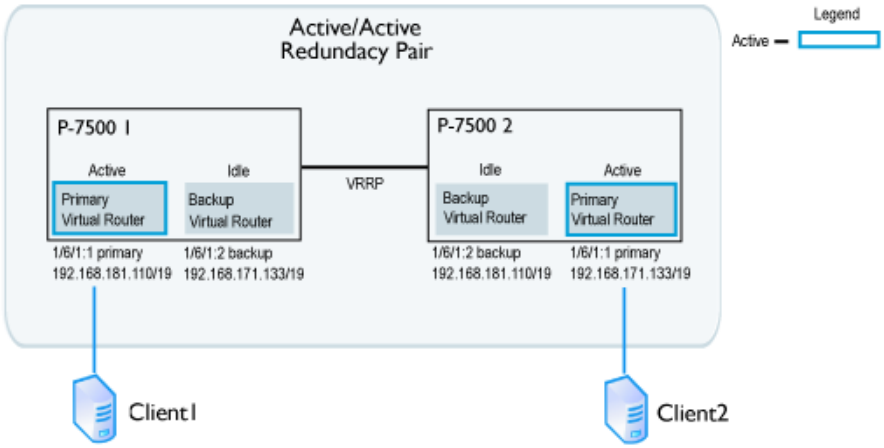
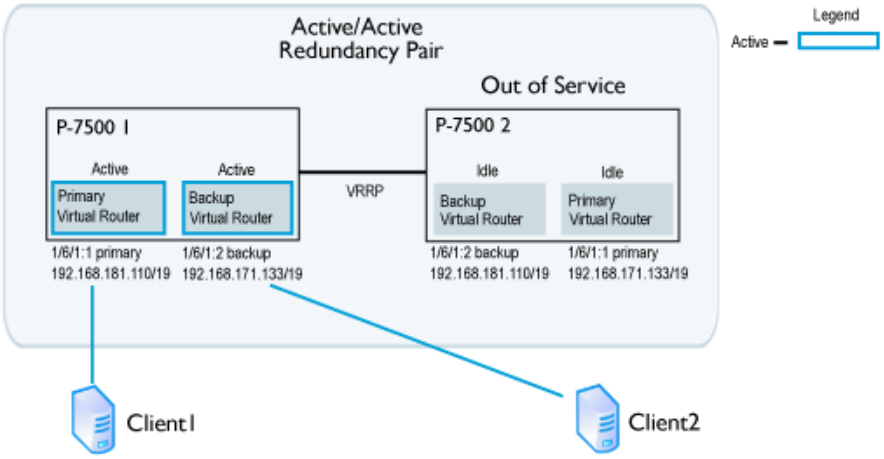


Figure 9 Simplified Active and Backup Configuration in Failover



Additional Redundant IP Interfaces

In addition to the IP interfaces to which a client connect, the following components of the P-7500 system must also be associated with an IP interface and given a redundant configuration:

- VRRP interface—A P-7500 redundant pair uses the Virtual Router Redundancy Protocol (VRRP) as described in RFC 3768 to indicate the status of the virtual routers. To facilitate communication between each system of the redundant pair, a VRRP interface is used on each system. Primary and backup instances are also required for each VRRP interface, and to enable redundancy, the IP addresses assigned for both primary VRRP interfaces must match the IP addresses for their backup VRRP interfaces.
- RV Interface—The RV interface is used for the RVGD to communicate with the NAB and for generating client _INBOX subscriptions. On each system of the redundant pair, one instance of the RV interface must be configured as primary and another as backup, and both instances must be assigned a IP address. To enable redundancy, the IP addresses assigned for both primary RV interfaces must match the IP addresses for their backup RV interfaces.
- eth2 Interface—The RV Gateway uses the Ethernet 2 (eth2) physical interface to communicate with the TIBCO Messaging Appliance P-7500 system and other RV entities in the network. The eth2 interface is active only when RV Gateway services are running on the system. Therefore, if RV Gateway services are not running on your network, you do not need to configure eth2.

  In a redundant configuration, two IP interfaces must be configured for eth2.

On each system of the redundant pair, one IP interface of eth2 must be configured as primary (eth2:1) and another as backup (eth2:2), and both IP interfaces must be assigned an IP address. The IP addresses for both primary eth2 interfaces must match the IP addresses for their backup eth2 interfaces.

For more information on configuring RV Gateway services, refer to Chapter 3, "Managing TIBCO Rendezvous Tasks".

Redundancy Priority Level Definitions

A number of TIBCO Messaging Appliance P-7500 priority levels have been defined for redundancy. These priority levels are advertised by the virtual routers.

When activity switches occur between redundant pairs, the priority levels advertised by the virtual routers of each system change to indicate their current state and role. These advertisements are broadcast between redundant pairs through VRRP. For example, the virtual router that advertises the highest priority level for a given VRID is the active virtual router for that VRID. All messages and system requests for that VRID are then forwarded to that virtual router.

For more information on the advertised local priority levels and how to monitor current priority levels, refer to “Monitoring Redundancy” on page 169.

Activity Switches Between Redundancy Pairs

The typical activity switches for the TIBCO Messaging Appliance P-7500 redundancy facility are:

- the failure activity switch, described below
- the recovery activity switch, described on page 157

Note: Many other activity switch scenarios are possible, but they are beyond the scope of this chapter. For more information, contact TIBCO.

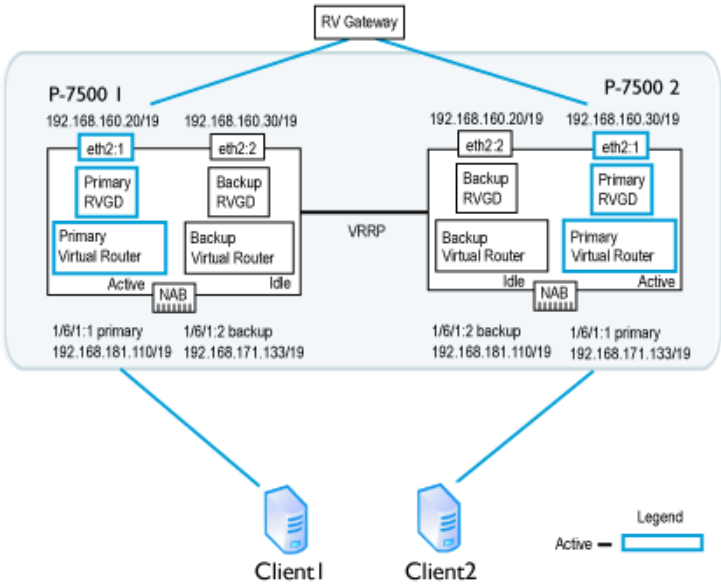
Failure Activity Switch

When a TIBCO Messaging Appliance P-7500 system is described as failed, the system is not able to participate in message routing and forwarding for a period of time. This might be a transient outage, which is relatively short-lived, or a longer-term outage, and includes both planned and unplanned causes such as:

- reset or power-cycle of the system (transient outage, planned or unplanned)
- hardware failure of the system (longer-term outage, unplanned)
- physical link to the system is down (could be transient or longer-term, planned or unplanned)
- software upgrade of the system (transient outage, planned)

Figure 10 system has been placed in the standby state as a result of the network operator entering the release-activity Router Redundancy CONFIG command through the P-7500 Command Line Interface (CLI) (longer-term outage, planned)

Active/Active Redundancy Pairing



In an active/active network configuration, such as that illustrated in Figure 10, the following series of operations occur if one of the systems (in the following example P-7500 2) goes out of service for any reason:

1. VRRP on P-7500 1 detects the failure of P-7500 2.
2. P-7500 1 becomes active for the IP address 192.168.171.133/19. When this occurs, the backup virtual router for P-7500 1 goes from an idle state to an active state.
3. P-7500 1 increases the priority of its VRRP advertisements for the IP address 192.168.171.133/19 to Assert-Activity. It also sends out a gratuitous ARP to let other network devices know that it is taking over the IP address. At this point, network traffic to the IP address 192.168.171.133/19 flows to P-7500 1.
4. As this redundant pair is interacting with RV services on other networks, the backup RVGD and the backup eth2 interface (eth2:2) for P-7500 1 become active.
5. RV messages directed to the IP address 192.168.160.30/19 now flow to eth2:2 on P-7500 1. P-7500 also sends out a gratuitous ARP through eth2:2 to let other network devices know that it is taking over 192.168.160.30/19. As the backup for eth2:1 on P-7500 2, eth2:2 on P-7500 1 uses the same IP address.
6. Clients that had already established TCP connections to P-7500 2 receive error messages back from P-7500 1 because the TCP connections are not present on P-7500 1. This causes the clients to tear down the existing TCP sessions and

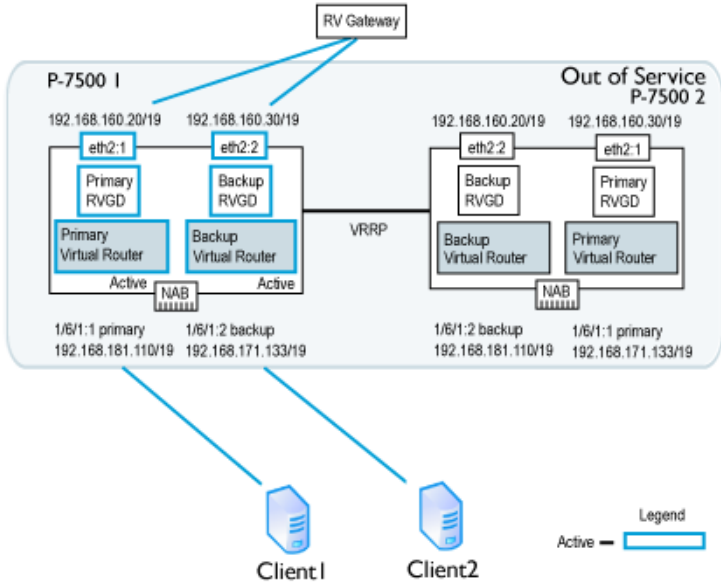
immediately establish new TCP sessions. These new connections are accepted by P-7500 1.

7. P-7500 1 accepts subscription updates and published messages from its own clients and those that typically have service from P-7500 2.

Recovery Activity Switch

Figure 11 illustrates a common recovery activity switch scenario, where system P-7500 2 has failed and its mate system, P-7500 1, is acting on behalf of P-7500 2.

Figure 11 Failure Activity Switch Behavior



Once P-7500 2 returns to the network, the following series of operations occur:

1. As P-7500 2 starts up, its primary virtual router uses a VRRP advertisement of Primary-Reconcile, and its backup virtual router uses a VRRP advertisement of Backup-Reconcile. These advertisements indicate that the virtual routers are initializing, but are not yet ready to take on client activity.
2. Once P-7500 2 has fully started, its primary virtual router increases the priority of its VRRP advertisements to Assert-Activity. This priority level causes the backup virtual router of its mate system to relinquish activity. P-7500 2 then sends a gratuitous ARP to let the other network services know it is taking over the IP address 192.168.171.133/19 for client connections.

3. P-7500 1 disconnects any TCP sessions that it had established for clients receiving service from IP address 192.168.171.133/19 and for RV messages flowing through eth2:2 on IP address 192.168.160.30/19.
4. The primary virtual router for P-7500 1 advertises a local priority level of Active, and the backup virtual router advertises a local priority level of Backup.

Note: Through the auto-revert Router Redundancy CONFIG command, the network administrator can configure whether the standby system in a redundancy pair should automatically revert back at this point to the primary when the primary comes back online after a service outage. Refer to "Enabling the Backup System to Automatically Revert Activity" on page 167 for details.

5. At this point, the redundancy state of P-7500 2 causes eth2:2 and the backup RVGD to become idle.
6. P-7500 2 accepts new TCP connections to IP address 192.168.171.133/19 and delivers messages to, and accepts messages from, clients using this IP address.
7. RV messages flowing through IP address 192.168.160.30/19 now use eth2:1 on P-7500 2..

Configuring Redundancy

You can use the active/active redundancy facility of the TIBCO Messaging Appliance P-7500 system to eliminate the potential for a single point of failure in a message routing network. Please start by reading and following the Prerequisites, and then following the "Steps to Configure Redundancy" on page 160.

Prerequisites

ALERT

ALERT! Before configuring redundancy on TIBCO Messaging Appliance P-7500 systems, read all of the following information:

1. Primary and backup IP interfaces must use valid IP addresses that are part of the same IP subnet. This requirement is not enforced by the system, but operation is unpredictable unless you meet this requirement.
2. The underlying signaling for TIBCO Messaging Appliance P-7500 redundancy is based on RFC 3768. Observe all precautions in RFC 3768 regarding VRRP Virtual Router Identifier (VRID) and uniqueness of protected addresses when configuring system redundancy. In particular, the vrrp-vrid must not conflict with a RFC 3768 VRRP VRID that is active on the same Local Area Network (LAN) segment.
3. Before you can configure redundancy on a P-7500 system, you must first stop Rendezvous services on that system.
4. The systems in a redundant pair must have equivalent physical interfaces configured. For example, if all of the physical interfaces for one system are configured in a single LAG, all of the physical interfaces for its mate should also be configured in a single LAG. This requirement is not enforced by the CLI.

Load Limitations

The enforced operating limits for a single P-7500 system are as follows:

- 6000 active connections
- 500 concurrent services
- 5 million unique subscriptions

- 10 million non-unique subscriptions

However, when P-7500 systems are used in a redundant pair, the total maximum load for the pair should be the same as that of a single P-7500 system operating in a non-redundant mode. As a result, the individual load allocated to each P-7500 system in a redundant pair should be much less than its potential, individual maximum load.

By limiting the maximum total load for a redundant pair to the same as that of a standalone system ensures that in a failover situation the active system has sufficient operating capacity to also handle the connections typically served by its mate.

Steps to Configure Redundancy

To configure an active/active redundancy pairing for two systems use the following procedure. The exact steps required may vary depending on your network conditions and preferred configuration.

The physical interfaces (or ports) on the NAB used by a P-7500 system can be configured as a single LAG, as independent ethernet ports with their own IP addresses, or as a combination of both (that is, some of the ports can be grouped into a LAG and the remainder addressed independently).

For more information on the configuration of physical interfaces on the NAB or the Command Line Interface (CLI) commands used in the following procedure, refer to Chapter 16, "Configuring IP Interfaces and Addresses".

NOTICE

NOTICE: Rendezvous clients communicate with the TIBCO Messaging Appliance P-7500 system through physical interfaces on the NAB (whether they are configured in a LAG or independently), while the Rendezvous Gateway communicates with other Rendezvous entities in the network through the eth2 interface on the system (once Rendezvous Gateway services are started). If you are using RV Gateway services, to facilitate low latency communications between the Rendezvous Gateway and TIBCO Messaging Appliance P-7500 system, configure the IP interfaces in the same IP subnet and connect the physical interfaces to the same Layer 2 network.

Perform these tasks on each P-7500 in a redundancy pair:

1. If you are configuring redundancy on an existing P-7500 system that uses Rendezvous services, stop Rendezvous services on the system:

```
tibco(config)# rv
tibco(config-rv)# shutdown
```

```
tibco(config-rv)# exit
```

2. If you want to use an independent IP interface on the NAB, from the Global CONFIG level, configure an independent IP interface and then start it:

   ```
   tibco(config)# create interface <phy-interface>
   tibco(config-interface)# no shutdown
   ```

   where <*ip-interface*> is an ASCII string specifying the ethernet interface port. Valid values are <fabric>/<slot>/<port> (for example, 1/1/8). There is no default value.

