Text Part Number: 78-5546-09

Release Notes for Cisco uBR904 Cable Access Router for Cisco IOS Release 11.3 NA

August 9, 1999

These release notes for the Cisco uBR904 cable access router support Cisco IOS Release 11.3 NA, up to and including 11.3(11)NA. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of the software caveats that apply to Release 11.3 NA, see "Caveats" section on page 10 and *Caveats for Cisco IOS Release 11.3 T* that is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Use these release notes with *Release Notes for Cisco IOS Release 11.3* and *Release Notes for Cisco uBR7200 Series for Cisco IOS Release 11.3 NA* located on CCO and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

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

Introduction

The Cisco uBR904 cable access router gives residential or small office/home office (SOHO) subscribers, high-speed Internet or Intranet access by using a shared two-way cable system and IP backbone network. The router connects computers and other customer premise devices at a subscriber site to the service provider's hybrid/fiber coax (HFC) and IP backbone network.

The Cisco uBR904 cable access router interoperates with any bidirectional, DOCSIS-qualified Cable Modem Termination System (CMTS). The Cisco uBR904 ships from the Cisco factory with a Cisco Internetwork Operating System (IOS) software image stored in nonvolatile memory (NVRAM) that supports DOCSIS-compliant bridging or routing data operations. The Cisco uBR904 functions as a cable modem–a modulator/demodulator at a subscriber site to convey data communications on the cable television system.

Based on the feature licenses your company purchased, you can download other Cisco IOS images from CCO. You can configure each Cisco uBR904 cable access router in your network to support special operating modes based on your cable plant's service offering and the practices in place for your network. The Cisco uBR904 can function as an advanced router, providing wide area network (WAN) data connectivity in a variety of configurations.

System Requirements

This section describes the system requirements for Release 11.3(11)NA:

Memory Requirements

Table 1 Memory Requirements for the Cisco uBR904

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs From	Feature Status
IP Routing Standard Feature Sets					
MCNS Base	ubr900-y4-mz	4 MB Flash	8 MB DRAM	RAM	Added in Release 11.3(4)NA
MCNS Base with Privacy	ubr900-k1y4-mz	4 MB Flash	8 MB DRAM	RAM	Encryption image added in Release 11.3(5)NA

Headend Interoperability

To support data features sets that involve encryption/decryption, Cisco IOS images must contain encryption/decryption software at both the CMTS and the Cisco uBR904. Both the CMTS router and the Cisco uBR904 must be enabled and configured per the software feature set. Should you have the Cisco uBR7200 series equipment, also reference applicable release notes for the corresponding images at the headend that support the feature set.

Hardware Supported

There are no new hardware features supported by the Cisco uBR904 for Cisco IOS Release 11.3 NA.

Determining the Version of Your Cisco IOS Software Release

To determine the version of Cisco IOS software running on your Cisco uBR904 cable access router, log in to the router and enter the **show version** EXEC command:

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) 904 Software (UBR904-y4-mz), Version 11.3(11)NA...
```

Upgrading to a New Software Release

For information about upgrading to a new software release, see *Cisco IOS Software Release 11.3 Upgrade Paths and Packaging Simplification product bulletin* on CCO at:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 11.3**, click **Cisco IOS Software Release 11.3 Upgrade Paths (#703: 12/97)**.

This product bulletin does not contain information specific to Cisco IOS Release 11.3 NA, but provides generic upgrade information that may apply to Cisco IOS Release 11.3 NA.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Table 2 Feature Sets Supported by the Cisco uBR904

Feature Set	Feature Set Matrix Term	Software Image	Platforms
MCNS Base	Basic[1]	uBR900-y4-mz	Cisco uBR904
MCNS Base with Privacy	Basic, Baseline Privacy[2]	uBR900-k1y4-mz	Cisco uBR904

1 This feature is offered in the Basic feature set.
2 This feature is offered in the encryption feature sets which consist of 56bit DES (k1) data encryption feature sets.

Caution Cisco IOS images with strong encryption (including, but not limited to 56-bit data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, you must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 3 lists the features and feature sets supported by Cisco IOS Release 11.3(11)NA for the Cisco uBR904 cable access router and uses the following conventions to identify features:

- Yes—The feature is supported in the feature set.
- No—The feature is not supported in the feature set.
- In—The Cisco IOS release that first introduced a feature. For example, (4) means a feature is introduced in 11.3(4)NA. If a cell in this column is empty, the feature was included in the initial base release.

Table 3 Feature List by Feature Set for the Cisco uBR904

	Feature Sets		
Feature	**In**	**MCNS Base**	**MCNS Base with Privacy**
Cable Device MIB	(4)	Yes	Yes
Cisco Standard MIBs	(4)	Yes	Yes
Full and MCNS-compliant Bridging	(4)	Yes	Yes
Network Address Translation and Port Address Translation (NAT/PAT)	(4)	Yes	Yes
Radio Frequency Interface (RFI) MIB	(4)	Yes	Yes
Routing (RIP V2)	(4)	Yes	Yes

New and Changed Information

The following sections list the new features supported by the Cisco uBR904 cable access router in Cisco IOS Release 11.3 NA.

New Features In Release 11.3(6)NA through Release 11.3(11)NA

There are no new features supported by the Cisco uBR904 in Cisco IOS Release 11.3(11)NA.

New Features In Release 11.3(5)NA

The following new features are supported by the Cisco uBR904 beginning in Cisco IOS Release 11.3(5)NA.

DOCSIS Baseline Privacy

The DOCSIS Baseline Privacy feature is based on the DOCSIS Baseline Privacy Interface Specification. It provides data privacy across the HFC network by encrypting traffic flows between the Cisco uBR904 and the cable operator's CMTS.

Baseline Privacy security services are defined as a set of extended services within the DOCSIS MAC sublayer. Two new MAC management message types, BPKM-REQ and BPKM-RSP are employed to support the Baseline Privacy Key Management (BPKM) protocol.

The BPKM protocol does not use authentication mechanisms such as passwords or digital signatures; it provides basic protection of service by ensuring that a cable modem, uniquely identified by its 48-bit IEEE MAC address, can only obtain keying material for services it is authorized to access. The Cisco uBR904 is able to obtain two types of keys from the CMTS: the Traffic Exchange Key (TEK), which is used to encrypt and decrypt data packets, and the Key Exchange Key (KEK), which is used to the decrypt the TEK.

For more information on this feature, refer to the DOCSIS Baseline Privacy Interface Specification (SP-BPI-IO1-970922).

New Features In Release 11.3(4)NA

The following new feature was introduced in the Cisco uBR904 for Cisco IOS Release 11.3(4)NA:

Cable Device MIB

The Cable Device MIB is for DOCSIS-compliant cable modems and Cable Modem Termination Systems (CMTS). The Cable Device MIB records statistics related to the configuration and status of the cable modem. Statistics include an events log and device status. The following list details the components of the Cable Device MIB:

- The **docsDevBase** group extends the MIB-II “system” group with objects needed for cable device system management.
