smartguard

smartguard

the smartest way to manage **broadband**

XS Infoways

the invincible technology

XS Infoways

the invincible technology

ver. **4.0.4**

Updated:06/27/2006

smartguard

XS Infoways End user license agreement

Please read this end user license agreement ("eula") carefully before downloading or using this software. By accepting the license agreement, opening the package, downloading the product, or using the equipment that contains this product, you Are consenting to be bound by this agreement.

If you do not agree to all of the terms of this agreement, you will not be able to continue.
In addition:

(1) if you purchased the product, return the product to the place of purchase for a full refund; or,

(2) if you are otherwise attempting to download the product and you do not agree with the terms of this agreement, do not Complete the download; or,

(3) if your software was included in equipment which you purchased and you do not agree with the terms of this agreement,

Do not use the software.

IMPORTANT - READ CAREFULLY: this Eula is a legal agreement between you (either an individual or a single entity) and XS Infoways. ("XS Infoways"), covering your use of the software product(s) identified above (the "program"). The program includes computer software, and may include associated media, printed materials, and "online" or electronic documentation. By installing, copying, downloading, accessing or otherwise using the program, you agree to be bound by the terms of this Eula.

If you do not agree to the terms of this Eula, XS Infoways is unwilling to license the program to you, you may not use or copy the program, and you should follow the instructions above concerning return or non-use of the unused product(s) for a refund. The program is protected by copyright laws as well as other intellectual property laws and treaties.

The program and the accompanying documentation are licensed, not sold, to you. This includes any updates or upgrades to the program licensed to you by XS Infoways.

If the program is labeled as an upgrade, you must be properly licensed to use a product identified by XS Infoways as being eligible for the upgrade in order to use the program.

If the program is an upgrade of a component of a package of software programs that you licensed as a single product, the program may be used and transferred only as part of that single product package and may not be separated for use on more than one computer. Subject to the terms of this agreement, you have a non-exclusive and non-transferable right to use the program and documentation.

For each registered serial number and software license key you purchase, you may use this program on a single computer within the United States and its territories or any other country to which this program can legally be exported. This program is "in use" on a computer when it is loaded into temporary memory or installed in permanent memory (hard drive, CD-Rom or other storage device). The term "computer" as used herein shall mean the hardware, if the hardware is a single computer system, or shall mean the computer system with which the hardware operates, if the hardware is a computer system component. You agree to use your best efforts to prevent and protect the contents of the program and documentation from unauthorized use or disclosure. You agree that you will register this program and its serial number only with XS Infoways or one of its authorized distributors and that you will only install a software license key obtained directly from XS Infoways.

You may not rent, lease, sell or otherwise transfer or distribute copies of the program to others, nor may you create derivative works of the program.

You may not modify or translate the program or documentation without the prior consent of XS Infoways. You may not reverse engineer, reverse compile, disassemble, or otherwise attempt to create the source code from the program.

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

You may not release the results of any performance or functional evaluation of any XS Infoways program to any third party without written approval of XS Infoways for each such release.

The customer agrees that aspects of the licensed materials, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of XS Infoways.

The customer agrees not to disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of XS Infoways. Customer agrees to implement reasonable security measures to protect such trade secrets and copyrighted material.

Title to the program and documentation shall remain solely with XS Infoways. You may not redistribute, bundle, or package any free program or software downloaded or obtained from XS Infoways without the prior written consent of XS Infoways.

You may not use any free program or software downloaded or obtained from XS Infoways in the production of a commercial product without the prior written consent of XS Infoways. You may make copies of the program and software license key for backup purposes. You may physically transfer the program, documentation, and software license key from one computer to another provided that the software license key is only installed or used on the original computer that generated the program's serial number.

The only way that this license may be transferred to another computer is by physically moving the hard disk that the program and operating system is installed on to the new computer. Except as expressly provided in this eula, you may not otherwise make copies of the program, including the printed materials accompanying the program. This license is effective until terminated. You may terminate this license at any time by destroying the program, documentation, and software license key as well as each backup copy.

Without prejudice to any other rights, XS Infoways may terminate this eula if you fail to comply with the terms and conditions of this eula. In such event, you must destroy all copies of the program and all of its component parts. This license automatically terminates if you fail to comply with its terms and conditions. You agree that, upon such termination, you will either destroy (or permanently erase) all copies of the program,

Documentation, and software license key.

This eula does not grant you any rights in connection with any trademarks or service marks of XS Infoways or its suppliers. All title and intellectual property rights in and to the program (including but not limited to any images, photographs, animations, video, audio, music, text and

XS Infoways,
T-3, Govind Bhawan,
4384/4a, Ansari Road, Darya ganj
New Delhi - 110002, India.
Contact No. 91-011-23253236, 32908202, and 32533074
Website: http://www.XS Infoways.com
Email: sales@XSInfoways.com

"Applets," incorporated into the program, the accompanying printed materials, and any copies of the program, are owned by XS Infoways or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the program is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This Eula grants you no rights to use such content.

To the maximum extent permitted under applicable law, XS Infoways and its supplier's entire liability and your exclusive remedy under the express warranty is, at XS Infoways' option, either **(a)** return of the price paid; or **(b)** repair or replacement of the program which does not meet the warranty and which is returned to XS Infoways with written confirmation of your purchase of the program. The warranty is void if failure of the program has resulted from accident, abuse or misapplication. Any replacement program will be warranted for 30 days.

smartguard

The following is without prejudice to any rights you may have at law which cannot legally be excluded or restricted. XS Infoways and its distributors provide the program and documentation "as is" without warranty of any kind either express, implied or statutory, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, non infringement or arising from a course of dealing, usage or trade Practice. You acknowledge that no promise, representation, warranty or undertaking has been made or given by XS Infoways to any person or company on its behalf in relation to the profitability of or any other consequences or benefits to be obtained from the delivery or use of the program, manuals or written materials. You have relied upon your own skill and judgment in deciding to acquire the program and any accompanying manuals and written materials for use by you. In no event does XS Infoways warrant that the program is error free or that you will be able to operate the program without problems or interruptions.

In no event will XS Infoways or its licensors be liable for any lost revenue or data or other direct or indirect damages or other relief arising out of your use or inability to use the program for any reason whatsoever including, by way of illustration and not limitation, lost profits, lost business or lost opportunity, business interruption, loss of business information, or any special, incidental or consequential or exemplary damages, including legal fees, arising out of such use or inability to use the program, or supply or non-supply the program, even if XS Infoways, its licensors or authorized distributors or supplier has been advised of the possibility of such damages, or any claim by any other party. This limitation on liability is equally applicable to any damages arising out of any year 2000 date problem or any other non-year 2000 date problem of any kind whatsoever, whether the damages result from actions or inactions of XS Infoways or are the result of third parties. XS Infoways' total liability under any provision of this agreement is in any case limited to the amount actually paid by you for the program. The Foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. Some states do not allow limitation or exclusion of liability for consequential or incidental damages.

© 2002 XS Infoways. All rights reserved. End user license agreement. Revised, Oct, 2006

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

smartguard

INDEX

TABLE OF CONTENTS

1. INTRODUCTION 10

1.1 INTERNET TRAFFIC PROBLEM 10
- IT Undermined : 10
- Inefficient Systems : 10
- Wasted Time : 10

1.2 SMART GUARD FEATURES 12
1.3 INTRODUCTION TO SMARTGUARD BROAD BAND MANAGER 16
1.4 SMARTGUARD IN NETWORK 17

2. GETTING STARTED 20

2.1 INSTALLATION 20
2.1.1 Minimum System Requirement 20
2.1.2 Installation Instruction 20

3. WELCOME TO SMARTGUARD 28

3.1 LOGIN PAGE 28
3.1.1 ADMIN CONTROL PANEL 28
Admin Login Window 28
Main Menu 28

4. FIREWALL 31

4.1 FIREWALL 38
4.1.1 FIREWALL 38
4.2 FIREWALL NAT 42

5. CONTENT FILTER 44

5.1 CACHE SERVER 44
8.1.1 Configuration 51
8.1.2 Block Sites 56

6. BANDWIDTH MANAGEMENT 58

6.1 POOL MANAGEMENT 60
6.1.1 Create Pool 61
6.1.2 Modify Pool 62
6.1.3 Delete Pool 63
6.1.4 Pool Bustable 64
6.2 PORT MANAGEMENT 64
6.2.1 Ports 65
6.2.1.1 Create Port 66
6.2.1.2 Modify Port 67
6.2.1.3 Delete Port 68
6.2.2 Ports packaging 69
6.2.2.1 Create Port package 69
6.2.2.2 Modify Port package 71

6.2.2.3 Delete Port package 72
6.3 ACCESS POLICY 73
6.3.1 Create Access Policy 73
6.3.2 Modify Access Policy 74
6.3.3 Delete Access Policy 75
6.4 DATA TRANSFER POLICY 76
6.4.1 Create Data Transfer Policy 76
6.4.2 Modify Data Transfer Policy 77
6.4.3 Delete Data Transfer Policy 78
6.5 SURFING POLICY 79
6.5.1 Create Surfing Policy 80
6.5.2 Modify Surfing Policy 80
6.5.3 Delete Surfing Policy 81
6.6 BANDWIDTH POLICY 82
6.6.1 Create Bandwidth Policy 82
6.6.2 Modify Bandwidth Policy 83
6.6.3 Delete Bandwidth Policy 84
6.7 PACKAGE 85
6.7.1 Create package 86
6.7.2 Modify package 88
6.7.3 Delete package 89
6.8 PACKAGE SWITCHING 90
6.8.1 Create Package Switching 91
6.8.3 Delete Package Switching 91
6.9.1 CREATE NEW USERS 92
6.9.1.1 Basic User 93
6.9.1.2Advanced User 96
6.9.2 USER PROFILE 100
6.9.2.1 Change Password 101
6.9.2.2 Package 102
6.9.2.3 Renew User 103
6.9.2.4 Disconnect 104
6.9.2.5 Time Usage 104
6.9.2.6 Data Usage 105
6.9.2.7 Graph 106
6.9.2.8 Spy Watch 108
6.9.2.9 Installation 109
6.9.2.10 Information 110
6.9.2.11 IP 111
6.9.2.12 View Package 112
6.9.2.13 Flush IP Cache 113
6.9.3 VIEW ALL USERS 113
6.9.4 SEARCH 114
6.9.5 ONLINE USER 116
6.9.6 OFFLINE USERS 117

8.DHCP SERVER 119

8.3 DHCP SERVER 122
8.3.1 Edit DHCP Server 122
8.3.2 Add User Mac ID 123

9.MAIL SERVER 125

9.1 MAIL SERVER 125
9.2.1 User Manage 155
9.2.2 Mail Relay 156
9.2.3 Spam Configuration 157

9.2.4 Web mail 158
9.2.5 Domain Map 158
9.4 FETCHMAIL SERVER 159

10. LOAD BALANCING/MULTIPLE ISP/FAILOVER 161

10.3 NETWORKING 161
10.3.1 LAN 161
10.3.2 GATEWAY 162
10.3.3 DNS 163
10.3.4 WAN 163
10.3.4.1 ISP 1 164
10.3 NETWORKING 166

11. PRE PAID COUPONS 176

12. TOOLS 180

12.1 GREETING MESSAGE 180
12.2 SYSTEM 181
12.2.1 System Info 182
12.2.2 Reboot Server 183
12.2.3 Shutdown 183
12.3 NETWORKING 184
12.3.1 LAN 184
12.3.2 GATEWAY 185
12.3.3 DNS 186
12.3.4 WAN 186
12.3.4.1 ISP 1 187
12.3.5 VIRTUAL INTERFACE 188
12.5 NETWORK UTILITIES 188
12.6 BLOCK MESSENGER 189
12.7 TIME 190

13. SERVER MANAGEMENT 192

13.1 CACHE SERVER 192
13.1.1 Configuration 193
13.1.2 Block Sites 194
13.2 MAIL SERVER 194
13.2.1 User Manage 195
13.2.2 Mail Relay 195
13.2.3 Spam Configuration 196
13.2.4 Web mail 196
13.2.5 Domain Map 197
13.3 DHCP SERVER 197
13.3.1 Edit DHCP Server 197
13.3.2 Add User Mac ID 198
13.4 FETCHMAIL SERVER 199

14. SERVICES 202

14.1 RESTART MANAGEMENT SERVICES 202
14.2 SERVICES STATUS 202

15. BACKUP AND RESTORE 205

15.1 BACKUP DEFINE 205
15.2 BACKUP 206
15.3 UPLOAD SOFTWARE 206

15.4 SOFTWARE CATEGORY....206
15.5 UPLOAD SOFTWARE....207
15.6 DOWNLOAD SOFTWARE....207
15.7 LIVE USERS....208
15.8 LIVE SUPPORT....208
15.9 RESTORE....208
15.10 ADD IP RANGE....209
15.11 MULTIPLE IP....209
15.12 SINGLE IP....209
15.13 PUBLIC IP SUPPORT....210

16. REPORTS....213

16.1 USER DETAILS....213
16.1.1 Data Transfer....214
16.1.2 Time Usage....214
16.1.3 Expire Package....215
16.1.4 User Details....215
16.2 RENEW....216
16.2.1 Renewed Users....216
16.2.2 Renew Due....217
16.3 CR/DR STATEMENT....217
16.4 REVENUE REPORT....217
16.5 GRACE PERIOD USERS....218
16.6 PACKAGE WISE USERS....218
16.7 VIEW LOGS....219
16.7.1 Event Logs....219
16.7.2 Network Logs....220
16.7.3 System Logs....221
16.7.4 Server Logs....222
16.8 PREPAID CODE LOGS....224
16.9 RENEW USER REPORTS....225

17. GRAPHS....227

17.1 LAN....227
17.2 WAN....229
17.3 POOL....230

18. DOWNLOADS....234

19. FAQ....236

20. GLOSSARY....239

21. REAL LIFE SCENARIOS AND CASE STUDIES....267

smartguard

Chapter 1

Introduction

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

1. INTRODUCTION

1.1 Internet Traffic Problem

Lost Your Way?

The requested web page wasn't found.

This could be for a variety of reasons, including:

- You followed a broken or out-of-date link.
- You entered the URL incorrectly.
- The file no longer exists.

Internet is the key of any company's future. But, this critical resource is subject to traffic congestion and slows down, as a result of increasing levels of IP traffic and the Inherent unmanaged nature of the internet. The cost of sitting back and not effectively managing your Internet traffic is great:

- **IT Undermined :**

  Today, most of the company's backbone is IT department. If in that department users complaint's about Internet access, and, What next? nothing It damages the company's credibility financially as well as morally.

- **Inefficient Systems :**

  The other cause is the traffic congestion slows access for all the user that needs access to the t net whether they belong to a giant company or a small one.

- **Wasted Time :**

  You use to waste the time tracking down what users are doing with internet connection and services but, it doesn't have to be this way. SmartGuard Broadband Bandwidth Manager allows you to take back control of your Internet Connection, by prioritizing your limited bandwidth capacity based on criticality and merit guaranteeing that mission critical services, users and tasks always have Internet bandwidth when it's needed.

Because of Internet Security Vulnerabilities:

The SANS Top 20 Internet Security Vulnerabilities

Four years ago, the SANS Institute and the National Infrastructure Protection Center (NIPC) at the FBI released a document summarizing the Ten Most Critical Internet Security Vulnerabilities. Thousands of organizations used that list, and the expanded Top-20 lists that followed one, two, and three years later, to prioritize their efforts so they could close the most dangerous holes first. The vulnerable services that led to worms like Blaster, Slammer, and Code Red have been on these lists.

This SANS Top-20 2005 is a marked deviation from the previous Top-20 lists. In addition to Windows and UNIX categories, we have also included Cross-Platform Applications and Networking Products. The change reflects the dynamic nature of the evolving threat landscape and the vulnerabilities that attackers target. Unlike the previous Top-20 lists, this list is not "cumulative" in nature. We have only listed critical vulnerabilities from the past year and a half or so. If you have not patched your systems for a length of time, it is highly recommended that you first patch the vulnerabilities listed in the Top-20 2004 list.

We have made a best effort to make this list meaningful for most organizations. Hence, the Top-20 2005 is a consensus list of vulnerabilities that require immediate remediation. It is the result of a process that brought together dozens of leading security experts. They come from the most security-conscious government agencies in the UK, US, and Singapore; the leading security software vendors and consulting firms; the top university-based security programs; many other user organizations; and the SANS Institute. A list of participants may be found at the end of this document.

The SANS Top-20 is a living document. It includes step-by-step instructions and pointers to additional information useful for correcting the security flaws. We will update the list and the instructions as more critical vulnerabilities and more current or convenient methods of protection are identified, and we welcome your input along the way. This is a community consensus document -- your experience in fighting attackers and in eliminating the vulnerabilities can help others who come after you. Please send suggestions via e-mail to top20@sans.org.

Top Vulnerabilities in Windows Systems

- W1. Windows Services
- W2. Internet Explorer
- W3. Windows Libraries
- W4. Microsoft Office and Outlook Express
- W5. Windows Configuration Weaknesses

Top Vulnerabilities in Cross-Platform Applications

- C1. Backup Software
- C2. Anti-virus Software
- C3. PHP-based Applications
- C4. Database Software
- C5. File Sharing Applications
- C6. DNS Software
- C7. Media Players

- C8. Instant Messaging Applications
- C9. Mozilla and Firefox Browsers
- C10. Other Cross-platform Applications

Top Vulnerabilities in UNIX Systems

- U1. UNIX Configuration Weaknesses
- U2. Mac OS X

Top Vulnerabilities in Networking Products

- N1. Cisco IOS and non-IOS Products
- N2. Juniper, CheckPoint and Symantec Products
- N3. Cisco Devices Configuration Weaknesses

For all the tensions and vulnerabilities sit back and relax SmartGuard is here with righto solution:

1.2 Smart Guard Features

- **Subscriber Internet Management**
- **Bandwidth Management**
- **Load Balancing**
- **Multiple ISP support**
- **Easy Administration**
- **Firewall**
- **Mail Server**
- **Virus Scanning**
- **Proxy Server**
- **Cache Server**
- **Wi-Fi Support**
- **Master-Slave Module**
- **Port Management**
- **Package Management**
- **Billing (Invoicing)**
- **Pre-Paid Coupon (PPC)**
- **Real Time Usage Reporting**
- **Extensive Management Report**
- **Reports**
  - Top Site access report

smartguard

- Denied Site Reports
- Site Wise User Reports
- Data Transfer & System Reports
- Upload & Download Data Transfer Of Individual Subscribers
- Debit & Credit Account Statement

- **Advanced Ticketing Support System**
- **MRTG Generated Individual Pool graphs**
- **MRTG Generated LAN/WAN Graphs**

Smartguard is a complete software solution for Internet & Bandwidth Management in IT savvy Enterprises, and optimizing IT Resources. In addition, it is bundled with capabilities of providing network security, Site to Site access. With increasing growth of Internet Usage at Work Place and accessibility of different resources, Software plays a crucial role in providing you with Manageability and Control.

Software with features like Bandwidth Control, Policy Maker, Flexible URL/Keyword Filtering, Restrictions, Security, Web Caching, Firewall, Printer Control and much more will help you to Increase Productivity and save on Expensive Bandwidth

Time and Day Internet Access with clear definition of Surfing & Service, organization can very well make most efficient use of available bandwidth and reduce the traffic with caching feature of This Software.

The Reporting tool gives a comprehensive Analysis of Internet usage in the organization and can be viewed remotely with valid user rights. Reports can show a Bird's Eye view of the Internet and IT Resource usage as well as a more detailed report on Group / Departments and Individual Logs. With details based on Data transfer, URL Visited, Time & Date, IT managers can keep a detailed track of the enterprise activities on the Internet.

Software helps the IT Manager to easily define and implement the Internet Policy in the organization that meets Employee's Expectations. This can be done without compromising the productivity and reduces wastage of Resources. Software is the Tool of the Future that would help transform your enterprise into a truly best E-Organization.

"Software saves Enterprises the cost of purchase and support of Multiple Network Appliances. Software reduces network related calls, provides security, and increases productivity."

Specification

· Enterprise & Bandwidth Management Software .
· Application software is Linux Based & Seamlessly Integrated
· No Client Application required.

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

smartguard

· **Username / Password Based Internet Access**
· **Restrictions based on Services / Website / Printing available**
. **Firewall / UTM**
. **Pre-Paid Module**
· **Complete Application works on Server Class Machine**
· **Proprietary Product with company own support & services**

1. Bandwidth Management
a. Based on IP, User, Group
b. Based on Services & Application
c. CIR & CBR - Upload / Download (E.g. 16 Kbps Upload / 64 Kbps Download)
d. Scheduling on Week days & Time
e. Multiple Link Support & Management
f. Bandwidth Sharing & Individual Connection
g. Bandwidth Online Utilization Graphs & Reports

2. Content Management with Online Web Categorization
a. Based on URL & Keywords
b. Based on Online Website Screening & Categorization
c. Preloaded Websites & Categories
d. Stops Pop-Ups & Tickers
e. Categorization & Managing various File Types
f. Stops Internet Messaging (Yahoo, MSN, AOL etc)
g. Content Caching & Reporting

3. Traffic Discovery & Application Control
a. Identification of Traffic
b. Traffic Reporting & Analysis
c. Application Control on P2P, FTP, Mail etc
d. Control to based on Scheduling (Day & Time)
e. User Base Control Support

4. User Policy Management
a. Surfing Policy based on Total Days & Hours
b. Time Based Policy based on Week Days / Time / User / Group
c. Access Based Policy
d. Security Policy based on Sites, Domain & Services

5. Anti Virus & Anti Spam
a. Based on Gateway Level
b. Based on Concurrent Connection to Internet
c. Scanning on HTTP, FTP, SMTP, POP3 & Spam Control
d. Relevant, continues & real-time detection
e. Detailed reporting
f. Third Party solution can be integrated on same server

6. DNS, Proxy & Firewall
a. Inbuilt DNS Services
b. Inbuilt NAT Support
f. DHCP Support
h. Restriction based on IP & Ports
i. Intrusion Detection & Prevention ystem

7. Online Reports for Users & Links
a. Online Reports of Users Connected to Internet
b. Online Internet usage report on Time, Data Transfer & Bandwidth utilization
c. Based on User & IP
d. Online Bandwidth Monitoring & Graphs
e. Reporting for Multiple Gateway Links

8. MIS Reporting & Trend Analysis
a. Web Site Accessed by Individual User / Group basis
b. Total Upload & Download Date Report based on User / Group
c. Report on Total Number of Pages / Document Printed by User
d. Bandwidth Graphs based on Daily, Weekly, Monthly & Yearly Basis
e. Cache Efficiency & Bandwidth Gain Reports
f. Multiple Gateway Load balancing Graphs
g. Trend Analysis Report on User to Internet Usage
i. Top 10 Sites Visited
ii. Top 10 Sites Data Transfer
iii.Top Content Type
iv.Average Hit per Hour for Duration
v. Top 10 Users
vi.Category-wise Reports & Analysis on User/Group

9. Load Balancing & Gateway Fail-over
a. Multiple Link Support
b. Auto Balancing of Traffic on Multiple Links
c. Auto Fail-over from Failed Link to Live Link
d. Maintain continues Traffic Flow
e. Prevent Loss of Information
f. Reports & Graphs

10. Administrative Tools
a. Access Control based on Source, Destination IP & Port
b. GUI Based Interface for Management
c. Console for Configuration
d. Administrative, Manager & Operative Level Security
e. Web Based Remote Access Facility
f. System Diagnosis - Cache, CPU, Memory, LAN, etc Utilization
g. View Network Connectivity & Services - DNS, Ping, Gateway, etc

h. Single Sign-on Integration with Windows Authentication
j. User Data & Policies - Export & Import Facility
k. Message Broadcasting to User / Group

11. Database Storage, Back up & Restoration
a. Based on Scheduling
b. Date Selection & Download of Database
c. Auto Purge of Logs
d. Database Service Check & Repair
e. Restoration & configuration

12. Printer Control and Management
a. User wise restriction on number of pages to be printed per cycle
b. Example: User 'john' can print at the most 20 pages per week
c. Daily, weekly, monthly, yearly Printing Policy
d. User wise reporting of pages printed
e. Reporting includes Document name, username, and number of pages printed

1.3 Introduction to SmartGuard Broad Band Manager

SmartGuard Broad band is a complete software solution for Broad Band Internet Management. SmartGuard provide, manage and control internet bandwidth, access, email, firewall and many more broadband services on your Broadband Network. The Software has a unique capability of converting a flat fee based broadband connection / DSL connection/ Cable Connection / Vsat link /Fiber etc. into differentiated packaged internet connections for:

- **ISP 's**
- **Cable Operators**
- **Cyber Café**
- **Hotels**
- **Institutes / Colleges**
- **Corporate**
- **Call Centers**

smartguard

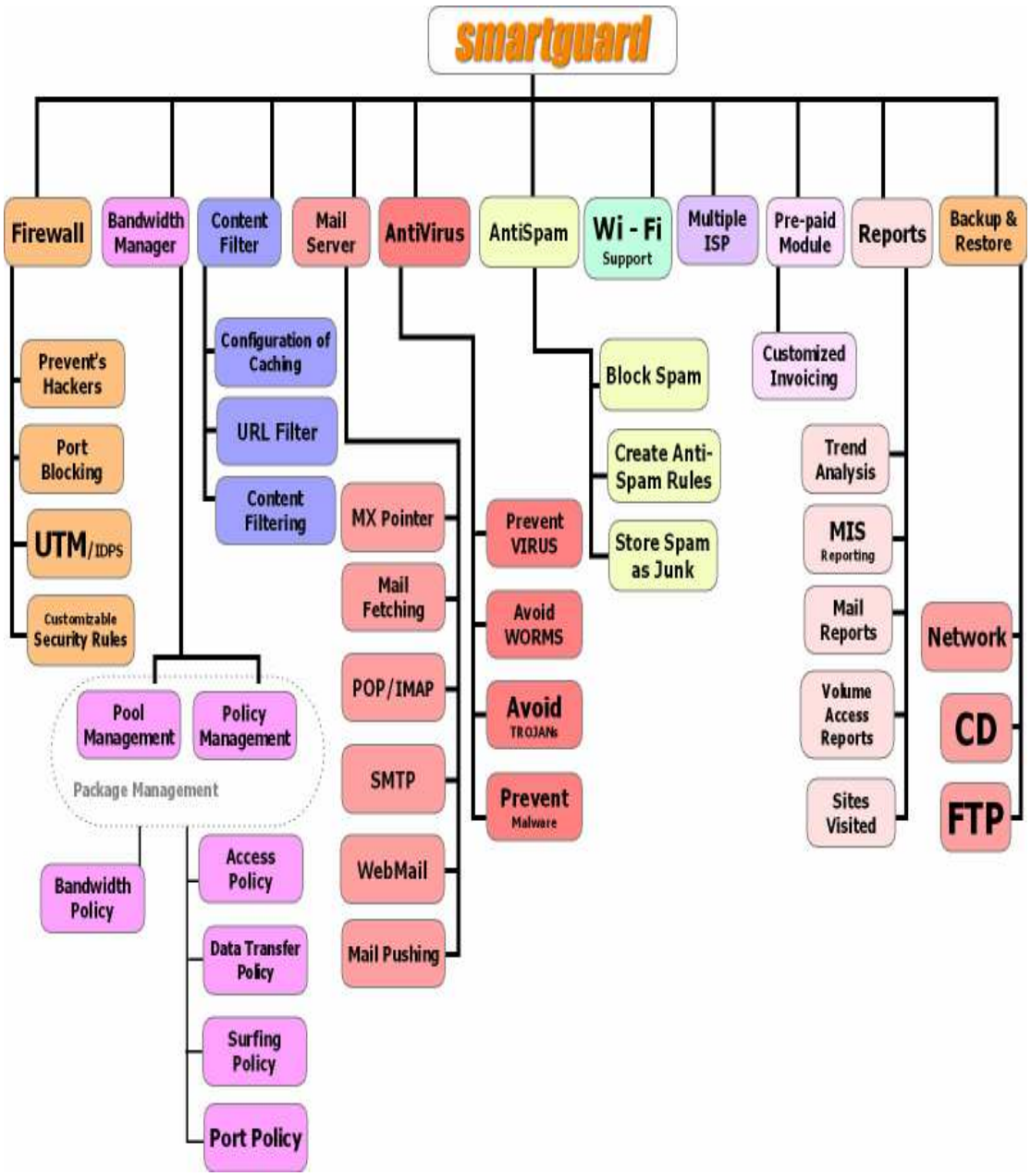
1.4 SmartGuard in Network

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

smartguard

SmartGuard At a Glance



XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

smartguard

Chapter 2

GETTING STARTED

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

2. GETTING STARTED

2.1 INSTALLATION

2.1.1 Minimum System Requirement

- 512 MB/1GB (DDR 333/DDR 400 memory)
- Pentium IV(with 533/800 MHz system bus) or Faster CPU
- Serial ATA HDD 40 GB or Above (Recommended 7200 RPM)
- Two 10/100 Mbits/sec Ethernet Network Interface Card.
- Two Static IP address (Optional)
- One CD –ROM drive.
- Domain name for email server.

2.1.2 Installation Instruction

Insert the CD in the CD-Rom drive and Boot the system from the CD-Rom drive. [To boot from CD set the CD-Rom drive as First Boot Device in the BIOS] & Remove cables in Ethernet card.

Warning: -☞ All Your previous data will be lost when you Install SmartGuard.

After Inserting CD, Reboot your system. Quick Installation completes in 10 minutes.

Note: -☞ When Installation process is going on do not press any key from keyboard.

After successful installation the CD is ejected automatically.

Note: -☞ Now Remove the SmartGuard CD.

The system will reboot automatically.

When system restarts it will wait for the service ZZZ_httpd to start in the background for the first time as its installation process is going on. It takes **10-15 minutes**. This file execution time depends on your processor. Wait for completely execution of ZZZ_httpd file.

Note: - ☞ Do not interrupt the process or use keyboard at that time.

When Installation completes it shows you the login screen
SmartGuard
Broadband Manager
Login:
Reboot your system again by pressing ctrl+alt+delete keys simultaneously.

When Reboot process is complete its shows you login screen again

SmartGuard
Broadband Manager
Login:

Here you type login name and press enter then type password and press enter

Login: root
Password: com123

```
login as: root
root@192.168.10.9's password:
```

Note:-Password will not be displayed. [In fact no characters will be displayed.]

```
                    TOOLS
-----------------------------------------------

          1.        WAN IP [ISP1] Configuration
          2.        LAN IP Configuration
          3.        WANIP [ISP 2] Configuration
          4.        DEFAULT GATEWAY
          5.        D.N.S [Domain Name Server]
          6.        Backup All
          7.        Database Backup
          8.        Restore Database
          9.        MRTG Generate
          10.       Repair Database
          11.       Cache Server Stop
          12.       Cache Server Start
          13.       Cache Server Restart
          14.       User Watch
          15.       Bandwidth Watch
          16.       DISK SPACE
          17.       Route Table
          18.       Open WebSite [Check Internet]
          19.       Ping
          20.       Network Restart
          21.       HTTP Restart
          22.       Bandwidth Calculation stop
     23.      Shutdown
          24        Quit
                    PRESS [CTRL+ C ]KEY for QUIT
-----------------------------------------------
 Enter Option?
```

Type 1 for WAN IP configuration

Enter here your WAN IP [Example] 202.122.51.190

Enter Subnet	255.255.255.248
Enter Gateway	202.122.51.185

Type 2 for LANIP configuration

	[Example]
Enter LAN IP	10.0.0.1
Enter Subnet	255.255.255.0

Type 4 for Default Gateway

	[Example]
Enter Default Gateway	202.122.51.185

Type 5 for DNS Enter

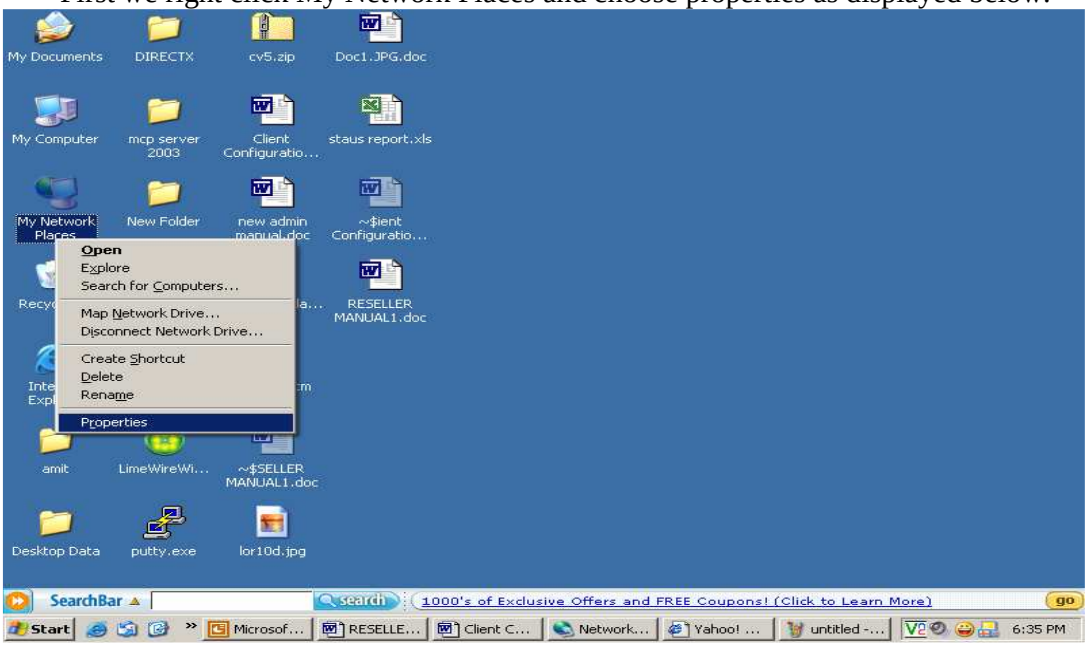
	[Example]
Enter Name Server 1	10.0.0.1
Enter Name Server 2	203.196.128.4
Enter Name Server 3	4.2.2.2

Now press Ctrl+c, and give the command ***service network restart*** *at root. And now the server is live on internet.*

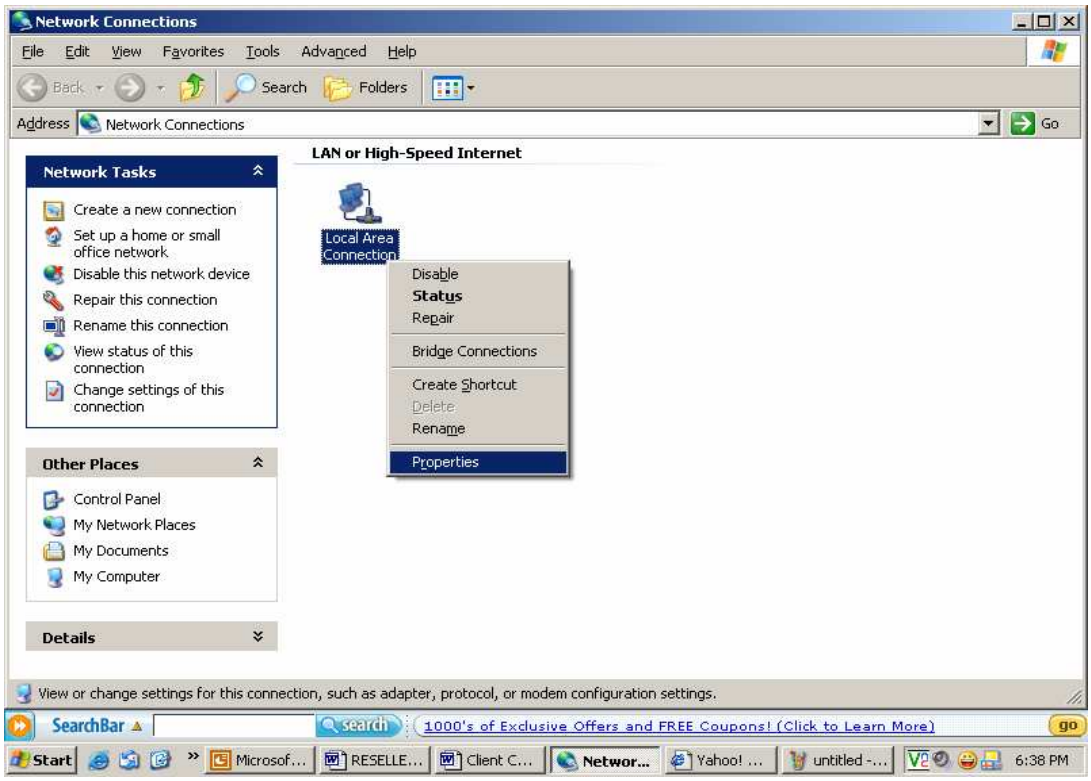
After installation there are some perquisites needed to be done on any system on LAN in order to access server's admin page.

So, here taking the example of Windows XP (LAN PC) we come to discuss about the network settings at that computer:-

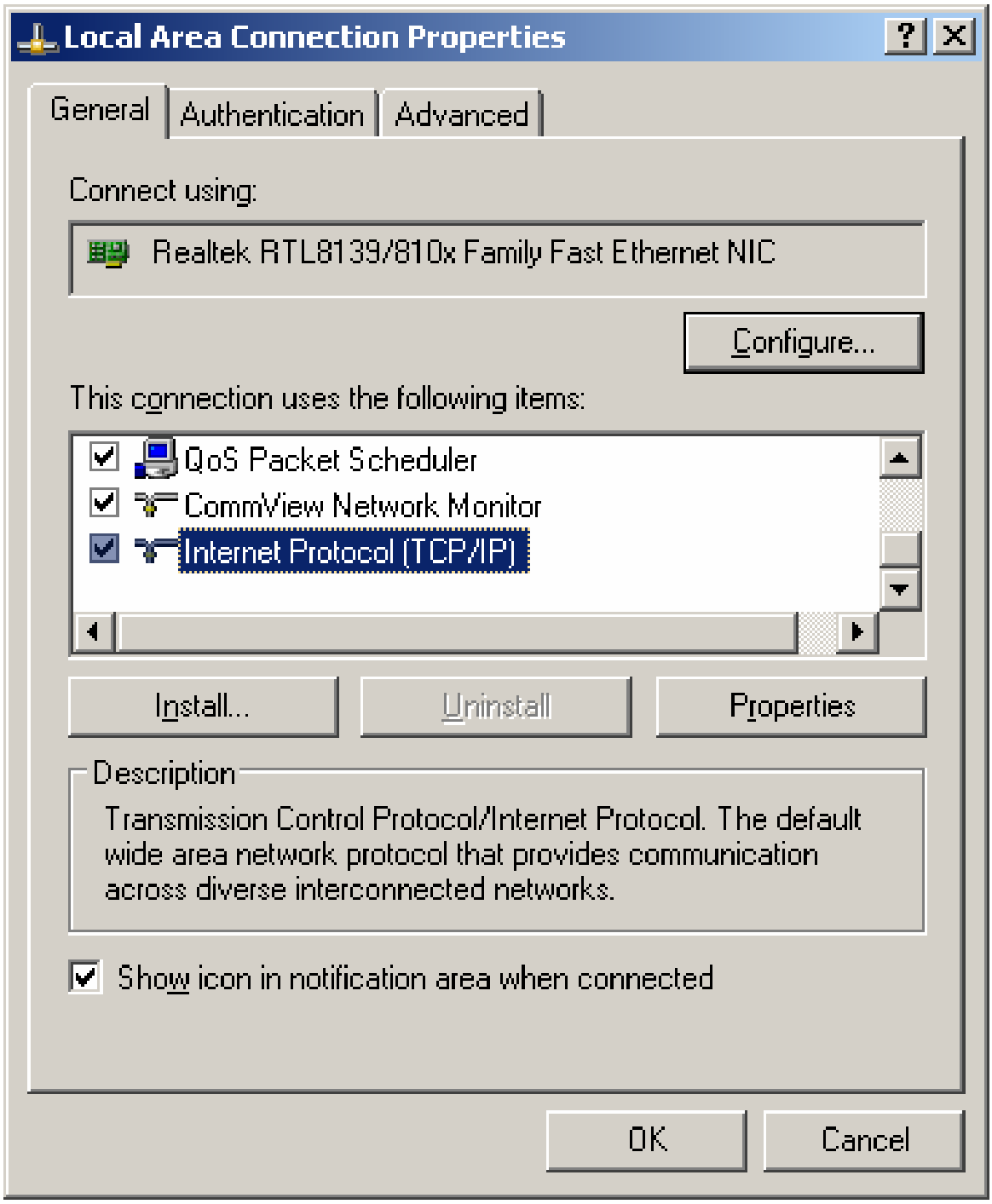
First we right click My Network Places and choose properties as displayed below:-



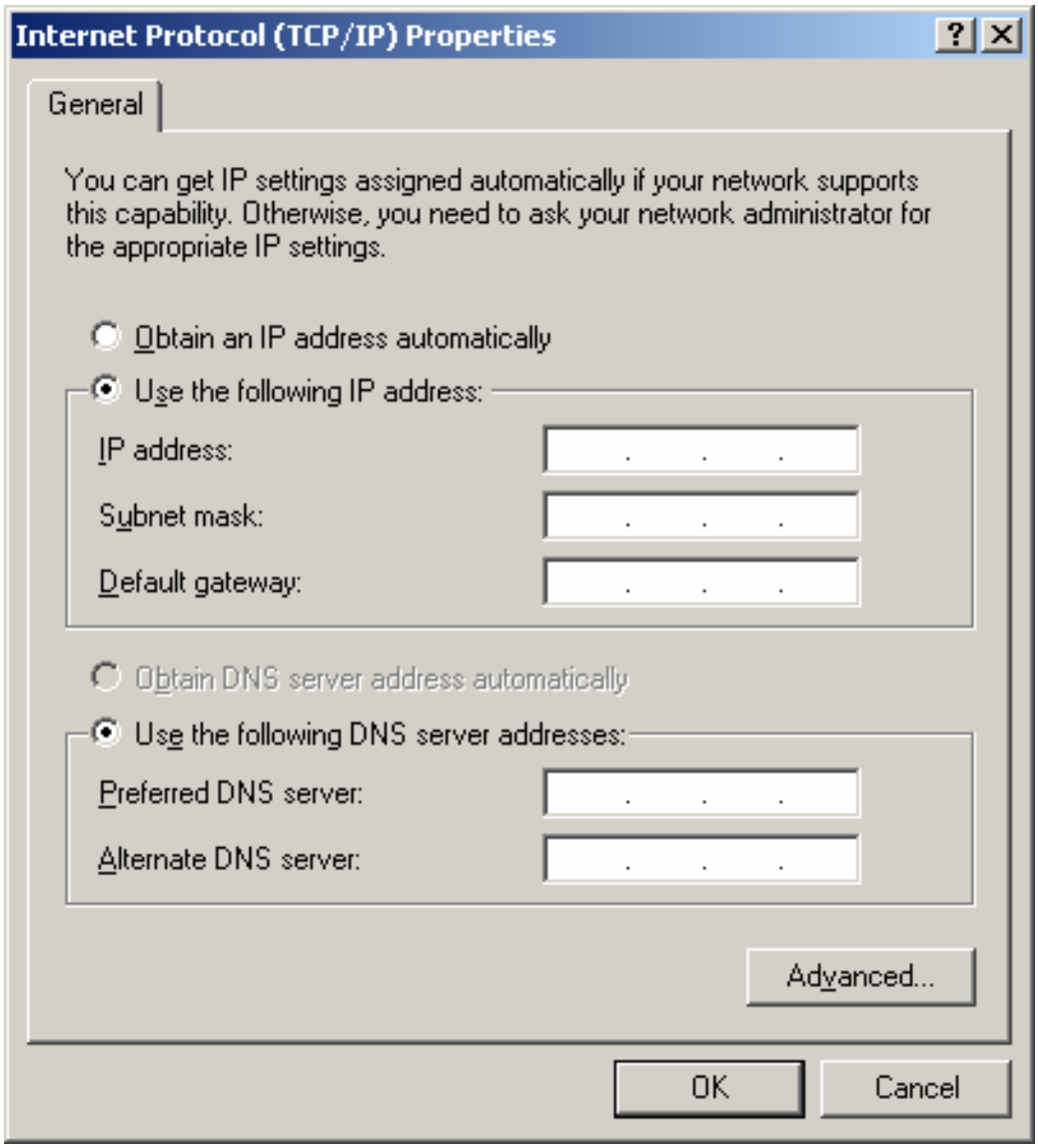
Now, when we click on properties following screen is displayed:-



Now, after clicking on properties we are directed to following page.


Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Realtek RTL8139/810x Family Fast Ethernet NIC
Configure...
This connection uses the following items:
QoS Packet Scheduler
CommView Network Monitor
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK
Cancel

Again click on properties, to come to this page as follows:



Here, we need to map the following network details (For Example):

IP Address:	192.168.0.2
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
DNS Server:	192.168.0.1

And at last click on OK.

Note: Here we are considering that 192.168.0.1 is the LAN IP mapped on server, so we will be using it as our Default Gateway & DNS on all our LAN machines and the IP for the LAN machines (users) will be of the same series **i.e. (192.168.0.1-192.168.0.254).**

smartguard

Chapter 3

WELCOME TO SMARTGUARD

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

3. WELCOME TO SMARTGUARD

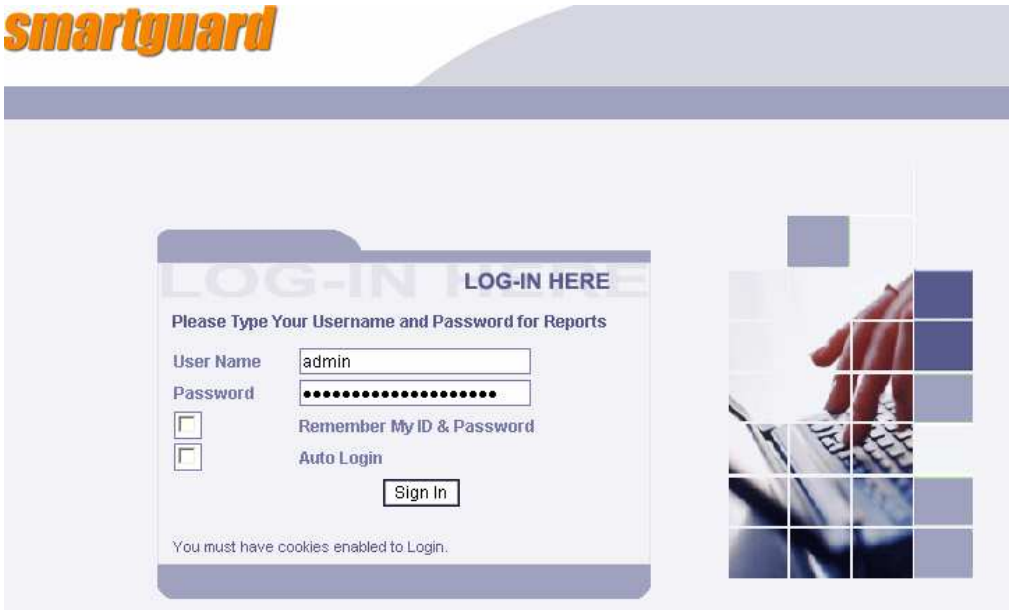
3.1 LOGIN PAGE

This is a server IP address

3.1.1 ADMIN CONTROL PANEL

Admin Login Window

Open Internet Explorer write in address bar Type http://10.0.0.1/admin.php
Its Shows Admin Login page. Type in **Login ID:** admin **Password:** smart123

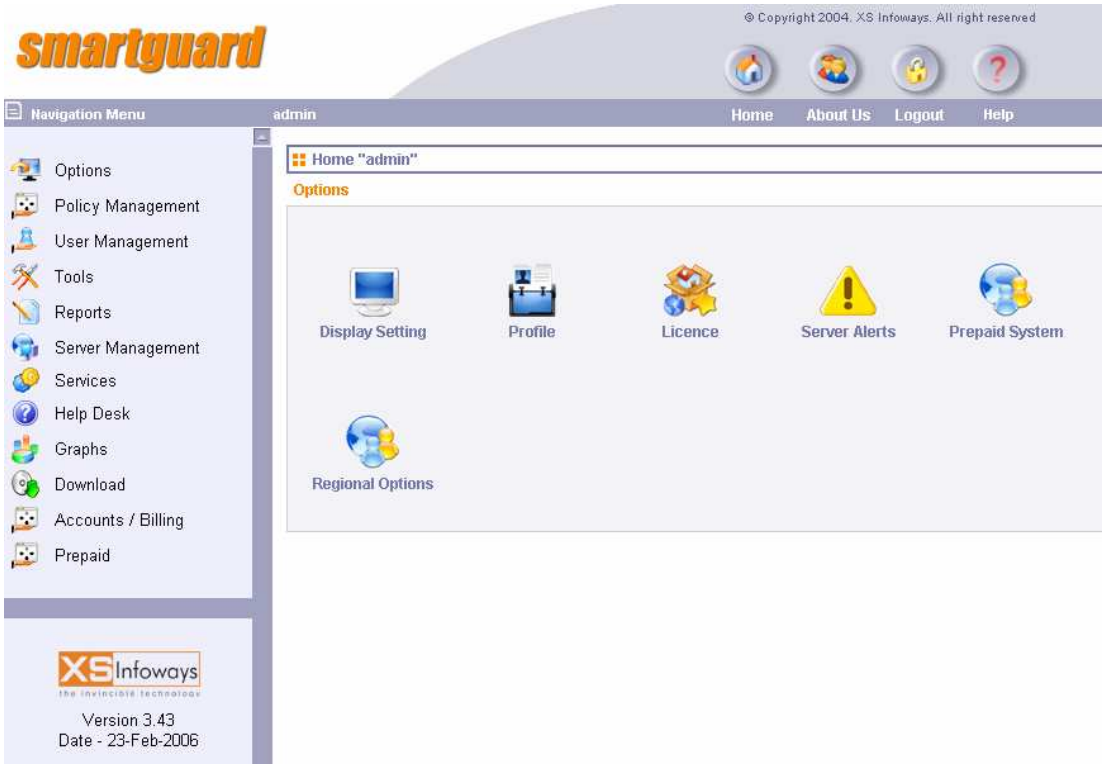


Main admin navigation menu

At the main admin page after successful login following menus are displayed

Main Menu

smartguard



XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

smartguard

Chapter 4

Firewall

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

4. Firewall

What Is NAT?

