Network *Products*

Traffic Server 4.0

Installation Guide for IRIX

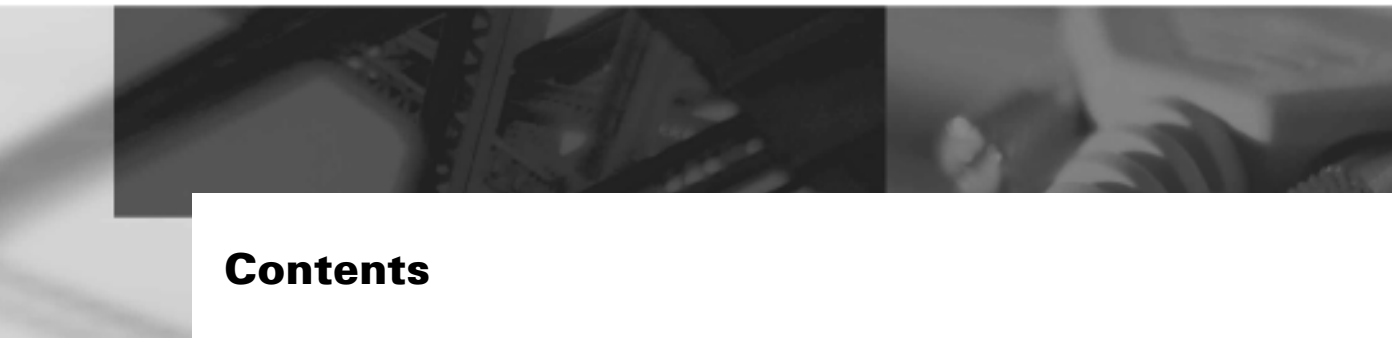
June 20, 2001

Inktomi®

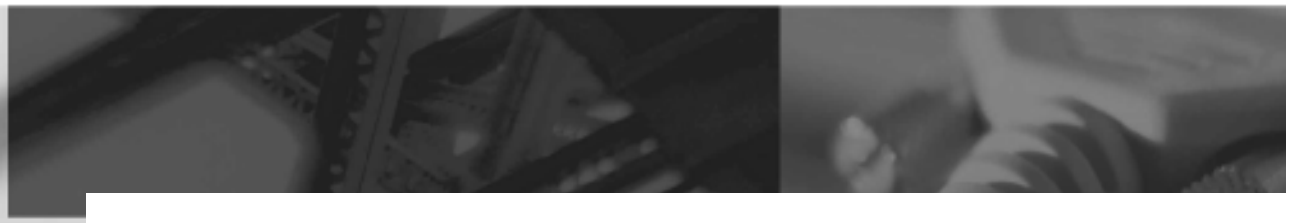
Document Revision A (software release 4.0.14/IRIX, June 20, 2001)

Revision History

Initial document release (software release 4.0.7/IRIX, March 16, 2001)



Contents



List of Procedures

Preface

This manual describes how to install or upgrade an Inktomi® Traffic Server™ system, either as a single node, or as a cluster of nodes.

The Preface discusses the following topics:

Who should read this manual

This manual is intended for Traffic Server system administrators, who configure, run, and administer Traffic Server systems.

The manual assumes that you have experience in UNIX® and Web server administration, and that you are comfortable performing complex system configuration tasks, such as partitioning and formatting disks, setting up TCP/IP ports, and establishing DNS round robin services.

How to use this manual

This manual organizes Traffic Server installation information around five areas:

- ✔ Preparing for installation
- ✔ First-time Traffic Server installation
- ✔ Upgrading, reinstalling, and uninstalling
- ✔ Post-installation
- ✔ Background information about:
  - ✗ Traffic Server's transparent proxying option
  - ✗ How installation affects the UNIX file system hierarchy

The following table provides a concise directory to help you get to the information you are interested in.

To...	See...
understand the installation types	*Understanding Traffic Server installation types, on page 21*
understand the details about installation options	*What to expect during Traffic Server installation, on page 22*
use a concise worksheet to prepare for installation	*Configuration Worksheet, on page 71*
install Traffic Server for the first time	*Installing Traffic Server on a single node, on page 29* *Installing Traffic Server in a cluster, on page 33*
upgrade or reinstall Traffic Server	*Upgrading, reinstalling, and uninstalling Traffic Server, on page 39*
know what to do after installation	*After Installing Traffic Server, on page 49*
understand transparent proxying	*Serving Traffic Transparently, on page 55*
understand what files are installed on your system	*UNIX Installation File Hierarchy, on page 63*

Related documentation

Always read the *Release Notes* which accompany every Traffic Server release. The *Release Notes* contain vital information that affects Traffic Server installation and operation.

To learn about using and configuring Traffic Server, see the *Traffic Server Administrator's Guide*.

This book describes the Traffic Server 4.0 release for IRIX. Any revisions of this book will bear the same title, but will show different publication dates on the front cover, as well as a Document Revision designator on the second page.

Conventions used in this manual

This manual uses the following typographic conventions:

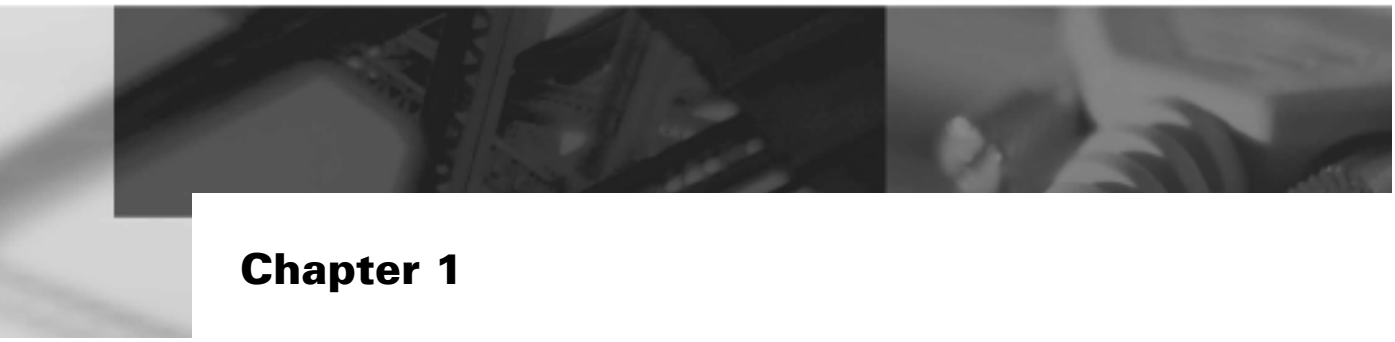
Convention	Purpose
italics	Italics represent file names, directories, host names, and domain names, as in the example "see the */inktomi* directory." Italics also introduce terms, as in the example "the Inktomi *coupled cluster*."
`monospaced face`	Represents commands, as in the example, "use the `reconfigure` command." File content and computer output also appear in a monospaced face.
`monospaced bold`	Represents commands that you should enter literally, as in the example, type **`logclean -m`**
`monospaced italic`	Represents variables for which you should substitute a value, as in the example, "enter a *`filename`*."
brackets []	In command syntax, brackets enclose optional command arguments, as in the example **`add`** ***`pathname`*** [*`size`*]
vertical bar |	In command syntax, vertical bars separate value options.

This manual also presents installation command syntax and coding examples in a monospaced font, offset in shaded tables.

Here is an example of a UNIX command line:

Example

```
cd /export/home/inktomi
```



Chapter 1

Before Installing Traffic Server

This chapter helps you prepare to install Traffic Server.

Before you install Traffic Server, decide which type of installation you want to perform, then gather the information required for that installation. *Use the configuration worksheet at the end of this book to help you plan your Traffic Server installation*.

This chapter covers the following topics:

Before you begin

Before you begin installing Traffic Server, be sure that you have the information and materials described here.

What you need to know

You should understand clearly what combination of Traffic Server's features your deployment will use, to correctly answer prompts during installation. Among the possibilities are forward, reverse, transparent, and explicit proxy caching. See the *Traffic Server Traffic Server Administrator's Guide* for explanations of these features.

Information to prepare

Prepare this information about your system and network:

- ✔ hostname
- ✔ fully qualified domain name (FQDN)
- ✔ IP address(es)
- ✔ netmask
- ✔ broadcast address
- ✔ nameserver IP address(es)
- ✔ default gateway IP address

Background information for installation

The rest of this chapter tells you what you should know before you install:

- ✔ *Reviewing your network design, on page 17*
- ✔ *System requirements, on page 18*
- ✔ *Understanding Traffic Server installation types, on page 21*
- ✔ *What the installer prompts you to do, on page 23*

What you need to have

To install Traffic Server you must have:

- ✔ root privileges on your target nodes
- ✔ network access so that your system can download software over FTP

Reviewing your network design

Before you install Traffic Server, it's a good idea to review the state of your network, using diagnostic tools like `snoop` and `tcpdump`. Base your investigation on questions like these:

- ✔ how will traffic get to Traffic Server?
- ✔ how many clients will the deployment serve, and at what bitrate–and can the network deliver the total bandwidth required?

One common network problem that is very damaging to proxy cache performance, *mode select mismatch*, is described in the next section.

Preparing network interfaces

Every network interface, whether on a computer, a router, or any other of hardware, can operate at different speeds and in different modes. Speed is measured in baud rate, and there are several speeds. There are two modes: half-duplex and full-duplex.

Avoiding mode select mismatch

Every network interface communicates with some other interface at the opposite end of a *link*. If the two interfaces are set to different *speeds*, a speed mismatch occurs, breaking the link in both directions. If two interfaces are operating in different *modes*, they are suffering from a disabling *mode select mismatch*. In a mode select mismatch, a link can function, but performance over the link is impaired. This makes mode select mismatch hard to detect.

How does mode select mismatch happen? The answer lies in the way interface speed and mode are set.

You can set the speed and mode of a network interface *explicitly*. Or, you can direct the interface to *autoconfigure*. An autoconfiguring interface senses the speed of the interface at the opposite end of a link, and sets itself accordingly. It cannot, however, sense the mode of the other interface, although it can *negotiate* with the other interface, so that the two interfaces agree on a mode.

When one interface is set explictly, but the other interface is set to autoconfigure, a mismatch can occur, as an autoconfiguring interface sets itself to half duplex in an attempt to negotiate with a non-negotiating explicitly-set interface.

For more information about mode select mismatch visit the Tech Notes section of Inktomi's Technical support website:

`http://support.inktomi.com/`

System requirements

Before installing Inktomi Traffic Server, ensure that your target IRIX installation node meets the minimum requirements documented in this table:

Component	Requirement
CPU	SGI MIPS
Physical Memory (RAM)	256 MB (use of more than one cache disk requires more RAM)
Operating System	IRIX 6.5.6
Disks for cache	Minimum 1 raw disk device (in addition to the disk where the operating system resides); 6 to 8 recommended for maximum performance
Network interfaces	100 MB Ethernet (two or more interfaces for clustered configuration)

Check the *Release Notes* for more information.

