



## FHRP—VRRP Enhancements

---

The First-Hop Redundancy Protocol (FHRP)—VRRP Enhancements feature adds support for the following capabilities:

- Message Digest 5 (MD5) Authentication—Added to routers that are configured for Virtual Router Redundancy Protocol (VRRP), similar to the Hot Standby Router Protocol (HSRP) to provide a method of authenticating peers using a more simple method than the method in RFC 2338.
- Bridged Virtual Interface (BVI)—Added configuration of VRRP capability on BVIs that is similar to the existing HSRP support for BVIs.

### History for the FHRP—VRRP Enhancements Feature

Release	Modification
12.3(14)T	This feature was introduced.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About FHRP—VRRP Enhancements, page 2](#)
- [How to Configure FHRP—VRRP Enhancements, page 5](#)
- [Configuration Examples for FHRP—VRRP Enhancements, page 17](#)
- [Additional References, page 19](#)
- [Command Reference, page 20](#)



---

**Corporate Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

# Information About FHRP—VRRP Enhancements

To configure the FHRP—VRRP Enhancements feature, you should understand the following concepts:

- [Virtual Router Redundancy Protocol, page 2](#)
- [Hot Standby Router Protocol, page 2](#)
- [Authentication Support for VRRP Groups, page 2](#)
- [Integrated Routing and Bridging, page 3](#)
- [VRRP Support for Integrated Routing and Bridging, page 4](#)

## Virtual Router Redundancy Protocol

The Virtual Router Redundancy Protocol (VRRP) is a protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to use the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the virtual-router master with the other routers acting as backups in case of the failure of the master router.

## Hot Standby Router Protocol

IP routing redundancy is designed to allow for transparent fail-over at the first-hop IP router. Both Hot Standby Router Protocol (HSRP) and VRRP enable two or more devices to work together in a group, sharing a single IP address, the virtual IP address. The virtual IP address is configured in each end-user workstation as a default gateway address and is cached in the host Address Resolution Protocol (ARP) cache.

In an HSRP or VRRP group, one router is elected to handle all requests sent to the virtual IP address. With HSRP, this is the active router. An HSRP group has one active router, at least one standby router, and perhaps many listening routers. A VRRP group has one master router and one or more backup routers

## Authentication Support for VRRP Groups

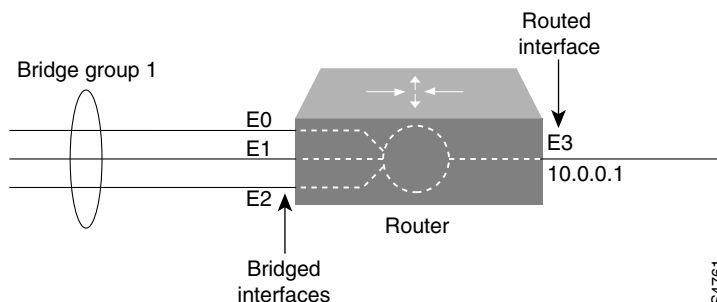
Authentication allows each VRRP group member to use text strings or MD5 authentication for security. MD5 provides greater security than the alternative plain-text authentication, because it enables each group member to use a secret key to generate an MD5 hash of a part of an outgoing packet. A keyed hash of an incoming packet is generated and if the generated hash does not match the hash within the incoming packet, the packet is ignored. The MD5 key can be configured using a key string or key chain.

With this release, MD5 has been added for VRRP groups so that routers in the group can authenticate peers using a more simple method than the method in RFC 2338.

## Integrated Routing and Bridging

Integrated routing and bridging (IRB) makes it possible to route a specific protocol between routed interfaces and bridge groups, or route a specific protocol between bridge groups. Local or unroutable traffic can be bridged among the bridged interfaces in the same bridge group, while routable traffic can be routed to other routed interfaces or bridge groups. [Figure 1](#) illustrates how IRB in a router interconnects a bridged network with a routed network.

**Figure 1** IRB Connecting a Bridged Network with a Routed Network



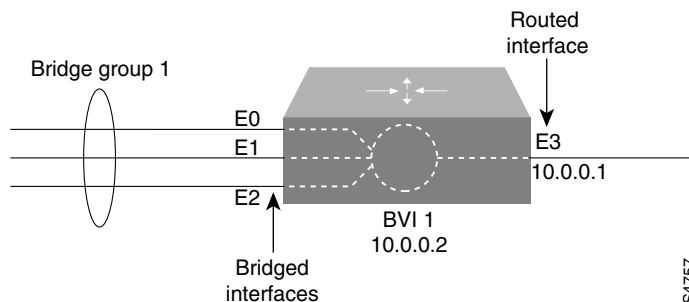
Cisco IOS software can be configured to route a specific protocol between routed interfaces and bridge groups or to route a specific protocol between bridge groups. Specifically, local or unroutable traffic is bridged among the bridged interfaces in the same bridge group, while routable traffic is routed to other routed interfaces or bridge groups. Using IRB, you can do the following:

- Switch packets from a bridged interface to a routed interface
- Switch packets from a routed interface to a bridged interface
- Switch packets within the same bridge group

## Bridge-Group Virtual Interface

In IRB, a bridge-group virtual interface (BVI) is used to avoid confusing the protocol configuration model when a specific protocol is both bridged and routed in a bridge group. [Figure 2](#) illustrates the BVI as a user-configured virtual interface residing within a router.

