



Release Notes for Cisco ATA 186 Release 2.14

May 20, 2002

OL-1269-05 Rev. B0

These release notes describe newly incorporated features including resolved and open issues for the Cisco Analog Telephone Adaptor (ATA) 186 Release 2.14 for the SIP and H.323 images.

Contents

These release notes provide the following information:

- [Introduction: Cisco ATA 186 Analog Telephone Adaptor, page 1](#)
- [New Features in Release 2.14, page 2](#)
- [Changes for H.323 and SIP, page 5](#)
- [Open Issues in Cisco ATA 186 Release 2.14, page 10](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation, page 10](#)
- [Obtaining Technical Assistance, page 11](#)

Introduction: Cisco ATA 186 Analog Telephone Adaptor

The Cisco ATA 186:

- Is an analog telephone adaptor that interfaces analog telephones to IP-based telephony networks.
- Is installed at the subscriber's premises and supports two voice ports, each with its own independent telephone number.



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

Downloading and Upgrading the Software

To take advantage of the features of Cisco ATA 186 Release 2.14, you must upgrade the Cisco ATA 186 software. You can download the software at:

<http://www.cisco.com/cgi-bin/tablebuild.pl/ata186>

For more information, see the *Cisco ATA 186 Installation and Configuration Guide*.

New Features in Release 2.14

This section contains information on new and changed features for Cisco ATA 186 Release 2.14.

- [SIP Proxy Server Redundancy](#)
- [OutBoundProxy Support](#)
- [UseTFTP Value](#)
- [INVITE Messages](#)
- [SIPPort Configuration Parameter](#)
- [SIPRegInterval Configuration Parameter](#)
- [RequestURL](#)
- [NAT/PAT Translation](#)
- [Proxy Redundancy](#)
- [Dial-String Prefixes Support](#)
- [Hotline and Warmline Functionality](#)

New Features in Release 2.14

SIP Proxy Server Redundancy

SIP Proxy Server redundancy can be enabled by entering FQDN or IP address (and optional port number) in GkOrProxy and AltGk, with the proper value of AltGkTimeout. If hostnames are given for GkOrProxy or AltGk, they are resolved by the configured DNS. DNS results are cached for a hard-coded period of 10 minutes.

If DNS returns multiple IP addresses, only the first IP address is used. If AltGk is set to “0” (disabled) and DNS returns two or more IP addresses for GkOrProxy, then the first IP address is used as the primary proxy and the second IP address as the secondary proxy. If GkOrProxy is an IP address or DNS returns one IP address, then the backup SIP proxy is not available in this case. A special case exists if GkOrProxy and AltGk are the same and are not IP addresses. Then AltGk is treated as “0”.

OutBoundProxy Support

If OutBoundProxy is an FQDN and DNS returns multiple IP addresses, the first IP address is used as the primary outbound proxy and the second IP as the secondary outbound proxy. If OutBoundProxy is an IP address or DNS returns only one IP address, then a backup outbound proxy is not available. The backup proxy timeout value for the outbound proxy is also determined by the AltGkTimeout parameter.

If the backup proxy fails, the Cisco ATA 186 automatically switches back to the primary proxy if the unit has stayed with the backup proxy for at least 30 seconds. This effectively prevents the Cisco ATA 186 from switching indefinitely between a failing primary and failing backup proxy for the same transactions.

Switching between primary and secondary proxies and retrying can only happen for initial INVITE and REGISTER requests. Other requests, such as CANCEL, BYE, ACK, and re-INVITE, do not retry the alternate proxy but give up if the current proxy fails. This avoids such dilemmas as honoring Record-Route information inserted by a failing proxy. If the primary proxy fails after the call has been established, neither side can end the call with a BYE. The UA times out and goes back to idle after this happens.

When OutBoundProxy is enabled, the Cisco ATA 186 needs to determine whether it should retry with the backup OutBoundProxy or backup SIP proxy if the INVITE or REGISTER request fails. The Cisco ATA 186 assumes that if the reason for failure is an ICMP error (such as unreachable host), then it must retry with the backup outbound proxy. If failure is due to timeout while waiting for a response or a 5xx response, it retries the backup SIP proxy. The Cisco ATA 186 assumes that a response can only come from the SIP proxy server, where the outbound proxy is a pure forwarder or some ALG.

