AA-QKVZD-TE

DECbrouter 90 Release Notes
Firmware Version 11.1(6)
January 1997

These release notes describe the new features for DECbrouter 90 Internetwork Operating System (Cisco IOS) Release 11.0 up to and including Release 11.1(6).

Important: Read This First

On networks containing both DECbrouter 90 and Cisco routers, some customers have attempted to load system images obtained from Cisco on the DECbrouter 90.

Because of differences in hardware architecture between the DECbrouter 90 and Cisco routers, system images for Cisco routers (for example, Cisco 2500 software) should not be loaded on the DECbrouter 90. The only software supported on the DECbrouter 90 is that which is distributed via Digital, and should only be installed under instruction by Digital to resolve specific identified problems.

Contents

Introduction

This document contains quick-start instructions and important notes for the DECbrouter 90 unit.

Change in Product Classification

The DECbrouter 90 unit has been reclassified from FCC Class A to FCC Class B and from VCCI Class 1 to VCCI Class 2. The notices pertaining to this reclassification are as follows:

FCC Notice – Class B Computing Device:
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. Any modifications to this device – unless expressly approved by the manufacturer – can void the user’s authority to operate this equipment under Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference and (2) This device must accept any interference that may cause undesirable operation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

VCCI Notice – Class 2 Computing Device:
This equipment is in the 2nd Class category (information equipment to be used in residential area or an adjacent area) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential area.

When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Performance Guidelines

For optimum network reliability, observe the following recommendations and guidelines:

- You can operate the synchronous serial interface on the DECbrouter 90T1 at speeds of up to 2048 Kb/s.

- You can operate one synchronous serial interface on the DECbrouter 90T2 and 90T2a at clock speeds of up to 2048 Kb/s and the other port at speeds no faster than 64 Kb/s.

- The DECbrouter 90 is designed to serve as an "Access or Leaf" router. Though the DECbrouter 90 supports numerous routing, bridging, and protocol translation features, it is not recommended that more than four of these protocols run simultaneously on any one router. Furthermore, when utilizing the DECbrouter 90 in large Frame-Relay or X.25 networks it is not recommended that this product serve as the central router for "star topology" style implementations.

  Although this restriction is heavily dependent on the number and types of protocols running and the amount of traffic the DECbrouter 90 is processing, it is not recommended that more than 15 virtual circuits (DLCIs, PVCs or SVCs) be configured per DECbrouter 90 when connecting to a Frame-Relay cloud or an X.25 PSDN.

Configuring the DECbrouter 90 Unit

The DECbrouter 90 unit is preconfigured to transparently bridge all network protocols using the IEEE 802.1d spanning tree protocol. HDLC encapsulation is used on the serial interfaces. This allows the DECbrouter 90 to be used immediately with no other configuration required. Refer to the Installation Guide for instructions on connecting the serial line and Ethernet cables and applying power.

To configure the DECbrouter 90 to route selected protocols, and to enable remote network management, follow the configuration setup procedure described below.

Running the Configuration Script

To run the DECbrouter 90 configuration script, proceed as follows:

1. Verify that you have a VT100 compatible terminal and an H8571-J adapter.
2. To adapt to Digital's MMJ connector, connect the H8571-J adapter to the console port of the DECbrouter 90, then attach the VT100 compatible terminal to the 9-pin console port. The port is the same as a PC/AT serial port. Set the terminal for 9600 baud, 8 bit, no parity, and disable XON/XOFF flow control.
3. Issue the following commands:

```
Router> ENABLE
Router# SETUP
```

The DECbrouter 90 prompts you for information that establishes default parameters for each protocol that you select, and uses HDLC on the serial interface. The DECbrouter 90 allows you to establish the network addresses for each interface, and enable remote management via SNMP, LAT, and Telnet. If you have any specialized configuration requirements, use the CONFIGURE command. Refer to the configuration and reference volumes to determine the required commands.

Using Flash Load Helper

The following sections describe Flash Load Helper, which now comes standard with the Bootstrap Software (IGS-RXBOOT) Version 10.2(11) being shipped with the DECbrouter 90 product.

Overview

This section describes the requirements, purpose, and advantages of Flash Load Helper. Flash Load Helper is a software function that provides a method for users of the DECbrouter 90 to upgrade their system software. The main advantage of Flash Load Helper is that it simplifies the upgrade procedure without requiring additional hardware; however it does require some brief network downtime. Flash Load Helper involves an automated procedure that switches from the current running image to the ROM-based bootstrap image, downloads to Flash, and switches back to the newly downloaded image.

Flash Load Helper includes the following features:

- It performs extensive validations before erasing the current Flash image. That is, it confirms access to the specified source file on the specified server before erasing Flash and reloading to the ROM image for the actual upgrade.