**Figure 2** BVI in a Router



A BVI does not support bridging, but does represent its corresponding bridge group to the routed interface. It has all the network layer attributes (such as a network layer address and filters) that apply to the corresponding bridge group. The interface number assigned to the BVI corresponds to the bridge group that the BVI represents. This number is the link between the virtual interface and the bridge group.

When routing is enabled for a given protocol on a BVI, packets coming from a routed interface, but destined for a host in a bridged domain, are routed to the BVI and are forwarded to the corresponding bridged interface. All traffic routed to the BVI is forwarded to the corresponding bridge group as bridged traffic. All routable traffic received on a bridged interface is routed to other routed interfaces as if it is coming directly from the BVI.

To receive routable packets arriving on a bridged interface but destined for a routed interface or to receive routed packets, the BVI must also have the appropriate addresses. The BVI borrows a MAC address of one of the bridged interfaces in the bridge group associated with the BVI. To route and bridge a given protocol in the same bridge group, the network layer attributes of the protocol on the BVI must be configured. No protocol attributes should be configured on the bridged interfaces, and no bridging attributes can be configured on the BVI.

**Note**

---

When a bridged domain contains learning devices (such as switches or bridges) that can learn the MAC address of a BVI, the BVI must be configured with its own MAC address—separate from the MAC addresses of the bridged interfaces in the bridge group that are associated with the virtual interface. The MAC address is configured by using the **mac-address** virtual interface command.

---

Because there can be only one BVI representing a bridge group, and the bridge group can be made up of different media types configured for several different encapsulation methods, the BVI may need to be configured with the particular encapsulation methods required to switch packets correctly. For example, the BVI has default data link and network layer encapsulations that are the same as those available on Ethernet interfaces, but the BVI can be configured with encapsulations that are not supported on an Ethernet interface.

In some cases, the default encapsulations provide appropriate results; in other cases they do not. For example, with default encapsulation, Advanced Research Projects Agency (ARPA) packets from the BVI are translated to Subnetwork Access Protocol (SNAP) when bridging IP to a Token Ring- or FDDI-bridged interface. But for Internet Packet Exchange (IPX), Novell-ether encapsulation from the BVI is translated to raw-token or raw-FDDI when bridging IPX to a Token Ring- or FDDI-bridged interface. Because this behavior is usually not what you want, IPX SNAP or Service Advertisement Protocol (SAP) encapsulation must be configured on the BVI. Refer to “Configuring Transparent Bridging Technology Overview” chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide* for more information on IRB.

## VRRP Support for Integrated Routing and Bridging

For redundancy, the BVIs are configured for HSRP or VRRP to prevent a single point of failure. In Cisco IOS Release 12.3(14)T, configuration of VRRP on BVIs has been added and is similar to the existing HSRP support for BVIs.

# How to Configure FHRP—VRRP Enhancements

This section contains the following procedures:

- [Configuring VRRP Support for Text-String Authentication, page 5](#)
- [Configuring VRRP Support for MD5 Authentication, page 7](#)
- [Configuring IRB and VRRP Support for IRB, page 12](#)

## Configuring VRRP Support for Text-String Authentication

Perform this task to configure text-string authentication for VRRP groups.

### Restrictions

Interoperability with vendors who may have implemented the RFC 2338 method is not enabled.

Text authentication cannot be combined with MD5 authentication for a VRRP group. When MD5 authentication is configured, the text authentication field in VRRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **vrrp group ip ip-address [secondary]**
6. **vrrp group priority level**
7. **vrrp group authentication text-string | text text-string**
8. Repeat Steps 1 through 7 on each router that will communicate.
9. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p><b>interface</b> <i>type number</i></p> <p><b>Example:</b> Router(config)# interface ethernet0/1</p>	<p>Configures an interface and enters interface configuration mode. The <i>type</i> argument is the type of interface to be configured. The <i>number</i> argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system.</p> <p><b>Note</b> Refer to the <i>Cisco IOS Interface and Hardware Command Reference</i>, Release 12.3T for more information.</p>
Step 4	<p><b>description</b> <i>string</i></p> <p><b>Example:</b> Router(config-if)# description md5auth</p>	<p>(Optional) Adds a description or comment to an interface to help you identify the interface.</p>
Step 5	<p><b>vrrp group ip</b> <i>ip-address</i> [<b>secondary</b>]</p> <p><b>Example:</b> Router(config-if)# vrrp 1 ip 10.21.0.10</p>	<p>Enables VRRP on an interface and identifies the IP address of the virtual router. The arguments and keyword are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—Virtual router group number.</li> <li><i>ip-address</i>—IP address of the virtual router.</li> <li><b>secondary</b>—(Optional) Additional IP addresses supported by this group.</li> </ul>
Step 6	<p><b>vrrp group priority</b> <i>level</i></p> <p><b>Example:</b> Router(config-if)# vrrp 1 priority 110</p>	<p>Assigns a priority level to the VRRP group. The arguments are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—Virtual router group number.</li> <li><i>level</i>—Priority of the router within the VRRP group. The range is from 1 to 254. The default is 100.</li> </ul>
Step 7	<p><b>vrrp group authentication</b> <i>text-string</i>   <b>text</b> <i>text-string</i></p> <p><b>Example:</b> Router(config-if)# vrrp 1 text f00c4s</p>	<p>Specifies either a text authentication or Message Digest 5 (MD5) authentication to the VRRP group. The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—VRRP group number.</li> <li><i>text-string</i>—Alphanumeric characters used to validate incoming VRRP packets.</li> <li><b>text</b>—Plain text authentication. The <i>text-string</i> argument is alphanumeric characters.</li> </ul>
Step 8	<p>Repeat Steps 1 through 7 on each router that will communicate.</p>	—
Step 9	<p><b>end</b></p> <p><b>Example:</b> Router(config-if)# end</p>	<p>Ends the configuration.</p>

