

# DIGITAL GIGAswitch/IP Solution for ATM

---

## Installation and Configuration

Part Number: EK-DAGGI-IG. B01

**March 1997**

This document describes the installation and configuration of the DIGITAL GIGAswitch/IP products.

**Revision/Update Information:** This is a revised manual.

Digital Equipment Corporation makes no representations that the use of its products in the manner described in this publication will not infringe on existing or future patent rights, nor do the descriptions contained in this publication imply the granting of licenses to make, use, or sell equipment or software in accordance with the description.

Possession, use, or copying of the software described in this publication is authorized only pursuant to a valid written license from Digital or an authorized sublicensor.

© Copyright Ipsilon Networks, Incorporated 1996. All rights reserved.

© Portions copyright Digital Equipment Corporation 1997. All rights reserved. Printed in U.S.A.

The following are trademarks of Digital Equipment Corporation: clearVISN, DECconnect, DEChub, DECnet, DECswitch, DIGITAL, FLOWmaster, GIGAswitch, and the DIGITAL logo.

The following are third-party trademarks:

AppleTalk is a registered trademark of Apple Computer, Inc.

Novell and IPX are registered trademarks of Novell, Inc.

Netscape Communications, Netscape, and Netscape Navigator are trademarks of Netscape Communications Corporation.

PENTIUM is a registered trademark of Intel Corporation.

All other trademarks and registered trademarks are the property of their respective holders.

**FCC Notice** — Class A Computing Device:

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference. Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference. 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.

**VCCI Notice** — Class 1 Computing Device:

This equipment is in the 1st Class category (information equipment to be used in commercial and/or industrial areas) 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 commercial and/or industrial areas. Consequently, when used in a residential area or in an adjacent area thereto, radio interference may be caused to radios and TV receivers. Read the instructions for correct handling.

**CE Notice** — Class A Computing Device:

**Warning!**

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

**Achtung!**

Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

**Avertissement!**

Cet appareil est un appareil de Classe A. Dans un environnement résidentiel cet appareil peut provoquer des brouillages radioélectriques. Dans ce cas, il peut être demandé à l'utilisateur de prendre les mesures appropriées.

# Contents

---

## Preface

Overview .....	vii
Intended Audience .....	vii
Content .....	vii
Conventions .....	viii
Online Services .....	viii
BBS .....	viii
WWW .....	viii
How to Order Additional Documentation .....	ix

## 1 System Overview

DIGITAL GIGAswitch/IP Controller .....	2
DIGITAL IP Switch Gateway .....	2

## 2 Installing and Configuring a Network

Overview of the Installation Process .....	3
Designing a Network .....	3
Network Numbers and Network Masks .....	4
Logical Names .....	5
Routing Protocols .....	6
Sample Network Design .....	6
Installing DIGITAL GIGAswitch/IPs and DIGITAL IP Switch Gateways in Your Network .....	8
Upgrading the Software .....	8
Configuring the Network .....	10
Using the Lynx Browser .....	11
Preparing to Use the Netscape Navigator Browser .....	13
Using the Netscape Navigator Browser .....	14
Configuring the Network with the Configuration Tool .....	15
Verifying the Configuration .....	17

Step 1: Check that the DIGITAL GIGAswitch/IP Switch Controller and DIGITAL GIGAswitch/ATM Have Synchronized . . . . .	17
Step 2: Verify Interface Configuration . . . . .	18
Step 3: Check Whether Remote Interface Addresses Have Been Established . . . . .	18
Step 4: Check That Neighbors Are Reachable. . . . .	19
Step 5: Examine the Unicast Routing Tables. . . . .	19
Backing Up Files. . . . .	21
Restoring a Configuration File from a Backup. . . . .	22
Accessing the Configuration File. . . . .	22
Interpreting ifconfig Output . . . . .	23

### 3 Example Configuration

Overview . . . . .	25
Configuration Overview . . . . .	25
Configuring the Sample Network with clearVISN IP Switch Manager . . . . .	28

### 4 DIGITAL GIGAswitch/ATM Configuration Commands

Overview . . . . .	39
For More Information . . . . .	39
Prerequisites . . . . .	40
Check the Equipment. . . . .	40
Upgrade the DIGITAL GIGAswitch/ATM Firmware. . . . .	41
configure_ipswitch Command . . . . .	42
Configuration Overview . . . . .	42
Use the configure_ipswitch Command . . . . .	42
Sample configure_ipswitch Session. . . . .	44
delete_ipswitch_config Command . . . . .	45
Create a New Configuration . . . . .	45
Use the delete_ipswitch_config Command . . . . .	45
show_ipswitch_config Command . . . . .	46
Use the show_ipswitch_config Command . . . . .	46
Sample show_ipswitch_config Session . . . . .	46

## 5 Troubleshooting

Overview .....	47
Problem: The DIGITAL GIGAswitch/IP Switch Controller and DIGITAL GIGAswitch/ATM do not synchronize. ....	47
Problem: Interfaces are not configured .....	48
Problem: No IFMP synchronization .....	49
Problem: Unable to ping neighbors .....	50
Problem: When doing a traceroute, unable to get all the way to the place I am tracing .....	51
Problem: No multicast reachability .....	53
Problem: The IP switching network does not learn about routes from my RIP attached router ..	54

## 6 Network Design Table

## 7 Network Identifiers: Addresses and Interface IDs

Overview .....	61
IP Addressing .....	61
Subnetting .....	61
Subnet Mask Reference Charts .....	62



---

# Preface

---

## Overview

This document describes the upgrade and configuration procedures for the DIGITAL GIGAswitch/IP products.

## Intended Audience

This document is intended for the network administrator who is installing DIGITAL products for the first time or who is upgrading and configuring an existing installation.

## Content

The major topics covered in this book are:

---

<b>To Find Information About:</b>	<b>See this Section:</b>
Technical specifications	System Overview on page 1
How the DIGITAL GIGAswitch/IP and DIGITAL IP Switch Gateway fit into a network	System Overview on page 1
How to design a network	Designing a Network on page 3
How to install DIGITAL GIGAswitch/IP Switch Controllers and DIGITAL IP Switch Gateways	Designing a Network on page 3
How to configure a network	Designing a Network on page 3, and Chapter 3, Example Configuration
How to configure IP switching on the DIGITAL GIGAswitch/ATM	DIGITAL GIGAswitch/ATM Configuration Commands on page 39
Troubleshooting	Troubleshooting on page 47

---

## Conventions

This manual uses the following conventions:

---

<i>italic text</i>	Indicates a document title or a variable in examples.
<code>typewriter text</code>	Indicates a command, program, filename, or pathname.
<b>bold typewriter text</b>	Indicates text that you type in examples.
SMALL CAPS	Represents the name of a key on the keyboard, of a button displayed on your screen, or of a button or switch on the hardware. For example, press the RETURN key or click the CANCEL button.

---

## Online Services

To locate product-specific information, refer to the following online services:

### BBS

To read the Bulletin Board System, set your modem to 8 bits, no parity, 1 stop bit and dial 508-486-5777 (U.S.).

### WWW

The Digital Equipment Corporation Network Products Business Home Page on the World Wide Web is at the following addresses:

North America: <http://www.networks.digital.com>

Europe: <http://www.networks.europe.digital.com>

Australia: <http://www.digital.com.au/networks>

The DIGITAL GIGAswitch/IP specific files are located at the following address:

<http://www.networks.digital.com/dr/gigaip/firmware/>

The DIGITAL GIGAswitch/ATM files are located at the following address:

<http://www.networks.digital.com/dr/gigatm/firmware/>



## How to Order Additional Documentation

To order additional documentation, use the following information:

<b>To Order:</b>	<b>Contact:</b>
By Telephone	USA (except Alaska, New Hampshire, and Hawaii): 1-800-DIGITAL (1-800-344-4825) Alaska, New Hampshire, and Hawaii: 1-603-884-6660 Canada: 1-800-267-6215
Electronically (USA only)	Dial 1-800-DEC-DEMO (For assistance, call 1-800-DIGITAL)
By Mail (USA and Puerto Rico)	DIGITAL EQUIPMENT CORPORATION P.O. Box CS2008 Nashua, New Hampshire 03061 (Place prepaid orders from Puerto Rico with the local DIGITAL subsidiary: 809-754-7575)
By Mail (Canada)	DIGITAL EQUIPMENT of CANADA LTD. 940 Belfast Road Ottawa, Ontario, Canada K1G 4C2 Attn.: A&SG Business Manager
Internationally	DIGITAL EQUIPMENT CORPORATION Attn.: A&SG Business Manager c/o local DIGITAL subsidiary or approved distributor
Internally	U.S. Software Supply Business (SSB) DIGITAL EQUIPMENT CORPORATION 8 Cotton Road Nashua, New Hampshire 03063



# System Overview

---

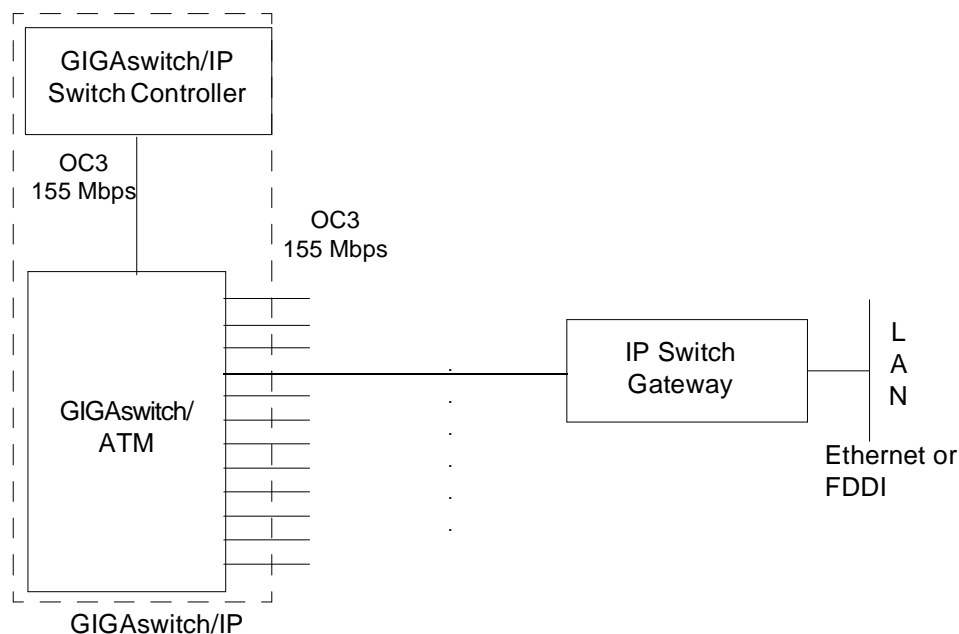
The DIGITAL GIGAswitch/IP software supports two DIGITAL products:

- DIGITAL GIGAswitch/IP Switch Controller
- DIGITAL IP Switch Gateway

The DIGITAL GIGAswitch/ATM and DIGITAL GIGAswitch/IP Switch Controller are connected by an Asynchronous Transfer Mode (ATM) link. Collectively, these components are referred to as the GIGAswitch/IP. The GIGAswitch/IP Switch Controller, the GIGAswitch/ATM, and the IP Switch Gateway each consist of both hardware and software.

Figure 1-1 shows the logical connections among the components:

**Figure 1-1: Logical Connections Among the Components of a Network**



## DIGITAL GIGAswitch/IP Switch Controller

### Hardware

The DIGITAL GIGAswitch/IP Switch Controller consists of:

- PENTIUM processor
- 16 megabytes (MB) memory
- 1.2 gigabytes (GB) storage capacity on disk
- One ATM Network Interface Card (NIC) 155 megabits per second (Mbps) — required for connection to the GIGAswitch/ATM
- One diagnostic Ethernet port

### Software

The GIGAswitch/IP Switch Controller software is shipped preloaded. It provides the functionality necessary to perform IP switching, routing, network management through SNMP, network management through the Web, and configuration.

## DIGITAL IP Switch Gateway

### Hardware

The DIGITAL IP Switch Gateway consists of the same components as the DIGITAL GIGAswitch/IP Switch Controller, except it has:

- 32 megabytes (MB) memory

In addition to the ATM NIC, it includes one of the following PCI NICs:

- Single-port 10Mb/100Mb Ethernet NIC
- Fiber Distributed Data Interface (FDDI) NIC

### Software

The IP Switch Gateway software is shipped preloaded. It provides the functionality necessary to perform IP switching, routing, network management through SNMP, network management through the Web, and configuration.

# Installing and Configuring a Network

---

## Overview of the Installation Process

Both the DIGITAL GIGAswitch/IP and DIGITAL IP Switch Gateway have the software preloaded. This document covers the process of physically installing the switches and gateways and configuring them as part of your network.

The instructions for installation are divided into four sections that represent the four main steps in the installation process:

1. Designing a Network on page 3
2. Installing DIGITAL GIGAswitch/IPs and DIGITAL IP Switch Gateways in Your Network on page 8
3. Upgrading the Software on page 8
4. Verifying the Configuration on page 17

These four steps must be performed in the specified order. Within each of these steps, you can choose various options depending on the type of network you are configuring and on your level of expertise. In addition, Chapter 3, Example Configuration steps you through the process of configuring the example network shown in Figure 2-1 on page 5.

## Designing a Network

Before you can configure a GIGAswitch/IP or IP Switch Gateway, you must:

- Choose a network number and a network mask length for each network connected to the GIGAswitch/IP.
- Obtain the network number and network mask length for each network connected to the IP Switch Gateway.

- Identify the logical name for each interface on each GIGAswitch/IP Switch Controller and IP Switch Gateway.
- Know which unicast and multicast routing protocol(s) are running on each network connected to each IP Switch Gateway.

## Network Numbers and Network Masks

Each connection between a GIGAswitch/IP and another GIGAswitch/IP or IP Switch Gateway must have its own subnetwork number. These subnetwork numbers must be different from any other subnetwork number. Your subnetwork numbers are allocated by your Internet service provider, although once you have been allocated a block of numbers you may choose how to assign them to your machines.

For IPv4, an IP address is a 32-bit value consisting of two parts. The first part is the subnetwork number. The remainder of the bits are used to distinguish the hosts on the subnetwork, and are called the host interface numbers. IP allows for subnetwork numbers to have different lengths. The length of the subnetwork number in bits is referred to as the network mask length.

For example, a network mask of length 24 means that IP addresses using this mask consist of 24 bits of subnetwork number and 8 bits of host interface numbers. By convention, a host number of all 0 bits identifies the network itself and a host number of all 1 bits is the broadcast address.

We recommend that ATM links in your network use a network mask length of 30 bits. Using large netmasks helps conserve IP address space on subnetworks that will have only a few hosts attached.

