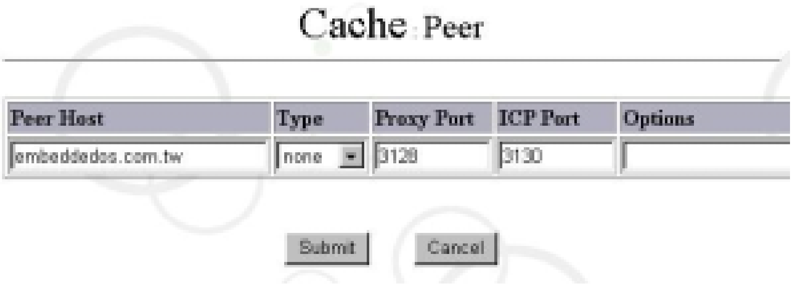
6.2.4 Cache Peer

In the “Cache Peer” screen of “Cache”, we can configure to communicate with other Proxy Servers. This configuration is possible for the communication with proxy servers on upper levels or on the same level.

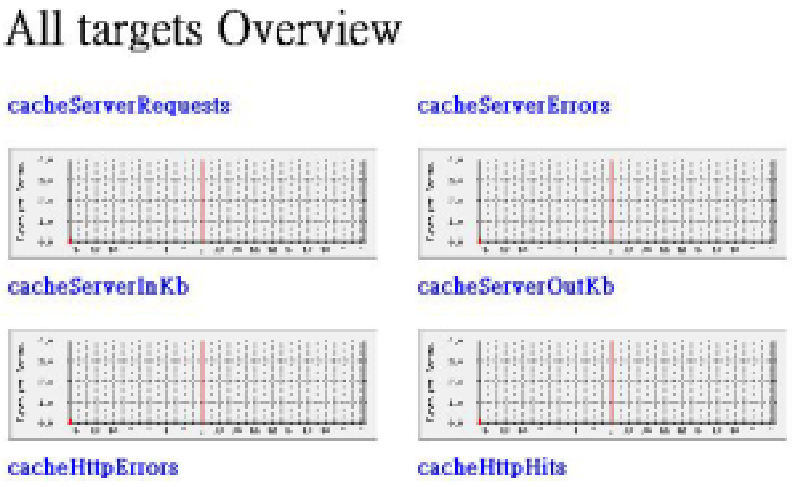


Cache Peer

Peer Host	Type	Proxy Port	ICP Port	Options
embeddedos.com.tw	none	3128	3130	

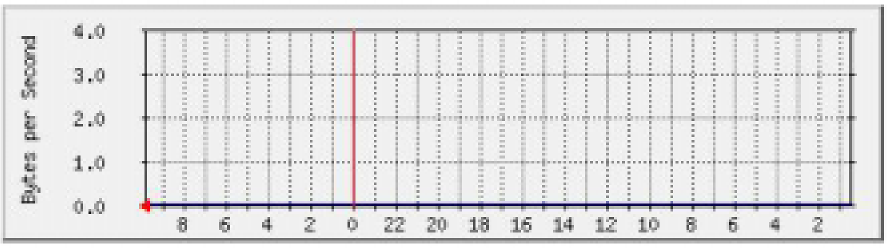
6.2.5 Multi Router Traffic Grapher (MRTG)

In general, Multi Router Traffic Grapher (MRTG) graphically shows performance analysis of cache service, including analysis of cacheServerRequests, cacheServerErrors, cacheServerInKb, cacheServerOutKb, and CPU utilization. As shown in the figure below:



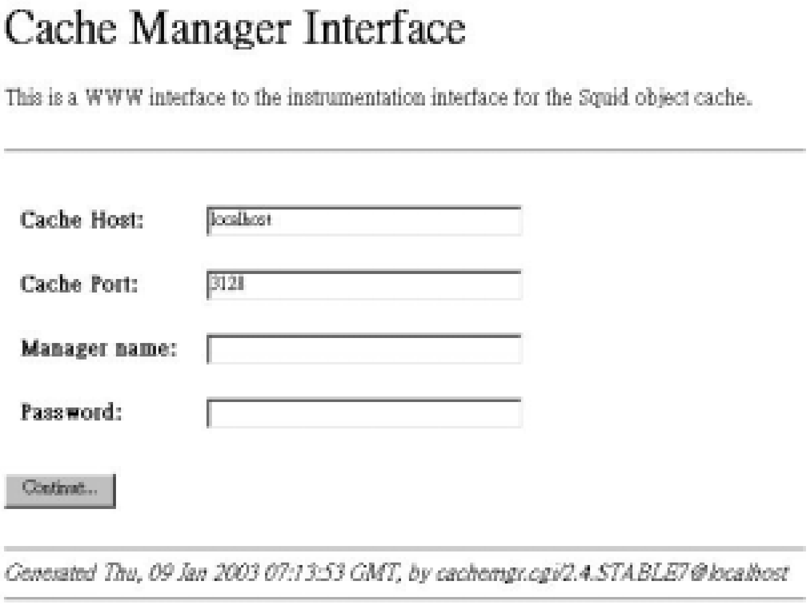
All targets Overview

In addition, if you click any small graph in All targets Overview, the cache traffic analysis on daily, weekly, monthly, and annual basis will display as shown in the figure below:



6.2.6 Cache Management

You can check whether the cache is operating properly via Cache Manager Interface. Click “Statistics” in Cache service menu. The following screen will appear:



Cache Manager Interface

This is a WWW interface to the instrumentation interface for the Squid object cache.

Cache Host: localhost

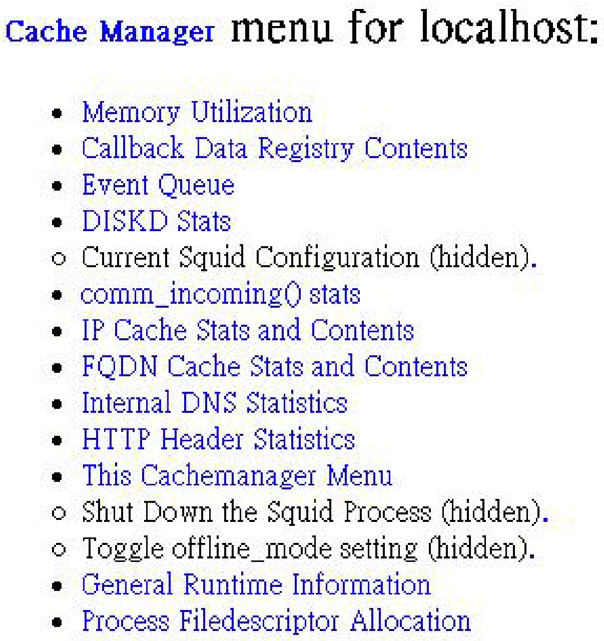
Cache Port: 3128

Manager name:

Password:

Generated Thu, 09 Jan 2003 07:13:53 GMT, by cachemgr.cgi/2.4.STABLE7@localhost

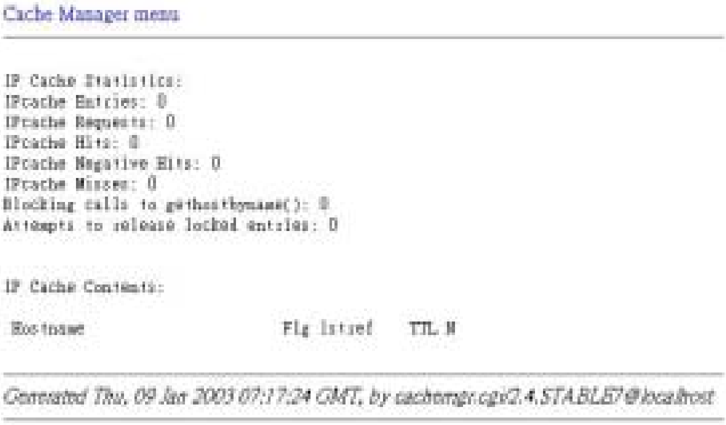
Click “Continue” button directly (it is unnecessary to complete Manager name and Password since the system will enter the data automatically). The options of Cache Manager will appear as shown in the figure below, wherein “IP Cache Stats and Contents” and “Cache Client List” are frequently used by managers, and thus the rest of the Cache Manager options will not be described here.



Cache Manager menu for localhost:

- Memory Utilization
- Callback Data Registry Contents
- Event Queue
- DISKD Stats
- ○ Current Squid Configuration (hidden).
- comm_incoming() stats
- IP Cache Stats and Contents
- FQDN Cache Stats and Contents
- Internal DNS Statistics
- HTTP Header Statistics
- This Cachemanager Menu
- ○ Shut Down the Squid Process (hidden).
- ○ Toggle offline_mode setting (hidden).
- General Runtime Information
- Process Filedescriptor Allocation

1. IP Cache Stats and Contents – shows all of the websites visited by the client-end and the corresponding IP addresses, plus the log data of pre-caching, as shown in the figure below:



Cache Manager menu

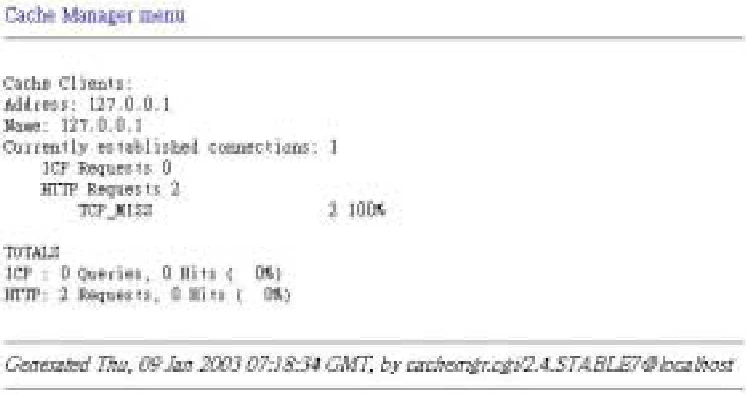
```
IP Cache Statistics:
IPcache Entries: 0
IPcache Requests: 0
IPcache Hits: 0
IPcache Negative Hits: 0
IPcache Misses: 0
Blocking calls to gethostbyname(): 0
Attempts to release locked entries: 0

IP Cache Contents:

 Hostname                    Flg lstref    TTL N
```

Generated Thu, 09 Jan 2003 07:17:24 GMT, by cachemgr.cgi/2.4.STABLE7@localhost

2. Cache Client List – shows all of the Client-end information on the used cache service, as shown in the figure below:



Cache Manager menu

```
Cache Clients:
Address: 127.0.0.1
Name: 127.0.0.1
Currently established connections: 1
    ICP Requests 0
    HTTP Requests 2
        TCP_MISS                     2 100%

TOTALS
ICP : 0 Queries, 0 Hits (   0%)
HTTP: 2 Requests, 0 Hits (   0%)
```

Generated Thu, 09 Jan 2003 07:18:34 GMT, by cachemgr.cgi/2.4.STABLE7@localhost

6.3 DHCP Service

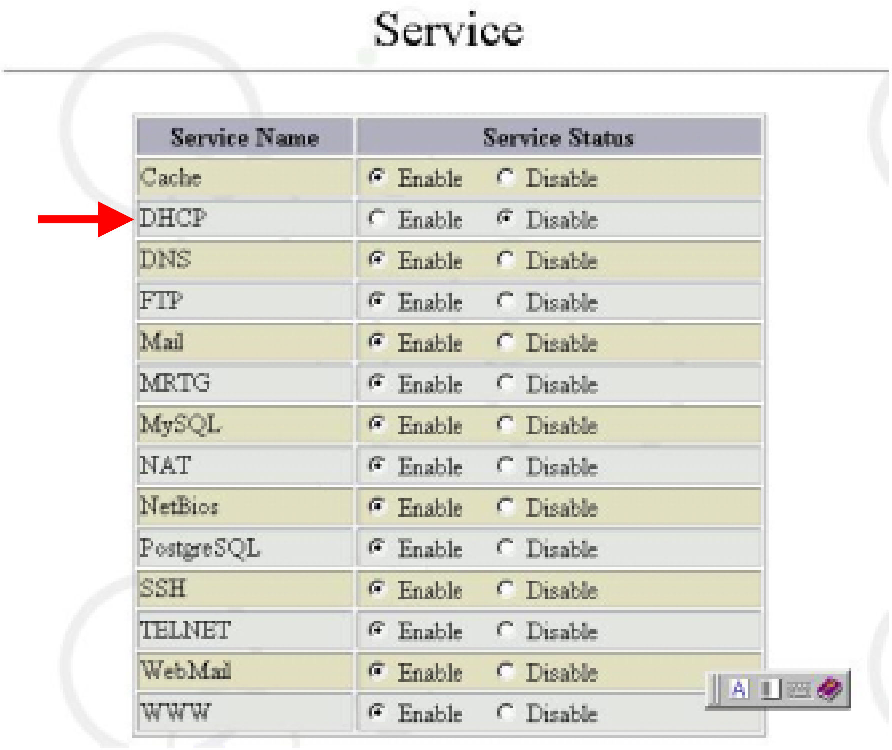
DHCP (Dynamic Host Configuration Protocol) is a communication protocol used to distribute IP addresses and other configurations between Client PSs and DHCP server. It mainly features to enable one computer broadcasts through its own MAC address to obtain configurations related to IP, Netmask, Default Gateway and DNS. Thus a network administrator only needs to configure DHCP server, so that Client PC can automatically obtain IP related configurations through DHCP protocol, saving efforts to configure on each client PC.DHCP and NAT (transferred Virtual IP to legal IP) are not directly related. Please make sure not to error.

DHCP servers are all easy to use and set up. Therefore, if your PC fails to obtain an IP address, the problem generally originates in such PC devices as network cabling, NIC of PCs, HUB, switches, NT servers, printer servers, or / and interweaving of internal and external networks.

6.3.1 Steps of DHCP Configuration

1. Enable DHCP

Click “Service” in the “System Management Tools” screen and select Enable for “DHCP” as shown in the figure below:

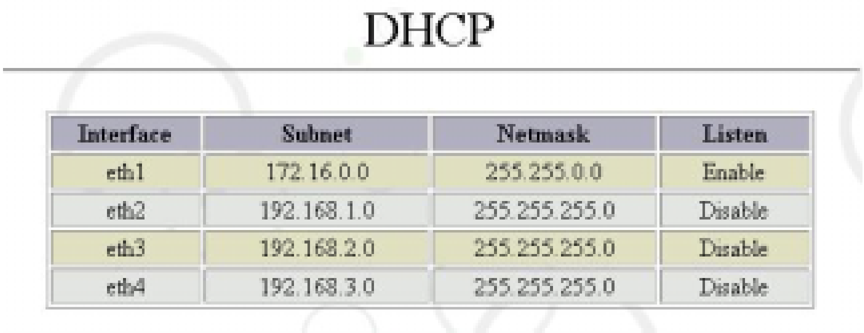


Service

Service Name	Service Status
Cache	● Enable ○ Disable
DHCP	○ Enable ● Disable
DNS	● Enable ○ Disable
FTP	● Enable ○ Disable
Mail	● Enable ○ Disable
MRTG	● Enable ○ Disable
MySQL	● Enable ○ Disable
NAT	● Enable ○ Disable
NetBios	● Enable ○ Disable
PostgreSQL	● Enable ○ Disable
SSH	● Enable ○ Disable
TELNET	● Enable ○ Disable
WebMail	● Enable ○ Disable
WWW	● Enable ○ Disable

2. Default Value of DHCP Service Configuration

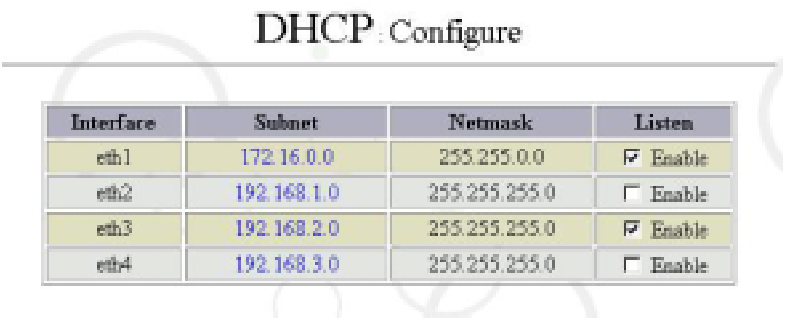
Then click “DHCP” in the “Service” screen. A NIC screen showing that DHCP is enabled will appear as shown in the figure below:



DHCP

Interface	Subnet	Netmask	Listen
eth1	172.16.0.0	255.255.0.0	Enable
eth2	192.168.1.0	255.255.255.0	Disable
eth3	192.168.2.0	255.255.255.0	Disable
eth4	192.168.3.0	255.255.255.0	Disable

The above figure shows that the NIC (eth1) had enabled DHCP. If you want to use other NICs to enable DHCP, you can select “Enable” for the specified NIC on the “Configuration” screen as shown in the figure below:

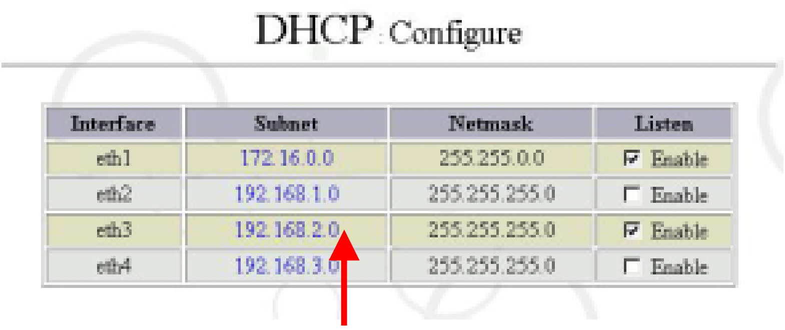


DHCP : Configure

Interface	Subnet	Netmask	Listen
eth1	172.16.0.0	255.255.0.0	☑ Enable
eth2	192.168.1.0	255.255.255.0	□ Enable
eth3	192.168.2.0	255.255.255.0	☑ Enable
eth4	192.168.3.0	255.255.255.0	□ Enable

3. Change in NIC Configurations of DHCP

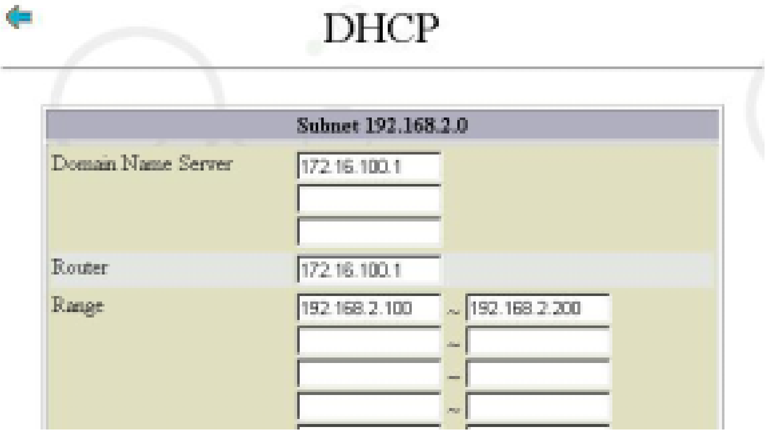
In the “Configure” screen of “DHCP”, we can choose to carry out related configurations for the NIC that starts the DHCP. As shown in the figure below, check the Sub-domain “192.168.2.0” (pointed out by the arrow) to enter the configuration screen of that NIC.



DHCP : Configure

Interface	Subnet	Netmask	Listen
eth1	172.16.0.0	255.255.0.0	☑ Enable
eth2	192.168.1.0	255.255.255.0	□ Enable
eth3	192.168.2.0	255.255.255.0	☑ Enable
eth4	192.168.3.0	255.255.255.0	□ Enable

In the NIC Configure screen with DHCP of 192.168.2.0 as shown below, we have set up such parameters as “172.16.100.1” for the server, “172.16.100.1” for the router, and the IP-address range available in the DHCP server. These settings are related information provided by the DHCP server when DHCP clients request the server for an IP address.



DHCP

Subnet 192.168.2.0

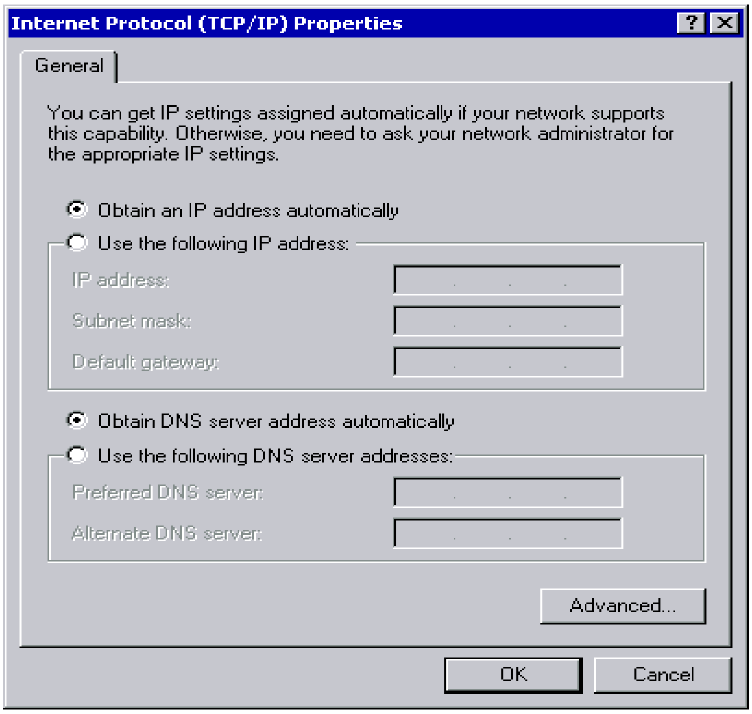
Domain Name Server	172.16.100.1		
Router	172.16.100.1		
Range	192.168.2.100	~	192.168.2.200

6.3.2 DHCP Client-End Configuration

Client-end configurations are very simple, just requiring a few of steps as shown below:

1. DHCP Configuration (Microsoft Windows 2000 taken as an example here)

Click the right mouse button on "My Network Places" and select "Properties". Then select "TCP / IP" → NIC (e.g. NE2000).



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

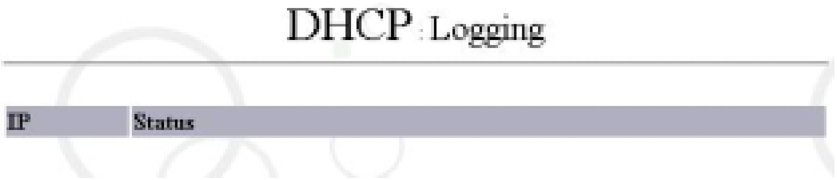
Preferred DNS server:

Alternate DNS server:

Except selecting "Automatic Obtain IP Address" (Shown as in the figure above) on "IP Address", you do not need to configure related options. Click on "OK", Client PC will reboot. After rebooting computer, you can use command winipcfg to check if a set of IP values automatically obtained.

6.3.3 DHCP Logging

After selecting “Logging” of “DHCP”, the system will display the utilization status of DHCP clients, such as IP addresses and lease time, MAC addresses, and host names of the client PC, so that MIS staffs are able to conduct related administration, as shown in the figure below:

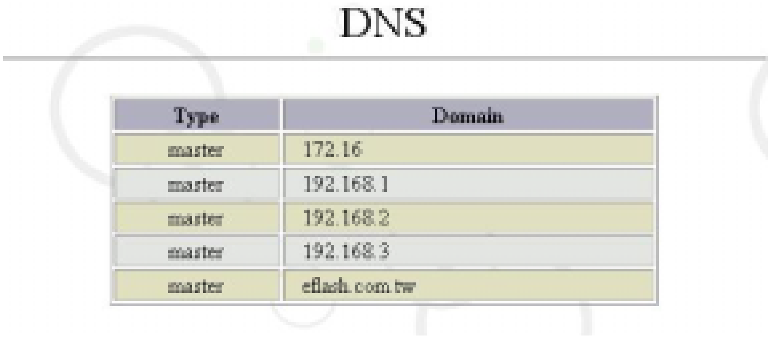


DHCP : Logging

IP	Status

6.4 DNS

Select “DNS” in “Service”: (Related configurations below are for demonstration only)



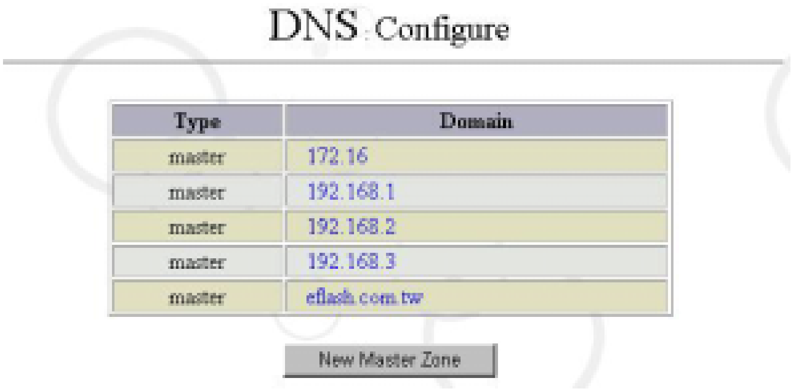
DNS

Type	Domain
master	172.16
master	192.168.1
master	192.168.2
master	192.168.3
master	eflash.com.tw

As shown in the figure above, configuration list for “DNS” appears. The list shows all current configurations of “DNS”.

6.4.1 Configurations

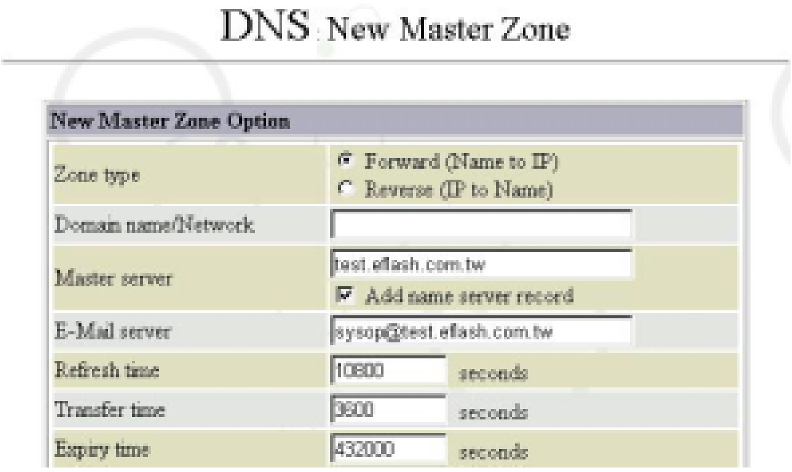
The configurations allow administrators to add primary domain or sub-domain.



DNS : Configure

Type	Domain
master	172.16
master	192.168.1
master	192.168.2
master	192.168.3
master	eflash.com.tw

Select “New Master Zone” to add a new primary domain:

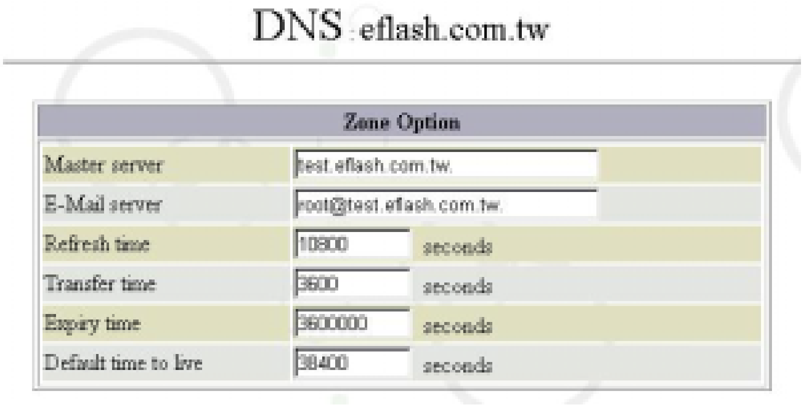


DNS : New Master Zone

New Master Zone Option	
Zone type	● Forward (Name to IP) ○ Reverse (IP to Name)
Domain name/Network	
Master server	test.eflash.com.tw ☑ Add name server record
E-Mail server	sysop@test.eflash.com.tw
Refresh time	10800 seconds
Transfer time	3600 seconds
Expiry time	432000 seconds

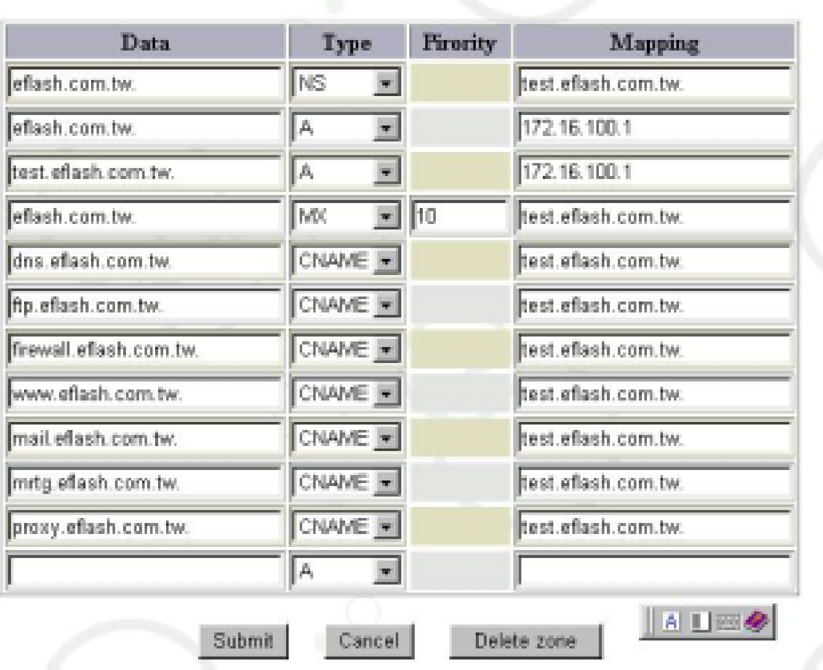
Note:

1. (master) eflash.com.tw, (master) 192.168.2, (master) 172.16:
   are the Forward and Reverse of DNS. “(master) eflash.com.tw” is the Forward Domain Name Analysis of this domain, while “(master) 192.168.2” and “(master) 172.163” are its Reverse Domain Name Analysis.



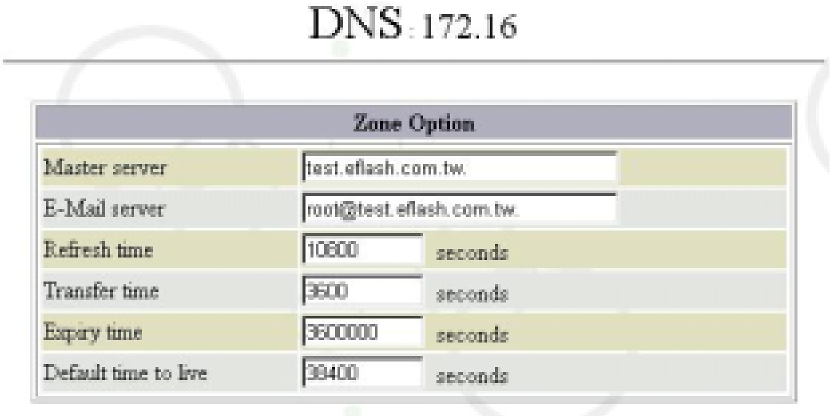
DNS : eflash.com.tw

Zone Option	
Master server	test.eflash.com.tw.
E-Mail server	root@test.eflash.com.tw.
Refresh time	10800 seconds
Transfer time	3600 seconds
Expiry time	3600000 seconds
Default time to live	38400 seconds



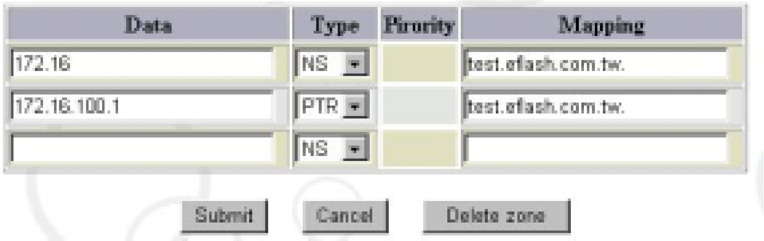
Data	Type	Pirority	Mapping
eflash.com.tw.	NS		test.eflash.com.tw.
eflash.com.tw.	A		172.16.100.1
test.eflash.com.tw.	A		172.16.100.1
eflash.com.tw.	MX	10	test.eflash.com.tw.
dns.eflash.com.tw.	CNAME		test.eflash.com.tw.
ftp.eflash.com.tw.	CNAME		test.eflash.com.tw.
firewall.eflash.com.tw.	CNAME		test.eflash.com.tw.
www.eflash.com.tw.	CNAME		test.eflash.com.tw.
mail.eflash.com.tw.	CNAME		test.eflash.com.tw.
mrtg.eflash.com.tw.	CNAME		test.eflash.com.tw.
proxy.eflash.com.tw.	CNAME		test.eflash.com.tw.
	A		

The two figures above are the detailed configurations of the Forward Domain Name Analysis of “(master)eflash.com.tw”.