The Internet is expanding at an exponential rate. As the amount of information and resources increases, it is becoming a requirement for even the smallest businesses and homes to connect to the Internet. Network Address Translation (NAT) is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. This allows home users and small businesses to connect their network to the Internet cheaply and efficiently.

The impetus towards increasing use of NAT comes from a number of factors:

- A world shortage of IP addresses
- Security needs
- Ease and flexibility of network administration

SmartGuard has extensive experience in developing Network Address Translation software. InterGate is SmartGuard's primary NAT solution

IP Addresses

In an IP network, each computer is allocated a unique IP address. In the current version of IP protocol, IP version 4, an IP address is 4 bytes. The addresses are usually written as x1.x2.x3.x4, with x1, x2, x3 and x4 each describing one byte of the address. For example, address 16843009 (hex 1010101) is written as 1.1.1.1, since each byte of this address has a value of 1.

Since an address is 4 bytes, the total number of available addresses is 2 to the power of 32 = 4,294,967,296. This represents the TOTAL theoretical number of computers that can be directly connected to the Internet. In practice, the real limit is much smaller for several reasons.

Each physical network has to have a unique Network Number, comprising some of the bits of the IP address. The rest of the bits are used as a Host Number to uniquely identify each computer on that network. The number of unique Network Numbers that can be assigned in the Internet is therefore much smaller than 4 billion, and it is very unlikely that all of the possible Host Numbers in each Network Number are fully assigned.

An address is divided into two parts: a network number and a host number. The idea is that all computers on one physical network will have the same network number - a bit like the street name, the rest of the address defines an individual

computer - a bit like house numbers within a street. The size of the network and host parts depends on the class of the address, and is determined by address' network mask. The network mask is a binary mask with 1s in the network part of the address, and 0 in the host part.

To allow for a range from big networks, with a lot of computers, to small networks, with a few hosts, the IP address space is divided into 4 classes, called class A, B, C and D. The first byte of the address determines which class an address belongs to:

- Network addresses with first byte between 1 and 126 are class A, and can have about 17 million hosts each.
- Network addresses with first byte between 128 and 191 are class B, and can have about 65000 hosts each.
- Network addresses with first byte between 192 and 223 are class C, and can have 256 hosts.
- All other networks are class D, used for special functions or class E which is reserved.

Most class A and B addresses have already been allocated, leaving only class C available. This means that total number of available addresses on the Internet is 2,147,483,774. Each major world region has an authority which is given a share of the addresses and is responsible for allocating them to Internet Service Providers (ISPs) and other large customers. Because of routing requirements, a whole class C network (256 addresses) has to be assigned to a client at a time; the clients (e.g.. ISPs) are then responsible for distributing these addresses to their customers.

While the number of available addresses seems large, the Internet is growing at such a pace that it will soon be exhausted. While the next generation IP protocol, IP version 6, allows for larger addresses, it will take years before the existing network infrastructure migrates to the new protocol.

Because IP addresses are a scarce resource, most Internet Service Providers (ISPs) will only allocate one address to a single customer. In majority of cases this address is assigned dynamically, so every time a client connects to the ISP a different address will be provided. Big companies can buy more addresses, but for small businesses and home users the cost of doing so is prohibitive. Because such users are given only one IP address, they can have only one computer connected to the Internet at one time. With an NAT gateway running on this single computer, it is possible to share that single address between multiple local computers and connect them all at the same time. The outside world is unaware of this division and thinks that only one computer is connected.

Security Considerations

Many people view the Internet as a "one-way street"; they forget that while their computer is connected to the Internet, the Internet is also connected to their computer. That means that anybody with Net access can potentially access

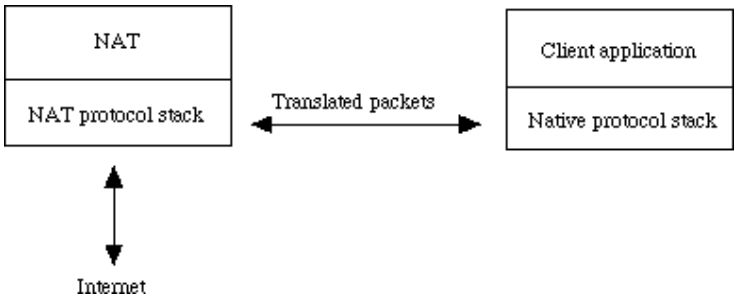
resources on their computers (such as files, email, company network etc). Most personal computer operating systems are not designed with security in mind, leaving them wide open to attacks from the Net. To make matters worse, many new software technologies such as Java or Active X have actually reduced security since it is now possible for a Java applet or Active X control to take control of a computer it is running on. Many times it is not even possible to detect that such applets are running; it is only necessary to go to a Web site and the browser will automatically load and run any applets specified on that page.

The security implications of this are very serious. For home users, this means that sensitive personal information, such as emails, correspondence or financial details (such as credit card or cheque numbers) can be stolen. For business users the consequences can be disastrous; should confidential company information such as product plans or marketing strategies be stolen, this can lead to major financial losses or even cause the company to fold.

To combat the security problem, a number of firewall products are available. They are placed between the user and the Internet and verify all traffic before allowing it to pass through. This means, for example, that no unauthorised user would be allowed to access the company's file or email server. The problem with firewall solutions is that they are expensive and difficult to set up and maintain, putting them out of reach for home and small business users.

NAT automatically provides firewall-style protection without any special set-up. That is because it only allows connections that are originated on the inside network. This means, for example, that an internal client can connect to an outside FTP server, but an outside client will not be able to connect to an internal FTP server because it would have to originate the connection, and NAT will not allow that. It is still possible to make some internal servers available to the outside world via inbound mapping, which maps certain well know TCP ports (e.g.. 21 for FTP) to specific internal addresses, thus making services such as FTP or Web available in a controlled way.

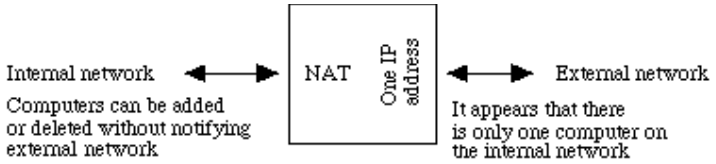
Many TCP/IP stacks are susceptible to low-level protocol attacks such as the recently-publicised "SYN flood" or "Ping of Death". These attacks do not compromise the security of the computer, but can cause the servers to crash, resulting in potentially damaging "denials of service". Such attacks can cause abnormal network events that can be used as a precursor or cloak for further security breaches. NATs that do not use the host machine protocol stack but supply their own can provide protection from such attacks:



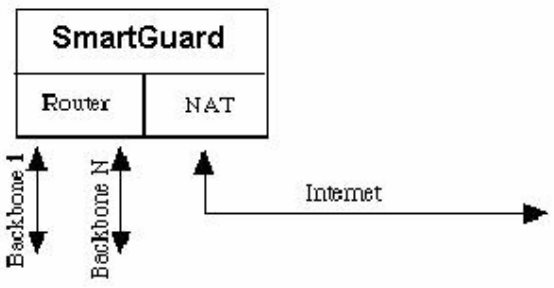
IP networks are more difficult to set up than local desktop LANs; each computer requires an IP address, a subnet mask, DNS address, domain name, and a default router. This information has to be entered on every computer on the network; if only one piece of information is wrong, the network connection will not function and there is usually no indication of what is wrong. In bigger networks the task of co-ordinating the distribution of addresses and dividing the network into subnets is so complicated that it requires a dedicated network administrator.

NAT can help network administration in several ways:

- It can divide a large network into several smaller ones. The smaller parts expose only one IP address to the outside, which means that computers can be added or removed, or their addresses changed, without impacting external networks. With inbound mapping, it is even possible to move services (such as Web servers) to a different computer without having to do any changes on external clients.



- Some modern NAT gateways contain a dynamic host configuration protocol (DHCP) server. DHCP allows client computers to be configured automatically; when a computer is switched on, it searches for a DHCP server and obtains TCP/IP setup information. Changes to network configuration are done centrally at the server and affect all the clients; the administrator does not need to apply the change to every computer in the network. For example, if the DNS server address changes, all clients will automatically start using the new address the next time they contact the DHCP server.
- Many NAT gateways provide for a way to restrict access to the Internet. For example, Smart Guard has built-in CyberPatrol filtering, which allows administrators to prohibit access to dubious material.
- Another useful feature is traffic logging; since all the traffic to and from the Internet has to pass through a NAT gateway, it can record all the traffic to a log file. This file can be used to generate various traffic reports, such as traffic breakdown by user, by site, by network connection etc.
- Since NAT gateways operate on IP packet-level, most of them have built-in internetwork routing capability. The internetwork they are serving can be divided into several separate sub networks (either using different backbones or sharing the same backbone) which further simplifies network administration and allows more computers to be connected to the network:



To summarise, a NAT gateway can provide the following benefits:

- Firewall protection for the internal network; only servers specifically designated with "inbound mapping" will be accessible from the Internet
- Protocol-level protection
- Automatic client computer configuration control
- Packet level filtering and routing

NAT and Proxies

A proxy is any device that acts on behalf of another. The term is most often used to denote Web proxying. A Web proxy acts as a "half-way" Web server: network clients make requests to the proxy, which then makes requests on their behalf to the appropriate Web server. Proxy technology is often seen as an alternative way to provide shared access to a single Internet connection. The main benefits of Web proxying are:

- Local caching: a proxy can store frequently-accessed pages on its local hard disk; when these pages are requested, it can serve them from its local files instead of having to download the data from a remote Web server. Proxies that perform caching are often called caching proxy servers.
- Network bandwidth conservation: if more than one client requests the same page, the proxy can make one request only to a remote server and distribute the received data to all waiting clients.

Both these benefits only become apparent in situations where multiple clients are very likely to access the same sites and so share the same data.

Unlike NAT, Web proxying is not a transparent operation: it must be explicitly supported by its clients. Due to early adoption of Web proxying, most browsers, including Internet Explorer and Netscape Communicator, have built-in support for proxies, but this must normally be configured on each client machine, and may be changed by the naive or malicious user.

Web proxying has the following disadvantages:

- Web content is becoming more and more dynamic, with new developments such as streaming video & audio being widely used. Most of

the new data formats are not cacheable, eliminating one of the main benefits of proxying.

- Clients have to be explicitly set to use Web proxying; whenever there is a change (e.g. proxy is moved to a new IP address) each and every client has to be set up again.
- A proxy server operates above the TCP level and uses the machine's built-in protocol stack. For each Web request from a client, a TCP connection has to be established between the client and the proxy machine, and another connection between the proxy machine and the remote Web server. This puts lot of strain on the proxy server machine; in fact, since Web pages are becoming more and more complicated the proxy itself may become bottleneck on the network. This contrasts with a NAT which operates on packet level and requires much less processing for each connection.

NAT Operation

The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address.

The TCP/IP protocols include a multiplexing facility so that any computer can maintain multiple simultaneous connections with a remote computer. It is this multiplexing facility that is the key to single address NAT.

To multiplex several connections to a single destination, client computers label all packets with unique "port numbers". Each IP packet starts with a header containing the source and destination addresses and port numbers:

Source address	Source port	Destination address	Destination port

This combination of numbers completely defines a single TCP/IP connection. The addresses specify the two machines at each end, and the two port numbers ensure that each connection between this pair of machines can be uniquely identified.

Each separate connection is originated from a unique source port number in the client, and all reply packets from the remote server for this connection contain the same number as their destination port, so that the client can relate them back to its correct connection. In this way, for example, it is possible for a web browser to ask a web server for several images at once and to know how to put all the parts of all the responses back together.

A modern NAT gateway must change the Source address on every outgoing packet to be its single public address. It therefore also renumbers the Source Ports to be unique, so that it can keep track of each client connection. The NAT gateway uses a port mapping table to remember how it renumbered the ports for each client's outgoing packets. The port mapping table relates the client's real

local IP address and source port plus its translated source port number to a destination address and port. The NAT gateway can therefore reverse the process for returning packets and route them back to the correct clients.

When any remote server responds to an NAT client, incoming packets arriving at the NAT gateway will all have the same Destination address, but the destination Port number will be the unique Source Port number that was assigned by the NAT. The NAT gateway looks in its port mapping table to determine which "real" client address and port number a packet is destined for, and replaces these numbers before passing the packet on to the local client.

This process is completely dynamic. When a packet is received from an internal client, NAT looks for the matching source address and port in the port mapping table. If the entry is not found, a new one is created, and a new mapping port allocated to the client:

- Incoming packet received on non-NAT port
- Look for source address, port in the mapping table
- If found, replace source port with previously allocated mapping port
- If not found, allocate a new mapping port
- Replace source address with NAT address, source port with mapping port

Packets received on the NAT port undergo a reverse translation process:

- Incoming packet received on NAT port
- Look up destination port number in port mapping table
- If found, replace destination address and port with entries from the mapping table
- If not found, the packet is not for us and should be rejected

Each client has an idle time-out associated with it. Whenever new traffic is received for a client, its time-out is reset. When the time-out expires, the client is removed from the table. This ensures that the table is kept to a reasonable size. The length of the time-out varies, but taking into account traffic variations on the Internet should not go below 2-3 minutes. Most NAT implementations can also track TCP clients on a per-connection basis and remove them from the table as soon as the connection is closed. This is not possible for UDP traffic since it is not connection based.

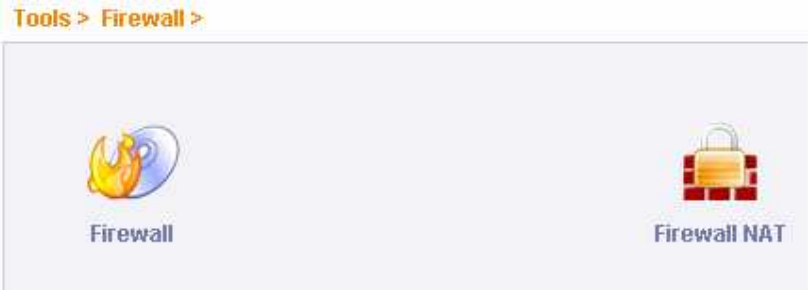
Many higher-level TCP/IP protocols embed client addressing information in the packets. For example, during an "active" FTP transfer the client informs the server of its IP address & port number, and then waits for the server to open a connection to that address. NAT has to monitor these packets and modify them on the fly to replace the client's IP address (which is on the internal network) with the NAT address. Since this changes the length of the packet, the TCP sequence/acknowledge numbers must be modified as well. Most protocols can be supported within the NAT; some protocols, however, may require that the clients themselves are made aware of the NAT and that they participate in the address translation process. [Or the NAT must be protocol-sensitive so that it can monitor or modify the embedded address or port data]

Because the port mapping table relates complete connection information - source and destination address and port numbers - it is possible to validate any or all of this information before passing incoming packets back to the client. This checking helps to provide effective firewall protection against Internet-launched attacks on the private LAN.

Each IP packet also contain checksums that are calculated by the originator. They are recalculated and compared by the recipient to see if the packet has been corrupted in transit. The checksums depend on the contents of the packet. Since the NAT must modify the packet addresses and port numbers, it must also recalculate and replace the checksums. Careful design in the NAT software can ensure that this extra processing has a minimal effect on the gateway's throughput. Before doing so it must check for, and discard, any corrupt packets to avoid converting a bad packet into a good one.

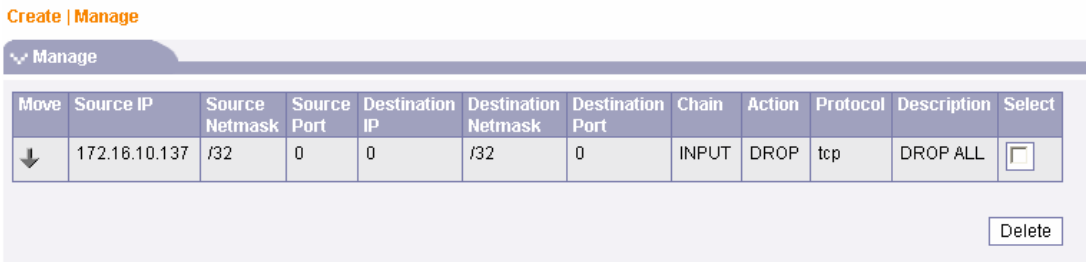
4.1 FIREWALL

STEP **Click on Tools option in left side of main menu → click on Firewall icon.**



4.1.1 FIREWALL

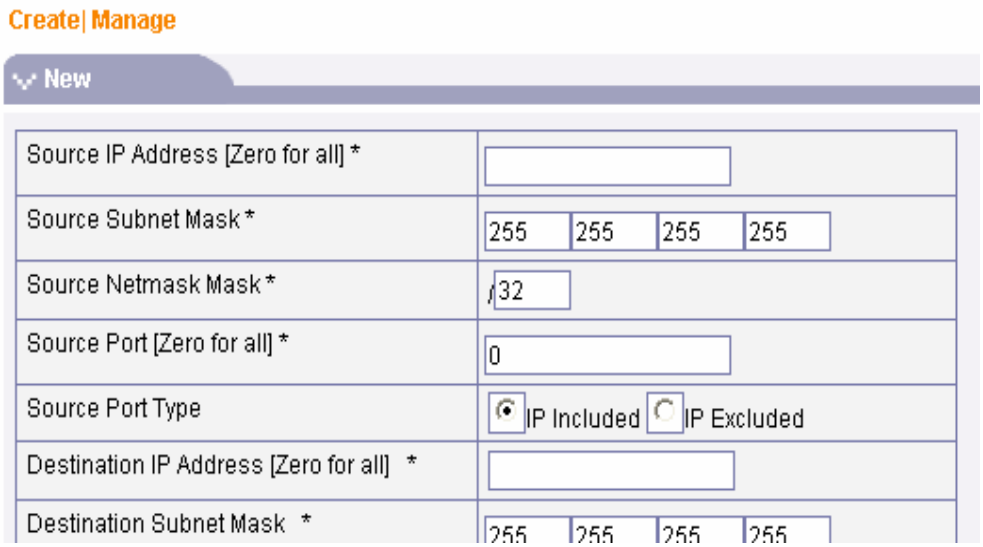
STEP **Click on Tools option in left side of main menu → click on Firewall icon → then click on firewall icon.**



Create

STEP **Click on Tools option in left side of main menu → click on Firewall icon → click on firewall icon → then click on create option.**

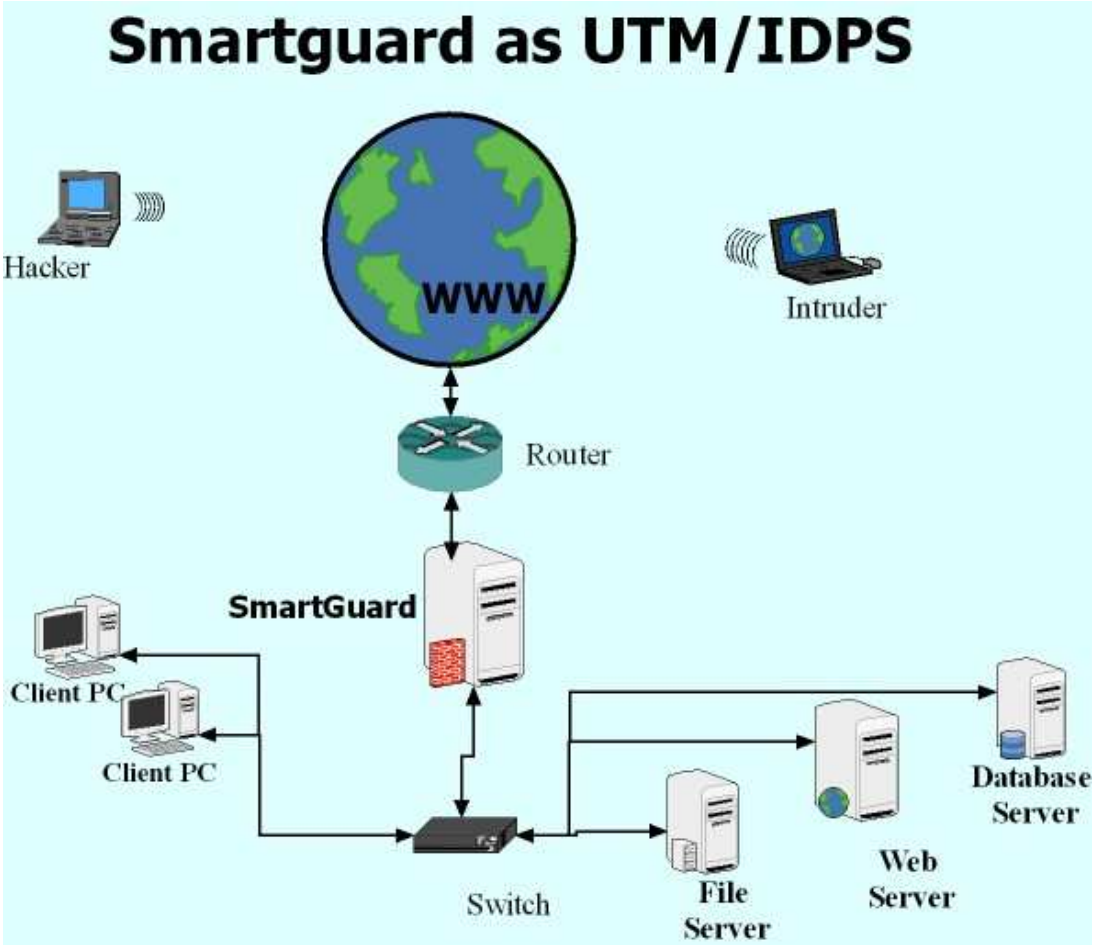
After click on create option following options will be displayed.



