TIBCO Messaging Appliance™ P-7500

Concepts

Software Release 8.7
August 2012

two-second advantage™

TIBCO®
The Power of Now®

Important Information

Contents

Figures

Preface

TIBCO Messaging Appliance™ P-7500 implements TIBCO Rendezvous® messaging semantics in accelerated hardware.

This book contains information for system administrators, network administrators and IT managers.

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 TIBCO Messaging Appliance P-7500 systems required
- that these TIBCO Messaging Appliance 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 Documentation

These documents form the TIBCO Messaging Appliance documentation set:

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

Other TIBCO Documentation

For detailed information about TIBCO Rendezvous®, see the documentation set for that product.

Typographical Conventions

The following typographical conventions are used in this manual.

Table 1 General Typographical Conventions

Convention	Use
TIBCO_HOME	All TIBCO products are installed under the same directory. This directory is referenced in documentation as *TIBCO_HOME*. The value of *TIBCO_HOME* depends on the operating system. For example, on UNIX systems, the default value is `/tibco`.
`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.
	The note icon indicates information that is of special interest or importance, for example, an additional action required only in certain circumstances.

Table 1 General Typographical Conventions (Cont'd)

Convention	Use
	The tip icon indicates an idea that could be useful, for example, a way to apply the information provided in the current section to achieve a specific result.
	The warning icon indicates the potential for a damaging situation, for example, data loss or corruption if certain steps are taken or not taken.

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 Introduction

This chapter presents an overview of TIBCO Messaging Appliance™ P-7500, and its integration with other TIBCO Rendezvous® products.

Topics

Product Overview

TIBCO Messaging Appliance P-7500 provides TIBCO Rendezvous® message semantics and Rendezvous daemon functionality with high throughput, ultra-low latency and high scalability.

Client Connections

From the perspective of Rendezvous client applications, P-7500 acts as remote daemon. Clients connect to P-7500 using TCP/IP.

Benefits

This section outlines several use cases for TIBCO Messaging Appliance P-7500.

Scaling

You can use P-7500 to increase throughput capacity while reducing operating costs.

Performance

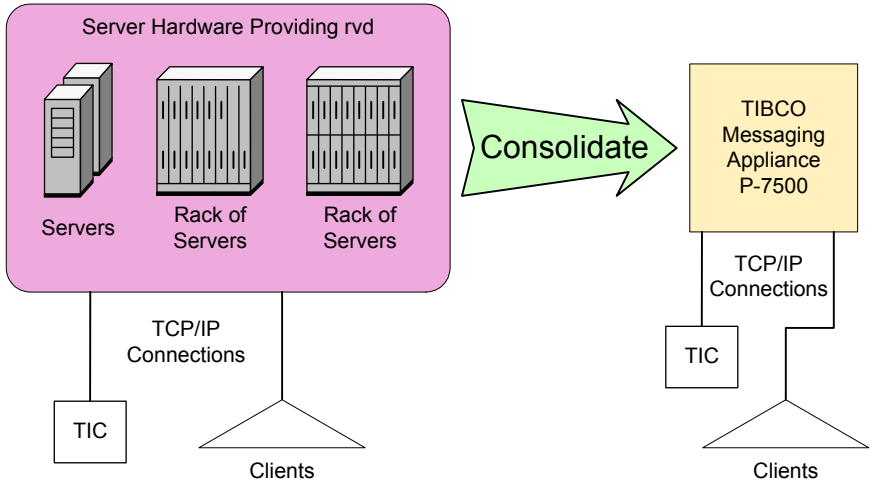
You can use P-7500 to achieve predictably low average message latency, even in high-throughput conditions.

Total Cost of Ownership

A Rendezvous daemon server is a server-class hardware unit that runs an instance of the Rendezvous daemon (`rvd`). Many remote Rendezvous clients connect to each daemon server.

In deployments with several Rendezvous daemon servers, you can use P-7500 to consolidate those servers—each P-7500 can replace several daemon servers. Consolidation can reduce hardware real estate and power consumption.

Figure 1 Consolidate Daemon Servers



Multicast Bandwidth

You can use P-7500 to reduce multicast network bandwidth usage.

Large-scale multicasting imposes complex requirements on network topology and sizing. Reliable delivery uses additional bandwidth for retransmission.

P-7500 provides the same delivery semantics as network multicasting, but implements it using switching hardware. As result, P-7500 reduces network infrastructure and bandwidth usage without affecting Rendezvous client applications.

Using TIBCO Messaging Appliance P-7500

You can leverage TIBCO Messaging Appliance P-7500 either as your complete Rendezvous environment, or by connecting it to an existing Rendezvous environment. This section broadly outlines the general process for introducing a P-7500 into your enterprise.

1. Deploy and configure P-7500. For complete instructions, see *TIBCO Messaging Appliance P-7500 Hardware Installation* and *TIBCO Messaging Appliance P-7500 Operations Guide*.
2. Arrange for applications to connect to P-7500 as if to a remote `rvd`. For details, see the programming language reference books in the Rendezvous documentation set.

Supplementing an Existing Rendezvous Environment

3. When integrating P-7500 with an existing Rendezvous environment (in which applications connect to daemons), do this additional third step.

   Configure the Rendezvous gateway within the P-7500. For more information, see Chapter 4, Rendezvous Gateway, on page 17.

Backward Compatibility

For best results we recommend building client applications using the most recent release of Rendezvous software. Nonetheless, TIBCO Messaging Appliance P-7500 can interoperate with clients built using previous releases of Rendezvous software back to release 5.

Rendezvous Release 6 and Later

As a provider of Rendezvous 8 functionality, P-7500 is compatible with Rendezvous releases 8, 7 and 6 in all respects (except for new or obsolete features).

Rendezvous Release 5

The remainder of this section describes compatibility between P-7500 and Rendezvous release 5. (For more information about compatibility among Rendezvous releases, see Compatibility with Earlier Releases in *TIBCO Rendezvous Concepts*.)

API Libraries
- P-7500 accepts connections from programs compiled and linked with the Rendezvous release 5 API.

rvd
- P-7500 can interoperate with `rvd` from release 5.

rvrd
- Rendezvous gateway of P-7500 and an `rvrd` process from release 5 *cannot* establish a neighbor connection.
- `rvrd` processes from release 5 can coexist in the same network as the Rendezvous gateway of P-7500.

Chapter 2 Hardware Overview

TIBCO Messaging Appliance P-7500 hardware includes server blade of three types. This brief chapter briefly describes the blades. For detailed information about TIBCO Messaging Appliance P-7500 hardware, see *TIBCO Messaging Appliance P-7500 Operations Guide*.

Topics

Topic Routing Blade

Topic routing blades (TRB) implement Rendezvous message semantics in firmware. Each TIBCO Messaging Appliance P-7500 includes one topic routing blade.

Network Acceleration Blade

The network acceleration blade (NAB) implements network functionality:

- TCP-IP connectivity to applications and to additional TIBCO Messaging Appliance P-7500s
- Network trunking

Management Blade

This blade provides general-purpose computing to support Rendezvous acceleration hardware. For example, this blade hosts management software, including hardware control, statistics, HTTP interface, and command line interface components.