- It warns the user if the image being downloaded is not appropriate for the system. Though the Flash Load Helper will not detect oversized files that are too large for the DECbrouter 90.
- It has improved recovery chances after Flash upgrade failures for remote Telnet users without console access.
- Flash Load Helper prevents reloads to the ROM image for Flash upgrade if the system is not set up for auto booting and the user is not on the console terminal. By doing this, at least the boot ROM image can be brought up as a last resort rather than have the system wait at the ROM monitor's prompt for input from the console terminal.
- Flash Load Helper retries Flash downloads automatically up to six times. The retry sequence is as follows:

  — First try

  — Retry after 120 seconds

  — Retry after 240 seconds

  — Reload ROM image

  — First try after reloading ROM image

  — Retry after 120 seconds

  — Retry after 240 seconds
- Users have an opportunity to save any configuration changes made before they exit out of the system image.
- Users logged into the system are notified of the impending switch to the boot ROM image, so that they do not lose their connections unexpectedly.
- Console output during the Flash Load Helper operation is logged into a buffer that is preserved through system reloads. Users can retrieve the buffer contents from a running image; the output would be useful where console access is unavailable or there is a failure in the download operation.

Reconfiguring Before Upgrading Flash

There may be some cases when, because of your current configuration, the Flash Load Helper operation may fail. For example, this could occur when IP is being bridged, or when IP-unnumbered is being used for the IP address on a serial interface. The host from which the router is trying to retrieve the TFTP or MOP image must have a routed or bridged connect to the DECbrouter 90 independent of the DECbrouter 90 itself. The DECbrouter 90 does not route or bridge any traffic while in the ROM boot mode. In these cases, you may have to reconfigure your network and system(s) before attempting to upgrade the Flash image.

Executing Flash Load Helper for Copy TFTP Flash

This section describes how to execute Copy TFTP Flash from the ROM-based bootstrap image to Flash memory. Enter the `COPY TFTP FLASH` command beginning in privileged EXEC mode, which automatically invokes the Flash Load Helper.

The COPY TFTP FLASH command can always be invoked from a console terminal. The command can, however, be invoked from a virtual terminal (for example, a Telnet session) only if the system is configured for auto booting. This means that the boot bits in the system configuration register must be nonzero.

```
Router# copy tftp flash
ERR: Config register boot bits set for manual booting
```

The above error message is displayed if the user is on a Telnet session and the system is set for manual booting (the boot bits in the configuration register are zero). This step helps minimize the chance of having the system go down to the ROM monitor prompt (and taken out of the remote Telnet user's control) in case of any catastrophic failure in the Flash upgrade. The system would try to bring up at least the boot ROM image if it cannot boot an image from Flash. The user must go into global configuration mode and change the configuration register value (through the CONFIG-REGISTER command) so that the boot bits are nonzero before reinitiating the copy tftp flash command.

If any terminals other than the one on which this command is being executed are active, the following notice is displayed:

```
*************************** NOTICE ********************************
Flash load helper v1.0
This process will accept the TFTP copy options and then terminate the
current system image to use the ROM based image for the copy. Router
functionality will not be available during that time. If you are logged
in via Telnet, this connection will terminate. Users with console access
can see the results of the copy operation.
*******************************************************************

Router# copy tftp flash

                         ****  NOTICE  ****
Flash load helper v1.0
This process will accept the copy options and then terminate
the current system image to use the ROM based image for the copy.
Routing functionality will not be available during that time.
If you are logged in via telnet, this connection will terminate.
Users with console access can see the results of the copy operation.
                         ---- ******** ----
Proceed? [confirm]y

System flash directory:
File  Length   Name/status
  1   5557240  igs-j-l.103-7
  [5557304 bytes used, 2831304 available, 8388608 total]
  Address or name of remote host [255.255.255.255]? 39.5.5.35
  Source file name? /var/kits/igs-j-l.111-6
  Destination file name [/var/kits/igs-j-l.111-6]? igs-j-l.111-6
  Accessing file '/var/kits/igs-j-l.111-6' on ALVIN...
  Loading /var/kits/igs-j-l.111-6 from 39.5.5.35 (via Ethernet0): !
[OK]
```

Next, you are asked whether you want to erase Flash. If you indicate "yes," the dialog continues as follows. The COPY TFTP FLASH operation verifies the request from the running image by trying to TFTP a single block from the remote TFTP server. Then the Flash Load Helper is executed, causing the system to reload to the ROM-based system image.

```
Erase flash device before writing? [confirm] y
Flash contains files. Are you sure you want to erase? [confirm] y

Copy '/var/kits/igs-j-l.111-6' from server
as 'igs-j-l.111-6' into Flash WITH erase? [yes/no] y

%SYS-5-RELOAD: Reload requested

%FLH: /var/kits/igs-j-l.111-6 from 39.5.5.35 to flash ...
System flash directory:
File  Length   Name/status
  1   5557240  igs-j-l.103-7
  [5557304 bytes used, 2831304 available, 8388608 total]
  Accessing file '/var/kits/igs-j-l.111-6' on 39.5.5.35...
  Loading from 39.5.5.35:
  Erasing device...  ... erased
  Loading from 39.5.5.35: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!

Verifying checksum...  OK (0xFEEF)
Flash copy took 383244 msecs
%FLH: Re-booting system after download
Loading igs-j-l.111-6 at 0x3000040, size = 6912704 bytes [OK]

F3: 6704824+207848+262824 at 0x3000060

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

          cisco Systems, Inc.
          170 West Tasman Drive
          San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-J-L), Version 11.1(6), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 09-Sep-96 13:25 by tej
Image text-base: 0x03037D24, data-base: 0x00001000
%SYS-5-CONFIG_I: Configured from memory by console
%SYS-5-RESTART: System restarted --

Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-J-L), Version 11.1(6), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 09-Sep-96 13:25 by tej
Router>
```