Destination Netmask *	/32
Destination Port [Zero for all] *	0
Destination Port Type	(•) IP Included ( ) IP Excluded
Select Chain	( ) Input ( ) Output (•) Forward
Select Action	( ) Accept ( ) Reject (•) Drop
Select Protocol	(•) tcp ( ) udp ( ) icmp ( ) all
Description	

Create

smartguard

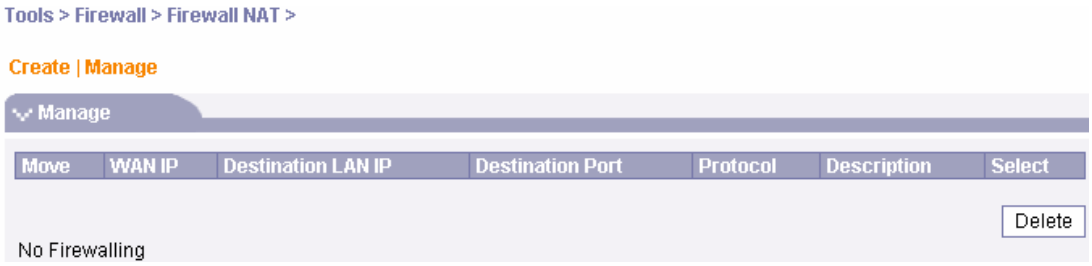


XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

4.2 FIREWALL NAT

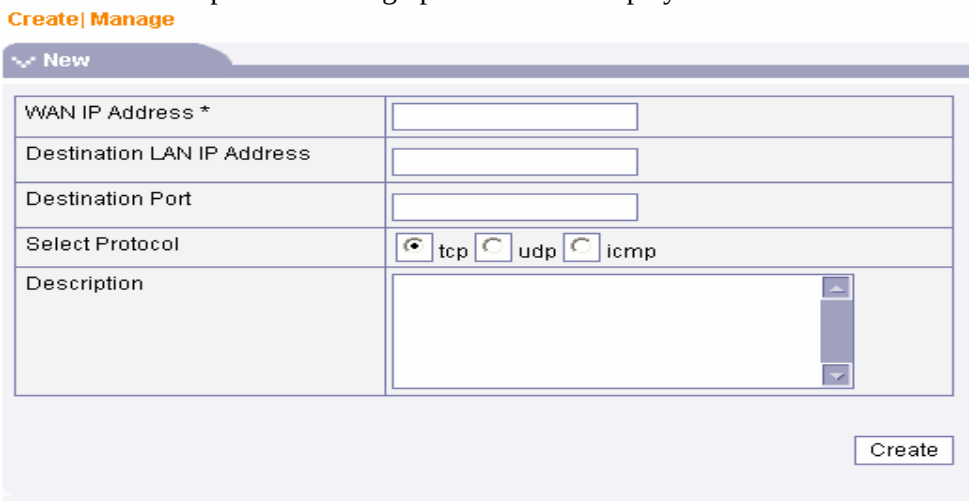
STEP **Click on Tools option in left side of main menu → click on Firewall icon → then click on firewall NAT icon.**



Create

STEP **Click on Tools option in left side of main menu → click on Firewall icon → click on firewall NAT icon → then click on create option.**

After click on create option following options will be displayed.



smartguard

Chapter 5

Content Filter

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

5. Content Filter

5.1 CACHE SERVER

Why we need Internet caching ?

As the usage of Internet resources grows, available bandwidth for organizations and service providers on the Internet becomes increasingly valuable. In some countries, the cost of increasing bandwidth to the Internet is extremely high.

Therefore, solutions for caching Web information, such as Cache (Proxy) servers, are becoming more and more popular. Typically, such solutions cache Web data when it's first accessed by an end user, and reuses it when another user requests the same information.

This saves time for the end user and bandwidth for the organization. Caching solutions are based on the assumption that large groups of end users share common interests, and therefore the same information will often be accessed more than once.

In addition, cache servers will invariably update cached information should there be changes to the original Web site.

Obviously, caching information from dynamic sites (for example, those whose content is created on-the-fly from a database) is pointless. Problems Surrounding the Use of Cache (Proxy) Servers When employing cache servers, there are some issues to consider. The main ones involve the use of single and multiple cache servers.

Single Cache Server

End-User Configuration

In order to use a cache server, end users must have such a server configured to their browser applications. For systems managers of large corporations or ISPs, this involves tremendous management overhead and is a continuous procedure. Some users, such as business travelers, need to have Internet access from varying locations, and therefore need to change their proxy configuration at each location, or access the Internet directly. Should the systems manager wish to change the cache server address, for whatever reason, all the end users will have to be reconfigured.

Single Point of Failure

Using a single cache server creates a single point of failure; if the server is down, all users configured to it cannot access the Internet. We are all familiar with this problem of proxy failure.

Cache, or proxy, server failure means that the Internet cannot be accessed directly. This is because once a user is configured to a cache server, the HTTP requests are different. The destination address of the request is the cache server, and the target Web site address is described only inside the request. Therefore if the cache server is down, there is no reply from the destination address of the request, and Internet access is rendered impossible.

Control Over Consumed Bandwidth Since the use of cache servers depends on the user browser configuration, a situation may arise where some users are not configured to the cache server, or a user turns off the cache server. In such cases, users will access the Internet directly, and the systems manager will have no control over the bandwidth consumption. Scalability Once an organization requires an additional cache server, scalability becomes a problem.

Adding another cache server significantly increases the organization's overhead, and the network or systems manager will have to reconfigure half of the end users of that organization.

Multiple Cache Servers

Using more than one cache server creates additional problems that need to be dealt with in order to optimize the use of Internet caching. When more than one cache server is available, end users are divided into groups according to the number of cache servers, with each group of users being configured to one of the cache servers.

Inefficient Caching and Bandwidth Usage Since each user is configured to a single cache server, there is no relation between the caching operations on each server. If we consider the assumption that groups of users, with common interest areas, often access the same Web information, then such use of multiple cache servers will result in the caching of some Web pages more than once on a number of different cache servers.

This situation results in inefficient use of caching disk space. Time is wasted for the end user who waits for the same data to be recached, and on top of that, unnecessary bandwidth is wasted. This creates an absurd situation where the more cache servers you add, the more bandwidth is wasted.

Lack of Fault Tolerance

Once end users are configured to a specific cache server they do not benefit from the other cache servers on the site. For example, redundancy and fault tolerance are absent between the cache servers despite the investment of more than one cache server. Thus, if one cache server fails the result is the same as having a single cache server, meaning that users can't access the Internet while the server is down.

What is a SmartGuard Cache Server?

A SmartGuard Cache Server is a generic name used to describe a network device that intercepts HTTP requests from end users, redirecting them to one or more cache servers. Such a device should be transparent both to the end users accessing the Internet and to the caching technology deployed on the network. How to Resolve Cache (Proxy) Server Problems with a SmartGuard Cache Server Single cache Server

End-User Configuration

A device such as a SmartGuard Cache Server should eliminate all the configuration procedures in the end user's browser. It should transparently intercept all users requests to the Internet and direct them to one or more cache servers. The redirected request should appear as if it came from a well-configured client, meaning it should include all the information required for the cache server to do the caching. For example, the redirected request should include the full URL of the requested page, and not just the relative path of the specific page.

Single Point of Failure

One of the main reasons for employing a SmartGuard Cache Server is to avoid situations where access to the Internet is impossible as a result of cache server problems. Hence, such a device should automatically detect a cache server failure, and, in such a case, redirect all requests directly to the Internet until the cache server is back in service. This way, the SmartGuard Cache Server ensures smooth, efficient and uninterrupted Internet access.

Control Over Consumed Bandwidth Using a SmartGuard Cache Server allows the systems manager to define which users will access the Internet directly and which will use caching facilities. This means that the inconvenience of configuring individual users can be avoided, and users can't change the definition themselves. This allows for better control over the organization's bandwidth consumption.

Scalability

Scaling is easy once a SmartGuard Cache Server is deployed, as there is no configuration on the end user's browser. Therefore, any changes are transparent to the end user, and they need to be configured only on the SmartGuard Cache Server itself. As a result, adding cache servers to an existing server or cache server farm, becomes a very easy process.

Multiple Cache Servers

Efficient Caching and Bandwidth Usage A SmartGuard Cache Server ideally eliminates any caching inefficiencies when more than one cache server is deployed. The way to achieve such efficiency is through the following operations:

1. Directing requests for previously cached pages to the cache server holding the cached data.

2. Directing new requests to the least loaded cache server.

3. Ensuring, over time, that cached pages are spread evenly across the cache servers for efficient load sharing; meaning, taking into account the popularity of specific cached pages. By doing the above, a SmartGuard Cache Server ensures that there is no duplication of Web material during caching, and that the load is evenly distributed between the cache servers. This ensures maximum performance.

Full Fault Tolerance To ensure uninterrupted access to the Internet and maximum cache usage, the SmartGuard Cache Server should be able to detect any type of cache server failure, such as H/W or S/W, and direct cache requests to another cache server when a server is out of service. In cases where all the cache servers are out of service, the SmartGuard Cache Server should redirect the request directly to the Internet. When one of the cache servers is recovering, the SmartGuard Cache Server should be able to recover from an unbalanced situation and initiate a transfer of part of the cached data to the recovered cache server.

Other Beneficial Features

Grouping End-Users

Large corporations and ISPs often need to group end users, such as finance-oriented users that need access to updated data. In cases where you want to give some users direct access to the Internet without going via the cache server, the SmartGuard Cache Server should be able to differentiate such users from others and direct them to the cache server only if they specifically require it; for example, through browser configuration.

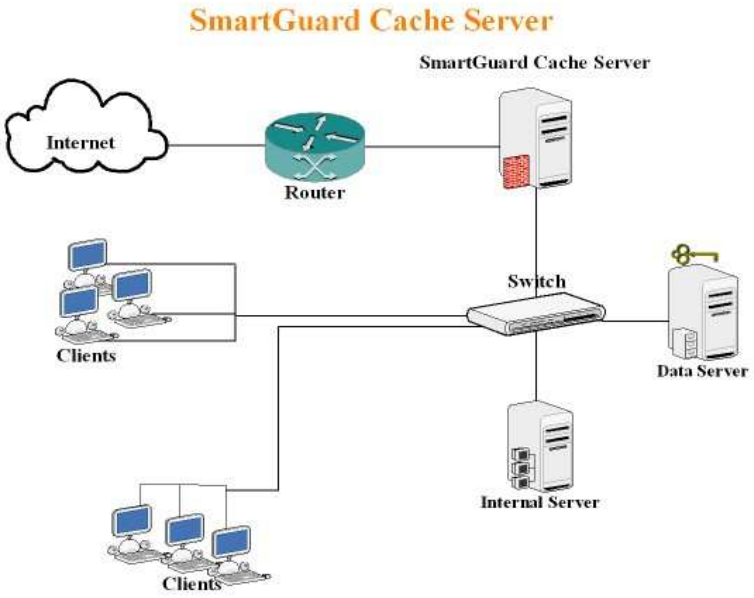
SmartGuard Cache Server Redundancy

One of the reasons for using a SmartGuard Cache Server device is to avoid a single point of failure on the cache server. Moving the single point of failure to the SmartGuard Cache Server is therefore undesirable. In order to ensure complete, uninterrupted and efficient Internet access, one can implement a redundant configuration of SmartGuard Cache Server s. Such a device needs to be capable of having a redundant unit that takes over automatically once the other units fails to operate. This means, it has to recognize not only a box failure but also a problem in the network links that are disrupting operation. Flexibility in Cache Servers Topology For most organizations, it is very important to maintain full flexibility when deciding where to integrate cache servers. Therefore, limitations such as having all the cache servers residing on the same segment should not be imposed by the cache directing device. The SmartGuard Cache Server should be able to execute the same operations even if the servers are spread across the network and sit behind routers.

Possible Configurations

smartguard

A SmartGuard Cache Server adjacent to the Internet access point.



SmartGuard Cache Server and Internet Cache Protocol

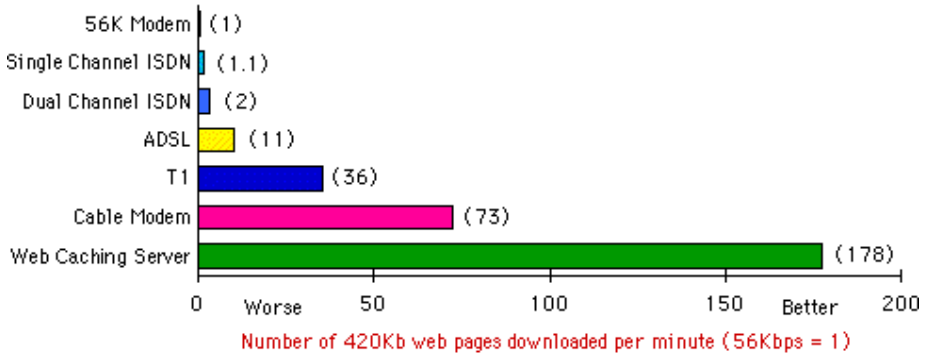
One of the attempts to solve caching inefficiency problems concerning multiple cache server configurations (described above) has been accomplished through Internet Cache Protocol (ICP). Internet Cache Protocol defines hierarchical caches. It provides a means for cache servers to communicate with each other to prevent caching inefficiencies.

There are two types of hierarchical caches: sibling and parent-child. In a sibling design, a cache that doesn't have a requested page requests the data from all other caches in the group. In a parent-child design, the cache hierarchy is vertical: The child cache only asks its parent for a page. Both designs use ICP version 2, specified in RFCs 2186 and 2187.

There are significant drawbacks to using ICP. First, it is not supported by all cache servers, therefore there might be a backward compatibility problem when adding a new cache server that needs to operate with an existing one. In addition, multiple cache servers that operate together through ICP are far less efficient than cache servers that are managed by a cache directing device. This is because for each request, the cache servers need to communicate with each other to ascertain that the requested data has been previously cached, or not. On the other hand, a cache directing device knows if and where the requested data is cached, and immediately directs the request to the correct server.

Another limitation of ICP operation is that it does not offer a solution for load sharing and balancing between cache servers, and therefore does not ensure maximal cache server performance.

The purpose of LAN based caching is to improve network efficiency by reducing the amount of traffic between the LAN and the Internet. The most obvious, and most frequently cited benefit is the shorter time required for the caching server to deliver cached content. Delivery time and therefore the end user experience are enhanced dramatically. For example, delivery of a 100KB web page from the originating server to the end user would take about 17 seconds over a 56Kbps modem, or 7.8 seconds over a dual channel Multilink PPP ISDN connection, assuming that there was no additional traffic congestion at the ISP or on the Internet backbone (this is not necessarily the case). The same page would take one second to deliver over a T1 connection, again assuming perfect Internet traffic conditions. However, this same page would be delivered from the caching server to the end user in about one tenth of a second *regardless of Internet traffic conditions.* This is the first and most obvious benefit of caching.



Some will point out that this is only a benefit if the same content is viewed a second time by a different user. If this does not occur, it may be argued, caching would be of no benefit. However, repeat visits to the same Web sites are more frequent than one may think. A recent test[2] representing a small business setup with a LAN comprising about 30 computers revealed that up to 70% of content delivered during any one hour period came from the cache, and as little as 30% came from the Internet. An independent laboratory study[3] recently showed average response times reduced by 87% with the use of a caching server.

There are additional benefits as well. By delivering content from its own cache, the caching server reduces bandwidth use between the LAN and the Internet. This means that more bandwidth becomes available for users requesting fresh content directly from the Internet. These users experience improved response times even if they request content that is not stored in the cache.

Ironically, there are cases where a browser may display web content from the LAN based web cache faster than from its own disk cache. Because browsers are optimized for content delivered over the network, some may actually display a page delivered over the LAN more quickly than if the same page were read from their own computer's disk

smartguard

Summary

By employing a **SmartGuard**, organizations and ISPs can maximize the usage of their single cache servers or cache server farms, as well as minimize the management overhead when using cache servers.

Cache directing is an important step toward more efficient use of bandwidth, as well as a means to ensure smooth and uninterrupted Internet access.

Cache (pronounced kash) is a collection of data duplicating original values stored elsewhere , where the original data are expensive (usually in terms of Access Time/ Bandwidth Consumption) to fetch or compute relative to reading the cache. Once the data are stored in the cache, future use can be made by accessing the cached copy rather than refetching or recomputing the original data, so that the average access time is lower.

SMARTGUARD CACHING ENGINE caches web documents accessed providing plus points to an enterprise as :

* Reduced Bandwidth Consumption (cached page fetched locally)
* Speedy Downloads
* Reduced Requests to web hence less load on network.

In Smartguard Caching Engine Web documents retrieved may be stored (cached) for a time so that they can be conveniently accessed if further requests are made for them. The issue of whether the most up-to-date copy of the file is retrieved is handled by the caching program which initially makes a brief check and compares the date of the file at its original location with that of the copy in the cache. If the date of the cached file is the same as the original, then the cached copy is used.

Smartguard maintain a cache of retrieved documents and this cache is used for retrievals where possible. In addition, the user may configure particular request to point to a caching server or request should go directly to the web. The caching server would supply the files from its cache if they were current, or pass on the request to the originating server if they were not.

SmartGuard caches all sites visited by Subscribers locally in to the server's hard drive. Caching not only serve the pages faster but also saves expensive Bandwidth. Caching can be configured at the package level, so it is possible for the administrator to bypass caching server for some Subscribers. SmartGuard Cache Server Administrator can also

- Modify Cache Memory and Hard Drive Space

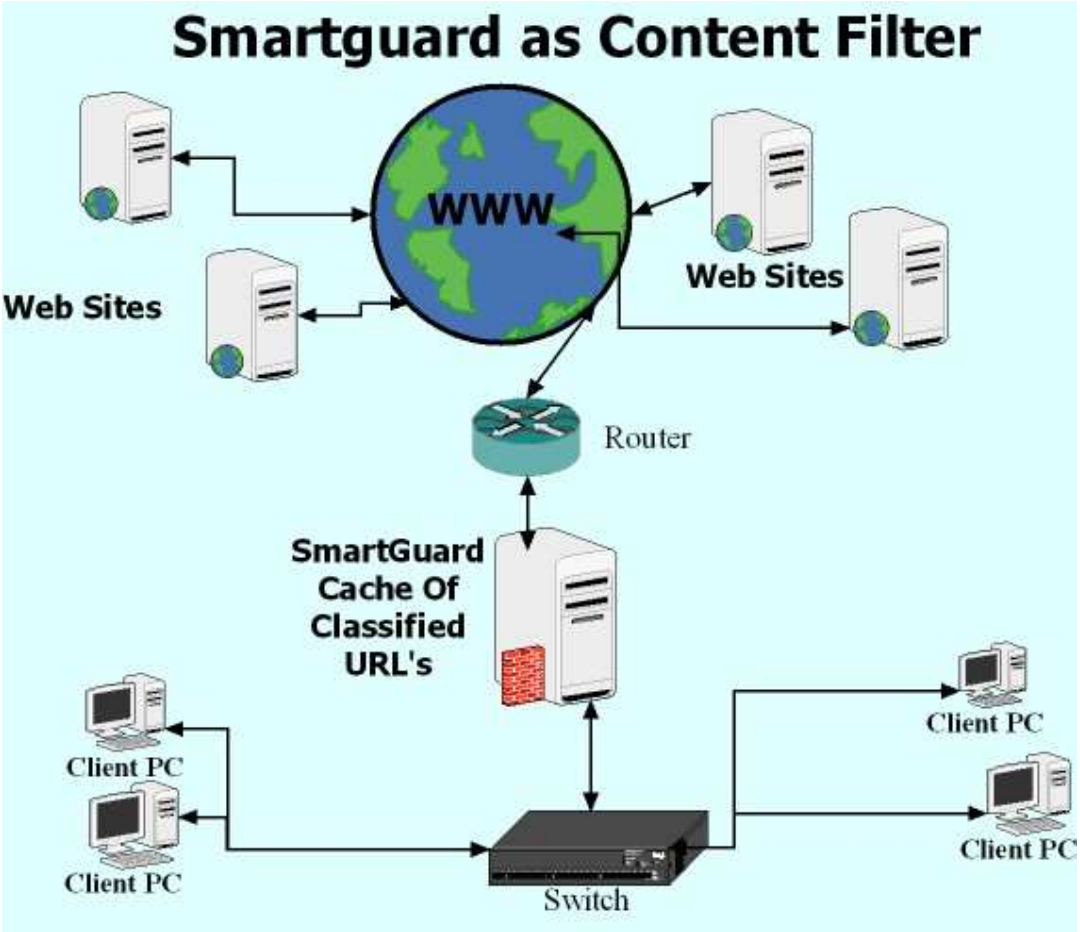
- Specify Keyword/URL not to cache

8.1.1 Configuration

RAM Size in MB* Available Size 51	50 Update RAM
Hard Disk Size* Avialable Size 2196	256 Update HardDisk
LAN IP*	192.168.70.1 - 192.168.70.254 Update LANIP
Public IP	203.122.51.186 - 203.122.51.189 UpdatePublicIP
Don't from Cache	www.hotmail.com Update
Cascading Require	Yes No
Parent Cache Server IP	172.16.1.1 Update
Flush Cache	Flush Cache

Administrator can update and edit Cache Ram, HDD Size, LAN IP series, Public IP series and all other configurations.

smartguard



What is Content Filtering ?

A facility to block or allow Internet sites and content from being accessed and viewed by an individual, a group of individuals, or all the connected users. The blocking, or "filtering," of undesirable Internet content. Smartguard can ensure Businesses to block content based on traffic type. For example, Web access might be allowed, but file transfers may not be allowed. Content can also be filtered by site through the use of lists of URLs that are cataloged by content (these catalogs are updated frequently).Administrators can control and restrict their clients access to inappropriate content via content filtering feature of Smartguard.

Content Filtering (Surfing/Browsing Protection)

Smartguard Web content filtering helps you increase productivity by filtering or blocking Web site privileges. The SmartGuard filtering is a customizable management tool with click interface that lets you control Web surfing and deny access to objectionable material. Filtering is transparent to users and requires no additional client software or configuration.

Smartguard's Content Filtering application can measure or block access to categories of web sites. Sophisticated URL classification methods ensure accuracy and completeness in identifying questionable web sites. Comprehensive reporting gives administrators the data to analyze web behavior in their organization.

Policy Creation - HOW ?

Smartguard's Content Filtering lets administrators define web access policies quickly and precisely. A point-and-click web interface makes it easy to define profiles of inappropriate web sites from among 11 categories. Administrators can tailor profiles for their organization by aggregating the categories into 11 customizable groups and by creating white lists and blacklists of web sites.

Database Recognition :

A database of categorized web sites currently includes more than 60 million entries. This is the largest database available for any commercial URL filtering system. If a user requests a web page that is not included in the database, the URL is sent to the web crawlers/spiders and classified within 24 hours.

Crystal-Clear Reports

Smartguard's Content Filtering provides detailed reporting of web traffic and denial incidents. Administrators can use these capabilities to understand user behavior, prioritize problems, and determine appropriate web use policies.

Content Filtering (Surf Protection)
Smartguard's Content Filtering application can measure or block access to 60 categories of web sites. Sophisticated URL classification methods ensure accuracy and completeness in identifying questionable web sites. Comprehensive reporting gives administrators the data to analyze web behavior in their organization.
Flexible Policy Creation
Smartguard's Content Filtering lets administrators define web access policies quickly and precisely. A point-and-click web interface makes it easy to define profiles of inappropriate web sites from among 60 categories. Administrators can tailor profiles for their organization by aggregating the categories into 18 customizable groups and by creating white lists and blacklists of web sites that should be accessible or blocked.

Comprehensive Coverage
A database of categorized web sites currently includes more than 60 million entries. This is the largest database available for any commercial URL filtering system.
To assign web pages to categories they are analyzed using sophisticated classification techniques such as:

Text Classification: Web pages are rated using factors such as the frequency of word occurrences and word combinations.

Optical Character Recognition: Text on images is captured and analyzed.

Visual Object Recognition: Symbols, logos, and trademarks are used to categorize web sites.

Porn Detection: Flesh tone images and face recognition are used to identify pictures with high concentrations of non-facial flesh.

The database classifies web pages in 13 languages.

If a user requests a web page that is not included in the database, the URL is sent to the web crawlers and classified within 24 hours.

Detailed Reporting

Smartguard's Content Filtering provides detailed reporting of web traffic and denial incidents. Administrators can use these capabilities to understand user behavior, prioritize problems, and determine appropriate web use policies.

Web-based e-mail, file downloads, IM, P2P, and unauthorized Web surfing can expose your enterprise network to serious, debilitating attacks and undesirable code, including spyware, adware, malware, and pornography. Smartguard URL Filter offers a proactive security solution that protects your enterprise against known, emerging, and customer-specific threats before they reach your network. And your IT staff will appreciate how easy it is to deploy and manage Smartguard Web protection. With fewer administrative headaches, they can focus on other important assignments and projects.

Smartguard allows you to actively monitor network use and abuse anywhere in your organization. You can even extend real-time protection to mobile users who connect to the corporate network . The same corporate security rules apply, so mobile devices are shielded from unwanted intrusions, minimizing unexpected shutdowns that lead to lapses in productivity.

Our readily accessible, centralized monitoring and reporting tools give IT staff and executives 360-degree visibility to enterprise Internet, e-mail and IM usage, making it easy to set and manage Internet policy, protect sensitive data, avoid liability issues, and comply with regulatory initiatives such as HIPAA or Sarbanes-Oxley.

Smartguard Suite is easy to deploy and maintain, saving IT costs and freeing up your resources for other critical tasks. And, you have the flexibility of choosing our software option, which offers a high degree of granular control, or our plug-and-play automatic network appliances. Available in a wide array of configurations for multiple networking platforms, Smartguard seamlessly integrates into your enterprise infrastructure.