DNS : 172.16

Zone Option		
Master server	test.eflash.com.tw.	
E-Mail server	root@test.eflash.com.tw.	
Refresh time	10800	seconds
Transfer time	3600	seconds
Expiry time	3600000	seconds
Default time to live	38400	seconds



Data	Type	Pirority	Mapping
172.16	NS		test.eflash.com.tw.
172.16.100.1	PTR		test.eflash.com.tw.
	NS		

The two figures above are the detailed configurations of the Reverse Domain Name Analysis of “(master)172.16”.

2. The system will automatically apply newly configured DNS configurations after you make a change in all of the aforementioned settings.

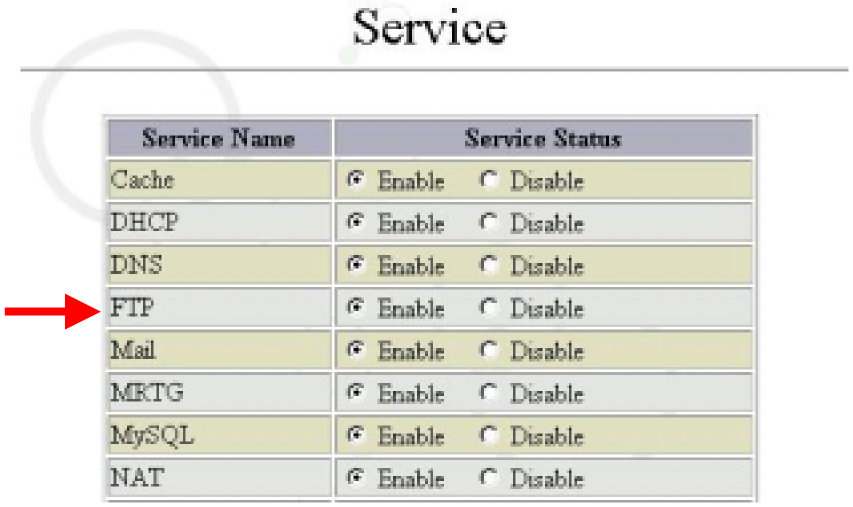
6.5 FTP

Actually, FTP stands for “File Transfer Protocol”, which allows LAN or Internet users to upload and download files and data in a snap, and thereby makes network HD storage and resource sharing possible.

6.5.1 Steps of FTP Configuration

1. Enable FTP

Click “Service” in the “System Management Tools” screen, select “Enable” FTP as shown in the figure below:

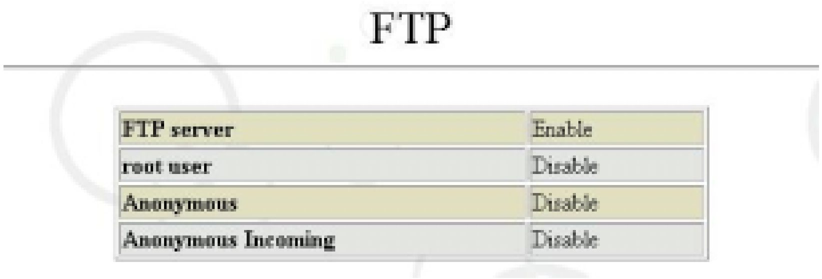


Service

Service Name	Service Status
Cache	● Enable ○ Disable
DHCP	● Enable ○ Disable
DNS	● Enable ○ Disable
FTP	● Enable ○ Disable
Mail	● Enable ○ Disable
MRTG	● Enable ○ Disable
MySQL	● Enable ○ Disable
NAT	● Enable ○ Disable

2. FTP Configuration

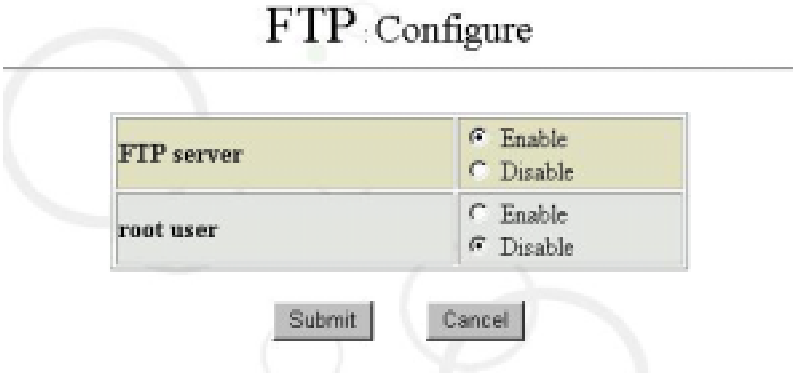
Then click “FTP” in the “Service” screen, and you will see a FTP service default offered by the system. As shown in the figure below, the system has enabled FTP server, disabled root user, enabled Anonymous and disabled Anonymous Incoming:



FTP

FTP server	Enable
root user	Disable
Anonymous	Disable
Anonymous Incoming	Disable

A click of “Configuration” in the “FTP” screen enables you to change FTP configurations. If you want to enable ROOT user to use FTP as well, check “Enable” for root user, as shown in the figure below:

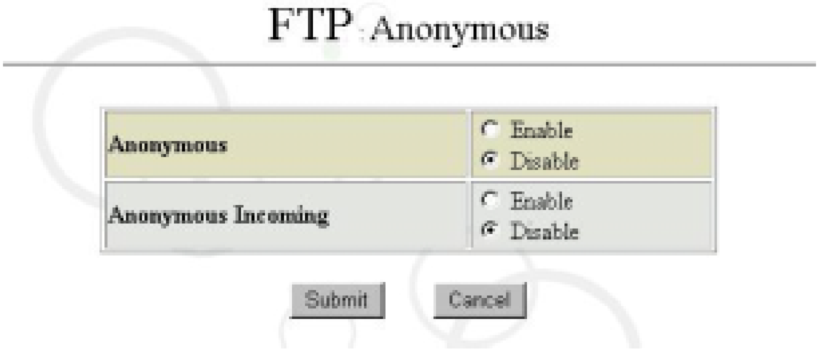


FTP : Configure

FTP server	● Enable ○ Disable
root user	○ Enable ● Disable

6.5.2 Anonymous Configuration

Click “Anonymous FTP” in the “FTP” screen.



FTP : Anonymous

Anonymous	○ Enable ● Disable
Anonymous Incoming	○ Enable ● Disable

As shown in the figure above, configuration list for “Anonymous FTP” appears. This list shows all the applied configurations of “Anonymous FTP”. This item is used to enable each configuration.

※ Note: “Anonymous FTP” means that the FTP is obtainable via universal user account, requiring no account authentication. Whether to enable this function depends on “Anonymous FTP status”. The universal user account here only has permission of reading files, and it is the “Anonymous FTP Incoming” that decides whether granting permission of writing files.

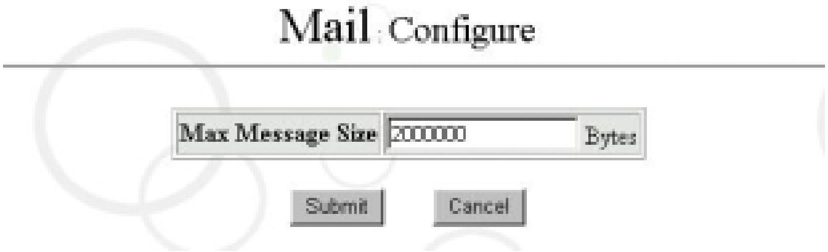
6.6 Mail

In generally, Mail configurations refer to the files under the directories of /etc/mail/sendmail.cf, /etc/aliases, and /etc/mail. If you fail in receiving any mails, it is often a result of incorrect DNS settings or inconsistency between the Forward and Reverse Domains of the domain name you have applied. However, the failure may be sometimes caused by the mistakes of these configuration files' content or those of file permissions.

6.6.1 Mail Configuration

It is mainly used to configure email size limit.

Please select "Configure" in "Mail Service" interface. Then a screen will appear as follows:



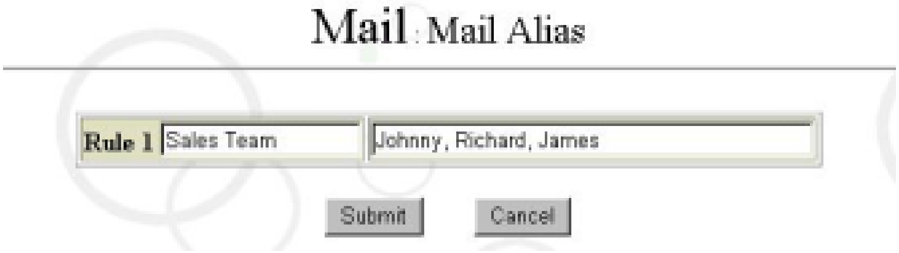
Mail : Configure

Max Message Size 2000000 Bytes

Now you can configure mail size; if you do not specify, mail size will be 0 Bytes. (Note: The unit is Bytes. So if you want to configure as 1MB, you should configure as 1024000 Bytes.)

6.6.2 Mail Alias

Click on "Mail Alias" you can specify the alias for whom to receive the mail. For example; If you specify "Johnny, Richard, James" as the alias for "Sales Team". All the mail to "Sales Team" will be forwarded to Johnny, Richard and James. The screen will appear as follows:



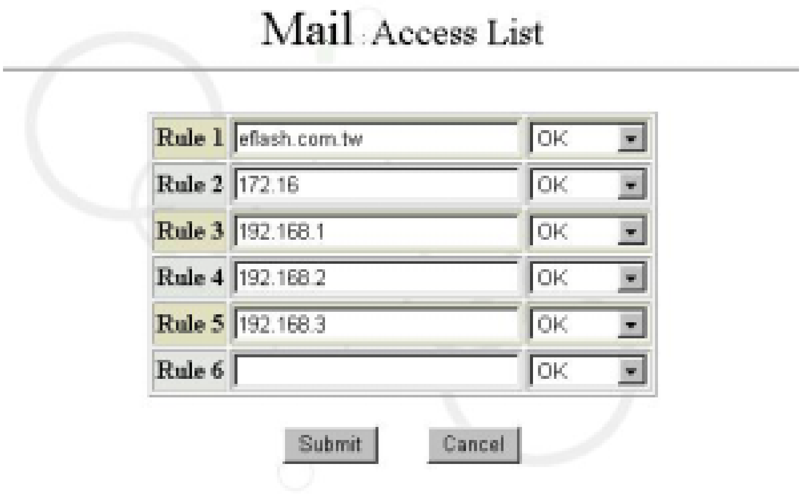
Mail : Mail Alias

Rule 1 Sales Team Johnny, Richard, James

6.6.3 Mail Access List Configuration

In general, the settings configure the accessible IP address block or domain name for the mail. During installation, the management interface will automatically set up a default value for the properties here. Therefore, in general, it is unnecessary to change these settings unless you want to edit, add or delete some DNS configurations yourself.

Please select "Mail Access List Configuration" in "Mail" of the "Service" interface. Then a screen will appear as follows:



Mail : Access List

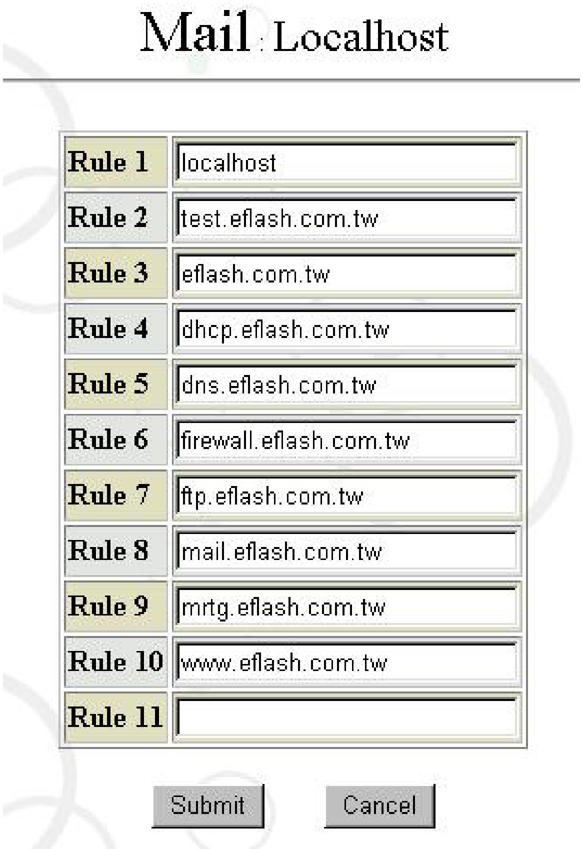
Rule 1	eflash.com.tw	OK
Rule 2	172.16	OK
Rule 3	192.168.1	OK
Rule 4	192.168.2	OK
Rule 5	192.168.3	OK
Rule 6		OK

You can configure accessed domain range for mail service. Access service is not available for those not listed on the Access List. The range can be Domain Name or IP address. (Note: The rule fields of the system allow continuous entry of data, without any limitation on the space shown in the screen.)

6.6.4 Configure Mail Domain for Localhost

Here you can configure the domain names or other names that are available in the host, with default values automatically configured during installation. Therefore, in general, it is unnecessary to change these settings unless you want to edit, add or delete some DNS settings by yourself.

Select “Localhost” in “Mail” of the “Service” interface. Then a screen will appear as follows:



Mail : Localhost

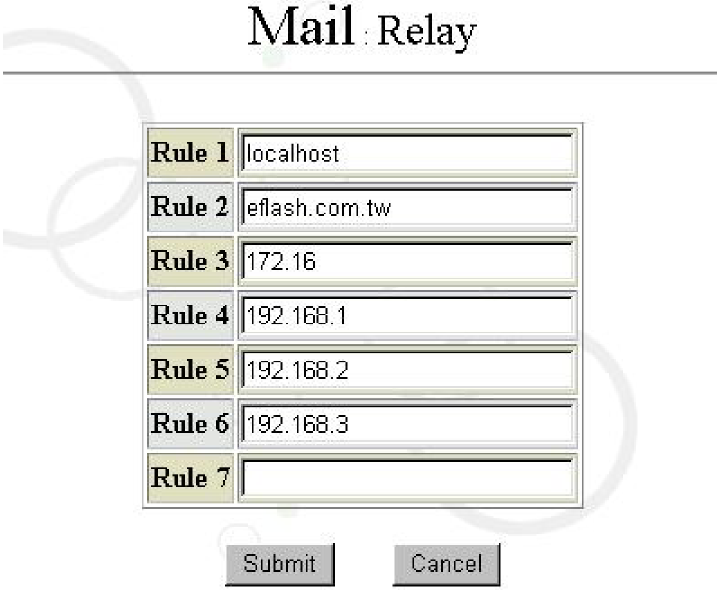
Rule 1	localhost
Rule 2	test.eflash.com.tw
Rule 3	eflash.com.tw
Rule 4	dhcp.eflash.com.tw
Rule 5	dns.eflash.com.tw
Rule 6	firewall.eflash.com.tw
Rule 7	ftp.eflash.com.tw
Rule 8	mail.eflash.com.tw
Rule 9	mrtg.eflash.com.tw
Rule 10	www.eflash.com.tw
Rule 11	

(Note: The rule fields of the system allow continuous entry of data, without any limitation on the space shown in the screen.)

6.6.5 Configure Email-Relay Domain

Here you can configure the domain or IP address block to have the mail service accept relayed emails. During installation, the management interface will automatically configure a default value for the properties here. Therefore, in general, it is unnecessary to change these configurations unless you want to edit, add or delete some DNS configurations yourself.

Please select “Email-relay Domain” in “Mail” of the “Service” interface. Then a screen will appear as follows:



Mail : Relay

Rule 1	localhost
Rule 2	eflash.com.tw
Rule 3	172.16
Rule 4	192.168.1
Rule 5	192.168.2
Rule 6	192.168.3
Rule 7	

The range here can be on a basis of domain names or IP addresses.

(Note: The rule fields of the system allow continuous entry of data, without any limitation on the space shown in the screen.)