3. Repeat step 2 for each IP interface you want to configure. A maximum of eight independent physical interfaces are possible.

4. If you want to use a LAG on the NAB, enter the following:

   ```
   tibco(config)# create interface 1/1/lag1
   tibco(config-interface)# no shutdown
   ```

5. If you created a LAG in the proceeding step, enter the following for each port you want to include in the LAG group:

   ```
   tibco(config-interface)# member <fabric>/<slot>/<port>
   ```

   Each port must use a unique number from the available range (1-8).

6. If you created a LAG group in the proceeding steps, start it:

   ```
   tibco(config-interface)# no shutdown
   ```

7. Return to the Global CONFIG command level

   ```
   tibco(config-interface)# exit
   tibco(config)#
   ```

8. Go to the VRF IP CONFIG command level, create a primary IP interface for a physical interface on the NAB, and assign it an IP address:

   ```
   tibco(config)# ip vrf msg-backbone
   tibco(config-ip-vrf)# create interface <ip-interface> primary
   tibco(config-ip-vrf-interface)# ip-address <ip-addr>
   ```

   where <*ip-interface*> is an ASCII string specifying the ethernet interface port or LAG.

   where <*ip-addr*> is an IP address and network mask in Classless Inter-Domain Routing (CIDR) form: n.n.n.n/y (n is 0-255, y is 0-32).

   As the primary IP interface for this system, clients attempting to connect to this IP interface connect to this system when it is active. If this system goes out of service, clients connect to the same IP interface configured as the backup on the mate system.

9. Start the primary IP interface, and return to the VRF IP CONFIG command level:

   ```
   tibco(config-ip-vrf-interface)# no shutdown
   ```

```
tibco(config-ip-vrf-interface)# exit
```

10. Create a backup IP interface for the same physical interface on the NAB, and assign it an IP address:

```
tibco(config)# ip vrf msg-backbone
tibco(config-ip-vrf)# create interface <ip-interface> backup
tibco(config-ip-vrf-interface)# ip-address <ip-addr>
```

The IP interface type number used for the backup instance of the VRF Interface must differ from that used by the primary. For example, 1/1/lag1:1 primary and 1/1/lag1:2 backup.

This IP interface is used for client connections when the mate to this system is out of service.

11. Start the backup IP interface, and return to the VRF IP CONFIG command level:

```
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
```

12. Repeat step 8 to step 11 for each physical interface configured on the NAB.
13. If you need a route to reach clients, add a default IP route for VRF object msg-backbone:

```
tibco(config-ip-vrf)# route default <ip-addr>
```

where <*ip-addr*> is an IP address in CIDR form: n.n.n.n (n is 0-255).

14. Leave this command level, and go to the Global CONFIG command level to configure the primary virtual router:

```
tibco(config-ip-vrf)# exit
tibco(config-ip)# exit
tibco(config)# virtual-router primary
```

15. Assign the primary virtual router an RV interface:

```
tibco(config-virtual-router)# rv-interface <ip-interface>
```

where <*ip-interface*> is an ASCII string specifying an ethernet interface port or LAG on the NAB.

16. Assign the primary virtual router an IP interface over which the VRRP will be run and a VRRP VRID (Virtual Router Identifier):

```
tibco(config-virtual-router)# vrrp-interface <ip-interface>
tibco(config-virtual-router)# vrrp-vrid <vrid>
```

where <*ip-interface*> is an ASCII string specifying an ethernet interface port or LAG on the NAB.

where <*vrid*> is a value between 1 and 255 (this value must differ from the VRRP VRIDs being used by anything else on the local subnet; there is no default value).

The VRRP VRID for the primary virtual router must be the same as the VRRP VRID for the backup virtual router on the mate system.

17. Leave this command level, and go to the Router Redundancy CONFIG to configure the backup virtual router:

```
tibco(config-virtual-router)# exit
tibco(config)# virtual-router backup
```

18. Assign the backup virtual router an RV interface:

```
tibco(config-virtual-router)# rv-interface <ip-interface>
```

The IP interface type number used for the backup instance of the virtual router must differ from that used by the primary. For example, 1/1/lag1:1 primary and 1/1/lag1:2 backup.

19. Assign the backup virtual router an IP interface over which the VRRP will be run and a VRRP VRID:

```
tibco(config-virtual-router)# vrrp-interface <ip-interface-id>
tibco(config-virtual-router)# vrrp-vrid <vrid>
```

where <*ip-interface*> is an ASCII string specifying an ethernet interface port or LAG on the NAB.

where <*vrid*> is a value between 1 and 255 (this value must be different from the VRRP VRIDs being used by anything else on the local subnet; there is no default value).

The VRRP VRID for the backup virtual router must be the same as the VRRP VRID for the primary virtual router on the mate system.

20. Leave this command level, and go to the Global CONFIG command level:

```
tibco(config-virtual-router)# exit
```

21. If you are running RV Gateway services, configure the primary and backup eth2 interfaces.

```
tibco(config)# ip vrf management
tibco(config-ip-vrf)# interface eth2:1
tibco(config-ip-vrf-interface)# ip-address <ip-addr>
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# interface eth2:2
tibco(config-ip-vrf-interface)# ip-address <ip-addr>
tibco(config-ip-vrf-interface)# exit
```

```
tibco(config-ip-vrf)# exit
tibco(config-ip)# exit
```

where <*ip-addr*> is an IP address in CIDR form: n.n.n.n (n is 0-255).

22. Go to the Router Redundancy CONFIG command level, and start router redundancy:

```
tibco(config)# router redundancy
tibco(config-router-redundancy)# no shutdown
```

23. Go to the Rendezvous CONFIG command level, and restart the Rendezvous Service on this system:

```
tibco(config-router-redundancy)# exit
tibco(config-router)# exit
tibco(config)# rv
tibco(config-rv)# no shutdown
```

24. Leave the Rendezvous CONFIG command level:

```
tibco(config-rv)# exit
tibco(config)#
```

25. Repeat step 1 to step 24 for the mate system.

When you configure the primary and backup IP interfaces on the mate system, you must use the same IP addresses assigned to the first system, but in a reverse fashion, to ensure that redundancy protection is enabled. For example, if the system P-7500 1 uses 192.168.161.110/19 for its primary IP interface and 192.168.171.133/19 for its backup IP interface, P-7500 2 must use 192.168.171.133/19 for its primary IP interface and 192.168.161.110/19 for its backup IP interface.

You have completed this procedure. The two systems are now configured as an active/active redundancy pair.

If you are running Rendezvous Gateway services, the primary and backup RVGDs used on each P-7500 system must use the same configuration, but in a reverse fashion, to ensure that redundancy protection is enabled. For example, the configuration of the primary RVGD used on system P-7500 1 should match the configuration of the backup RVGD used on the mate system P-7500 2, and the configuration of the backup RVGD used on P-7500 1 should match the configuration of the primary RVGD used on P-7500 2. For more information on configuring RV Gateway services, refer to Chapter 3, "Managing TIBCO Rendezvous Tasks".

