

Placing the BlackBerry Router in the DMZ

Contents

BlackBerry Router	1
Remote implementation	1
DMZ implementation.....	1
System requirements.....	2
Remote service requirements	2
Impact	3
Network connectivity	3
Installation	4
Provisioning.....	4
Registry entries	4
Flexibility	4
Wireless LAN.....	5
Multihoming	5
BlackBerry Router chaining.....	5
Security.....	5
Disaster recovery.....	6
Failover requirements.....	6

BlackBerry Router

The BlackBerry® Router is the component of the BlackBerry Enterprise Server® that connects to the wireless network. It also routes data to BlackBerry devices that are connected using the BlackBerry Handheld Manager.

The BlackBerry Enterprise Server distinguishes between a BlackBerry Router and a direct Server Routing Protocol (SRP) connection. When it detects a BlackBerry Router, it identifies the IP addresses, writes them to the configuration database, and when a BlackBerry device that is running BlackBerry Handheld Software version 4.0 is provisioned, sends that information in a wireless service book packet to the BlackBerry device.

If the BlackBerry Router is replaced at any time, the BlackBerry Router address changes, but the BlackBerry devices do not need to be reconnected to the administration or desktop computer to receive a new service book and BlackBerry Router address. The change is automatically detected by the BlackBerry device. However, there is a delay before the BlackBerry device detects the change. If the BlackBerry device is connected to the computer at that time, serial bypass (least cost routing) does not work.

See the *BlackBerry Enterprise Server version 4.0 Feature and Technical Overview Guide* for your messaging platform for more information on serial bypass.

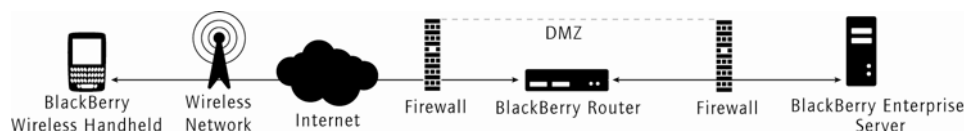
Remote implementation

If installed on a remote computer, the BlackBerry Router continues to route BlackBerry traffic to and from the BlackBerry Infrastructure for one or more BlackBerry Enterprise Servers that must all point to the same SRP address. You must use the BlackBerry Configuration Panel to configure the BlackBerry Enterprise Server connection through the BlackBerry Dispatcher to the BlackBerry Router. The BlackBerry Router is designed to have minimal impact on performance, so most organizations that choose this configuration do so for ease of deployment in their environment.

See the *BlackBerry Enterprise Server version 4.0 Administration Guide* for your messaging platform for more information on configuring the connection.

DMZ implementation

You can install the BlackBerry Router in a remote location outside the firewall and configure the SRP connections so that all traffic bypasses the firewall. The SRP connections between the BlackBerry Enterprise Server and BlackBerry Router and between the BlackBerry Router and the BlackBerry Infrastructure are stored in the BlackBerry Router local registry. The location outside the firewall is referred to as the DMZ (demilitarized zone).



BlackBerry Router implemented in the DMZ

The DMZ is a neutral subnetwork between the trusted corporate LAN, and the untrusted external wireless network and public Internet. The BlackBerry Router can safely be implemented in the DMZ because all traffic that passes through the BlackBerry Router is encrypted, and all connections to the BlackBerry Router are authenticated. No encryption keys are stored in or transferred through the BlackBerry Router.

Least cost routing in the DMZ

Serial bypass is referred to as least cost routing because it eliminates the cost to an organization of using the BlackBerry Infrastructure. Although the BlackBerry solution enables wireless BlackBerry connectivity through serial bypass, you must have a network connection in place to enable the communication to occur.

When the least cost routing solution is implemented

- Multiple BlackBerry Wireless Handhelds can connect through the same BlackBerry Handheld Manager.
- BlackBerry Wireless Handhelds can be deployed and all normal functions, with the exception of wireless enterprise activation, used through the BlackBerry Handheld Manager and the BlackBerry Router without

use of the radio. After wireless enterprise activation is initiated, the BlackBerry Wireless Handheld can be connected to the computer to enable enterprise activation to continue without the use of the radio.