If the configuration has been modified but not yet saved, you will be prompted to save the configuration, as follows:

```
System configuration has been modified. Save? [confirm]
```

If you confirm to save the configuration, you might also receive this message:

```
Warning: Attempting to overwrite an NVRAM configuration previously
written by a different version of the system image. Overwrite the
previous NVRAM configuration? [confirm]
```

Users with open Telnet connections will be notified of the system reload, as follows:

```
**System going down for Flash upgrade**
```

In case of TFTP failures, the copy operation will retry up to three times. If the failure happens in the middle of a copy operation (part of the file has been written to Flash), the retry will not erase Flash unless you specified an `erase`. The partly written file will be marked as deleted and a new file opened with the same name. If Flash runs out of free space in this process, the copy operation is terminated.

After the Flash Load Helper finishes its copy operation (whether successful or not), it attempts to do a default boot from Flash. This means that if the Flash was erased and a new image downloaded, the new image is booted up. If Flash was not erased and a file appended in Flash, the original Flash image is booted up. If the default boot from Flash fails, the bootstrap image in ROM is booted up.

Executing Flash Load Helper for Copy MOP Flash

This section describes how to execute Copy MOP Flash from the ROM-based bootstrap image to Flash memory. Enter the `COPY MOP FLASH` command beginning in privileged EXEC mode, which automatically invokes the Flash Load Helper. The same rules outlined in the Copy TFTP Flash example from the preceding section pertain to this section also.

```
Router# copy mop flash
                         ****  NOTICE  ****
Flash load helper v1.0
This process will accept the copy options and then terminate
the current system image to use the ROM based image for the copy.
Routing functionality will not be available during that time.
If you are logged in via telnet, this connection will terminate.
Users with console access can see the results of the copy operation.
                         ---- ******** ----

Proceed? [confirm] y

System flash directory:
File  Length   Name/status
  1   5557248  igs-j-l.sys_103-7
  [5557312 bytes used, 2831296 available, 8388608 total]

  Source file name? IGS-BFPX.SYS
  Destination file name [IGS-BFPX.SYS]?
  Erase flash device before writing? [confirm] y

Copy 'IGS-BFPX.SYS' from server
  as 'IGS-BFPX.SYS' into Flash WITH erase? [yes/no] y
```

```
%SYS-5-RELOAD: Reload requested
%FLH: igs-bfpx.sys from MOP server to flash ...

System flash directory:
File  Length   Name/status
  1   5557248  igs-j-l.sys_103-7
  [5557312 bytes used, 2831296 available, 8388608 total]
Mop2flash: Loading igs-bfpx.sys into flash from interface Ethernet0
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Verifying checksum...  OK (0xFEEF)
Flash copy took 435844 msecs
%FLH: Re-booting system after download
Loading igs-bfpx.sys at 0x3000040, size = 6913024 bytes [OK]

F3: 6704824+207848+262824 at 0x3000060

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

          cisco Systems, Inc.
          170 West Tasman Drive
          San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-J-L), Version 11.1(6), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 09-Sep-96 13:25 by tej
Image text-base: 0x03037D24, data-base: 0x00001000

DECbrouter 90 router (68030) processor (revision A) with 6144K/2048K
bytes of m.
Processor board ID 00000000, with hardware revision 00000000
Bridging software.
SuperLAT software copyright 1990 by Meridian Technology Corp).
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software (copyright 1994 by TGV Inc).
1 Ethernet/IEEE 802.3 interface.
2 Serial network interfaces.
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)

Press RETURN to get started!
```

```
%SYS-5-CONFIG_I: Configured from memory by console
%SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-J-L), Version 11.1(6), RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 09-Sep-96 13:25 by tej

Router>
```

Monitoring Flash Load Helper

Use the `show flh-log` command in EXEC mode to view the system console output generated during the Flash Load Helper operation. Because you may be a remote Telnet user performing the Flash upgrade without a console connection, this command allows you to retrieve console output when your Telnet connection has terminated because of the switch to the ROM image. The output indicates what happened during the download, and would be particularly useful if the download failed.

Assuming the sample Flash Load Helper operation shown in the preceding section, "Executing Flash Load Helper for Copy TFTP Flash," the output of the `show flh-log` command would appear as follows:

```
Router# show flh-log

%FLH: igs-bfpx.sys from MOP server to flash ...
System flash directory:
File  Length   Name/status
  1   5557248  igs-bfpx.sys
[5557312 bytes used, 2831296 available, 8388608 total]

Erasing device...  ... erased
Mop2flash: Loading igs-bfpx.sys into flash from interface Ethernet0
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Verifying checksum...  OK (0xFEEF)
Flash copy took 435844 msecs
%FLH: Re-booting system after download
Loading igs-bfpx.sys at 0x3000040, size = 6913024 bytes [OK]

F3: 6704824+207848+262824 at 0x3000060
```

Release 11.1 Memory Requirements

The DECbrouter 90 software Version 11.1(6) image size exceeds 4 MB. This image can be used only with DECbrouter 90 models DEWB1-N Rev=C, DEWB2-N Rev=C, and DEWBR-N Rev=C or higher. The DEWB1-M, DEWB2-M, and DEWBR-M models do not have the correct boot ROM or enough DRAM or enough OS flash to load and run V11.1(6). The models DEWB1-N Rev A/B, DEWB2-N Rev A/B, and DEWBR-N Rev A/B have the correct boot flash and enough DRAM to load this image; however, they do not contain enough OS flash to run the V11.1(6) image.