The rest of this section describes how to prepare your SGI IRIX node for Traffic Server installation:

✔ *Using disk partition 7 for the cache, on page 18*

✔ *Preparing cache disks, on page 18*

✔ *Creating a non-privileged user account, on page 19*

✔ *Installing SNMP on your SGI IRIX node, on page 19*

✔ *Preparing to install a Traffic Server cluster, on page 19*

Using disk partition 7 for the cache

You must use disk partition 7 for the cache. You must prepare the disk using the IRIX `fx` utility before installation.

▼ To create partition 7 on a disk

1. Create a script file fx.script with this entry:

   ```
   dks0d2s0 standard option
   ```

2. Execute this command:

   ```
   fx -s fx.script -x
   ```

3. Verify that you have correctly partitioned the disk with this command:

   ```
   prtvtoc dks0d2vol
   ```

   Your partitions should look something like this:

   ```
   * /dev/rdsk/dks0d2vol (bootfile "/unix")
   * 512 bytes/sector
   Partition  Type    Fs  Start: sec Size: sec  Mount Directory
   7          xfs     yes 4096       8884447
   8          volhdr      0          4096
   10         volume      0          8888543
   ```

Preparing cache disks

Traffic Server's cache must be installed on raw disks without partitions. If your system's disks have got partitions on them, follow the procedure below to remove the partitions *from the disks you intend to use for the Traffic Server cache*.

▼ To prepare cache disks:

1. Log in as `root`.
2. Use the `umount` command to unmount the disks you plan to use for the cache.
3. Comment out any lines in the `/etc/fstab` file that refer to these disks.
4. Run `/sbin/fdisk` on the unmounted disks.
5. Within `fdisk`, enter the command `d` to delete all partitions
6. Then (still within `fdisk`) enter the command `w` to commit the changes.

Warning Do not to run `fdisk` against a system partition, or data can be erased. Use

```
/sbin/fdisk [/dev/xxx]
```

only where `xxx` is the name of a non-system disk.

Creating a non-privileged user account

The installer automatically creates a user account for you during installation—the default account is `inktomi`— but you may want to create an account ahead of time. You need to designate a non-privileged user account for Traffic Server operation on each target node.

▼ To create a user account on your target installation node:

1. Log in as `root`.
2. Use the `addUserAccount` command to add a new account.

Here is an example of `addUserAccount` syntax:

```
/usr/sysadmin/privbin/addUserAccount -l -u 10001 -g 10 -C-H /export/home/
your_account
```

For more information on creating user accounts, see your system's `useradd(8)` man page for more options.

Installing SNMP on your SGI IRIX node

SNMP (Simple Network Management Protocol) is a standard protocol for managing everything in your network environment. The installer sets up `init.d` scripts for SNMP, but the administrator must fully configure or disable SNMP after installation through the Traffic Manager U I.

You must install the SGI SNMP distribution, or `eoe.sw.netman`, before installing Traffic Server. You can locate it on the SGI IRIX Foundation media.

SNMP only supports version 1 requests.

You must configure both the SGI SNMP master agent and the SNMP Research master agent to perform security checks and access control. You configure the SGI SNMP to perform access control by editing the `etc/snmpd.auth` configuration file.

See the *Traffic Server Administrator's Guide* for more information on the Traffic Server implementation of SNMP.

Preparing to install a Traffic Server cluster

A Traffic Server management cluster provides centralized administration by multicasting configuration messages to all of its nodes at once. This is what happens when an administrator configures the cluster through Traffic Manager, Traffic Server's browser-based user interface.

To correctly install a Traffic Server cluster, *you must have a multicast route in the routing table of each node*. If the multicast route is not present, plan to add it during Traffic Server installation. Assign a

multicast group address anywhere in the address range between 224.0.1.27 and 224.0.1.254, inclusive. Traffic Server's default multicast group address is 224.0.1.37.

Testing for a multicast route

Enter this command to see if you have a multicast route in the routing table:

```
netstat -rn
```

Multiple network interfaces are required for cluster nodes. During installation you designate a *cluster interface*, dedicating one network interface to intra-cluster communication. The installer automatically adds a default route for multicast traffic through the IP address of the chosen cluster interface.

Note The cluster interface is not used for network communication with HTTP or NNTP clients and servers.

Traffic Server clusters must be homogeneous

If you install a Traffic Server cluster, *you must configure all the nodes identically.* You cannot mix and match nodes of differing platforms, using different operating systems, different versions of the same operating system, different operating system patches, or different versions of Traffic Server. The username under which you install Traffic Server must be identical for all nodes in the cluster.

Traffic Server clusters and virtual IP failover

If you plan to install a Traffic Server cluster, decide whether your deployment should use virtual IP failover, as described in the *Traffic Server Administrator's Guide*. This feature involves configuration which you should be aware of when planning Traffic Server installation.

Understanding Traffic Server installation types

Before beginning Traffic Server installation, choose the type of installation you want to perform. There are five types of Traffic Server installation:

- ✔ First-time single-node installation
- ✔ First-time cluster installation
- ✔ Upgrade
- ✔ Reinstall
- ✔ Uninstall

First-time single-node installation When you install Traffic Server for the first time, you create a user account, decide where to install Traffic Server on your system, select a destination directory for logging, and make basic configuration decisions.

First-time cluster installation When you install a Traffic Server cluster, you choose:

- ✔ a name of your cluster
- ✔ a network interface for cluster communication, and
- ✔ a multicast address for cluster communication.

When configured properly, the nodes will recognize one another and form a cluster automatically.

Upgrade When you upgrade Traffic Server, the installer retains all of the configuration selections from your existing version of Traffic Server.

Reinstall When you reinstall Traffic Server, you replace an older version with a newer version, either using the directories you created during your previous installation of Traffic Server or choosing new ones. You might replace your Traffic Server to make major configuration changes, replace corrupted software, or correct a bad configuration. If you have a previous version of Traffic Server on your machine, you do not need to delete it.

Uninstall When you uninstall Traffic Server, you remove Traffic Server from your system.

Installation types and the organization of this book

This book has a chapter for each first-time installation scenario:

- ✔ *Installing Traffic Server on a single node, on page 29*
- ✔ *Installing Traffic Server in a cluster, on page 33*

These are followed by a chapter about upgrading and reinstalling Traffic Server:

- ✔ *Upgrading, reinstalling, and uninstalling Traffic Server, on page 39*

These chapters are followed by a description of things you may want to do after installation, *After Installing Traffic Server, on page 49*.

What to expect during Traffic Server installation

To install Traffic Server, you run a script called the *installer*, which is included in the Traffic Server software package. The installer first prompts you for configuration choices in an interactive dialog, then configures your system using the settings you've given it.

The installer prompts you to set, or choose between settings of, configuration parameters. Your network environment and deployment plans determine your choices. Many prompts include default answers, which are identified by square brackets following a question. To accept a default answer, press **Return**; otherwise, respond as appropriate. You can interrupt the installation at any time by typing **control-C (^C)**.

After taking you through its interactive dialog, the installer configures your system by:

- ✔ Copying Traffic Server files to the directories you specified.
- ✔ Changing ownership of devices.
- ✔ Modifying system files according to the information you entered during the interactive dialog.
- ✔ Creating a log file called `TSinstall.log` which is a transcript of the installation session.

For more information on what the installer modifies and installs, see *Appendix A, UNIX Installation File Hierarchy*.

The following table shows where to find information about what the installation script prompts you to do.

To find out about…	See…
Setting an install directory	*page 23*
Setting a logging path	*page 23*
Deciding whether to install a Traffic Server cluster	*page 23*
Setting a name for your Traffic Server cluster	*page 24*
Setting the cluster interface	*page 24*
Setting the multicast address for cluster communication	*page 24*
Setting up Traffic Server as a reverse proxy	*page 24*
Setting Traffic Server port assignments	*page 25*
Setting up Traffic Server to serve requests transparently	*page 25*
Setting up Traffic Server to proxy NNTP	*page 25*
Setting an administrator mail address	*page 26*
Setting the Traffic Server administrator user name and password	*page 26*
Configuring the Traffic Server cache	*page 26*

If you want to make configuration changes after installation, use the Traffic Manager User Interface or Traffic Line. See the *Traffic Server Administrator's Guide* for more information.

What the installer prompts you to do

During installation, the installer prompts you to set, or choose between settings of, the configuration parameters described in this section.

Setting an install directory

The installer creates an *install directory*, in which it places Traffic Server's operating software.

By default, the install directory is named for the version of Traffic Server you are installing, and goes in the home directory of user `inktomi`. If the home directories on your system are located in `/home/`, for example, and you install Traffic Server 4.0.14, the install directory will be:

```
/home/inktomi/4.0.14/
```

In this book, any directory location not preceded by a slash (`/`) is assumed to be relative to Traffic Server's install directory. Continuing our example, the full path for Traffic Server's `bin` directory will be:

```
/home/inktomi/4.0.14/bin/
```

The installer prompts you to accept or change the default install directory location. If you change this setting, choose a location with at least 100 MB of space available.

Creating an install directory

If the directory you specify does not exist, the installer asks you if you would like to create one. If you do not wish to create a new directory, the installer prompts you to choose a different directory.

Creating a user account

If you have not created the user account for Traffic Server (the default account selected by the installation script is `inktomi`), the installer prompts you to do so.

The installer saves the installation path in `/etc/traffic_server`.

Setting a logging path

The installer prompts you for the location where you want Traffic Server to store activity logs, called the *logging path*.

By default, the logging path goes in the install directory. For instance, if your install directory is `/home/inktomi/4.0.14/`, the logging path will be:

```
/home/inktomi/4.0.14/logs
```

The logging path and the install directory can not be the same.

2 GB is the default value for the maximum amount of space Traffic Server will fill with log files. Inktomi recommends that you make your log directory a separately mounted filesystem, since logging is an active process that requires a lot of space.

The installer prompts you to accept or change the default logging path.

Cluster logging paths

If you install a Traffic Server cluster, the logging paths must be the same on all nodes in the cluster. In fact, all nodes in the cluster must be configured identically in every respect.

Creating a logging path

If the directory you specify does not exist, the installer asks you if you would like to create one. If you do not wish to create a new directory, the installer prompts you to choose a different directory.

You may choose logging options after installation. For more information on logging, see the *Traffic Server Administrator's Guide*.

Deciding whether to install a Traffic Server cluster

The installer prompts you to decide whether to install a Traffic Server cluster. If you say yes, you are prompted to do these three things:

✔ Enter the cluster name for the Traffic Server cluster to which you are adding the present node.