## Configuring VRRP Support for MD5 Authentication

This section contains the following procedures that show how to configure VRRP support for MD5 authentication:

- [Configuring MD5 Authentication Using Key Strings, page 7](#) (required)
- [Configuring MD5 Authentication Using Key Chains, page 9](#) (required)
- [Verifying the VRRP MD5 Authentication Configuration, page 11](#) (optional)

### Configuring MD5 Authentication Using Key Strings

Perform this task to configure MD5 authentication for VRRP groups using a key string.

#### Restrictions

Interoperability with vendors who may have implemented the RFC 2338 method is not enabled.

Text authentication cannot be combined with MD5 authentication for a VRRP group. When MD5 authentication is configured, the text authentication field in VRRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **vrrp group ip** *ip-address* [**secondary**]
6. **vrrp group priority** *level*
7. **vrrp group authentication md5 key-string** [*key-string*]
8. Repeat Steps 1 through 7 on each router that will communicate.
9. **end**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p><b>interface</b> <i>type number</i></p> <p><b>Example:</b> Router(config)# interface ethernet0/1</p>	<p>Configures an interface and enters interface configuration mode. The <i>type</i> argument is the type of interface to be configured. The <i>number</i> argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system.</p> <p><b>Note</b> Refer to the <i>Cisco IOS Interface and Hardware Command Reference</i>, Release 12.3T for more information.</p>
Step 4	<p><b>description</b> <i>string</i></p> <p><b>Example:</b> Router(config-if)# description md5auth</p>	<p>(Optional) Adds a description or comment to an interface to help you identify the interface.</p>
Step 5	<p><b>vrrp group ip</b> <i>ip-address</i> [<b>secondary</b>]</p> <p><b>Example:</b> Router(config-if)# vrrp 1 ip 10.21.0.10</p>	<p>Enables VRRP on an interface and identifies the IP address of the virtual router. The arguments and keyword are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—Virtual router group number.</li> <li><i>ip-address</i>—IP address of the virtual router.</li> <li><b>secondary</b>—(Optional) Additional IP addresses supported by this group.</li> </ul>
Step 6	<p><b>vrrp group priority</b> <i>level</i></p> <p><b>Example:</b> Router(config-if)# vrrp 1 priority 110</p>	<p>Assigns a priority level to the VRRP group. The arguments are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—Virtual router group number.</li> <li><i>level</i>—Priority of the router within the VRRP group. The range is from 1 to 254. The default is 100.</li> </ul>
Step 7	<p><b>vrrp group authentication md5 key-string</b> [<i>key-string</i>]</p> <p><b>Example:</b> Router(config-if)# vrrp 1 authentication md5 key-string f00c4s</p>	<p>Specifies either a text authentication or Message Digest 5 (MD5) authentication to the VRRP group. The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—VRRP group number.</li> <li><b>md5</b>—MD5 authentication.</li> <li><b>key-string</b>—Authentication string. The optional <i>key-string</i> argument can be up to 64 characters. It is recommended that the string be at least 16 characters. No prefix to the <i>key-string</i> argument means that the key is unencrypted.</li> </ul> <p><b>Note</b> The key-string authentication method is encrypted if the <b>service password-encryption</b> command has been specified.</p>
Step 8	<p>Repeat Steps 1 through 7 on each router that will communicate.</p>	—
Step 9	<p><b>end</b></p> <p><b>Example:</b> Router(config-if)# end</p>	<p>Ends the configuration.</p>

## Configuring MD5 Authentication Using Key Chains

Perform this task to configure MD5 authentication for VRRP groups using a key chain.

### Restrictions

Interoperability with vendors who may have implemented the RFC 2338 method is not enabled.

Text authentication cannot be combined with MD5 authentication for a VRRP group. When MD5 authentication is configured, the text authentication field in VRRP hello messages is set to all zeroes on transmit and ignored on receipt, provided the receiving router also has MD5 authentication enabled.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **interface** *type number*
8. **description** *string*
9. **vrrp group ip** *ip-address* [**secondary**]
10. **vrrp group priority** *level*
11. **vrrp group authentication md5 key-chain** *key-chain*
12. Repeat Steps 1 through 11 on each router that will communicate.
13. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>key chain</b> <i>name-of-chain</i>  <b>Example:</b> Router(config)# key chain vrrp1	Specifies a name of a key chain and enters key configuration mode. A key chain must have at least one key and can have up to 2147483647 keys.  <b>Note</b> You must configure a key chain with keys to enable authentication. Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol.