Router	Minimum Required Code Memory	Required Main Memory	Release 11.1 Runs from...
Enterprise Set	8 MB Flash	8 MB RAM	Flash

New Features in Release 11.0 - 11.1

Payload Compression for Frame Relay

This feature was previously unavailable in Release 11.0. It allows payload compression of data within Frame Relay packets. Compression is performed on a packet-by-packet basis, yielding a compression ratio of approximately 1.5 to 1, depending on the packet and data characteristics. The command `frame-relay payload-compress packet-by-packet` is added.

Multilink PPP

Beginning with IOS Release 11.0(3), Multilink Point-to-Point Protocol over single or multiple interfaces is supported. Implementation of Multilink PPP supports the fragmentation and packet-sequencing specifications in RFC 1717.

PPP Callback

Supports PPP callback, which provides a client-server relationship between the end points of a point-to-point serial connection. PPP callback allows a router to request that a dial-up peer router call back. The callback feature can be used to control access and toll costs between the routers. This feature is a partial implementation of the PPP Callback specifications in RFC 1570.

General Features

This section describes general features that are new in the initial release of IOS Release 11.0.

- **Weighted fair queuing**–Weighted fair queuing is a sophisticated traffic priority management algorithm that identifies conversations (traffic streams) and then breaks up the trains of packets belonging to each conversation to ensure that the capacity is shared fairly between individual conversations. Fair queuing provides an automated way to stabilize network behavior during congestion and results in increased performance and reduced retransmission. The algorithm automatically sorts among conversations without requiring the user to define access lists. Instead, by examining sufficient fields in the packet header, the algorithm can identify unique conversations.

  Conversations are sorted into two categories: those that are attempting to use a lot of bandwidth with respect to the interface capacity (for example, FTP) and those that need less bandwidth (for example, interactive traffic). For streams that use less bandwidth, the queuing algorithm always attempts to provide access with little or no queuing and shares the remaining bandwidth between the other conversations.
- **Custom and priority queuing enhancements**–The number of queues that can be used for custom queuing and priority queuing has been increased to 16.
- **Custom and priority queuing Management Information Base (MIB)**–This MIB provides detailed access to custom and priority queuing information. This information was previously available only via the show queue EXEC command.

Backbone Protocol Routing Features

This section describes the backbone protocol routing features that are new in the initial release of IOS Release 11.0.

TCP/IP Features

The following features have been added to the IOS TCP/IP software:

- **Routing security enhancements with Message Digest 5 (MD5)**–MD5 authentication is now available for Open Shortest Path First (OSPF) and also for TCP connections between Border Gateway Protocol (BGP) peers. MD5 authentication provides a standards-based method to greatly enhance the probability that the IOS software will detect and ignore hostile or erroneous routing messages.

- **IP multicast fast switching**–Fast switching of IP multicast packets is now available. Previously, IP multicast packets were only process switched.

- **Rate limiting of IP multicast traffic**–Using access lists, you can control how fast a sender can transmit to a multicast group.

- **Protocol Independent Multicast (PIM) Nonbroadcast, Multiaccess (NBMA) mode**–PIM NBMA mode allows the router to replicate packets for each neighbor on the NBMA network.

- **Multicast static routes**–IP multicast static routes allow you to have multicast paths diverge from unicast paths. The most common reason for using separate unicast and multicast paths is tunneling. The multicast packets can use the tunnel without having unicast packets use the tunnel.

- **Session directory (SD) listener support**–The multicast backbone is widely used for multimedia conferencing. The session directory tool helps announce multimedia conference sessions and provide setup information to potential participants. A session directory client multicasts announcement packets on a well-known multicast address and port. You can enable the router to listen for such announcements.

- **Interactive input when tracing a branch of a multicast tree**–When you use the `mbranch` or `mrbranch` commands to trace a branch of a multicast tree, you can now enter information interactively.

- **Policy routing**–You can now implement IP routing policies based on source or destination IP addresses or packet lengths. Policy routing provides a more flexible method for routing packets than destination routing.

- **IP access list logging**–The router can now send a logging message to the console when a packet passes or fails an extended access list. The message includes the access list number, whether the packet was permitted or denied, the protocol, whether it was TCP, UDP, ICMP, or a number, and, if appropriate, the source and destination addresses and source and destination port numbers.

- **Open Shortest Path First (OSPF) point-to-multipoint**–Support for point-to-multipoint media types is added, allowing the IOS software to more optimally support Frame Relay-type networks using the OSPF routing protocol.

- **Border Gateway Protocol (BGP) peer groups**–You can group neighbors with the same update policies into BGP peer groups to simplify configuration and make updating more efficient.