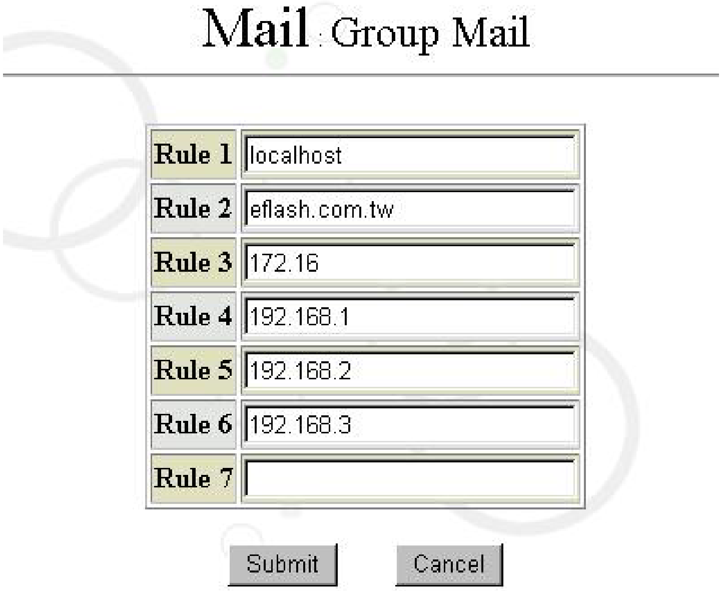
In order to prevent from any unauthorized utilization of mail relay. Maat system included an authentication facility to challenge user with user ID and password. When user’s domain that is not in “Relay” list, system will prompt for user ID and password. User will be denied if authentication does not successful.

If user wants to enable the authentication facility please refer to related Email application (such as Outlook Express) to make appropriate configuration.

6.6.6 Configure Group Mail Domain

In general, you can have emails sent in groups by configuring the settings here. In other words, whenever you send a mail within a domain, the mail will be delivered to every body of the same group as long as you keyed in a “group name @ mail server name” for the mail. Of course, you have to know the group’s name before doing so.

Please select “Group Mail Domain” in “Mail” of the “Service” interface. Then a screen will appear as follows:



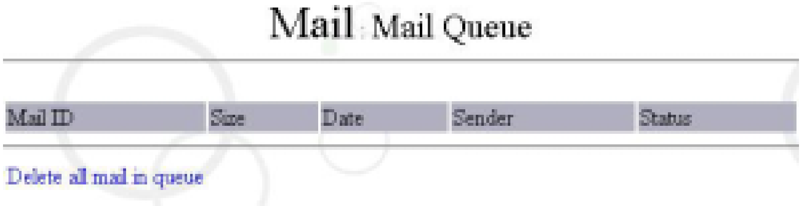
Mail : Group Mail

Rule 1	localhost
Rule 2	eflash.com.tw
Rule 3	172.16
Rule 4	192.168.1
Rule 5	192.168.2
Rule 6	192.168.3
Rule 7	

The range here can be on a basis of domain names or IP addresses. (Note: The rule fields of the system allow continuous entry of data, without any limitation on the space shown in the screen.)

6.6.7 Mail Queue

The main function of Mail Queue is to display all mails waiting for sent (shown as follows). You can click "Delete all mail in queue" to delete all mails waiting in queue.



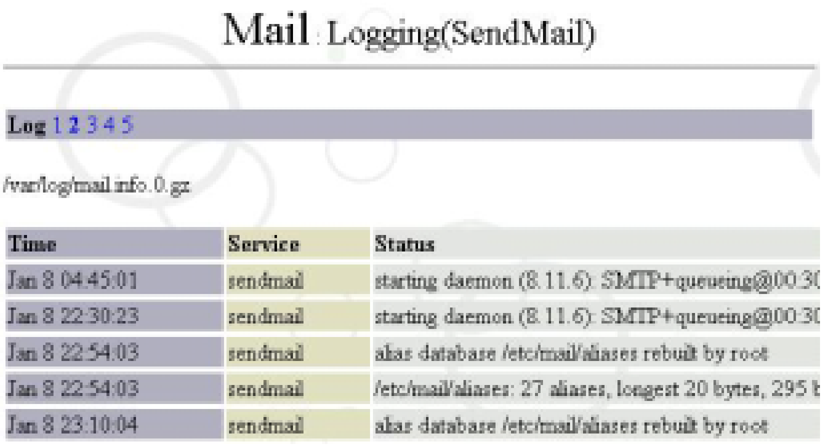
Mail : Mail Queue

Mail ID	Size	Date	Sender	Status

Delete all mail in queue

6.6.8 Mail Logging(SendMail)

By clicking "Logging(SendMail)" of "Mail", you can view whether the mail service is operating normally, whether there is a person delivering junk mails, or whether there are jammed mail boxes, so that you can take countermeasures in time, as shown in the figure below:



Mail : Logging(SendMail)

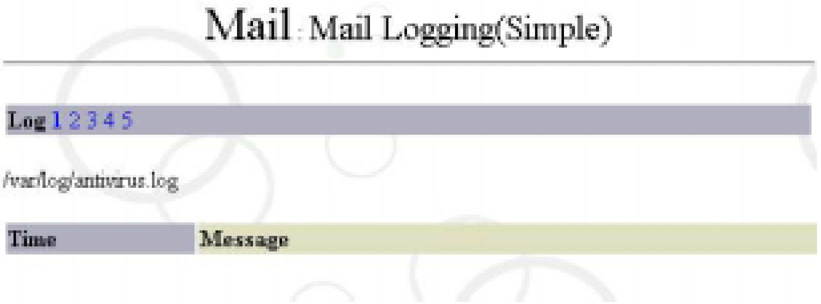
Log 1 2 3 4 5

/var/log/mail.info.0.gz

Time	Service	Status
Jan 8 04:45:01	sendmail	starting daemon (8.11.6): SMTP+queueing@00:3
Jan 8 22:30:23	sendmail	starting daemon (8.11.6): SMTP+queueing@00:3
Jan 8 22:54:03	sendmail	alias database /etc/mail/aliases rebuilt by root
Jan 8 22:54:03	sendmail	/etc/mail/aliases: 27 aliases, longest 20 bytes, 295 b
Jan 8 23:10:04	sendmail	alias database /etc/mail/aliases rebuilt by root

6.6.9 Mail Logging(Simple)

By clicking "Mail Logging(Simple)" of "Mail", you can view the mail service in simpler format, It include "From" , "To" , "ID" , "Size" and "Subject" as shown in the figure below:



Mail : Mail Logging(Simple)

Log 1 2 3 4 5

/var/log/antivirus.log

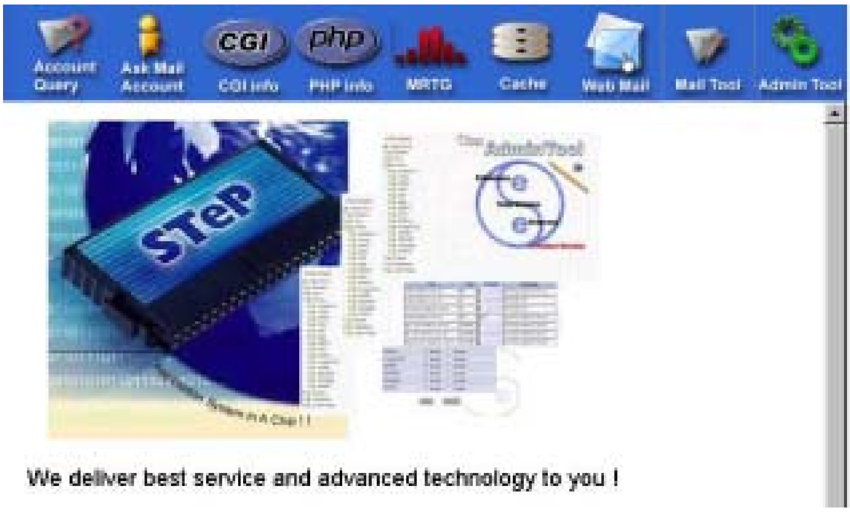
Time	Message

6.6.10 Mail for root & sysop Managers

After you finish configuring the system, "rootalias" will be set up automatically as a default account and there is no way to delete it. This account is mainly used to receive mails for sysop and root; in other words, whenever there are mails sent to the mailbox of sysop or root, the mails will be delivered to the rootalias account. Therefore the root and sysop managers are expected to use this account to receive mails. Please be kept in mind to periodically clean the mail for "rootalias". The "System Logging" in "System" GUI will come up with message as "save email panic and reject anywhere" if mailbox for "rootalias" became full. But this would not interfere other mail operation of Maat system.

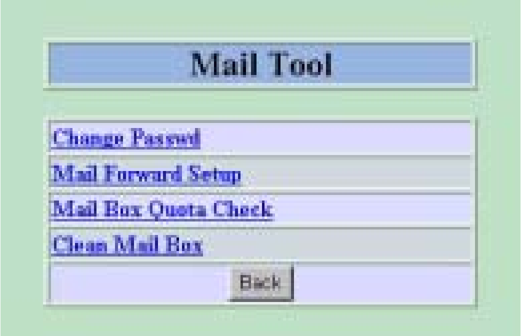
6.6.11 Mail Tools

Every Maat user have requirement to change their owned password and other action on mailbox. They will connect to Maat home page through the URL as http:// Maat' IP Address. The diagram show as below:



We deliver best service and advanced technology to you !

Click on “Mail Tool” button on the upper right side of screen. The Mail Tool management screen show as below:



Change Password: It allows you to change user password.
Mail Forward Setup: It allows you to set mail forwarding to another mail account.
Mail Box Quota Check: It allows you to check status of mail quota.
Clean Mail Box: It allows you to clean up mailbox content.

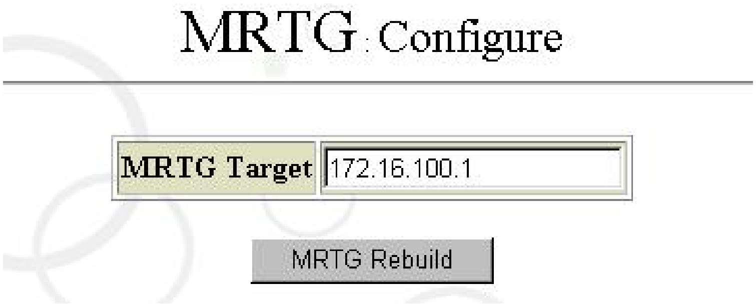
6.7 MRTG (Multi Router Traffic Grapher) Traffic Monitoring

MRTG (Multi Router Traffic Grapher) – MRTG is the web traffic statistics software with high popularity. One of its features is that it can draw a web-traffic statistic chart at anytime. We can use MRTG retrieve the SNMP information from such network equipments as routers and switches, and thereby enable MRTG to generate traffic information.

6.7.1 MRTG Configuration

To configure MRTG is quite easy. If you want to perform MRTG traffic monitoring on host, you only need to enter IP address. Remember to enable SNMP function. (Note: The system default is “Enabled” SNMP. If not, please enable on “System Management” of “System Management Tool”.)

Click on “MRTG” from “Service” to begin traffic monitoring, and then click on “Configure”. As shown in the figure below, full in IP address in the “MRTG Target” field, and then click on “MRTG Rebuild” to complete the configuration. (Note: Here the MRTG address stands for local host or other node needing traffic monitoring.)

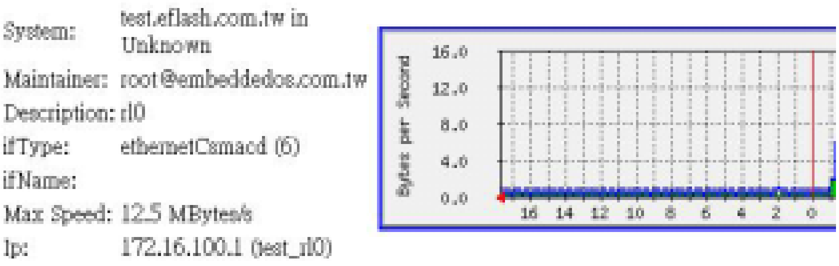

MRTG : Configure

MRTG Target: 172.16.100.1

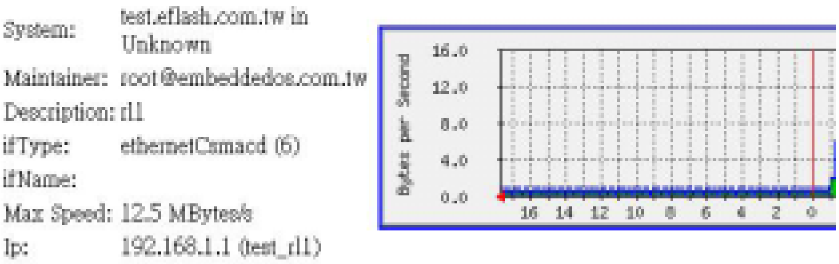
6.7.2 MRTG Logging

In essence, MRTG operates like a kind of simple network management software. It uses SNMP to detect (or query) the network equipments with SNMP you specified, and compile statistics the traffic of these equipments every five minutes, based on which a statistics graph is generated. The most fascinating feature of MRTG is that we can easily comprehend the actual web traffic from the statistics graph alone. Here you can see its exhaustive traffic graphs.

Click on “Logging” from “MRTG”, you can see basic description of host system and a traffic chart. The chart shows only some representations. (If the network facility is only a NIC, you will see a chart representing the traffic on the NIC) as shown in the figure below:

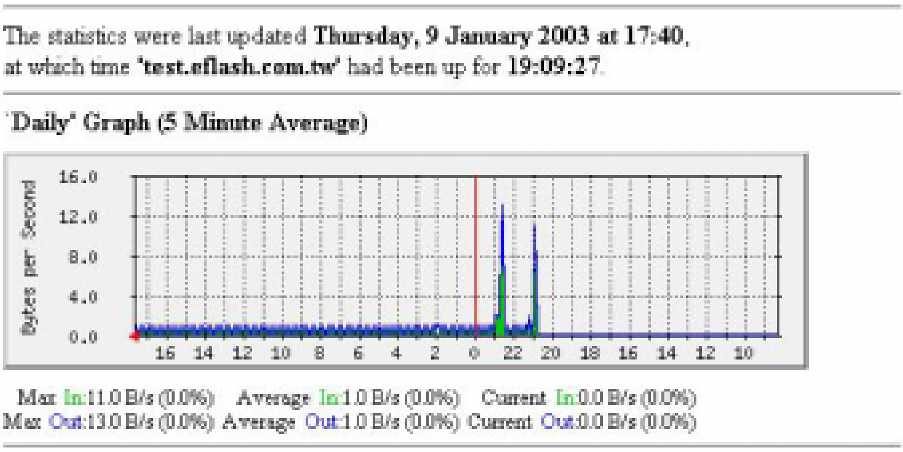


System:	test.eflash.com.tw in Unknown
Maintainer:	root@embeddedos.com.tw
Description:	rl0
ifType:	ethernetCsmacd (6)
ifName:	
Max Speed:	12.5 MBytes/s
Ip:	172.16.100.1 (test_rl0)



System:	test.eflash.com.tw in Unknown
Maintainer:	root@embeddedos.com.tw
Description:	rl1
ifType:	ethernetCsmacd (6)
ifName:	
Max Speed:	12.5 MBytes/s
Ip:	192.168.1.1 (test_rl1)

Click one of the traffic graphs above and then a screen will be shown as follows:



The statistics were last updated **Thursday, 9 January 2003 at 17:40**, at which time **'test.eflash.com.tw'** had been up for **19:09:27**.

'Daily' Graph (5 Minute Average)

Max In:11.0 B/s (0.0%) Average In:1.0 B/s (0.0%) Current In:0.0 B/s (0.0%)
Max Out:13.0 B/s (0.0%) Average Out:1.0 B/s (0.0%) Current Out:0.0 B/s (0.0%)

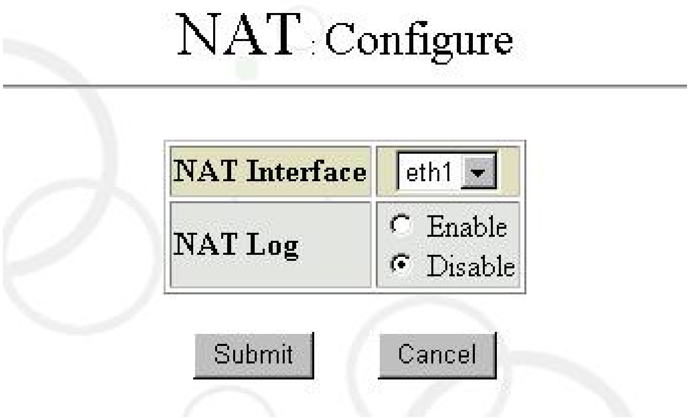
The figure above displays MRTG traffic monitoring, which generate traffic graphs on a basis of days, weeks, months, and years. In addition, it separately presents a graph of Max In / Out, Average In / Out, and Current In / Out, offering administrators with referential data to conduct system tuning and improve network performance.