Smartguard bolsters your defenses by providing:

- Bulletproof infrastructure security-Automatic, real-time security updates through our comprehensive threat database, which is constantly kept current with knowledge gathered by our global threat experts.
- Legal liability protection-Prevents circulation of inappropriate content that violates copyright laws or infringes on rights.
- Regulatory compliance-Helps you meet HIPAA, Sarbanes-Oxley, and other industry or government security requirements.
- Enhanced employee productivity-Limits Web surfing and downtime due to attacks and improves IT productivity because it's easy to implement and manage.

Smartguard Team is always busy in continuous monitoring of all Internet threats and analyze all Internet-borne threats, stemming from Web, e-mail, Instant Messaging and

Peer-to-Peer file-sharing and provides the most powerful protection against today's emerging threats. With extensive human review the accuracy of Smartguard protection is assured. Html stripped text, e-mail, and application components are analyzed for prioritization, and categorized using adaptive intelligence technologies that scan for embedded malicious codes, spyware, viruses, inappropriate image signatures, inappropriate text, worms, Trojans etc.

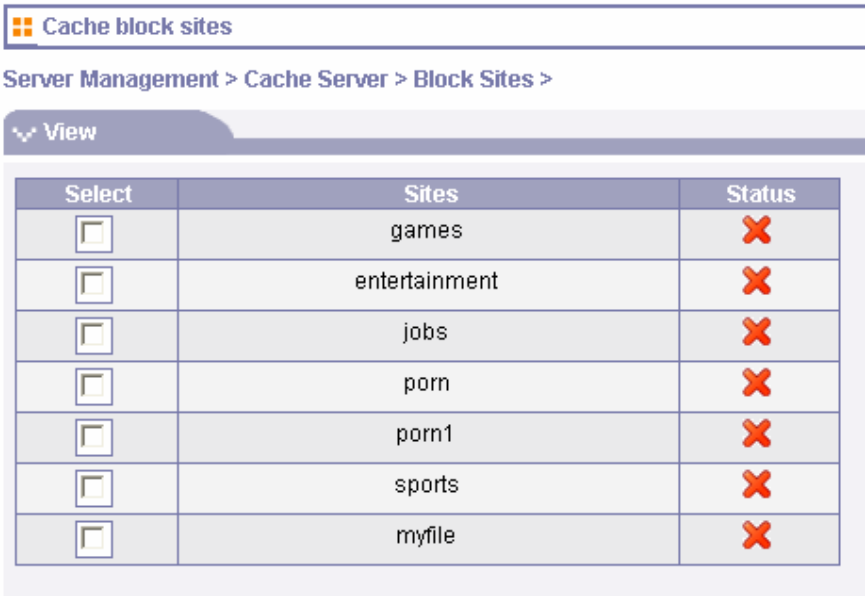
In the Smartguard`s Database millions of Internet sites, IM and P2P applications, and e-mail activities are continuously researched via a global network of Internet link-mining spiders, probe e-mail accounts, and honey pots. Html stripped text, e-mail, and application components are analyzed for prioritization, and categorized using adaptive intelligence technologies that scan for embedded malicious codes, spyware, viruses, worms inappropriate image signatures and inappropriate text.

Web content filtering helps you increase productivity by filtering or blocking Web site privileges. The SmartGuard filtering is a customizable management tool with click interface that lets you control Web surfing and deny access to objectionable material. Filtering is transparent to users and requires no additional client software or configuration.

a. Based on URL & Keywords
b. Based on Online Website Screening & Categorization
c. Preloaded Websites & Categories
e. Categorization & Managing various File Types
f. Stops Internet Messaging (Yahoo, MSN, AOL etc)
g. Content Caching & Reporting
h. Provision for Configuring External Cache
i. Database of restricted websites will be updated daily through automized process

8.1.2 Block Sites

Administrator can select the various groups for blocking sites as mentioned in the menu given below. Administrator just needs to click the specific group and mention the list of sites it wants to get blocked / Unblocked.



smartguard

Chapter 6

Bandwidth Management

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

6. BANDWIDTH MANAGEMENT

BANDWIDTH MANAGEMENT: - SmartGuard allows network administrators to guarantee minimum bandwidth and prioritize traffic based on Rules created from web based management interface. By controlling the amount of bandwidth to an application or user, the network administrator can prevent a small number of applications or users to consume all available bandwidth.

Bandwidth management describes the use of software tools to put into place policies that govern how network traffic runs should carry on when passing a WAN (wide area network) or Internet connection. These tools enable detailed regulation over traffic, often on a per-flow basis. Network managers can apply policies that the network will apply according to destination address, protocol type, user and/or source address, application type, and other factors.

Enterprises can build a business case for bandwidth management by first estimating the cumulative savings from delayed bandwidth upgrades. The next step involves examining the high cost of network and application downtime to their organizations' bottom lines, then monitoring the status of their networks to see if any core business applications are creating productivity losses during periods of congestion. The aggregate savings from implementing a bandwidth management solution is almost always a compelling business case with a rapid ROI for the organization. Enterprises would like to gain the benefits of converged WAN services while still maintaining the application response times that will suit users and make application deployments successful. Monitoring only bandwidth management systems provide the dual benefits of providing this baseline business case data, and potentially replacing current or planned network monitoring platforms. To achieve a win-win situation, it is likely that some level of bandwidth management will be required.

The first step to successful bandwidth management is monitoring applications, protocols and users by using products that inspect network layer behavior and conditions as well as specific application performance levels, and have the ability to correlate the two. Before you can successfully manage application performance across a network by setting network policies and classifying traffic, you must have a way to discover the various applications, protocols, and users on the network and evaluate how they are behaving.

Bandwidth management involves classifying and marking traffic as to its priority. For example, delay sensitive applications like voice over IP (VoIP) usually would have a small amount of bandwidth guaranteed to them, and VoIP packets would be marked for placement in the top-priority queue. Citrix traffic requires that a small (but consistent) amount of bandwidth always be available in order for sessions not to break.

Real-time reports are invaluable in troubleshooting immediate network problems, while long-term reporting is best for analyzing network trends, such as daily congestion conditions on a given circuit. The most useful and versatile systems also provide policy-based bandwidth management capabilities since you will want to address the problems identified by your reports. A high-quality seven-layer monitoring tool should also provide easy access to a wide variety of real- time and long-term

reporting features. Use of a full-stack (seven-layer) device is especially powerful, because it pinpoints issues down to individual sessions, applications, protocols and users.

Together, classification and assigning actions to traffic classes form a network policy that will optimize your: bandwidth utilization, application performance and your business/IT resource alignment.

Setting enterprise-wide network policies should be a joint effort between the executive staff, departments and business units and the IT organization. Establishing a policy framework for your bandwidth management system should be closely tied to your strategic corporate goals, and affords you the opportunity to align your IT and networking resources with those goals. When you are comfortable that your traffic is being classified and grouped according to your objectives, policies can be created that direct your bandwidth management system on the proper handling of each traffic type. Once your policy framework is defined, most systems make it easy to create service groups to help classify traffic based on variables such as application, user, server, time of day, and time of week.

Once you have discovered what's running on your network, you can classify traffic as to its priority during periods of congestion. This type of monitoring requires DPI so that applications can be identified that don't utilize fixed port assignments, or use fixed ports but carry different traffic types.

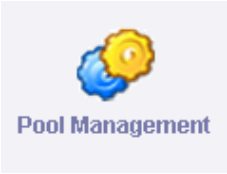
UBM or Unified Bandwidth Management is the name for a new emerging trend in the network management and control market. New UBM appliances incorporate multiple network management and control functions, including network load balancing (also referred to as dual-WAN load balancing, ISP aggregation or multi-homing) with built-in dynamic DNS, network redundancy, VPN tunnel reliability and optimization, and packet and/or traffic shaping. Some appliances also incorporate additional network monitoring functions for determining the status of network servers as well as reporting on network utilization.

Traditionally these functions were handled by multiple appliances and/or software based systems, however with the ever growing power and feature set of various appliances, this new trend has emerged as the next wave in network management and control solutions.

The rapid rise in UBM appliances can be attributed to the growing problems faced by organizations; which include an increasing amount of required bandwidth and ever growing remote user base which must have low latency access to critical network resources.

POLICY MANAGEMENT

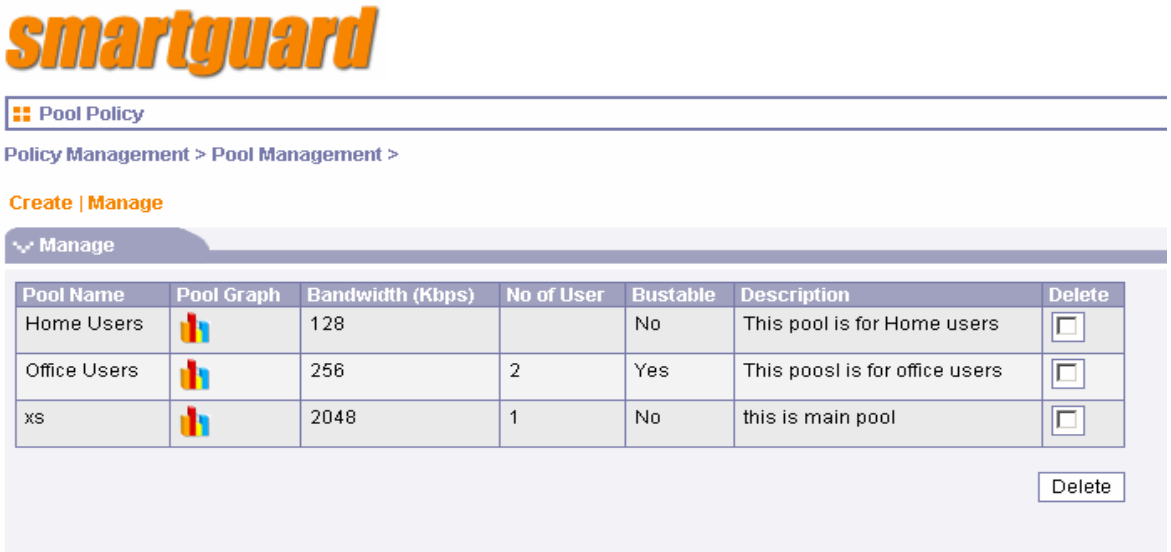
6.1 POOL MANAGEMENT



Pool Management is used for **division of incoming bandwidth** in a proper way. For Example: if our incoming total bandwidth is 384 then we distribute this bandwidth in two groups (for e.g. **Home & office**). An office user requires higher bandwidth and faster usage so we set our office bandwidth is 256 kbps and home 128 kbps.

Despite our incoming bandwidth is 384 Kbps all our "home" users will be restricted in a shell of 128Kbps only, this means whatever happens we have a pure 256kbps reserved for our office users. Pool Policy will be select by administrator in **Bandwidth Management** which is described bottom. Pool Management shows by default two Pools which is store in database.

STEP **Click on Policy Management in left side of main menu → now click on pool management icon.**

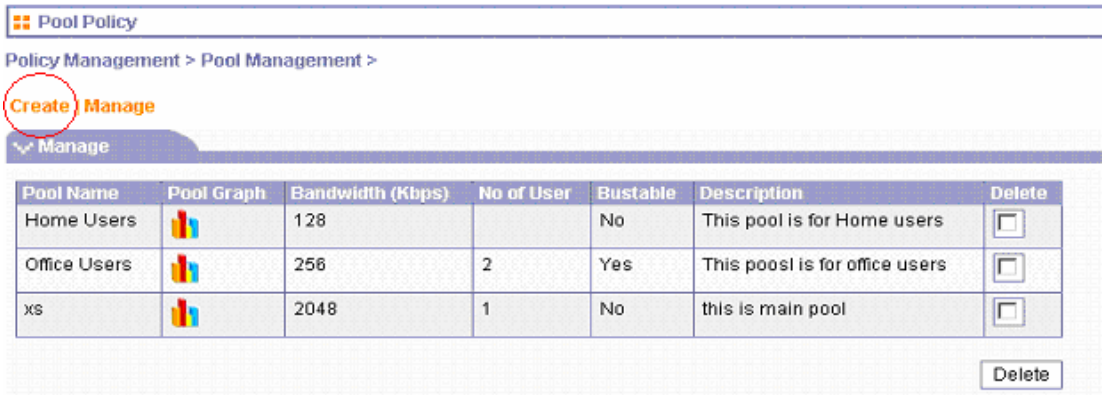


6.1.1 Create Pool

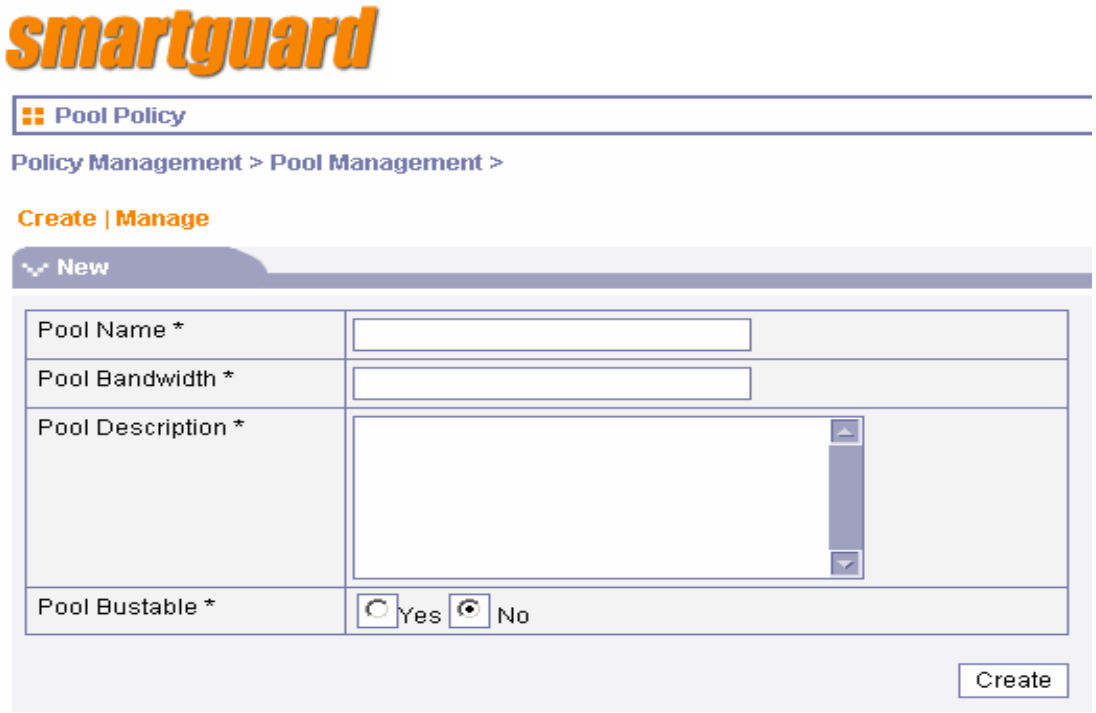
You can create new pool and modify by click on existing pool for example: click on Home Users. Its shows you this form which is used for modification.

.

STEP **Click on Policy Management in left side of main menu → Select pool management icon → then click on create option.**



After click on create option following window will be displayed.

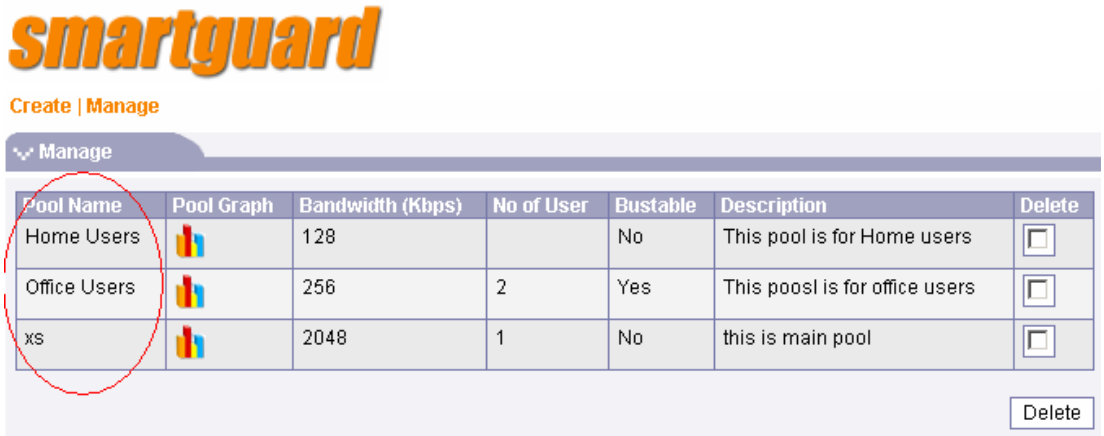


Create Pool	You can create New Pool
Modify Pool	You can Modify Pool. For Modification Click on List name(for ex. Home users) After click it Shows a Edit Form where you can change the values.
Delete Pool	You can Delete Pool by click on checkbox which pool you want to delete after that click on Delete Button.
Pool Bustable	If we want allow one pool to borrow Bandwidth from other pools then make it "Yes" else "No". Bustable is used for increase Bandwidth and speed.

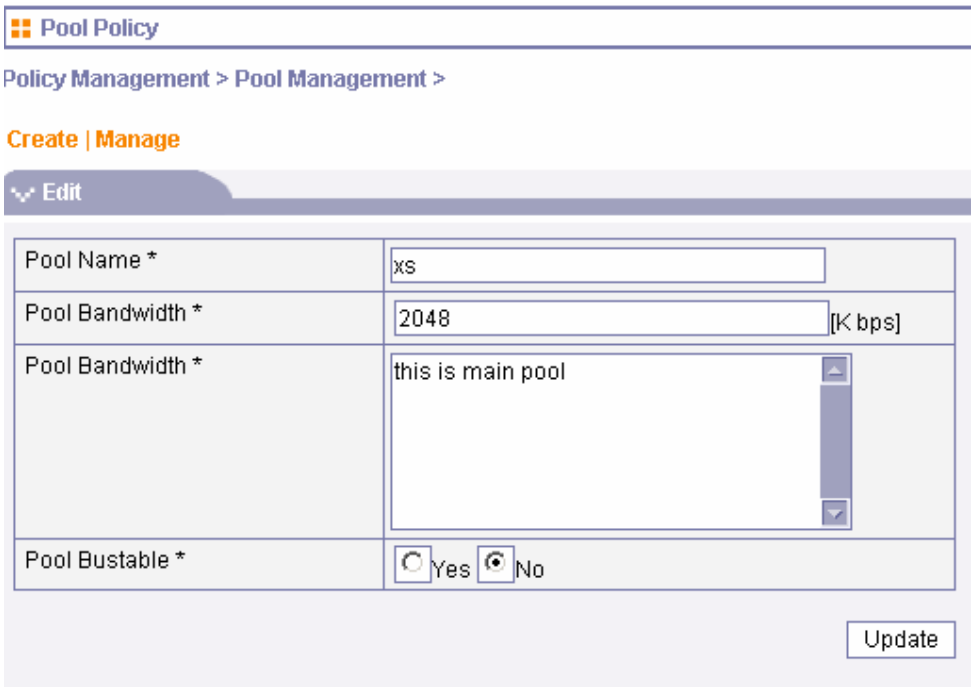
6.1.2 Modify Pool

If you want to modify in existing poll then click on existing poll name in poll management window example: you want to modify in XS poll name then click on XS. Its shows you this form which is used for modification.

STEP **Click on Policy Management in left side of main menu → Select pool management icon → then click on pool name.**



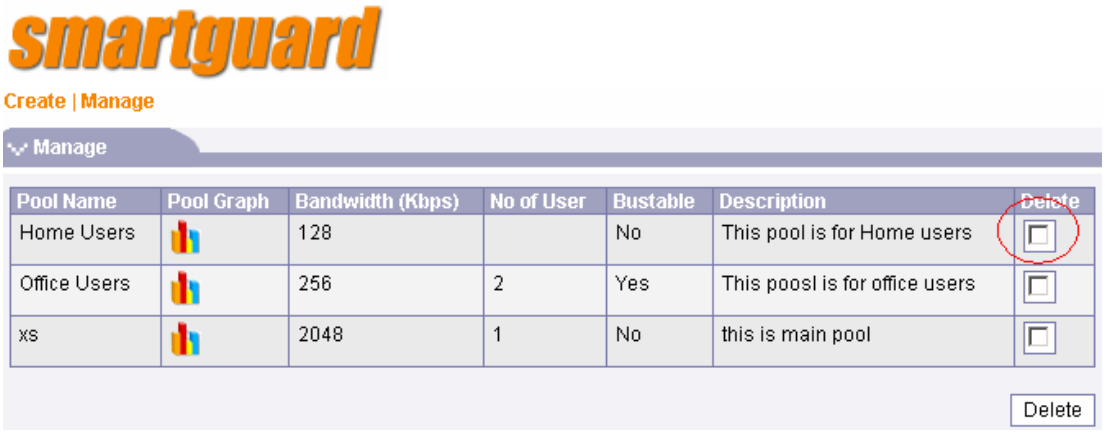
After click on pool name following window will be displayed.



6.1.3 Delete Pool

You can delete pool by click on checkbox which pool you want to delete after that click on Delete Button.

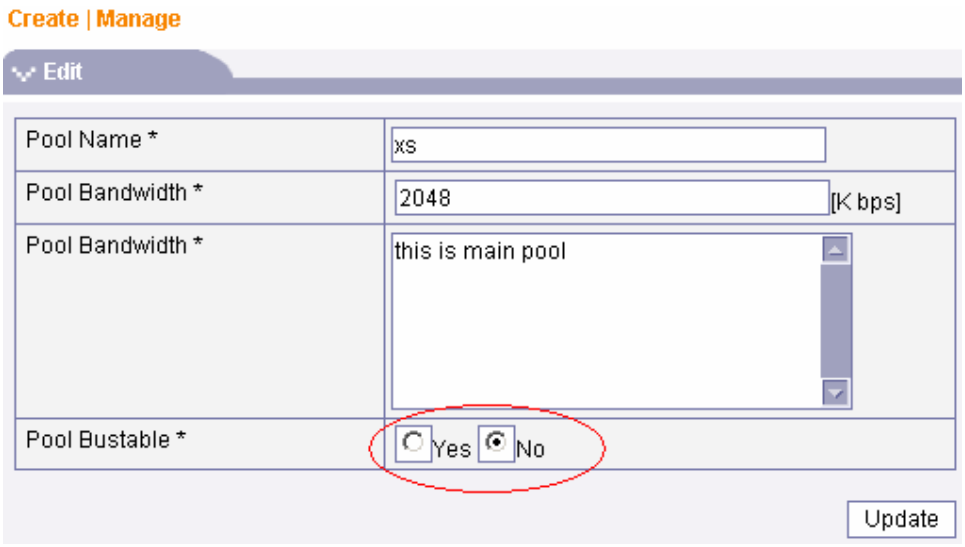
STEP **Click on Policy Management in left side of main menu → Select pool management icon → click on check box → now click on delete button.**



6.1.4 Pool Bustable

If we want allow one pool to borrow Bandwidth from other pools then make it "Yes" else "No". Bustable is used for increase Bandwidth and speed.

STEP **Click on Policy Management in left side of main menu → Select pool management icon → then click on pool name.**

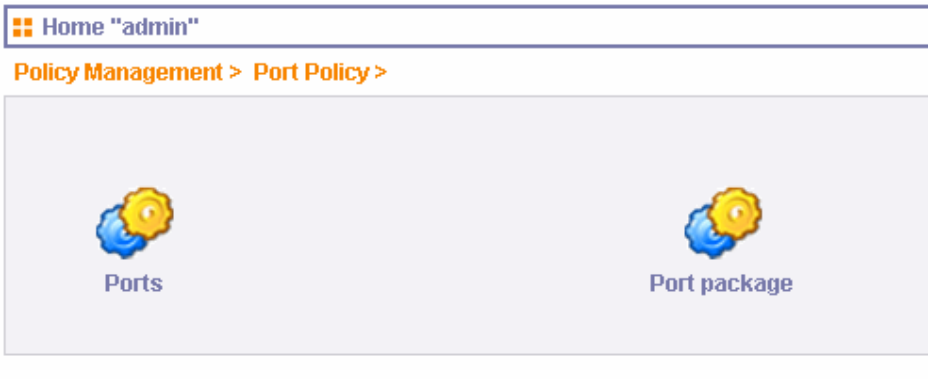


6.2 PORT MANAGEMENT

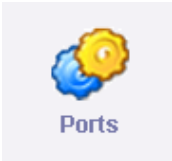
Port Management is used to specify port access of particular user's or groups. Port

policy means allow to user's access particular port for example surfing, mailing, chatting and etc.. Port Management has two categories: Single port or Group Port. In a single port (Port Policy Management) you can create a single port policy for example port name : http, port no :80 which is used only for surfing only and if you want user's can access multiple ports or selective port then you define multiple ports or single port in a port group.