This blade also includes a general-purpose ethernet link to other Rendezvous networks; see Chapter 4, Rendezvous Gateway, on page 17.

Chapter 3 Redundancy & Fault Tolerance

TIBCO Messaging Appliance P-7500 machines can operate in redundant pairs for fault tolerance. This chapter presents a brief overview of the redundancy model; for details of configuration and operation, see System Redundancy on page 163 in *TIBCO Messaging Appliance P-7500 Operations Guide*.

Topics

Redundancy Model

The redundancy model for TIBCO Messaging Appliance P-7500 pairs two P-7500 machines, each of which serves as a backup for the other.

Concepts

Virtual Router

Each P-7500 has exactly two virtual router instances. Each virtual router can route messages among its clients (Rendezvous application programs), and between clients and the Rendezvous gateway.

You can configure two P-7500s so that their virtual routers complement one another to provide fault tolerance through redundancy.

Roles

Each virtual router serves one of two roles—primary or backup.

Clients

Virtual routers and redundancy roles are transparent to clients. Instead, clients connect to a fixed IP address for Rendezvous functionality. A pair of virtual routers (in primary and backup roles) distributed over two P-7500s respond to those client connection requests.

In Figure 2 on page 13, clients that connect to IP address M receive Rendezvous service from virtual router A1 of P-7500 A. If P-7500 A fails, those clients reconnect to IP address M, and receive service from the redundant virtual router B2 (which serves the backup role on P-7500 B).

As in a mirror image, clients that connect to IP address N receive Rendezvous service from virtual router B1 of P-7500 B. If P-7500 B fails, those clients reconnect to IP address N, and receive service from the redundant virtual router A2 (which serves the backup role on P-7500 A).

Reconnection during failover is automatic. No explicit action is required by programmers. Rendezvous clients automatically reconnect to the same IP address, and cannot distinguish whether they are connected to the primary or the backup.

Active-Active

The arrangement in Figure 2 is called an *active-active* configuration, because under ordinary circumstances the two primaries are both active simultaneously—each serving its own set of clients. (Meanwhile, both backups are inactive.) In a failover situation, the virtual router in the backup role becomes active, replacing the failed primary.

Logical Ports

A logical port is a Rendezvous virtual IP interface, representing either a physical port of the network acceleration blade (NAB), or a link aggregation group (LAG) that spans several physical ports of the NAB. When configuring a virtual router, you must specify exactly one logical port:

- For the primary virtual router, specify one of the primary logical ports.
- For the backup virtual router, specify one of the backup logical ports.

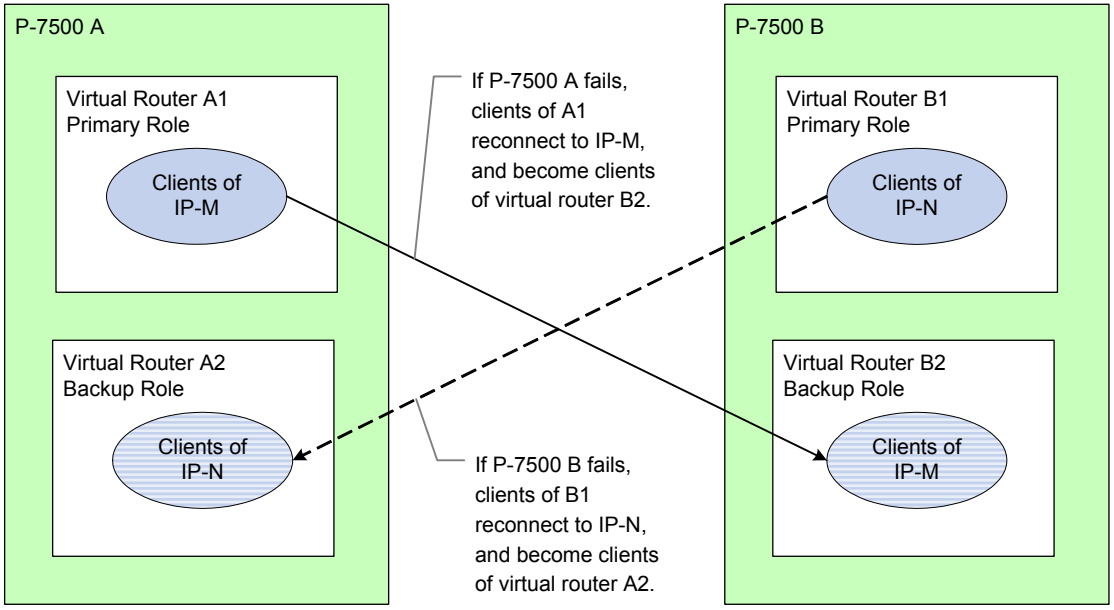
If you configure the NAB with a combination of LAGs and independent physical ports, then for lowest latency, we recommend configuring the virtual routers to use a logical port that represents a LAG (rather than an independent physical port). In all other situations, the choice of logical port is arbitrary—though it must have the same type, primary or backup, as the virtual router (as above).

Gateway

P-7500 runs two instance of the Rendezvous gateway, corresponding to the two virtual routers. The gateway bridges between NAB LANs and the GP LAN. After failover, gateways also bridge between the two virtual routers in a P-7500.

Each gateway connects to the NAB using the logical port of its corresponding virtual router.

Figure 2 Redundancy Model



Symmetric Configuration

In Figure 2 on page 13, the configuration of each virtual router must be identical with its diagonal opposite (except for its virtual router ID). More generally, in each pair of P-7500s configured for redundancy, the following two conditions must both hold:

- The virtual router that serves the primary role on P-7500 A and the virtual router that serves the backup role on P-7500 B must have identical configurations.
- Conversely, virtual router that serves the primary role on P-7500 B and the virtual router that serves the backup role on P-7500 A must have identical configurations.

An identical configuration includes identical IP addresses, and logical ports that refer to identical physical ports or LAGs.

In contrast, if a redundant pair of virtual routers are associated with Rendezvous gateways (on their respective P-7500s), then those gateways must have symmetric configurations (though not identical). For details, see Redundancy and the Gateway on page 28.

Failover

Client reconnection during failover is automatic. No explicit action is required by programmers. Rendezvous clients automatically reconnect to the same IP address, and cannot distinguish whether they are connected to the primary or the backup.

Failover preserves inbox names (because they are keyed to the IP address). Clients continue to receive point-to-point messages at the same inbox names.

The failover sequence appears to a client application as a transient TCP disconnect:

1. During failover, the Rendezvous client transport presents an `RVD.DISCONNECTED` advisory.
2. TCP disconnect causes a Rendezvous application to reconnect to the redundant pair.