✔ Select a network interface for communication within the cluster.

✔ Enter the multicast address for cluster communications.

These three prompts are explained in detail in the next few pages.

If you choose *not* to install a Traffic Server cluster, your next prompt from the installer is *Setting up Traffic Server as a reverse proxy, on page 24*.

Setting a name for your Traffic Server cluster

The installer prompts you for a cluster name, which can be any convenient identifier, since it is only for internal Traffic Server cluster configuration and administration, and is invisible outside that realm.

Traffic Server cluster names must:

✔ be the same for all nodes in a given cluster

✔ use only alphanumeric US ASCII characters

Setting the cluster interface

Multiple network interfaces are required for cluster nodes. The installer prompts you to designate a *cluster interface*, dedicating one network interface to intra-cluster communication. The installer automatically adds a default route for multicast traffic through the IP address of the chosen cluster interface.

Note The cluster interface is not used for network communication with HTTP or NNTP clients and servers.

Setting the multicast address for cluster communication

A Traffic Server management cluster provides centralized administration by multicasting configuration messages to all of its nodes at once. This is what happens when an administrator configures the cluster through Traffic Server's browser-based user interface.

The installer prompts you to assign a multicast address for communication within the cluster, over the cluster interface selected in the previous step. The multicast address can be anywhere in the address range between 224.0.1.27 and 224.0.1.254, inclusive. Traffic Server's default multicast address for cluster communication is 224.0.1.37. The installer calls this the *multicast group address*.

The installer automatically adds a default route for multicast traffic through the IP address of the dedicated cluster interface.

Setting up Traffic Server as a reverse proxy

Traffic Server can function as a *reverse proxy*, or *web server accelerator*. In a reverse proxy deployment, Traffic Server receives all HTTP requests intended for, and serves the requested content on behalf of, a web server or group of web servers.

The installer prompts you to decide whether to configure Traffic Server as a reverse proxy for HTTP. If you say yes, the installer sets the Traffic Server Proxy Port to port 80, because, as a reverse proxy, Traffic Server must normally be able to receive HTTP traffic on port 80.

Important Setting Traffic Server's Proxy Port to port 80 *is only part* of the configuration required to perform reverse proxy. Further configuration is required to enable Traffic Server to perform reverse proxy. See the *Traffic Server Administrator's Guide* for a complete description of reverse proxy configuration.

Setting Traffic Server port assignments

The installer prompts you to enter a starting port number for the 11 ports that Traffic Server uses. The installer displays a numbered list of the ports based on your selections, informs you if it has found any conflicts, and prompts you to accept the list as it stands or make changes.

This table defines the Traffic Server communications ports, and lists the default setting for each port:

Port	Description	Default setting
Traffic Server Proxy Port	Port for Traffic Server to use in acting as a network proxy for web traffic, or when serving web traffic transparently.	8080
Web Administration Port	The port to which you connect the web server that runs the Traffic Manager UI.	8081
Overseer Port	The port from which the Traffic Manager UI receives data for plotting real-time charts.	8082
Auto-config Port	The port to which the browser connects to get configuration information. You can write a Proxy Auto Configuration (PAC) script that will automatically connect to this port.	8083
Process Manager Port	Process manager port.	8084
Logging Server Port	Port to which all clustered nodes send log collation information.	8085
Clustering Port	Cluster communication port. Port used in cache clustering for sending, receiving, controlling and caching object data.	8086
Reliable Service Port	Cluster communication port. Port which Traffic Managers running on different nodes use to communicate configuration information to one another.	8088
Multicast Port	Cluster communication port. The port at which the node listens for cluster configuration instructions from the Traffic Manager. You must set this port identically for every node in a cluster.	8089
SNMP Encapsulation Port	The port on which the Traffic Server SNMP agent responds to requests from SNMP managers and sends SNMP traps.	8090

Setting up Traffic Server to serve requests transparently

Transparency is an option that allows Traffic Server to perform proxy caching without requiring end users to explicitly configure their browsers to use Traffic Server as a proxy. Traffic Server supports transparency for HTTP (port 80) and NNTP (port 119) traffic only.

Traffic Server's Adaptive Redirection Module (ARM) must be installed for transparency to be enabled. The installer prompts you to decide whether to install ARM. Say yes if you want to enable transparency. If your node has more than one network interface, the installer prompts you to choose which interface should receive client traffic.

Besides Traffic Server with ARM installed, a transparent deployment must also have a transparency device in the network. See *Chapter 8, Serving Traffic Transparently* for details.

Saying no to enabling WCCP

If you choose to install ARM, the installer then prompts you to decide whether to enable WCCP (Web Cache Control Protocol). Traffic Server 4.0.14 for IRIX does not support WCCP; answer no to this question.

Setting an administrator mail address

The installer prompts you for an email address to which Traffic Server can send system warnings. You can change this setting after installation by using the Traffic Server UI.

For more about system warnings, see the *Traffic Server Administrator's Guide*.

Setting the Traffic Server administrator user name and password

The installer prompts you for a user name and password for the Traffic Manager UI and Traffic Line, Traffic Server's command-line interface. The installer encrypts the passwords and stores them in the `records.config` file, in Traffic Server's `config` directory.

This user name and password apply *only to the Traffic Manager UI and Traffic Line*. They have no relationship to UNIX user privileges or password security.

Note Traffic Server processes do not run as root. For more about Traffic Server processes, see the *Traffic Server Administrator's Guide*.

For more about the Traffic Manager browser and about Traffic Line, see the *Traffic Server Administrator's Guide*.

Configuring the Traffic Server cache

Traffic Server acts as a proxy for end user requests, obtaining web objects and news articles from HTTP and NNTP origin servers, then serving them to end users while storing the content in its cache. Traffic Server then serves subsequent requests from the cache, without pulling the content from the origin servers.

In a first-time install of Traffic Server, the installer prompts you to allocate disk resources for the cache, displaying a list of disk drives, along with instructions for making selections.

Once you are satisfied with your selections, quit the disk drive selection process. At this point, the installer automatically configures your cache and proceeds to configure your system.

Important Do not interrupt the cache configuration during installation, or you will be forced to reinstall Traffic Server before you can use the cache.

Other scenarios during and after installation

This section explains several scenarios other than simple installation.

Making configuration changes after installation

If you want to make configuration changes after installation, use the Traffic Manager User Interface or Traffic Line. See the *Traffic Server Administrator's Guide* for more information.

Quitting while installation is underway

If you quit while installation is underway, the installer removes all files that it has installed on your system. If this happens during an upgrade, the installer removes those files and then reverts to the previously installed version of Traffic Server.

Uninstalling Traffic Server

When you uninstall Traffic Server, the installer removes all files that it installed on your system *except* the cache files and the files created by the program logging files. The installer marks these files for deletion. Your system removes these files upon reboot. No further action is required.

Note Always reboot your machine after uninstalling Traffic Server.

Upgrading an existing cache

After an upgrade, Traffic Server examines your existing cache to determine if the content is compatible with the new version. If the old and new cache are compatible, Traffic Server incorporates the old content into the new cache. Otherwise Traffic Server clears the cache while running temporarily in proxy-only mode.

If you are running a Traffic Server released prior to version 2.0, your cache is incompatible with the current release of Traffic Server as well as all versions of Traffic Server released after version 2.0.

Chapter 2

Installing Traffic Server on a single node

This chapter describes how to install Traffic Server on a single IRIX node.

If you are not installing for the first time on your target node, see *Upgrading, reinstalling, and uninstalling Traffic Server, on page 39*.

The chapter assumes that you have collected the information required for Traffic Server installation. See *Before you begin, on page 16*.

This chapter contains one section**:**

Installing Traffic Server

You install Traffic Server from the Inktomi website.

Traffic Server installation can be described as a five-part process:

- ✗ Starting the installer
- ✗ Configuring the Traffic Server environment
- ✗ Establishing Traffic Server in the network
- ✗ Setting up your administrator account
- ✗ Configuring the Traffic Server cache

The installer makes no distinction between these parts. This chapter just breaks Traffic Server installation into parts for the sake of clearer explanation.

Part 1: Starting the installer

1. Log in as `root`.
2. Download the Traffic Server package from the Inktomi website.
3. Uncompress the Traffic Server package, using the `gunzip` command.
4. Untar the uncompressed Traffic Server package, using the `tar -xvf` command. This creates a directory with the name of the package you are installing from, for example `4.0.14`.
5. `cd` into the directory that was created in the previous step.
6. Run this command:

   ```
   ls -al
   ```

   You should see this file structure:

   ```
   -rwxrwxr-x    1 inktomi  user         195357 Mar  9 17:47 install.sh*
   -rw-rw-r--    1 inktomi  user      186531840 Mar  9 17:48 irix.tar
   -rw-rw-r--    1 inktomi  user        1658880 Mar  9 17:48 irixarm.tar
   -rw-rw-r--    1 inktomi  user         532480 Mar  9 17:48 irixinst.tar
   -rw-rw-r--    1 inktomi  user        2488320 Mar  9 17:48 traffic.tar
   ```

   Notice the file `install.sh`, which is the installer script.
7. Run the executable `install.sh` to start the installation procedure:

   ```
   ./install.sh
   ```

Part 2: Configuring the Traffic Server environment

The installer prompts you to decide on separate locations for Traffic Server operating software and Traffic Server log files.

▼ To configure Traffic Server's environment:

1. Enter the full path of the directory in which to install Traffic Server.
2. Enter the full path of the directory in which to store Traffic Server log files.

Part 3: Establishing Traffic Server in the network

The installer prompts you for the network parameters which determine how Traffic Server responds to client traffic.

Note If your node has more than one network interface, the installer prompts you to choose which interface Traffic Server should use to communicate with end users and origin servers.

▼ To establish Traffic Server in the network:

1. Choose **N** when the installer asks if you are installing a cluster.
   If Traffic Server detects only one network interface, you will not see this question.
2. Choose whether to configure Traffic Server as a reverse proxy cache (sometimes called a web server accelerator).
   If you choose yes, the installer sets the Traffic Server Proxy Port to port 80.
3. Enter the starting port number for the 11 ports Traffic Server uses on your node (the default is 8080).
4. The installer displays a numbered list of the port selections you have made, informs you if it has found any conflicts, and prompts you to accept the list as it stands or make changes, using the commands in this table:

Command	Description
1-10, S	Changes the corresponding port number. Enter the number from the list that corresponds to the port assignment you would like to change, then enter a new port assignment. The SNMP Encapsulation Port is designated port S.
0	Accepts the displayed choices and quits Traffic Server port configuration
I	Ignores warnings and quits Traffic Server port configuration.
h	Display the command list again.
N	Chooses a new base port assignment.