6.8 NAT

NAT (Network Address Translation) allows you to define a virtual IP address in a private network whenever you need to do so, without the hassle of applying for a realistic one. Each PC in a private network communicates with each other via a private (i.e., virtual) IP address. When you want a private PC to communicate with the public Internet, you can use a NAT-enabled device (such as routers or the host itself) to translate the private IP address into a legal IP address (i.e., an officially applied IP address) to conduct communications. NAT can resolve most of the problems of moving private data transparently across the Internet.

6.8.1 Configuration

It is also very simple to configure NAT in this host. To start, please click “Service” and “NAT” from “System Management Tools”. Then click “Configurations” to configure which NIC is for the public network and whether to enable NAT and whether to log, and log directory、size and times as shown in the figure below:



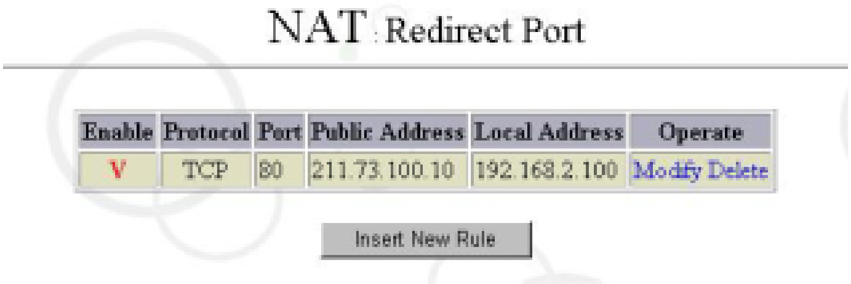
NAT : Configure

NAT Interface	eth1
NAT Log	○ Enable ● Disable

6.8.2 Port Redirection

Port Redirection function can redirected the packet externally connected to specified port number to specified host. This makes server for intranet available for external use. Also, it prevents server for intranet from direct exposure and attack from outside.

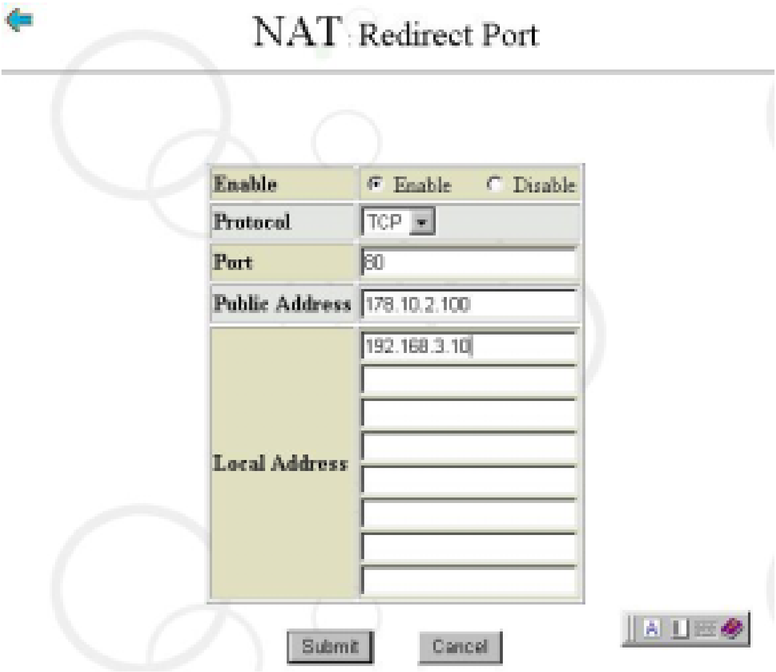
Click “Redirec Port” from “NAT” as shown in the figure below:



NAT : Redirect Port

Enable	Protocol	Port	Public Address	Local Address	Operate
V	TCP	80	211.73.100.10	192.168.2.100	Modify Delete

Click the “Insert New Rule” and input the detail information as shown in the figure below:

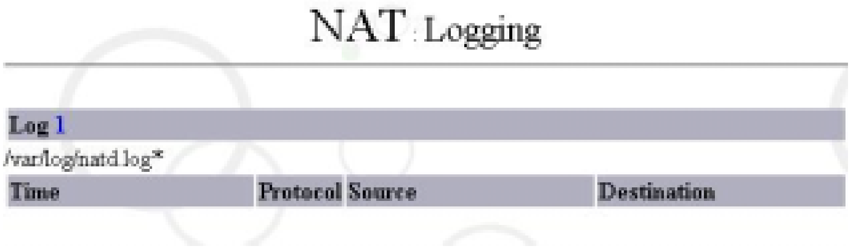


NAT Redirect Port

Enable	● Enable ○ Disable
Protocol	TCP
Port	80
Public Address	178.10.2.100
Local Address	192.168.3.10

6.8.3 NAT Logging

Click ”Logging” from “NAT”, then you can see the user records of NAT as shown in the figure below:



NAT Logging

Log 1

/var/log/natd.log*

Time	Protocol	Source	Destination

6.9 NetBios Services

NetBios Services features to make all users using Windows operating system see and share local file services on My Network Places.

6.9.1 NetBios Configuration

Click “Service” from “System Management Tool”, then click “Configure” from “NetBios Services”. You can configure the following item:

Netbios Name: It’s the host name configuring from “Network Interface”.

Comment: The “Comment” is not mandatory.

Allow Hosts/Networks: It’s to designate the host or network that allow to access this

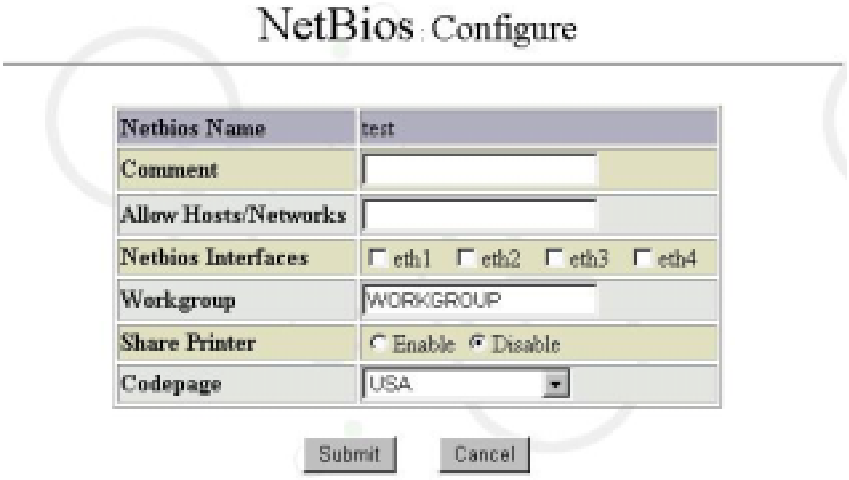
Maat file server.

Netbios Interface: It’s to activate the network interface for file share function.

Workgroup: It is the workgroup name that designate in Microsoft network environment.

Share Printer: It allowed you to “Enable” or “Disable” the printer share function.

Codepage: It’s to define the language code that you using in your nation. For example, in Japan area you will choose the “Japanese” to correctly show any file name that in Japanese word.

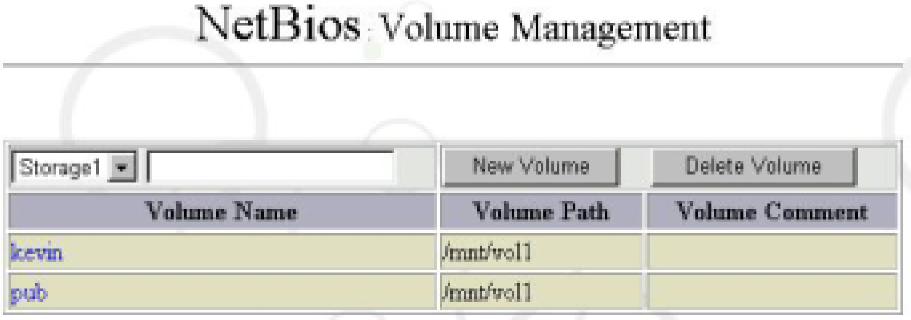


NetBios Configure

Netbios Name	test
Comment	
Allow Hosts/Networks	
Netbios Interfaces	□ eth1 □ eth2 □ eth3 □ eth4
Workgroup	WORKGROUP
Share Printer	○ Enable ● Disable
Codepage	USA

6.9.2 Volume Management

Click on the “Volume Management” you will see as follow:

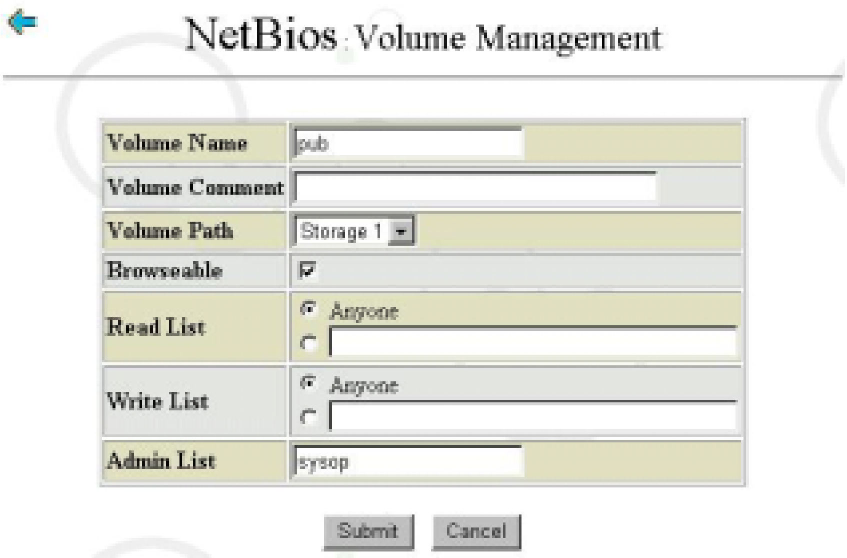


NetBios Volume Management

Storage1

Volume Name	Volume Path	Volume Comment
kevin	/mnt/vol1	
pub	/mnt/vol1	

Choose the Volume Name you going to configure. Here to choose “pub”. The screen show as below:



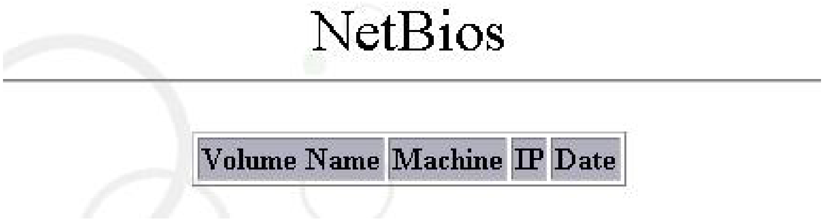
NetBios : Volume Management

Volume Name	pub
Volume Comment	
Volume Path	Storage 1
Browseable	☑
Read List	● Anyone ○
Write List	● Anyone ○
Admin List	sysop

You are allowed to modify the parameter for specific volume. There is default value shown as above.

6.9.3 Connection

Click "Connection" from "NetBios Services"; you can see the whole user connections established as shown in the figure below. They include "Volume Name", "Machine", "IP" and "Date".

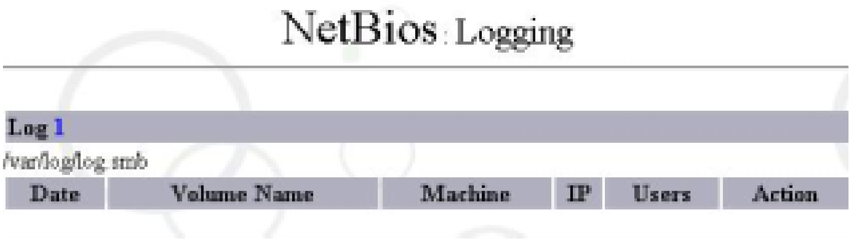


NetBios

Volume Name	Machine	IP	Date

6.9.4 NetBios Logging

Click "Logging" from "NetBios Services"; you can see if NetBios starts normally as shown in the figure below:



NetBios : Logging

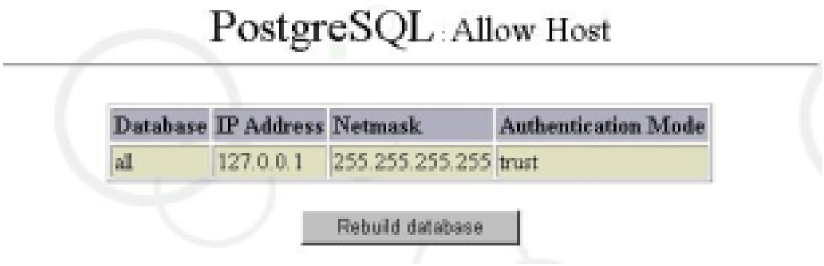
Log 1

/var/log/log.smb

Date	Volume Name	Machine	IP	Users	Action

6.10 PostgreSQL

PostgreSQL is a powerful object associated database containing many support capabilitites that are not provided by other databases. PostgreSQL features its support to various programming languages and provides commonly used accesses such as ODBC and JDBC. It also provides excellent support to Chinese. For the information of technical support, please refer to our official website: www.postgresql.org.

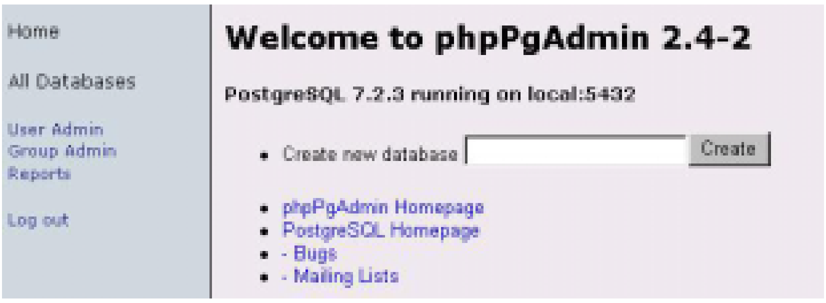


PostgreSQL : Allow Host

Database	IP Address	Netmask	Authentication Mode
all	127.0.0.1	255.255.255.255	trust

6.10.1 Database Admin

This system provides a simple and easy-to-use database administration system phpPgAdmin. To create a new database, or select or insert views in the database or table, users need only to click their mice several times and enter the required name as shown in the following figure.



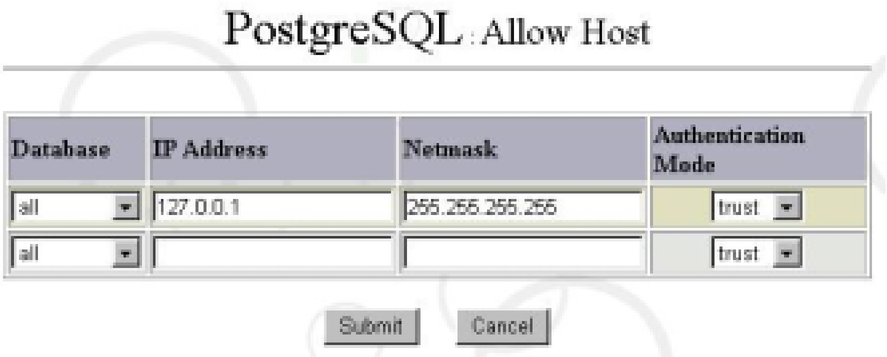
Welcome to phpPgAdmin 2.4-2

PostgreSQL 7.2.3 running on local:5432

- Create new database
- phpPgAdmin Homepage
- PostgreSQL Homepage
- - Bugs
- - Mailing Lists

6.10.2 Server Access Admin

This function is used to configure who may connect to PostgreSQL to use the database. To execute the configuration, select the database you want to configure and enter the address and netmask. You may then select trust to pass the configuration or select reject to block it in Authentication Mode.