When implementing least cost routing while the BlackBerry Router is in the DMZ, the computer that is running the BlackBerry Handheld Manager must be able to make a TCP connection to port 4101 of the server that is running the BlackBerry Router that is used by that BlackBerry device.

System requirements

The system requirements for a remote BlackBerry Router can be found in the *BlackBerry Enterprise Server version 4.0 Installation Guide* for your messaging platform.

Note: Complete the remote installation of the BlackBerry Router component before installing the BlackBerry Enterprise Server. You establish the connection to the remote computer when you configure the BlackBerry Enterprise Server.

The full system configuration options for installing a remote BlackBerry Router in the DMZ to deploy the BlackBerry 7270 Wireless Handheld™ on a wireless LAN can be found in the *BlackBerry Enterprise Server version 4.0 Implementation Guide for Wireless LAN*.

Remote service requirements

Tip: If you have installed a remote BlackBerry Router, do not restart the computer or the service until you have set the necessary registry values.

To implement a remote BlackBerry Router, you must manually enable remote services through the AllowRemoteServices registry value on the remote BlackBerry Router computer. This enables the BlackBerry Router to accept connections from other computers.

Because the BlackBerry Router does not make connections, you can open a port other than 3101, which requires you to add and configure a new ServicePort value and change the NetworkAccessNode and TcpPort values.

- \\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerryRouter\ServicePort
- \\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Dispatcher\NetworkAccessNode
- \\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Dispatcher\TcpPort

These system configuration values can be changed through the BlackBerry Server Configuration panel or through the registry. See the *BlackBerry Enterprise Server version 4.0 Administration Guide* for your messaging platform for more information on configuring the connection through the BlackBerry Server Configuration panel.

Enable remote services

To enable remote services such as the BlackBerry Dispatcher to connect so that the BlackBerry Router can route BlackBerry traffic, complete the following steps:

1. On the remote BlackBerry Router computer, open the registry editor.
2. Change the registry entry value for \\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerryRouter\AllowRemoteServices from 0 to 1.

Change BlackBerry Router listen port

To change the service port that the BlackBerry Router listens on (port 3101 by default), complete the following steps:

1. On the remote BlackBerry Router computer, open the registry editor.
2. Add a ServicePort registry key as a DWORD value to
\\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerryRouter
3. Set the key to the new BlackBerry Router listen port value (for example, port 80).

4. Restart the BlackBerry Router service on the remote computer.

Test the connection to the BlackBerry Infrastructure

The test program attempts to connect to the wireless network using the SRP address that you specified during the installation and the BlackBerry Router listen port.

1. On the computer on which you want to test the connection to the wireless network, at the command prompt, switch to the location in which the BlackBerry Enterprise Server Software is installed.
2. Type **bbsrptest <srpaddress> <port>**, where *<srpaddress>* is the SRP address that you provided during the installation and *<port>* is the BlackBerry Router listen port. For example, at the command line, type
bbsrptest.exe – host server.yourdomain.com –port 80
3. If the test is not successful, use the Microsoft® Windows® Socket (WINSOCK) error code to diagnose the problem. See "Common connection errors" in the *BlackBerry Enterprise Server version 4.0 Troubleshooting Guide* for your messaging platform for more information.

Configure the BlackBerry Dispatcher

The BlackBerry Dispatcher must know which network access node and TCP port to use when connecting to the BlackBerry Router. If you are using a remote BlackBerry Router, you might need to change the registry entries for these values (if you did not originally enter the remote values during the BlackBerry Router installation).

1. Stop the BlackBerry Dispatcher service on the BlackBerry Enterprise Server.
Note: Traffic to the BlackBerry devices on that BlackBerry Enterprise Server stops when the BlackBerry Dispatcher service is stopped.
2. On the BlackBerry Enterprise Server computer, open the registry editor.
3. Change the registry entry value for `\\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Dispatcher\NetworkAccessNode` from the default to the remote computer DNS name (for example, *server.yourdomain.com*).
4. Change the registry entry value for `\\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Dispatcher\TcpPort` to the ServicePort value that is specified on the BlackBerry Router (for example, 80).
Note: If a TCP port is not specified on the BlackBerry Router computer, the default value is 3101.
5. Restart the BlackBerry Dispatcher service.
6. Open the BlackBerry Manager to verify the SRP connection (for example, to *srp.xx.blackberry.net*). If the connection is not available (in other words, a red X appears on the server icon), restart the BlackBerry Manager.