Sample Redundancy Configuration

The following example illustrates a redundancy configuration for a new P-7500 system. In this particular example, all the physical interfaces on NAB-0801ET are configured as a single LAG (lag1).

```
tibco# configure
tibco(config)# create interface 1/1/lag1
tibco(config-interface)# member 1/1/1
tibco(config-interface)# member 1/1/2
tibco(config-interface)# member 1/1/3
tibco(config-interface)# member 1/1/4
tibco(config-interface)# member 1/1/5
tibco(config-interface)# member 1/1/6
tibco(config-interface)# member 1/1/7
tibco(config-interface)# member 1/1/8
tibco(config-interface)# no shutdown
tibco(config-interface)# exit
tibco(config)#
tibco(config)# ip vrf msg-backbone
tibco(config-ip-vrf)# create interface 1/1/lag1:1 primary
tibco(config-ip-vrf-interface)# ip-address 192.168.160.180/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# create interface 1/1/lag1:2 backup
tibco(config-ip-vrf-interface)# ip-address 192.168.164.183/19
tibco(config-ip-vrf-interface)# no shutdown
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# route default 192.168.160.1
tibco(config-ip-vrf)# exit
tibco(config-ip)# exit
tibco(config)# virtual-router primary
tibco(config-virtual-router)# rv-interface 1/1/lag1:1
tibco(config-virtual-router)# vrrp-interface 1/1/lag1:1
tibco(config-virtual-router)# vrrp-vrid 80
tibco(config-virtual-router)# exit
tibco(config)# virtual-router backup
tibco(config-virtual-router)# rv-interface 1/1/lag1:2
tibco(config-virtual-router)# vrrp-interface 1/1/lag1:2
tibco(config-virtual-router)# vrrp-vrid 83
tibco(config-virtual-router)# exit
```

Step 1: Create the IP Interfaces on the NAB

Step 2: Create the primary IP interface

Step 3: Create the backup IP Interface

Step 4: Configure the default IP route for the VRF object msg-backbone

Step 5: Configure the primary virtual router

Step 6: Configure the backup virtual router

```
tibco(config)#
tibco(config)# ip vrf management
tibco(config-ip-vrf)# interface eth2:1
tibco(config-ip-vrf-interface)# ip-address 192.168.162.80/19
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# interface eth2:2
tibco(config-ip-vrf-interface)# ip-address 192.168.162.83/19
tibco(config-ip-vrf-interface)# exit
tibco(config-ip-vrf)# exit
tibco(config-ip)# exit
tibco(config)# router redundancy
tibco(config-router-redundancy)# no shutdown
tibco(config-router-redundancy)# exit
tibco(config-router)# exit
tibco(config)# rv
tibco(config-rv)# no shutdown
tibco(config-rv)# exit
tibco(config)#
```

Step 7: If you are using RV services, configure eth2:1 and eth2:2.

Step 8: Start router redundancy

Managing Redundancy

To make changes to the redundancy configuration of a P-7500 system, you must stop redundancy on that system. In addition to stopping and starting a P-7500 system, you can restore the default redundancy configuration of a P-7500 system.

Both the redundancy facility and Rendezvous services must be turned off before any commands other than the release-activity Router Redundancy CONFIG command are run. The redundancy facility is turned off by default.

Starting Redundancy

The no shutdown Router Redundancy CONFIG command starts the redundancy facility on the P-7500 system. You can use this command to restart redundancy after changing any redundancy settings for the system.

The redundancy facility is turned off by default.

```
tibco# configure
tibco(config)# router redundancy
tibco(config-router-redundancy)# no shutdown
```

Rendezvous services on a system must be shutdown before redundancy can be started for that system.

Stopping Redundancy

The shutdown Router Redundancy CONFIG command stops the redundancy facility on the P-7500 system. You can use this command to stop the redundancy facility, which is required to make changes to the system's redundancy settings.

```
tibco# configure
tibco(config)# router redundancy
tibco(config-router-redundancy)# shutdown
```

Rendezvous services on a system must be shutdown before its redundancy configuration can be changed.

Restoring Default Redundancy Settings

The no redundancy Router Redundancy CONFIG command removes all of the currently configured redundancy configuration settings for a P-7500 system and restores the default redundancy settings:

```
tibco# configure
tibco(config)# router
tibco(config-router)# no redundancy
```

Enabling the Backup System to Automatically Revert Activity

The auto-revert Router Redundancy CONFIG command enables the backup P-7500 system to automatically revert activity back to the primary system (provided the mate system is available, otherwise an error message is received):

```
tibco(config)# router redundancy
tibco(config-router-redundancy)# auto-revert
```

The no version (no auto-revert) disables the backup system from automatically giving up activity, even when the mate system is ready to provide service to the messaging clients.

When auto revert is disabled (system default), the backup system does not automatically give up activity, even if the mate router is ready to provide service to the messaging clients. When disabled, activity only reverts back to the primary system if any one of the following occurs:

- the backup system fails
- the redundancy revert-activity Admin EXEC command is run on the backup system
- the release-activity Router Redundancy CONFIG command is run on the backup system

Forcing a Redundancy Switch on the Backup System

The redundancy revert-activity Admin EXEC command administratively forces a P-7500 system acting as backup in a redundant system pair to give up service (provided the mate system is available, otherwise an error message is received):

```
tibco# admin
tibco(admin)#
tibco(admin)# redundancy revert-activity
```

Optimizing Activity Switch Performance During Maintenance

During maintenance on redundant P-7500 pairs, always switch activity to the one system before performing service-interrupting activities. This optimizes switch activity performance.

For example, enter and run the release-activity Router Redundancy CONFIG command to surrender activity to the backup system before entering any of these commands:

- the reload Privileged EXEC command (to restart one of the paired systems)
- the boot Privileged EXEC command (to upgrade or downgrade P-7500 software on one of the paired systems)
- the power-down Privileged EXEC command (to turn off power to one of the paired systems)

Note: Remember to enter and run the no release-activity Router Redundancy CONFIG command on the primary system once maintenance on the redundant system pair is completed to return activity back to the active system.

Monitoring Redundancy

You can use a show command to monitor the redundancy configuration and status on P-7500 systems.

show redundancy

To view the redundancy configuration and status on a P-7500 system, enter the show redundancy User EXEC command:

```
tibco> show redundancy
```

Example:

```
tibco> show redundancy

Configuration Status:     Enabled
Auto Revert:              No
VRRP Interface Status:    Up

                          Primary CVRID          Backup CVRID
                          ---------------------  ---------------------
CSMP Virtual Router Id    192.168.160.174:80     192.168.160.154:80
Activity Statu            Local Active           Mate Active
VRRP Status               Master                 Backup
Local Priority            Active                 Standby
Primary Router            192.168.160.74:80      154
VRRP Virtual Router Id    174
Last Update Status        OK                     OK
```

When no parameters are entered, a configuration status summary is displayed, using these terms:

Enabled — indicates that the operator entered the no shutdown Router Redundancy CONFIG command through the P-7500 CLI to start the redundancy facility on the system.

Shutdown — indicates that the operator entered the shutdown Router Redundancy CONFIG command through the P-7500 CLI to stop the redundancy facility on the system.

Released — indicates that the operator entered the release-activity Router Redundancy CONFIG command through the P-7500 CLI to surrender activity to the backup system for the primary CVRID.

The information listed in Table 14 describes the general status items for the system's virtual routers:

Table 14 General Status Items

Item	Description	Values
Activity Status	Indicates whether the activity status of the virtual router for its assigned state (primary or backup).	Local Active Mate Active
VRRP Status	Indicates whether the virtual router is a primary or backup.	Master Backup
Local Priority	The priority the virtual router is announcing for the primary VRID.	Assert Activity Active Standby Primary-Reconcile Backup-Reconcile Release

The information listed in Table 15 describes the possible Local Priority Values. These values are sent between virtual routers by VRRP so that each virtual router is aware of its mate's status.

Table 15 Local Priority Levels

Level	Description
Assert-Activity	The priority level the virtual router uses when it wants to assert itself as the "master" of the VRID. After a timeout period, when the virtual router is sure that the mate router does not claim to be the "master", the local priority value for the virtual router is reduced to Active.
Request-Activity	The priority level the virtual router uses when it wants to request that it be the "master" of the VRID.
Active	The normal priority level to indicate that the virtual router is currently active.
Standby	The priority level that a backup virtual router uses to advertise that it is not currently active, but it is capable of taking activity if the primary virtual router becomes unavailable.

Table 15 Local Priority Levels

Level	Description
Primary-Reconcile	The priority level that a virtual router uses on start up, to ensure that it does not take activity before it is ready.
Backup-Reconcile	The priority level that a backup virtual router uses to indicate that it is initializing, and it will not be able to take activity even if the primary virtual router is unavailable.
Release	The priority level that a virtual router uses to indicate that it is no longer willing to act on behalf of the IP address. This priority level is advertised when the release-activity Router CONFIG command is used. It is also the priority advertised for the backup virtual router whenever the redundancy feature is shutdown on the virtual router.