   Since the primary is unavailable, the client transport automatically connects to the backup—though the client cannot detect this difference. (For further details of this process, see Activity Switches Between Redundancy Pairs on page 171 in *TIBCO Messaging Appliance P-7500 Operations Guide*.)
3. When reconnected, the client transport presents an `RVD.CONNECTED` advisory, and messages continue to flow as before.

During the period between disconnect and reconnect, dataloss can occur (without specific `DATALOSS` advisories).

Chapter 4 Rendezvous Gateway

The Rendezvous gateway bridges between clients of TIBCO Messaging Appliance P-7500 and Rendezvous clients on other networks.

Topics

Overview

The Rendezvous gateway enables communication between clients of a TIBCO Messaging Appliance P-7500 and Rendezvous clients on other networks. The other networks can be either a standard Rendezvous network (with daemons), or another P-7500.

Operation

When enabled, the gateway starts automatically when P-7500 starts. (To enable, see `enable-rv-gateway` in *TIBCO Messaging Appliance P-7500 Operations Guide.)*

Rendezvous gateway has two operational states—*running* and *idle*:

- When *running*, the gateway establishes neighbor connections and routes messages. The browser administration interface is also available for configuring parameters.
- When *idle*, the gateway neither routes messages nor establishes neighbor connections. However, the browser administration interface is available for configuring parameters.

To configure the gateway, use its browser administration interface. (For details, see `rvrd` in *TIBCO Rendezvous Administration*, because the gateway's browser administration interface is similar to that of `rvrd`).

Redundancy

A redundant configuration uses two gateways—one corresponding to each virtual router. The gateway for the primary virtual router operates in the running state, while the gateway for the backup virtual router is idle. At failover, when the backup virtual router activates, its gateway enters the running state.

Comparing the Gateway with rvrd

The Rendezvous gateway implements the full functionality of a Rendezvous routing daemon (`rvrd`), plus additions to accommodate its special role in the P-7500. Those additions are the focus of this chapter; for all other aspects of the gateway, see `rvrd` documentation in *TIBCO Rendezvous Administration*.

The gateway interoperates seamlessly with `rvrd`. (However, the gateway cannot establish neighbor connections with `rvrd` from Rendezvous release 5.)

The gateway is available for TRDP only—it is not available for PGM.

The default reliability value for the gateway is 5 seconds (in contrast, the default for daemons in Rendezvous distribution packages is 60 seconds).

NAB and GP

The Rendezvous gateway bridges between two types of networks:

- **Network Acceleration Blade LAN (NAB LAN)** A local network on the network acceleration blade interface
- **General Purpose LAN (GP LAN)** A local network on the general purpose interface

Correspondingly, it is helpful to distinguish between two types of Rendezvous client transports that can communicate through the gateway (and could not communicate without the gateway):

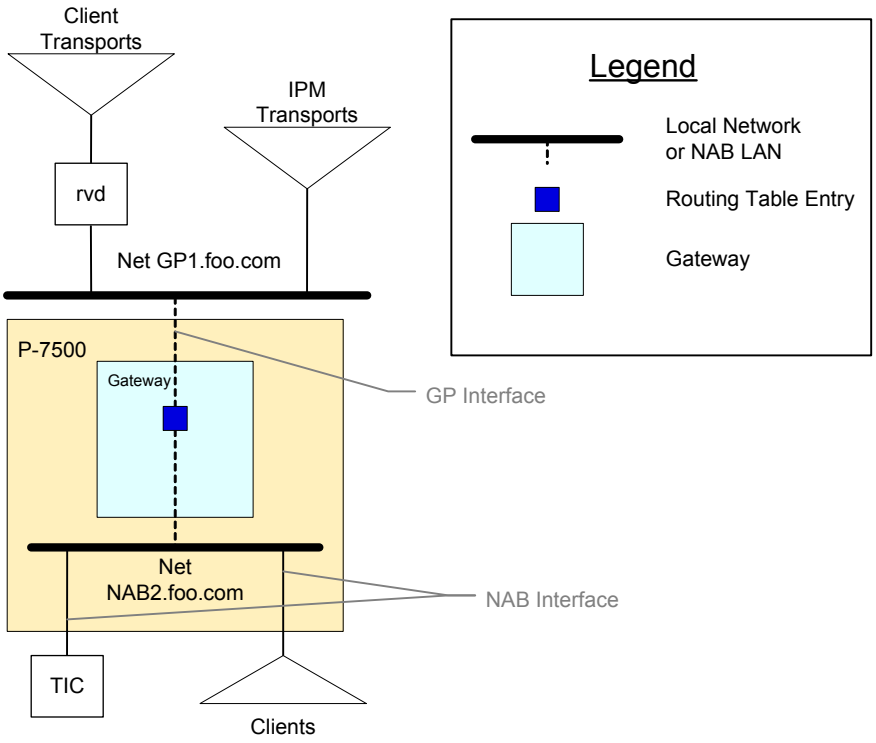
- **NAB Clients** are Rendezvous clients that connect to TIBCO Messaging Appliance P-7500 through a NAB port or LAG.

  NAB clients take advantage of subject-based multicast in P-7500 hardware.

- **GP Transports** are Rendezvous transports that connect to an `rvd` on the GP LAN, or transports that use TIBCO Rendezvous® In-Process Module. Clients of a remote P-7500 (which is not a redundant partner) are also in this category.

  GP transports use IP multicast capabilities of Rendezvous software.

Figure 3 Gateway: NAB and GP



Example Use Cases

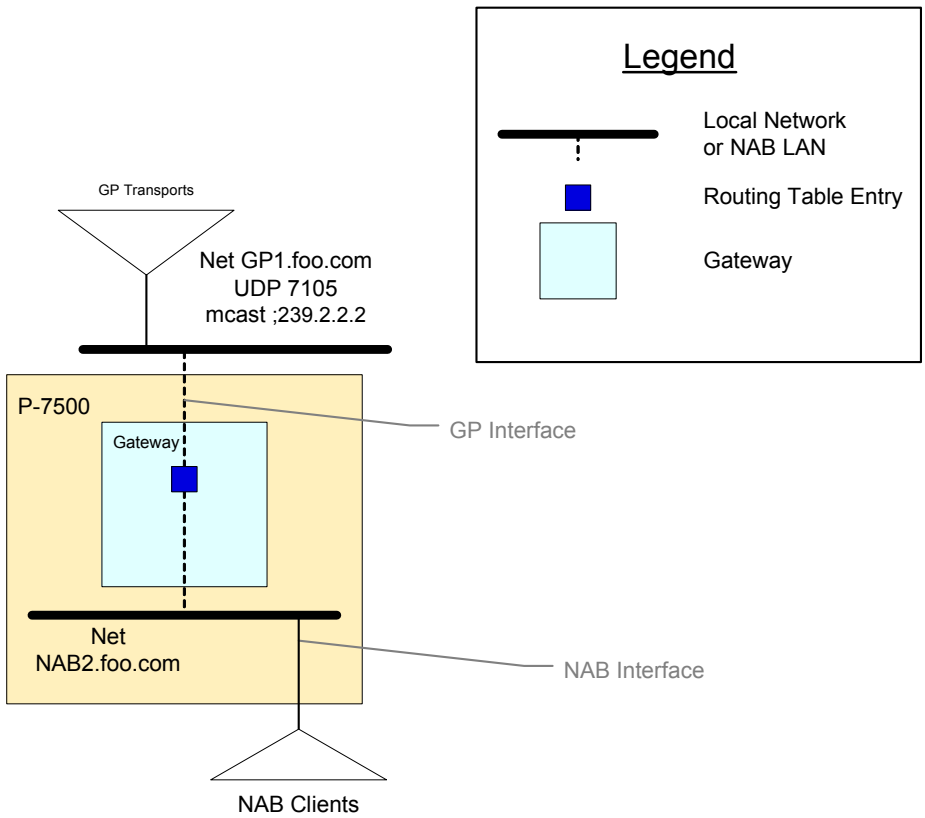
This section presents examples that illustrate the use of the Rendezvous gateway in typical situations.