- The **docsDevNmAccess** group provides a minimum level of SNMP access security.
- The **docsDevSoftware** group provides information for network downloadable software upgrades.
- The **docsDevServer** group provides information about the progress of interaction with various provisioning servers.
- The **docsDevEvent** group provides information about the progress of reporting.
- The **docsDevFilter** group configures filters at link layer and IP layer for bridge data traffic.

The Cable Device MIB is very similar to the RFI MIB in that both allow access to statistics; they are different in that the Cable Device MIB reports statistics on the Cisco uBR904 cable access router, and the RFI MIB reports statistics on the radio frequency transmissions over the cable television line.

Cisco Standard MIBs

The Cisco Standard MIBs consist of the following components:

- CISCO-PRODUCT-MIB
- CISCO-SYSLOG-MIB
- CISCO-FLASH-MIB
- BRIDGE-MIB

- IF-MIB
- CiscoWorks/CiscoView

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on CCO at: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**

Network Address Translation and Port Address Translation (NAT/PAT)

Network Address Translation (NAT):

- Allows customers to maintain their own private networks while giving them full Internet access through the use of one or more global IP addresses.
- Allows several private IP addresses to use the same global IP address by using address overloading.
- Facilitates configuration and permits a large network of users to reach the network by using one Cisco uBR904 cable access router and the same DOCSIS cable interface IP address.
- Eliminates the need to readdress all hosts with existing private network addresses (one-to-one translation) or by enabling all internal hosts to share a single registered IP address (many-to-one translation, also known as Port Address Translation [PAT]).
- Enables packets to be routed correctly to and from the outside world by using the Cisco uBR904 cable access router.
- Allows personal computers on the Ethernet interface to have IP addresses to be mapped to the cable interface's IP address.

Routing protocols will run on the Ethernet interface instead of the cable interface, and all packets received are translated to the correct private network IP address and routed out the Ethernet interface. This eliminates the need to run RIP on the cable interface.

To implement the Cisco uBR904 cable access router, the Ethernet interface is configured with an "inside" address and the cable interface is configured with an "outside" address. The Cisco uBR904 cable access router also supports configuration of static connections, dynamic connections, and address pools.

Full and DOCSIS-Compliant Bridging

Full and DOCSIS-Compliant Bridging for the Cisco uBR904 cable access router complies with the DOCSIS standards for interoperable cable modems.

Radio Frequency Interface MIB

The Radio Frequency Interface (RFI) MIB module is for DOCSIS-compliant radio frequency interfaces in cable access routers and cable access router termination systems. On the cable access router, RFI MIB entries provide:

- upstream and downstream channel characteristics
- class of service (COS) attributes
- physical signal quality of the downstream channels

- attributes of the cable access router MAC interface
- status of several MAC layer counters

The RFI MIB includes tables describing both the CMTS and the cable modem side of the cable interface. All cable modem tables are implemented.

Routing (RIP V2)

A routing configuration for the Cisco uBR904 cable access router is most likely used when the cable access router is being added to an existing personal computer network. If set to support routing mode, the Cisco uBR904 cable access router will automatically configure the headend's IP address as its IP default gateway. When the IP host-routing is being configured, this automatic configuration of the headend's IP address as its IP default gateway will allow the Cisco uBR904 cable access router to send packets not intended for the Ethernet interface to the headend.

RIP V2 routing is useful for small internetworks in that it enables optimization of NIC-assigned IP addresses by defining VLSMs for network addresses, and it allows CIDR addressing schema.

Important Notes

The following section contains important notes about Cisco IOS Release 11.3 that may apply to the Cisco uBR904.