Chapter 10 Managing Rendezvous Client Queues

This chapter describes:

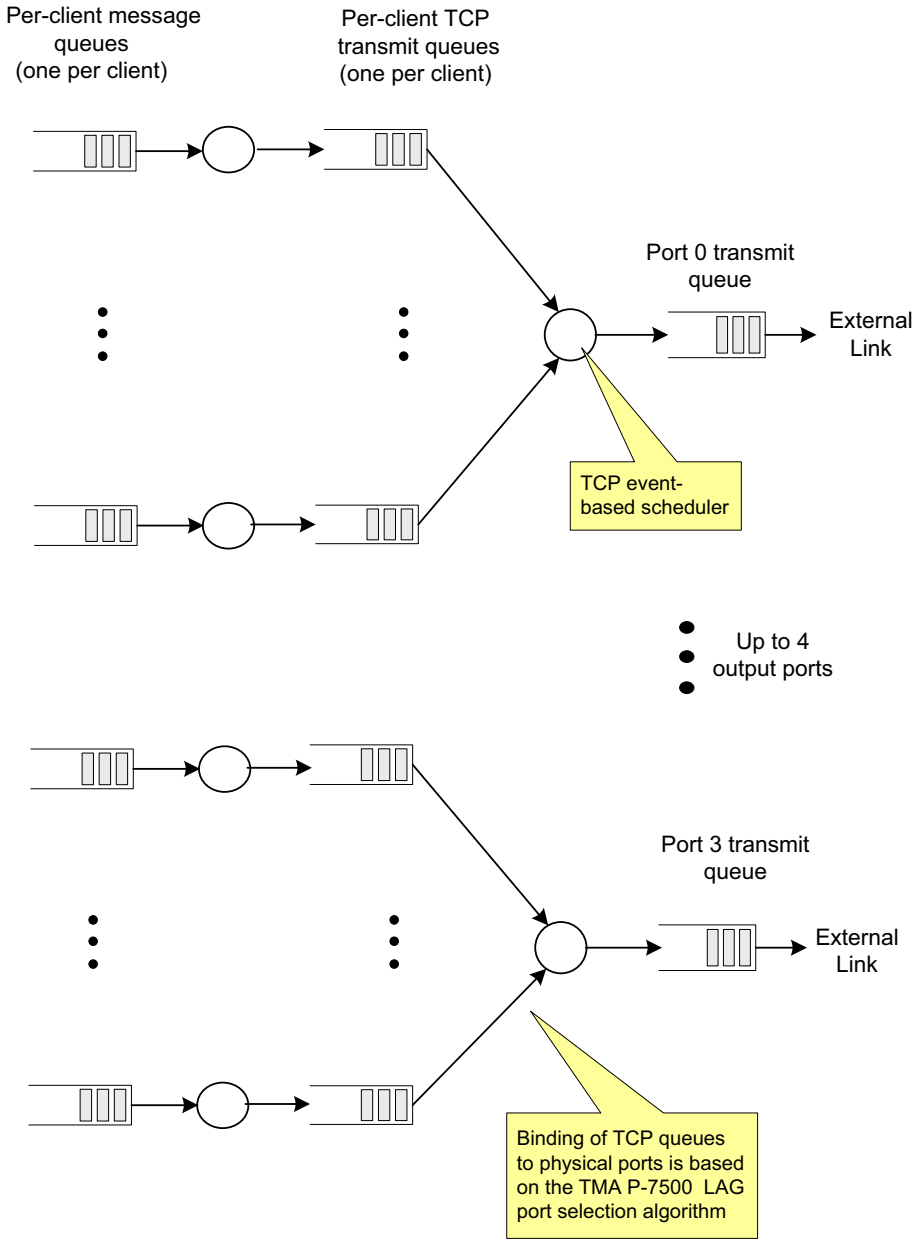
- the client egress queuing structure of TIBCO Messaging Appliance P-7500 systems
- the Command Line Interface (CLI) commands used to configure either the egress client message queues or the TCP transmit queues on P-7500 systems

Topics

Functional Description

During the delivery of a routed message to a client, the message passes through the queuing structure shown in Figure 12.

Figure 12 Client Egress Queue Hierarchy



The message first passes through the application message queue to the TCP transmit queue. A scheduler then selects it from the TCP transmit queues and places the message into a TCP send queue.

The act of enqueuing the message triggers the TCP stack to evaluate if the connection can send more data from that queue. If the TCP stack determines that it is acceptable to send data on the TCP connection, then data from the message is copied to a per-port transmit queue on the way to the Ethernet interface. The data remains on the TCP queue until it is acknowledged by the client through a TCP ACK message.

The per-port transmit queue is not strictly bounded in depth. However, its total depth never exceeds:

- the maximum amount of unacknowledged TCP data for all active TCP connections
- plus a few additional buffers for low-level protocols like ARP and Link Aggregation Group (LAG)

Note: For more information on LAGs, refer to Configuring 802.3ad Link Aggregation on page 13.

The per-client TCP transmit queues have a configurable maximum depth, measured in bytes. When a transmit queue is full, no more data is taken from the message queues.

The per-client message queues also have a configurable maximum depth, measured in work units of 2048 bytes. When these queues become full, messages are discarded, and the dataplane statistic for Transmit Congestion--Slow Consumer is incremented.

Per-client TCP Queues

Each active client has one TCP queue for message delivery.

The TCP queue holds data that is either waiting for delivery out of the P-7500, or is data that has already been sent, but is waiting for acknowledgement.

Before messages are placed in the TCP queue, the current depth of the TCP queue is checked against its configured maximum. If the current depth of the TCP queue is less than its maximum, the entire message is placed on the queue. This can cause the TCP queue to temporarily exceed its configured maximum depth. If the depth is at or greater than the maximum depth, the message is left on the per-client message queues. When a message is placed on the TCP queue, the exact byte length of that message is added to its current depth.

Per-port Transmit Queues

Each active client has one transmit queue for message delivery. The transmit queue holds data that is waiting on the hardware to send data out of one of the four Ethernet ports.

While the size of the per-port transmit queues is not configurable, the P-7500 ensures that ingress traffic cannot be affected by too many buffers in this queuing point.

For TCP connections, the TCP windows of the connections limit the number of buffers that can be on per-port transmit queues.

Configuring Client Queues

ALERT

ALERT! Always contact TIBCO for technical support before you attempt to configure any client queue on a P-7500. Failure to do so may result in data loss or service interruption due to unwanted secondary effects on system performance from use of the Client Profile Queue CONFIG level within the CLI.

To configure egress client message queues or the TCP transmit queues on P-7500 systems, you enter the Client Profile CONFIG level for a named profile. The only client profile currently supported is named default.

Next, you enter queue *type* at the Client Profile CONFIG level to move to the Client Profile Queue CONFIG level, where *type* is the queue type to be configured. The only queue type currently supported is egress. Here is an example:

```
tibco(config)# client-profile default
tibco(config-client-profile)# queue egress
tibco(config-client-profile-queue)#
```

Now you are at a level where you can configure parameters for the egress queue of the default client profile. You can set the maximum queue depth and minimum burst length tolerance for the per-client message queues.

Note: For more information on clients and client profiles, refer to Chapter 2, Managing TIBCO Rendezvous Tasks, on page 21.

max-depth

Each per-client message queue has an associated maximum depth. The depths are measured in work units, each work unit representing 2048 bytes of a message. The formula to convert a message size to number of work units is:

NumWorkUnits = *CEILING*(*message.length*/2048)

Before a new message is placed on the message queue, its depth in work units is checked against the maximum depth set for the queue. If the current depth is less than the maximum, the message is placed on the queue regardless of the number of work units that the message needs, even if it causes the queue to exceed its maximum depth.