Bridging to a Local Network

Motivation

NAB clients must communicate with Rendezvous clients in a local network, as in Figure 4. The local network is geographically near the TIBCO Messaging Appliance P-7500.

Figure 4 Bridging to a Local Network



Configuration

1. Determine the Rendezvous service and the network specification (IP multicast group) that the NAB clients use. In the gateway, configure a NAB local network with the same service and the same network specification.

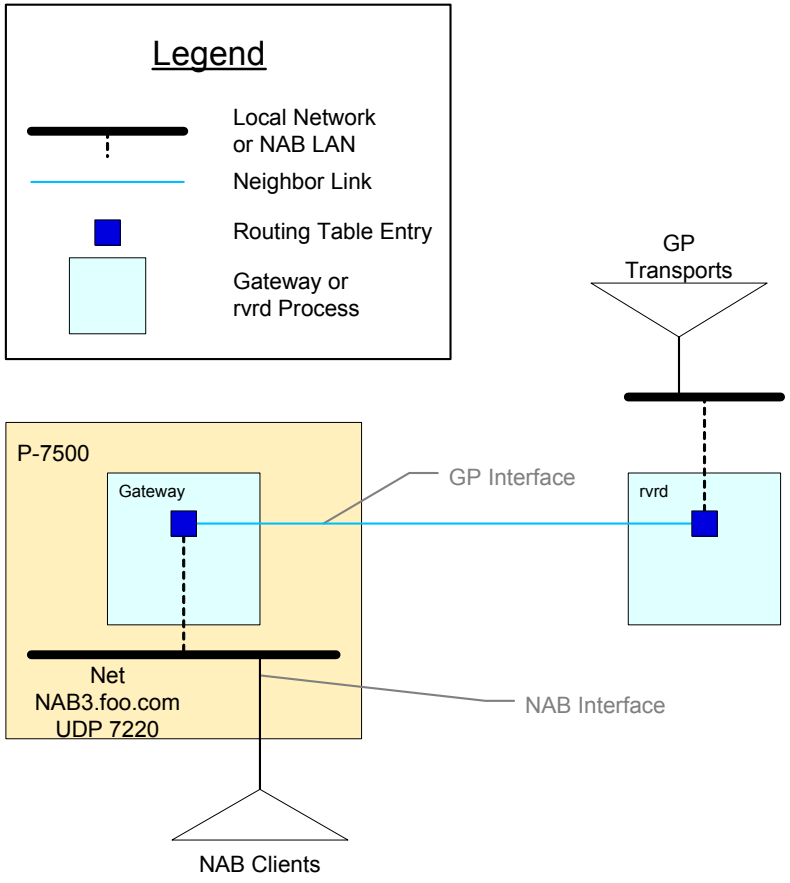
2. Determine the Rendezvous service and the network specification (IP multicast group) that the GP transports use. In the gateway, configure a GP local network with the same service and the same network specification. The example in Figure 4 uses service `7105` and network `;239.2.2.2`.

Bridging to a Routing Daemon

Motivation

NAB clients must communicate with Rendezvous clients in a remote network, as in Figure 5. The remote network is either geographically remote (across a WAN) or conceptually remote. In either case, the remote network contains an instance of the Rendezvous routing daemon (`rvrd`).

Figure 5 Bridging to a Routing Daemon



Configuration

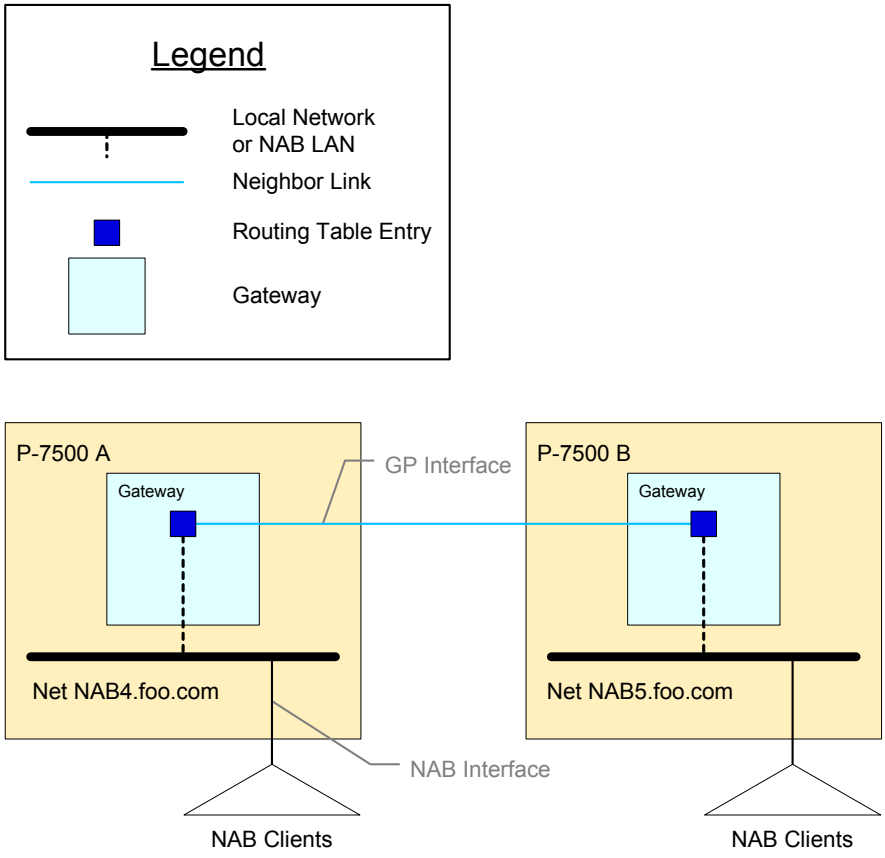
1. Determine the Rendezvous service and the network specification (IP multicast group) that the NAB clients use. In the gateway, configure a NAB local network with the same service and the same network specification.
2. Configure the gateway and the routing daemon as neighbors.

Bridging to Another P-7500

Motivation

NAB clients must communicate with NAB clients of another P-7500, as in Figure 6. The two machines are geographically remote, connected by a WAN.