STEP **Click on Policy Management in left side of main menu → now click on port management icon.**

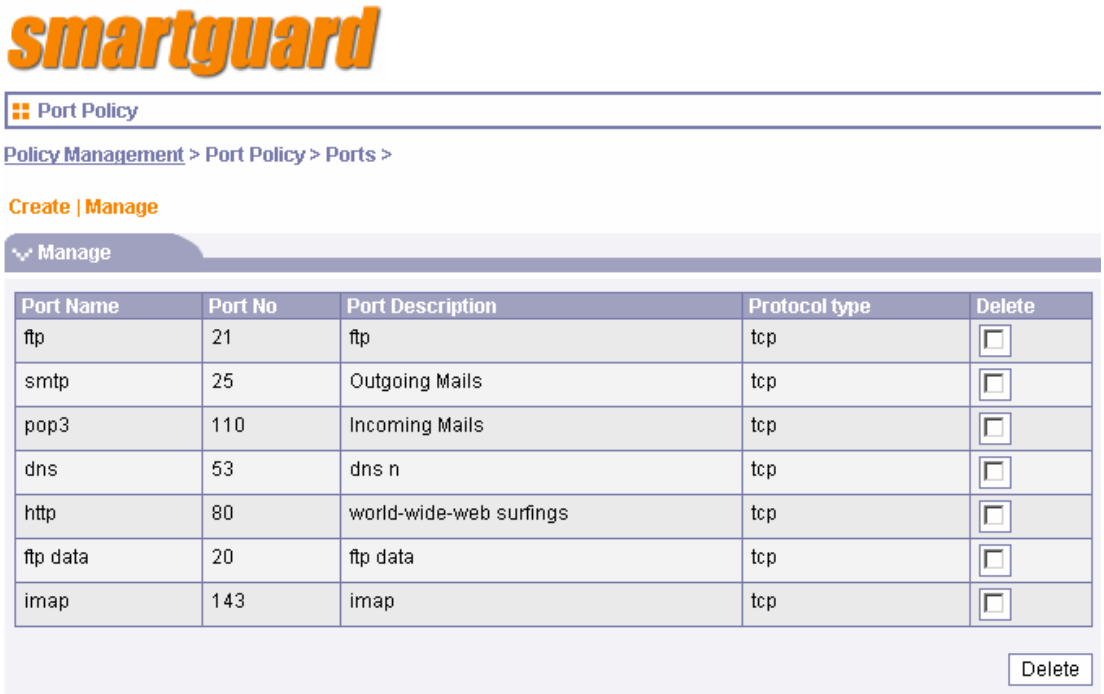


6.2.1 Ports



STEP **Click on Policy Management in left side of main menu → click on port management icon → now click on ports icon**.

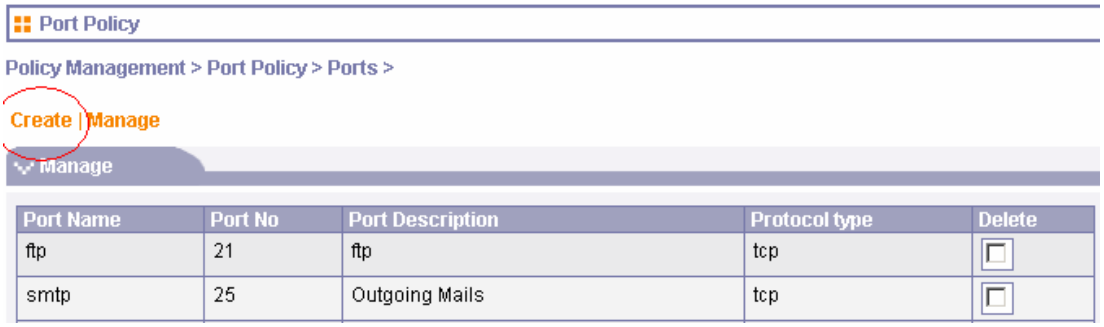
After clicking on Port option following interface will be displayed.



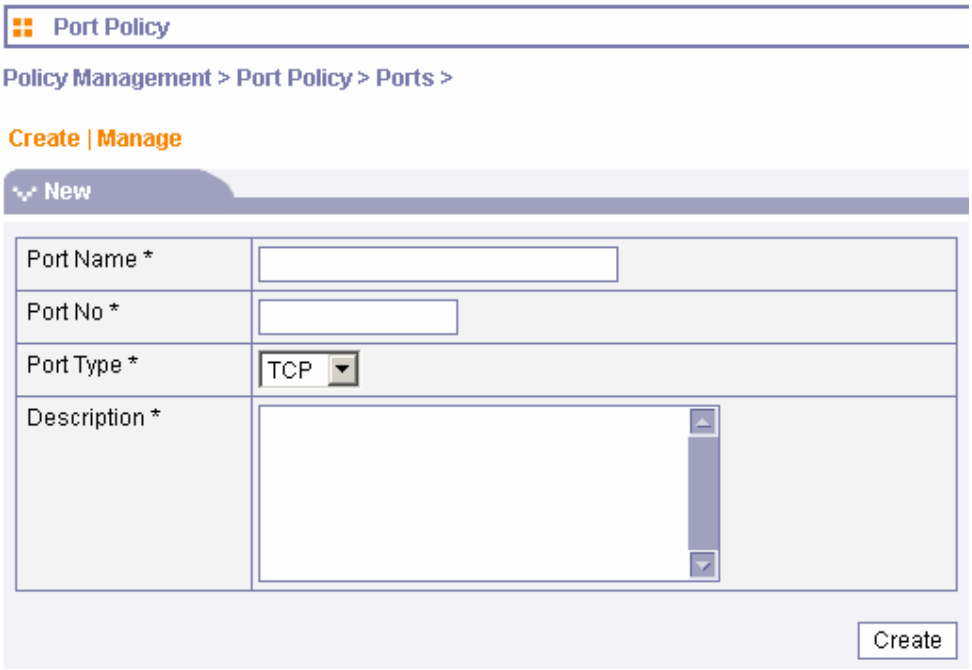
6.2.1.1 Create Port

You can create new Port by clicking on create option.

STEP **Click on Policy Management in left side of main menu → Select port policy icon → Select ports icon → then click on create option.**



After click on create option following window will be displayed.

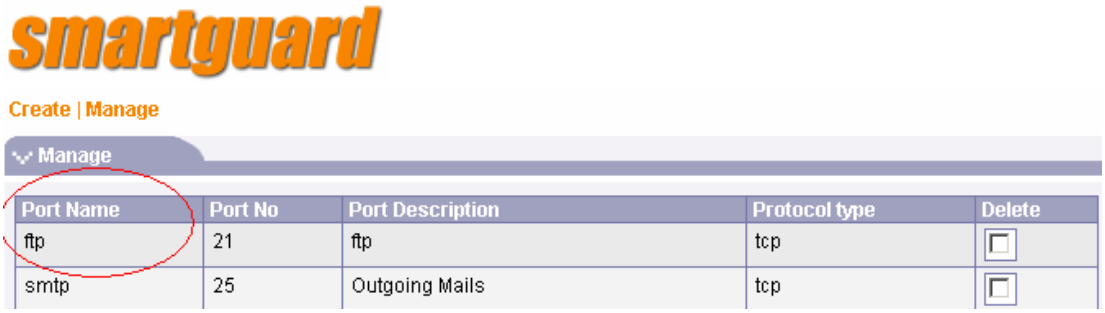


Port Name	Enter the Port Name
Port No.	Enter the Port No
Port Type	Enter the Port Type for ex: tcp/udp/ icmp
Description	Describe the Port details why you create this port

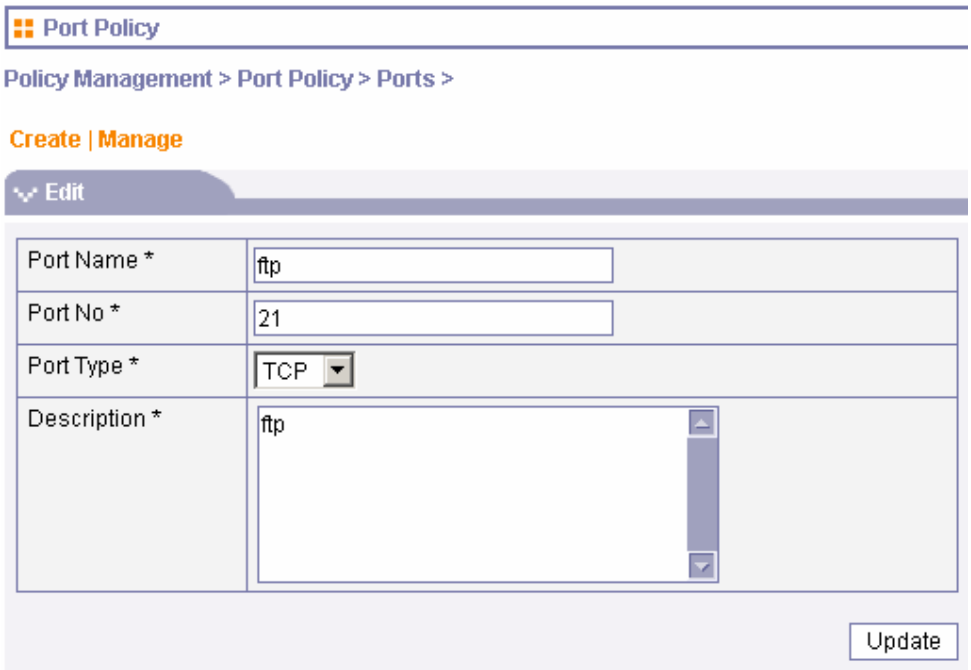
6.2.1.2 Modify Port

If you want to modify in existing port then click on existing port name in port policy window example: you want to modify in ftp port then click on ftp, then you will be directed to following option.

STEP **Click on Policy Management in left side of main menu → Select port policy icon → Select ports icon → then click on port name.**



After click on port name following window will be displayed.



☞ If any modification require in port no or port type field then first of all you have to disconnect all users.

6.2.1.3 Delete Port

STEP **Click on Policy Management in left side of main menu → Select port policy icon → now click on ports icon → click on check box → click on delete button**

Manage

Port Name	Port No	Port Description	Protocol type	Delete
ftp	21	ftp	tcp	☐
smtp	25	Outgoing Mails	tcp	☐

You can delete desired port by click on checkbox which port you want to delete after that click on Delete Button your port was delete.

6.2.2 Ports packaging

This option is used for port specification to users. All Ports or some particular ports we can specify here. In Port Group you can create/modify/Delete Port package.

STEP **Click on Policy Management in left side of main menu → click on port policy icon → now click on port package icon.**

Port Group Policy

Policy Management > Port Policy > Port package >

Create | Manage

Manage

Port Group Name	Port Name	Delete
All Ports without cache	All Ports	☐
All Ports with cache	All Ports	☐
Browsing/mailing port	smtp pop3 dns http	☐

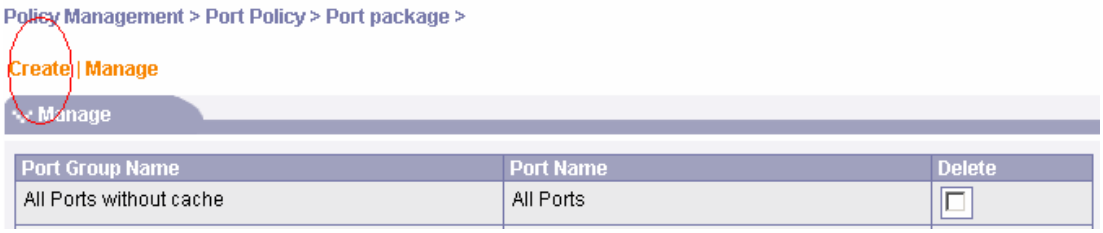
Delete

6.2.2.1 Create Port package

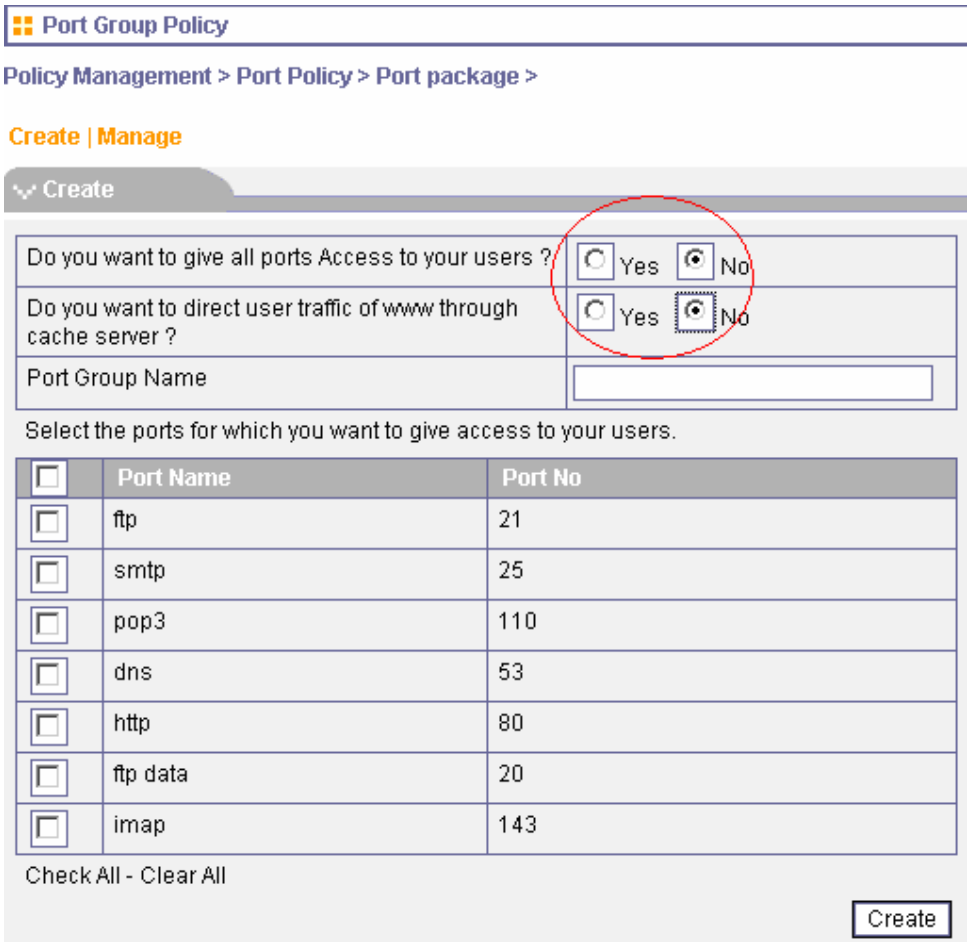
You can create Port package Then click on create option in port package. Port package settings are By Default Select All Ports No and cache Server also No.

after click on create option you will display this window.

STEP **Click on Policy Management in left side of main menu → click on port policy icon → now click on port package icon → then click create** option.



After click on create option following window will be displayed.



1. **All Ports** = If you have no idea about port No then Choose "Yes" otherwise select any port.

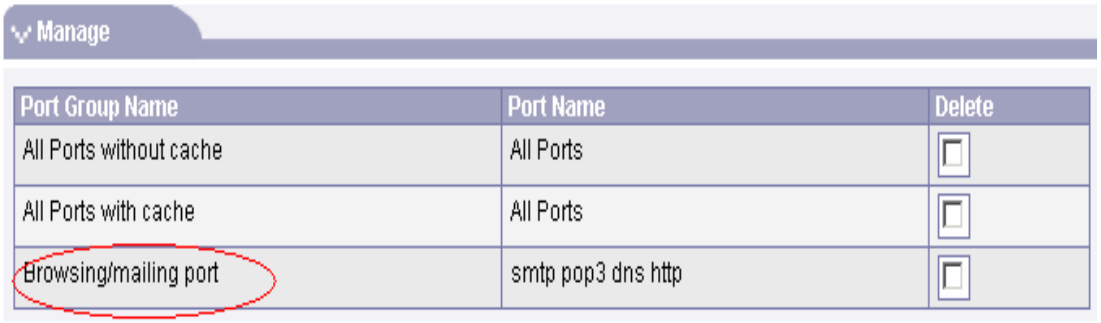
2. **Select Ports** = Specific Ports is used for assigning particular port access to particular user's. For ex: You want user only Mailing then click on checkbox smtp, pop3

3. **Cache Server** = Cache server option enables Subscribers/users to take advantage of cache of SmartGuard Broad Band Manager. SmartGuard caches all sites visited by Subscribers/users locally in to its own hard drive. Once site is cached locally benefit of cache is given to all users who visit same site. The advantage of Cache Server is that it will store the web pages once requested by the users and there after if any user requests the same page it will forward the same web page that is stored in Cache and forward it to the Users. This will be applicable if the Cache Server is enabled. Thus it also saves expensive Bandwidth.

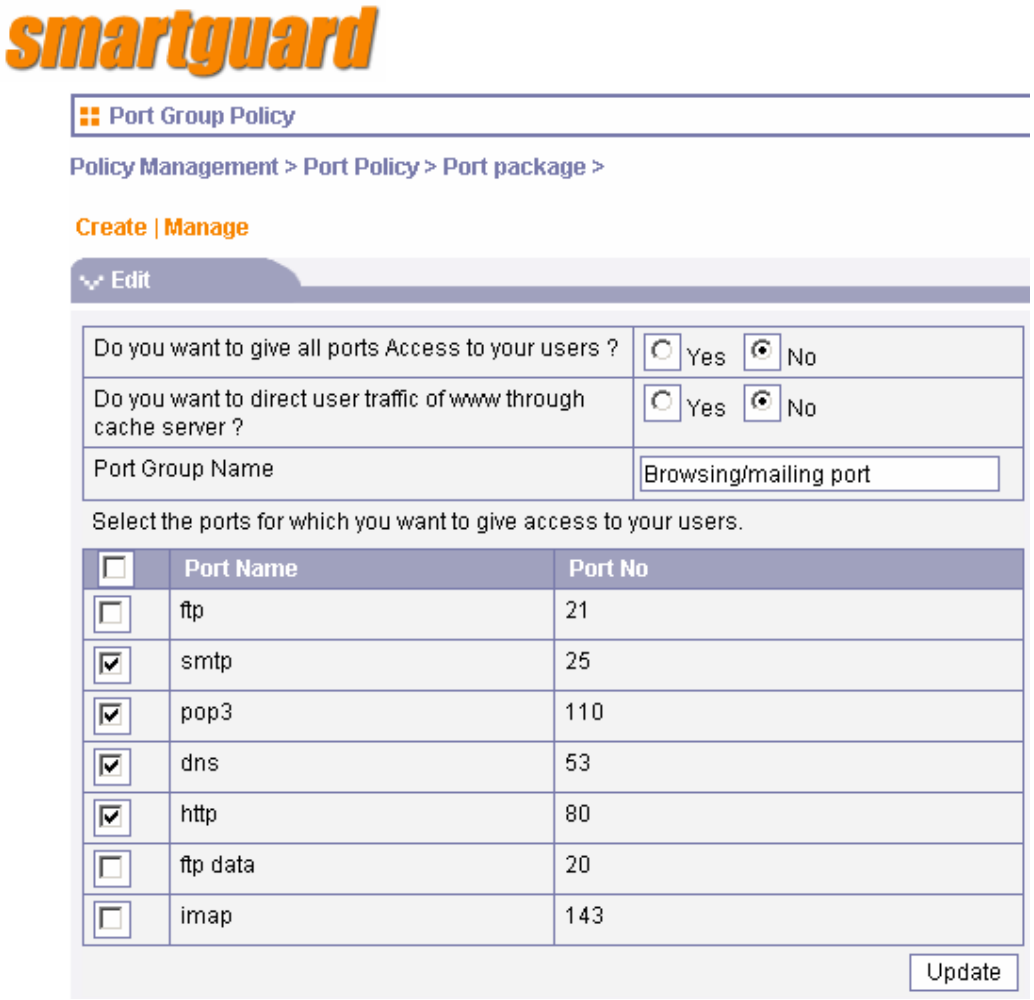
6.2.2.2 Modify Port package

If you want to modify in existing port group then click on existing port group name in port policy window example: you want to modify in Browsing/milling port group then click on Browsing/milling port group. Its shows you following interface which is used for modification.

STEP **Click on Policy Management in left side of main menu → click on port policy icon → now click on port package icon → then click on port group name**.



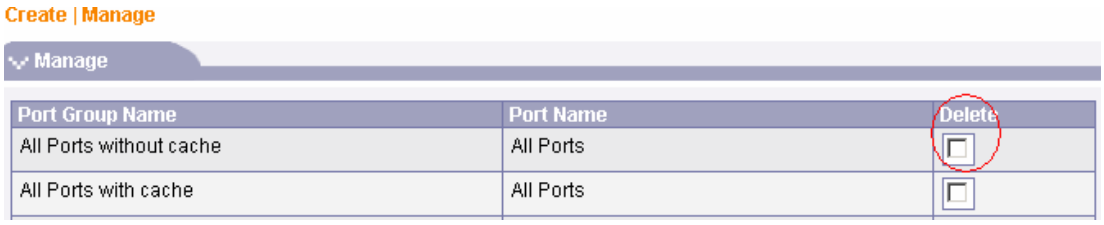
After click on port group name following window will be displayed.



1. **Create Port =** You can create new port . **Note:** You have to create port for selection in Port Group Management
2. **Modify Port =** You can modify port.
3. **Delete Port =**You can delete port

6.2.2.3 Delete Port package

STEP **Click on Policy Management in left side of main menu → click on port policy icon → now click on port package icon → click on delete button.**



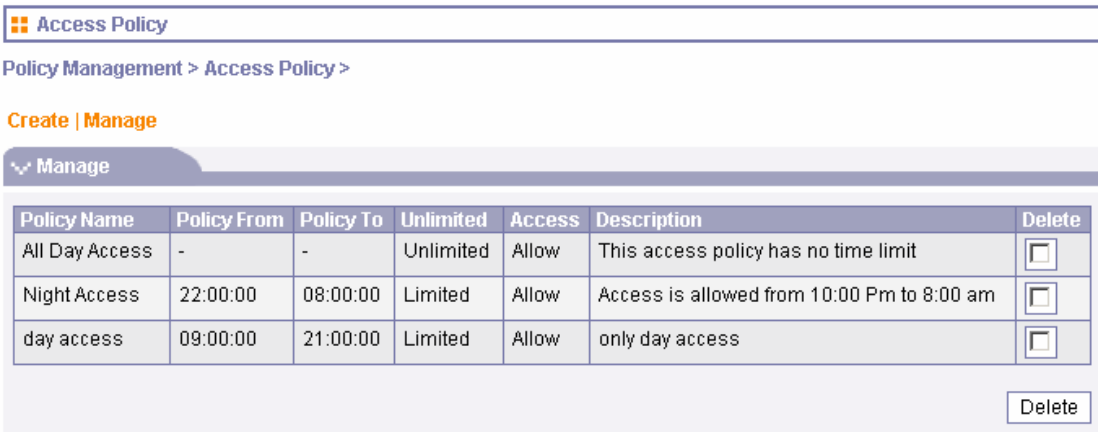
You can delete port group by click on checkbox which port group you want to delete after that click on Delete Button.

6.3 ACCESS POLICY

Access Policy is used to specify the time period for Internet Access of particular group or Users. For example: User can access Internet All Day, In Night Only or Evening Only. This Access policy will be select in package by Administrator which is required for user's Internet access particular time period

STEP **Click on Policy Management in left side of main menu → now click on access policy icon.**

After click on Access Policy following default policy name will be displayed.