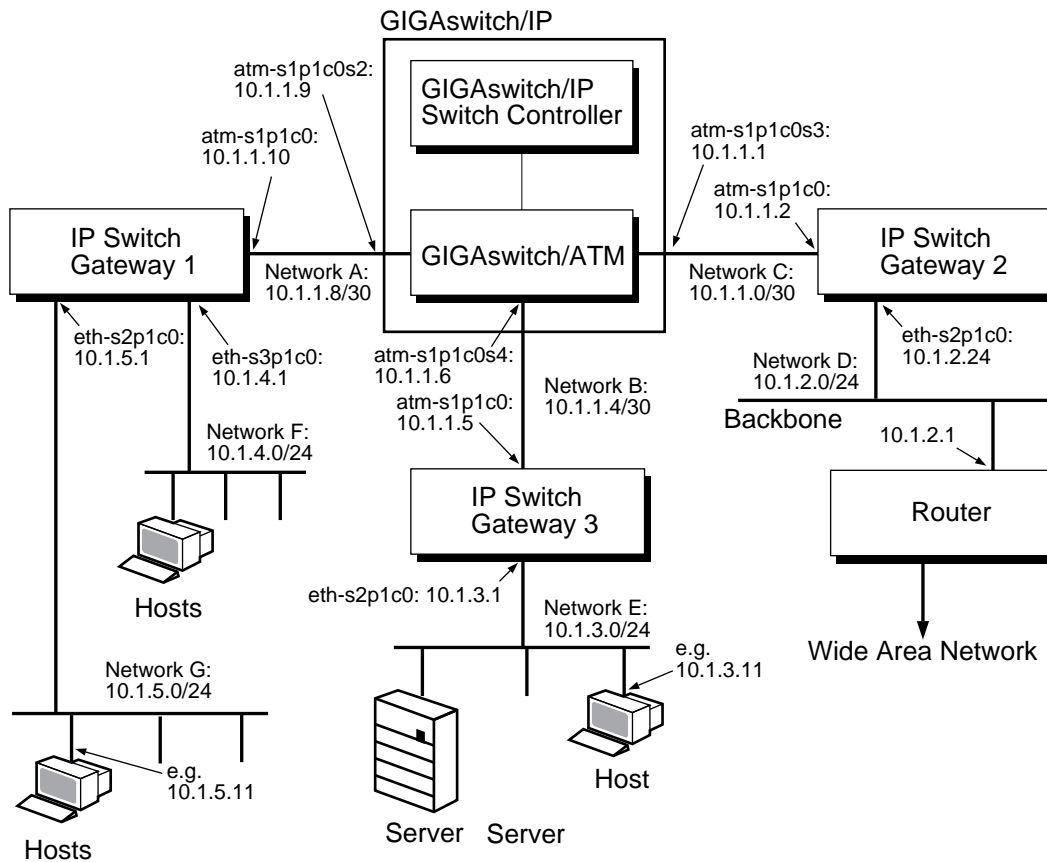
The ATM links are point-to-point interfaces, so each can support only two hosts. The 30-bit netmask leaves two bits for host addressing, for a total of four available addresses. Two of these addresses correspond to the subnetwork and broadcast addresses, and the other two are used for the host machine:

- 0 for the subnetwork itself
- 1 and 2 for the two ends of the subnetwork (one at the GIGAswitch/IP and the other at another GIGAswitch/IP or at an IP Switch Gateway)
- 3 for the broadcast address

You also need to know the subnetwork numbers and network mask lengths for each network that you will connect to an IP Switch Gateway.

Figure 2-1 shows a sample network layout, with 30-bit and 24-bit network masks as described in this section. The mask length is indicated by a slash (/) and a number representing the length at the end of an IP address.

Figure 2-1: An Example Network



LKG-10302-96F

Table 2-1 shows the equivalent network mask length notations for 24- and 30-bit net masks in quad and CIDR notation;

Table 2-1: Equivalent Network Mask Notations

Network mask length	Quad notation	CIDR notation
24	255. 255. 255. 0	/24
30	255. 255. 255. 252	/30

### Logical Names

Use the following logical names for interfaces on GIGAswitch/IP Switch Controllers and IP Switch Gateways.

- For GIGAswitch/IP Switch Controllers:
  - atm-s1p1c0 for the ATM interface on the GIGAswitch/IP Switch Controller and atm-s1p1c0\_1 for the port on the GIGAswitch/ATM that connects to the GIGAswitch/IP Switch Controller
  - atm-s1p1c0sn, where *n* is a number from 2 to 16 (for example, atm-s1p1c0s2), for the interfaces from the GIGAswitch/ATM to other GIGAswitch/ATMs or IP Switch Gateways

- For IP Switch Gateways:
  - `atm-s1p1c0` for the ATM interface that connects to the GIGAswitch/ATM
  - `eth-snp1c0`, where *n* is a number from 0 to 11 (for example, `eth-s2p1c0`), for the interfaces from the GIGAswitch/IP Switch Gateway to other networks
  - `fddi-s2p1c0` for an FDDI interface from the IP Switch Gateway to other networks

## Routing Protocols

The GIGAswitch/IP and IP Switch Gateway support the following routing protocols:

- **OSPF:** Always use this unicast routing protocol for the interfaces that connect a GIGAswitch/IP with another GIGAswitch/IP or IP Switch Gateway. In addition, use it for interfaces that connect an IP Switch Gateway to a network that already runs OSPF.
- **RIP:** Use this unicast protocol for interfaces that connect an IP Switch Gateway to a network that already runs RIP.
- **DVMRP:** Use this protocol if you want to run multicast. It allows interfaces to connect an IP Switch Gateway to a network that already runs DVMRP, and it should be used for the connection between that IP Switch Gateway and the GIGAswitch/IP.
- **Router Discovery:** Use this service to advertise the ability to serve as a default router for a stub segment. Router discovery can be used as a failover mechanism with small timeouts (less than 15 seconds), although this is not recommended.

## Sample Network Design

To help you get started, fill in a table like the one in Figure 2-2. A blank form similar to the one in Figure 2-2 is provided on page 64. The first few rows have been filled in with information corresponding to Figure 2-1, with the following assumptions:

- The interfaces on network D are running RIP
- The interfaces on networks E, F, and G are running OSPF and DVMR



Figure 2-2: Sample Network Design Table

Network Number	Mask Length	From			To			Uses OSPF?	Uses RIP?	Uses DVMRP?	Uses Router Disc.?
		Where	Logical Name	IP Address	Where	Logical Name	IP Address				
10.1.1.8	30	GIGAswitch/ IP	atm- s1p1c0s2	10.1.1.9	Gateway 1	atm- s1p1c0	10.1.1.10	Yes		Yes	
10.1.1.0	30	GIGAswitch/ IP	atm- s1p1c0s3	10.1.1.1	Gateway 2	atm- s1p1c0	10.1.1.2	Yes		Yes	
10.1.1.4	30	GIGAswitch/ IP	atm- s1p1c0s4	10.1.1.6	Gateway 3	atm- s1p1c0	10.1.1.5	Yes		Yes	
10.1.2.0	24	Gateway 2	eth- s2p1c0	10.1.2.24	Network D				Yes	Yes	
10.1.3.0	24	Gateway 3	eth- s2p1c0	10.1.3.1	Network E			Yes		Yes	
10.1.4.0	24	Gateway 1	eth- s3p1c0	10.1.4.1	Network F			Yes		Yes	
10.1.5.0	24	Gateway 1	eth- s2p1c0	10.1.5.1	Network G			Yes		Yes	

## Installing DIGITAL GIGAswitch/IPs and DIGITAL IP Switch Gateways in Your Network

1. Prepare a diagram of the desired topology of your network, labelled with IP addresses.

The installation instructions in this guide are based on the sample network illustrated in Figure 2-1. In preparation for installation, create a drawing similar to that figure that illustrates your network topology.

2. Familiarize yourself with the description of the hardware in Chapter 1, DIGITAL GIGAswitch/IP Products Overview of the *DIGITAL GIGAswitch/IP Solution for ATM Products Reference*.
3. Follow the instructions for physically setting up your GIGAswitch/IPs and IP Switch Gateways in Chapter 2, Installing DIGITAL GIGAswitch/IP Products of the *DIGITAL GIGAswitch/IP Solution for ATM Products Reference*.

## Upgrading the Software

The GIGAswitch/IP Switch Controller and IP Switch Gateway software are shipped preloaded. However, if you need to upgrade the software, complete the following steps:

1. Obtain the upgrade kit from the following location:

<http://www.networks.digital.com/dr/gigaip/firmware/>

The upgrade kit is distributed as a single file, with the name `ipso-version-D.tgz` where *version* is the software version. For example, `ipso-1_2_1-D.tgz` is version 1.2.1 of the software.

2. Log in to the system to be upgraded using the username, `root`. You can log in to the system in one of two ways:
  - Remotely using TELNET
  - Locally by attaching a VT-series compatible terminal to the console port of the system.
3. Create a temporary directory for the kit using the `mkdir` command as follows:

```
# mkdir /kit
# cd /kit
```

4. Invoke `ftp` as in the following example where *filename* is the name of the file that you want to copy:

```
# ftp filename.com
Connected to filename.com.
220 filename.com FTP server ready.
User (filename.com:(none)): anonymous
```

```

331 Anonymous login okay, send ID as password
Password:
230 User anonymous logged in.
Use binary mode of ftp to copy the file to the system as in the
following example:
ftp> bin
200 Type set to I.
ftp> get ipso-1_2_1-D.tgz
200 PORT command successful.
150 Opening BINARY mode data connection for ipso-1_2_1-D.tgz
226 Transfer complete.
ftp> quit
#

```

---

### Note

The file you have copied is a compressed archival file. **Do not** decompress or unpack the compressed file. The software upgrade process does that automatically.

---

5. Issue the setup command to start the software upgrade process, as follows:

```

# setup
.
.
.

Checking existing software: (this may take some time...)

```

Product	Version	Created On	Installed on
-----	-----	-----	-----
ipso	1.2.1-D	02/12/97	02/19/97

Do you wish to proceed? [y] **Y**

6. Enter **Y** to proceed with the upgrade. The upgrade process prompts you to answer a series of questions, as shown in the following example:

```

Please select one of the following:
  1. Install/Upgrade software
  2. Check existing software installations
  3. Restore to previous installation
  4. Delete backup files from previous installations
  5. Quit (and exit this program)

Please enter your choice [ 1 ]: 1

Please select install media type:
  1. File from local file system
  2. FTP with username and password
  3. Anonymous FTP
  4. Quit this menu.

```

```
Enter choice [ 1 ] : 11
Enter install filename : /kit/ipso-1_2_1-D.tgz

You have entered the following information:
    target: /kit/ipso-1_2_1-D.tgz
Proceed with the above information? [y] y
```

7. Enter Y to start the upgrade.
8. When the upgrade is complete, exit the upgrade utility, and reboot the system. You may verify the upgrade as follows:
  - a. Access the clearVISN IP Switch Manager interface on the Web.
  - b. Access the Monitor page.
  - c. Check the firmware version.

## Configuring the Network

Digital Equipment Corporation provides two methods for configuring your network:

- **The ASCII-based Lynx Browser.** If you have no network connectivity between your network, your GIGAswitch/IPs, and your IP Switch Gateways, use the ASCII-based Lynx browser running on a terminal connected to the serial port on each GIGAswitch/IP Switch Controller or IP Switch Gateway. The Lynx 2.4.2 browser is supplied as part of the standard GIGAswitch/IP software.<sup>1</sup>
- **The Graphical Browser.** If you have network connectivity and have access to a host machine capable of running Netscape Navigator™ version 2 or later, use the graphical Configuration Tool to configure your network remotely. The Configuration Tool has been designed to run with and was tested with Netscape Navigator 2.0. Configuration Tool online help uses the separate window feature of Netscape Navigator 2.0 to make reading help topics easier.

Even if you are familiar with the browser you will use, read the section on that browser for important start-up information.

There are a number of possible ways to configure your network, using Lynx, Netscape Navigator, and the system command line (commands issued other than from inside a browser). You must configure the first node using either Lynx or the command line, because it is not possible to configure with Netscape Navigator until there is connectivity between a host running Netscape and the first node. The next sections briefly describe how to use the Lynx and Netscape Navigator browsers to configure your network.

---

1. Although you can use the Lynx 2.4.2 browser for configuration, do not use it for running the Monitor Tool because Lynx does not support HTML 3.0 tables.

- Using the Lynx Browser on page 11
- Preparing to Use the Netscape Navigator Browser on page 13
- Using the Netscape Navigator Browser on page 14

The section describes how to create a `configuration` file for a node with Configuration Tool, using either browser.

- Configuring the Network with the Configuration Tool on page 15

Chapter 3, Example Configuration walks through the entire process of configuring the example network shown in Figure 2-1 (page 5).

## Using the Lynx Browser

1. Log in to an IP Switch Gateway as root, through the serial port.  
The log-in procedure leads you through the process of providing a host name, system type, and passwords for the `root`, `admin`, and `monitor` accounts.
2. When prompted, enter the host name:  
`hostname.acme.com`
3. When prompted, confirm the displayed host name by typing `y` if it is correct, or `n` if it is not.
4. When prompted, enter 1 if you are configuring an IP Switch Gateway or 2 if you are configuring a GIGAswitch/IP Switch Controller.
5. When prompted, enter passwords for the `root`, `admin`, and `monitor` accounts.  
You are prompted to enter each password twice.
6. If you are using Lynx from a terminal window that can display 40 or more lines of output at a time, use the `stty` command to tell it to display 40 lines:  
`stty rows 40`
7. To configure your node with the Lynx browser, type the following command on a VT100 console connected to the IP Switch Gateway:  
`lynx`  
Ignore the message that flashes briefly on your screen:  
`Alert!: Access without authorization denied -- retrying`
8. When prompted for a User ID, enter:  
`admin`
9. Enter the admin password and select OK.  
The first view that is displayed is the CONFIGURATION MENU. When the CONFIGURATION MENU appears, only the first item is choosable: CREATE OR MODIFY CONFIGURATION FILE.
10. Select CREATE OR MODIFY CONFIGURATION FILE by pressing RETURN.

Note that when this view is displayed, only the first menu item is highlighted. After you create or modify the configuration file, the other menu items become highlighted.

If you are not already familiar with Lynx, the use of highlighting may be confusing. The highlighted items are the menu items that currently can be chosen. Items that can be chosen are called active items. The cursor is indicated by an extra single space of highlighting at the left end of a highlighted item.

The cursor initially points at the first active item on the current view. Because this cursor can be difficult to detect, you can use the up and down arrows to move the cursor, making it more visible.