Figure 6 Bridging to a Remote P-7500



Configuration

1. Determine the Rendezvous service and the network specification (IP multicast group) that the NAB clients use. In each gateway, configure a NAB local network with the same service and the same network specification.
2. Configure the two gateways as neighbors.

Configuring the Gateway

Configure the Rendezvous gateway using its browser administration interface, which behaves the same as the `rvrd` interface—except for the items documented in this chapter.

Local Network Interfaces

Rendezvous documentation uses the term *service group* to refer to a group of Rendezvous transport objects that specify equivalent service and network parameters—equivalent parameters enable them to share messages with one another.

On its NAB interface, TIBCO Messaging Appliance P-7500 does not use UDP protocols nor IP multicast groups (instead, it routes messages within its specialized hardware). Nonetheless, it emulates the semantics of UDP services and IP multicast groups; that is, the service and network parameters of NAB client transports still govern communication among clients.

Network Specification Field

Rendezvous documentation describes the 3-part network specification—network, multicast groups and send address.

Overrides the Interface (Part 1)

Part 1 of the 3-part network specification determines the hardware interface through which data flows into and out of a gateway's local network. In the P-7500 these interfaces are fixed, so the gateway overrides this part of the network specification—using only parts 2 and 3 (IP multicast information).

You need not specify part 1 when supplying the network specification field, and we recommend that you omit it for clarity. In Figure 7 on page 26, notice that when adding the `NAB5` network, the administrator specifies only part 2 (that is, `;239.5.5.5`); the gateway supplies part 1. If the administrator were to specify part 1 (for example, `1.1.10.3;239.5.5.5`), the gateway would override it.

No Loopback No Broadcast

It is invalid to specify a loopback address or a broadcast address in any part of the network specification field. Similarly, it is invalid to supply a network specification that defaults to a broadcast address or loopback address; for example, the value `;;224.1.1.1` is invalid because the listen address (part 2) defaults to the interface's broadcast address. (Nonetheless, an empty network specification is valid.)

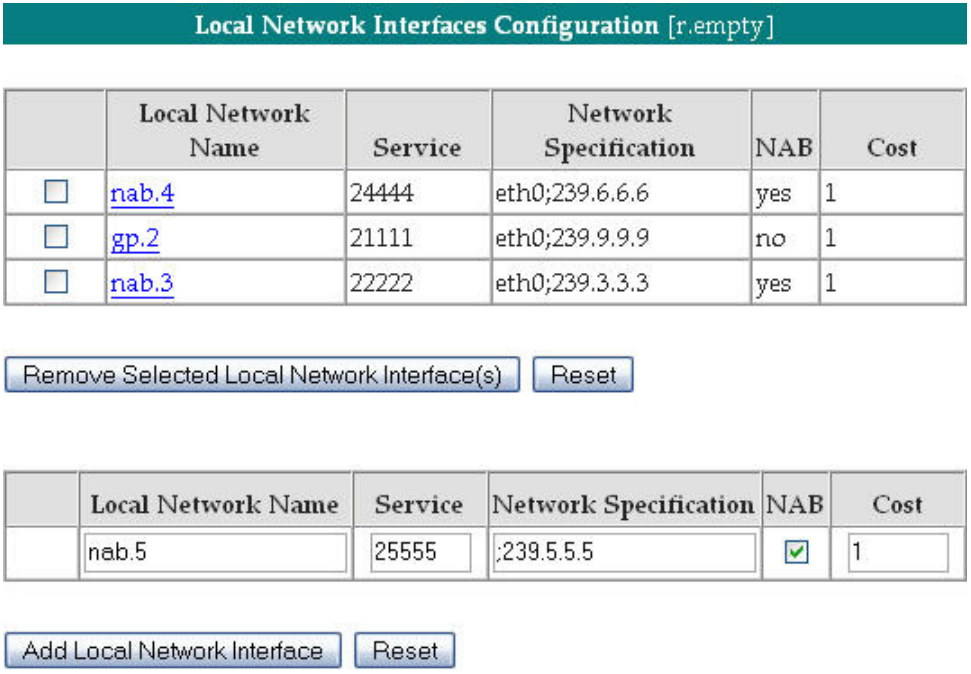
For background information, see Network Selection in *TIBCO Rendezvous Administration*.

NAB Local Network

For a service group of NAB clients to communicate with GP transports, you must configure a *NAB local network interface* in the gateway. The network and service parameters of the NAB local network must match the network and service parameters of the NAB clients. Configure one local network in the gateway for each service group of NAB clients.

When configuring a NAB local network, you must enable the **NAB** check-box (see Figure 7 on page 26).

Figure 7 Configuring Local Networks



See Also To navigate to this screen, see Routing Daemon (rvrd): Local Network Interfaces Configuration, in *TIBCO Rendezvous Administration*.

GP Local Network

For a service group of GP transports to communicate with NAB clients, you must configure a *GP local network interface* in the gateway. The network and service parameters of the GP local network must match the network and service parameters of the GP transports.

Each service group of GP transports requires a separate GP local network in the gateway in order to communicate with NAB clients.

Subject Gating

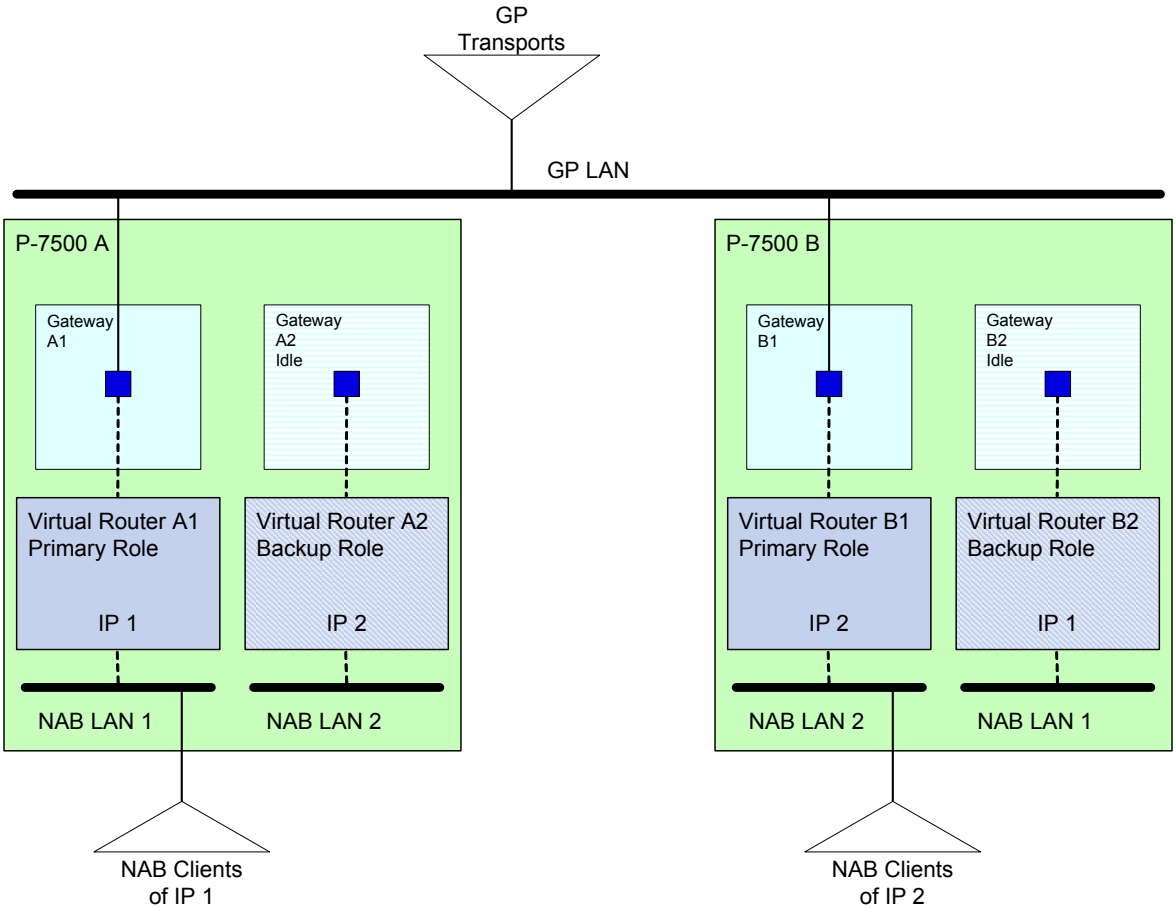
You must also configure *subject gating* for each local network interface, to import and export subjects with respect to the local network. Messages do not flow into or out from a local network until you configure subject gating.