Impact

If you install the BlackBerry Router on a remote computer in the DMZ, consider the following issues.

Network connectivity

The BlackBerry Router can only connect to a single SRP address (for example, *srp.na.blackberry.net*).

If your users use the BlackBerry Desktop Software or the BlackBerry Handheld Manager, make sure that those applications can connect to the BlackBerry Router.

If you are implementing the WLAN-capable BlackBerry 7270 Wireless Handheld for both data and voice, the Session Initiation Protocol (SIP) proxy server and the BlackBerry Router must be accessible on the same route. This means that a remote BlackBerry Router that is installed in the DMZ requires a route to the SIP proxy server outside the firewall.

Note: Access to the BlackBerry Router allows for data access only (messaging, calendar, and browser use); it does not allow for voice call access through the SIP infrastructure.

Installation

Multiple BlackBerry Enterprise Servers can share a single, remote BlackBerry Router. Because the BlackBerry Router does not connect to any services, it can be run under any account. If the BlackBerry Router service is installed and run under the BlackBerry Enterprise Server administration account, the BlackBerry Router that is located in the DMZ requires a route to the internal Windows domain. If the remote BlackBerry Router is a standalone Windows server, it cannot be installed and run with a BlackBerry Enterprise Server administration account that belongs to the internal Windows domain.

Provisioning

You can push the BlackBerry Handheld Manager to user computers so that when users connect the BlackBerry device to a computer and run the BlackBerry Handheld Manager (which can be configured to start automatically at startup); the BlackBerry Handheld Manager connects to the BlackBerry Router on the BlackBerry Enterprise Server. The BlackBerry Router uses this connection to route data to the BlackBerry device instead of through the wireless network.

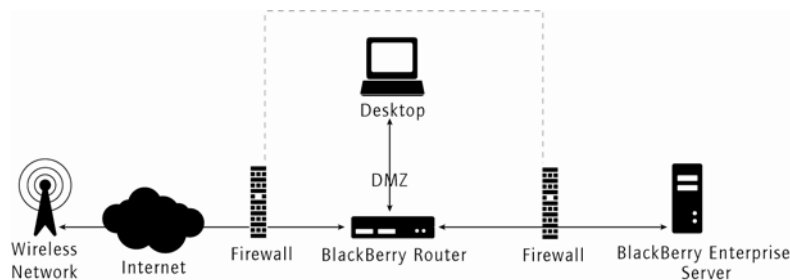
Registry entries

You might need to change registry values to allow remote access and accommodate port value changes. See "Remote service requirements" for more information.

Flexibility

A typical issue during deployment of the BlackBerry Enterprise Server is a security policy that dictates that no internal system can make a connection directly to the Internet; therefore, all systems must connect through another system in the DMZ.

When the BlackBerry Router is implemented in the DMZ, there is the option of enabling a desktop to login remotely (for example, from a hotel room) to the corporate LAN.



BlackBerry Router and desktop computer

It is possible to connect to the corporate LAN and deploy BlackBerry devices from a remote LAN through a desktop computer that is running the BlackBerry Handheld Manager.

If you are implementing VPN as a security solution, placing the BlackBerry Router in the DMZ serves no security or flexibility advantage. You control the BlackBerry Router and the BlackBerry Enterprise Server, so deployment might be eased by the option of opening up a port other than port 3101, which is the standard relay port.

A barrier to typical deployment is that you have to open port 3101. If the BlackBerry Router is placed in the DMZ, to use least cost routing, you will need to open up port 4101 on the internal-facing firewall to enable communication between the BlackBerry Handheld Manager and the BlackBerry Router.

Because the BlackBerry Router is routing traffic between the BlackBerry Enterprise Server and `srp.xx.blackberry.net`, you can also configure it to perform Port Address Translation (PAT) and to listen for BlackBerry traffic on another port. For example you can configure the BlackBerry Router to accept connections from the BlackBerry Dispatcher Service on Port 80 and connect to `srp.xx.blackberry.net` on port 3101.

Note: If you select Port 80 as the service port, you need to disable or uninstall Internet Information Services on the BlackBerry Router computer because a conflict will occur on that port.