	Command or Action	Purpose
Step 4	<p><b>key</b> <i>key-id</i></p> <p><b>Example:</b> Router(config-key) key 1</p>	Specifies an ID number for a key chain. The range is from 0 to 2147483647. The numbers do not have to be consecutive.
Step 5	<p><b>key-string</b> <i>string</i></p> <p><b>Example:</b> Router(config-key)# key-string Abc246</p>	Specifies the authentication string that must be sent and received in the packets using the routing protocol being authenticated. The <i>string</i> argument can contain from 1 to 80 uppercase and lowercase alphanumeric characters, except that the first character cannot be a number.
Step 6	<p><b>exit</b></p> <p><b>Example:</b> Router(config-key)# exit</p>	Exits to global configuration mode.
Step 7	<p><b>interface</b> <i>type number</i></p> <p><b>Example:</b> Router(config)# interface ethernet0/1</p>	<p>Configures an interface and enters interface configuration mode. The <i>type</i> argument is the type of interface to be configured. The <i>number</i> argument is the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system.</p> <p><b>Note</b> Refer to the <i>Cisco IOS Interface and Hardware Command Reference</i>, Release 12.3T for more information.</p>
Step 8	<p><b>description</b> <i>string</i></p> <p><b>Example:</b> Router(config-if)# description md5auth</p>	(Optional) Adds a description or comment to an interface to help you identify the interface.
Step 9	<p><b>vrrp</b> <i>group ip ip-address</i> [<b>secondary</b>]</p> <p><b>Example:</b> Router(config-if)# vrrp 1 ip 10.21.0.10</p>	<p>Enables VRRP on an interface and identifies the IP address of the virtual router. The arguments and keyword are as follows:</p> <ul style="list-style-type: none"> <li>• <i>group</i>—Virtual router group number.</li> <li>• <i>ip-address</i>—IP address of the virtual router.</li> <li>• <b>secondary</b>—(Optional) Additional IP addresses supported by this group.</li> </ul>
Step 10	<p><b>vrrp</b> <i>group priority level</i></p> <p><b>Example:</b> Router(config-if)# vrrp 1 priority 110</p>	<p>Assigns a priority level to the VRRP group. The arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <i>group</i>—Virtual router group number.</li> <li>• <i>level</i>—Priority of the router within the VRRP group. The range is from 1 to 254. The default is 100.</li> </ul>

	Command or Action	Purpose
Step 11	<pre> <b>vrrp group authentication md5 key-chain</b> key-chain  <b>Example:</b> Router(config-if)# vrrp 1 authentication md5 key-chain vrrp1 </pre>	<p>Specifies either a text authentication or MD5 authentication to the VRRP group. The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—VRRP group.</li> <li><b>md5</b>—MD5 authentication.</li> <li><b>key-chain</b>—Authentication using a live key and key ID. The <i>key-chain</i> argument specifies a string and must match the assigned key-chain name using the <b>key chain</b> command.</li> </ul> <p><b>Note</b> The key-chain name must match the name specified in Step 3.</p>
Step 12	Repeat Steps 1 through 11 on each router that will communicate.	—
Step 13	<pre> <b>end</b>  <b>Example:</b> Router(config-if)# end </pre>	Ends the configuration.

## Verifying the VRRP MD5 Authentication Configuration

To verify the MD5 authentication configuration, perform the following steps.

### SUMMARY STEPS

1. **show vrrp**
2. **debug vrrp authentication**

### DETAILED STEPS

#### Step 1 **show vrrp**

Use this command to verify that the authentication is configured correctly, for example:

```

Router# show vrrp

Ethernet0/1 - Group 1
State is Master
Virtual IP address is 10.21.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption is enabled
  min delay is 0.000 sec
Priority is 100
Authentication MD5, key-string "f00d4s"
Master Router is 10.21.0.1 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec

```

This output shows that MD5 authentication is configured with the f00d4s key string.

**Step 2 debug vrrp authentication**

Use this command to verify that both routers have authentication configured, that the MD5 key ID is the same on each router, and the MD5 key strings are the same on each router, for example:

```
Router# debug vrrp authentication

VRRP: Grp 1 Advertisement from 10.24.1.1 has incorrect authentication type 0 expected 254

!MD5 key IDs differ on each router.

VRRP: Grp 1 recalculate MD5 digest: "3n};oHp8_)_7-C"
VRRP: Grp 1 Advertisement from 10.24.1.1 has FAILED MD5 authentication

!The MD5 key strings differ on each router.

VRRP: Grp 1 received MD5 digest:
"_M^uMiWo^|t?t2m"
VRRP: Grp 1 Advertisement from 10.24.1.1 has FAILED MD5 authentication

!The text authentication strings differ on each router.

VRRP: Grp 1 Advertisement from 172.24.1.1 has FAILED TEXT authentication
```

## Configuring IRB and VRRP Support for IRB

This section contains the following procedures:

- [Enabling BVI Bridging and Configuring a BVI Group, page 12](#) (required)
- [Configuring the BVI Interface and Enabling VRRP Support on the BVI for IRB, page 14](#) (required)
- [Enabling IRB on the Interfaces, page 16](#) (required)

### Enabling BVI Bridging and Configuring a BVI Group

Perform this task to enable BVI bridging and to configure a BVI group.