To follow a link, move the cursor to an item and press RETURN or the right arrow key. To move between highlighted fields, use the up and down arrow keys.

---

### Note

Do not use the left arrow key to go back to a link you have followed. Select the HOME or MENU link at the bottom of the view. The one exception to this is if you have selected the HELP link. Use the left arrow key to return from the HELP view

---

Active items come in a variety of forms. The main ones you encounter in the Configuration Tool are:

- Square brackets delimiting an item: this item has a menu of values that you can access by pressing the right arrow key. Select an item from the menu with the up and down arrow keys, and exit the menu by pressing RETURN. Figure 2-3 shows a menu of values that you see before you press the arrow keys.

**Figure 2-3: A Menu of Values**

```
Currently editing:
Select File: eth-s2p1c0.conf Select File:*****
                * eth-s2p1c0.conf *
                * gateway1.conf *
                * gateway2.conf *
                * gateway3.conf *
                * network1.conf *
                *****
```

- A string of hyphens: this is a fill-in-the-blank field that you can type into. When you have supplied the value for the field, move the cursor to the next field with the down arrow button. If it is the last field on a view, move the cursor to the OK field and press the right arrow key.

**Figure 2-4: A Fill-in-the-Blank Field**

```
Create a new configuration file.
Filename: -----
```

- A list of items, each with a set of parentheses next to it: this is a list of radio buttons. One item from the list must be selected at all times. The selected item in the list is indicated by an asterisk between the parentheses. To change which item is selected, move the cursor to the item you want to choose and press RETURN.

**Figure 2-5: Radio Buttons**

```
Edit: ( )New ( )Copy (*)Modify ( )Delete
```

## Preparing to Use the Netscape Navigator Browser

1. Log in to the IP Switch Gateway as root.

The log-on procedure leads you through the process of providing passwords for the `root`, `admin`, and `monitor` accounts. You must supply passwords for these accounts.

Before starting the Netscape Navigator browser, you must assign an IP address to each IP Switch Gateway so that other machines on the network can establish communication with the IP Switch Gateways.

2. Temporarily assign an address to the IP Switch Gateway so that the host can communicate with the GIGAswitch/IP through a browser. For 10 Mbps Ethernet, type the following command, substituting your actual IP address for the example address (*10.1.3.1*) and the actual netmask length for the example netmask (*24*):

```
ifconfig eth-s2p1c0 10.1.3.1/24 up
```

or

If 100 Mbps is desired, use the following command instead:

```
ifconfig eth-s2p1c0 10.1.3.1/24 link2 up
```

3. Go to each IP Switch Gateway in succession and verify that the IP address and netmask were set up successfully:

```
ifconfig -a
```

The following example output illustrates the `ifconfig -a` command from IP Switch Gateway 3:

```
lo0: flags=8009<UP,LOOPBACK,MULTICAST> mtu 16384
    inet 127.0.0.1/8
ppp0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
```

```
s10: flags=c010<POINTOPOINT,LINK2,MULTICAST> mtu 552
tun0: flags=10<POINTOPOINT> mtu 1500
eth-s2p1c0: flags=ca63<UP,BROADCAST,NOTRAILERS,RUNNING,ALLMULTI,
SIMPLEX,LINK2,MULTICAST> mtu 1500
    inet 10.1.3.1/24 broadcast 10.1.3.255
    ether 00:00:c0:16:82:bf
atm-s1p1c0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.5/30 --> 10.1.1.6
    fddi-
s2p1c0: flags=8a63<UP,BROADCAST,NOTRAILERS,RUNNING,ALLMULTI,
SIMPLEX,MULTICAST> mtu 4470
```

Examine the output to confirm that the IP address and netmask for `eth-s2p1c0` are the values you intended.

4. Establish routing to the IP Switch Gateway so that the browser can communicate with the Configuration Tool. Use the following command, substituting for the example address (*10.1.1.8*) the address of the host machine you are typing on:

```
route add default 10.1.1.8
```

5. From a host, ping each IP Switch Gateway to make sure it is reachable:

```
ping 10.1.3.1
```

If the command is successful, a message is displayed once a second. If it is unsuccessful, either no messages are displayed or an error message is displayed. Type CTRL-C to stop ping.

## Using the Netscape Navigator Browser

To configure your network with the Netscape Navigator Browser:

1. Start up the Netscape Navigator browser on a host machine that can communicate with the IP Switch Gateway, and that is running a windowing system that can display the browser.
2. Select the OPEN button at the top of the Netscape window by clicking the left mouse button. (From here on, the term clicking refers to clicking the left mouse button unless otherwise specified.) Type the Uniform Resource Locator (URL) of the `eth-s2p1c0` computer port on the GIGAswitch/IP or IP Switch Gateway to be configured and press RETURN:

```
10.1.3.1
```

This displays the clearVISN IP Switch Manager Main Menu.

3. Click on the CONFIGURATION TOOL icon to activate the Configuration Tool. This displays a dialog box that requests a username and password.
4. Type this User ID:  

```
admin
```
5. Enter the admin password and click on OK.



This displays the CONFIGURATION MENU. When the CONFIGURATION MENU appears, only the first item can be chosen: CREATE OR MODIFY CONFIGURATION FILE.

6. Select CREATE OR MODIFY CONFIGURATION FILE by clicking on it.

If you are not already familiar with Netscape, the use of highlighting (text in another color) may be confusing. The highlighted items are the menu items that currently can be chosen. Items that can be chosen are called active items.

Click on any active item to follow the link.

---

### Note

Do not use the BACK button at the top of the Netscape window to go back to a link you have followed. Select the HOME or MENU button at the bottom of the view.

---

## Configuring the Network with the Configuration Tool

This section describes the process of creating a configuration file, regardless of which browser is used. When creating the configuration file, you choose interfaces and routing protocols, and generate files used to configure the system when it restarts. In this section, the term select is used instead of the following browser-specific instructions:

- Lynx: positioning the cursor on
- Netscape: clicking on

---

### Note

This procedure assumes that you have started up the browser of your choice, logged in to the Configuration Tool as admin, and selected CREATE OR MODIFY CONFIGURATION FILE from the CONFIGURATION MENU. When you begin this procedure, you should be looking at the CONFIGURATION FILE MANAGER view.

---

To create a configuration file, complete the following steps:

1. Indicate that you wish to edit a new configuration file.
2. Type the name for your configuration file.  
The suggested convention is to use the .conf name suffix to indicate the type of the file.
3. Select OK.
4. Return to the CONFIGURATION MENU.

Now that you have defined the configuration file, you will configure the interfaces.

1. Select CONFIGURE INTERFACES.

2. Select `CREATE`. This displays the Interfaces view.
3. Using the table you created in Sample Network Design on page 6, configure an interface as follows:
  - a. Select a logical name from the menu.
  - b. Enter the IP address for the selected interface.
  - c. Enter the length of the network mask from the subnet that this interface is on.

Refer to Network Numbers and Network Masks on page 4 for more information about mask lengths.
  - d. Select any number of protocols you want to run on this interface from the following:
    - OSPF (Open Shortest Path First)
    - RIP (Routing Information Protocol)
    - DVMRP (Distance Vector Multicast Routing Protocol)
    - Router Discovery Server

Select `HELP` at the bottom of the view for detailed descriptions and guidelines.

4. Select `OK`.
5. If you do not need to set specific parameters for the network protocols, select `BASIC`.

or

If you need to set specific parameters for OSPF, RIP, DVMRP, or Router Discovery Server, then select the `ADVANCED` option.

For stub networks, you need to select `ADVERTISE TO OSPF` from the `ADVANCED` menu. You need to select the `ADVANCED` option to run the Ethernet at 100 Mbps, or to run full duplex for FDDI. Select `HELP` at the bottom of the view for additional assistance with the `ADVANCED` menu.

6. Select `OK` to write the changes to your `configuration file`.
7. If you have additional interfaces to configure:
  - a. Select `EDIT ANOTHER INTERFACE`.
  - b. Select `CREATE` and then `OK`.
  - c. Repeat steps 3 through 6 until all of your interfaces are configured.
8. When you are ready to apply this `configuration file` to your system, select `RETURN TO CONFIGURATION MENU`.
9. Select `GENERATE FILES FOR NEXT BOOT`.
10. Select `INSTALL`.

Messages are displayed indicating the files that were generated.

11. Select RETURN TO CONFIGURATION MENU.
12. Select APPLY CONFIGURATION CHANGES.
13. Select APPLY CHANGES AND THEN REBOOT.
14. Confirm your selection.  
The system restarts, using the files you just created.

## Verifying the Configuration

This section describes how to verify that the configuration described with the Configuration Tool is accurate and working on the GIGAswitch/IP or the IP Switch Gateway.

This section provides a step-by-step approach to testing and verifying a given configuration. You can follow all the steps in order to test and verify your configuration, or you can jump directly to step 4 to first see whether the network is functioning.

### Step 1: Check that the DIGITAL GIGAswitch/IP Switch Controller and DIGITAL GIGAswitch/ATM Have Synchronized

If you are configuring a GIGAswitch/IP, you need to verify that the GIGAswitch/IP Switch Controller and the GIGAswitch/ATM have synchronized. When the GIGAswitch/IP Switch Controller and the GIGAswitch/ATM synchronize, the GIGAswitch/IP Switch Controller creates interfaces corresponding to the ports on the GIGAswitch/ATM. The interfaces allow the GIGAswitch/IP Switch Controller and the GIGAswitch/ATM to communicate.

To get a list of the available interfaces, log in to the GIGAswitch/IP Switch Controller (through the console or using telnet), and use the following command:

```
ifconfig -a
```

The following is typical output from `ifconfig -a`:

```
lo0: flags=8009<UP,LOOPBACK,MULTICAST> mtu 16384
    inet 127.0.0.1/8
ppp0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
sl0: flags=c010<POINTOPOINT,LINK2,MULTICAST> mtu 552
tun0: flags=10<POINTOPOINT> mtu 1500
atm-s1plc0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s1: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s7: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu
1500
    inet 10.1.1.9/30 --> 10.1.1.10
atm-s1plc0s6: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu
1500
    inet 10.1.1.1/30 --> 10.1.1.2
atm-s1plc0s5: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
```

```
atm-s1p1c0s4: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1p1c0s3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu
1500
    inet 10.1.1.6/30 --> 10.1.1.5
atm-s1p1c0s2: flags=8051<POINTOPOINT,RUNNING,MULTICAST> mtu
1500
```

If the GIGAswitch/IP Switch Controller and the GIGAswitch/ATM are synchronized, then interfaces appear in the interface list on the GIGAswitch/IP Switch Controller with the form:

```
atm-sxp1c0syy
```

where *X* corresponds to the ATM interface number on the GIGAswitch/IP Switch Controller (*X* is typically 0 on most customer installations) and *YY* corresponds to the port numbers on the GIGAswitch/ATM.<sup>1</sup> For more information about GIGAswitch/ATM port number assignment policies, read the GIGAswitch/ATM firmware release notes.

If the interfaces you expect are not listed, refer to Chapter 5, Troubleshooting.

For more information on reading `ifconfig` output, refer to Interpreting `ifconfig` Output on page 23.

## Step 2: Verify Interface Configuration

This verifies that the interfaces are configured correctly. To verify the interface configuration, use the following command to get a list of all interfaces including their current status, configured IP address, and the mask length of the interface:

```
ifconfig -a
```

Compare the output for `ifconfig` with the desired configuration to ensure that they match. For each configured interface, verify the following items:

- Is the interface UP flag set?
- Does the interface have the correct IP address?
- Does the interface have the correct network mask length?

If any of these items is not correct, then refer to Chapter 5, Troubleshooting.

## Step 3: Check Whether Remote Interface Addresses Have Been Established

In order for the ATM interfaces to transmit IP packets across a link, the two ends of the link must synchronize with the IP Flow Management Protocol (IFMP). This step determines whether the synchronization has occurred.

If the ATM interfaces have been configured as point-to-point interfaces with only the local address configured, initially the remote address is 0.0.0.0. When the

---

1. As an alternative to the `ifconfig` command, the Configuration Tool or the Monitor Tool can be used to get a list of available interfaces. Refer to the online documentation for these tools for more information.

IFMP synchronization occurs, the remote address is modified to contain the address of the remote side of the link.

The remote address of the point-to-point link can be examined using the `ifconfig` command to produce a list of interfaces and their configurations:

```
ifconfig -a
```

If the remote side is 0.0.0.0, then the two sides of the ATM link have not synchronized. If the remote address is nonzero, then the IFMP has synchronized.

If the interfaces do not synchronize, refer to Chapter 5, Troubleshooting.

## Step 4: Check That Neighbors Are Reachable

After interfaces are configured, verify that IP packets can reach machines on the directly attached networks. Run this test for all configured interfaces.

To test the network, use the `ping` command. The `ping` command transmits an ICMP echo request to a named machine and listens for an ICMP echo reply. This exercises the IP layer. If the `ping` command is successful, there is IP network connectivity between the local and remote devices.

To run `ping` over an interface, you need the IP address of another machine connected to the interface's network. For ATM interfaces, that address is the remote side of the point-to-point link. For other interfaces such as FDDI or Ethernet, this can be any machine attached to the subnet.

The following is an example of the `ping` command:

```
# ping 10.1.2.4
PING 10.1.2.4 (10.1.2.4): 56 data bytes
64 bytes from 10.1.2.4: icmp_seq=0 ttl=255 time=0.856 ms
64 bytes from 10.1.2.4: icmp_seq=1 ttl=255 time=0.821 ms
64 bytes from 10.1.2.4: icmp_seq=2 ttl=255 time=1.009 ms
64 bytes from 10.1.2.4: icmp_seq=3 ttl=255 time=0.832 ms
64 bytes from 10.1.2.4: icmp_seq=4 ttl=255 time=0.822 ms
64 bytes from 10.1.2.4: icmp_seq=5 ttl=255 time=0.822 ms
64 bytes from 10.1.2.4: icmp_seq=6 ttl=255 time=0.824 ms
64 bytes from 10.1.2.4: icmp_seq=7 ttl=255 time=0.842 ms
```

If the command is successful, a message is displayed once a second. If it is unsuccessful, either no messages are displayed or an error message is displayed. If the interfaces do not synchronize, refer to Chapter 5, Troubleshooting.

To stop the `ping` command, type CTRL-C.