Note The `I` option only appears if there is a port conflict.

5. Choose whether to install the Adaptive Redirection Module (ARM).

Important You must install ARM if you want to configure Traffic Server for transparency. For more information about transparency and ARM, see *Serving Traffic Transparently, on page 55*.

If you choose to install ARM:

- ✗ If your node has two or more network interfaces, the installer prompts you to choose an interface to which ARM should redirect incoming traffic.
- ✗ The installer asks whether to enable WCCP. Say no, because WCCP is not supported by Traffic Server 4.0.14 for IRIX.
- ✗ The installer asks whether Traffic Server should proxy NNTP. See the *Traffic Server Administrator's Guide* for more information about NNTP.

Part 4: Setting up your administrator account

The installer prompts you to specify an address to which Traffic Server can send system warnings as email messages; and to specify a user name and password for administrative use with Traffic Manager and Traffic Line.

Warning Do not use the hash symbol(#) in your user name or password.

▼ To set up your administrator account:

1. Enter the Traffic Server administrator email account.
2. Enter the Traffic Server administrator name.
3. Enter and confirm the Traffic Server administrator password.

Part 5: Configuring the Traffic Server cache

The installer checks for disks suitable for the cache—disks that have no mounted filesystems or secondary swap partitions—and prompts you to allocate disk space for the cache from a list of those disks.

Important The space you allocate for the cache cannot be used for any other purpose.

▼ To configure the Traffic Server cache:

1. Choose the disk resources to use for the cache from the installer's numbered list of available disk drives and options.

   Use the commands in this table to make and modify your selections as necessary:

Command	Description
a	Add a cache storage location
r	Remove a cache storage location
s	Select all cache storage locations
d	End disk drive selection and continue Traffic Server installation
q	Quit Traffic Server installation process immediately

   After each command that you enter (except for `d` or `q`), the installer displays an updated list of your choice of disk drives.

Important Carefully examine the suggested list of selected disk drives to verify that the installer has chosen the correct devices.

2. Continue this process until you have allocated your disk resources.
3. Type `d` to end the disk drive selection and continue Traffic Server installation.

   The installer displays your final choices of disk drives for cache storage, proceeds to install Traffic Server files, and then configures the cache.

Warning Do not interrupt cache configuration, or you will render your cache unusable.

When the installer has finished this process, installation ends. The installer displays the appropriate variant of this message:

```
Your Traffic Server 4.0.14 installation is complete.
Please reboot this system before starting Traffic Server.
To start Traffic Server, login as inktomi and enter the command
  start_traffic_server
A log file of this installation process has been written to
/home/inktomi/TSinstall.log
Please consult the Traffic Server Installation Guide for full
operating information.
```

For more information about what to do when installation is complete, see *After Installing Traffic Server, on page 49*.

Chapter 3

Installing Traffic Server in a cluster

This chapter describes how to install a Traffic Server cluster on a group of IRIX systems.

If you are upgrading or reinstalling Traffic Server, rather than installing for the first time, see *Upgrading, reinstalling, and uninstalling Traffic Server, on page 39*.

The chapter assumes that you have collected the information required for Traffic Server installation. See *Before you begin, on page 16*.

This chapter contains one section**:**

Installing Traffic Server

You install a Traffic Server cluster one host node at a time from Inktomi website. Perform the instructions in this chapter on each node in turn.

Traffic Server installation can be described as a five-part process:

- ✗ Starting the installer
- ✗ Configuring the Traffic Server environment
- ✗ Establishing Traffic Server in the network
- ✗ Setting up your administrator account
- ✗ Configuring the Traffic Server cache

The installer makes no distinction between these parts. This chapter just breaks Traffic Server installation into parts for the sake of clearer explanation.

Part 1: Starting the installer

1. Log in as `root`.
2. Download the Traffic Server package from the Inktomi website.
3. Uncompress the Traffic Server package, using the `gunzip` command.
4. Untar the uncompressed Traffic Server package, using the `tar -xvf` command. This creates a directory with the name of the package you are installing from, for example `4.0.14`.
5. `cd` into the directory that was created in the previous step.
6. Run this command:

   ```
   ls -al
   ```

   You should see this file structure:

   ```
   -rwxrwxr-x    1 inktomi  user         195357 Mar  9 17:47 install.sh*
   -rw-rw-r--    1 inktomi  user      186531840 Mar  9 17:48 irix.tar
   -rw-rw-r--    1 inktomi  user        1658880 Mar  9 17:48 irixarm.tar
   -rw-rw-r--    1 inktomi  user         532480 Mar  9 17:48 irixinst.tar
   -rw-rw-r--    1 inktomi  user        2488320 Mar  9 17:48 traffic.tar
   ```

   Notice the file `install.sh`, which is the installer script.
7. Run the executable `install.sh` to start the installation procedure:

   ```
   ./install.sh
   ```

Part 2: Configuring the Traffic Server environment

The installer prompts you to decide on separate locations for Traffic Server operating software and Traffic Server log files.

Note If your node has more than one network interface, the installer prompts you to choose which interface Traffic Server should use to communicate with end users and origin servers.

▼ To configure the Traffic Server environment:

1. Enter the full path of the directory in which to install Traffic Server.
2. Enter the full path of the directory in which to store Traffic Server log files.

Part 3: Establishing Traffic Server in the network

The installer prompts you for the network parameters which determine how Traffic Server responds to client traffic.

Note If your node has more than one network interface, the installer prompts you to choose which interface Traffic Server should use to communicate with end users and origin servers.

▼ To establish Traffic Server in the network:

1. The installer asks if you are installing a cluster. Choose **Y** to install a cluster.
2. Enter the cluster name for the Traffic Server cluster to which you are adding this node.
3. Select a network interface for communication within the cluster.
4. Enter the multicast group address for cluster communications.
5. Choose whether to configure Traffic Server as a reverse proxy cache (sometimes called a web server accelerator).
   If you choose yes, the installer sets the Traffic Server Proxy Port to port 80.
6. Enter the starting port number for the 11 ports Traffic Server uses on your node (the default is 8080).
7. The installer displays a numbered list of the port selections you have made, informs you if it has found any conflicts, and prompts you to accept the list as it stands or make changes, using the commands in this table:

Command	Description
1-10, S	Changes the corresponding port number. Enter the number from the list that corresponds to the port assignment you would like to change, then enter a new port assignment. The SNMP Encapsulation Port is designated port S.
0	Accepts the displayed choices and quits Traffic Server port configuration
I	Ignores warnings and quits Traffic Server port configuration.
h	Display the command list again.
N	Chooses a new base port assignment.

Note The `I` option only appears if there is a port conflict.

8. Choose whether to install the Adaptive Redirection Module (ARM).

Important You must install ARM if you want to configure Traffic Server for transparency. For more information about transparency and ARM, see *Serving Traffic Transparently, on page 55*.

If you choose to install ARM:

- ✗ If your node has two or more network interfaces, the installer prompts you to choose an interface to which ARM should redirect incoming traffic.
- ✗ The installer asks whether to enable WCCP. Say no, because WCCP is not supported by Traffic Server 4.0.14 for IRIX.
- ✗ The installer asks whether Traffic Server should proxy NNTP. See the *Traffic Server Administrator's Guide* for more information about NNTP.

Part 4: Setting up your administrator account

The installer prompts you to specify an address to which Traffic Server can send system warnings as email messages; and to specify a user name and password for administrative use with Traffic Manager and Traffic Line.

Warning Do not use the hash symbol(#) in your user name or password.

▼ To set up your administrator account:

1. Enter the Traffic Server administrator email account.
2. Enter the Traffic Server administrator name.
3. Enter and confirm the Traffic Server administrator password.

Part 5: Configuring the Traffic Server cache

The installer checks for disks suitable for the cache—disks that have no mounted filesystems or secondary swap partitions—and prompts you to allocate disk space for the cache from a list of those disks.

Important The space you allocate for the cache cannot be used for any other purpose.

▼ To configure the Traffic Server cache:

1. Choose the disk resources to use for the cache from the installer's numbered list of available disk drives and options.

   Use the commands in this table to make and modify your selections as necessary:

Command	Description
a	Add a cache storage location
r	Remove a cache storage location
s	Select all cache storage locations
d	End disk drive selection and continue Traffic Server installation
q	Quit Traffic Server installation process immediately

   After each command that you enter (except for `d` or `q`), the installer displays an updated list of your choice of disk drives.

Important Carefully examine the suggested list of selected disk drives to verify that the installer has chosen the correct devices.

2. Continue this process until you have allocated your disk resources.
3. Type `d` to end the disk drive selection and continue Traffic Server installation.

   The installer displays your final choices of disk drives for cache storage, proceeds to install Traffic Server files, and then configures the cache.

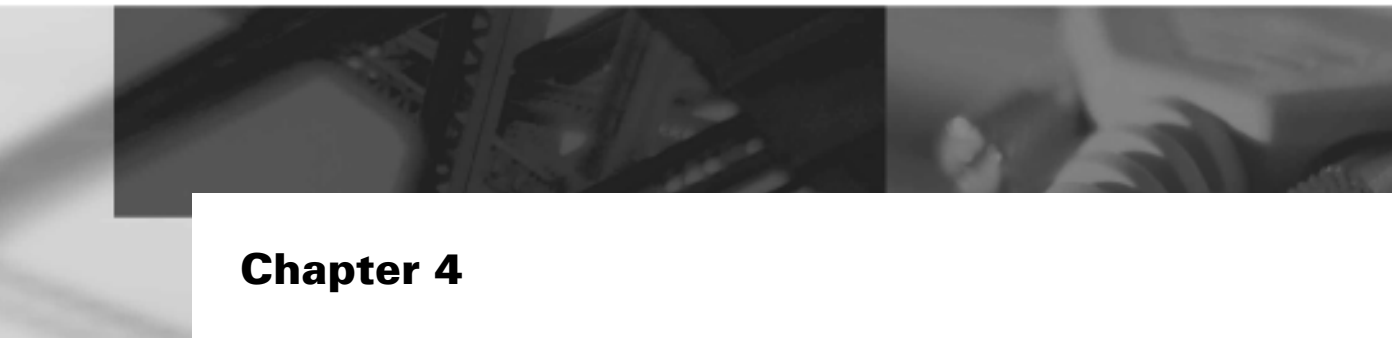
Warning Do not interrupt cache configuration, or you will render your cache unusable.

When the installer has finished this process, installation ends. The installer displays the appropriate variant of this message:

```
Your Traffic Server 4.0.14 installation is complete.
Please reboot this system before starting Traffic Server.
To start Traffic Server, login as inktomi and enter the command
  start_traffic_server
A log file of this installation process has been written to
```

```
/home/inktomi/TSinstall.log
Please consult the Traffic Server Installation Guide for full
operating information.
```

For more information about what to do when installation is complete, see *After Installing Traffic Server, on page 49*.