ATM Multipoint Signaling

Prior to Cisco IOS Release 11.1(13) and 11.2(8), the **atm multipoint-signaling** command was used on the main interface and affected all subinterfaces. For Release 11.1(13), 11.2(8), and later releases (including Release 11.3), explicit configuration on each subinterface is required to obtain the same functionality. See caveat CSCdj20944, which is described as follows:

The **atm multipoint-signaling** interface command is currently only available on the main ATM interface. The effect is that signaling behavior (point-to-point or point-to-multipoint) for all clients on all subinterfaces is determined by the command on the main interface.

Clients on different subinterfaces can have different behavior. Specifically, RFC 1577 requires point-to-point, and PIM allows point-to-multipoint. The command should be on a per-subinterface basis.

Enable the **atm multipoint-signaling** command on all subinterfaces that require it. Previously, you only needed to enable the command on the main interface.

Cisco IOS Release 11.3, 11.3 NA and 11.3 T End of Sales and End of Engineering

End of Engineering (EOE) means there are no more regularly scheduled maintenance releases. The following maintenance releases scheduled on the EOE date are only available through CCO and Field Service Operations—not through manufacturing:

- Cisco IOS Releases 11.3, 11.3 NA, and 11.3 T are scheduled to reach End of Sales (EOS) status with maintenance Releases 11.3(10), 11.3(10)NA, and 11.3(10)T.
- Releases 11.3, 11.3 NA, and 11.3 T are scheduled to reach EOE with Releases 11.3(11), 11.3(11)NA, and 11.3(11)T.

EOS and EOE releases are subject to change. For the most up-to-date information on the status of EOS or EOE, see *End of Sales and End of Engineering for Cisco IOS Software Releases* product bulletins on CCO.

Ongoing support for functionality in Releases 11.3, 11.3 NA, and 11.3 T is available in Cisco IOS Release 12.0(3)T and later maintenance releases of Cisco IOS Release 12.0.

On CCO, click on this path:

Service & Support: **Product Bulletins**: **Software**

Under Cisco IOS 11.3, click on **End of Sales and End of Engineering for Cisco IOS Software Releases 11.3 and 11.3 T (#847: 12/98)** or **Cisco IOS Software 11.3 NA EOS and EOE (#849:12/98)**

Image Deferral, Cisco IOS Release 11.3(8)T

Cisco IOS Release 11.3(8)T was deferred to Release 11.3(8)T1 on all software images to incorporate corrections to the following caveats:

- CSCdk86294—The D channel is always in the shutdown state when non-facility associated signalling is configured.
- CSCdk80809—Enhanced Interior Gateway Routing Protocol (EIGRP) has difficulty converging on certain routes.

For more information on these caveats, see Bug Navigator II. Bug Navigator II is available at http://www.cisco.com/support/bugtools or on CCO at:

Service & Support: Online Technical Support: Software Bug Toolkit: Bug Navigator II.

Enabling IPX Routing

Whenever IPX routing is enabled, the Token Ring interface resets.

Forwarding of Locally Sourced AppleTalk Packets

Cisco's implementation of AppleTalk does not forward packets with local-source and destination network addresses. This behavior does not conform to the definition of AppleTalk in Apple Computer's *Inside AppleTalk* publication. However, this behavior is designed to prevent any possible corruption of the AppleTalk Address Resolution Protocol (AARP) table in any AppleTalk node that collects MAC addresses.

Missing Source-Route Bridging Commands

Due to a production problem, many source-route bridging commands were omitted from the printed version of the *Cisco IOS Software Command Summary* (78-4746-XX). For documentation of all source-route bridging commands, see *Bridging and IBM Networking Command Reference* (78-4743-XX). You can also obtain the most current documentation on CCO or on the Documentation CD-ROM.

New TACACS+ Attribute-Value Pair

A new authorization feature that allows you to separately configure and authorize Multilink PPP was added in Cisco IOS Release 11.3(1). This feature can cause MLP authorization to fail in TACACS+ servers that do not include the relevant authorization permissions in the configuration.

For TACACS+, add the following attribute-value (AV) pair for all users who are allowed to negotiate Multilink PPP:

```
service = ppp protocol = multilink {
```

Using LAN Emulation

Note the following information regarding the LAN Emulation (LANE) feature in Cisco IOS Release 11.3:

- LANE is available for use with Cisco 4500 and Cisco 4700 series routers, and Cisco 7000 and Cisco 7500 series routers connected to either an LS100 or LS1010 switch. LANE requires at least Version 3.1(2) of the LS100 software, which requires a CPU upgrade if you are currently running software earlier than Version 2.5.
- Do not use the LS2020 for LANE because it does not support UNI 3.0 and point-to-multipoint SVCs.
- Routing of IP, IPX, AppleTalk, DECnet, VINES, and XNS is supported.
- Hot Standby Router Protocol (HSRP) is supported.
- LANE does not support Connectionless Network Service (CLNS) or LANE over Permanent Virtual Circuits (PVCs).
- Do not route AppleTalk Phase 1 to AppleTalk Phase 2 by using LANE.

40-bit Encryption Images are Unavailable in Release 11.3(1)

Cisco is conducting an internal review of the build and distribution processes associated with its 40-bit Cisco IOS cryptographic products. To provide seamless access to Cisco IOS 40-bit encryption capability, Cisco will provide access to the most current 40-bit encryption images, beginning with Cisco IOS Release 11.2 (12), 11.2(12)P, and 11.3(2).

The following 40-bit encryption images are unavailable indefinitely:

- 11.2(1)–11.2(11.2)
- 11.2(2)P–11.2(11.1)P
- 11.2(1)F–11.2(4)F
- 11.3(1)

This review is not related to any new or previously unreported caveats. The information gathered in the review will be used to implement new automated development and order-processing applications.

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-* MIBS are currently migrated into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in the following table:

Table 4 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In Development
OLD-CISCO-DECNET-MIB	
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBS)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

This section only contains open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Releases 11.3 and 11.3 T are also in Release 11.3(11)NA.

For information on caveats in Cisco IOS Release 11.3, see "Important Notes and Caveats for Release 11.3" section in *Cross-Platform Release Notes for Cisco IOS Release 11.3* on CCO and the Documentation CD-ROM. These release notes list severity 1 and 2 caveats affecting all maintenance releases.

For information on caveats in Cisco IOS Release 11.3 T, refer to the *Caveats for Cisco IOS Release 11.3 T* on CCO and the Documentation CD-ROM.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Service & Support**: **Online Technical Support**: **Software Bug Toolkit**, or at http://www.cisco.com/support/bugtools.

Caveats for Release 11.3(1) through 11.3(11)NA

This section describes possibly unexpected behavior by Release 11.3(11)NA. Unless otherwise noted, these caveats apply to all 11.3 releases and platforms up to and including Release 11.3(11)NA.

Miscellaneous

- CSCdm47012

  The latest versions of Smart Modular and Sharp Flash cards used to store Diagnostics and IOS SW images can report unrecoverable write errors.

  Affected Flash cards use a new Sharp (LH28F016SCT) chip set. The original Smart Modular and Intel Flash cards are not affected.

  Affected platforms are 7200 and all derivatives, 7500, GSR, and maybe others.

  There is no workaround. If the problem occurs, try to reformat the Flash, store less images, or try storing images in a different order. This may help under some circumstances.

- CSCdm68266

  When running 11.3.10NA image, ingress gw can display wrong cause code.

- CSCdm68546

  This fixes CM status display in CMTS when the modem goes offline with BPI turned on and key expiration.

Caveats for Release 11.3(1) through 11.3(10)NA.

This section describes possibly unexpected behavior by Release 11.3(10)NA. Unless otherwise noted, these caveats apply to all 11.3 releases up to and including Release 11.3(10)NA. For additional caveats applicable to Release 11.3(10)NA, see the caveats sections for later 11.3 releases. The caveats for later releases precede this section.

All the caveats listed in this section are resolved in release 11.3(11)NA.

Access Server

- CSCdm50856

  The **sh modem** command on an AS5200 router has different results from snmpwalk of the cmInitialLineConnections variable defined in CISCO-MODEM-MGMT-MIB. The IOS is 11.3(8)T1.

Basic System Services

- CSCdk80230

  Certain Internetwork Status Monitor (ISM) NetView users can issue non-enable mode commands without router authentication. Users accessing the router through NetView must be authenticated through NetView's security methods, which can include RACF and SAF. Mainframe users can be restricted from issuing any router commands by the restriction of the RUNCMD within NetView. Users issuing enable mode commands must be authorized to issue

this level of command by ISM, and must possess the ENABLE mode password. If the router is controlled by TACACS+, the ISM user must have a TACACS+ User ID and Password to issue enable level commands.

show user : command has been modified : the user field is filled up by the host name.

Two options have been added to the following commands : **sna host** and **dspu host**.

The options are: **no-enable** and **high-security**.

Configure these options with focalpoint.

no-enable : when this is set, it does not allow enable command from the host

high-security : when this is set, it allows the following commands in USER mode. (PRIVILEGE mode is not affected by this option.) You must enter all these commands in full or else the command will not be allowed (that is, sh versi is not allowed for **show version**)

- CSCdm45535

  C7500 router can erroneously detect output stuck conditions causing interfaces to reset or perform cbus restarts for no apparent reason. This causes all IPs in the router to reset.

DECnet

- CSCdk23805

  When decnet accounting is implemented, it's possible for the router to crash depending on the amount of connections.

- CSCdm28939

  When you are configuring Decnet on a router, you can specify an Address Translation Gateway (ATG) network number in the range 0 to 3. If the *ATG-network-number* is specified incorrectly while configuring an interface, the router will reload.

  If the *ATG-network-number* is not required the problem will not occur.

  If the *ATG-network-number* is required, then a workaround is to ensure that the *ATG-network-number* specified when enabling an interface matches the *ATG-network-number* specified when decnet routing is enabled globally; for example:

  decnet *1* **routing** *2.3* **interface** *ethernet 0/0* **decnet** *1* **cost** *5*

EXEC and Configuration Parser

- CSCdm39355

  If the length of the entire command after completion exceeds PARSEBUF, then the router crashes

  Fix: Don't allow the "command completion" if it exceeds PARSEBUF

IBM Connectivity

- CSCdm30793

  A Cisco 7206 configured for dlsw priority peers may crash with a bus error in Release 11.3(9)T.

  Workaround: None.

- CSCdm39124

Console message flooding may occur when an XID3 loop occurs with APPN in the router. The following messages are repeated for each iteration of the loop:

```
%APPN-3-logcsCS_XXXXIP11_LOGMSG_01: CS - Sending Alert to MS, sense_code = 83E0001,
proc_name = XXXXIP32, port_name = HMAC04, ls_name = @LS00289
%APPN-3-logcsCS_XXXXIP11_LOGMSG_03: CS - Associated outbound XID data in alert (length
>= 29): %APPN-3-Error:
327307700000000000F7C1000000008000010B5100050000000000007000E11F4C4C5C2E5D4E4F0F04BD5D5C
3C9D7F0F110380037110C0804F1F2F0F0F0F00908F0F0F0F0F0F0F01406C3C9E2C3D640C1D7D7D540D5D561
C4D3E4D90F0FC3C9E2C3D640C1D7D7D540D5D52207000000083E0001
%APPN-3-logcsCS_XXXXIP11_LOGMSG_05: CS - Associated inbound XID data in alert (length
>= 29): %APPN-3-Error:
326705D56F010000B0081000000000000010B410005B8000000000700103700231 10C0804F0F3F0F0F0F00
F06D4E240E2D5C140E2C5D9E5C5D90908F0F0F0F0F0F0F0131103100010F0F0F0F0F0F0F0F0F0F0F0F00E
0FF4C4C5C2E5D4E4F0F04BC3E3F5F6C6
```

Avoid console logging.

- CSCdm49573

  The router crashes with bus error when executing a **show dlsw circui**t command if there is a circuit with a local rif of 18 bytes.

  This is a regression introduced by CSCdk83294.

- CSCdm50361

  DLSw Lite peers leak CLS connect request buffers. If possible, try using a different peer type. This patch frees an outstanding connect request if additional requests are received while the first request is still pending.

Interfaces and Bridging

- CSCdk10376

  SYMPTOM: Crash in frf9_preComp()

  This ondition most frequently occurs during times when router traffic is heavy, which causes memory usage to increase and a possible low-memory condition to occur.

  WORKAROUND: Disable compression or use a different type.

  Since this problem is aggravated by a low-memory condition, tuning the memory can prevent this condition from occurring, but there are no guarantees.

- CSCdm41644

  This is caused by an over-write issue in bss area with FDDI modules equipped which has potential to cause serious problem such as crash in 12.0T.

- CSCdm46735

  A PA-4R-DTR port may reset under the following circumstances:

  1) A high rate of traffic is traversing the port (200 pps or better) .

  2) The PA-4R-DTR port is the active monitor of the physical ring.

  3) An event on the ring forces the active monitor to purge the ring.

  When this problem occurs, the PA-4R-DTR port resets, and the ring experiences a beacon.

  Workaround: Make sure the DTR port is not the active monitor on the ring. This can be done by ensuring that the mac-address of the DTR card is not the highest mac-address on the physical ring.

IP Routing Protocols

- CSCdm20483

  IP access lists fail to block pings on the interfaces configured for policy routing with IP route-cache policy.

- CSCdm28898

  ARP to a router fails on the serial interface when bridging is enabled and after the router is reloaded.