## Step 5: Examine the Unicast Routing Tables

This step examines the local unicast routing table to determine whether the routing is correct. The local routing table is displayed using the `netstat` command as follows:

```
netstat -rn
```

This displays the routing table. The following is a typical routing table:

Routing tables

Internet:

Destination	Gateway	Flags	Refs	Use	Netif	Expire
default	10.1.1.9	UGc	0	0	atm-s1p1c0	
127	127.0.0.1	URc	0	0	lo0	
127.0.0.1	127.0.0.1	UH	0	25	lo0	
10.1.1.1	10.1.1.9	UGH	0	0	atm-s1p1c0	
10.1.1.2	10.1.1.9	UGH	0	0	atm-s1p1c0	
10.1.1.5	10.1.1.9	UGH	0	0	atm-s1p1c0	
10.1.1.6	10.1.1.9	UGH	0	0	atm-s1p1c0	
10.1.1.9	10.1.1.10	UGH	0	0	atm-s1p1c0	
10.1.1.10	10.1.1.9	UGH	0	0	atm-s1p1c0	
10.1.2	10.1.1.9	UGc	0	0	atm-s1p1c0	
10.1.3	10.1.1.9	UGc	0	0	atm-s1p1c0	
10.1.4	10.1.1.9	UGc	0	0	atm-s1p1c0	
10.1.5	10.1.1.9	UGc	0	1	atm-s1p1c0	
10.1.6	10.1.6.1	UGc	3	11339	eth-s2p1c0	
10.1.6.11	0:0:c0:1f:82:bf	UHLW	12	0	eth-s2p1c0	64
10.1.6.32	0:c0:95:f8:1:5e	UHLW	0	0	eth-s2p1c0	20
10.1.6.212	0:80:3f:f4:7:40	UHLW	6	1801520	eth-s2p1c0	1018

The fields reported by netstat are:

**Destination**

The destination network, as described by the address and network mask. All packets matching this address in the mask bits of this route, but not any route with a higher number of bits set, exit this interface towards the next hop. A route to an individual host has all 32 bits of the destination mask set.

**IP Switch Gateway**

The next-hop IP router to use when getting to this destination.

**Flags**

Any flags listed are turned on. Definitions for these flags are as follows:

1	RTF_PROTO2	Protocol specific routing flag #1
2	RTF_PROTO1	Protocol specific routing flag #2
3	RTF_PROTO3	Protocol specific routing flag #3
B	RTF_BLACKHOLE	Just discard pkts (during updates)
C	RTF_CLONING	Generate new routes on use
c	RTF_PRCLONING	Protocol-specified generate new routes on use
D	RTF_DYNAMIC	Created dynamically (by redirect)
G	RTF_GATEWAY	Destination requires forwarding by intermediary
H	RTF_HOST	Host entry (net otherwise)
L	RTF_LLINFO	Valid protocol to link address translation
M	RTF_MODIFIED	Modified dynamically (by redirect)
R	RTF_REJECT	Host or net unreachable
S	RTF_STATIC	Manually added
U	RTF_UP	Route usable
W	RTF_WASCLONED	Route was generated as a result of cloning

X      RTF\_XRESOLVE    External daemon translates proto to  
link address

**Ref**

Number of current references to the route.

**Use**

Number of times the route has to be used.

**Netif**

The output interface associated with the route.

**Expire**

Time (in seconds) until this routing entry is removed from the routing table.

Compare the output from `netstat` with the desired configuration to ensure that they match. For each configured interface, verify the following items:

- Do routes exist to all of the directly attached subnets?
- Do the routes have the appropriate masks?
- If appropriate, have routes to any nonlocal subnets been established and are they correct?

If there are routing problems, proceed to Chapter 5, Troubleshooting.

If the routes are correct, you should attempt to reach machines that are not on directly attached networks. This can be done by using the `ping` command described in Step 4: Check That Neighbors Are Reachable. If this fails, refer to Chapter 5, Troubleshooting.

After successfully completing the installation and configuration verification, your network is ready to use.

## Backing Up Files

When you are satisfied with your configuration, Digital Equipment Corporation recommends making backup copies of all your configuration (`.conf`) files on a floppy diskette for easy restoration in the event of a disk crash. To facilitate this, we provide a utility that simplifies the process of making backup configuration files. This program copies your configuration files to a floppy diskette in `gzip tar` format. To run the `ipsbackup` script to back up your files, enter the following command at the console connected to the node you are backing up:

```
ipsbackup rfd0
```

where `rfd0` is the name of your floppy drive. When the script finishes, your backup is complete for that node. This must be done on each node in the network.

Back up your configuration files each time you make changes to your interfaces or upgrade the GIGAswitch/IP software.

## Restoring a Configuration File from a Backup

To restore the `configuration` file from a backup, complete the following steps:

1. Access the Configuration Tool main menu.
2. In the SYSTEM CONFIGURATION menu click on SECURITY AND ACCESS CONTROL to access the SECURITY page.
3. In the Allow `ftp` access field, click on the YES radio button.
4. Click APPLY.  
The Apply Successful message appears.
5. At a remote console, start an `ftp` session.
6. Use an IP address of one of the interfaces to connect to the IP Switch device.
7. At the login prompt, enter either `admin` or `monitor` followed by the appropriate password.
8. Set the directory path to the configuration database, as in the following example:  

```
cd /usr/local/config/db
```
9. Use the `ftp put` command to load the files you want to restore.

### Accessing the Configuration File

1. Check to ensure that the `configuration` file is available:
  - a. In the Netscape browser, click on the CONFIGURATION TOOL icon to select the Configuration Tool.
  - b. In the CONFIGURATION TOOL menu, click the MANAGE CONFIGURATION SETS menu to show the CONFIGURATION DATABASE MANAGEMENT view. This view displays the `configuration` file names currently available as well as the `configuration` file name for the currently active session.  
Figure 2-6 shows the CONFIGURATION DATABASE MANAGEMENT view.
2. Click the radio button which corresponds to the `configuration` file you want to use.



Figure 2-6: Configuration Database Management View

clearVISN

Home Top Up Help On Doc

---

## Configuration database management for gigaswitch.digital.com

---

Current configuration database: **initial**

Databases currently available

- initial

Save current state to new config database

[Delete Configuration Databases](#)

---

**Apply**

## Interpreting ifconfig Output

The following is typical output from `ifconfig -a`:

```

lo0: flags=8009<UP,LOOPBACK,MULTICAST> mtu 16384
inet 127.0.0.1/8
ppp0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
sl0: flags=c010<POINTOPOINT,LINK2,MULTICAST> mtu 552
tun0: flags=10<POINTOPOINT> mtu 1500
atm-s1plc0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s1: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s7: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu
1500
        inet 10.1.1.9/30 --> 10.1.1.10
atm-s1plc0s6: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu
1500
        inet 10.1.1.1/30 --> 10.1.1.2
atm-s1plc0s5: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s4: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu
1500
        inet 10.1.1.6/30 --> 10.1.1.5
atm-s1plc0s2: flags=8051<POINTOPOINT,RUNNING,MULTICAST> mtu
1500

```

The first line contains the interface name, the interface flag, and the maximum transmission unit (MTU). The flag field provides the hexadecimal representation

of the flags (8009 in the example) and a text description of the flags (delimited by < and >).

Some of the common flags are:

- **UP**: The interface is configured as able to send and receive packets.
- **BROADCAST**: Indicates a broadcast capable interface (**BROADCAST** and **POINTOPOINT** may not both be in effect for the same interface).
- **MULTICAST**: Indicates a multicast-capable interface.
- **POINTOPOINT**: Indicates a point-to-point capable interface (**POINTOPOINT** and **BROADCAST** may not both be in effect for the same interface).
- **RUNNING**: The interface is capable of sending packets.
- **ALLMULTI**: This interface is receiving all multicast packets on the link.
- **LINK1**: On ethernet or FDDI interfaces, runs full duplex. If not set, then the interface runs half duplex.
- **LINK2**: On Ethernet interfaces, indicates that the link is running at 100 Mbps. If **LINK2** is not listed, the link is running at 10 Mbps.

The `mtu` is the largest packet size that can be transmitted over this network link.

If the interface is configured, the next line contains the address family and the address for this interface. On **DIGITAL** products the address family is `inet`. The address has the form:

```
127.0.0.1/8
```

where the numbers before the / denote the IP address for the interface, and the number after the / denotes the network mask length.

If the link is a point-to-point network, then the remote IP address follows the local IP address.

If the link is a broadcast network, then the broadcast address follows the IP address.

If the interface is an Ethernet or FDDI interface, the Medium Access Control (MAC) address of the interface is given on the next line.

# Example Configuration

---

## Overview

This chapter walks you through configuring the sample network introduced in Chapter 2 *Installing and Configuring a Network*. Two sets of instructions for configuring the sample network are included:

- Configuration Overview on page 25 describes the 12 main steps required to configure this network.
- Configuring the Sample Network with clearVISN IP Switch Manager on page 28 walks you through all the actions required to complete these 12 steps using clearVISN IP Switch Manager.

Figure 3-1 and Figure 3-2 are two different depictions of the sample network that is configured in this chapter. (They are repeats of Figure 2-1 and Figure 2-2, included here for convenience.)

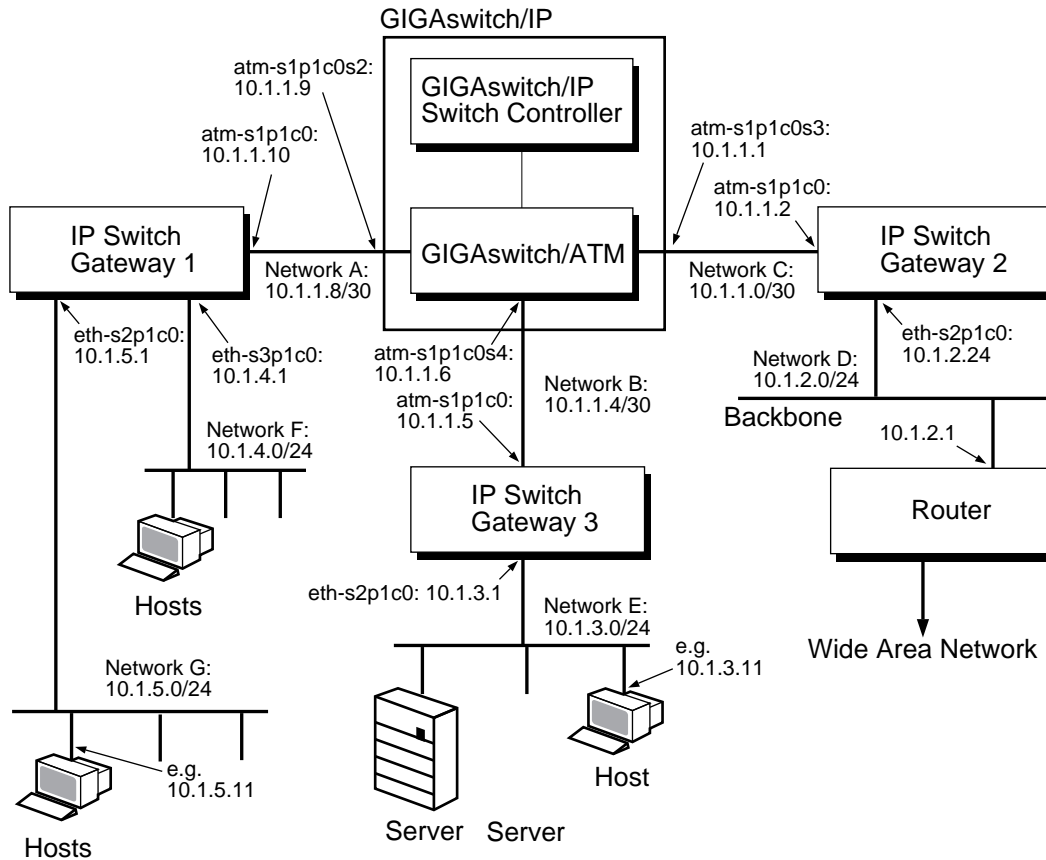
## Configuration Overview

To configure a network, you must configure each node in the network. To configure a node using the clearVISN IP Switch Manager Configuration Tool, you first need network connectivity to that node. You get this by connecting a terminal to the node's serial port and configuring the node for basic access.

Nodes must be configured in a particular order. The first node configured is, by definition, the root node. Configuring this node establishes network connectivity between the node and a host machine running a Web browser.

The leaf nodes at the ends of the branches farthest from the root node must be configured before the nodes closer to the root. However, you cannot access a node to configure it until all the nodes in between it and the root node have connectivity.

Figure 3-1: An Example Network



LKG-10302-96F

To get around this, you first partially configure the nodes between the root and the leaf nodes. (This is sometimes called configuring a Stub Network.) After the leaf nodes have been configured, you return to the branch nodes, reconfiguring them one by one to route OSPF, if needed. You continue working closer to the root until all nodes are configured. The main steps required to configure the example network shown in Figure 3-1 are as follows:

1. Start with a host machine that has the Netscape Navigator 2.0 (or later) browser loaded on it. Make sure you know the following information about this host machine:
  - Its IP address
  - The IP address of its default IP Switch Gateway
 Make sure that you have serial access from the host machine to all the machines (IP Switch Gateways and GIGAswitch/IP Switch Controllers) that you plan to configure.
2. Connect a terminal to the serial port of IP Switch Gateway 1, and establish sufficient configuration to allow the host machine and Web browser to access IP Switch Gateway 1.
3. Use the browser (on the host machine) to connect to IP Switch Gateway 1, and configure this IP Switch Gateway.

Figure 3-2: Sample Network Design Table

Network Number	Mask Length	From			To			Uses OSPF ?	Uses RIP?	Uses DVMRP?	Uses Router Disc.?
		Where	Logical Name	IP Address	Where	Logical Name	IP Address				
10.1.1.8	30	GIGAswitch/ IP	atm- s1p1c0s2	10.1.1.9	Gateway 1	atm- s1p1c0	10.1.1.10	Yes	Yes		
10.1.1.0	30	GIGAswitch/ IP	atm- s1p1c0s3	10.1.1.1	Gateway 2	atm- s1p1c0	10.1.1.2	Yes	Yes		
10.1.1.4	30	GIGAswitch/ IP	atm- s1p1c0s4	10.1.1.6	Gateway 3	atm- s1p1c0	10.1.1.5	Yes	Yes		
10.1.2.0	24	Gateway 2	eth- s2p1c0	10.1.2.24	Network D			Yes	Yes		
10.1.3.0	24	Gateway 3	eth- s2p1c0	10.1.3.1	Network E			Yes	Yes		
10.1.4.0	24	Gateway 1	eth- s3p1c0	10.1.4.1	Network F			Yes	Yes		
10.1.5.0	24	Gateway 1	eth- s2p1c0	10.1.5.1	Network G			Yes	Yes		

4. Connect a terminal to the serial port of GIGAswitch/IP Switch Controller 1, and establish sufficient configuration to allow the host machine and Web browser to access the GIGAswitch/IP Switch Controller through the IP Switch Gateway you just configured.
5. Use the browser (on the host machine) to connect to the GIGAswitch/IP Switch Controller and configure it.
6. Use the browser (on the host machine) to reconnect to IP Switch Gateway 1 and modify its configuration.
7. Connect a terminal to the serial port of IP Switch Gateway 3, and establish sufficient configuration to allow the host machine and Web browser to access IP Switch Gateway 3 through the IP Switch Gateway and GIGAswitch/IP Switch Controller you just configured.
8. Use the browser (on the host machine) to connect to IP Switch Gateway 3 and configure it.
9. Connect a terminal to the serial port of IP Switch Gateway 2, and establish sufficient configuration to allow the host machine and Web browser to access IP Switch Gateway 2 through IP Switch Gateway 1 and the GIGAswitch/IP Switch Controller you previously configured.
10. Use the browser (on the host machine) to connect to IP Switch Gateway 2 and configure it.
11. Use the browser (on the host machine) to reconnect to the GIGAswitch/IP Switch Controller and modify its configuration.
12. Test your network by pinging from node to node in enough possible combinations to demonstrate that all nodes are configured correctly.