Messages that are received when the depth is greater or equal to the maximum are discarded, and also get counted as a Transmit Congestion--Slow Consumer dataplane statistic.

To configure the maximum depth of the specified queue, enter:

tibco(config-client-profile-queue)# max-depth *depth*

where *depth* is the integer value representing the queue depth in KB for the number of work units for the client message queues. Valid range is 50 to 262144 for client message queues. Default is 100000 work units for the client message queues. Changing this value does not affect messages already successfully placed on the queue.

Note: The no version of this command (no max-depth) resets the queue depth to the default of 100000 work units.

min-msg-burst

Minimum burst length tolerance is used to ensure that messages are not lost when bursts of very large messages are received on a client egress queue. It specifies the number of messages per queue that are always allowed, regardless of the queue's current maximum depth setting.

For example, in a case where there are three messages currently on a queue, and the minimum burst length tolerance of the queue is set to 4, one more message is allowed to be placed on the queue, regardless of whether the three current messages have filled the queue past its maximum depth. The minimum burst length tolerance setting of 4 allows the queue to temporarily exceed its maximum depth by always allowing the 4th message to be placed on the queue, regardless of its current depth and maximum depth setting.

To configure the minimum number of messages that must be on a client message queue before the queue's depth is checked against the maximum depth setting, enter:

tibco(config-client-profile-queue)# min-msg-burst *depth*

where *depth* is the integer value representing the queue burst depth in messages. Valid range is 0 to 262144. The default is 4. Changing this value does not affect messages already successfully placed on the queue.

The no version of this command (no min-msg-burst) resets the minimum burst length tolerance in messages to the default of 4.

Chapter 11 Network Acceleration Blade

The TIBCO Network Acceleration Blade (NAB) is a hardware line card for the TIBCO Messaging Appliance P-7500 system. The NAB provides hardware-based protocol termination and acceleration of numerous system datapath functions, and provides data buffering protection for TCP connections. The NAB is intended to support network applications requiring:

- high throughput
- high fanout
- low latency

The NAB is available in the following versions:

- The NAB-0210EM supports up to two 10 Gigabit Ethernet (10GigE) interfaces configured through Small Form-factor Pluggable+ (SFP+) modules with LC connectors. It occupies the first slot of the Fabric Expansion Cartridge (FEC).
- The NAB-0801ET supports up to eight GigE interfaces through RJ-45 connectors only. It occupies the first two slots of the FEC.

The NAB supports 802.3ad link aggregation, multiple IP Addresses, or a mixture of both on an interface. Refer to Chapter 8, Configuring IP Interfaces and Addresses for details.

The TIBCO Messaging Appliance P-7500 system supports one NAB.

Topics

NAB-0210EM

This section provides the following information for NAB-0210EM:

SFP+ Modules

NOTICE

NOTICE: Only optical SFP+ modules work on NAB-0210EM. Ensure the network switch is set to 10 Gbps Full Duplex and **disable** autonegotiation.

The interfaces on NAB-0210EM are two 10GigE SFP+ optical module ports that provide flexibility and convenience in connecting to a wide array of 10GigE devices.

The NAB-0210EM comes equipped with 10GBase-SR SFP+ modules that provide a 10 Gbps optical GigE connection to a network through an 850nm (SR) fiber-optic link using an LC physical connector.

Note: To determine the type of SFP+ modules installed in a NAB-0210EM, enter the show interface User EXEC command, and observe the displayed "Media type" value returned for the physical interfaces 1/1/1 and 1/1/2. A value of 10GE SR represents the 10GBase-SR SFP+ module. The SFP+ modules do not support speeds other than 10 Gbps.

The NAB-0210EM 10GBase-SR SFP+ modules are field-replaceable, hot-swappable, and provide uplink interfaces when inserted into the SFP+ ports of the NAB?thereby linking the P-7500 systems with the backbone network.

Use fiber-optic cables with LC connectors (Figure 13) to connect to the 10GBase-SR SFP+ modules.

Figure 13 Fiber Optic LC Connector

The NAB-0210EM comes equipped with 10GBase-SR SFP+ modules that provide a 10 Gbps optical GigE connection to a network through an 850nm (SR) fiber-optic link using an LC physical connector.

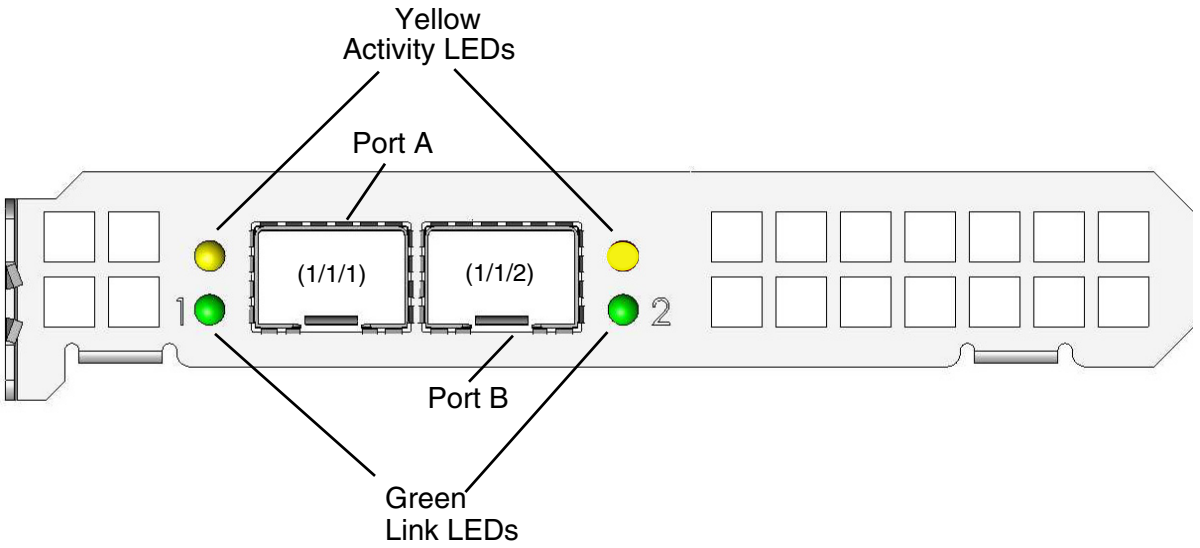
Note: To determine the type of SFP+ modules installed in a NAB-0210EM, enter the show interface User EXEC command, and observe the displayed "Media type" value returned for the physical interfaces 1/1/1 and 1/1/2. A value of 10GE SR represents the 10GBase-SR SFP+ module. The SFP+ modules do not support speeds other than 10 Gbps.

Faceplate LEDs

As shown in Figure 14, NAB-0210EM has two faceplate LEDs on each of the SFP+ module ports to indicate their link and activity status as reported by NAB-0210EM:

- the green link LED indicates network connectivity when on
- the yellow activity LED indicates receive activity when blinking

Figure 14 SFP+ Module Port Locations on NAB-0210EM



Connecting to 10GBase-SR Devices

The 10GBase-SR SFP+ modules on NAB-0210EM have LC connectors for optical fiber connections using shortwave laser optics over multimode optical fiber (MMF) cable.

Refer to Table 16 for LC multimode optical fiber cables specifications for 10Gbase-SR ports.

Note: Fiber optic cabling characteristics are defined in IEC 60793-2:1992 (A1a, A1b, and B1) and IEEE 802.3-2002 Clause 38.11.

Table 16 LC Multimode Optical Fiber Cable Specifications for 10GBase-SR

Parameter	Specification
Connector type	LC
Cable type	
10GBase-SR	MMF with 50 µm core diameter
Maximum cable distance	

Table 16 LC Multimode Optical Fiber Cable Specifications for 10GBase-SR

Parameter	Specification
50 um core diameter	980 ft. (300 m)

Inserting and Removing SFP+ Modules

This section describes how to insert and remove SFP+ modules from NAB-02010EM.