Chapter 4

Upgrading, reinstalling, and uninstalling Traffic Server

You can upgrade, reinstall, or uninstall Traffic Server on a node where Traffic Server was previously installed.

Upgrade Traffic Server if you want to retain the configuration of your existing version of Traffic Server, while replacing an older version of Traffic Server with a newer version.

Reinstall Traffic Server to make major configuration changes, to replace corrupted software, or to correct a bad configuration.

Uninstall Traffic Server if you are preparing to install Traffic Server Media-IXT, which is Traffic Server with a plugin for proxy caching of streaming media.

This chapter covers these topics:

Preparing for an upgrade

Normally, you need not perform any special tasks to prepare your Traffic Server node for an upgrade. This section describes the few exceptions to this rule. Whether or not they apply to your situation, remember that an existing Traffic Server is unavailable during upgrade or reinstall.

Upgrading early versions of Traffic Server

The Upgrade option is available for existing Traffic Server 3.0.x or later installations. To upgrade an earlier version of Traffic Server, use the Reinstall option.

Upgrading can overwrite some configuration files

When you upgrade to the 4.0 release of Traffic Server, the installer overwrites some configuration files with their defaults.

Workaround Before upgrading, back up the affected files; after upgrading, replace the new (default) versions of the files with the backups you have made.

When upgrading to Traffic Server version 4.0:

- ✔ from any version of Traffic Server, back up and migrate the `/body_factory/` directory structure.
- ✔ from Traffic Server 3.5.4, back up and migrate the `arm_security.config` file.
- ✔ from Traffic Server 4.0, back up and migrate the hosting.config, arm_security.config, and ftp_remap.config files.

Upgrading Traffic Server

When you upgrade Traffic Server, the installer retains all of the configuration selections from your existing version of Traffic Server. The installer examines Traffic Server configuration files, enabling it to differentiate between single node and clustered Traffic Server installations. All you need to do during an upgrade is choose your install directory and logging path.

For details on information required to complete any of the steps, see the section, *What to expect during Traffic Server installation, on page 22*.

Upgrading Traffic Server

▼ To upgrade Traffic Server:

1. Log in as `root`.
2. Download the Traffic Server package from the Inktomi website.
3. Uncompress the Traffic Server package, using the `gunzip` command.
4. Untar the uncompressed Traffic Server package, using the `tar -xvf` command. This creates a directory with the name of the package you are installing from, for example `4.0.14`.
5. `cd` into the directory that was created in the previous step.
6. Run this command:

   ```
   ls -al
   ```

   You should see this file structure:

   ```
   -rwxrwxr-x    1 inktomi  user         195357 Mar  9 17:47 install.sh*
   -rw-rw-r--    1 inktomi  user      186531840 Mar  9 17:48 irix.tar
   -rw-rw-r--    1 inktomi  user        1658880 Mar  9 17:48 irixarm.tar
   -rw-rw-r--    1 inktomi  user         532480 Mar  9 17:48 irixinst.tar
   -rw-rw-r--    1 inktomi  user        2488320 Mar  9 17:48 traffic.tar
   ```

   Notice the file `install.sh`, which is the installer script.
7. Run the executable `install.sh` to start the installation procedure:

   ```
   ./install.sh
   ```

   The installer detects a previous installation of Traffic Server on your system, and gives you several options:

Command	Description
U	Upgrades Traffic Server
R	Reinstalls Traffic Server
Q	Quits installing Traffic Server
?	Gives you more information about the installation options

8. Select **U** to upgrade this installation.

   The installer uses your existing user account and stops any Traffic Server processes.
9. Enter the full path of the directory in which to install Traffic Server.
10. Enter the full path of the directory in which to store Traffic Server log files.

    This ends the installation upgrade dialog. The installer now installs the Traffic Server files, and maintains your cache configuration choices while clearing your existing cache.

Warning *Do not interrupt cache configuration, or you will render your cache unusable.*

The installer copies your old configuration files to the new configuration directory and deletes obsolete files.

11 Start your Traffic Server. See *Starting Traffic Server, on page 50*.

Reinstalling Traffic Server on a single node

Reinstalling replaces an older version of Traffic Server with a newer version. A reinstall retains *only the existing user account* from your current Traffic Server; *all other configuration information is replaced*. You might reinstall your Traffic Server to make major configuration changes, replace corrupted software, or correct a bad configuration.

You reinstall Traffic Server one host node at a time from the Inktomi website.

For details on information required to complete any of the steps, see the section, *Understanding Traffic Server installation types, on page 21*.

Traffic Server installation can be described as a five-part process, in which the parts are:

- ✗ Starting the installer
- ✗ Configuring the Traffic Server environment
- ✗ Establishing Traffic Server in the network
- ✗ Setting up your administrator account
- ✗ Configuring the Traffic Server cache

You will see no distinction between these parts while installing. This chapter just breaks Traffic Server installation into parts for the sake of clearer explanation.

Part 1: Starting the installer

1. Log in as `root`.
2. Download the Traffic Server package from the Inktomi website.
3. Uncompress the Traffic Server package, using the `gunzip` command.
4. Untar the uncompressed Traffic Server package, using the `tar -xvf` command. This creates a directory with the name of the package you are installing from, for example `4.0.14`.
5. `cd` into the directory that was created in the previous step.
6. Run this command:

   ```
   ls -al
   ```

   You should see this file structure:

   ```
   -rwxrwxr-x    1 inktomi  user         195357 Mar  9 17:47 install.sh*
   -rw-rw-r--    1 inktomi  user      186531840 Mar  9 17:48 irix.tar
   -rw-rw-r--    1 inktomi  user        1658880 Mar  9 17:48 irixarm.tar
   -rw-rw-r--    1 inktomi  user         532480 Mar  9 17:48 irixinst.tar
   -rw-rw-r--    1 inktomi  user        2488320 Mar  9 17:48 traffic.tar
   ```

   Notice the file `install.sh`, which is the installer script.
7. Run the executable `install.sh` to start the installation procedure:

   ```
   ./install.sh
   ```

   The installer detects a previous installation of Traffic Server on your system and gives you several options:

Command	Description
U	Upgrades your Traffic Server

R	Reinstalls your Traffic Server
Q	Quits this installation
?	Gives you more information about the installation options

8 Select **R** to reinstall.

9 The installer prompts you to enter the name of the account you will use to administer Traffic Server. You can use the account which you used before, or choose another one.

10 Complete your installation, following the instructions beginning with *Part 2: Configuring the Traffic Server environment, on page 30*.

Reinstalling a Traffic Server cluster

You install a Traffic Server cluster one host node at a time from the Inktomi website. Perform the instructions in this chapter on each node in turn.

Traffic Server installation can be described as a five-part process, in which the parts are:

- ✗ Starting the installer
- ✗ Configuring the Traffic Server environment
- ✗ Establishing Traffic Server in the network
- ✗ Setting up your administrator account
- ✗ Configuring the Traffic Server cache

You will see no distinction between these parts while installing. This chapter just breaks Traffic Server installation into parts for the sake of clearer explanation.

Part 1: Starting the installer

1. Log in as `root`.
2. Download the Traffic Server package from the Inktomi website.
3. Uncompress the Traffic Server package, using the `gunzip` command.
4. Untar the uncompressed Traffic Server package, using the `tar -xvf` command. This creates a directory with the name of the package you are installing from, for example `4.0.14`.
5. `cd` into the directory that was created in the previous step.
6. Run this command:

   ```
   ls -al
   ```

   You should see this file structure:

   ```
   -rwxrwxr-x    1 inktomi  user         195357 Mar  9 17:47 install.sh*
   -rw-rw-r--    1 inktomi  user      186531840 Mar  9 17:48 irix.tar
   -rw-rw-r--    1 inktomi  user        1658880 Mar  9 17:48 irixarm.tar
   -rw-rw-r--    1 inktomi  user         532480 Mar  9 17:48 irixinst.tar
   -rw-rw-r--    1 inktomi  user        2488320 Mar  9 17:48 traffic.tar
   ```

   Notice the file `install.sh`, which is the installer script.
7. Run the executable `install.sh` to start the installation procedure:

   ```
   ./install.sh
   ```

   The installer detects a previous installation of Traffic Server on your system and gives you several options:

Command	Description
U	Upgrades Traffic Server.
R	Reinstalls Traffic Server.
Q	Quits installing Traffic Server.
?	Gives you more information about the installation options.

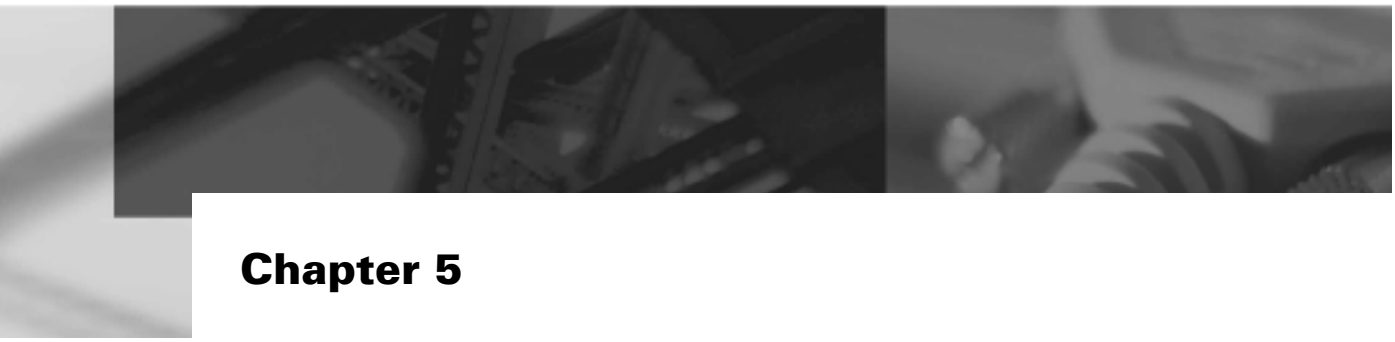
8. Select **R** to reinstall this installation.

9 The installer prompts you to enter the name of the account you will use to administer Traffic Server. You can use the account which you used before, or choose another one.

10 Complete your installation, following the instructions beginning with *Part 2: Configuring the Traffic Server environment, on page 34*.

Uninstalling Traffic Server

Uninstall Traffic Server to remove Traffic Server from your SGI IRIX node. For uninstall procedures, contact Inktomi Technical Support.



Chapter 5

After Installing Traffic Server

This chapter describes several things you may want to do after you have completed installing Traffic Server.

This chapter discusses the following topics:

Starting Traffic Server

You need to start Traffic Server manually only if you did not start it at the conclusion of your node installation or if a node fails and does not recover.