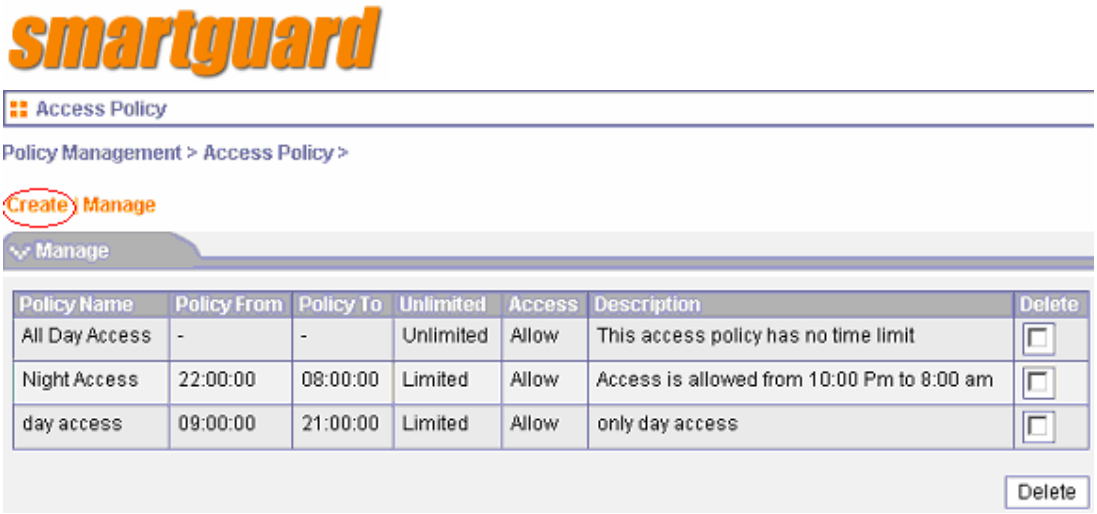


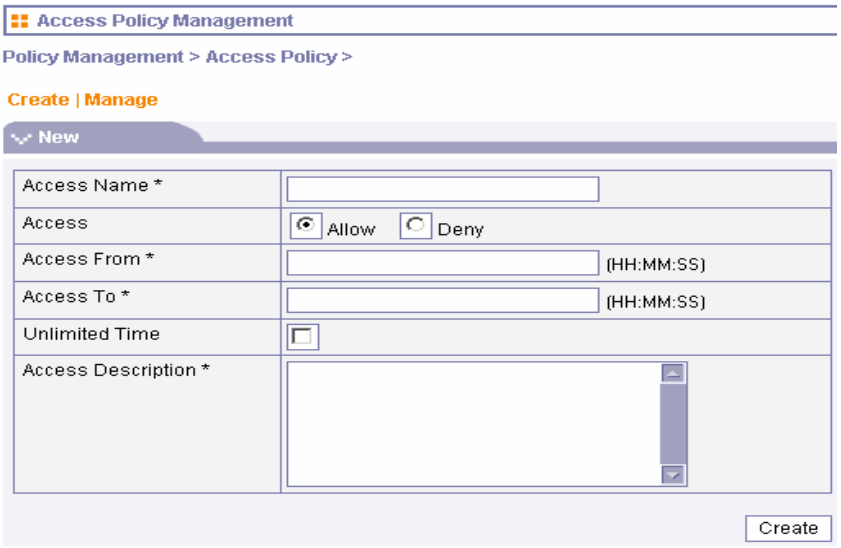
Policy Name	Policy From	Policy To	Unlimited	Access	Description	Delete
All Day Access	-	-	Unlimited	Allow	This access policy has no time limit	
Night Access	22:00:00	08:00:00	Limited	Allow	Access is allowed from 10:00 Pm to 8:00 am	
day access	09:00:00	21:00:00	Limited	Allow	only day access	

6.3.1 Create Access Policy

STEP **Click on Policy Management in left side of main menu → click on access policy icon → now select create option.**

If you want to create a policies then click on create option.





Access = If you click on "Allow" that means Group or a User will Allow access Internet in a particular time or "Deny" means that User or Group will not be access Internet in a particular time period.

Unlimited Access = If you click on Unlimited access Checkbox then User or Group will access Internet Unlimited time. That means User or Group has no restriction about Internet access time. You have to specify in "From" and "To" field 00:00:00. Otherwise you have to specify time in morning or evening in "From" and "To" field. For example: From 08:00:00 To 06:00:00

6.3.2 Modify Access Policy

If you want to modify in existing Access policy then click on existing Access policy name.

For Example: You want to modify in Day Access policy name then click on Day Access policy. Its shows you this form which is used for modification.

STEP **Click on Policy Management in left side of main menu → click on access policy icon → now click on policy name options.**

Create | Manage

Manage

Policy Name	Policy From	Policy To	Unlimited	Access	Description	Delete
All Day Access	-	-	Unlimited	Allow	This access policy has no time limit	☐
Night Access	22:00:00	08:00:00	Limited	Allow	Access is allowed from 10:00 Pm to 8:00 am	☐

After click on policy name following window will be displayed.

Access Policy

Policy Management > Access Policy >

Create | Manage

Edit

Access Name *	day access
Access	◉ Allow ○ Deny
Access From *	09:00:00 (HH:MM:SS)
Access To *	21:00:00 (HH:MM:SS)
Unlimited Time	☐
Access Description *	only day access

Update

6.3.3 Delete Access Policy

STEP **Click on Policy Management in left side of main menu → click on**

access policy icon → click on check box → then click on delete button.

Create | Manage

Manage

Policy Name	Policy From	Policy To	Unlimited	Access	Description	Delete
All Day Access	-	-	Unlimited	Allow	This access policy has no time limit	☐
Night Access	22:00:00	08:00:00	Limited	Allow	Access is allowed from 10:00 Pm to 8:00 am	☐

You can delete Access Policy by click on checkbox which Access policy name you want to delete after that click on Delete Button.

6.4 DATA TRANSFER POLICY

Data transfer policy is used to specify the "data transfer limit". This policy will be helping you to control on user's data transfer and bandwidth also. If over usage of data transfer then you can charge for over usage of data transfer limit. This data transfer policy also select in Package Creation by Administrator.

STEP **Click on Policy Management in left side of main menu → click on data transfer policy icon.**

Data Transfer Policy

Policy Management > Data Transfer Policy >

Create | Manage

Manage

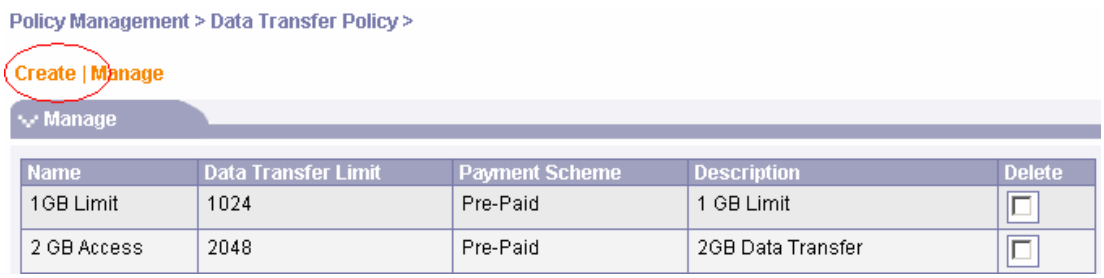
Name	Data Transfer Limit	Payment Scheme	Description	Delete
1GB Limit	1024	Pre-Paid	1 GB Limit	☐
2 GB Access	2048	Pre-Paid	2GB Data Transfer	☐
Unlimited	10000000000000	Pre-Paid	Unlimited Data Transfer	☐
ak	50	Pre-Paid	limit 50 MB	☐

Delete

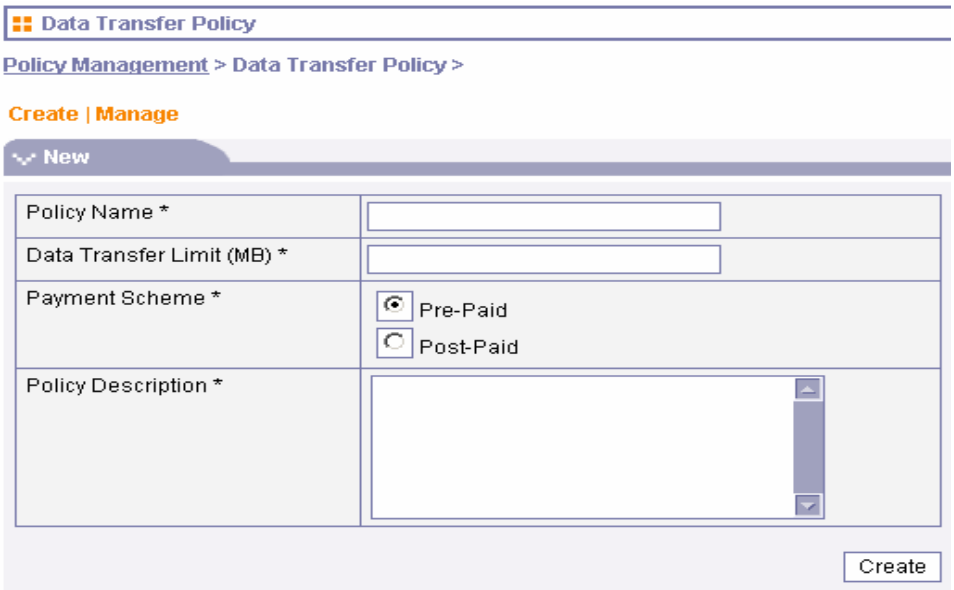
6.4.1 Create Data Transfer Policy

If you want to create a policies then click on create option

STEP **Click on Policy Management in left side of main menu → click on data transfer policy icon → Now click on create option.**



After click on create option following window will be displayed.



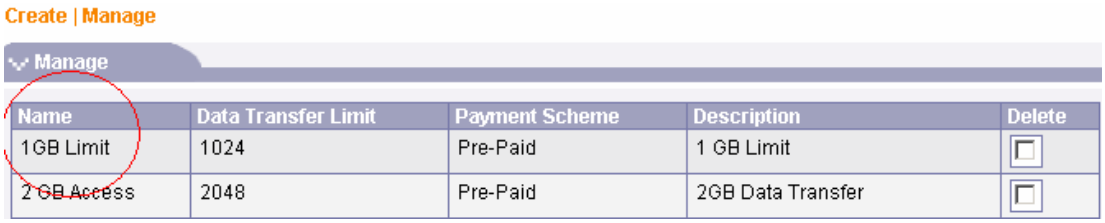
1. **Pre-Paid**
2. **Post-Paid**

6.4.2 Modify Data Transfer Policy

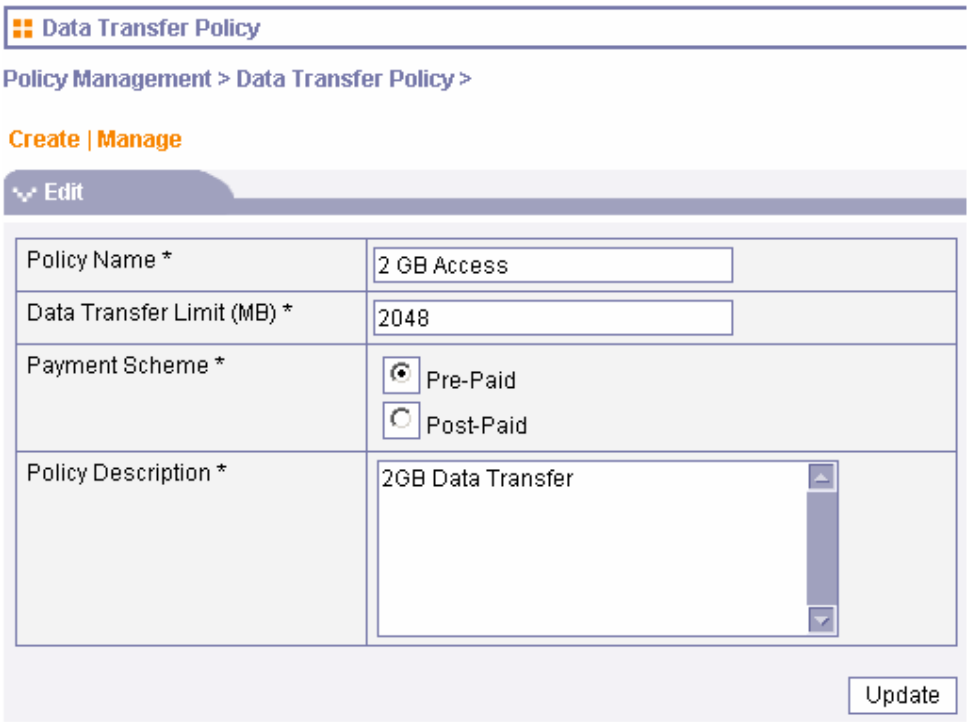
If you want to modify in existing Data Transfer policy then click on existing policy name.

For Example: you want to modify in 2GB Access policy then click on 2GB Access. Its shows you this form which is used for modification.

STEP **Click on Policy Management in left side of main menu → click on data transfer policy icon → now click on policy name.**

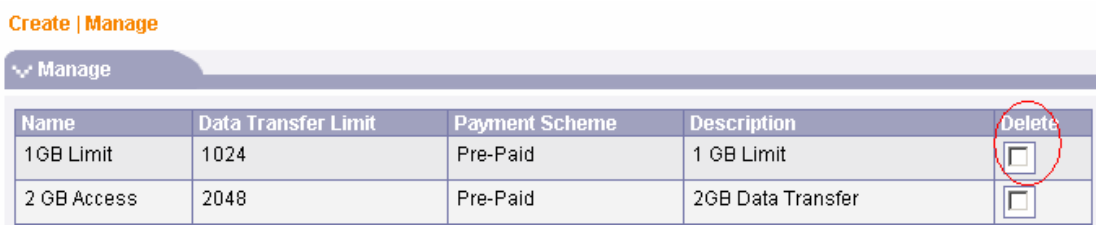


After click on policy name following window will be displayed.



6.4.3 Delete Data Transfer Policy

STEP **Click on Policy Management in left side of main menu → click on data transfer policy icon → now click on checkbox → click on delete button.**



Name	Data Transfer Limit	Payment Scheme	Description	Delete
1GB Limit	1024	Pre-Paid	1 GB Limit	
2 GB Access	2048	Pre-Paid	2GB Data Transfer	

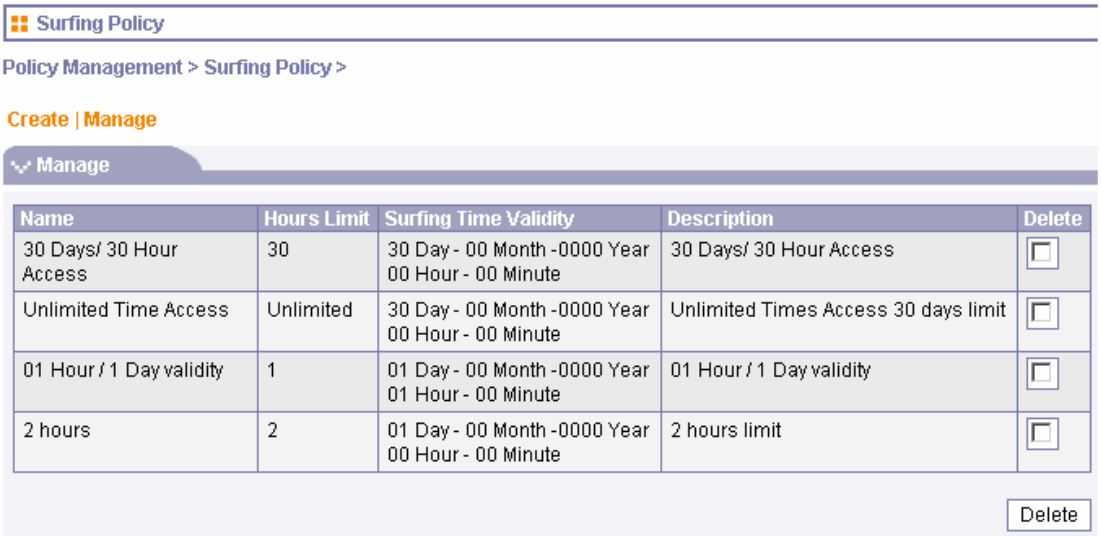
You can delete Access Policy by click on checkbox which Access policy name you want to delete after that click on Delete Button.

6.5 SURFING POLICY

Surfing Policy is used for allot surfing "hour" and "days" to particular user's or group. In Surfing policy you have to specify the total usage hours and days for a user's or group. This policy will help you for billing and renew package. If days and hours limit expire then as per users request for renewal. Administrator can renew the package and charge for new package to the users. This policy is also select in package policy. Under Surfing Policy Management has submenu of Create/Delete/Modify

STEP **Click on Policy Management in left side of main menu → click on surfing policy icon**

After click on Surfing Policy you will display this window.

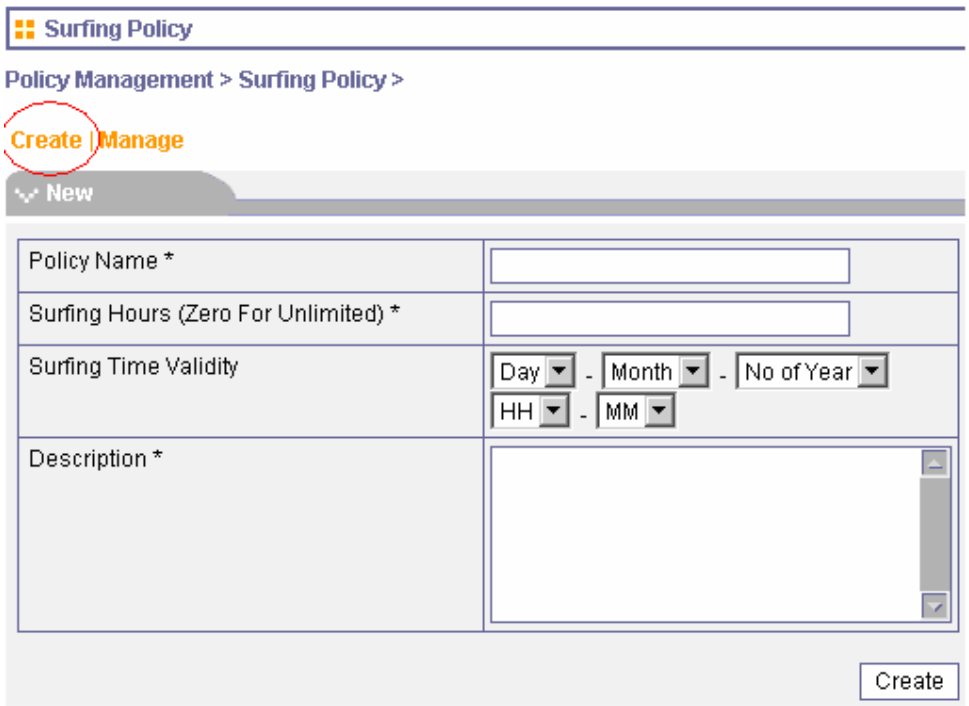


Name	Hours Limit	Surfing Time Validity	Description	Delete
30 Days/ 30 Hour Access	30	30 Day - 00 Month -0000 Year 00 Hour - 00 Minute	30 Days/ 30 Hour Access	
Unlimited Time Access	Unlimited	30 Day - 00 Month -0000 Year 00 Hour - 00 Minute	Unlimited Times Access 30 days limit	
01 Hour / 1 Day validity	1	01 Day - 00 Month -0000 Year 01 Hour - 00 Minute	01 Hour / 1 Day validity	
2 hours	2	01 Day - 00 Month -0000 Year 00 Hour - 00 Minute	2 hours limit	

6.5.1 Create Surfing Policy

STEP **Click on Policy Management in left side of main menu → click on surfing policy icon → now click on create option.**

If you want to create a policies then click on create option



6.5.2 Modify Surfing Policy

STEP **Click on Policy Management in left side of main menu → click on surfing policy icon → now click on policy name.**

If you want to modify in existing Surfing Policy then click on existing policy name.

For Example: You want to modify in 2 hours pack then click on 2 hours. Its shows you this form which is used for modification

01 Hour / 1 Day validity	1	01 Day - 00 Month -0000 Year 01 Hour - 00 Minute	01 Hour / 1 Day validity	☐
2 hours	2	01 Day - 00 Month -0000 Year 00 Hour - 00 Minute	2 hours limit	☐

Delete

Surfing Policy

Policy Management > Surfing Policy >

Create | Manage

Edit

Policy Name *	2 hours
Surfing Hours(Zero For Unlimited) *	2
Surfing Time Validity	01 Day - 00 Month - 0 Year 0 Hour - 0 Minute
Description *	2 hours limit

Update

6.5.3 Delete Surfing Policy

STEP **Click on Policy Management in left side of main menu → click on surfing policy icon → now click on checkbox → click on delete button.**

You can delete Surfing Policy by click on checkbox which Surfing policy name you want to delete after that click on Delete Button.

Manage

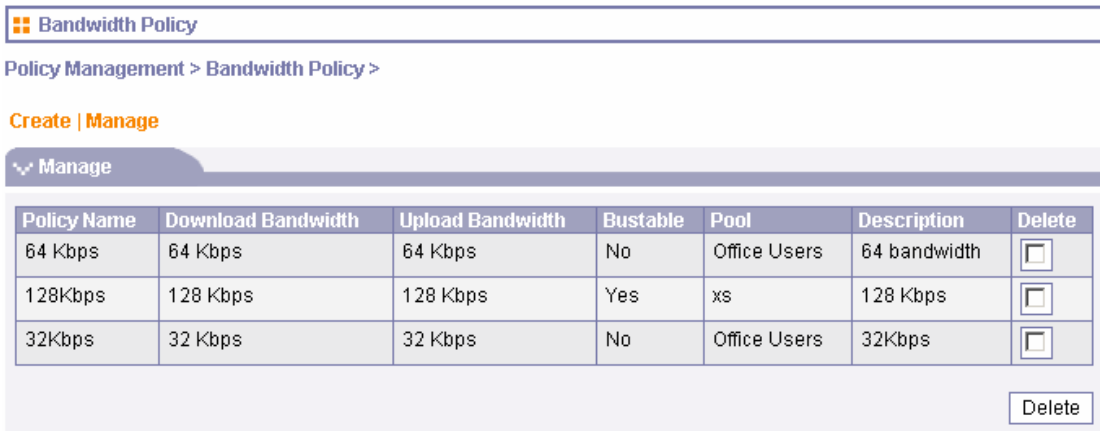
Name	Hours Limit	Surfing Time Validity	Description	Delete
30 Days/ 30 Hour Access	30	30 Day - 00 Month -0000 Year 00 Hour - 00 Minute	30 Days/ 30 Hour Access	☐
Unlimited Time Access	Unlimited	30 Day - 00 Month -0000 Year 00 Hour - 00 Minute	Unlimited Times Access 30 days limit	☐

6.6 BANDWIDTH POLICY

Bandwidth Policy management is used to specify the maximum limit of "upload" & "download" speed for a particular group or user's. If you makes "Bustable" "Yes" then the customer can utilized (free bandwidth) available in the pool. This policy will help you to control bandwidth. You can view Upload & download speed of login user's on User Management page and also view graphically representation in system>graph. This Bandwidth policy is select by administrator in Package Management.

STEP **Click on Policy Management in left side of main menu → click on bandwidth policy icon.**

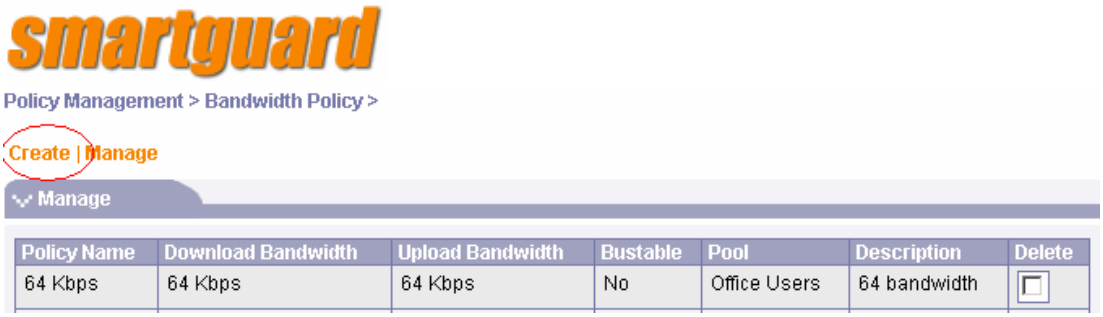
After click on Bandwidth Policy following interface will be displayed.