However, subject gating is not sufficient for messages to flow. Clients must also express interest in a subject (by subscribing) before messages can flow across the network boundary.

Redundancy and the Gateway

Figure 8 illustrates gateway configuration for redundant operation, and Figure 9 on page 32 illustrates the behavior during failover.

Figure 8 Gateway: Symmetric Configuration for Redundancy



Configuration

Configure the two gateway pairs symmetrically.

Task A Routing Table Entries

1. Configure A1 and B2 so they each have a routing table entry with the same name. The router names of these two entries must be identical (for an explanation, see below at Router Name on page 30).
2. Configure B1 and A2 so they each have a routing table entry with the same name. The router names of these two entries must be identical, but different from the router name in step 1.

Task B NAB LANs

3. Configure A1 and B2 identically regarding NAB LAN 1. Even though these local networks are NAB LANs within separate P-7500s, they represent the same set of NAB clients that connect to address IP 1.
4. Configure B1 and A2 identically regarding NAB LAN 2. Even though these local networks are NAB LANs within separate P-7500s, they represent the same set of NAB clients that connect to address IP 2.

Task C Neighbors

5. Add an active neighbor connection at A2, connecting to A1.
6. Add a passive neighbor connection at A1, permitting connection from A2.
7. Add an active neighbor connection at B2, connecting to B1.
8. Add a passive neighbor connection at B1, permitting connection from B2.

Task D GP LAN

9. Configure A1 with a local network on the GP LAN.

   Do *not* configure this local network for B2. To understand the reason, see the neighbor connection in Figure 9 on page 32, which you added in Task C.

10. Configure B1 with a local network on the GP LAN.

    Do *not* configure this local network for A2. To understand the reason, see the neighbor connection in Figure 9 on page 32, which you added in Task C.

Task E Subject Gating

11. Configure A1 and B2 identically regarding subject gating with respect to NAB LAN 1.
12. Configure B1 and A2 identically regarding subject gating with respect to NAB LAN 2.

13. Configure A1 regarding subject gating with respect to the GP LAN.
14. Configure B1 regarding subject gating with respect to the GP LAN.
15. Copy subject gating from A1 (see step 13) to B1 (*not* B2). To understand the reason, see the neighbor connection in Figure 9 on page 32, which you added in Task C.
16. Copy subject gating from B1 (see step 14) to A1 (*not* A2). To understand the reason, see the neighbor connection in Figure 9 on page 32, which you added in Task C.

    After steps 13–16, A1 and B1 should have identical subject gating configurations with respect to the GP LAN.

To configure identical values, you can copy an individual value from the browser administration interface of one gateway, and paste that value into the browser administration interface of the other gateway.

Router Name

In steps 1 and 2, the router name of the backup gateway must be identical to the router name of its counterpart primary gateway. One might think this is illegal, because router names must be unique throughout a WAN (see Routing Table Entry in *TIBCO Rendezvous Administration*).

Nonetheless, in this situation the backup gateway remains idle until failover. While idle, the backup gateway does not expose its router instances to the WAN, so name collision does not occur.

At failover, the backup gateway enters the running state, and exposes its router instances to the WAN. At that time, the primary gateway is unavailable, so name collision still does not occur.

Normal Operation

Figure 8 on page 28 illustrates gateway operation in the normal situation, in which both P-7500s are available:

- Virtual router A1 is active in the primary role. NAB clients connect to it at IP 1.

  Virtual router B2 is waiting in the backup role.
- Virtual router B1 is active in the primary role. NAB clients connect to it at IP 2.

  Virtual router A2 is waiting in the backup role.
- Gateways A1 and B1 are running, connecting the corresponding virtual routers to the GP LAN.

- Gateways A2 and B2 are idle.

An *idle* gateway does *not* communicate with neighbors or local networks, and does *not* forward any data. You can configure it through its browser administration interface, but otherwise it is effectively invisible and inert. In this respect, an idle gateway behaves like an idle routing daemon.

(In contrast, *routing daemons*, instances of `rvrd`, are in a redundant configuration, they are always *running*—rather than waiting *idle.* They can communicate with their neighbors and local networks, and they can forward data.)