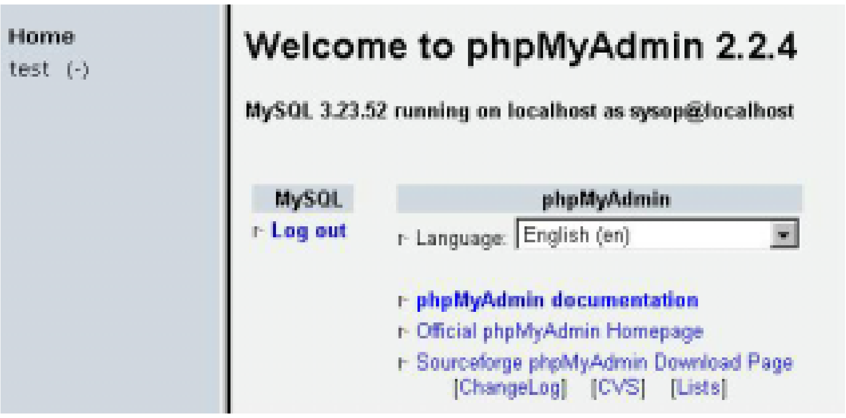
PostgreSQL : Allow Host

Database	IP Address	Netmask	Authentication Mode
all	127.0.0.1	255.255.255.255	trust
all			trust

6.11 MySQL

The Maat supported MySQL database from release of v3.01. MySQL database is more friendly and simple for programmers even their functions are very similar to PostgreSQL. The programmers can use PHP script language and MySQL to build a database function of web page. Any further questions please refer to the URL: www.mysql.com.

As the same as phpPgAdmin in PostgreSQL, The Maat also provided phpMyAdmin for MySQL database management. It is very simple and easy to create, select or insert the database table. Please refer to the following screen:



Home
test (-)

Welcome to phpMyAdmin 2.2.4

MySQL 3.23.52 running on localhost as sysop@localhost

MySQL
- Log out

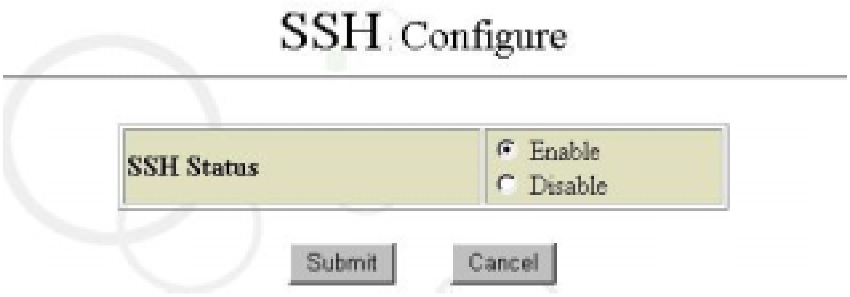
phpMyAdmin
- Language: English (en)
- phpMyAdmin documentation
- Official phpMyAdmin Homepage
- Sourceforge phpMyAdmin Download Page
  [ChangeLog] [CVS] [Lists]

6.12 SSH

SSH is a simple way to provided secure transmission of remote login session. It encrypted the command word and transmission data to prevent from any data monitoring. We are recommend you to use the SSH instead of Telnet to benefit the better security communication.

6.12.1 SSH Configuration

Click “Configure” from “SSH” service. You have choice to select “Enable” or “Disable” the SSH function. (For security issue, we recommended you to “Enable” the SSH function)


SSH Configure

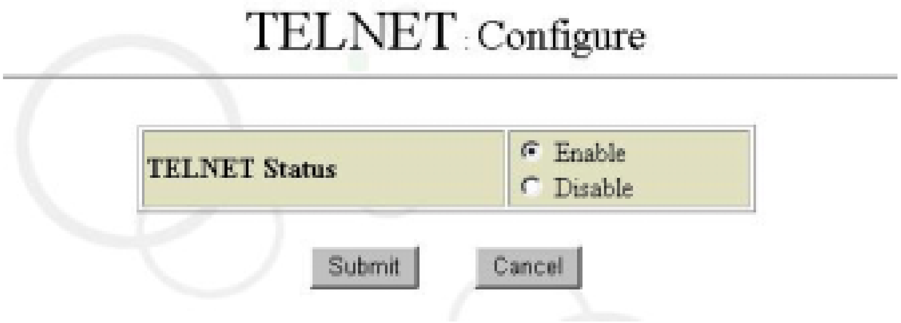
SSH Status	● Enable ○ Disable

6.13 TELNET

Telnet is a host, enabling login into remote-end host from near-end terminal (For example using Windows built-in telnet or other Terminal Freeware such as NetTerm or MultiTerm.)

6.13.1 TELNET Configuration

Click “TELNET” from “System Management Tools”. After clicking “TELNET Configure” you can optionally choose to start this function or not (For safety consideration it is recommended to close this function.) As shown in the figure below:


TELNET Configure

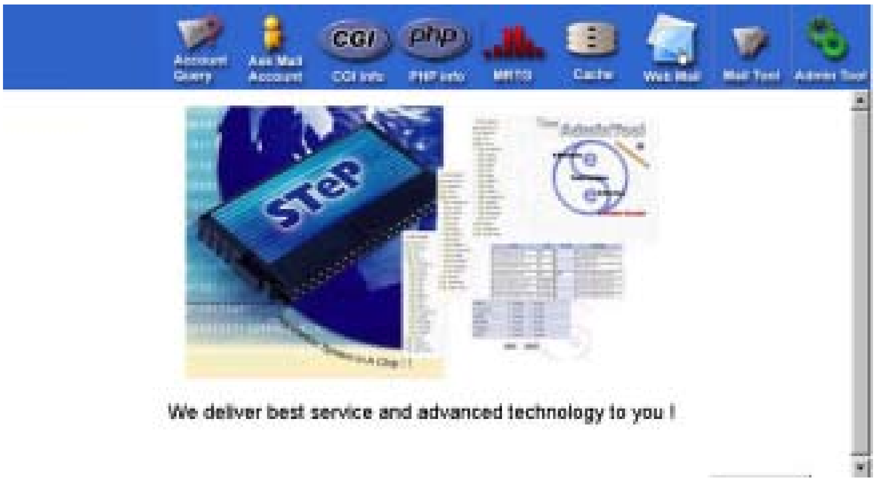
TELNET Status	● Enable ○ Disable

6.14 Web Mail

Open WebMail basically provides the same functions as other mail servers. The only difference is that it shows mails on web pages, which provides access flexibility for any location, any time and easy-use. No matter where users are, they need only browser at hand, then they can send and receive their own mail as they like.

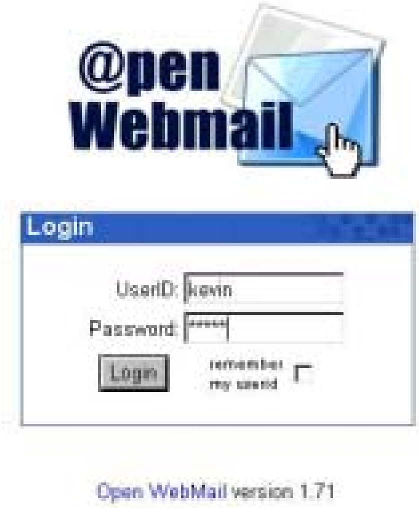
6.14.1 Operation Procedure to enter Open WebMail

Open browser directly to enter the system’s “hostname · domain” or “IP” in the web address column. Remember not to add “10000” and directly enter the system’s main screen. Click on “Web Mail” of “Service” , main screen of Web Mail appears as shown in Figure below:



We deliver best service and advanced technology to you !

Here are basic instructions to use Open WebMail. If you want to configure or view other functions, you can click to login your User ID and password. As shown in the figure below: Click “Web Mail” from “Mail Tool” to enter the Open WebMail login screen. Use your user ID and password to login.



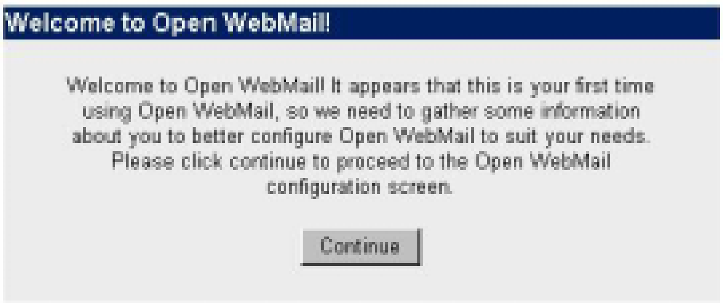
UserID: kevin

Password: *****

remember my userid □

Open WebMail version 1.71

If you are a new user or using the account for the first time, the following screen appears, indicating personal data and configurations are required. Click “Continue” to proceed.



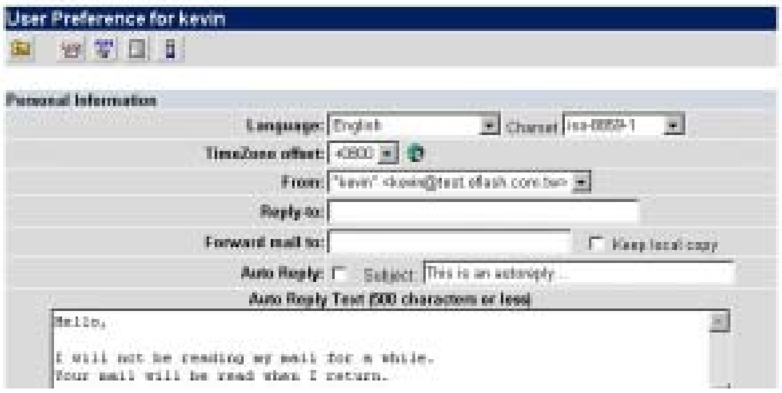
Welcome to Open WebMail!

Welcome to Open WebMail! It appears that this is your first time using Open WebMail, so we need to gather some information about you to better configure Open WebMail to suit your needs. Please click continue to proceed to the Open WebMail configuration screen.

Open WebMail version 1.71

6.14.2 User Preferences

Now configure personal data and personalized settings:



User Preference for kevin

Personal Information

Language: English Charset: iso-8859-1

TimeZone offset: +0800

From: "kevin" <kevin@test.eflash.com.tw>

Reply to:

Forward mail to: □ Keep local copy

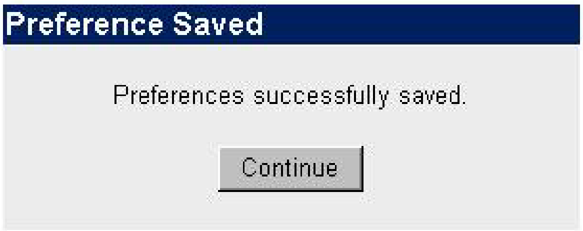
Auto Reply: □ Subject: This is an autoreply...

Auto Reply Text (500 characters or less)

```
Hello,

I will not be reading my mail for a while.
Your mail will be read when I return.
```

Click “Save” to save the configurations:

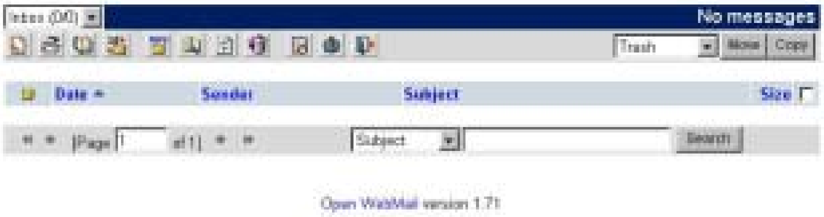


Preference Saved

Preferences successfully saved.

Open WebMail version 1.71

After clicking “Continue”, you can enter the Open WebMail screen. Select the folder on the upper left to enter the desired working mailbox, and then use tool icons on the Tool Bar to continue operation. As shown in the figure below:



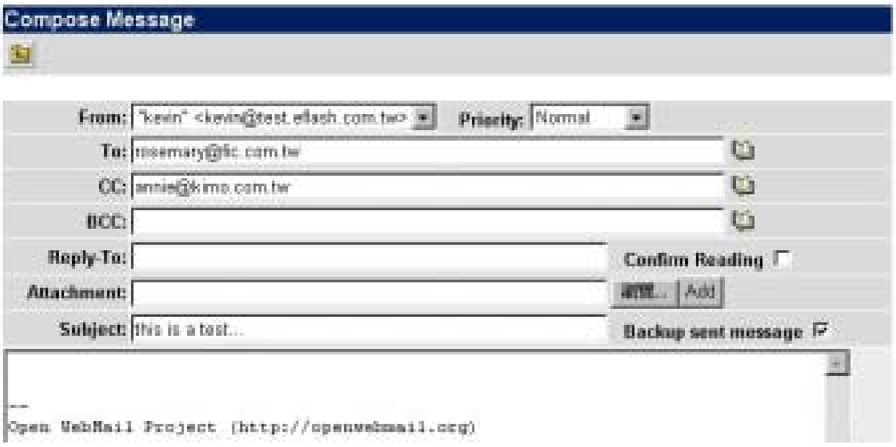
Inbox (0/0)

No messages

Open WebMail version 1.71

6.14.3 Compose Message

Click on “Compose Message” icon (shown as the Figure above) on the upper left to display new Compose Window. Its usage is similar to other e-mail software. After composing a new mail, click “Send” below the screen. As shown in the figure below:



Compose Message

From: "kevin" <kevin@test.eflash.com.tw>

Priority: Normal

To: rosemary@fic.com.tw

CC: annie@kimo.com.tw

BCC:

Reply-To:

Confirm Reading □

Attachment:

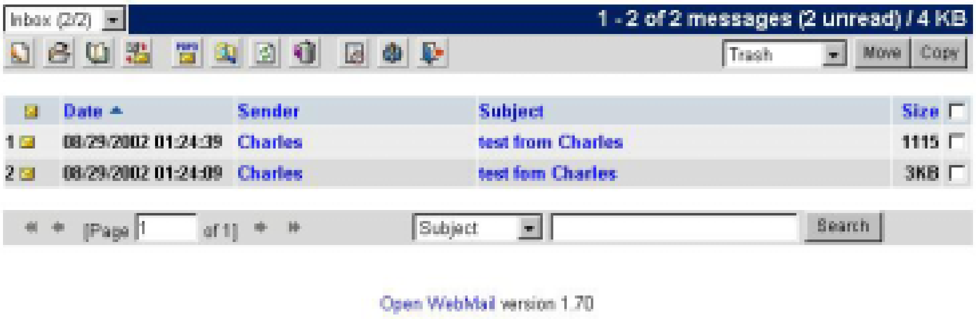
Subject: this is a test...