Disabling Access To The Web Interface

To prevent tampering and unauthorized access to the Cisco ATA 186 configuration, the Cisco ATA 186 built-in web server can now be disabled.

Operation:

Parameter: OpFlags
 Bit: 7
 Bitmask: 0x00000080
 IVR code: 323
 Values: 0 = Enable web server
 1 = Disable web server

Once the web server is disabled, you may only configure the Cisco ATA 186 through TFTP or IVR.



Note

When configuring the ATA 186 via the IVR, hexadecimal values must be entered as decimal values. This may be awkward, and it is recommended that TFTP configuration be used.

Examples:

1. Assuming an existing OpFlags value of 0x2, to disable the web server, select menu option 323 from the IVR and enter the value 130 (0x82).

When you attempt to access the ATA 186 via the web, the following error messages will be displayed.

- Netscape: The document contained no data. Try again later, or contact the server's administrator.
- Explorer: The page cannot be displayed.

2. Assuming an existing OpFlags value of 0x82, to enable the web server, select menu option 323 from the IVR and enter the value 2 (0x2).

Hardware Information Display

The Cisco ATA 186 hardware information is now displayed in the lower left corner of the web interface.

Changes in Release 2.14

This section lists the changes in the Cisco ATA 186 Release 2.14.

UseTFTP Value

The default value for UseTFTP is now set to “1”.

Changes for the SIP Protocol

This section lists the changes in the Cisco ATA 186 Release 2.14 when using the SIP protocol.

INVITE Messages

The Cisco ATA 186 no longer accepts original INVITE messages with a To-Tag. In Cisco ATA 186 Release 2.14, such INVITES are rejected with a 481 response.

If the Cisco ATA 186 receives a Re-INVITE message containing an SDP identical to the one most recently received from the far end, it treats this Re-INVITE as an Audit message and sends in response a 200 OK message with the SDP most recently sent to the far end. The Cisco ATA 186 then takes no further action regarding the Audit message. Prior to Cisco ATA 186 Release 2.14, the Cisco ATA 186 did not distinguish an Audit message from a regular INVITE message.

SIPPort Configuration Parameter

If the SIPPort configuration parameter is set to 0, the Cisco ATA 186 uses 5060 as the operating SIPPort value. Prior to Cisco ATA 186 Release 2.14, all port values less than 5060 were replaced by 5060.

SIPRegInterval Configuration Parameter

The Cisco ATA 186 allows the SipRegInterval configuration parameter to be a minimum of 1 second and a maximum of one day ($24 \times 3600 = 86400$ seconds). If SipRegInterval is set to 0, the Cisco ATA 186 uses the default value of 3600 seconds. Prior to Cisco ATA 186 Release 2.14, the minimum allowable value of SIPRegInterval was 120 seconds, the maximum allowable value was 7200 seconds, and a configured value of 0 directed the Cisco ATA 186 to use 120 seconds as its operating value.

RequestURL

The Cisco ATA 186 now uses the first URL from the Record-Route as the RequestURL in SIP requests sent when the Cisco ATA 186 is a callee. Prior to Cisco ATA 186 Release 2.14, SIP requests generated by the Cisco ATA 186 as a callee use the Contact Header information in the RequestURI, while SIP requests generated by the Cisco ATA 186 as a caller use the Record-Route information in the RequestURL.

NAT/PAT Translation

To maintain NAT/PAT translation for a session, the Cisco ATA 186 can now be configured to periodically send dummy UDP packets to a server (the Cisco ATA 186 does not expect any response from the server).

Configuration

The retransmission period (in seconds) is specified in the lower 12 bits of the new 32-bit NatTimer configuration Parameter. At present, the upper 20 bits are set to 0. NatTimer values are entered in hexadecimal format.