Failover Behavior

Figure 9 Gateway: Redundant Failover

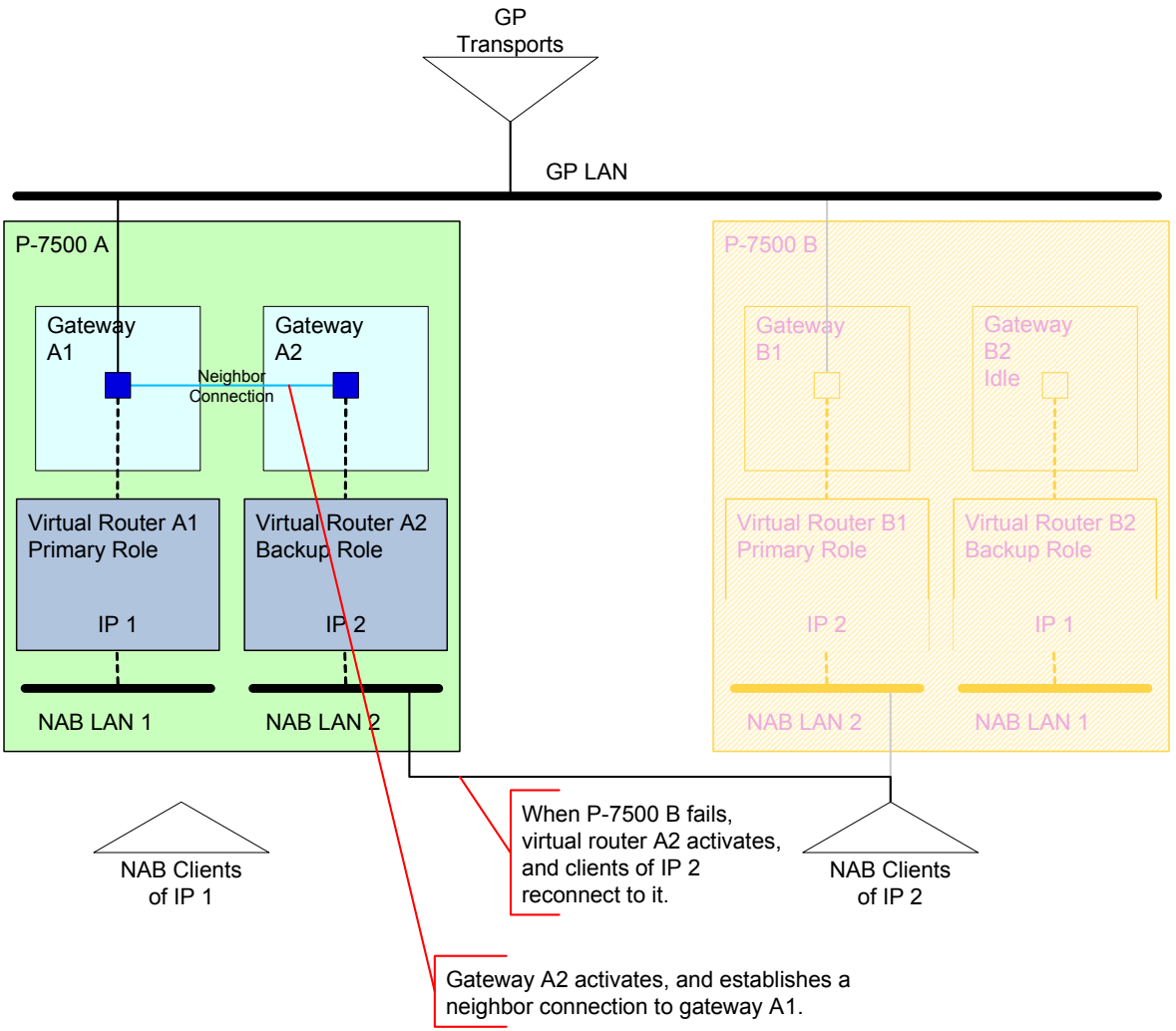


Figure 9 illustrates failover when P-7500 B fails:

- Virtual router A2 activates, and clients of IP 2 reconnect to it.
- Gateway A2 transitions from idle to running, and establishes a pre-configured neighbor connection to gateway A1. This connection completes a route from clients of IP 1 to the transports on the GP LAN, as well as a route from clients of IP 1 to clients of IP 2.

Performance Considerations

Impedance

TIBCO Messaging Appliance P-7500 is high-performance hardware. High-volume publishing on the NAB LAN can overwhelm the capacity of slower hardware on the GP LAN.

It is your responsibility to route only an appropriate subset of messages from the NAB network to the GP network.

We recommend moving high-volume senders and consumers to the NAB network.

Latency

The NAB interface can maintain low latency even under high throughput conditions. Messages that remain within the NAB network exhibit low latency. In contrast, messages that travel through the gateway incur latency penalties. For messages that require ultra-low latency, avoid forwarding through the gateway.

Chapter 5 Access Control List

TIBCO Messaging Appliance P-7500 supports access control lists (ACLs) as an optional security feature.

Topics

Overview

Access

Support for access control lists (ACLs) is a security feature of the TIBCO Messaging Appliance P-7500. When enabled (unlocked), ACLs let you control access along these dimensions:

- the clients that may connect to the TIBCO Messaging Appliance P-7500
- the message subjects to which clients may subscribe
- the message subjects to which clients may publish

Logging

Whenever an ACL denies a client attempt to connect, subscribe or publish, it logs information about the incident. You can review the logs using the browser administration interface or the command line interface.

Redundancy

When two P-7500 appliances operate as a redundant pair, their ACL configuration must be identical. Any change to ACL configuration on one P-7500 must be mirrored on the other. The administrator is responsible for maintaining these configurations in synchrony.

On each P-7500, a single ACL configuration controls access for *both* virtual routers (rather than a separate ACL configuration for each virtual router).

Enabling the ACL Feature

As a factory default, the ACL feature is *disabled* (*locked*). When the ACL feature is disabled, a TIBCO Messaging Appliance P-7500 does not control client access in any way. Administrators cannot configure access controls when the ACL feature is disabled.

You can *enable* (*unlock*) ACL functionality by obtaining a product key from TIBCO, and installing that product key using the browser administration interface or the command line interface.

If you subsequently remove the product key, the P-7500 appliance automatically erases any previous ACL configuration, then restarts with ACL functionality disabled.

See Also For information about the browser administration interface and the command line interface for the ACL feature, see *TIBCO Messaging Appliance P-7500 Operations Guide*.

Client Connection

The first layer of access control determines which clients may connect to a TIBCO Messaging Appliance P-7500.

Default Action and Exceptions

To control client connections to a P-7500, you can configure two aspects—the default behavior and exceptions.

Default Action

You can set the default action either to allow connections from all clients, or to disallow connections from all clients.

- If the default action is to *allow* connections from all clients, then any exceptions specify clients that are expressly disallowed.
- Conversely, if the default action is to *disallow* connections from all clients, then any exceptions specify clients that are expressly allowed.

Exceptions

The client connection rule can include zero or more exceptions to its default action.

You must specify each exception as a CIDR address. Notice that CIDR addresses can specify the IP address of an individual computer, a small subnet, or even a large network—-depending upon the number bits in the network mask portion of the address.

Example 1 ACL Client CIDR Addresses

CIDR Address	Description
`15.300.2.121/32`	32 bits specifies an individual computer (or network interface card).
`15.300.2.000/24`	24 bits specifies all IP addresses on subnet `2`.

Initial Configuration

When you first enable the ACL feature, the default action is to allow all connections, with no exceptions.

You may change the default action. You may add exceptions.

Enforcement

P-7500 enforces ACL connection controls whenever a client attempts to connect.

After a client is already connected to a P-7500, changing either aspect of the ACL configuration to disallow that client does not have any effect; all connected clients remain connected.

Subject Access

The second layer of access control determines the Rendezvous message subjects to which a connected client can subscribe and publish.

Subject access controls use independent settings for subscribing and publishing, but the configuration and semantics are similar.