▼ To start Traffic Server:

1. Log in as the Traffic Server user account.
2. `cd` to the `bin` directory in Traffic Server's install directory.
3. Type this command:

   ```
   start_traffic_server
   ```

   This runs the `start_traffic_server` script, which starts the Traffic Server processes.

(For a full discussion of Traffic Server processes, see the *Traffic Server Administrator's Guide*.)

Starting a Traffic Server cluster

To start a Traffic Server cluster, simply start Traffic Server on any one of the cluster's nodes. Follow the procedure given above.

Starting the Traffic Manager UI

The `traffic_cop` process starts the `traffic_manager` process; it also starts Traffic Manager, Traffic Server's web browser-based interface for monitoring and configuration. Traffic Manager requires Java and JavaScript; be sure to enable Java and JavaScript in your web browser.

▼ To operate Traffic Manager:

1. Open your web browser.
2. Point your browser at one of these locations:

Standard HTTP	`http://`*`nodename`*`:`*`adminport`*`/`
SSL HTTP	`https://`*`nodename`*`:`*`adminport`*`/`

   where `nodename` names one of your Traffic Server nodes and `adminport` is the port number assigned to Traffic Server's administrator process.

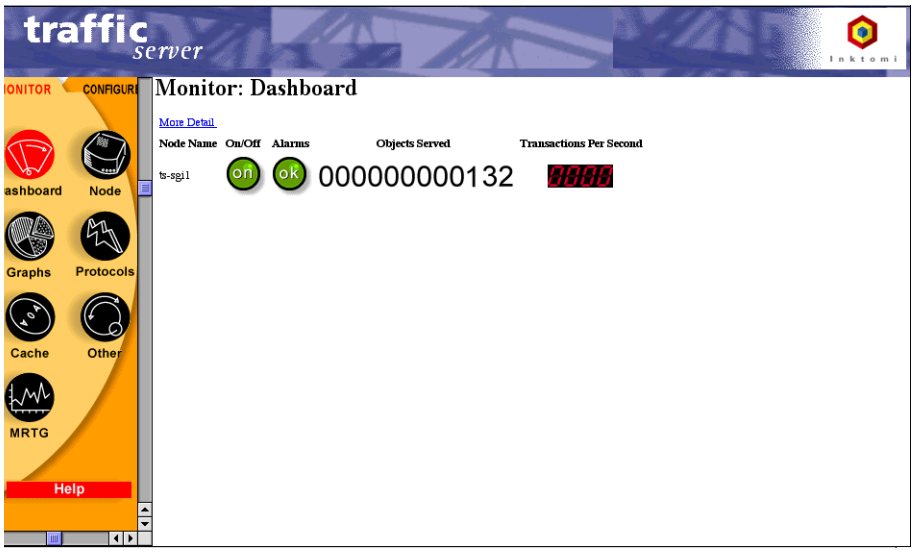
   (Node names and the port number of the administrator process are set when you install Traffic Server. To change the port number, refer to the *Traffic Server Administrator's Guide*.)

Note Use the SSL HTTP location only if you have restricted access to the Traffic Manager to SSL connections; otherwise, use the standard HTTP address.

3. Log on using your administrator's user name and password.

   (You set the administrator ID and password during Traffic Server installation; to learn how to change them, refer to the *Traffic Server Administrator's Guide*.)

Traffic Manager appears in your browser.



Adding devices to Traffic Server nodes

Only when Traffic Server recognizes a device as its own can it incorporate that device into the network environment. During installation, the installer changes ownership of all necessary devices to the name of your Traffic Server user account. By devices, we mean primarily disks and network interfaces.

Devices added *after* installation are, by default, owned by root. For Traffic Server to use a device added after installation, make the Traffic Server user account the device's owner.

For example, you must change ownership of a new disk to Traffic Server to allow Traffic Server to use that disk for cache.

▼ To change ownership of devices:

This example assumes that your Traffic Server user account is `inktomi`.

1. Become `root`.
2. Change ownership of the device:

   ```
   chown inktomi /device
   ```

3. Run the `add` command with the options appropriate to the device you're adding.
4. Check to see that the device has the correct owner by entering this command:

   ```
   ls -l /device
   ```

5. Add entries to `/etc/ioperms` as described in ioconfig (1M).
6. Reboot Traffic Server.

Enabling bypassing of transparent traffic

A few clients and servers fail to operate correctly with transparent web proxies, because of software bugs, server IP authentication issues, or applications sending non-HTTP traffic over HTTP ports. Traffic Server contains an adaptive learning module that recognizes these problems and automatically routes the traffic around Traffic Server. This is called *bypassing* of transparent traffic, and Traffic Server supports two methods of bypassing: dynamic, and static.

- ✔ Dynamic (also called adaptive) bypass rules are generated dynamically if you configure Traffic Server to bypass the cache when it detects non-HTTP traffic on port 80, or when it encounters certain HTTP errors.
- ✔ Static bypass rules must be manually configured in the bypass configuration file (`bypass.config`). Traffic Server avoids serving requests coming from or directed to a particular IP address or range of IP addresses defined by static bypass rules.

Do not confuse bypass rules with client access control lists. Bypass rules are generated in response to interoperability problems. Client access control is simply restriction of the client IP addresses that can access the Traffic Server cache.

See the *Traffic Server Administrator's Guide* for details and configuration procedures.

Using the records.config file for dynamic bypassing

To enable dynamic bypassing, you edit the `records.config` file in Traffic Server's `config` directory entering *dynamic bypass rules*.

Using the bypass.config file for static bypassing

To enable dynamic bypassing, you edit the `bypass.config` file in Traffic Server's `config` directory entering *static bypass rules*.

Chapter 6

Serving Traffic Transparently

This chapter describes Traffic Server transparency options and how to install them. Transparency enables you to route user traffic directly to Traffic Server without requiring users to explicitly configure their browsers to use your Traffic Server system as a proxy.

For a more complete description of transparency, see the *Traffic Server Administrator's Guide*.

This chapter covers these topics:

What is transparency?

When clients are *not* configured to explicitly direct their requests to Traffic Server, but the network is designed so that Traffic Server receives the client requests anyway, we say that Traffic Server is *transparent* to the client.

A transparent Traffic Server deployment works like this:

When clients request content from a web server, a *transparency device* intercepts the request and redirects it to Traffic Server. Traffic Server checks whether the content is in cache and fresh, and if so, serves the content to the client. Serving content from Traffic Server's cache offloads traffic from the original web server and provides faster delivery, if Traffic Server is closer to the client than the web server. The proxy transaction is transparent in that the client is unaware that the object is served from a cache.

Transparency requires your network to have a transparency device, which may be any one of the following:

- ✔ a Layer 4-aware switch
- ✔ a router that implements policy-based routing
- ✔ Traffic Server configured to perform software routing

Transparency devices are explained in more detail below.

Traffic Server offers transparent proxy caching for HTTP requests on port 80 and NNTP requests on port 119.

Traffic Server's transparency option is not enabled by default. This chapter explains what Traffic Server's transparency option requires you to choose during Traffic Server installation, and what capabilities it requires your network to have.

To learn more about transparency, see the *Traffic Server Administrator's Guide*.

Requirements of Traffic Server transparency

In a transparent deployment, you must have control of the route your end users follow to the Internet. Traffic Server must be deployed at a network choke point—in the path of all Internet traffic—so that all traffic flows through the Traffic Server platform.

During Traffic Server installation, you choose whether to install the Adaptive Redirection Module (ARM), a component of Traffic Server that allows transparency to work. *You must install ARM if you want to run Traffic Server transparently.* If you are unsure whether your Traffic Server should serve requests transparently, do not install ARM. For more information on ARM, see *Understanding the Adaptive Redirection Module, on page 58*, and the *Traffic Server Administrator's Guide*.

Traffic Server 4.0.14 for IRIX supports three different transparency solutions:

Layer 4-aware switch A layer 4-aware switch operates between the end users and Traffic Server. The layer 4-aware switch watches for TCP packets aimed at port 80, and redirects them to Traffic Server.

Policy-based routing A router capable of policy-based routing operates between the end users and Traffic Server. The router inspects all traffic and redirects HTTP requests to the Traffic Server.

Software routing A software-based solution where Traffic Server itself acts as a router; Traffic Server supports advanced software routing that recognizes and redirects HTTP requests so that the Traffic Server can serve them transparently.

For more information on these transparency solutions, see the *Traffic Server Administrator's Guide*.

How you choose to implement transparency depends on what you have already deployed in your network, and what you're willing to put there. You configure and enable transparency options during Traffic Server installation. See *Setting up Traffic Server to serve requests transparently, on page 25* for more information about enabling transparency.

Understanding the Adaptive Redirection Module

When a transparency device redirects an HTTP or NNTP request to Traffic Server, the request is addressed to an origin server. When the request reaches Traffic Server, it is received by ARM. ARM changes the destination IP address and port in the message header of the request, readdressing the request to Traffic Server. Traffic Server then obtains the requested content from cache or from an origin server. The request now goes back to ARM from Traffic Server. ARM restores the destination port in the message header to its original state as the served request re-enters the network.

Because the end user making requests receives response packets addressed just as they would be if Traffic Server were not present between the client and the origin server, Traffic Server is transparent to the end user. The technique that ARM uses here is called *network address translation (NAT)*.

Transparency cannot be enabled without ARM. If you want to run Traffic Server transparently, you must install ARM.

When readdressing an incoming packet, ARM changes the packet's destination IP address and destination port.

For HTTP, ARM typically:

- ✔ readdresses the HTTP packet destination IP with Traffic Server's IP address
- ✔ readdresses the HTTP packet destination port with Traffic Server's HTTP Proxy Port

(Usually, Traffic Server's Proxy Port is port 8080).

For NNTP, ARM

- ✔ readdresses the NNTP packet destination IP with Traffic Server's IP address
- ✔ readdresses the destination NNTP port as with Traffic Server's NNTP port, *if* Traffic Server uses a port other than 119 for NNTP

You can configure packet readdressing by editing the redirection rules in the `ipnat.conf` file. See *Understanding the ARM configuration file (ipnat.conf), on page 60*.