## Configuring the Sample Network with clearVISN IP Switch Manager

This script assumes that you are using the Netscape Navigator 2.0 (or later) graphical Web browser. If you are using another browser, some aspects of the session may vary from this script. We do not attempt to describe the behavior of other browsers in this script. The first time a Netscape action is used it is explained; thereafter it is referred to by name only.

Before beginning this script, all the hardware must be connected as described in Chapter 2, Installing DIGITAL GIGAswitch/IP Products of the *DIGITAL GIGAswitch/IP Solution for ATM Products Reference*. All references to IP Switch Gateways and GIGAswitch/IP Switch Controllers correspond to those shown in Figure 3-1.

1. Start with a host machine that has the Netscape Navigator 2.0 (or later) browser loaded on it. Make sure you know the following information about this host machine:

- Its IP address
- The IP address of its default IP Switch Gateway

Make sure that you have serial access from the host machine to all the machines (IP Switch Gateways and GIGAswitch IP Switch Controllers) that you plan to configure.

2. Connect a terminal to the serial port of IP Switch Gateway 1, and establish sufficient configuration to allow the host machine and Web browser to access IP Switch Gateway 1. Follow these steps:

- a. Type `root` as the login name:

```
Login: root
```

- b. Enter passwords for `root`, `admin`, and `monitor` as prompted.

- c. Temporarily assign an address to the IP Switch Gateway so that the host can communicate with the IP Switch Gateway through a browser. For 10 Mbps Ethernet, type the following command:

```
ifconfig eth-s2p1c0 10.1.3.1/24 up
```

or

For a 100 Mbps Ethernet, use the following command instead:

```
ifconfig eth-s2p1c0 10.1.3.1/24 link2 up
```

- d. Verify that the IP address and network mask length were set up successfully:

```
ifconfig -a
```

The following example output illustrates the `ifconfig -a` command from IP Switch Gateway 3 (from Figure 3-1):

```
lo0: flags=8009<UP,LOOPBACK,MULTICAST> mtu 16384
    inet 127.0.0.1/8
ppp0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
sl0: flags=c010<POINTOPOINT,LINK2,MULTICAST> mtu 552
tun0: flags=10<POINTOPOINT> mtu 1500
eth-s2p1c0: flags=ca63<UP,BROADCAST,NOTRAILERS,RUNNING,
    ALLMULTI,SIMPLEX,LINK2,MULTICAST> mtu 1500
    inet 10.1.3.1/24 broadcast 10.1.3.255
    ether 00:00:c0:16:82:bf
```

Examine the output to confirm that the IP address and network mask length for `eth-s2p1c0` are the values you intended.

- e. Ping the IP Switch Gateway from the host machine to make sure it is reachable:

```
ping 10.1.3.1
```

If the command is successful, a message is displayed once a second. If it is unsuccessful, either no messages are displayed or an error message is displayed. Type CTRL-C to stop ping.

3. Use the browser (on the host machine) to connect to IP Switch Gateway 1, and configure this IP Switch Gateway. Follow these steps:
  - a. Start the Netscape browser on the host.
  - b. Type the IP address of the IP Switch Gateway's `eth-s2p1c0` interface (the same address you used in step 2) into the Location field and press RETURN:  
`10.1.5.1`
  - c. Select the Configuration Tool by clicking the left mouse button on the CONFIGURATION TOOL icon. (From here on, the term clicking refers to clicking the left mouse button unless otherwise specified.)

A dialog box appears, prompting you for a USER ID and PASSWORD. The first time you access a node from the browser it asks for a USER ID and PASSWORD; after that you can return to that node without providing a USER ID and PASSWORD. If you exit and restart the browser, you need to provide a USER ID and PASSWORD again.
  - d. Enter `admin` as the USER ID, provide the PASSWORD you defined in step 2, and click on OK.

This displays the CONFIGURATION MENU. When the CONFIGURATION MENU appears, only the first item can be chosen: CREATE OR MODIFY CONFIGURATION FILE.

---

### Note

In step 2, you assigned a temporary IP address to the IP Switch Gateway, to allow you to get to the point where you could run Configuration Tool on the IP Switch Gateway. Now you will use Configuration Tool to define configuration files that will automatically configure the IP Switch Gateway every time it starts.

---

- e. Create a configuration file by following these steps:
  - Select CREATE OR MODIFY CONFIGURATION FILES from the CONFIGURATION menu.

The CONFIGURATION FILE MANAGER view is displayed.
  - Click on NEW and then on OK to edit a new configuration file.
  - Type the filename for your configuration file and click on OK.

The suggested convention is to use `.conf` as the filename suffix.
  - Scroll to the bottom of the screen (if necessary) and click on OK.
- f. Configure the `eth-s2p1c0` interface by following these steps:
  - Click on CONFIGURE INTERFACES.
  - Click on CREATE. This displays the CREATE INTERFACE view.



- Using the table you created in Sample Network Design on page 6, configure the interface between the host machine and the IP Switch Gateway as follows:
  - Select `eth-s2p1c0` from the menu.
  - Enter the IP address for `eth-s2p1c0`:  
`10.1.5.1`
  - Enter the length of the network mask for `eth-s2p1c0`:  
`24`

Refer to Network Numbers and Network Masks on page 4 for more information about mask lengths.

- Enable OSPF and DVMRP (Multicast) by clicking in the check boxes next to them.
- Select the `ADVANCED` option at the bottom of the view.
- Select `OK`. Because you selected the `ADVANCED` option, this now displays the `ADVANCED CREATE INTERFACE` view.
- Under `INTERFACE OPTIONAL DATA`, select `100 Mbit`, then click on `OK`.

g. Configure the `atm-s1p1c0` interface by following these steps:

- Click on `EDIT ANOTHER INTERFACE`.

Using the table you created in Sample Network Design on page 6, next you will configure the interface between the IP Switch Gateway and the GIGAswitch/IP Switch Controller.

- Select `atm-s1p1c0` from the menu.
- Enter the IP address for `atm-s1p1c0`:  
`10.1.1.10`
- Enter the length of the network mask for `atm-s1p1c0`:  
`30`
- Select the `Advanced` option at the bottom of the view and click on `OK`.
- Under `INTERFACE OPTIONAL DATA`, enter the `Point-to-Point Remote IP Address`:  
`10.1.1.9`

h. Configure the `eth-s3p1c0` interface by following these steps:

- Click on `EDIT ANOTHER INTERFACE`.

Using the table you created in Sample Network Design on page 6, next you will configure the interface between IP Switch Gateway 1 and Network F, which in turn is connected to the router.

- Select `eth-s3p1c0` from the menu.
- Enter the IP address for `eth-s3p1c0`:  
`10.1.4.1`

- Enter the length of the network mask for `eth-s3p1c0`:  
24
  - Enable OSPF and DVMRP (Multicast).
  - Select the Advanced option at the bottom of the view and click on OK.
  - Under `INTERFACE OPTIONAL DATA`, select 100 Mbit, then click on OK.  
Next you are prompted to confirm that you want to write the changes to the `configuration file`.
  - Click on OK to confirm writing the changes to the `configuration file`.
- i. Set global parameters for this IP Switch Gateway by following these steps:
- Select `RETURN TO CONFIGURATION MENU`.
  - Select `SET OSPF AND RIP GLOBAL PARAMETERS`.
  - Select `ADVERTISE INTERFACES TO OSPF` and click on OK to confirm writing the changes to the `configuration file`.
- j. Generate the files you just defined by following these steps:
- Select `RETURN TO CONFIGURATION MENU`.
  - Select `GENERATE FILES FOR NEXT BOOT`.
  - Click on OK to confirm the installation.  
Messages are displayed indicating the files that were generated.
- k. Apply the files you just generated by following these steps:
- Select `RETURN TO CONFIGURATION MENU`.
  - Select `APPLY CONFIGURATION CHANGES`.
  - Select `APPLY CHANGES AND THEN REBOOT`.  
You are asked to confirm the request to reboot.
  - Confirm by clicking on `YES`.  
The system reboots using the files you just created.  
Wait for the IP Switch Gateway to reboot.
4. Connect a terminal to the serial port of GIGAswitch/IP Switch Controller 1, and establish sufficient configuration to allow the host machine and Web browser to access the GIGAswitch/IP Switch Controller through the IP Switch Gateway you just configured. Follow the steps outlined in step 2, substituting these commands:
- a. Temporarily assign an address to the GIGAswitch/IP Switch Controller:  
`ifconfig eth-s2p1c0 10.1.1.9/30 10.1.1.10 up`
  - b. Enable IP Switch Gateway 1 to communicate with the GIGAswitch/IP Switch Controller:  
`route add default 10.1.1.10`

- c. Verify that the IP address and netmask were set up successfully:  
`ifconfig -a`
- d. Ping the GIGAswitch/IP Switch Controller to make sure it is reachable:  
`ping 10.1.1.9`

---

### Note

In step 4, you assigned a temporary IP address to the GIGAswitch/IP Switch Controller to allow you to get to the point where you could run Configuration Tool on the GIGAswitch/IP Switch Controller. Now you will use Configuration Tool to define `configuration` files that will automatically configure the GIGAswitch/IP Switch Controller every time it starts.

---

5. Use the browser (on the host machine) to connect to the GIGAswitch/IP Switch Controller and configure it.
  - a. Type the IP address of the GIGAswitch/IP Switch Controller's `atm-s1p1c0s2` interface (the same address you used in step 4) into the Location field and press RETURN:  
`10.1.1.9`
  - b. In step 3 you learned how to create a `configuration` file with the Configuration Tool. To configure the GIGAswitch/IP Switch Controller, create a `configuration` file with the Configuration Tool that contains the following information:
    - The `atm-s1p1c0s2` interface:
      - IP address:  
`10.1.1.9`
      - Network mask length:  
`30`
      - Enable OSPF and DVMRP (Multicast).
      - Point-to-Point Remote IP Address:  
`10.1.1.10`
    - The `atm-s1p1c0s4` interface (the interface between the GIGAswitch/IP Switch Controller and IP Switch Gateway 3):
      - IP address:  
`10.1.1.6`
      - Network mask length:  
`30`
      - Point-to-Point Remote IP Address:  
`10.1.1.5`
    - The `atm-s1p1c0s3` interface:
      - IP address:  
`10.1.1.1`

- Network mask length:  
30
  - Point-to-Point Remote IP Address:  
10.1.1.2
  - Advertise Interfaces to OSPF.
- c. Confirm writing the changes to the `configuration` file.
  - d. Return to the CONFIGURATION MENU.
  - e. Generate files for the next boot.
  - f. Apply the configuration changes and reboot.

---

**Note**

In step 3, you configured the IP Switch Gateway just enough to allow you to get to the point where you could run Configuration Tool on the GIGAswitch/IP Switch Controller. Now you will use Configuration Tool to enable OSPF on the IP Switch Gateway.

6. Use the browser (on the host machine) to reconnect to IP Switch Gateway 1 and modify its configuration. Follow these steps:
  - a. Type the IP address of the IP Switch Gateway's `eth-s2p1c0` interface into the Location field and press RETURN:  
10.1.5.1
  - b. Modify the `configuration` file with the Configuration Tool so that it contains the following information:
    - The `atm-s1p1c0` interface:
      - Enable OSPF.
    - Deselect Advertise Interfaces to OSPF.

---

**Note**

For an interface that has OSPF enabled, Advertise Interfaces to OSPF should not be selected.

- c. Confirm writing the changes to the `configuration` file.
  - d. Return to the CONFIGURATION MENU.
  - e. Generate files for the next boot.
  - f. Apply the configuration changes and reboot.
7. Connect a terminal to the serial port of IP Switch Gateway 3, and establish sufficient configuration to allow the host machine and Web browser to access IP Switch Gateway 3 through the IP Switch Gateway and GIGAswitch/IP Switch Controller you just configured. Follow the steps outlined in step 2, substituting these commands:

- a. Temporarily assign an address to the GIGAswitch/IP Switch Controller:  
`ifconfig atm-s1p1c0 10.1.1.5/30 10.1.1.6 up`
- b. Enable IP Switch Gateway 1 to communicate with the GIGAswitch/IP Switch Controller:  
`route add default 10.1.1.6`
- c. Verify that the IP address and netmask were set up successfully:  
`ifconfig -a`
- d. Ping IP Switch Gateway 3 to make sure it is reachable:  
`ping 10.1.1.5`

---

### Note

In step 7, you assigned a temporary IP address to IP Switch Gateway 3, to allow you to get to the point where you could run Configuration Tool on the IP Switch Gateway. Now you will use Configuration Tool to define configuration files that will automatically configure IP Switch Gateway 3 every time it starts.