Transparent Bridging Features

The following feature has been added to transparent bridging software:

- **Concurrent routing and bridging (CRB)**–This feature allows a given routable protocol to be routed on some interfaces and bridged on other interfaces within the same router. System managers can consolidate multiple IP subnet assignments into one IP subnet by bridging IP hosts on multiple data-link segments into one network segment. For networks that rely on packet absorption, CRB provides a `bridge-group` command that causes packets in a given protocol to be "absorbed" rather than bridged within the bridge group.

Desktop Protocol Features

This section describes the desktop protocol features that are new in the initial release of IOS Release 11.0.

AppleTalk Features

The following features have been added to AppleTalk software:

- **AppleTalk Name Binding Protocol (NBP) filters**–NBP provides directory services in AppleTalk. AppleTalk NBP filtering allows network administrators to use routers to build firewalls, dial-on-demand triggers, and queuing options based on any designed NBP type or object.

  Benefits of using NBP filters include:

  — Reducing switched circuit costs by using dial-on-demand triggers.

  — Controlling access to specific AppleTalk resources on the network (printers, file servers, and so on) with NBP access firewalls.

  — Reducing WAN costs using NBP-based traffic firewalls to prevent unnecessary NBP packets from traversing cost-per-packet network services, such as X.25, Switched Multimegabit Data Service (SMDS), and Frame Relay.

  — Minimizing NBP traffic overhead by using NBP queuing.

  — Increased AppleTalk management granularity by combining AppleTalk NBP filters with network and zone filters in a single access list.

- **AppleTalk Update-Based Routing Protocol (AURP) options**–Optional features of AURP, network number mapping, loop detection, and hop count reduction have been added.

- **AppleTalk floating static routes**–Previously available for TCP/IP and Novell/IPX environments, the floating static routes feature is now available for AppleTalk internetworking environments. Static routes are traditionally implemented so that they always take precedence over any dynamically learned routes to the same destination network. A floating static route is a statically configured route that can be overridden by dynamically learned routing information. Thus, a floating static route can help create a path of last resort that is used only when no dynamic information is available. Floating static routes can be used to provide backup routes in topologies where dial-on-demand routing (DDR) is used.

- **AppleTalk Simple Multicast Routing Protocol (SMRP)**–SMRP provides multicast routing functions for AppleTalk traffic. SMRP routes AppleTalk packets to all members of a multipoint group so that packets are not replicated on a link. Applications produced by Apple Computer, Inc., such as QuickTime Conferencing (QTC) will require support by SMRP.

Banyan VINES Features

The following feature has been added to Banyan VINES software:

- **VINES floating static routes**–Previously available for TCP/IP and Novell/IPX environments, the floating static routes feature is now available for Banyan/VINES internetworking environments. Static routes are traditionally implemented so that they always take precedence over any dynamically learned routes to the same destination network. A floating static route is a statically configured route that can be overridden by dynamically learned routing information. Thus, a floating static route can help create a path of last resort that is used only when no dynamic information is available. Floating static routes can be used to provide backup routes in topologies where dial-on-demand routing (DDR) is used.

Novell Features

The following feature has been added to Novell software:

- **Sequence Packet Exchange (SPX) spoofing**–Some SPX-based services in a Novell environment use SPX watchdog packets to verify the integrity of end-to-end communications when guaranteed and sequenced packet transmission is required. SPX spoofing implemented in the IOS software will receive, recognize, and successfully acknowledge these watchdog packets both at the server end and at the client end of the wide-area link. Requests for the transmission of legitimate information will trigger the dial-up connection. SPX spoofing can drastically reduce communications costs associated with dial-on-demand circuits.

Wide-Area Networking Features

This section describes the wide-area networking features that are new in the initial release of IOS Release 11.0.

X.25 Enhancements

The following feature has been added to X.25 software:

- **Transparent bridging over multiprotocol Link Accessed Procedure, Balanced (LAPB)**–This feature provides encapsulation of transparent bridging packets over a multiprotocol LAPB connection.

Frame Relay

The following features have been added to Frame Relay software:

- **Fast-switched Frame Relay bridging**–This feature allows Frame Relay bridging traffic (transparent bridging, source-route bridging (SRB), and remote SRB (RSRB)) to be fast-switched.

- **Data-link connection identifier (DLCI) prioritization**–This feature allows up to four DLCIs to be created between any two sites so that each DLCI has a different priority level. These DLCIs can be used to send different types of traffic such as File Transfer Protocol (FTP), Telnet, or Systems Network Architecture (SNA) on different circuits. Congestion problems that result from mixing batch and interactive traffic over a common DLCI can be alleviated for process-switched packets, and greater granularity for performance management can be attained.

- **Payload compression for Frame Relay**–This feature allows for payload compression of data within Frame Relay packets. Compression is performed on a packet-by-packet basis, yielding a compression ratio of approximately 1.5 to 1, depending on the packet and data characteristics.

IBM Functionality Features

This section describes the IBM networks software features and support that are new in the initial release of IOS Release 11.0.