Due to the forwarding delay that is associated with the initialization of a BVI interface, it is necessary to set the VRRP advertise timer to a value equal to or greater than the forwarding delay on the BVI interface. This setting prevents a VRRP router on a recently initialized BVI interface from unconditionally taking over the master role. See the [“Configuring the BVI Interface and Enabling VRRP Support on the BVI for IRB”](#) section on page 14.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge irb**
4. **bridge *bridge-group* protocol {dec | ibm | ieee | vlan-bridge}**
5. **bridge *bridge-group* route protocol {appletalk | cln | decnet | ip | ipx}**
6. **bridge *bridge-group* forward-time *seconds***
7. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>bridge irb</b></p> <p><b>Example:</b> Router(config)# bridge irb</p>	<p>Enables the Cisco IOS software to route a given protocol between routed interfaces and bridge groups or to route a given protocol between bridge groups.</p>
Step 4	<p><b>bridge bridge-group protocol {dec   ibm   ieee   vlan-bridge}</b></p> <p><b>Example:</b> Router(config)# bridge 100 protocol ieee</p>	<p>Defines the type of Spanning Tree Protocol (STP). The argument and keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <i>bridge-group</i>—Number of the bridge group.</li> <li>• <b>dec</b>—Digital STP.</li> <li>• <b>ibm</b>—IBM STP.</li> <li>• <b>ieee</b>—IEEE Ethernet STP.</li> <li>• <b>vlan-bridge</b>—virtual local-area network (VLAN) STP.</li> </ul> <p><b>Note</b> IEEE 802.1D STP is the preferred method of running a bridge.</p>
Step 5	<p><b>bridge bridge-group route protocol {appletalk   cln   decnet   ip   ipx}</b></p> <p><b>Example:</b> Router(config)# bridge 100 route ip</p>	<p>Enables the routing of a specified protocol in a specified bridge group. The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <i>bridge-group</i>—Number of the bridge group specified using the <b>bridge protocol</b> command.</li> <li>• <i>protocol</i>—One of the following protocols: <ul style="list-style-type: none"> <li>– <b>appletalk</b></li> <li>– <b>cln</b></li> <li>– <b>decnet</b></li> <li>– <b>ip</b></li> <li>– <b>ipx</b></li> </ul> </li> </ul>

	Command or Action	Purpose
Step 6	<p><b>bridge</b> <i>bridge-group</i> <b>forward-time</b> <i>seconds</i></p> <p><b>Example:</b> Router(config)# bridge 100 forward-time 4</p>	<p>Sets the forward-delay interval for the bridge group. The arguments are as follows:</p> <ul style="list-style-type: none"> <li><i>bridge-group</i>—Bridge-group number specified using the <b>bridge route</b> command.</li> <li><i>seconds</i>—Forward-delay interval. It must be a value in the range from 4 to 200 seconds. The default is 30 seconds.</li> </ul> <p><b>Note</b> The forward time configured in this step should match the advertisement time set using the <b>vrrp timers advertise</b> command. See the “<a href="#">Configuring the BVI Interface and Enabling VRRP Support on the BVI for IRB</a>” section on page 14.</p>
Step 7	<p><b>end</b></p> <p><b>Example:</b> Router(config)# end</p>	<p>Ends the configuration.</p>

## Configuring the BVI Interface and Enabling VRRP Support on the BVI for IRB

Perform this task to configure the BVI interfaces.

The BVI interface does not appear in a router configuration until it is created by using the **interface** command. The number that is used to create the BVI must be the same number as the bridge group. For example, specify BVI 100 as the interface type and number with the **interface** command to create the BVI to be used with bridge-group 100.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **vrrp group ip** *ip-address* [**secondary**]
6. **vrrp group priority** *level*
7. **vrrp group authentication md5 key-chain** *key-chain*
8. **vrrp group timers advertise** [*seconds* | **msec msec** | **learn**]
9. **no shutdown**
10. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>interface</b> <i>type number</i></p> <p><b>Example:</b> Router(config)# interface bvi 100</p>	<p>Configures a BVI and enters interface configuration mode.</p> <p><b>Note</b> Specify BVI as the type of interface and the bridge-group number that is to be associated with this interface as the number.</p>
Step 4	<p><b>ip address</b> <i>ip-address mask</i> [<b>secondary</b>]</p> <p><b>Example:</b> Router(config-if)# ip address 10.2.3.2 255.0.0.0</p>	<p>Specifies the IP address of the interface and the associated subnet. The arguments and keyword are as follows:</p> <ul style="list-style-type: none"> <li><i>ip-address mask</i>—IP address and mask for the associated IP subnet.</li> <li><b>secondary</b>—(Optional) Configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul>
Step 5	<p><b>vrrp group ip</b> <i>ip-address</i> [<b>secondary</b>]</p> <p><b>Example:</b> Router(config-if)# vrrp 100 ip 10.24.1.254</p>	<p>Enables VRRP on an interface and identifies the IP address of the virtual router. The arguments and keyword are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—Virtual router group number.</li> <li><i>ip-address</i>—IP address of the virtual router.</li> <li><b>secondary</b>—(Optional) Additional IP addresses supported by this group.</li> </ul>
Step 6	<p><b>vrrp group priority</b> <i>level</i></p> <p><b>Example:</b> Router(config-if)# vrrp 1 priority 110</p>	<p>Assigns a priority level to the VRRP group. The arguments are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—Virtual router group number.</li> <li><i>level</i>—Priority of the router within the VRRP group. The range is from 1 to 254. The default is 100.</li> </ul>