---

8. Use the browser (on the host machine) to connect to IP Switch Gateway 3 and configure it. Follow these steps:
  - a. Type the IP address of the IP Switch Gateway's atm-s1p1c0 interface (the same address you used in step 7) into the Location field and press RETURN:  
`10.1.1.5`
  - b. In step 3 you learned how to create a configuration file with the Configuration Tool. To configure IP Switch Gateway 3, create a configuration file with the Configuration Tool that contains the following information:
    - The atm-s1p1c0 interface:
      - IP address:  
`10.1.1.5`
      - Network mask length:  
`30`
      - Enable OSPF and DVMRP (Multicast).
      - Point-to-Point Remote IP Address:  
`10.1.1.6`
    - The eth-s2p1c0 interface:
      - IP address:  
`10.1.3.1`
      - Network mask length:  
`24`
      - Enable DVMRP (Multicast).
      - Under Interface Optional Data, select 100 Mbit

- Advertise Interfaces to OSPF.
  - c. Confirm writing the changes to the `configuration` file.
  - d. Return to the CONFIGURATION MENU.
  - e. Generate files for the next boot.
  - f. Apply the configuration changes and reboot.
9. Connect a terminal to the serial port of IP Switch Gateway 2, and establish sufficient configuration to allow the host machine and Web browser to access IP Switch Gateway 2 through IP Switch Gateway 1 and the GIGAswitch/IP Switch Controller you previously configured. Follow the steps outlined in step 2, substituting these commands:
- a. Temporarily assign an address to the GIGAswitch/IP Switch Controller:  

```
ifconfig atm-s1p1c0 10.1.1.2/30 10.1.1.1 up
```
  - b. Enable IP Switch Gateway 1 to communicate with the GIGAswitch/IP Switch Controller:  

```
route add default 10.1.1.1
```
  - c. Verify that the IP address and netmask were set up successfully:  

```
ifconfig -a
```
  - d. Ping IP Switch Gateway 2 to make sure it is reachable:  

```
ping 10.1.1.2
```

---

### Note

In step 9, you assigned a temporary IP address to IP Switch Gateway 2, to allow you to get to the point where you could run Configuration Tool on the IP Switch Gateway. Now you will use Configuration Tool to define `configuration` files that will automatically configure IP Switch Gateway 2 every time it starts.

---

10. Use the browser (on the host machine) to connect to IP Switch Gateway 2 and configure it. Follow these steps:
  - a. Type the IP address of the IP Switch Gateway's `atm-s1p1c0` interface (the same address you used in step 9) into the `LOCATION` field and press `RETURN`:
 

```
10.1.1.2
```
  - b. In step 3 you learned how to create a with the Configuration Tool. To configure IP Switch Gateway 2, create a `configuration` file with the Configuration Tool that contains the following information:
    - The `atm-s1p1c0` interface:
      - IP address:
 

```
10.1.1.2
```
      - Network mask length:
 

```
30
```
      - Enable OSPF and DVMRP (Multicast).
      - Point-to-Point Remote IP Address:
 

```
10.1.1.1
```
    - The `eth-s2p1c0` interface:
      - IP address:
 

```
10.1.2.24
```
      - Network mask length:
 

```
24
```
      - Enable OSPF and DVMRP (Multicast).
      - Under Interface Optional Data, select 100 Mbit.
  - c. Confirm writing the changes to the `configuration` file.
  - d. Return to the `CONFIGURATION MENU`.
  - e. Generate files for the next boot.
  - f. Apply the configuration changes and reboot.

---

**Note**

In step 5, you configured the GIGAswitch/IP Switch Controller to allow you to get to the point where you could configure IP Switch Gateway 2 and IP Switch Gateway 3. Now you will use Configuration Tool to enable OSPF and DVMRP on the GIGAswitch/IP Switch Controller.

---

11. Use the browser (on the host machine) to reconnect to the GIGAswitch/IP Switch Controller and modify its configuration. Follow these steps:
  - a. Type the IP address of the GIGAswitch/IP Switch Controller's `atm-s1p1c0s2` interface into the `Location` field and press `RETURN`:
 

```
10.1.1.9
```

- b. Modify the `configuration` file with the Configuration Tool so that it contains the following information:
  - The `atm-s1p1c0s3` interface:
    - Enable OSPF and DVMRP (Multicast).
  - The `atm-s1p1c0s4` interface:
    - Enable OSPF and DVMRP (Multicast).
  - Deselect Advertise Interfaces to OSPF.

---

**Note**

For an interface that has OSPF enabled, Advertise Interfaces to OSPF should not be selected.

---

- c. Confirm writing the changes to the `configuration` file.
  - d. Return to the CONFIGURATION MENU.
  - e. Generate files for the next boot.
  - f. Apply the configuration changes and reboot.
12. Test your network by pinging from node to node in enough possible combinations to demonstrate that all nodes are configured correctly.



# DIGITAL GIGAswitch/ATM Configuration Commands

---

## Overview

IP switching is supported on the DIGITAL GIGAswitch/ATM. This chapter describes how to:

- Configure IP switching using the `configure_ipswitch` command
- Delete the current configuration using the `delete_ipswitch_config` command
- Display the current configuration using the `show_ipswitch_config` command

When you enter these commands, type them completely in lower case.

## For More Information

If you are unfamiliar with the DIGITAL GIGAswitch/ATM configuration, read these manuals for information:

- *GIGAswitch/ATM Installation and Service*  
Part number: AA-QCV7B-TE
- *GIGAswitch/ATM Management*  
Part number: AA-QCV8C-TE

## Prerequisites

Before you use the GIGAswitch/ATM configuration commands, do this:

1. Make sure you have the necessary equipment.  
Read the section, Check the Equipment on page 40.
2. Upgrade the GIGAswitch/ATM firmware, if necessary.  
Read the section, Upgrade the DIGITAL GIGAswitch/ATM Firmware on page 41.

### Check the Equipment

To complete the configuration, you need the following equipment:

- A GIGAswitch/ATM with the clock card installed.
- A DAGGL-BA line card installed in the GIGAswitch/ATM.  
The line card must be running firmware version 2.0.1ip or greater.
- A terminal emulator or VT series terminal connected to the GIGAswitch/ATM.

To attach a VT series terminal to the GIGAswitch/ATM, use a DIGITAL H8571-K connector and DIGITAL office connect cable. The default settings are 9600 baud, 8 data bits, 1 stop, no parity.

Attach the terminal directly to the 25-pin D connector on the clock card on the GIGAswitch/ATM. The 25-pin D connector is a serial port that acts as the interface to perform local configuration of the GIGAswitch/ATM.

Alternatively, you can use a Telnet session to accomplish the configuration task. The clock module has a 10mb Ethernet twisted-pair port that lets you access management and configuration functions using TCP/IP. For information about setting the TCP/IP address on the GIGAswitch/ATM and connecting using TCP/IP, read the *GIGAswitch/ATM Installation and Service manual*.

## Upgrade the DIGITAL GIGAswitch/ATM Firmware

Before you begin configuring the GIGAswitch/ATM for IP switching service, ensure that the firmware revisions of both the clock card and the DAGGL-BA line card are at the proper levels.

To check the firmware revisions, use this procedure:

- The Clock Module firmware must be version 1.74 or greater.

From the Clock Management Module Console `CLK>` prompt, enter the `B` command.

- The GIGAswitch/ATM firmware must be version 2.0.1ip or greater to support the operation of IP switching on the DAGGL-BA line card.
  1. At the terminal attached to the GIGAswitch/ATM, enter `^O`.
  2. From the Line Card Forwarding mode `GIGAswitch/ATM->` prompt, enter the `versions` command.

If you need to upgrade the GIGAswitch/ATM firmware to bring it into compliance, read the *GIGAswitch/ATM Installation and Service* manual for details on how to accomplish this task.

When upgrading the firmware, always read the release notes that accompany the firmware upgrade kit for answers to questions and solutions to problems. The release notes contain important information about new firmware features or syntactic changes to existing firmware functions.

## configure\_ipswitch Command

### Configuration Overview

To successfully configure IP switching on the GIGAswitch/ATM, follow these general steps:

1. Make sure you have the necessary equipment.  
Read the section, Check the Equipment on page 40.
2. Upgrade the GIGAswitch/ATM firmware, if necessary.  
Read the section, Upgrade the DIGITAL GIGAswitch/ATM Firmware on page 41.
3. Use the `show_ipswitch_config` command to display the current configuration, if applicable.  
Read the section, Use the `show_ipswitch_config` Command on page 42.
4. Use the `delete_ipswitch_config` command to delete the current configuration, if applicable.  
Read the section, Use the `delete_ipswitch_config` Command on page 42.
5. Use the `configure_ipswitch` command to configure IP switching.  
Read the section, Use the `configure_ipswitch` Command on page 42.

### Use the configure\_ipswitch Command

To configure IP switching on the GIGAswitch/ATM:

1. Enter `^O`, and press RETURN until you see the `GIGAswitch/ATM->` prompt.  
The `GIGAswitch/ATM->` prompt ensures that you are in the Line Card forwarding mode of the console.
2. Enter the console command `configure_ipswitch`.  
The `configure_ipswitch` command starts an interactive configuration process with the GIGAswitch/ATM. You may see an error message concerning the configuration records, but this is normal, and you can safely ignore it.  
If you have an active configuration for IP switching, it is displayed.  
A question appears, asking if you want to change this configuration.
3. Select 1 for yes to begin configuring the IP switching software.  
You always have the option of discarding a configuration after you have started, so you can make changes later if you want.  
A question appears, prompting you for the default VCI for IFMP.
4. Enter the default VCI value for IFMP you have chosen for your site.

---

For IP switching to function properly, you need to designate a VCI for IFMP. All entities participating in IP switching must have the same VCI for IFMP.

5. Enter the values that identify the line card and physical port number into which the IP switch controller is installed.

The values are entered on the same line separated by a single space.

The first number specifies the slot number. This number, clearly marked on the GIGAswitch/ATM chassis, is the GIGAswitch/ATM slot number into which the DAGGL-BA is installed.

The second number is the physical port number. The port numbers on the DAGGL-BA range from 1 to 4. For the 14-slot GIGAswitch/ATM, the cards are oriented vertically, and the ports are numbered top to bottom. For the 5-slot GIGAswitch/ATM, the cards are oriented horizontally, and the ports are numbered left to right. Typically, the controller is connected to port 1 on the DAGGL-BA.

The third number is the VCI for switch to controller communication. This number should be the same as the VCI number used for IFMP, although this is not an explicit requirement.

6. Select the default value of 20 for the rate in Mbp/s for multicast VCs.

If you have a site-specific reason, enter a value other than 20. Otherwise, select the default.

7. Enter the two values for the minimum and maximum VCI numbers to be made available for IP switching.

The minimum and maximum numbers are inclusive. Separate the values by a single space.

The default is 32 to 512. To accept the default, press RETURN.

8. Specify the physical port numbers (1, 2, 3, or 4) over which you wish to run IP switching for each DAGGL-BA line card you have installed in your system.

You are asked about each of these cards installed in your particular GIGAswitch/ATM. The ports not enabled for IP switching default to running ATM Forum LANE. You must enable IP switching on the line card and port number that you designated to connect to the controller.

When you have completed designating the ports that are to run IP switching, the configuration is printed.

9. Review the printed configuration carefully.

10. Select 1 to save the changes in flash if you decide to keep the changes, or select 2 if you decide to discard them.

If you saved the changes, restart the GIGAswitch/ATM for the changes to take effect.

If you did not save the changes, you are returned to the GIGAswitch/ATM console prompt.

## Sample configure\_ipswitch Session

The following log file shows a typical configure\_ipswitch session:

```
-----
GIGAswitch/ATM-> configure_ipswitch

==== Active IP Switch Configuration Information ====
Default VCI for IFMP:                               32
Slot Number, Link Number, VCI Number to IP Switch Controller: 3, 1, 32
Rate in MBits/Sec for Multicast VCs:                20
Minimum and Maximum VCIs Reserved on each Link for IP Switch: 32, 512
IP Switching enabled on the following slots and ports

Change IP Switch Configuration <1: Yes, 2: No>?      1
Default VCI for IFMP:                                32                <d>
Slot #, Link #, VCI # to IP Switch Controller:       3, 1, 32            <d d d>
Rate in MBits/Sec for Multicast VCs:                 20                <d>
Min and Max VCIs for each Link for IPSwitch:         32, 512            <d d>
    Ports enabled on slot 3:                          <d d d d> 1 2 3 4

New IP Switch Configuration
Default VCI for IFMP:                               32
Slot Number, Link Number, VCI Number to IP Switch Controller: 3, 1, 32
Rate in MBits/Sec for Multicast VCs:                20
Minimum and Maximum VCIs Reserved on each Link for IP Switch: 32, 512
IP Switching enabled on the following slots and ports
    Ports enabled on slot 3:                          01, 02, 03, 04
Save or discard new Configuration <1-Save, 2-Discard>? 1
New IP SWITCH Configuration written to Flash
-----
```

## delete\_ipswitch\_config Command

The `delete_ipswitch_config` command erases your IP switching configuration from the GIGAswitch/ATM flash.

### Create a New Configuration

When you want to reconfigure IP switching for the GIGAswitch/ATM, delete the current configuration with the `delete_ipswitch_config` command and then create a new configuration with the `configure_ipswitch` command.

To reconfigure IP switching on the GIGAswitch/ATM:

1. Upgrade the GIGAswitch/ATM firmware, if necessary.  
Read the section, Upgrade the DIGITAL GIGAswitch/ATM Firmware on page 41.
2. Display your current configuration, and note any settings that you want to use again.  
After you enter the `delete_ipswitch_config` command, you cannot retrieve or display the configuration. Because you may want to use some of the current configuration settings again, display the configuration to review and note these settings.  
Read the section, Use the `show_ipswitch_config` Command on page 46.
3. Use the `delete_ipswitch_config` command to delete the current configuration.  
Read the section, Use the `delete_ipswitch_config` Command on page 45.
4. Create a new IP switching configuration with the `configure_ipswitch` command.  
Read the section, Use the `configure_ipswitch` Command on page 42.

### Use the delete\_ipswitch\_config Command

To delete the current configuration:

1. Enter `^O`, and press RETURN until you see the `GIGAswitch/ATM->` prompt.  
The `GIGAswitch/ATM->` prompt ensures that you are in the Line Card forwarding mode of the console.
2. Enter the console command `delete_ipswitch_config`.  
The current IP switching configuration is erased from flash.
3. Enter the `reboot` command to reboot the GIGAswitch/ATM.  
To effect the change, you need to reboot the GIGAswitch/ATM.

## show\_ipswitch\_config Command

The `show_ipswitch_config` command displays the current IP switching configuration for the GIGAswitch/ATM.

### Use the show\_ipswitch\_config Command

To display the IP switching configuration on the GIGAswitch/ATM:

1. Upgrade the GIGAswitch/ATM firmware, if necessary.  
Read the section, Upgrade the DIGITAL GIGAswitch/ATM Firmware on page 41.
2. Enter `^O`, and press RETURN until you see the `GIGASWITCH/ATM->` prompt.  
The `GIGASWITCH/ATM->` prompt ensures that you are in the Line Card forwarding mode of the console.
3. Enter the console command `show_ipswitch_config`.  
The current IP switching configuration is displayed.