Backup sent message ☑

```
--
Open WebMail Project (http://openwebmail.org)
```

6.14.4 Check Mails

Click “Refresh” icon to receive your new mails. Remember to go to “Inbox” to view the received mails. As shown in the figure below:



Inbox (2/2)

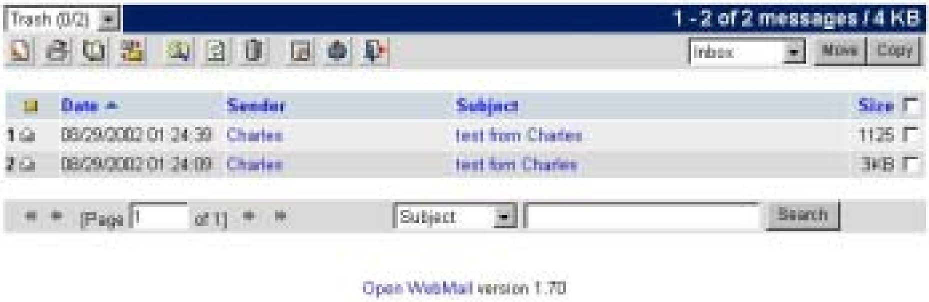
1 - 2 of 2 messages (2 unread) / 4 KB

	Date	Sender	Subject	Size
1	08/29/2002 01:24:39	Charles	test from Charles	1115 □
2	08/29/2002 01:24:09	Charles	test fom Charles	3KB □

Open WebMail version 1.70

6.14.5 Delete Mails

In any mailbox you only need to click on the checkbox on the right side of the mails, or if you want to select all mails, click on “All”. Then click on “Move” to move these mails to “Trash” (at this time these mails are not really deleted yet.). Go to “Trash” to make sure you want to delete the mails, click on “Empty Trash” icon, you can delete these emails permanently. As shown in the figure below:



Trash (0/2) 1 - 2 of 2 messages / 4 KB

Inbox Move Copy

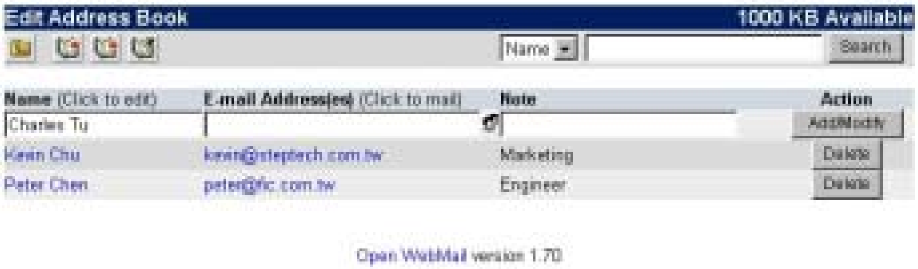
	Date ▲	Sender	Subject	Size □
1	08/29/2002 01:24:39	Charles	test from Charles	1125 □
2	08/29/2002 01:24:09	Charles	test fom Charles	3KB □

[Page 1 of 1] Subject Search

Open WebMail version 1.70

6.14.6 Address Book

Click on “Address Book” icon, you will enter “Edit Address Book”. You can input data manually or import data. As shown in the figure below:



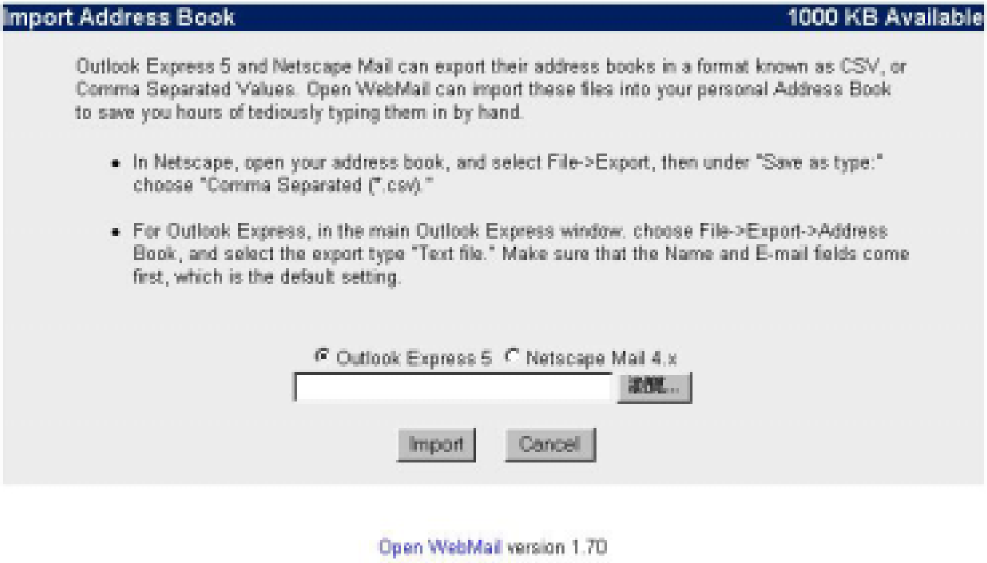
Edit Address Book 1000 KB Available

Name Search

Name (Click to edit)	E-mail Address(es) (Click to mail)	Note	Action
Charles Tu			Add/Modify
Kevin Chu	kevin@steptech.com.tw	Marketing	Delete
Peter Chen	peter@fic.com.tw	Engineer	Delete

Open WebMail version 1.70

In “Edit Address Book” you can see your personal address book. If you want to modify, you can click on name you want to modify. You can also import from exist file by click on “Import Addresses”. In Open WebMail the available formats are Outlook Express 5 and Netscape Mail 4.x. Noted that you should have files to be exported in Outlook Express 5 or Netscape Mail 4.x, then you can import to Open WebMail. As shown in the figure below:



Import Address Book 1000 KB Available

Outlook Express 5 and Netscape Mail can export their address books in a format known as CSV, or Comma Separated Values. Open WebMail can import these files into your personal Address Book to save you hours of tediously typing them in by hand.

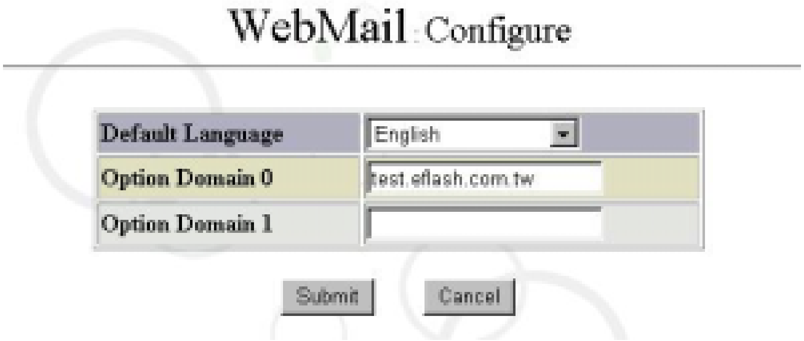
- In Netscape, open your address book, and select File->Export, then under "Save as type:" choose "Comma Separated (*.csv)."
- For Outlook Express, in the main Outlook Express window. choose File->Export->Address Book, and select the export type "Text file." Make sure that the Name and E-mail fields come first, which is the default setting.

● Outlook Express 5 ○ Netscape Mail 4.x

Open WebMail version 1.70

6.14.7 Web Mail Configure

Click “Configure” under “Web Mail” on “Service” of system management tool interface to set up language and domain name used on Open WebMail. The properties are automatically generated by the management interface when installing. Except to be used in modifying settings of DNS, normally they do not need to be modified.   (Note: This is closely related to mail services mentioned above. If the mail services are not activated, you cannot receive and send web-based mails either.) As shown in the figure below:

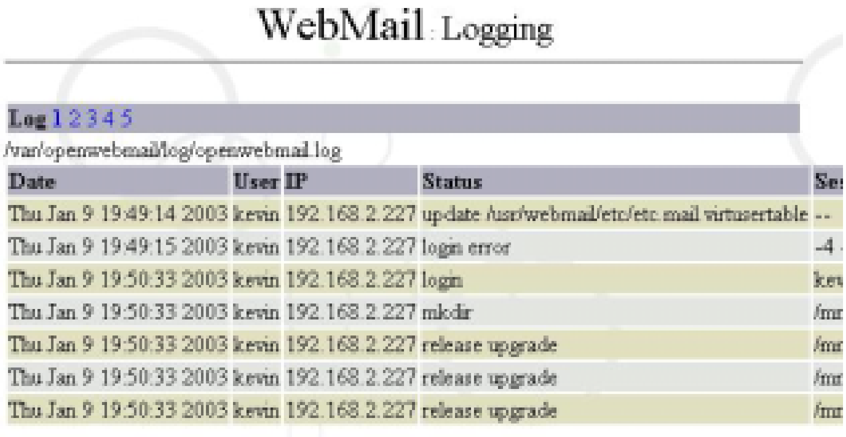


WebMail Configure

Default Language	English
Option Domain 0	test.eflash.com.tw
Option Domain 1	

6.14.8 Web Mail Logging

Click on “Web Mail” under “Service” from system management interface, and then click on “Logging”. You can view log file to analyze who the frequent users are and if there are any unauthorized users.



WebMail : Logging

Log 1 2 3 4 5

/var/openwebmail/log/openwebmail.log

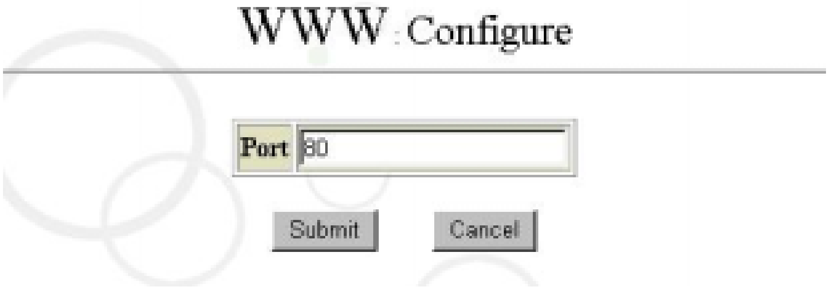
Date	User	IP	Status	Se
Thu Jan 9 19:49:14 2003	kevin	192.168.2.227	update /usr/webmail/etc/etc.mail virtusertable	--
Thu Jan 9 19:49:15 2003	kevin	192.168.2.227	login error	-4 -
Thu Jan 9 19:50:33 2003	kevin	192.168.2.227	login	kev
Thu Jan 9 19:50:33 2003	kevin	192.168.2.227	mkdir	/mr
Thu Jan 9 19:50:33 2003	kevin	192.168.2.227	release upgrade	/mr
Thu Jan 9 19:50:33 2003	kevin	192.168.2.227	release upgrade	/mr
Thu Jan 9 19:50:33 2003	kevin	192.168.2.227	release upgrade	/mr

6.15 Web Service

“Web Service” provides WWW Services. System presetting is “On”. If not activated, please click on “Service” on system management tool to change activation status.

6.15.1 Web Port Configure

Click on “Configure” you are allowed to configure “Port Number” for the web traffic. The default number is “80”.

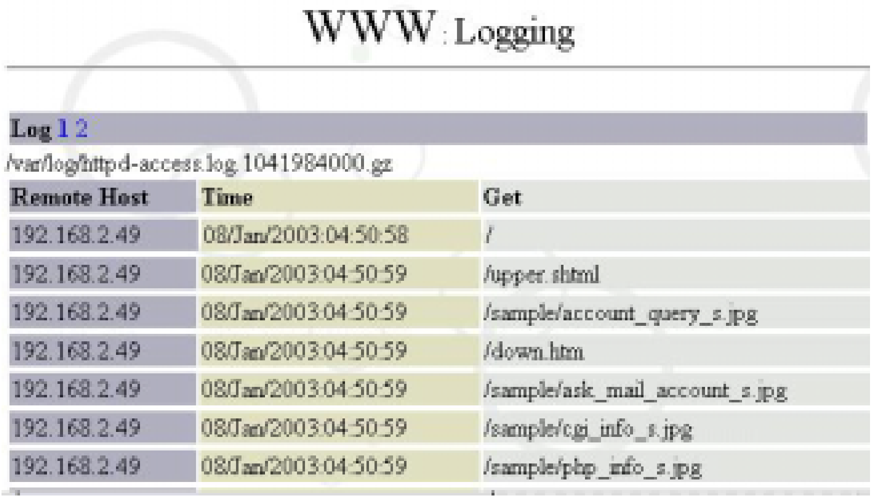


WWW : Configure

Port: 80

6.15.2 Web Service Logging

Click on “Web Service” under “Service” of system management tool, and then click on ‘Logging” to view the use of web services, and to check if there is any abnormal accesses.



WWW : Logging

Log 1 2

/var/log/httpd-access.log.1041984000.gz

Remote Host	Time	Get
192.168.2.49	08/Jan/2003:04:50:58	/
192.168.2.49	08/Jan/2003:04:50:59	/upper.shtml
192.168.2.49	08/Jan/2003:04:50:59	/sample/account_query_s.jpg
192.168.2.49	08/Jan/2003:04:50:59	/down.htm
192.168.2.49	08/Jan/2003:04:50:59	/sample/ask_mail_account_s.jpg
192.168.2.49	08/Jan/2003:04:50:59	/sample/cgi_info_s.jpg
192.168.2.49	08/Jan/2003:04:50:59	/sample/php_info_s.jpg

6.15.3 Place Homepage

1. **Place System Homepage**

   To place the finished homepage to Maat server, you must be administrator sysop, then you can use ftp to upload.

   For example, if the established web page is named index.htm（or index.html） and the host name is test.steptech.com.tw.

   Open a DOS Prompt (MS-DOS Mode) on Windows NT or Windows 9X.

   ```
   C：\> ftp test.steptech.com.tw
   User (test.steptech.com.tw：(none))：  sysop
   Password：  steptech
   ftp>put index.htm /www/data/index.htm
   ftp>bye
   C：\>
   ```

   Note: The preset homepage name is **index.htm** or **index.html** for the host.

2. **Place Personal Homepage**

   Supposed the personal user name is marx1976 and the host name is test.steptech.com.tw.

   Open a DOS Prompt (MS-DOS Mode) on Windows NT or Windows 9X.

   ```
   C：\> ftp test.steptech.com.tw
   User (test.steptech.com.tw：(none))：  marx1976
   Password：  xxx
   ftp>put index.htm /www/index.htm
   ```

```
ftp>bye
C：\>
```

Note: The preset homepage name is **index.htm** or **index.html** for the host.

In addition to using standard ftp command mode to upload web pages, you can also make use of various FTP package available on the market to meet your need and to upload more easily and quickly.

3. Show Web Page

We can enter "http：//your host name" in browser web address column, then we can see your system main pages. For each user's personal main page, enter "http：//your host/~user account/"; for example, the preset location of main page is http://test.steptech.com.tw and user web page is "http://test.steptech.com.tw/~marx1976/".

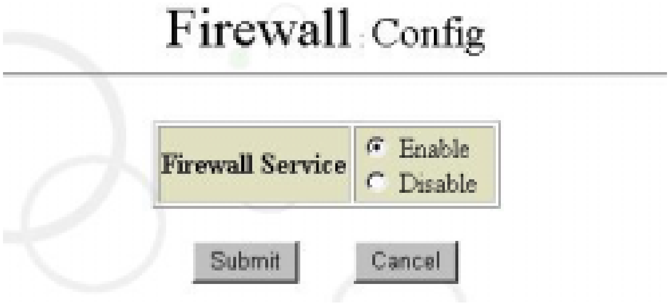
4. Supplement

▲ System main page location is under **/home/www/data/.** Each user's web page location is placed under users' personal directory www.

▲ When using ftp to upload, enter different account and password, the system will switch automatically to correct directory to avoid unnecessary troubles.

Chapter 7 Firewall

Maat system provided packet filter function for user to filter specific traffics. It allows user to define firewall rules by IP, port, protocol and direction of packet. This firewall function provided user a basic security infrastructure. Please click on “Configure” of “Firewall”. The diagram show as below:



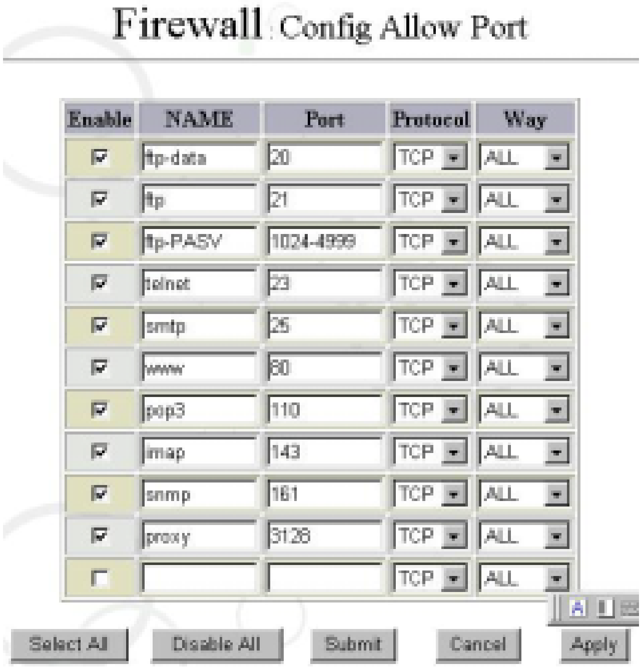
Firewall Config

Firewall Service	● Enable ○ Disable

Click on “Enable” to activate the firewall function.