Profiles and Mappings

Subject access controls requires two types of configuration that interact in a cascading fashion:

- A *profile mapping* associates each client connection with an ACL profile.
- Each *profile* determines the subjects to which associated client connections can subscribe and publish.

You can define several profiles.

You can map several client connections to the same profile.

Mappings

Each profile mapping associates a combination of username and Rendezvous service with an ACL profile. That is, you define a profile mapping by supplying three items:

- a username string (which you may omit)
- a Rendezvous service (which you may omit)
- a profile name

You may define several mappings.

Username — Client processes tacitly include their username with each client connection request. This value is the login username on the host computer where the client process is running. Subject access controls match this username against the profile mappings.

Semantics — Each mapping means that a client connection that matches its username and service can access Rendezvous subjects as defined in the profile. If you omit the username, then client connections with any username can match the mapping. If you omit the service, then client connections with any service can match the mapping.

When a client matches more than one profile mapping, the most specific mapping takes precedence (for details, see Table 3 on page 41 and Example 2 on page 42).

Table 3 ACL Profile Mappings: Specifity and Precedence

Specifity	Username	Service	Description
1	Present	Present	This mapping applies only to clients with this username connecting on this service. For each pairing of username and service, you can define at most one mapping at this specificity. This is the most specific type of mapping, and has the highest precedence.
2	Present	—	This mapping applies to clients with this username connecting on any service (but a mapping with specificity 1 takes precedence, overriding this mapping). For each username, you can define at most one mapping at this specificity.
3	—	Present	This mapping applies to clients with any username connecting on this service (but a mapping with specificity 1 or 2 takes precedence, overriding this mapping). For each service, you can define at most one mapping at this specificity.
4	—	—	This mapping applies to clients with any username connecting on any service (but a mapping with specificity 1, 2 or 3 takes precedence, overriding this mapping). The initial factory configuration maps all clients to the `default` profile with this specificity. You can define at most one mapping at this specificity. (To replace the existing mapping at this specificity, you must first remove it.) This is the most general mapping, and has the lowest precedence.

Example 2 ACL Profile Mappings and Precedence

For example, suppose that you have defined the following profile mappings:

Username	Service	Profile
User-1	1111	Profile-1
User-2	1111	Profile-2
User-1	—	Profile-3
—	8888	Profile-4
—	—	default

When User-1 connects on service 1111, then Profile-1 applies.
When User-1 connects on service 3333, then Profile-3 applies.
When User-1 connects on service 8888, then Profile-3 applies.

When User-2 connects on service 1111, then Profile-2 applies.
When User-2 connects on service 8888, then Profile-4 applies.
When User-2 connects on service 3333, then the default profile applies.

When User-5 connects on service 8888, then Profile-4 applies.
When User-5 connects on service 1111, then the default profile applies.

Subject Rules

Within each profile, you can configure exactly two subject rules—one *subscribe rule* and one *publish rule*. Each rule consists of a *default action* and a set of *exceptions*.

Default Action

The default action can either allow all subjects, or disallow all subjects.

- If the default action *allows* all subjects, then any exceptions specify subjects that are expressly disallowed.
- Conversely, if the default action *disallows* all subjects, then any exceptions specify subjects that are expressly allowed.

Exceptions

Each rule can include zero or more exceptions to its default action.

Example 3 ACL Allow Subject

For example, suppose profile `P1` has a subscribe rule that allows all subjects, and an exception disallowing `foo.>`. Then client connections that map to profile `P1` can subscribe to any subject except those that either match `foo.>` directly (for example, `foo.bar`, `foo.*.baz`) or *overlap* `foo.>` (for example, `*.bar`, `*.*`, `>`).

For a description of analogous behavior in `rvrd`, see Subject Filtering with Wildcards, in *TIBCO Rendezvous Administration*.)

Subscribing to a subject that is disallowed (even in part), produces an error advisory; see `CLIENT.SUBSCRIPTION.DISALLOWED` on page 46.

Example 4 ACL Disallow Subject

Conversely, suppose profile `P2` has a subscribe rule that disallows all subjects, and an exception allowing `Free.Chat.>`. Then client connections that map to profile `P2` can subscribe to any subject that matches `Free.Chat.>` directly (for example, `Free.Chat.Cats.>` and `Free.Chat.*.Feeding`).

Notice that overlapping subjects (such as `Free.*.*`) are not allowed. As a general rule, overlapping is sufficient to disallow, but not to allow.

Publish rules have similar semantics to the subscribe rule examples above.

Enforcement

Subscribing

P-7500 enforces subscription controls (that is, subscribe rules) whenever a client attempts to subscribe to a subject.

After a client has already subscribed to a subject, changing the ACL configuration to disallow that subject (or map the client to a different profile) does not have any effect; all existing subscriptions remain in effect.

Publishing

P-7500 enforces publishing controls (that is, publish rules) whenever a client attempts to publish to a subject.

Notice that the P-7500 filters each individual message that a client sends, using the publish rule that is in effect at the time the client sends the message.

Initial Configuration

When you first enable the ACL feature, a profile named `default` is factory configured. This profile has a subscribe rule that allows all subjects, and a publish rule that allows all subjects. All client connections (that is, any combination of username and service) map to this `default` profile (specificity 4).

You may change the subject rules of the `default` profile, but you cannot delete it.

You may map client connections (at any specificity) to other profiles.

Appendix A Advisory Messages

Rendezvous software presents *advisory messages* to inform programs of exceptional situations that might affect them. Advisory messages report errors, warnings and other useful information. This appendix describes the *system advisory messages* generated by TIBCO Messaging Appliance P-7500.

Topics

CLIENT.SUBSCRIPTION.DISALLOWED

Advisory

Subject Name Syntax

`_RV.WARN.SYSTEM.CLIENT.SUBSCRIPTION.DISALLOWED.`*subject*

Purpose

A listening client of a TIBCO Messaging Appliance P-7500 receives this advisory when it has subscribed to a subject, but the P-7500 disallows all or part of the subscription for that client.

Remarks

Only the specific client transport receives this advisory.

This message is a warning—although the client's subscribe call completed normally, the P-7500 does not direct any messages to the resulting listener object. The listener is inert.

The *subject* element of the advisory subject name is the subject that the client supplied in the call that created the listener. The *subject* element itself often consists of several elements, so the wildcard character ">" (rather than "`*`") is the correct way to match all subjects in this position.

Message Fields

Field Name	Description
`sub`	The subject that the client supplied in the call that created the listener.
`tport`	The transport ID.
`descr`	The client's description string.

Diagnosis

In order to allow a subscription, both of the following conditions must be true:

- The client's ACL profile must allow *all* of the subjects that match the subscription subject (that is, a superset of matching subjects).
- The client's ACL profile must *not* disallow any subject that matches or overlaps the subscription subject.

`SUBSCRIPTION.DISALLOWED` advisories indicates that the subscription violates one of the above conditions.

Because the listener cannot receive any messages, it is appropriate for the client program to destroy the listener object.

See Also

Subject Rules on page 42

Index

L

M

N

P

R

S

T

V