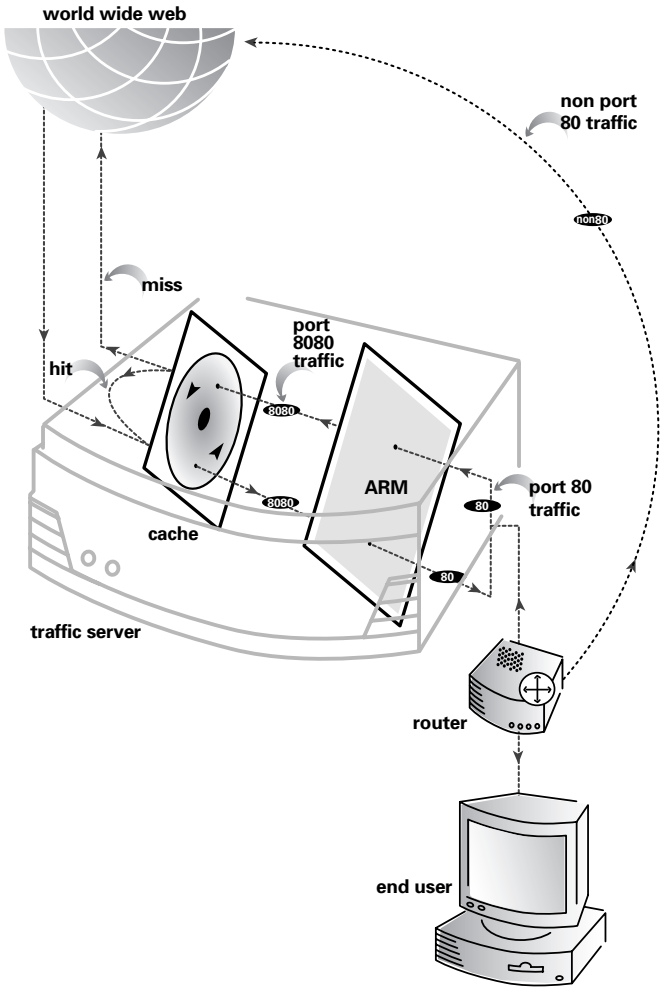


Figure 1 HTTP transparency in action

In Figure 1, an end user sends an HTTP request for content on an origin server on the Web. The request has port 80 as the destination port in the message header. When the request reaches ARM, ARM substitutes port 8080 for port 80 in the header. ARM then sends the request to Traffic Server. Port 8080, the port which Traffic Server is configured to accept, is called the *apparent port*; port 80, the original destination port of the packet, is called the *actual port*.

When Traffic Server's cache returns the requests, ARM changes the destination port back to port 80, as though the returned request originated from the origin server—not the cache. When the message is delivered to the end user, the end user is unaware that it came from Traffic Server rather than the origin server.

Understanding the ARM configuration file (`ipnat.conf`)

The `ipnat.conf` file contains redirection rules that specify how ARM should readdress incoming packets. The installer writes one redirect rule for HTTP, and another for NNTP, to `ipnat.conf`. The rules are based on the information that you enter when prompted by the installer.

HTTP

If you choose transparency for HTTP traffic, the installer creates a redirect rule so that ARM readdresses all incoming HTTP packets to Traffic Server's IP address, and Traffic Server's HTTP proxy port (usually port 8080).

The rule is in this form:

```
rdr hme0 0.0.0.0/0 80-> XXX.XXX.XXX.XXX port 8080 tcp
```

where `XXX.XXX.XXX.XXX` is Traffic Server's IP address.

NNTP

If you choose transparency for NNTP traffic, the installer creates a redirect rule so that ARM readdresses all incoming NNTP packets to Traffic Server's IP address. If Traffic Server uses a port other than 119 for NNTP, ARM readdresses the destination NNTP port as well.

The rule is in this form:

```
rdr hme0 0.0.0.0/0 119 -> XXX.XXX.XXX.XXX port 119 tcp
```

where `XXX.XXX.XXX.XXX` is Traffic Server's IP address.

Checking the ipnat.conf file

You can check the `ipnat.conf` file to make sure that the redirection rules are enabled.

You can inspect the redirection rules by printing them out.

▼ To print out a list of redirection rules:

1. `cd` to Traffic Server's `bin` directory
2. Enter the command:

```
ipnat -l
```

For more information on `ipnat.conf`, see the README file in `bin/ARMboot`. The default ARM configuration file looks like this:

```
# ARM Configuration File
#   $id$
#
# This file configures the Adaptive Redirection Module to allow for
# transparent proxy support.
#
# The configuration consists of a set of redirection(rdr) rules.
# For example:
#
#      rdr hme0 0.0.0.0/0 80 -> XXX.XXX.XXX.XXX port 8080 tcp
#
# The above rule instructs the Adaptive Redirection Module
# to redirect tcp traffic from any client coming into this machine
# over the hme0 ethernet interface to
# IP address XXX.XXX.XXX.XXX port 8080.
#
# You should use the above rule as a template, substituting hme0
# with the name of the ethernet interface that user traffic will
# enter this machine through. If you have multiple interfaces,
```

```
# simply have multiple redirect rules, one for each interface.
# For example:
#
#      rdr hme0 0.0.0.0/0 80 -> XXX.XXX.XXX.XXX port 8080 tcp
#      rdr hme1 0.0.0.0/0 80 -> XXX.XXX.XXX.XXX port 8080 tcp
#
# XXX.XXX.XXX.XXX should be replaced with one of the _real_ IP
# addresses for this machine. Do not use the loop back 127.0.0.*
# addresses. If you installed the Traffic Server to run on a port
# other than 8080, you should modify that as well.
#
# note: hash('#') denotes a comment in this file.
# rdr hme0 0.0.0.0/0 80 -> XXX.XXX.XXX.XXX port 8080 tcp
```

Appendix A

UNIX Installation File Hierarchy

This appendix describes the files installed on Sun IRIX nodes during Traffic Server installation, their functions, and what the installer modifies on your system. For more information on specific files, see the *Traffic Server Administrator's Guide*.

There are five sections in this appendix:

About Installation

Traffic Server software is automatically copied during installation. The installer copies these directories onto your system:

Files installed	What they contain
`./bin`	Contains executable programs and scripts
`./config`	Contains configuration files
`./diags.log`	Contains diagnostic output only if you turn it on
`./logs`	Contains access and error log files
`./mgmt_db`	Management database
`./ui`	Contains the files used by the Traffic Manager graphical interface

The installer copies files to your install directory based on your specifications. If you did not create a user account before installation, the installer creates a user account for you, and creates an entry in `/etc/password`. See the man pages (`man useradd`) for more information on creating a user account.

The installer then saves the installation path in `/etc/traffic_server`.

Depending on the system you are using, the installer also modifies your system. See *Modified files on IRIX, on page 70*, for more information.

What's in the logs directory?

The `logs` directory contains Traffic Server access and error log files.

Understanding Traffic Server log files

As logs roll, the log rolling facility moves old files into a log file with a date tagged on the end. Old log files in the `logs` directory take the following format:

`/log/hostname.datestamp`

as in the following example:

```
./logs/squid.log.market2.19980821.09h48m52s-19980822.00h00m00s.old
```

Access and error log files

File	Description
`./logs/error.log`	Current error log.
`./logs/.error.log.meta`	Work file for log rolling name control.
`./logs/squid.log`	Current squid log. Configurable in the UI on the **Configure: Event Logging** page or in records.config. Squid is the default log format. If you don't choose it, the file gets another name of your specification.
`./logs/.squid.log.meta`	Work file for log rolling name control.
`./logs/traffic.out`	The standard out of `traffic_server` and `traffic_manager` processes.

What's in the bin directory?

The `bin` directory contains Traffic Server executables. Consult the *Traffic Server Administrator's Guide* before trying to modify any of these executables. *If the executable is not documented in the Traffic Server Administrator's Guide, do not modify it.*

Executable scripts

File	Description
`./bin/ARMboot`	Transparency driver startup script.
`./bin/armlkm.o`	Contains Transparency executables.
`./bin/config`	Link to the `./config` directory.
`./bin/dumpstarts`	Used for MRTG.
`./bin/example_alarm_bin.sh`	Sample alarm script. You may edit this at anytime to suit your needs.
`./bin/example_prep.sh`	Shell script that saves core files in the event of a Traffic Server failure. You may edit this at anytime to suit your needs.
`./bin/ipnat`	Contains Transparency configuration files.
`./bin/mib2agt`	Used for SNMP.
`./bin/mrtgcron`	Used for MRTG.
`./bin/nntp_auth`	NNTP authorization command.
`./bin/print_bypass`	Contains Transparency man pages.
`./bin/shmem_clean`	Utility command.
`./bin/snmpdm`	Used for SNMP.
`./bin/start_traffic_server`	The Traffic Server start-up command. See the *Traffic Server Administrator's Guide* for more information.
`./bin/stop_traffic_server`	See the *Traffic Server Administrator's Guide* for more information.
`./bin/traffic_cop`	The `traffic_cop` process watches the `traffic_manager` and `traffic_server`, and other processes, to ensure that they are running. See the *Traffic Server Administrator's Guide* for more information.
`./bin/traffic_line`	The command-line facility that you can use to configure the Traffic Server and retrieve Traffic Server statistics. See the *Traffic Server Administrator's Guide* for more information.
`./bin/traffic_manager`	The `traffic_manager` process manages the Traffic Server, and has several functions. See the *Traffic Server Administrator's Guide* for more information.
`./bin/traffic_mom.tab`	Copy of the `cron.tab`.
`./bin/traffic_server`	The `traffic_server` process that runs the Traffic Server. See the *Traffic Server Administrator's Guide* for more information.
`./bin/update_mrtg`	Used for MRTG.
`./bin/vip_config`	Virtual IP command.

What's in the config directory?

The `config` directory contains Traffic Server configuration files.Understanding Traffic Server configuration filesAs you modify configuration files, they receive an underscore plus a number tagged on the end of the older version as in the example below.

Example

```
Aug 21 9:38 records.config_1
Aug 21 9:48 records.config_2
Aug 21 11:51 records.config_3
```

Tagged files are listed in decreasing age, the highest number being the most recent file.

The current version of the file has no number tagged on the end. As you make changes through Traffic Manager, tagging occurs.

The following table lists the configuration files that you see in your `config` directory after installing Traffic Server.

Configuration files

File	Description
`/admin_access.config`	Specifies additional users, beyond the administrator, that are allowed to access the web UI. Note: Duplicate user IDs are not permitted.
`/arm_security.config`	Contains the ARM access control list, which specifies the hosts that are allowed to communicate with the Traffic Server ARM.
`/bypass.config`	Contains the rules that Traffic Server uses to determine whether to bypass incoming client requests.
`/cache.config`	Contains caching rules. See the *Traffic Server Administrator's Guide* for more information.
`/cli`	Command line interface socket.
`/cluster.config`	Do not modify this file. This is a machine generated file.
`/filter.config`	Contains filtering rules. See the *Traffic Server Administrator's Guide* for more information.
`/ftp_remap.config`	Contains mapping rules that Traffic Server uses to direct any incoming FTP requests to the FTP server if the requested document is a cache miss or is stale.
`/hosting.config`	Used for assigning cache partitions to specific origin servers or domains.
`/icp.config`	Contains the name and configuration information for ICP peers. See the *Traffic Server Administrator's Guide* for more information.
`/internal/`	Do not modify this directory. This directory contains process lock files for active Traffic Server processes which ensure that only one copy of a process runs at a time.
`/ip_allow.config`	Controls client access to the Traffic Server. See the *Traffic Server Administrator's Guide* for more information.
`/ipnat.conf`	Contains redirection rules that specify how incoming packets should be readdressed when serving traffic transparently.
`/ldapsrvr.config`	Specifies Internet sites that Traffic Server clients can access without LDAP server authentication.
`/logs.config`	Contains transaction log file formats. See the *Traffic Server Administrator's Guide* for more information. You may edit this file at any time to suit your needs.