Example: NatTimer = 0x0000000a sets the period to 10 seconds

The server to which the dummy packet is sent is specified in the new NatServer configuration parameter. NatServer can contain up to 47 characters. This can be FQDN or IP format with an optional port parameter (separated from the address by a ':'). If port is not specified, the Cisco ATA 186 uses the value 5060.

Examples:

```
NatServer = server.cisco.com:1234
```

```
NatServer = 129.23.123.12:1234
```

```
NatServer = server.cisco.com
```

Proxy Redundancy

The Cisco ATA 186 now supports proxy redundancy by means of backup SIP proxy and backup OutBoundProxy. The Cisco ATA 186 configuration profile has 4 fields to configure proxy information:

- GkOrProxy: Primary SIP proxy server (FQDN or IP format with optional [:port])
- AltGk: Secondary or backup SIP proxy server; same format as GkOrProxy
- AltGkTimeOut: Time out in seconds for switching from backup proxy to primary proxy. If this parameter is set to 0, the Cisco ATA 186 uses the backup proxy until it fails.
- OutBoundProxy: A proxy (such as an ALG) to which all outbound SIP requests are sent as the next hop; same format as GkOrProxy

If the port parameter is not specified, 5060 is assumed.

Changes for H.323 and SIP

This section lists the changes in the Cisco ATA 186 Release 2.14 when using the SIP protocol.

Dial-String Prefixes Support

The Cisco ATA 186 now supports dial-string prefixes on a limited basis.

Configuration

Syntax: The DialPlan configuration parameter now accepts the rule “Ptntnnn”, where:

'P' = DialPlan Prefix Rule Identifier

't' = 0-9, *, #, 'n', 'N', 'a', or 'A'

'n' = 1-9

'N' = 0-9

'a' = 1-9, *, #

'A' = 0-9, *, #

'nnnn' = variable length prefix

't' is the trigger digit that adds a prefix to the dialed number if the rule is satisfied. The first digit dialed is compared against the trigger digit 't'. If the rule is satisfied, the prefix “nnnn” is added to the phone number.

Example: To add the prefix “408” to any dialed number that does not begin with a digit 0, the rule would be “Pn408”.

Hotline and Warmline Functionality

The Cisco ATA 186 now has Dial Plan support for hotline and warmline functionality.

Configuration

The DialPlan configuration parameter now accepts the rule “Hdnnnn”, where d is the post-off hook delay (in seconds — use 0-9 or a-z to specify a delay in the range of 0 to 35 seconds), and nnnn is the variable length phone number to call when no digit is entered for d seconds after the phone is taken off hook.

Example 1: H05551212 (call 5551212 immediately after the phone is taken off hook)

Example 2: H5923123456 (call 923123456 if no digit is entered for 5 seconds after the phone is taken off hook)

Receiver-tagged VIA header

Parameter: ConnectMode bit 22

- 0 = Disable processing of "received=" parameter in Via header (DEFAULT)
- 1 = Enable processing of "received=" parameter in Via header

Example:

- The default ConnectMode parameter value is 0x00060400.
- To enable processing of "received=" tag, set the ConnectMode parameter value to 0x00460400.

Operation:

When the Cisco ATA 186 is operating behind a NAT, the NATIP parameter must be set to the NAT router's external IP address. This allows the correct IP address to be placed in the Contact and SDP headers.

In release 2.14, you may leave the NAT IP address at the default value of "0" or "0.0.0.0" and let the ATA automatically scan the Via header for a "received=" parameter when a message is received. The parameter, if present, would indicate to the Cisco ATA 186 that it is operating behind a firewall.

The Cisco ATA 186 will then proceed as follows:

- If the "received=" parameter is in an INVITE response, the current INVITE is canceled and a new INVITE is sent with the new IP address extracted from the "received=<NAT IP address>" parameter in the Contact and SDP headers.

In addition, the ATA will cancel all previous registrations and re-register with the new IP address in the Contact header. This step is performed only if there is no on-going registration; in other words, only if registration is currently in an idle state.

- If the "received=" parameter is in a REGISTER response as a result of a REGISTER command, the ATA will cancel all previous registrations and re-register with the new IP address extracted from the "received=<NAT IP address>" parameter in the Contact header.