	Command or Action	Purpose
Step 7	<pre> <b>vrp</b> <i>group</i> <b>authentication md5 key-chain</b> <i>key-chain</i>  <b>Example:</b> Router(config-if)# vrrp 1 authentication md5 key-chain vrrp1 </pre>	<p>Specifies either a text authentication or MD5 authentication to the VRRP group. The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—VRRP group.</li> <li><b>md5</b>—MD5 authentication.</li> <li><b>key-chain</b>—Authentication using a live key and key ID. The <i>key-chain</i> argument specifies a string and must match the assigned key-chain name using the <b>key chain</b> command specified in Step 3.</li> </ul> <p><b>Note</b> Only the MD5 authentication method is shown here. Plain-text authentication can be configured also for BVIs. See the <a href="#">“Configuring VRRP Support for Text-String Authentication”</a> section on page 5.</p>
Step 8	<pre> <b>vrp</b> <i>group</i> <b>timers advertise</b> [<i>seconds</i>   <b>msec</b> <i>msec</i>]   <b>learn</b>  <b>Example:</b> Router(config-if)# vrrp 100 timers advertise 4 </pre>	<p>Configures the interval between successive advertisements by the master virtual router in a VRRP group. The arguments and keywords are as follows:</p> <ul style="list-style-type: none"> <li><i>group</i>—Virtual router group number.</li> <li><i>seconds</i>—(Optional) Advertisement interval in seconds. The range is from 1 to 255.</li> <li><b>msec</b>—(Optional) Unit of the advertisement time in milliseconds. If this keyword is not specified, the timer is set in seconds. The <i>msec</i> argument has a range from 50 to 999.</li> <li><b>learn</b>—(Optional) Learn timer values.</li> </ul> <p><b>Note</b> The interval time configured in this step should match the forward time set for the bridge group protocol and route. See the <a href="#">“Enabling BVI Bridging and Configuring a BVI Group”</a> section on page 12.</p>
Step 9	<pre> <b>no shutdown</b>  <b>Example:</b> Router(config-if) no shutdown </pre>	<p>Restarts the disabled interface configured in Step 3.</p>
Step 10	<pre> <b>end</b>  <b>Example:</b> Router(config)# end </pre>	<p>Ends the configuration</p>

## Enabling IRB on the Interfaces

Perform this task to enable IRB on the interfaces.

### Prerequisites

The bridge associated with the BVI interfaces must have the forwarding delay time set to its minimum value of 4 seconds with the **bridge forward-time** command.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bridge-group** *bridge-group*
5. Repeat Steps 3 and 4 until all of the interfaces are configured for the bridge group.
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface bvi100	Configures an interface and enters interface configuration mode.  <b>Note</b> Specify BVI as the type of interface and the bridge-group number that is to be associated with this interface as the number.
Step 4	<b>bridge-group</b> <i>bridge-group</i>  <b>Example:</b> Router(config-if)# bridge-group 100	Enables the bridge group on the interface. The <i>bridge-group</i> argument specifies the number of the group. The range is from 1 to 255.  <b>Note</b> Specify the bridge-group number that was used to create the BVI.
Step 5	Repeat Steps 3 and 4 until all of the interfaces are configured for the bridge group.	—
Step 6	<b>end</b>  <b>Example:</b> Router(config-if)# end	Ends the configuration.

## Configuration Examples for FHRP—VRRP Enhancements

This section contains the following configuration examples:

- [MD5 Authentication Configuration Using a Key String: Example, page 18](#)
- [MD5 Authentication Configuration Using a Key Chain: Example, page 18](#)
- [IRB and VRRP with MD5 Key-Chain Authentication Configuration: Example, page 18](#)

## MD5 Authentication Configuration Using a Key String: Example

The following example shows how to configure MD5 authentication using a key string:

```
interface Ethernet0/1
  description my-cat5a-7/10
  vrrp 1 ip 10.21.0.10
  vrrp 1 priority 110
  vrrp 1 authentication md5 key-string f00c4s
```

## MD5 Authentication Configuration Using a Key Chain: Example

The following example shows how to configure MD5 authentication using a key chain:

```
key chain vrrp1
  key 1
  key-string f00c4s
  exit
!
interface ethernet0/1
  description my-cat5a-7/10
  vrrp 1 ip 10.21.0.10
  vrrp 1 priority 110
  vrrp 1 authentication md5 key-chain vrrp1
```

In this example, VRRP queries the key chain to obtain the current live key and key ID for the specified key chain.