File	Description
/log_hosts.config	Lists origin server hostnames for which you want separate HTTP or FTP transaction log files.
/logs_xml.config	Defines custom log files, formats and filters in an XML-based file. (Use instead of the logs.config file when you want maximum logging customization.)
/mgmt_allow.config	Controls access to the Traffic Manager UI. See the *Traffic Server Administrator's Guide* for more information.
/mgr.cnf	SNMP configuration file.
/mibs/	Contains files used for the SNMP MIB.
/nntp_access.config	Controls user access to news articles cached by the Traffic Server. See the *Traffic Server Administrator's Guide* for more information.
/nntp_servers.config	Contains NNTP configuration rules. See the *Traffic Server Administrator's Guide* for more information.
/parent.config	Controls HTTP parent proxying. See the *Traffic Server Administrator's Guide* for more information.
/partition.config	Specifies partitions of different sizes for specific protocols.
/plugin.config	Lists all plugins to be loaded when traffic server is started.
/plugin.db	Contains information about the plugin database. Do not edit this file.
/process_server	Process server socket.
/proxy.pac	Default browser auto-configuration file.
/public_key.der	SSL public key for manager port.
/records.config	Contains a list of configurable variables that Traffic Server software uses. Do not change records.config variables unless you are certain of the effect. See the *Traffic Server Administrator's Guide* for more information
/remap.config	Contains reverse proxy mapping rules. See the *Traffic Server Administrator's Guide* for more information
/server.pem	Contains a demo certificate for trial SSL termination.
/snapshots/	Contains your configuration snapshots.
/snmpd.cnf	Contains parameters that control user access to MIB information and trap destinations.
/snmpinfo.dat	Lists all variables provided by Traffic Server.
/snmp-start.config	Used to setup environment variables and execute the SNMP daemon and subagent. Do not modify this file.
/snmpinfo.dat	This file maps SNMP OIDs to human-readable names. Do not modify this file.)
/socks.config	Controls traffic through the SOCKS server. See the *Traffic Server Administrator's Guide* for more information.
/splitdns.config	Specifies the DNS server that Traffic Server should use for resolving hosts under specific conditions.
/storage.config	This file lists all the files, directories, or partitions that make up the Traffic Server cache. See the *Traffic Server Administrator's Guide* for more information.
/update.config	Contains URLs and information that Traffic Server uses to perform scheduled updates of specific local cache content.

File	Description
/vaddrs.config	Virtual IP configuration file.
/wpad.dat	Contains a script that enables the browser to auto-configure itself for Web Proxy Auto-Discovery protocol (WPAD).

Modified files on IRIX

After the installer takes you through its interactive dialog, during which you enter your configuration information, it configures your system for you.

The installer modifies the following IRIX system files depending on the information you entered during the interactive dialog.

Start-up scripts

Files created	Description
`/etc/init.d/traffic_server`	Traffic Server start-up script
`/etc/rc2.d/S28traffic_server`	Link to Traffic Server start-up script (ARM not installed)
`/etc/rc0.d/K02traffic_server`	Link to Traffic Server stop script
`/etc/rc2.d/S33traffic_server`	Link to Traffic Server startup script (ARM installed)
`/etc/rc2.d/S33ipf`	Link to Traffic Server ARM module driver

System files

Files modified	Description
`/var/sysgen/master.d/bsd`	Changes the kernel variable `m_shget_off` value from 0 to 1
`/var/sysgen/stune`	Modified upon kernel rebuild.

Transparency files

Files modified	Description
`/etc/init.d/ARMboot`	Transparency driver start-up script.
`/etc/rc2.d/S33ARMboot`	Link to Transparency driver start-up script.

Configuration Worksheet

Use this worksheet to plan your Traffic Server installation. You may want to make several copies of these blank worksheets so you have them on hand if you rework your configuration, upgrade or install more than one Traffic Server in your network.

Question 1. What is your Traffic Server account name?

_____

Question 2. What is the full path of your destination installation directory?

_____

Question 3. What is the full path of your destination logging directory?

_____

Question 4. Is this installation part of a multi-machine Traffic Server cluster?

- ☐ Yes Go to Question 5.
- ☐ No Go to Question 6.

Question 5. What is the name of your Traffic Server cluster?

_____

Question 6. Which interface will you use for cluster communication?

_____

Question 7. What is your multicast group address?

_____

Question 8. Will this Traffic Server installation perform Reverse Proxy?

- ☐ Yes
- ☐ No

Question 9. What is your starting port number?

_____

Question 10. Will this installation serve requests transparently?

- ☐ Yes Install the Adaptive Redirection Module.
- ☐ No Go to Question 14.

Questions 11-13 apply to transparent Traffic Server installations only.

Question 11. Will this installation proxy NNTP?

☐ Yes Enter the primary news server system.

_____

☐ No Do not proxy NNTP.

Question 12. What is your Administrator user name?

_____

Question 13. What is your Administrator password?

_____

Question 14. Which of your disk resources will you use for cache storage?

_____

_____

_____

_____

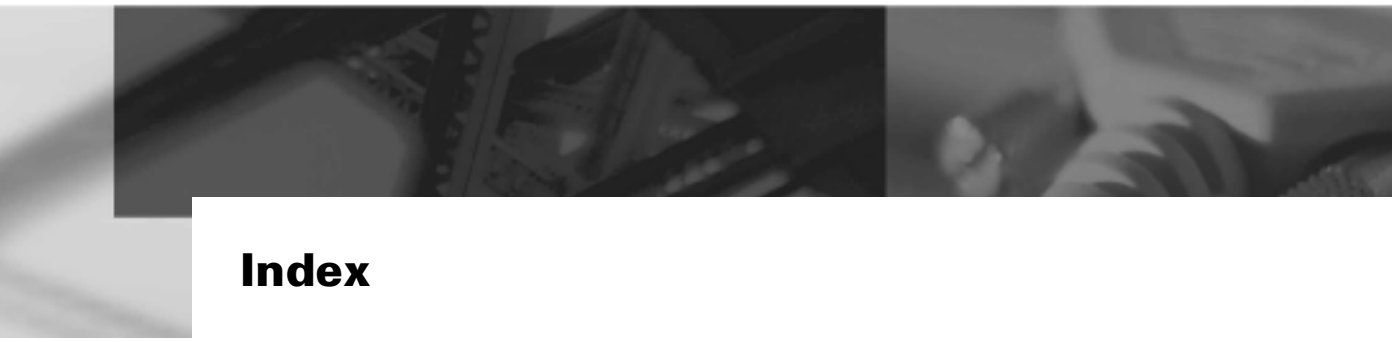
System requirements

If you are installing a clustered Traffic Server system, wherein several Traffic Server nodes act in concert with one another, you must configure all the nodes identically. You cannot mix and match nodes of differing platforms, using different operating systems, different versions of the same operating system, different operating system patches, or different versions of Traffic Server.

Keep a record of the operating environment on which you installed your Traffic Server.

Component	**Your Traffic Server installation**
Computer	
Operating System	
Disks used for cache	
Network interface(s)	

Notes



Index

COPYRIGHT NOTICES

Portions of Traffic Server include third party technology used under license. One or more of the following notices may apply in connection with the license and use of Traffic Server.

tcl-7.4 license. This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS-IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

RESTRICTED RIGHTS: Use, duplication or disclosure by the government is subject to the restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software Clause as DFARS 252.227-7013 and FAR 52.227-19.

SSLeay-0.6.6 License. Copyright © 1995-1997 Eric Young (eay@mincm.oz.au). All rights reserved.

Redistribution and use in source code and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product incorporates cryptographic software written by Eric Young (eay@mincom.oz.au)." The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4.If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement "This product includes software written by Tim Hudson (tjh@mincom.oz.au)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

RSAREF (for MD5). Copyright © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

BSAFE SSL-C and **BSAFE Crypto-C**.

Portions of Traffic Server include technology used under license from RSA Data Security, Inc.

libdb-1.85 License. Copyright © 1990, 1993, 1994 The Regents of the University of California. All rights reserved.

Redistribution and use in source code and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.

4.Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

gd 1.3 graphics library.

Portions copyright 1994, 1995, 1996, 1997, 1998, by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, by Boutell.Com, Inc.

GIF decompression code copyright 1990, 1991, 1993, by David Koblas (koblas@netcom.com).

Non-LZW-based GIF compression code copyright 1998, by Hutchison Avenue Software Corporation (http://www.hasc.com/, info@hasc.com).

libregx package. Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and distribute it, subject to the following restrictions:

1. The author is not responsible for the consequences or use of this software, no matter how awful, even if they arise from flaws in it.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.

4. This notice may not be removed or altered.

Emanate. Licensee agrees to preserve and reproduce the copyright notices contained in the Program Source and Software in the same form and location as any legend appearing on or in the original from which copies are made.

Portions of Traffic Server include Emanate software developed by SNMP Research International, Incorporated. Copying and distribution is by permission of SNMP Research International, Incorporated, and relevant third parties.

INN. Portions of Traffic Server include software developed by Rich Salz. Copyright 1991 Rich Salz. All rights reserved. Revision: 1.4

Redistribution and use in any form are permitted provided that the following restrictions are met:

1. Source distributions must retain this entire copyright notice and comment.

2. Binary distributions must include the acknowledgement "This product includes software developed by Rich Salz." in the documentation or other materials provided with the distribution. This must not be represented as an endorsement or promotion without specific prior written permission.

3. The origin of this software must not be misrepresented, either by explicit claim or by omission. Credits must appear in the source and documentation.

4. Altered versions must be plainly marked as such in the source and documentation and must not be misrepresented as being the original software.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

IP-Filter package. Portions of Traffic Server include technology used under license from Darren Reed.

MRTG (Multi-Router Traffic Grapher). This freeware is used under the GNU General Public License (see www.gnu.org).

Documentation Feedback

We hope you find this book useful. If you have suggestions for improving it, please send them to **docfeedback@inktomi.com**, along with the title and date of this book. Your product experience can help us improve our documentation. Thank you.

Inktomi Technical Publications Group