The modules can have any of three different types of latching devices to secure and detach themselves from a NAB port. The three types of latching devices used with SFP+ modules are:

- Mylar Tab
- Actuator/Button

- Bale-Clasp

ALERT! Protect your optical SFP+ modules by inserting clean dust plugs into them after the fiber cables are extracted from them. Be sure to clean the optic surfaces of the fiber cables before you plug them back into the optical bores of another SFP+ module. Avoid getting dust and other contaminants into the optical bores of your SFP+ modules as the optics do not work correctly when obstructed with dust.

ALERT!

- Always follow ESD prevention procedures when removing or inserting SFP+ modules and their components. Use an antistatic wrist strap, or another antistatic device. If no wrist strap or mat is available, ground yourself by touching the metal part of the router chassis.
- Always wear a grounded wrist strap when working on the router equipment.
- Treat all assemblies, components, and interface connections as static-sensitive.
- Avoid working in carpeted areas and keep body movement to a minimum while removing or installing SFP+ modules to minimize buildup of static charge.

ALERT! When hot swapping SFP+ modules, allow at least 15 seconds for the router to reinitialize the port. Also, note the current configuration of all interfaces before you remove or insert another SFP+ module so that you can revert back if necessary.

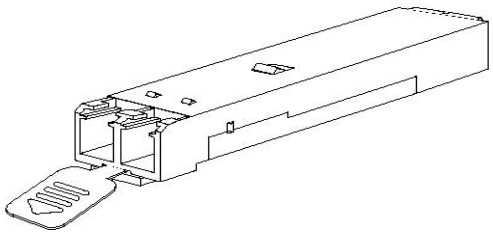
Mylar Tab SFP+ Modules

WARNING

WARNING! Invisible laser radiation may be emitted from disconnected optical fibers or connectors. Do not look into fiber or connectors or view directly with optical instruments.

The Mylar tab SFP+ module (Figure 15) has a tab that you must pull to remove the module from a NAB port.

Figure 15 Mylar Tab SFP+ Module



To insert a Mylar tab SFP+ module into a NAB port, follow this procedure:

1. Line up the SFP+ module with the port, with the printed label facing up.

ALERT

ALERT! Do not remove the rubber protectors on the end of optical SFP+ modules until they are installed and ready for cable connection and use. This is to avoid getting dust and other contaminants into the optical bores of your SFP+ modules as the optics do not work correctly when obstructed with dust.

2. Gently slide the SFP+ module into the port.
3. Gently press the SFP+ module into the port until it is firmly seated.
4. Connect the cable.

You have completed this procedure.

To remove a Mylar tab SFP+ module from a NAB port, follow this procedure:

1. Remove the cable connected to the SFP+ module, if any.
2. Grasp the Mylar tab between your thumb an index finger.

3. Carefully pull towards you, in a straight outward motion, the SFP+ module from the port.

ALERT

ALERT! When pulling the Mylar tab to remove the SFP+ module, be sure to pull in a straight outward motion so that you remove the module from the port in a parallel direction. Do not twist the Mylar tab while puling because you may disconnect it from the SFP+ module.

You have completed this procedure.

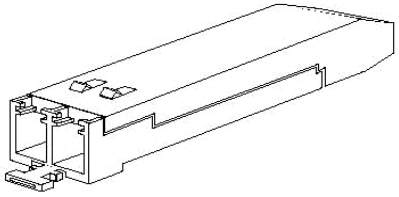
Actuator/Button SFP+ Modules

WARNING

WARNING! Invisible laser radiation may be emitted from disconnected optical fibers or connectors. Do not look into fiber or connectors or view directly with optical instruments.

The actuator/button SFP+ module (Figure 16) has a button that you must push to remove the module from a NAB port.

Figure 16 Actuator/Button SFP+ Module



To insert an actuator/button SFP+ module into a NAB port, follow this procedure:

1. Line up the SFP+ module with the port, with the printed label facing up.

ALERT

ALERT! Do not remove the rubber protectors on the end of optical SFP+ modules until they are installed and ready for cable connection and use. This is to avoid getting dust and other contaminants into the optical bores of your SFP+ modules as the optics do not work correctly when obstructed with dust.

2. Gently slide the SFP+ module into the port until the actuator/button clicks into place.

Note: Be careful not to press the actuator/button as you insert the SFP+ module because you may inadvertently disengage the module from the port.

3. Connect the cable.

You have completed this procedure.

To remove an actuator/button SFP+ module from a NAB port, follow this procedure:

1. Remove the cable connected to the SFP+ module, if any.
2. Gently press the actuator/button on the front of the SFP+ module until it clicks and the latch mechanism activates, releasing the module from the port.
3. Grasp the actuator/button between your thumb and index finger, and carefully pull the SFP+ module towards you out from the port.

You have completed this procedure.

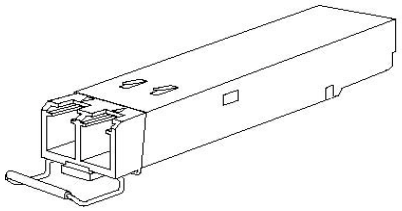
Bale-Clasp SFP+ Modules

WARNING

WARNING! Invisible laser radiation may be emitted from disconnected optical fibers or connectors. Do not look into fiber or connectors or view directly with optical instruments.

The bale-clasp SFP+ module (Figure 17) has a bale clasp that you use to secure the module in a NAB port.

Figure 17 Bale-Clasp SFP+ Module



To insert a bale-clasp SFP+ module into a NAB port, follow this procedure:

1. Close the bale-clasp before inserting the SFP+ module.
2. Line up the SFP+ module with the port, with the printed label facing up.

ALERT

ALERT! Do not remove the rubber protectors on the end of optical SFP+ modules until they are installed and ready for cable connection and use. This is to avoid getting dust and other contaminants into the optical bores of your SFP+ modules as the optics do not work correctly when obstructed with dust.

3. Gently slide the SFP+ module into the port.
4. Gently press the SFP+ module into the port until it is firmly seated.
5. Connect the cable.

You have completed this procedure.

To remove a bale-clasp SFP+ module from a NAB port, follow this procedure:

1. Remove the cable connected to the SFP+ module, if any.
2. Open the bale clasp on the SFP+ module with your index finger in a downward direction.

Note: If the bale clasp is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the bale clasp.

3. Grasp the SFP+ module between your thumb and index finger, and carefully pull the module towards you out from the port.

You have completed this procedure.

NAB-0801ET

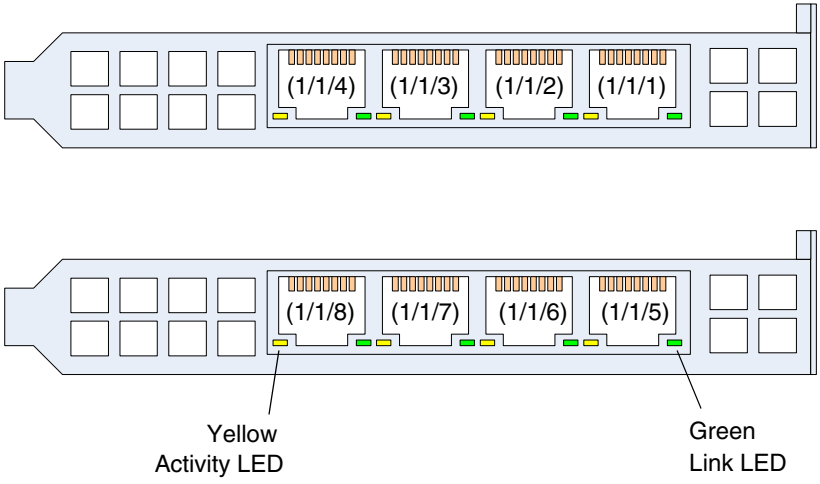
This section provides the following information for NAB-0801ET:

Faceplate LEDs

As shown in Figure 18, NAB-0801ET has two faceplate LEDs on each of the eight RJ-45 Ethernet ports to indicate their link and activity status as reported by the NAB:

- the green link LED indicates network connectivity when on
- the yellow activity LED indicates receive activity when blinking

Figure 18 Ethernet Port Locations on NAB-0801ET



Electrical GigE Wiring Specifications

The eight network interfaces on NAB-0801ET come with RJ-45 ports for the following standard unshielded twisted pair cable connections:

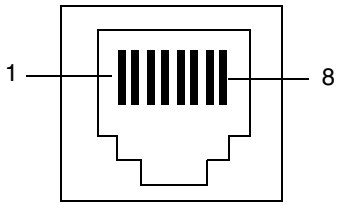
- 100 Mbps baseband Ethernet: two pairs of CAT-3 unshielded twisted pair cable required

- 1000 Mbps baseband Ethernet: four pairs of CAT-5 unshielded twisted pair cable required

Note: In all cases cable length should not exceed 330 feet (100 meters).