For the Cisco ATA 186 to automatically detect its presence behind a NAT, the SIP proxy server or remote user agent server **MUST** include the "received=" parameter in the Via header in the responses to the Cisco ATA 186 if it detects that the source address and port do not match those in the Via header.

Resolved Issues in Cisco ATA 186 Release 2.14

This section lists the issues in previous releases of the Cisco ATA 186 that are resolved in Release 2.14.

- [General Issues](#)
- [H.323 Issues](#)
- [SIP Issues](#)

General Issues

- CSCdu24665

Spurious DTMF tones can be heard in a call with another Cisco ATA 186. This problem is caused by aggressive criteria to detect even a very weak DTMF signal. The DTMF detection algorithm has been enhanced to improve the rejection of false DTMF digits by tracking changes in the signal level. This issue has been resolved.

- CSCdu83663

The audio breaks up after a connection has been up for a very long period. This problem is caused by ARP messages being sent during an active RTP session which slows down the audio process to wait for ARP responses. This issue has been resolved.

- CSCdw65856

The LoginID0 and LoginID1 configuration parameters have been extended to hold a maximum of 51 alphanumeric characters. Prior to Cisco ATA 186 Release 2.14, the limit was 19 alphanumeric characters. This issue has been resolved.

- CSCdx54579

There is a security hole in the web server of pre-020514 Cisco ATA 186 releases that allows bypass of the UI Password. This issue has been resolved. In addition, a configuration option allowing the user to disable web-based configuration. Users may invoke this feature by setting bit 0x80 of the "OpFlags" configuration parameter to 1.

- CSCdx57555

After an upgrade from Cisco ATA 186 Release 2.14 H.323/SIP software image to Cisco ATA 186 Release 2.14 Skinny/MGCP image, the Cisco ATA 186 may use an incorrect VLAN due to a problem with cookie handling. The workaround is to power-cycle the ATA 186. This issue has been resolved.

- CSCdx58880
In pre-020514 releases, the Cisco ATA 186 does not implement the DHCP REBINDING state. When timer T2 expires, the ATA will request a lease extension by unicast DHCPREQUEST to its original DHCP server. RFC 2131 dictates that an endpoint must broadcast its DHCPREQUEST message. Some DHCP servers will not accept the unicast DHCPREQUEST. Refer to RFC 2131 for details and definitions. This issue has been resolved.

H.323 Issues

- CSCdw07775
A single registration mode is added which allows the whole ATA186 to register with the gatekeeper as a single endpoint. This allows the ATA to register with a gatekeeper and the second port can also be called directly by a gateway or endpoint. To activate this mode, LoginID0 and LoginID1 are set to the same H323ID and UseLoginID is set to 1. The ATA registers as a single endpoint with alias names UID0, UID1 and the H323ID.
Do not configure the Cisco ATA 186 to register a gatekeeper (set GkOrProxy field to 0) or make calls to a registered Cisco ATA 186 via a gatekeeper. This issue has been resolved.
- CSCdw52406
When only one user ID is configured on the Cisco ATA 186, if a second call is made from the same line, there is no audio. This issue has been resolved.
- CSCdw55408
Periodically, one or both ports on the Cisco ATA 186 may hang in the off-hook state until the user repeated depresses flash-hook or resets the box. This issue has been resolved.
- CSCdw78907
The Cisco ATA 186 cannot connect to the configured NTP server when it is configured with a static IP address, resulting in the failure of all timestamp-related features, including:
 - Security. The Cisco ATA 186 fails to register with Gatekeeper if security is required.
 - Caller-ID. The Cisco ATA 186 provides an incorrect date for display.
 This issue has been resolved.
- CSCdw87545
The Cisco ATA 186 does not process RAS messages if they are not sent by the active Gatekeeper (either the statically configured Gatekeeper or an Alternate Gatekeeper). Thus, RAS messages sent from a load-balancing Gatekeeper are ignored. The ATA 186 now only requires that URQ messages be sent from the active Gatekeeper.