For example, if the BlackBerry Router in the DMZ is configured to accept connections on port 80 and connect to `srp.xx.blackberry.net` through port 3101, on the internal-facing part of the DMZ you would need to allow outbound initiated/bi-directional communication on port 80, and on the external-facing part of the firewall you would need to allow outbound initiated/bi-directional communication on port 3101.

Wireless LAN

If you are implementing a WLAN, you can put the access points outside the firewall, and the BlackBerry Router in the DMZ will be routable from the access points. This is an access security option that does not require a VPN or layer 3 access security infrastructure. See the *BlackBerry Enterprise Server version 4.0 Implementation Guide for Wireless LAN* on the BlackBerry support site (www.blackberry.com/support) for more information.

Note: Wireless provisioning does not currently work with BlackBerry 7270s for WLAN. The BlackBerry 7270s must be connected to the administration computer or a desktop computer to initialize synchronization. An initial synchronization connection is only needed with BlackBerry 7270s for WLAN.

Multihoming

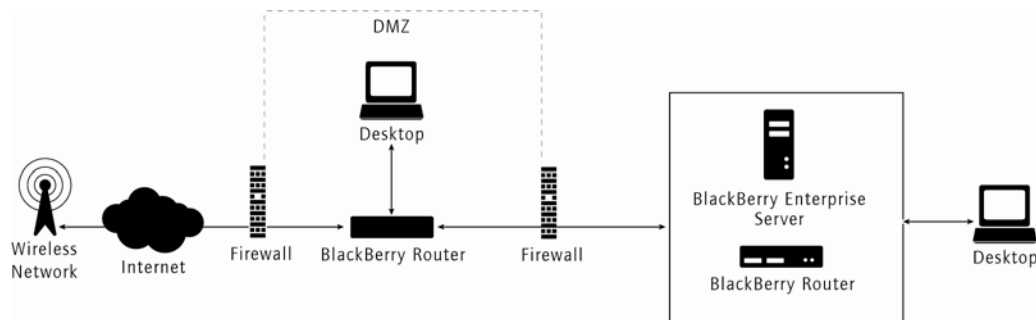
Use of multiple network cards on a desktop computer is supported. The BlackBerry Router might send a list of IP addresses if a desktop has multiple IP addresses, and try them in sequence. All desktop computers must be able to connect over 4101.

BlackBerry Router chaining

Installing multiple BlackBerry Routers that are separated by firewalls (in a "chain") permits the coexistence of a local BlackBerry Router and a remote BlackBerry Router (used specifically for WLAN, for example). Chaining BlackBerry Routers requires BlackBerry Enterprise Server version 4.0 Service Pack 1 or later.

When you implement a chain of BlackBerry Routers, internal users can access the BlackBerry Router locally on the BlackBerry Enterprise Server for least cost routing and also access the BlackBerry Router in the DMZ. The first BlackBerry Router forwards BlackBerry device authentication packets to the second BlackBerry Router in the chain.

BlackBerry devices that are connected through the second BlackBerry Router can authenticate and communicate with the BlackBerry Enterprise Server. The BlackBerry Enterprise Server pushes the BlackBerry Router IP addresses to the BlackBerry devices. The BlackBerry devices can attempt to connect with each BlackBerry Router in the chain in turn until they establish a successful connection.



"Chaining" BlackBerry Routers

Security

A remote BlackBerry Router might enable further security options because the BlackBerry Router does not have encryption keys and therefore does not compromise the security of the BlackBerry Infrastructure if the BlackBerry Router itself is compromised. However, implementing the BlackBerry Router in the DMZ does not necessarily increase security.

The desktop computer connects to the BlackBerry Router and reports the BlackBerry device PIN. The BlackBerry router rejects connections from unauthenticated devices.

The BlackBerry Router mediates encrypted traffic between the BlackBerry Enterprise Server and the BlackBerry device. It uses an authentication protocol that proves it knows the key but does not infer the key.

If the BlackBerry device is password protected, the user must type the password on the desktop computer that is running the BlackBerry Handheld Manager.

Disaster recovery

Failover requirements

If the computer that is running the BlackBerry Router fails, it is necessary to automatically or manually failover, or switch, to another computer that is running a BlackBerry Router.