## IRB and VRRP with MD5 Key-Chain Authentication Configuration: Example

This section contains the following examples:

- [IRB and Bridge-Group Configuration: Example, page 18](#)
- [BVI Interface and VRRP with MD5 Key-Chain Configuration for IRB: Example, page 19](#)
- [IRB Bridge Group on an Interface Configuration: Example, page 19](#)

## IRB and Bridge-Group Configuration: Example

The following example shows how to enable IRB:

```
bridge irb
!
bridge 100 protocol ieee
bridge 100 route ip
bridge 100 forward-time 4
```

## BVI Interface and VRRP with MD5 Key-Chain Configuration for IRB: Example

The following example shows how to configure a BVI interface for IRB, and VRRP with MD5 key-chain authentication:

```
interface BVI100
 ip address 10.24.1.1 255.255.255.0
 vrrp 1 ip 10.24.1.254
 vrrp 1 timers advertise 4
 vrrp 1 priority 200
 vrrp 1 authentication md5 key-chain vrrp1
 vrrp 100 ip 10.0.0.1
 vrrp 100 timers advertise 4
```

## IRB Bridge Group on an Interface Configuration: Example

The following example shows how to enable the BVI bridge group on an interface:

```
interface ethernet0/1
 bridge-group 100
!
interface ATM4/0/0
 bridge-group 100
```

## Additional References

The following sections provide references related to the FHRP—VRRP Enhancements feature.

## Related Documents

Related Topic	Document Title
IP addressing and services configuration tasks	<a href="#">Cisco IOS IP Configuration Guide</a> , Release 12.3
IP addressing and services commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<a href="#">Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</a> , Release 12.3T
IRB overview and configuration tasks	<i>Integrated Routing and Bridging (IRB) Support for the Cisco MGX-RPM-XF-512</i> , Cisco Release 12.3(14)T “Configuring Transparent Bridging Technology Overview” chapter of the <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> , Release 12.2
Bridging and switching overview and configuration tasks	<a href="#">Cisco IOS Bridging and IBM Networking Configuration Guide</a> , Release 12.3 <a href="#">Cisco IOS Switching Services Configuration Guide</a> , Release 12.3

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents one new command and modified commands only.

### New Commands

- [debug vrrp authentication](#)

### Modified Commands

- [show vrrp](#)
- [vrrp authentication](#)

# debug vrrp authentication

To display debugging messages for Virtual Router Redundancy Protocol (VRRP) Message Digest 5 (MD5) authentication, use the **debug vrrp authentication** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug vrrp authentication**

**no debug vrrp authentication**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Examples** The following sample output shows that MD5 authentication is enabled on one router but not the other:

```
Router# debug vrrp authentication

VRRP: Grp 1 Advertisement from 172.24.1.1 has incorrect authentication type 0 expected 254
```

The following sample output shows that the MD5 key IDs and key strings differ on each router:

```
Router# debug vrrp authentication

VRRP: Grp 1 recalculate MD5 digest: "3n};oHp8_)_7-C"
VRRP: Grp 1 received MD5 digest: "_M^uMiWo^|t?t2m"
VRRP: Grp 1 Advertisement from 172.24.1.1 has FAILED MD5 authentication
```

The following sample output shows that the text authentication strings differ on each router:

```
Router# debug vrrp authentication

VRRP: Grp 1 Advertisement from 172.24.1.1 has FAILED TEXT authentication
```

Related Commands	Command	Description
	<b>debug vrrp error</b>	Displays debugging messages about VRRP error conditions.
	<b>debug vrrp events</b>	Displays debugging messages about VRRP events.
	<b>debug vrrp state</b>	Displays debugging messages about the VRRP state transitions.

# show vrrp

To display a brief or detailed status of one or all configured Virtual Router Redundancy Protocol (VRRP) groups on the router, use the **show vrrp** command in privileged EXEC mode.

**show vrrp** [**brief** | *group*]

Syntax Description	Parameter	Description
	<b>brief</b>	(Optional) Provides a summary view of the group information.
	<i>group</i>	(Optional) Virtual router group number of the group for which information is to be displayed. The group number is configured with the <b>vrrp ip</b> command.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.0(18)ST	This command was introduced.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.3(2)T	This command was enhanced to display the state of a tracked object.
	12.3(14)T	This command was enhanced to display MD5 authentication for a VRRP using text strings, key chains or key strings.

**Usage Guidelines** If no group is specified, all groups are displayed.

**Examples** The following is sample output from the **show vrrp** command:

```
Router# show vrrp

Ethernet1/0 - Group 1
State is Master
Virtual IP address is 10.2.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3.000 sec
Preemption is enabled
  min delay is 0.000 sec
Priority 100
  Track object 1 state down decrement 15
Master Router is 10.2.0.1 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down interval is 9.609 sec

Ethernet1/0 - Group 2
State is Master
Virtual IP address is 10.0.0.20
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 1.000 sec
```

```

Preemption is enabled
  min delay is 0.000 sec
Priority 95
Master Router is 10.0.0.1 (local), priority is 95
Master Advertisement interval is 1.000 sec
Master Down interval is 3.628 sec

```

Table 1 describes the significant fields shown in the display.

**Table 1** *show vrrp Field Descriptions*

Field	Description
EthernetI/0 - Group	Interface type and number, and VRRP group number.
State is	Role this interface plays within VRRP (master or backup).
Virtual IP address is	Virtual IP address for this group.
Virtual MAC address is	Virtual MAC address for this group.
Advertisement interval is	Interval at which the router will send VRRP advertisements when it is the master virtual router. This value is configured with the <b>vrrp timers advertise</b> command.
Preemption is	Preemption is either enabled or disabled.
Track object	Object number representing the object to be tracked.
state	State value (up or down) of the object being tracked.
decrement	Amount by which the priority of the router is decremented (or incremented) when the tracked object goes down (or comes back up).
Priority	Priority of the interface.
Master Router is	IP address of the current master virtual router.
priority is	Priority of the current master virtual router.
Master Advertisement interval is	Advertisement interval of the master virtual router.
Master Down interval is	Calculated time that the master virtual router can be down before the backup virtual router takes over.