### Sample show\_ipswitch\_config Session

The following example shows a typical display:

```
-----  
GIGAswitch/ATM-> show_ipswitch_config  
  
===== Active IP Switch Configuration Information =====  
Default VCI for IFMP: 32  
Slot Number, Link Number, VCI Number to IP Switch Controller: 3, 1, 32  
Rate in MBits/Sec for Multicast VCs: 20  
Minimum and Maximum VCIs Reserved on each Link for IP Switch: 32, 512  
IP Switching enabled on the following slots and ports  
    Ports enabled on slot 3: 01, 02, 03, 04
```



# Troubleshooting

---

## Overview

This chapter lists potential problems and possible solutions to those problems.

### **Problem: The DIGITAL GIGAswitch/IP Switch Controller and DIGITAL GIGAswitch/ATM do not synchronize**

1. Check that the GIGAswitch/ATM is powered on.  
Check the power LED on the outside of the GIGAswitch/ATM. If the LED is not lit, check the power cables, and ensure that the power switch is in the ON position.
2. Check cables to make sure that they are properly connected.  
Check that the cable is connected from the GIGAswitch/IP Switch Controller to the GIGAswitch/ATM. The cable should plug into the lowest numbered port on the switch, and into the port labeled atm-s1p1c0 on the GIGAswitch/IP Switch Controller.  
Make sure both ends of the cables are firmly seated.
3. Look for a Link LED on the GIGAswitch/ATM and on the GIGAswitch/IP Switch Controller adapter.  
Check the physical Link LED on the GIGAswitch/IP Switch Controller and on the GIGAswitch/ATM. The Link LED on the GIGAswitch/IP Switch Controller is on the ATM NIC.  
If the Link LED on either component is not lit, then check the cable connectors and the cable.
4. Check the GSMP status of the switch.

Attach a serial line and a console emulating VT100 to the serial port of the GIGAswitch/ATM. From the console, log on to the switch and check whether the switch is exchanging packets with the GIGAswitch/IP Switch Controller. Refer to the *GIGAswitch/ATM System Management* manual for more information about using the GIGAswitch/ATM console.

## Problem: Interfaces are not configured

1. Check to see whether `pnpiif` is running.

The `pnpiif` daemon configures the network interfaces as they become available after the GIGAswitch/IP restarts. This is done on the GIGAswitch/IP Switch Controller using the `ps` command:

```
ps -auxww | grep pnpiif.pl
```

The output looks something like this:

```
root 56 0.2 5.8 544 820 d0- S 7:46PM 0:05.03 /usr/bin/perl/sbin/pnpiif.pl
```

This output from `ps` should show that a process called `pnpiif.pl` is running. If it does, then go to the next step. If `pnpiif.pl` is not running, then try starting it manually using the following command:

```
/sbin/pnpiif.pl &
```

Wait for 30 seconds and see whether the interfaces are configured. If `pnpiif.pl` is not running, proceed to the next step.

2. Determine whether the interfaces exist.

Get a list of the system interfaces using the following `ifconfig` command:

```
ifconfig -a | more
```

This produces a list of interfaces similar to the following:

```
lo0: flags=8009<UP,LOOPBACK,MULTICAST> mtu 16384 inet 127.0.0.1/8
ppp0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
sl0: flags=c010<POINTOPOINT,LINK2,MULTICAST> mtu 552
tun0: flags=10<POINTOPOINT> mtu 1500
atm-s1plc0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s1: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s7: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500 inet
10.1.1.9/30
--> 10.1.1.10
atm-s1plc0s6: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500 inet
10.1.1.1/30
--> 10.1.1.2
atm-s1plc0s5: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s4: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500 inet
10.1.1.6/30
--> 10.1.1.5
atm-s1plc0s2: flags=8051<POINTOPOINT,RUNNING,MULTICAST> mtu 1500
```

Search this list for the interface being configured. If the interface exists, then proceed to the next step. If the interface does not exist, and it corresponds to an

interface on the GIGAswitch/ATM, then proceed to the section Problem: The DIGITAL GIGAswitch/IP Switch Controller and DIGITAL GIGAswitch/ATM do not synchronize on page 47.

3. Check the Configuration Tool settings to make sure that they are properly assigned.

Return to the Configuration Tool and verify the interface settings. Check for typos in the interface name, IP address, and network mask, as well as inappropriate options. Examine the `if.conf` file for the proper settings.

Examine the contents of the interface configuration file, `if.conf`, using the `more` command:

```
more /etc/if.conf
```

This command produces output that looks similar to:

```
ifconfig atm-s1p1c0s3 10.1.1.6/30 -link2 -link1
ifconfig atm-s1p1c0s6 10.1.1.1/30 -link2 -link1
ifconfig atm-s1p1c0s7 10.1.1.9/30 -link2 -link1
```

Examine this output for the interface that is not configured. If it is not listed, return to the Configuration Tool and make sure that the configuration has been updated.

If the interface is listed, then examine the configuration line to see whether it uses the correct IP address and the correct network mask. If they are incorrect, return to the Configuration Tool.

4. If the previous steps were unsuccessful, try manually configuring the interface.

Use the `ifconfig` command:

```
ifconfig atm-s1p1c0 10.1.1.5/30 pnpif
```

Where `atm-s1p1c0` is the name of the interface to configure, `10.1.1.5` is the IP address to use, and `30` is the length of the network mask in number of bits.

If this step succeeds, recheck the configuration in the Configuration Tool and proceed to the next step.

## Problem: No IFMP synchronization

1. Check cables to make sure that they are properly connected.

Check the cables that connect each IP Switch Gateway and the GIGAswitch/ATM. The cables should be firmly seated into the connectors.

2. Check Link LEDs on the GIGAswitch/ATM and on the IP Switch Gateways.

Check the physical Link LED on the GIGAswitch/ATM and on the GIGAswitch/ATM adapter in the IP Switch Gateway. This indicates whether the cables are providing the correct connection.

If both Link LEDs are lit, proceed to the next step. If either one or both of the LEDs are not lit, then check the cable connections and the cables.

3. Check interface configurations to make sure that they are properly assigned.

Use the `ifconfig` command to get a list of all interfaces and their configurations. This should be done on the GIGAswitch/IPs and IP Switch Gateways that are not synchronizing. Issue the following command:

```
ifconfig -a | more
```

This produces a list of interfaces similar to the following:

```
lo0: flags=8009<UP,LOOPBACK,MULTICAST> mtu 16384
    inet 127.0.0.1/8
ppp0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
sl0: flags=c010<POINTOPOINT,LINK2,MULTICAST> mtu 552
tun0: flags=10<POINTOPOINT> mtu 1500
atm-s1p1c0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1p1c0s1: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1p1c0s7: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST>
mtu
    1500 inet 10.1.1.9/30 --> 10.1.1.10
atm-s1p1c0s6: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST>
mtu
    1500 inet 10.1.1.1/30 --> 10.1.1.2
atm-s1p1c0s5: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1p1c0s4: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1p1c0s3: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST>
mtu
    1500 inet 10.1.1.6/30 --> 10.1.1.5
atm-s1p1c0s2: flags=8051<POINTOPOINT,RUNNING,MULTICAST> mtu
1500
```

4. Search this list for the interface that is not synchronizing.

Make sure that the correct IP address and the correct network mask are set for this interface. Check the UP flag for the interface. If it is not set or the interfaces are not appropriately configured, refer to the section **Problem: Interfaces are not configured** on page 48.

## Problem: Unable to ping neighbors

1. Check for IFMP synchronization on ips interfaces.

Do steps 1 through 4 in the section, **Problem: No IFMP synchronization** on page 49.

2. Check the routing table for an appropriate route.

Dump the contents of the routing table with the `netstat` command. Issue the following command to provide a listing of the kernel routing table:

```
netstat -rn | more
```

The output looks similar to the following:

Routing tables

```
Internet:
Destination      Gateway          Flags           Refs      Use     Netif Expire
default          10.1.1.9        UGc             0         0       atm-s1p1c0
127              127.0.0.1       URc             0         0       lo0
127.0.0.1        127.0.0.1       UH              0         25      lo0
```

10.1.1.1	10.1.1.9	UGH	0	0	atm-s1p1c0
10.1.1.2	10.1.1.9	UGH	0	0	atm-s1p1c0
10.1.1.5	10.1.1.9	UGH	0	0	atm-s1p1c0
10.1.1.6	10.1.1.9	UGH	0	0	atm-s1p1c0
10.1.1.9	10.1.1.10	UGH	0	0	atm-s1p1c0
10.1.1.10	10.1.1.9	UGH	0	0	atm-s1p1c0
10.1.2	10.1.1.9	UGc	0	0	atm-s1p1c0
10.1.3	10.1.1.9	UGc	0	0	atm-s1p1c0
10.1.4	10.1.1.9	UGc	0	0	atm-s1p1c0
10.1.5	10.1.1.9	UGc	0	1	atm-s1p1c0
10.1.6	10.1.6.1	UGc	3	11339	eth-s2p1c0
10.1.6.11	0:0:c0:1f:82:bf	UHLW	12	0	eth-s2p1c0
964					
10.1.6.32	0:c0:95:f8:1:5e	UHLW	0	0	eth-s2p1c0
520					
10.1.6.212	0:80:3f:f4:7:40	UHLW	6	1801520	eth-s2p1c0
1018					
10.1.4	10.1.4.1	UGc	3	21378	eth-s3p1c0
10.1.4.10	0:0:94:60:68:4d	UHLW	10	0	eth-s3p1c0
1070					
10.1.4.13	0:20:af:6d:7f:bd	UHLW	0	0	eth-s3p1c0
1062					
10.1.4.21	0:80:c8:c:f1:cb	UHLW	6	163911	eth-s3p1c0
1086					
224	link#6	UCS	17	0	
224.0.0.5	127.0.0.1	UH	0	26155	lo0
224.0.0.6	127.0.0.1	UH	0	0	lo0

Look through this list to determine whether a route exists to the machine you are trying to ping. If the route does not exist and does not appear to point to the correct interface, proceed to the next section Problem: When doing a traceroute, unable to get all the way to the place I am tracing on page 51.

## Problem: When doing a traceroute, unable to get all the way to the place I am tracing

1. Make sure that `gated` is running.

The `gated` daemon handles the unicast routing function for the GIGAswitch/IP. Verify that it is running with the `ps` command. Issue the following command:

```
ps auxww | grep gated
```

The output looks something like the following:

```
admin 19544 0.0 0.4 176 48 p0 R+ 7:29AM 0:00.01 grep gated
root 107 0.0 7.1 936 1004 ?? S Sat05PM 1:04.20 /usr/local/sbin/gated
```

The output from `ps` should show that a process called `gated` is running. If `gated` is running, then proceed to the next step. Otherwise, try to start `gated` manually with the following command:

```
/usr/local/sbin/gdc start
```

2. Make sure that the multicast route exists.

To function properly, the multicast route to 224.0.0.0 must be in the routing table for `gated` and `mrouted`. To check for this route, issue the `netstat` command:

```
netstat -rn | more
```

One of the output lines should contain an entry to:

```
224.0.0.0
```

If this route does not exist, check the configuration.

3. Make sure the interfaces exist, are running, and are configured properly.

Check that each of the configured interfaces exists. To display a list of all interfaces, use the following `ifconfig` command:

```
ifconfig -a | more
```

This produces a list of interfaces similar to the following:

```
lo0: flags=8009<UP,LOOPBACK,MULTICAST> mtu 16384
    inet 127.0.0.1/8
ppp0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
sl0: flags=c010<POINTOPOINT,LINK2,MULTICAST> mtu 552
tun0: flags=10<POINTOPOINT> mtu 1500
atm-s1plc0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s1: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s7: flags=8051<UP, POINTOPOINT, RUNNING, MULTICAST>
mtu
    1500 inet 10.1.1.9/30 --> 10.1.1.10
atm-s1plc0s6: flags=8051<UP, POINTOPOINT, RUNNING, MULTICAST>
mtu
    1500 inet 10.1.1.1/30 --> 10.1.1.2
atm-s1plc0s5: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s4: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
atm-s1plc0s3: flags=8051<UP, POINTOPOINT, RUNNING, MULTICAST>
mtu
    1500 inet 10.1.1.6/30 --> 10.1.1.5
atm-s1plc0s2: flags=8051<POINTOPOINT, RUNNING, MULTICAST> mtu
1500
```

Make sure each interface that should be configured is listed in this output. If any interfaces are missing, refer to the Troubleshooting section in the *DIGITAL GIGAswitch/IP Solution for ATM Products Reference*.

If all the interfaces exist, then search this list for the interface that is not synchronizing. Make sure the correct IP address and the correct network mask are set for this interface. Check that the UP flag is set for the interface. If either test fails, proceed to the section Problem: Interfaces are not configured on page 48.

4. Check the Configuration Tool settings to make sure they are properly assigned. Rerun the Configuration Tool to check that the routing was properly configured.

## Problem: No multicast reachability

Multicast routing and forwarding is overseen by a daemon called `mrouterd`. If multicast is not working across a hop:

1. Log in to that router and use the Configuration Tool to make sure SDVMP is enabled on the interfaces.
2. While still logged in to that router, ensure that `mrouterd` is running and that there is a route to `244.0.0.0/5` which is directed out a well-configured multicast-capable interface.
3. If `mrouterd` seems to be running properly, produce an `mrouterd.dump` file. To do this, use the `ps` command to identify the `mrouterd` process, and then send a `kill -USR1` signal to the `mrouterd` process:

```
# ps auxww | grep mrouterd
root 5580 0.0 5.2 628 716 ?? S 11:31PM 0:05.15 mrouterd
# kill -USR1 5580
```

The `mrouterd.dump` file contains a header which describes each of the interfaces present in the system. The following is an example of the first portion of an `mrouterd.dump` file:

```
Vif Name Local-Address M Thr Rate Flags
0 atm-slplc0s3 10.1.1.6 subnet: 10.1.1.4/30 1 1 0
querier leaf
peers: 10.1.1.5 (3.8) (0xf)
pkts in : 0
pkts out: 56
```

All interfaces that support multicast should be present and show nonzero packet counts (if they should be active). The peers list should explicitly list all multicast routers expected to be active on the link the interface is connected to.

The second portion of the `mrouterd.dump` file contains a single line entry for each DVMRP route currently in the forward routing map:

```
Origin-Subnet From-GIGAswitch/IP Switch Gateway Metric Tmr
In-Vif Out-Vifs
10.1.3.0/24 1 140 1 0 2* 3* 4*
```

It is important to verify that the networks listed have the proper masks, and that all networks that should be multicast reachable are listed. If the node has a connection to the global multicast network (currently the MBONE), there should be a large number of entries corresponding to remote sites.