The following new IBM software features are available:

- **Data-link switching plus (DLSw+) over QLLC/Frame Relay**–DLSw+ has been enhanced to support both Qualified Logical Link Control (QLLC) and direct encapsulation in Frame Relay.
- **Dial backup support for SNA Frame Relay Access Support (FRAS)**–SNA FRAS feature has been enhanced to support dial backup.

New MIB Support

The following new MIBs are available:

- **TCP/IP offload MIB**–This MIB manages configuration of the TCP offload feature.
- **STUN MIB**–This MIB provides configuration and operational information on serial tunnel (STUN) implementation.

TCP/IP Features

The following features have been added to the IOS TCP/IP software:

- **Next Hop Resolution Protocol (NHRP) Enhancements for IPX**–NHRP allows routers to dynamically discover data-link addresses for other routers on a WAN cloud, eliminating the need to configure network layer- and data link layer-addresses for all neighbors on a WAN cloud.

  NHRP has been enhanced to support IPX in addition to the IP support introduced in IOS Release 10.3. With NHRP, you can dynamically resolve IPX addresses in large-scale WAN environments in addition to resolving IP addresses. NHRP will operate using ATM, SMDS, or GRE tunneling.

- **Fast Install for Static Routes**–Floating static routes are static routes that have a higher administrative distance than other dynamic or static routes, and are often used to back up a leased-line or Frame Relay service in conjunction with the IOS software dial-on-demand routing (DDR) functionality.

  Fast Install ensures that the floating static route is installed as soon as either the routing protocol or interface reports a connectivity loss. This enables faster convergence when using dial-on-demand circuits to back up, for example, a leased-line or Frame Relay service.

- **Fast-Switched Generic Route Encapsulation (GRE)**–GRE provides the ability to handle multiple network protocols in the same tunnel. In addition, GRE includes optional sequencing and an optional security key. This feature enables fast switching for GRE tunnels. Previously, encapsulation and de-encapsulation were process switched.

- **Routing Information Protocol Version 2 (RIPv2)**–While RIPv2 shares the same basic algorithms as RIPv1, it supports new features such as authentication. RIPv2 offers two modes of authentication: a plain text password or Message Digest 5 (MD5) notification.

Desktop Protocols

This section describes the desktop protocol features that are new in the initial release of Cisco IOS Release 11.1.

AppleTalk Features

The following features have been added to AppleTalk software:

- **Simple Multicast Routing Protocol (SMRP) Fast Switching**–Fast switching of the AppleTalk multicast routing protocol, SMRP.

Novell Features

The following features have been added to Novell software:

- **Enhanced IGRP to NLSP Route Redistribution**–Enhanced IGRP to NLSP Route Redistribution is the method by which routing information is passed between Enhanced IGRP and NLSP routing domains in IPX networks.

- **IPX Input Access Lists**–This is a security enhancement feature that provides the capability of applying access lists to incoming router interfaces and the added flexibility in building secure IPX networks.

- **IPX Per-host Load Sharing**–This load-sharing process transmits successive packets (or a traffic stream) for a given end host over the same path when multiple equal-cost paths are present. Load sharing is achieved when traffic streams for different end hosts use different paths.

- **NetWare Link Services Protocol (NLSP) Route Aggregation**–NLSP is the link-state routing protocol for IPX networks.

IBM Functionality Features

This section describes the IBM network software features and support that are new in the initial release of IOS Release 11.1.

The following new IBM software features are available:

- **Downstream Physical Unit (DSPU) Network Management Events**–DSPU has been enhanced to support six new network management events.

Data Link Switching+ (DLSw+) Features and Enhancements

The following features have been added to DLSw+ software:

- **DLSw+ Management Information Base (MIB)**–DLSw+ now offers a MIB for faster problem determination. In addition, the DLSw+ MIB is the basis for DLSw+ Logical Maps.
- **DLSw+ Multidrop PU 2.0/2.1 Support**–Multidrop PU 2.0 and PU 2.1 support enables multiple PU 2.1 devices to share the same SDLC line. In addition, PU 2.0 and PU 2.1 devices can also now share the same SDLC line.
- **80D5 (Ethernet version 2) Support**–80D5 (Ethernet version 2) is now supported by DLSw+. This support extends DLSw+ to environments that have not converted to IEEE 802.3.
- **Local DLC Conversion over DLSw+**–DLSw+ now supports local conversion between SDLC or QLLC and LLC2. With local conversion, only one DLSw+ router is required for conversion of a link-level protocol. Previously, a remote peer was required to perform this conversion.
- **DLSw+ Backup Peer Enhancements**–DLSw+ allows you to specify a backup peer to use in the event that a primary peer fails. Previously, when the primary peer recovered, the backup peer connection terminated along with any sessions using that peer. The backup peer feature has been enhanced to allow the backup peer to remain active after the primary recovers, to prevent disrupting SNA and NetBIOS sessions a second time. Once the primary peer is active, all new sessions are established using the primary peer. The backup peer connection remains active until there are no active LLC2 connections on it or after a user-configurable idle time.
- **Identification Protocol Support**–The Identification Protocol (also called "ident" or "the Ident Protocol"), specified in RFC 1413, is a protocol for reporting the identity of a TCP connection initiator to the connection-receiving host.

Security Features

This section describes the security feature that is new in the initial release of IOS Release 11.1.