Refer to Table 17 for RJ-45 pin assignment and signaling for 100BaseTX and 1000BaseT ports.

Table 17 RJ-45 Pin Assignment and Signaling for 100BaseTX and 1000BaseTX Ports

RJ-45 Port Pin Assignment	Pin Number	100 BaseTX Ports	1000 BaseTX Ports
	1	RD+	A+
	2	RD-	A-
	3	TD+	B+
	4	CMT	C+
	5	CMT	C-
	6	TD-	B-
	7	CMT	D+
	8	CMT	D-

NAB Data Buffering Protection for TCP Connections

The NAB provides data buffering protection against a small number of TCP connections consuming an undue number of internal buffers or service time, where such consumption could degrade service to other TCP connections. This data buffering protection applies to ingress and egress TCP connections on the P-7500 system.

Ingress TCP Data Protection

If the NAB detects that a backlog of at least 5k buffers has built up in the system's message processing stage, and there is received data ready for processing on more than one TCP connection, the NAB gives a higher service priority to TCP connections that have been recently sending data to the NAB at a lower-than-average rate over TCP connections than to those that have been recently sending data to the NAB at a higher-than-average rate.

While this data buffering protection applies to all TCP connections, it is most typically used against clients that are sending data to the NAB at a rate that is disproportionately consuming NAB resources.

If the NAB detects that a backlog of at least 10k buffers has built up in the system's message processing stage, the NAB momentarily defers service of all ingress TCP data, to limit the ingress data rate to a level that the P-7500 can service.

In either case, when the NAB stops servicing ingress TCP data on some or all TCP connections, the peer TCP client limits its sending rate and, if necessary, applies back pressure to the sending client application.

Egress TCP Data Protection

If the NAB detects that more than 70% of its allotted egress buffers are in use, and there are some TCP connections which have had backlogged egress data more than 88% of the time in at least the preceding minute, those TCP connections are disconnected and their buffers are freed.

While this protection applies to all TCP connections, it is most typically used against clients that are unable to process the volume of data sent to them as a result of their subscriptions.

Chapter 12 Topic Routing Blade

The TIBCO Topic Routing Blade (TRB) is a hardware module which performs subject-based message routing for TIBCO Rendezvous clients through the TIBCO Messaging Appliance P-7500 system.

The TRB provides the subject-based message routing functionality for Rendezvous clients through customized hardware implemented using Field Programmable Gate Array (FPGA) technology that removes skew and jitter from time-sensitive data applications for:

- high throughput
- low latency
- operational predictability

The TIBCO Messaging Appliance P-7500 system supports one TRB.

Topics

Features

The TRB provides these performance benefits for the P-7500 and Rendezvous clients:

- supports traditional subject-based message routing at throughput rates greater than 10 million subject matches per second
- interacts with the TIBCO Network Acceleration Blade (NAB) to support ultra-low latency for subject-based messaged routing. This all-hardware data path facilitates latency that is:
  - measured in the tens of microseconds
  - low and deterministic even during periods of data bursts and volatility
- provides operational predictability for time-sensitive Rendezvous client data applications through FPGA technology
- supports up to 10 million Rendezvous client network subscriptions

Monitoring Topic Routing Blades

To monitor the blade status and performance for a P-7500, you can use the show hardware command. The show hardware User EXEC command displays the serial number, firmware versions, and error counts for all of the TRBs installed in the system:

```
tibco> show hardware [detail]
```

where detail asks to show detailed information about the P-7500 system.

This is a sample output for the show hardware User EXEC command for a P-7500 system equipped with a TRB and NAB:

```
tibco> show hardware
Platform: TIBCO Messaging Appliance P-7500
Chassis Product #: CHS-3260XX-01-A
Chassis revision:  1.1
Chassis serial:    S000000002
Power Redundancy:  2 + 2

Disk 1:
  Serial #: 9QE4TZ4F

Fabric 1:
Product #: CHS-FC1040-01-A
 Slot 1/1: Network Acceleration Blade
   Product #:          NAB-0801ET-01-A
   Serial #:           K002327730
   Assembly Number:    10000893
   Assembly Revision:  1.4
   Firmware version:   1.17b.347
   MAC Address for 1/1/1: 00:50:c2:44:bf:54
   MAC Address for 1/1/2: 00:50:c2:44:bf:55
   MAC Address for 1/1/3: 00:50:c2:44:bf:56
   MAC Address for 1/1/4: 00:50:c2:44:bf:57
   MAC Address for 1/1/5: 00:50:c2:44:bf:50
   MAC Address for 1/1/6: 00:50:c2:44:bf:51
   MAC Address for 1/1/7: 00:50:c2:44:bf:52
   MAC Address for 1/1/8: 00:50:c2:44:bf:53

 Slot 1/2: in use by slot 1/1

 Slot 1/3: empty

 Slot 1/4: empty

 Slot 1/5: Topic Routing Blade
   Product #:          TRB-000000-01-A
   Serial #:           01385600
   Assembly Revision : 1.4
```

This is a sample output for the show hardware detail User EXEC command for a P-7500 equipped with a TRB and NAB:

```
tibco> show hardware detail
Platform: TIBCO Messaging Appliance P-7500
Chassis Product #: CHS-3260XX-01-A
Chassis revision:  1.1
Chassis serial:    S000000002
Board serial:      QSSL73900819
Board Part Number: D44771-805
Board Version:     Not Specified
BIOS Version:      S5000.86B.10.00.0085.112920071426
CPU1 Version:      Intel(R) Xeon(R) CPU          E5450  @ 3.00GHz
CPU2 Version:      Intel(R) Xeon(R) CPU          E5450  @ 3.00GHz
Power Redundancy:  2 + 2

Disk 1:
  Serial #: 9QE4TZ4F

Fabric 1:
Product #: CHS-FC1040-01-A
 Slot 1/1: Network Acceleration Blade
   Product #:          NAB-0801ET-01-A
   Serial #:           K002327730
   Assembly Number:    10000893
   Assembly Revision:  1.4
   Firmware version:   1.17b.347
   MAC Address for 1/1/1: 00:50:c2:44:bf:54
   MAC Address for 1/1/2: 00:50:c2:44:bf:55
   MAC Address for 1/1/3: 00:50:c2:44:bf:56
   MAC Address for 1/1/4: 00:50:c2:44:bf:57
   MAC Address for 1/1/5: 00:50:c2:44:bf:50
   MAC Address for 1/1/6: 00:50:c2:44:bf:51
   MAC Address for 1/1/7: 00:50:c2:44:bf:52
   MAC Address for 1/1/8: 00:50:c2:44:bf:53

 Slot 1/2: in use by slot 1/1

 Slot 1/3: empty

 Slot 1/4: empty

 Slot 1/5: Topic Routing Blade
   Product #:          TRB-000000-01-A
   Serial #:           01385600
   Assembly Revision : 1.4
```