4. Things to try:
  - Use `tcpdump -i interfacename proto igmp` (see the `tcpdump` man page for details) to verify that multicast traffic is being seen from all the mrouterd on the subnet.
  - Check that the network masks of all mrouterd on the link are configured to be the same value.
  - Use `netstat -p ip` and `netstat -p igmp` to look for anomalous error counters.

- Check to make sure the thresholds on the vifs are set to reasonable boundaries. Within a single administrative domain all thresholds should be 1.
  - Check the rate pacing on the vifs to see if the rate is reasonable for your environment.
  - Ensure that addresses that fall on configured administrative boundaries are not expecting to transit this node.
  - Use the `mtrace` command to check the multicast routing path from the receivers toward the sender. If there is a failure, it is indicated as downstream of the last multicast router to respond to the `mtrace`.
5. If the problem is still not apparent, `mrouted` can be restarted with the `-d` option to show up to nine levels of debugging information. Although this can produce a large volume of output, explicit errors are logged, which can help to diagnose the problem.

## Problem: The IP switching network does not learn about routes from my RIP attached router

1. Check the Configuration Tool to make sure RIP is properly configured.

In order for IP switching nodes to learn about routes propagated by the RIP protocol, an IP Switch Gateway connected to a network running RIP must have RIP enabled on that interface. If you want routes from RIP to be used in the IP switching network but not emitted, you can select this by turning off the RIP OUT toggle on the ADVANCED INTERFACE page (accessed by creating or modifying an interface) in the Configuration Tool.

One other important configuration option, the ADVERTISE RIP ROUTES TO OSPF toggle, must be selected on the Advanced Interface page in order to propagate RIP routes into OSPF.

2. Check to see whether the routes are being picked up by the IP Switch Gateway that is listening to RIP.

Issue the following command to provide a listing of the kernel routing table:

```
netstat -rn | more
```

The output looks similar to the following:

Routing tables

```
Internet:
Destination      Gateway          Flags           Refs          Use          Netif Expire
default          10.1.1.9        UGc             0             0            atm-s1p1c0
127              127.0.0.1       URc             0             0            lo0
127.0.0.1        127.0.0.1       UH              0             25           lo0
10.1.1.1         10.1.1.9        UGH             0             0            atm-s1p1c0
10.1.1.2         10.1.1.9        UGH             0             0            atm-s1p1c0
10.1.1.5         10.1.1.9        UGH             0             0            atm-s1p1c0
10.1.1.6         10.1.1.9        UGH             0             0            atm-s1p1c0
10.1.1.9         10.1.1.10       UGH             0             0            atm-s1p1c0
```



10.1.1.10	10.1.1.9	UGH	0	0	atm-s1p1c0
10.1.1.2	10.1.1.9	UGc	0	0	atm-s1p1c0
10.1.1.3	10.1.1.9	UGc	0	0	atm-s1p1c0
10.1.1.4	10.1.1.9	UGc	0	0	atm-s1p1c0
10.1.1.5	10.1.1.9	UGc	0	1	atm-s1p1c0
10.1.1.6	10.1.6.1	UGc	3	11339	eth-s2p1c0
10.1.6.11	0:0:c0:1f:82:bf	UHLW	12	0	eth-s2p1c0
964					
10.1.6.32	0:c0:95:f8:1:5e	UHLW	0	0	eth-s2p1c0
520					
10.1.6.212	0:80:3f:f4:7:40	UHLW	6	1801520	eth-s2p1c0
1018					
10.1.4	10.1.4.1	UGc	3	21378	eth-s3p1c0
10.1.4.10	0:0:94:60:68:4d	UHLW	10	0	eth-s3p1c0
1070					
10.1.4.13	0:20:af:6d:7f:bd	UHLW	0	0	eth-s3p1c0
1062					
10.1.4.21	0:80:c8:c:f1:cb	UHLW	6	163911	eth-s3p1c0
1086					
224	link#6	UCS	17	0	
224.0.0.5	127.0.0.1	UH	0	26155	lo0
224.0.0.6	127.0.0.1	UH	0	0	lo0

3. Examine the list of routes and determine whether the advertised RIP routes are included in the table.
4. Check to see whether these routes are being installed in the IP Switch Gateway that is listening to RIP, but not elsewhere. Follow these steps:
  - a. Acquire root privileges (password required):

```
su root
```

- b. Enter the following two commands:

```
echo "localhost 127.0.0.1" > /tmp/filename
/usr/local/sbin/ospf_monitor /tmp/filename
```

where *localhost* is the logical name of the IP Switch Gateway, and */tmp/filename* is a file that contains a list of machines for *ospf\_monitor*, of which you can check the OSPF status. The output is similar to the following:

```
listening on 0.0.0.0.1025
invalid address (localhost) on line 1
```

- c. Enter the following command:

```
dest command params > @1 o
```

The output is similar to the following:

```
remote-command <o> sent to 0.0.0.0
```

```
Source <<10.11.10.34 127.0.0.1>>
AS Border Routes:
Router      Cost AdvRouter      NextHop(s)
-----
Area 0.0.0.0:
10.11.1.129 7 10.11.1.129 10.11.12.102
10.11.10.103 3 10.11.10.103 10.11.10.42
10.11.10.90 1 10.11.10.90 10.11.10.42
```

```

10.11.10.83      2 10.11.10.83  10.11.10.42
10.11.10.52      4 10.11.10.52  10.11.10.42
10.11.6.5        2 10.11.6.5    10.11.12.102
10.11.6.3        2 10.11.6.3    10.11.12.102
10.11.6.1        2 10.11.6.1    10.11.12.102

```

Total AS Border routes: 8

Area Border Routes:

```

Router          Cost AdvRouter      NextHop(s)
-----
Area 0.0.0.0:

```

Summary AS Border Routes:

```

Router          Cost AdvRouter      NextHop(s)
-----

```

Networks:

```

Destination      Area          Cost Type NextHop      AdvRouter
-----
10.11.12         0.0.0.0      1 Net  10.11.12.102 10.11.10.34
10.11.6          0.0.0.0      2 Net  10.11.12.102 10.11.6.5
10.11.5          0.0.0.0      3 Stub 10.11.12.102 10.11.6.1
.
.
.
10.11.10.70     0.0.0.0      2 Stub 10.11.10.42  10.11.10.90
10.11.10.90     0.0.0.0      3 Stub 10.11.10.42  10.11.10.83
10.11.10.83     0.0.0.0      2 Stub 10.11.10.42  10.11.10.90

```

ASEs:

```

Destination      Cost E      Tag NextHop      AdvRotuer
-----
10.11.7          2 1 c0000000 10.11.12.102 10.11.6.5
10.11.14         2 1 c0000000 10.11.12.102 10.11.6.5
0.0.0.0          3 3 c0000000 10.11.12.102 10.11.6.3
10.11.0          3 3 c0000000 10.11.12.102 10.11.6.3
10.11.9          4 1 c0000000 10.11.10.42  10.11.10.52
10.11.10.120    2 1 c0000000 10.11.10.42  10.11.10.83
10.11.8          3 1 c0000000 10.11.10.42  10.11.10.103
10.11.10.139    1 1 c0000000 10.11.10.42  10.11.10.90

```

Total nets: 33

Intra Area: 8 Inter Area: 25 ASE: 8

done

The RIP routes appear in the ASEs section if they are being inserted into the OSPF routing by RIP.

5. Check to see whether the routes are being included in the local routing table.

If the routes are not being included in the local routing table, issue the following command to watch for RIP packets on the interface:

```
tcpdump -s 512 udp port 520
```

The output is similar to the following:

```
12:08:55.690741 external.my.org.router > 10.11.6.255.router:
rip-resp 10: 10.11.25.2(1) 10.11.25.6(1) 10.11.25.10(1)
10.11.25.1(1) 10.11.3.0(1) 10.11.1.0(1) 10.11.5.0(1)
10.11.7.0(1) 10.11.14.0(1) 10.11.15.0(1) [ttl 1]
```

The first name/address on the first line of the `tcpdump` output is the advertising router, the second is the broadcast address, and each of the following entries is a network with the metric in parentheses.

6. Check for packets that arrive with metric 15 or 16.

In `tcpdump`, routes with metrics of 15 or 16 are listed but are not reachable. The RIP infinity metric is 16, so packets that arrive with metric 15 or 16 might be discarded. If this is the case, either the diameter of your network is too large or administrative weights are being added along the path.

7. If no RIP packets are being received, check the IP connectivity on that interface and ensure that the broadcast address matches that of the advertising routing.

Use the `ping` command to check for IP connectivity, and use the `ifconfig` command to check that the broadcast address matches that of the advertising routing.

8. If RIP packets are arriving at the IP Switch Gateway, but not being placed into the routing table, check the configuration of your IP Switch Gateway.

Examine the `gated.conf` file for a statement similar to the following:

```
rip yes {
    broadcast ;
    interface eth-s2plc0 ripin ripout version 1;
};
```

There should be a statement like this with an interface clause for each interface running RIP.

9. If the routes are not being sent to the OSPF listener on the ATM network, check your configuration.

Examine the `gated.conf` file for a statement similar to the following:

```
export proto ospfase {
    proto rip {all metric 1;};
};
```

There should be a statement like `thi`, which causes the RIP routes to be sent to the OSPF routed components.

10. Check the Configuration Tool on the GIGAswitch/IP Switch Controller to make sure that OSPF has been enabled on the interface connected to the GIGAswitch/IP Switch Controller.



# Network Design Table

---

The blank table on the next page is structured like the one used as an example in Chapter 2, *Installing and Configuring a Network*. We recommend that before you begin installation, you photocopy the next page and fill out the table with information that describes your network configuration.



# Network Identifiers: Addresses and Interface IDs

---

## Overview

This chapter describes subnet masks and lists the subnets, host addresses, and broadcast numbers.

## IP Addressing

For IPv4, an IP address is a 32-bit value which consists of two parts. The first part is the subnetwork number. The remainder of the bits are used to distinguish the hosts on the subnetwork, and are called the host interface numbers. IP allows for subnetwork numbers to have different lengths.

## Subnetting

Each connection between a DIGITAL IP Switch and another DIGITAL IP Switch Gateway must have a unique subnetwork number. Your subnetwork numbers are allocated by your Internet service provider, although once you have been allocated a block of numbers, you may choose how to assign them to your machines.

The length of a subnetwork number (in bits) is referred to as the network mask. A network mask length equal to 24 means that IP addresses using this mask consist of 24 bits of subnetwork number and 8 bits of host interface numbers. By convention, a host number of all 0 bits identifies the network itself and a host number of all 1 bits is the broadcast address.

Digital Equipment Corporation recommends that ATM links in your network use a network mask length of 30 bits. Using large netmasks helps conserve IP address space on subnetworks that have only a few hosts attached.

ATM links are point-to-point interfaces, so each can support only two hosts. The 30-bit netmask leaves two bits for host addressing, for a total of four available

addresses. Two of these addresses correspond to the subnetwork and broadcast addresses, and the other two are used for the host machine.

You also need to know the subnetwork numbers and network mask lengths for each network that you connect to an IP Switch Gateway.

## Subnet Mask Reference Charts

Mask length 30 corresponds to a subnet mask of 255.255.255.252.

Subnet	Host addresses	Broadcast
0	1-2	3
4	5-6	7
8	9-10	11
12	13-14	15
16	17-18	19
20	21-22	23
24	25-26	27
28	29-30	31
32	33-34	35
36	37-38	39
40	41-42	43
44	45-46	47
48	49-50	51
52	53-54	55
56	57-58	59
60	61-62	63
64	65-66	67
68	69-70	71
72	73-74	75
76	77-78	79
80	81-82	83
84	85-86	87
88	89-90	91
92	93-94	95
96	97-98	99
100	101-102	103
104	105-106	107
108	109-110	111
112	113-114	115
116	117-118	119
120	121-122	123
124	125-126	127
128	129-130	131
132	133-134	135
136	137-138	139
140	141-142	143
144	145-146	147
148	149-150	151
152	153-154	155
156	157-158	159
160	161-162	163



---

<b>Subnet</b>	<b>Host addresses</b>	<b>Broadcast</b>
164	165-166	167
168	169-170	171
172	173-174	175
176	177-178	179
180	181-182	183
184	185-186	187
188	189-190	191
192	193-194	195
196	197-198	199
200	201-202	203
204	205-206	207
208	209-210	211
212	213-214	215
216	217-218	219
220	221-222	223
224	225-226	227
228	229-230	231
232	233-234	235
236	237-238	239
240	241-242	243
244	245-246	247
248	249-250	251
252	253-254	255

---

Mask length 29 corresponds to a subnet mask of 255.255.255.248.

---

<b>Subnet</b>	<b>Host addresses</b>	<b>Broadcast</b>
0	1-6	7
8	9-14	15
16	17-22	23
24	25-30	31
32	33-38	39
40	41-46	47
48	49-54	55
56	57-62	63
64	65-70	71
72	73-78	79
80	81-86	87
88	89-94	95
96	97-102	103
104	105-110	111
112	113-118	119
120	121-126	127
128	129-134	135
136	137-142	143
144	145-150	151
152	153-158	159
160	161-166	167
168	169-174	175
176	177-182	183
184	185-190	191

---

<b>Subnet</b>	<b>Host addresses</b>	<b>Broadcast</b>
192	193-198	199
200	201-206	207
208	209-214	215
216	217-222	223
224	225-230	231
232	233-238	239
240	241-246	247
248	249-254	255

Mask length 28 corresponds to a subnet mask of 255.255.255.240.

<b>Subnet</b>	<b>Host addresses</b>	<b>Broadcast</b>
0	1-14	15
16	17-30	31
32	33-46	47
48	49-62	63
64	65-78	79
80	81-94	95
96	97-110	111
112	113-126	127
128	129-142	143
1444	145-158	159
160	161-174	175
176	177-190	191
192	193-206	207
208	209-222	223
224	225-238	239
240	241-245	255

Mask length 27 corresponds to a subnet mask of 255.255.255.224.

<b>Subnet</b>	<b>Host addresses</b>	<b>Broadcast</b>
0	1-30	31
32	33-62	63
64	65-94	95
96	97-126	127
128	129-158	159
160	161-190	191
192	193-222	223
224	225-254	255

Mask length 26 corresponds to a subnet mask of 255.255.255.192.

<b>Subnet</b>	<b>Host addresses</b>	<b>Broadcast</b>
0	1-62	63
64	65-126	127
128	129-190	191
192	193-254	255

Mask length 25 corresponds to a subnet mask of 255.255.255.128.

<b>Subnet</b>	<b>Host addresses</b>	<b>Broadcast</b>
0	1-126	127
128	129-254	255

Mask length 24 corresponds to a subnet mask of 255.255.255.0.

<b>Subnet</b>	<b>Host addresses</b>	<b>Broadcast</b>
0	1-254	255