  ```
  ----eth---2500---serial---2500---eth---
  ```

  Router : 2500 IOS : 112.(17), 12.0(3.7)

  Workaround: Remove IP address on serial and enter again.

- CSCdm44957

  Some IP fragments may be incorrectly filtered out by access lists.

- CSCdm53317

  DNS replies passing from "inside" to "outside" through NAT are not NAT translated correctly in many cases. There is no work around.

Miscellaneous

- CSCdk45491

  Symptom: The NM-1FE-TX fails to autonegotiate properly when connected through an SMF connector.

  Analysis: Manually setting the speed to 100 solves the problem. An interface speed command with the following syntax is being added to overcome this. The default behaviour would be to autonegotiate:

  ```
  [no] speed {10 | 100 | auto}
  ```

- CSCdm18910

  When port info is passed from LAC and ’vpdn aaa attribute nas-port vpdn-nas’ is configured, it should be mapped to the correct NAS-Port-Type value.

- CSCdm22032

  Configuring ppp encaplusation on an interface and making that interface a member of a bridge group gives “tracebacks” and “fair-queue not initialized properly” messages. Remove bridging from the interface or turn off fair queueand the massages dissappear.

  ```
  00:06:39: -Traceback= 601C9C58 602015E0 60556558 60553958 6021D034 6021D020 00:06:39:
  Fair Queue:packet not initialized properly: 0, 0 , 38 00:06:39: -Traceback= 601C9C58
  602015E0 60556558 60553958 6021D034 6021D020 00:06:39: Fair Queue:packet not
  initialized properly: 0, 0 , 38 00:06:39: -Traceback= 601C9C58 602015E0 60556558
  60553958 6021D034 6021D020 00:06:40: Fair Queue:packet not initialized properly: 0, 0 ,
  38 00:06:40: -Traceback= 601C9C58 602015E0 60556558 60553958 6021D034 6021D020
  00:06:40: Fair Queue:packet not initialized properly: 0, 0 , 38 00:06:40: -Traceback=
  601C9C58 602015E0 60556558 60553958 6021D034 6021D020 00:06:40: Fair Queue:packet not
  initialized properly: 0, 0 , 38 00:06:40: -Traceback= 601C9C58 602015E0 60556558
  60553958 6021D034 6021D020 00:06:40: Fair Queue:packet not initialized properly: 0, 0 ,
  38 00:06:40: -Traceback= 601C9C58 602015E0 60556558 60553958 6021D034 6021D020
  00:06:40: Fair Queue:packet not initialized properly: 0, 0 , 38 00:06:40: -Traceback=
  601C9C58 602015E0 60556558 60553958 6021D034 6021D020
  ```

- CSCdm28631

  Under stressful conditions of (if the ESA is bringing up a large number of crypto sessions simultaneously), it may either enter a race condition or get the crypto initiation messages wedged in the input-q of the interface doing encryption.

- CSCdm31647

  A customer reset a VIP card in slot 8 of one Cisco 7513, and the VIP crashed. When the VIP came up, ISL trunking to slot 4 (PA-2FEISL-TX) started dropping large packets. However, small packets go through the interface just fine. Workaround is to reset the box.

- CSCdm33429

  A Cisco AS5300 gets a bus error when it is under a heavy load caused by outgoing Modem calls. Have tested with IOS 11.3(9)T and 11.3(8.5)T with same results.

  Problem is reproducible within minutes.

- CSCdm33707

  After the router is reloaded, ESA can not re-establish active crypto connection. The workaround is to remove the crpto map, reload the the router again, and reapply the crypto map.

- CSCdm44057

  When running virtual-profile, theCisco 7500 keeps on resetting the cbus.

  The first message is "%RSP-3-RESTART: interface Serial4/0:1, output stuck" .

  Then a little later, a reset occurs on the cbus. If debugging cbus, you can see the bus resetting. This also causes all attached controllers to loose connectivity. The only way to access the box is through the console port.

- CSCdm49454

  Problem description: When **cable ip-broadcast-echo** is enabled, under certain timing conditions, it may cause a buffer leak.

  Workaround: Do not enable **cable ip-broadcast-echo** and **cable ip-multicast-echo**.

VINES

- CSCdk80167

  Cisco 2500 series and Cisco 4000 series routers (68000-based routers) might reload a few minutes after VINES Sequenced Routing Update Protocol (SRTP) is configured.

  Workaround: Do not use VINES SRTP. If it is enabled, disable it by issuing the **no vines srtp-enabled** command.

Wide-Area Networking

- CSCdk37517

  DDR with **dialer dtr** does not reset DTR to a down state after an unsuccessful call attempt. Unsuccessful in this case means that DD; therefore DCD does not come up.

  This can be verified by viewing **show dialer** to ensure that the dialer state is idle; then enter **show interface serial x** to check the state of DTR.

  This problem does not seem to occur in Release 11.1.

- CSCdm30090

  When the router is operating as an X.25 switch and forwards an X.25 call containing certain facilities not interpreted by the router, the facility values can be corrupted. The problem most likely occurs when the call cannot be forwarded immediately (i.e., when using X25-over-TCP) with heavy traffic; the affected facilities include any local facilities and the Charging Information facility.

- CSCdm33448

  A router performing X.25 switching may reload when clearing many calls simultaneously during heavy traffic.

- CSCdm36123

  Customer repeatedly crashes (segV) when dialer rotor best is configured and 'deb dialer' is started once the traffic triggers a call.

- CSCdm37153

  5200 pri never sends UAf respond to telcos switch in Release 11.3.

- CSCdm37653

  Reliable PPP can cause an intermittent crash when used with WFQ. Workaround is to disable Reliable PPP or WFQ.

- CSCdm38291

  The router configured for dialer watch never dials back when backup interface times out if Watched route on dialer watch is not installed in routing table.

Related Documentation

The following sections describe related documentation available for the Cisco uBR904 cable access routers. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documentation, page 17
- Platform-Specific Documents, page 17
- Feature Modules, page 18
- Cisco IOS Software Documentation Set, page 18

Release-Specific Documentation

The following documents are specific to Release 11.3 NA and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 11.3*

  On CCO:

  Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Cross Platform Release Notes for Cisco Release 11.3

  On the Documentation CD-ROM:

  Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Cross Platform Release Notes for Cisco IOS Release 11.3

- Product bulletins, field notices, and other release-specific documents on CCO at:

  Service & Support: Technical Documents

- *Caveats for Cisco IOS Release 11.3 T*

  As a supplement to the caveats listed in "Caveats" section on page 10 in these release notes, see *Caveats for Cisco IOS Release 11.3 T*, which contains caveats applicable to all platforms for all maintenance releases of Release 11.3 NA.

  On CCO:

  Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

  On the Documentation CD-ROM:

  Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Service & Support**: **Online Technical Support**: **Software Bug Toolkit**, or at http://www.cisco.com/support/bugtools.

Platform-Specific Documents

These documents are available for the Cisco uBR904 on CCO and the Documentation CD-ROM:

- *Cisco uBR904 Cable Access Router Installation and Configuration Guide*
- *Cisco uBR904 Cable Access Router Quick Reference Guide*
- *Update to the uBR904 Cable Access Router Installation and Configuration Guide*
- *Bridging and Routing Features for the Cisco uBR904 Cable Access Router*
- *Regulatory Compliance and Safety Info. for the Cisco uBR904*
- *Troubleshooting Tips for the Cisco uBR904 Cable Access Router*

On CCO:

Service & Support: Documentation Home Page: Cisco Product Documentation: Broadband/Cable Solutions: Cisco uBR900 Series Cable Access Routers

On the Documentation CD-ROM:

Cisco Product Documentation: Broadband/Cable Solutions: **Cisco uBR900 Series Cable Access Routers**

Feature Modules

Feature modules describe new features supported by Release 11.3 and are an update to the Cisco IOS documentation set. Feature modules consist of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are only available online. The feature module information is incorporated in the next printing of the Cisco IOS documentation set.

- On CCO:

  Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3: New Features in Release 11.3

- On the Documentation CD-ROM:

  Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3: New Features in Release 11.3

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. These documents are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set: configuration guides and command references.

On CCO:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 Configuration Guides, Command References: Configuration Guide Master Index or **Command Reference Master Index**

On the Documentation CD-ROM:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: **Cisco IOS 11.3 Configuration Guides, Command References: Configuration Guide Master Index** or **Command Reference Master Index**

Release 11.3 Documentation Set

Table 5 describe the contents of the Cisco IOS Release 11.3 software documentation set. The document set is available in electronic form, and also in printed form upon request.

Note You can find the most current Cisco IOS documentation on CCO and the Documentation CD-ROM. These electronic documents might contain updates and modifications made after the paper documents were printed.

On CCO:

Service & Support: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 11.3

On the Documentation CD-ROM:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3

Table 5 Cisco IOS Software Release 11.3 Documentation Set

Books	Chapter Topics
• Configuration Fundamentals Configuration Guide • Configuration Fundamentals Command Reference	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management Interface Configuration System Management
• Network Protocols Configuration Guide, Part 1 • Network Protocols Command Reference, Part 1	IP Addressing IP Services IP Routing Protocols
• *Network Protocols Configuration Guide, Part 2* • *Network Protocols Command Reference, Part 2*	AppleTalk Novell IPX
• *Network Protocols Configuration Guide, Part 3* • *Network Protocols Command Reference, Part 3*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	Wide-Area Networking Overview ATM Frame Relay SMDS X.25 and LAPB
• *Security Configuration Guide* • *Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering Network Data Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options

Table 5 Cisco IOS Software Release 11.3 Documentation Set (continued)

Books	Chapter Topics
• *Dial Solutions Configuration Guide* • *Dial Solutions Command Reference*	Business Applications and Scenarios Dial-In Port Setup Dial-In Terminal Services and Remote Note Configuration Dial Authentication Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Dial-Related Addressing Services (NAT/Easy IP) Cost-Control Solutions Network Traffic over ISDN Channels X.25 over ISDN Virtual Private Dialup Networks
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Switching Paths for IP Networks NetFlow Switching Virtual LAN (VLAN) Routing LAN Emulation
• *Bridging and IBM Networking Configuration Guide* • *Bridging and IBM Networking Command Reference*	Transparent Bridging Source-Route Bridging Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point Support SNA Frame Relay Access Support APPN NCIA Client/Server Topologies IBM Channel Attach
• *Configuration Guide Master Index* • *Command Reference Master Index*	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see the *Cisco Network Management Toolkit* on CCO at **Service & Support: Software Center: Network Mgmt Products: Cisco Network Mgmt Toolkit: Cisco MIB**.

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in "Service and Support" in *Cisco Information Packet* shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems' primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account you can access the following URL, which contains links and tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path:

Products & Technologies: Products: Technical Tips

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Lists tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.
- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Lists other helpful documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

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

.

This document is to be used in conjunction with documents mentioned in the "Related Documentation" section on page 16.