7.1 Allow Port Configure

Maat system allows user to define their firewall rule depend on port, protocol (TCP or UDP) and direction of packet (Input or Output). System has pre-defined port number and protocol into the configuration table. User can click on desired item to enable (or disable) required configuration. Please click on “Config Allow Port”, the table show as below:

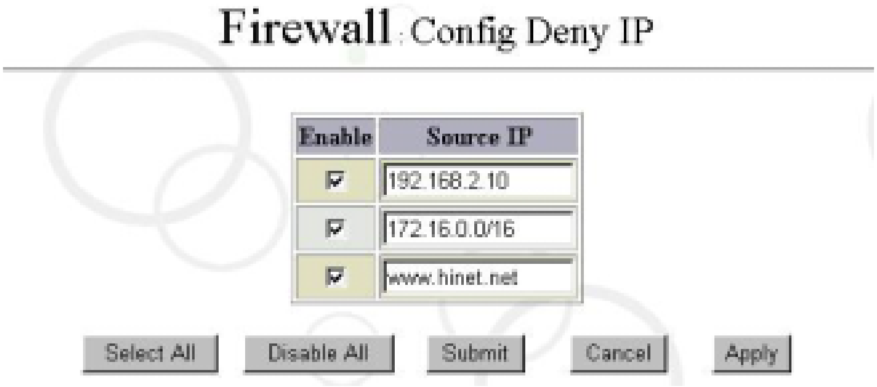


Firewall Config Allow Port

Enable	NAME	Port	Protocol	Way
☑	ftp-data	20	TCP	ALL
☑	ftp	21	TCP	ALL
☑	ftp-PASV	1024-4999	TCP	ALL
☑	telnet	23	TCP	ALL
☑	smtp	25	TCP	ALL
☑	www	80	TCP	ALL
☑	pop3	110	TCP	ALL
☑	imap	143	TCP	ALL
☑	snmp	161	TCP	ALL
☑	proxy	3128	TCP	ALL
□			TCP	ALL

7.2 Deny IP Configure

System allows user to deny single or multiple IP connections. User can input rules by IP address, Domain Name or Network. For example: 192.168.2.10, 172.16.0.0/16 or www.hinet.net. The input field will automatic expand without limitation. Please click on "Config Deny IP" the diagram show as below:



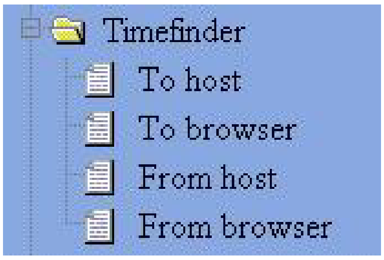
Firewall : Config Deny IP

Enable	Source IP
☑	192.168.2.10
☑	172.16.0.0/16
☑	www.hinet.net

Chapter 8 Timefinder

Timefinder is mainly used to backup and recover system data files. As for user data (such as homepage and mails) tape driver and disk array are needed to provide protection. The focus of host system design is an Internet Server, not a File Server. So the major function of Timefinder is to protect system's data files.

Timefinder features four main operations. The functions are divided into backup and recovery as shown in the Figure below:



Among them, "Timefinder from Browser" enables users to automatically upload data （browser→ host）after clicking, especially when using uploaded function of browser.

If you have any difficulty when operating Timefinder, it is mostly because MIME of your current browser is modified. Please reinstall browser.

Usually when you modified system settings or used management interface to change various functions and tested, you need to backup your Timefinder. If you are still at testing period, please do not backup the system data; otherwise the system will be unstable. That is why Timefinder did not activate automatic backup.

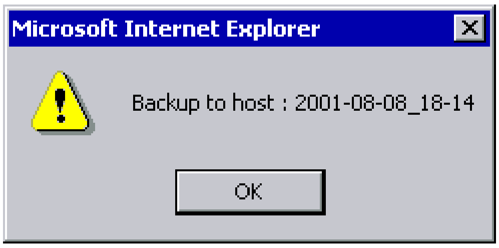
Timerfinder needs 200-300K to backup, Though the space is not considerably large, backup can include the settings of the whole system (except homepage and mail) and automatically keep ten times. The old ones will be automatically deleted when the system is restarted next time.

Timefinder's recovery function can not only recover the system settings, but also correct user directory with kernel (in case that accounts of system password files exceeded the number stored in current hard disk). Also it can correct the causes resulting in shutdown of system, such as /tmp、/var、/lost+found.（Note: The function enhancement of Maat kernel is finished. But these are not the original kernel functions for FreeBSD.）

The following operations are quite easy. Flow chart and figures are provided to help users understand.

8.1 Backup to Host

Select “To Host” on “Timefinder” of management interface, as shown in the figure below:



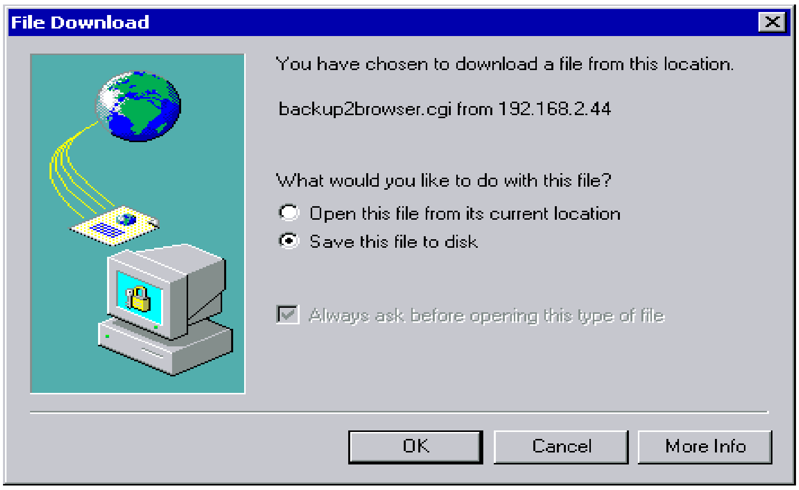
Microsoft Internet Explorer

Backup to host : 2001-08-08_18-14

Click “OK” to complete backup.

8.2 Backup and Download

Select “To browser” on “Timefinder” of management interface, as shown in the figure below:



File Download

You have chosen to download a file from this location.

backup2browser.cgi from 192.168.2.44

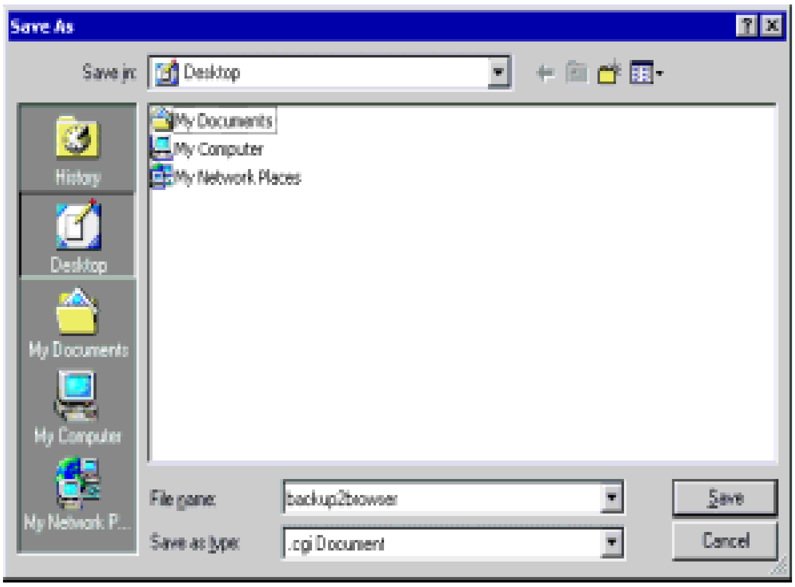
What would you like to do with this file?

○ Open this file from its current location

● Save this file to disk

☑ Always ask before opening this type of file

You can change directory and name and click “Save”.



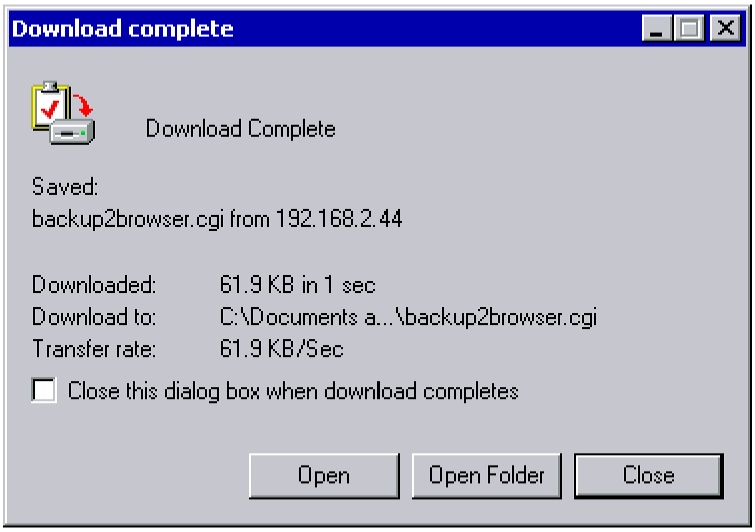
Save in: Desktop

My Documents
My Computer
My Network Places

File name: backup2browser

Save as type: .cgi Document

Click “Save” as shown below:



Download Complete

Saved:
backup2browser.cgi from 192.168.2.44

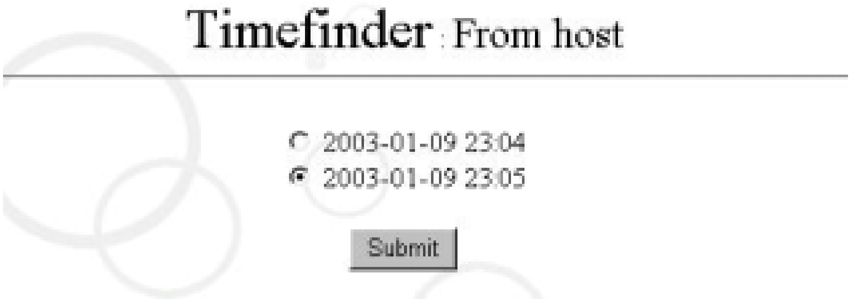
Downloaded: 61.9 KB in 1 sec
Download to: C:\Documents a...\backup2browser.cgi
Transfer rate: 61.9 KB/Sec

□ Close this dialog box when download completes

Now “Backup to Current Computer” is completed. Please remember the saved directory and file names for next restore.

8.3 Timefinder from Host

Select “From Host” on “Timefinder” of management interface, as shown in the figure below:

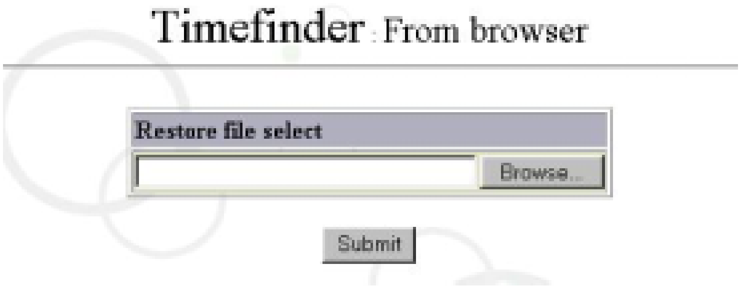


○ 2003-01-09 23:04
● 2003-01-09 23:05

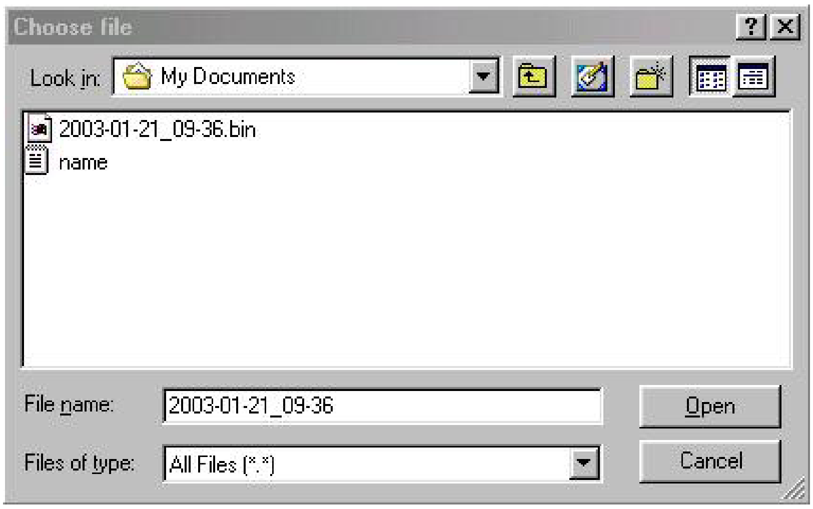
Click on the time you want to restore and click ” Submit”. This means “Timefinder from Host” is completed. The system will be rebooted and restored to your selected time point.

8.4 Timefinder from Browser

When you select “From Browser” from “Timefinder” as shown in the Figure below:



Click “Browse”, the Figure below appears.



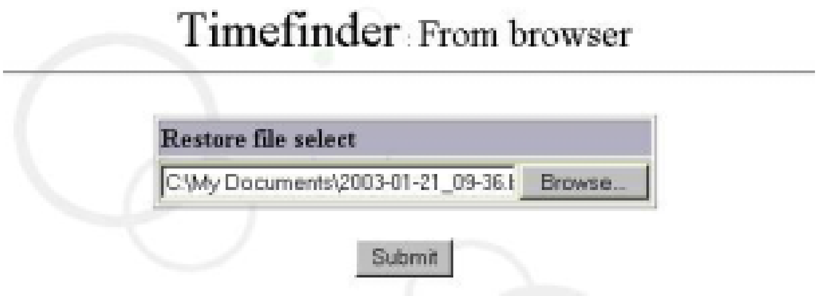
Look in: My Documents

2003-01-21_09-36.bin
name

File name: 2003-01-21_09-36

Files of type: All Files (*.*)

Select restored file as shown in the Figure below:

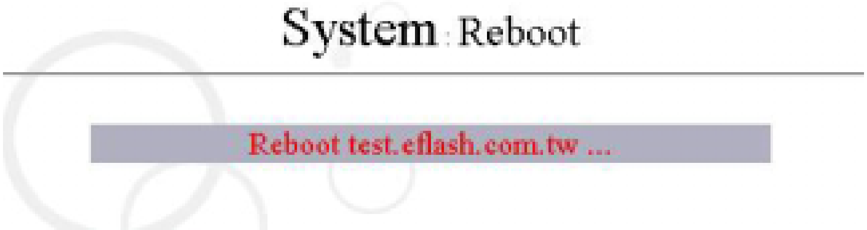


Timefinder : From browser

Restore file select

C:\My Documents\2003-01-21_09-36.t

Click ” Submit” to begin restoring files. When it has finished, the system will reboot.

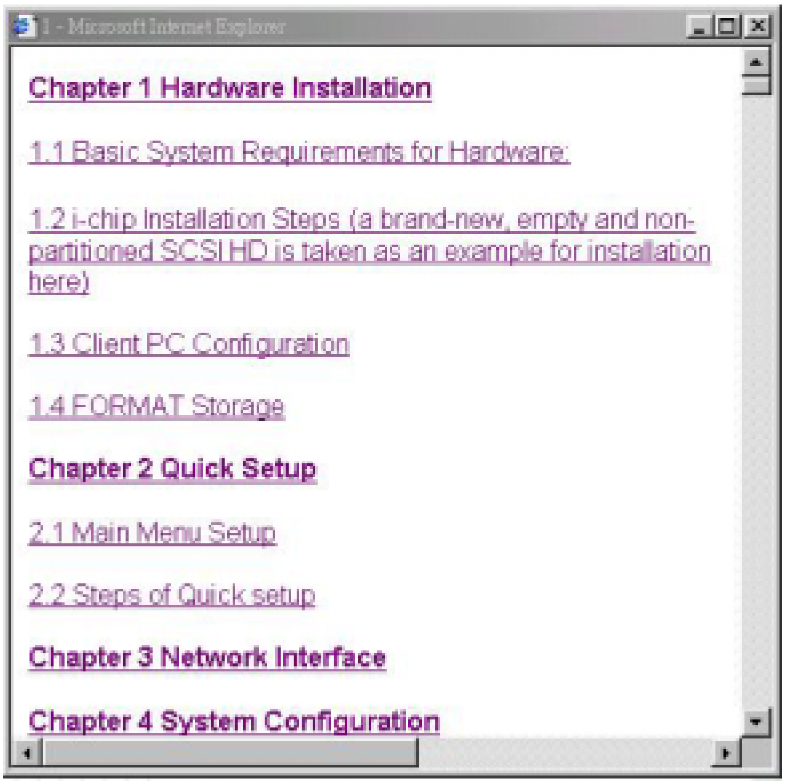


System : Reboot

Reboot test.eflash.com.tw ...

CHAPTER 9 Online Help

In this version of Maat is capable to support Online Help function. User just click on “Online Help” in left side of the GUI screen. The user manual’s text will pop on as shown as picture below:



Chapter 1 Hardware Installation

1.1 Basic System Requirements for Hardware:

1.2 i-chip Installation Steps (a brand-new, empty and non-partitioned SCSI HD is taken as an example for installation here)

1.3 Client PC Configuration

1.4 FORMAT Storage

Chapter 2 Quick Setup

2.1 Main Menu Setup

2.2 Steps of Quick setup

Chapter 3 Network Interface

Chapter 4 System Configuration

Click on the text will link to the section that you required. If you finished to view the Online Help just close the screen box. If any further questions please contact with your local representatives for technical support.

WARNING:

FCC Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiated radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.