SIP Issues

- CSCdv68960
After an initial successful registration with a proxy server, the Cisco ATA 186 can experience problems when sending the REGISTER message after a power reset (and subsequent DHCP, TFTP, and DNS/proxy server sequence). Debug reports from the Cisco ATA 186 show that the REGISTER message was sent and failed. However, a network analyzer shows that no message was actually sent. We advise upgrading to Cisco ATA 186 Release 2.13 or higher if encountering this issue. This issue has been resolved.

- CSCdv70761

Calls incorrectly branch back to the caller. In SIP mode, if a caller on Phone 1 leaves a message for a caller on Phone 2, and within 5 seconds the callee attempts to retrieve message, Phone 2 incorrectly dials Phone 1 instead of getting the voice prompt from the message center.

This issue is with the proxy. The Cisco ATA 186 clearly calls the correct voice mail number, but the proxy server still routes the call to the caller who has left the last message. This issue has been resolved.

- CSCdv70842

The message waiting indicator (MWI) tone is lost. The problem is caused by not remembering the MWI state before a soft reset. This issue has been resolved.

- CSCdv82362

After the Caller-ID feature is disabled, Phone 2 still shows the ID during call transfer. In SIP mode with Caller-ID disabled (set "CallFeatures" to 0xfff7fff7 to disable Caller-ID on Phone 1 and Phone 2), direct calls correctly result in the "Anonymous" message being displayed on the Caller-ID device of the callee. However, when Phone 1 of the Cisco ATA 186 transfers Phone 2 to a third party, the callee sees the Caller-ID information of the transferred party.

This situation happens during attended transfer. The call is established between the transferrer and the transfer target first. The Caller-ID on the transfer target's device shows the transferrer's number, who is the one that actually calls the transfer target.

When the transferrer hangs up, the transferee connects with the transfer target. However, there is no ringing involved at this point since the transfer target is already off-hook. Hence the Caller-ID cannot be changed.

This issue is closed since this is not a defect of the Cisco ATA 186, but is the way Caller-ID works (requires ringing).

- CSCdw79404

The Cisco ATA 186 now generates the correct MD5-sess credential for SIP authentication. This issue has been resolved.

- CSCdw79142

The Cisco ATA 186 now explicitly includes the optional port 5060 in the VIA and CONTACT header to allow the Cisco PIX firewall to correctly translate and route incoming SIP messages. This issue has been resolved.

- CSCdw80975

The Cisco ATA 186 now accepts the URL in the Record-Route header with or without a "maddr" parameter. When the Cisco ATA 186 receives a Record-Route header without this parameter, it uses the URL's host field to forward SIP messages. This issue has been resolved.

Open Issues in Cisco ATA 186 Release 2.14

This section lists open issues for Cisco ATA 186 Release 2.14.

- CSCdv90018

Symptom:

Fax passthrough fails when operating the Cisco ATA 186 in fax passthrough or fax mode at a transmission rate of 14.4Kbps or V.17 with a Cisco IOS-based gateway.

Condition:

This fax passthrough issue affects all VoIP protocols (H.323/SIP/MGCP/SCCP) when the fax transmission rate is higher than 9.6Kbps.

Workaround:

Fax passthrough enhancements have been made in the software but new hardware revisions of the Cisco ATA 186 (ATA186-I1 and ATA186-I2) are required for fax transmission up to 14.4 Kbps.



Note

The success of fax passthrough transmissions depends on network conditions and the tolerance of the fax modem or fax machine to those conditions. The network must have reasonably low network jitter, network delay, and packet loss rate.

Related Documentation

Use these release notes in conjunction with these documents:

- *Cisco ATA 186 and Cisco ATA 188 Installation and Configuration Guide (H.323)*
- *Cisco ATA 186 and Cisco ATA 188 Analog Telephone Adaptor Administrator's Guide (SIP)*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

<http://www.cisco.com/go/subscription>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn. Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides [Cisco.com](http://www.cisco.com) as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the [TAC website](#).

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section on page 10.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0203R)

Copyright © 2001–2002
Cisco Systems, Inc.
All rights reserved.