The following is sample output from the **show vrrp** command with the **brief** keyword:

```
Router# show vrrp brief
```

```

Interface      Grp  Prio  Time   Own  Pre  State   Master addr  Group addr
Ethernet1/0    1   100   3609           P  Master  1.0.0.4    1.0.0.10
Ethernet1/0    2   105   3589           P  Master  1.0.0.4    1.0.0.20

```

Table 2 describes the fields shown in the display.

**Table 2** *show vrrp brief Field Descriptions*

Field	Description
Interface	Interface type and number.
Grp	VRRP group to which this interface belongs.
Prio	VRRP priority number for this group.

**Table 2** *show vrrp brief Field Descriptions (continued)*

Field	Description
Time	Calculated time that the master virtual router can be down before the backup virtual router takes over.
Own	IP address owner.
Pre	Preemption status. P indicates that preemption is enabled. If this field is empty, preemption is disabled.
State	Role this interface plays within VRRP (master or backup).
Master addr	IP address of the master virtual router.
Group addr	IP address of the virtual router.

The following sample output shows the MD5 authentication for a VRRP group using a key string:

```
Router# show vrrp

Ethernet0/1 - Group 1
State is Master
Virtual IP address is 10.21.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption is enabled
  min delay is 0.000 sec
Priority is 100
Authentication MD5, key-string "f00b4r"
Master Router is 10.21.0.1 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec
```

See [Table 1](#) for descriptions of the significant fields in the output.

**Related Commands**

Command	Description
<b>vrrp ip</b>	Enables VRRP on an interface and identifies the IP address of the virtual router.

## vrrp authentication

To authenticate Virtual Router Redundancy Protocol (VRRP) packets received from other routers in the group, use the **vrrp authentication** command in interface configuration mode. To disable VRRP authentication, use the **no** form of this command.

```
vrrp group authentication {text text-string | md5 {key-string [0 | 7 | key-string] | key-chain key-chain}
```

```
no vrrp group authentication {text text-string | md5 {key-string [0 | 7 | key-string] | key-chain key-chain}
```

### Syntax Description

<i>group</i>	Virtual router group number for which authentication is being configured. The group number is configured with the <b>vrrp ip</b> command.
<b>text</b> <i>text-string</i>	Plain text authentication. The <i>text-string</i> argument is the authentication string and can be up to eight alphanumeric characters.
<b>md5</b>	Message Digest 5 (MD5) authentication. The arguments and keywords are as follows: <ul style="list-style-type: none"> <li>• <b>key-string</b>—Authentication string. The optional argument and keywords are as follows: <ul style="list-style-type: none"> <li>– <b>0</b>—(Optional) The key is unencrypted.</li> <li>– <b>7</b>—(Optional) The key is encrypted.</li> <li>– <i>key-string</i>—Up to 64 characters. It is recommended that the string be at least 16 characters. No prefix to the <i>key-string</i> argument means that the key is unencrypted.</li> </ul> </li> <li>• <b>key-chain</b>—Authentication using a live key and key ID. The <i>key-chain</i> argument specifies a string, and must match the assigned key-chain name using the <b>key chain</b> command.</li> </ul> <p><b>Note</b> The key-string authentication method is encrypted if the <b>service password-encryption</b> command has been specified.</p>

### Defaults

VRRP authentication is disabled.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	The <b>md5</b> , <b>key-string</b> , <b>0</b> , <b>7</b> , and <b>key-chain</b> keywords were added. The <i>text-string</i> , <i>key-string</i> , and <i>key-chain</i> arguments were added.

**Usage Guidelines**

When a VRRP packet arrives from another router in the VRRP group, its authentication string is compared to the string configured on the local system. If the strings match, the message is accepted. If they do not match, the packet is discarded.

All routers within the group must be configured with the same authentication string.

**Note**

Plain text authentication is not meant to be used for security. It simply provides a way to prevent a router that does not belong to a configured VRRP group from participating in it.

**Examples**

The following example shows how to configure an authentication text string of x30dn78k:

```
vrrp 1 authentication x30dn78k
```

The following example shows how to configure an MD5 key string:

```
interface Ethernet0/1
  description ed1-cat5a-7/10
  vrrp 1 ip 10.21.0.10
  vrrp 1 priority 110
  vrrp 1 authentication md5 key-string f00c4s
```

The key ID for key-string authentication is always zero. If a key chain is configured with a key ID of zero, then the following configuration will work:

**Router 1**

```
key chain vrrp1
  key 0
  key-string 54321098452103ab
!
interface Ethernet0/1
  vrrp 1 ip 10.21.0.10
  vrrp 1 authentication md5 key-chain vrrp1
```

**Router 2**

```
interface Ethernet0/1
  vrrp 1 ip 10.21.0.10
  vrrp 1 authentication md5 key-string 54321098452103ab
```

**Related Commands**

Command	Description
<b>key chain</b>	Enables authentication for routing protocols.
<b>service password-encryption</b>	Encrypts passwords.
<b>vrrp ip</b>	Enables VRRP and identifies the IP address of the virtual router.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