- **Lock-and-Key Access**–Lock-and-Key access allows you to set up dynamic IP access lists that grant access per user to a specific source or destination host through a user authentication process.

DECbrouter 90 IOS Release 11.1(6) Release Notes Caveats

This section describes possibly unexpected behavior by Release 11.1(6). Unless otherwise noted, these caveats apply to all 11.1 releases up to and including 11.1(6).

Upgrading to a New Software Release

If you are upgrading to IOS Release 11.1 from an earlier IOS software release, you should save your current configuration file before installing Release 11.1 software on your router.

AppleTalk

- When ARAP is configured, the message `%SYS-2-INPUTQ: INPUTQ set, but no idb, ptr=xxxxx %SYS-2-LINKED: Bad enqueue of xxxxx in queue yyyyy` might appear and the router might reload. **[CSCdi63635]**

- Additional debugging messages need to be created for the `arap logging` command. A new command, `arap logging debug-extensions`, is proposed. This command would enable seven advanced debugging messages in addition to the traditional `arap logging` messages. **[CSCdi68276]**

- If a `microcode reload` command is issued over a Telnet connection, the router may enter an infinite loop. **[CSCdi47580]**

- Interrupt-level IP fragmentation is not supported. **[CSCdi60461]**

- In cases where a complex queuing strategy is desired that uses rules based on interfaces intermixed with rules based on protocols, the desired strategy cannot be recovered from a saved configuration. The order that the rules are entered is the order that the rules are applied. This works as desired. However, the order of entry is currently not maintained when the rules are stored in a sorted order in the configuration. Hence upon reboot, the behavior is different because the order of the rules has changed. This does not affect homogeneous rule systems, for example, systems where all the rules are based on interfaces or on protocols. It affects only more complex strategies where the rules are intermingled. **[CSCdi63068]**

- When `service compress-config` is configured, accessing the configuration stored in NVRAM from simultaneous Exec sessions might leave the NVRAM locked and inaccessible. The only recourse is to reload the software. **[CSCdi68092]**

Bridging

- If you use the configuration script to enable bridging, it defaults to the "DEC" protocol spanning tree. This can cause problems in some networks. You may want to change this back to the IEEE protocol.

DECnet Phase V

- There may be interoperability issues between the DECbrouter 90 and other Digital Phase V routers in a Phase V network, depending on the version of routing code running on the routers. However, there are no interoperability issues if a DECbrouter 90 is used along with other Digital Phase V routers if the entire network is either all Phase IV or a pure OSI environment.

IBM Connectivity

- QLLC devices that are connected through a router using QLLC/LLC2 conversion might occasionally experience poor response time. **[CSCdi44923]**

- The router might crash when an SNMP `Get` command is issued for ciscoDlswIfSapList from a management station. **[CSCdi49400]**

- OID is returned on an SNMP `GetNext` message for ciscoDlswIfRowStatus, and ciscoDlswIfVirtualSegment is not incremented. This may cause the application on the management station issuing this command to go into an infinite loop. **[CSCdi49401]**

- The Cisco DLSw MIB returns an incorrect value for ciscoDlswVersions, which is inconsistent with the Cisco DLSw MIB definition. **[CSCdi49426]**

- The Cisco DLSw MIB returns an incorrect value for ciscoDlswVendorID, which is inconsistent with the Cisco DLSw MIB definition. **[CSCdi49430]**

- OID returned on an SNMP `GetNext` command for ciscoDlswCircuit is not incremented. This may cause the application on the management station issuing this command to go into an infinite loop. **[CSCdi49437]**

- Some IBM LLC2 implementation devices send an RNR when they run out of buffers and drop the frame. This causes data traffic flow to halt for 30 seconds. Non-IBM LLC2 devices using IEEE LLC2 send REJ rather than RNR, thus no delay occurs. **[CSCdi49447]**

- The `dlsw remote-peer frame-relay interface serial` command does not work on a point-to-point subinterface. The workaround is to use multipoint and do LLC mapping. **[CSCdi55085]**

- QLLC cannot use X.25 PVCs for DLSw+. The workarounds are to use RSRB or to use X.25 SVCs. **[CSCdi58735]**

- With Release 11.0 and a direct Escon-attached CIP, the host may "box" the CIP if the router is reloaded without the CIP being varied offline. This problem has not been seen with CIPs connected through a director or if the CIP is taken offline before the router is reloaded. The workaround is to vary the device offline before reloading the router. **[CSCdi59440]**

- When `source-bridge sdllc-local-ack` is enabled, the router stays in disconnect after the SDLC PUs are deactivated in VTAM. The workaround is to remove the `sdllc-local-ack`. **[CSCdi64640]**

- LSAP filters and NetBIOS host filters that are applied to the DLSw remote-peer statements do not work on DLSw border routers. **[CSCdi66251]**

- For STUN virtual multidrop configurations running `local-ack` and `STUN quick-response` to accommodate AS/400 polling requirements, an AS/400 NPR timeout occurs if a remote PU T2.1 or T1 controller fails to activate when responding to the initial XID poll. The workaround is to disable `STUN quick-response`, issue the `sdlc k 1` command on all SDLC interfaces, and place an idle-character mark on the SDLC lines to the AS/400. **[CSCdi66681]**

- When you perform buffer changes on a serial interface with SMDS encapsulation, the changes are not recognized after a reload. **[CSCdi62516]**

IP Routing Protocols

- A RIP update should be sent immediately when a dialer interface changes from "UP & UP" (spoofing) to "UP & UP." **[CSCdi59478]**

- If the router is reloaded when the OSPF `dead-interval` setting is the same as the original default (`40` for broadcast network and `120` for nonbroadcast network), and the `hello-interval` is not default, the router does not retain the OSPF `dead-interval` setting, even though the configuration in NVRAM shows the `dead-interval` set properly. The router sets a default value to the `dead-interval` instead of what is set in the NVRAM config.