Note: If there is ever downtime during which the BlackBerry Router is functional but the BlackBerry Dispatcher service is unavailable, the BlackBerry Router, using serial bypass, notifies any connected BlackBerry device(s) and synchronization of information between the BlackBerry Enterprise Server and the BlackBerry device stops.

Symptoms that the BlackBerry Router component is unavailable are that the synchronization of information between the BlackBerry Enterprise Server and the BlackBerry device stops and least cost routing through serial bypass stops. BlackBerry devices attempt to reconnect to the BlackBerry Router periodically.

To implement failover, install one or more remote BlackBerry Routers on independent computers, configuring each BlackBerry Router during the installation with the same host name or SRP connection address.

Failover is simplified if the BlackBerry Routers, installed on separate computers, are assigned the same network access node and listen on the same port. This enables failover to occur as soon as the BlackBerry Dispatcher is configured to point to the new remote computer DNS name (for example, *server.yourdomain.com*) and the new BlackBerry Router computer is brought online. When the BlackBerry Dispatcher connects to the BlackBerry Router, the BlackBerry Router sends the BlackBerry Router address(es) (which are configurable through the registry) to the BlackBerry Dispatcher to be added to the database and sent to the BlackBerry device(s) in a service book.

Note: You have the option of creating more BlackBerry Router addresses to be sent to the BlackBerry Dispatcher by creating a new key (`\\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerryRouter\Hostname`) and adding a string value under the created key using the format `Host[n]=server address`. For example, `\\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerryRouter\Hostname\[Value]Host1=router2`

Configure the BlackBerry Dispatcher (failover)

If the BlackBerry Router to which the BlackBerry Dispatcher is connected becomes unavailable, the BlackBerry Dispatcher registry entry must be changed to tell the BlackBerry Dispatcher which new network access node to use when connecting to the BlackBerry Router.

1. Stop the BlackBerry Dispatcher service on the BlackBerry Enterprise Server.

Note: Traffic to the BlackBerry devices on that BlackBerry Enterprise Server stops when the BlackBerry Dispatcher service is stopped.

2. On the BlackBerry Enterprise Server computer, open the registry editor.
3. Change the registry entry value for `\\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Dispatcher\NetworkAccessNode` from the default to the remote computer DNS name (for example, *server.yourdomain.com*).
4. If the failover BlackBerry Router listens on a different port, change the registry entry value for `\\HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\Dispatcher\TcpPort` to the ServicePort value that is specified on the BlackBerry Router (for example, 80).

Note: If a TCP port is not specified on the BlackBerry Router computer, the default value is 3101.

5. Restart the BlackBerry Dispatcher service.
6. Open the BlackBerry Manager to verify that the SRP connection (for example, to `srp.xx.blackberry.net`) has been re-established. If the connection is not available (in other words, a red X appears on the server icon), restart the BlackBerry Manager. You might also have to restart the BlackBerry Enterprise Server.

Tip: If the BlackBerry Routers are installed with the same host name or SRP connection address and IP address/DNS name and are behind a load director, automatic failover can be implemented.

Note: BlackBerry Router clustering is not supported.

Part number: SWD_X_BES(EN)-118.002

© 2005 Research In Motion Limited. All Rights Reserved. The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, "Always On, Always Connected", the "envelope in motion" symbol and BlackBerry are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The BlackBerry device and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents.shtml for a current listing of applicable patents.

This document is provided "as is" and Research In Motion Limited and its affiliated companies ("RIM") assume no responsibility for any typographical, technical or other inaccuracies in this document. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR ITS RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third party sources of information, hardware or software, products or services and/or third party web sites (collectively the "Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the Third Party Information or the third party in any way. Installation and use of Third Party Information with RIM's products and services may require one or more patent, trademark or copyright licenses in order to avoid infringement of the intellectual property rights of others. Any dealings with Third Party Information, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third party. You are solely responsible for determining whether such third party licenses are required and are responsible for acquiring any such licenses relating to Third Party Information. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use Third Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third Party Information shall be governed by and subject to you agreeing to the terms of the Third Party Information licenses. Any Third Party Information that is provided with RIM's products and services is provided "as is". RIM makes no representation, warranty or guarantee whatsoever in relation to the Third Party Information and RIM assumes no liability whatsoever in relation to the Third Party Information even if RIM has been advised of the possibility of such damages or can anticipate such damages.