  The workaround is to not set the `dead-interval` the same as the original default.

  When the fixed image is first loaded, the problem still happens. To resolve the problem, reconfigure the `dead-interval` again and perform a write memory operation. **[CSCdi62640]**

- The match keyword is not working with the `redistribute` command. The workaround is to use the `route-map` keyword. **[CSCdi64310]**

- IPX Enhanced IGRP updates do not propagate if the MTU size is less than the IPX Enhanced IGRP packet size. **[CSCdi65486]**

- Processing of input offset lists in Enhanced IGRP was disabled erroneously, so offset list processing is not available. There is no workaround. **[CSCdi65889]**

- iBGP peers configured in a cluster may not receive iBGP routes from the route reflector if the route is not synchronized. **[CSCdi66678]**

- If you have neighbor statements pointing to a subnet broadcast address, it may fail to send updates to that broadcast address. **[CSCdi67411]**

ISO CLNS

- If secondary addresses are configured on an interface that is otherwise configured unnumbered, the interface routes corresponding to these addresses are not advertised in IS-IS. A workaround is to number the interface. **[CSCdi60673]**

Novell IPX, XNS, and Apollo Domain

- After upgrading Cisco IOS software, a show processor memory command might indicate that the IPX SAP table memory usage has grown by almost 300 percent. **[CSCdi65740]**

- Using IPX-Enhanced IGRP can cause a memory leak when a link with an Enhanced IGRP neighbor is flapping. The SAP updates are queued and backed up, thus taking increasing amounts of memory. **[CSCdi66169]**

Wide-Area Networking

- TCP header compression does not work over Point-to-Point Protocol (PPP). The workaround is to turn off `ip tcp header-compression`. **[CSCdi19199]**

- Both the one-word connect feature and the EXEC connect command fail without printing any error indication. This only occurs in Enterprise software images. **[CSCdi41547]**

- When illegal bridging packets flow into Cisco routers running Release 11.0 and above, a crash might occur. **[CSCdi67157]**

- When parallel, nonmultilink connections exist in a dialer group, the loss of one connection will remove the route to the peer address even though one or more connections exist to forward packets to the destination. This defect occurred as a result of fixing CSCdi59425. **[CSCdi67844]**

- If multiple, parallel connections to the same peer are made and one connection drops, the remaining connections may be unusable because packets will not be forwarded over them. **[CSCdi68456]**

Accessing Online Information

Network Product Business Web Site

Further information on this network product or topic is available on Digital's Network Product Business Web Site as well as its Bulletin Board System. Both systems maintain a common, rich set of up-to-date information on NPB's products, technologies, and programs.

The Web Site can be reached at geographic locations via the following URLs:

Americas Network Product Business Home Page	http://www.networks.digital.com/
Europe Network Product Business Home Page	http:/www.networks.europe.digital.com/
Australia Network Product Business Home Page	http://www.digital.com.au/networks/
Digital Equipment Corporation Home Page	http://www.digital.com/

To get firmware and MIB information, please choose the "Technical Information" link, and from there choose the "Technical Information (Drivers, Manuals, Tech Tips, etc.)" link.

To connect to the Network Product Business Bulletin Board System, you need a PC and a modem. Dial 508-486-5777 (U.S.A.). Set your modem to 8 bits, no parity, 1 stop bit.

Using Electronic Mail

The DDN Network Information Center (NIC) of SRI International provides automated access to NIC documents and information through electronic mail. This is especially useful for users who do not have access to the NIC from a direct Internet link, such as BITNET, CSNET, or UUCP sites.

To use the mail service, follow these instructions:

1. Send a mail message to **SERVICE@NIC.DDN.MIL**.
2. In the SUBJECT field, request the type of service that you want followed by any needed arguments.

Normally the message body is ignored, but if the SUBJECT field is empty, the first line of the message body is taken as the request.

The following example shows the SUBJECT lines you use to obtain DDN NIC documents:

HELP

RFC 822

RFC INDEX

RFC 1119.PS

FYI 1

IETF 1IETF-DESCRIPTION.TXT

INTERNET-DRAFTS 1ID-ABSTRACTS.TXT

```
NETINFO DOMAIN-TEMPLATE.TXT

SEND RFC: RFC-BY-AUTHOR.TXT

SEND IETF/1WG-SUMMARY.TXT

SEND INTERNET-DRAFTS/DRAFT-IETF-NETDATA-NETDATA-00.TXT

HOST DIIS
```

Requests are processed automatically once a day. Large files are broken into separate messages.