Policy Name	Download Bandwidth	Upload Bandwidth	Bustable	Pool	Description	Delete
64 Kbps	64 Kbps	64 Kbps	No	Office Users	64 bandwidth	
128Kbps	128 Kbps	128 Kbps	Yes	xs	128 Kbps	
32Kbps	32 Kbps	32 Kbps	No	Office Users	32Kbps	

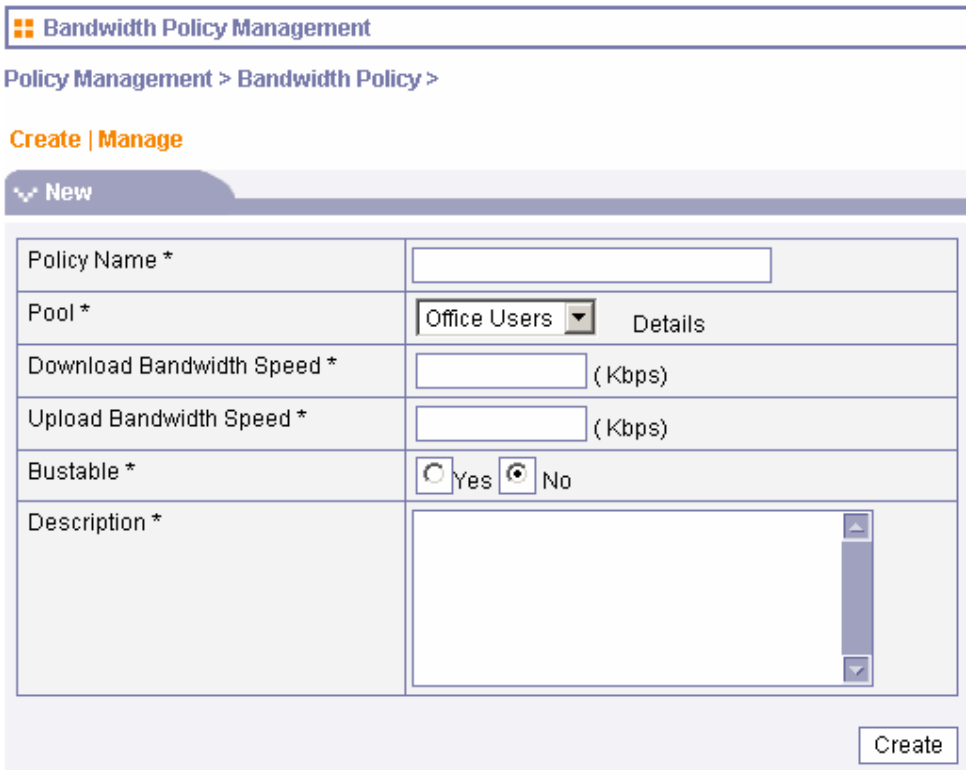
6.6.1 Create Bandwidth Policy

STEP **Click on Policy Management in left side of main menu → click on bandwidth policy icon → then select create option.**



Policy Name	Download Bandwidth	Upload Bandwidth	Bustable	Pool	Description	Delete
64 Kbps	64 Kbps	64 Kbps	No	Office Users	64 bandwidth	

If you want to create a Bandwidth Policies then click on create option. After click on create option following window will be displayed.



1. Pool = Select Pool which is already discussed above for eg. Office/ home User's

2. Download/ Upload Speed =Here you can specify download & upload data speed.

3. Bustable = we want to allow borrow (free) bandwidth available in the pool so, click on Bustable checkbox for "Yes".

6.6.2 Modify Bandwidth Policy

STEP **Click on Policy Management in left side of main menu → click on bandwidth policy icon → then click on policy name.**

Create | Manage

Manage

Policy Name	Download Bandwidth	Upload Bandwidth	Bustable	Pool	Description	Delete
64 Kbps	64 Kbps	64 Kbps	No	Office Users	64 bandwidth	
128Kbps	128 Kbps	128 Kbps	Yes	xs	128 Kbps	

If you want to modify in existing Bandwidth Policy then click on existing policy name.

For Example: you want to modify in 64 kbps pack then click on 64 kbps. Its shows you this form which is used for modification.

Bandwidth Policy Management

Policy Management > Bandwidth Policy >

Create | Manage

Edit

Policy Name *	64 Kbps
Pool *	Office Users Details
Download Bandwidth *	64
Upload Bandwidth Speed *	64
Bustable *	Yes No
Description *	64 bandwidth

Update

6.6.3 Delete Bandwidth Policy

STEP **Click on Policy Management in left side of main menu → click on bandwidth policy icon → then click on check box option → now click on delete button.**

Create | Manage

Manage

Policy Name	Download Bandwidth	Upload Bandwidth	Bustable	Pool	Description	Delete
64 Kbps	64 Kbps	64 Kbps	No	Office Users	64 bandwidth	☐
128Kbps	128 Kbps	128 Kbps	Yes	xs	128 Kbps	☐

You can delete Bandwidth Policy by click on checkbox which Bandwidth policy name you want to delete after that click on Delete Button.

6.7 PACKAGE

STEP **Click on Policy Management in left side of main menu → click on package icon.**

You can select different policies made earlier & make different package as required. In Package you can specify these policies:

- Access policy(time period)
- Surfing policy
- Data transfer Speed
- Bandwidth Speed
- Port no.
- Pool

After click on Package following interface will be displayed.

smartguard

Package Policy

Policy Management > Package >

Create | Manage

Manage

Name	Surfing Policy	Access Policy	Bandwidth Policy	Port Policy	ISP	Data Transfer Policy	Description	Delete
32Kbps NIGHT	Unlimited Time Access	Night Access	32Kbps	All Ports with cache	ISP 1	Unlimited	32kbps	
32kbps	Unlimited Time Access	All Day Access	32Kbps	All Ports with cache	ISP 1	Unlimited	32kbps	
64Kbps	Unlimited Time Access	All Day Access	64 Kbps	All Ports with cache	ISP 1	Unlimited	64 Kbps	
128Kb	Unlimited Time Access	All Day Access	128Kbps	All Ports with cache	ISP 1	Unlimited	128	
ak	2 hours	All Day Access	128Kbps	All Ports with cache	ISP 1	ak	2 hours pack	
ka	01 Hour / 1 Day validity	All Day Access	128Kbps	All Ports with cache	ISP 1	Unlimited	one hour package	

Delete

6.7.1 Create package

STEP **Click on Policy Management in left side of main menu → click on package icon → then select create option.**

Here you specify the Package Name, Select Surfing Policy, Access Policy, Bandwidth Policy, Port Policy, Data Transfer & package charges. All these policies describe above. If you want to create then you can create also.

If you want to create a Packages then click on create option

Policy Management > Package >

Create | Manage

Manage

Name	Surfing Policy	Access Policy	Bandwidth Policy	Port Policy	ISP	Data Transfer Policy	Description	Delete
32Kbps NIGHT	Unlimited Time Access	Night Access	32Kbps	All Ports with cache	ISP 1	Unlimited	32kbps	
32kbps	Unlimited Time Access	All Day Access	32Kbps	All Ports with cache	ISP 1	Unlimited	32kbps	

After click on create option following option will be displayed.

smartguard

Package Policy

Policy Management > Package >

Create | Manage

New

Package Name *	
Surfing Policy	30 Days/ 30 Hour Access Details
Access Policy	All Day Access Details
Bandwidth Policy :	64 Kbps Details
Port Policy :	All Ports without cache Details
Datatransfer Policy :	1GB Limit Details
Internet Service Provider Policy :	ISP1 Details
ISP Failover Allow	Yes No
Setup Charge *	
Package Charge *	
Description *	
Access Continue after Expiry ?	Yes No
Over Access Charges	
View Package to User	Yes
View Package to Reseller	Select Resellers Name admin sa (for multiple selection, Press Ctrl key + name)

Create

6.7.2 Modify package

STEP **Click on Policy Management in left side of main menu → click on package icon → then click on package name.**

In Package Management view list of all packages. You can create new package by click on Create option. If you want to modify the package the click on package Name it will shows Edit Package form.

For Example: You want to change in 128 kb pack then click on 128 kb. Its shows you this form which is used for modification.

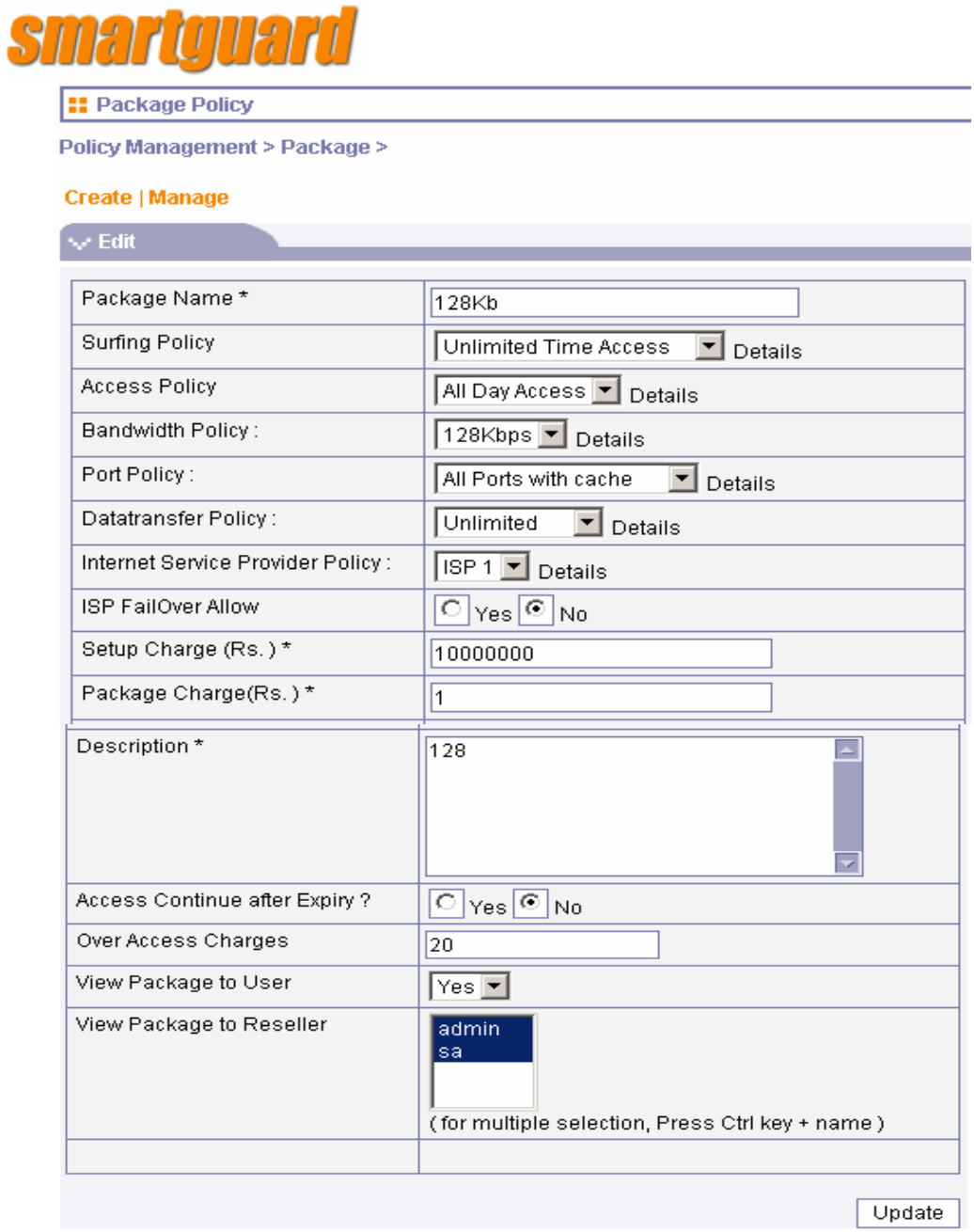
Policy Management > Package >

Create | Manage

Manage

Name	Surfing Policy	Access Policy	Bandwidth Policy	Port Policy	ISP	Data Transfer Policy	Description	Delete
32Kbps NIGHT	Unlimited Time Access	Night Access	32Kbps	All Ports with cache	ISP 1	Unlimited	32kbps	
32kbps	Unlimited Time Access	All Day Access	32Kbps	All Ports with cache	ISP 1	Unlimited	32kbps	
64Kbps	Unlimited Time Access	All Day Access	64 Kbps	All Ports with cache	ISP 1	Unlimited	64 Kbps	
128Kb	Unlimited Time Access	All Day Access	128Kbps	All Ports with cache	ISP 1	Unlimited	128	

After click on package name following option will be displayed.



6.7.3 Delete package

STEP **Click on Policy Management in left side of main menu → click on package icon → click on check box → then click on delete button.**

You can delete Package by click on checkbox which Package name you want to delete after that click on Delete Button.

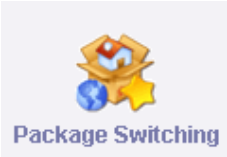
Policy Management > Package >

Create | Manage

Manage

Name	Surfing Policy	Access Policy	Bandwidth Policy	Port Policy	ISP	Data Transfer Policy	Description	Delete
32Kbps NIGHT	Unlimited Time Access	Night Access	32Kbps	All Ports with cache	ISP 1	Unlimited	32kbps	
32kbps	Unlimited Time Access	All Day Access	32Kbps	All Ports with cache	ISP 1	Unlimited	32kbps	
64Kbps	Unlimited Time Access	All Day Access	64 Kbps	All Ports with cache	ISP 1	Unlimited	64 Kbps	

6.8 PACKAGE SWITCHING



STEP **Click on Policy Management in left side of main menu → click on package switching icon.**

Package Switching Policy

Policy Management > Package Switching >

Create | Manage

Manage

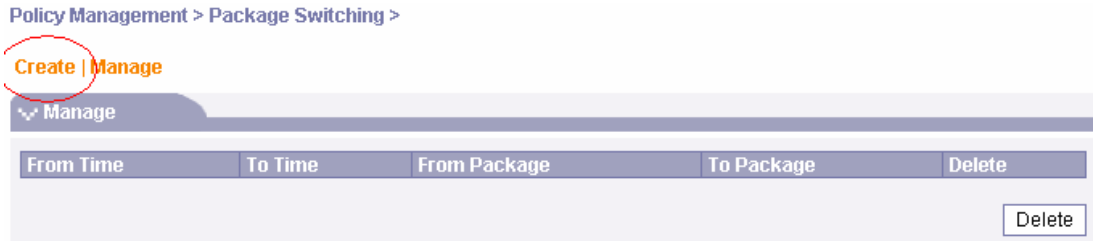
From Time	To Time	From Package	To Package	Delete

Delete

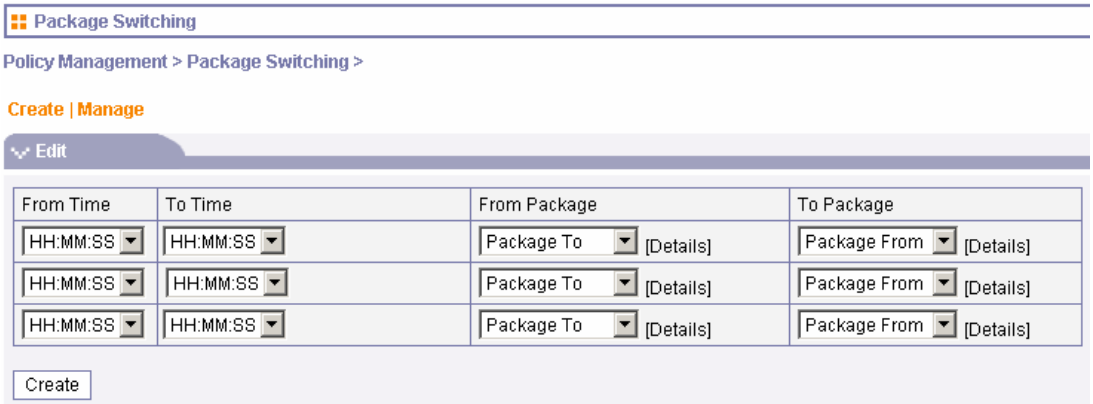
One Package Name should not be Same for another package Switching

6.8.1 Create Package Switching

STEP **Click on Policy Management in left side of main menu → click on package switching icon → click on create option.**



After click on create option following option will be displayed.



6.8.3 Delete Package Switching

STEP **Click on Policy Management in left side of main menu → click on package switching icon → click on check box → then click on delete button.**

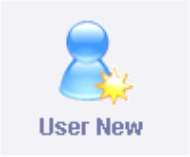
You can delete Package by click on checkbox which Package name you want to delete after that click on Delete Button.

6.9 User Management

STEP **Click on User Management in left side of main menu.**

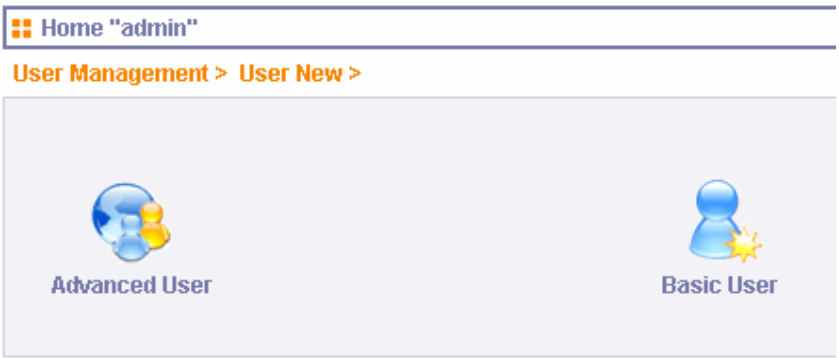
When you click on user management it will show you options as displayed below:

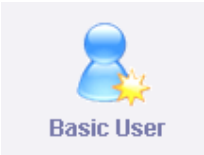
6.9.1 CREATE NEW USERS



STEP **Click on User Management in left side of main menu → click on user new icon.**

On clicking user new icon following options are displayed.

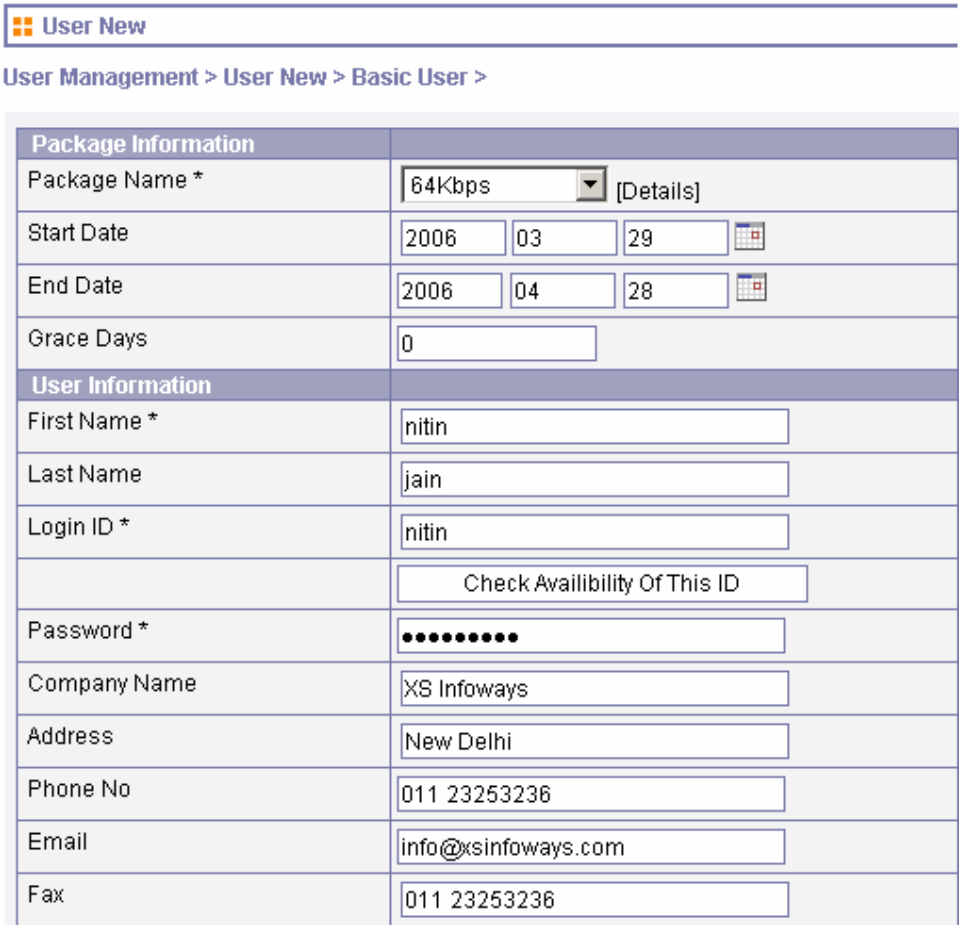




6.9.1.1 Basic User

STEP **Click on User Management in left side of main menu → click on user new icon → click on basic user icon.**

For creating new user you need to click on Basic user icon and enter the following details as



User New

User Management > User New > Basic User >

Package Information	
Package Name *	64Kbps [Details]
Start Date	2006 03 29
End Date	2006 04 28
Grace Days	0
User Information	
First Name *	nitin
Last Name	jain
Login ID *	nitin
	Check Availibility Of This ID
Password *	•••••••••
Company Name	XS Infoways
Address	New Delhi
Phone No	011 23253236
Email	info@xsinfoways.com
Fax	011 23253236

Validate User	
Authenticate User *	Yes No
Disconnect Automatically *	Yes No
Auto Disable	Yes No
IP Information	
IP Type	DHCP Static
IP Allocation Configuration*	Public IP Private IP
IP *	192.168.10.88 Get IP
Gateway *	192.168.10.19
Do you want to Authenticate by MacID?	Yes No
MAC ID	Get ID

Submit

After clicking on submit user is directed to offline users

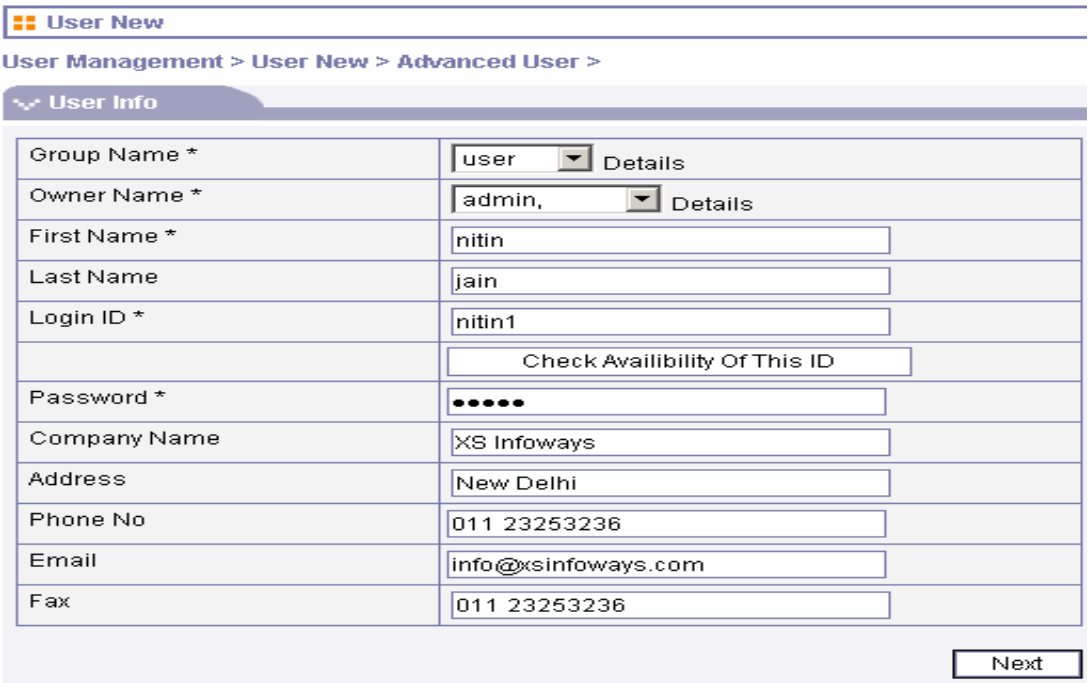
Authenticate User	Authenticate User option is used for authenticate the user with a valid username & password. For example: If select "Yes" then user has to enter Login ID & Password for Internet connection. IF "No" then user can directly connect Internet without verification of Login or Password.
Login / Password	Login ID & Password require for user authenticate.
IP	Every users on the Internet has IP Address no two machines has same IP Address. Administrator must specify IP Address to all users. This IP Address is allow you to connect with your SmartGuard server and access also Internet . Here you have an option of two types of IP **Public IP/Private IP.** Public IP is provided by your ISP for Internet connectivity. Private IP is assigned address for internal or private Network. IP address specify

	by clicking on GET IP. Its shows you available IP address. This IP Address is assigned to a user and required setting in User system which is mentioned in User panel(). IP Address must be entered. **Note:** After Clicking on GET IP Form if you do not receive any IP then insert users IP through **system > Manage User IP >Add IP**
Authenticate By MAC ID	MAC is LAN card physical address which is unique that no two cards have the same address. IP Address can be bind to MAC Address. If check box is selected, then user to which IP address is assigned cannot change his machine or network card. This restriction enhances security of users. Specify a Machine Name that can be used to identify the IP Address like name of an Area. If user change his/her LAN card then could not be able to access Internet.(Not allow to login users)
Active / Disable	Example : User Disable require for temporary because of Payment Delay or any other reason then Administrator has rights to temporary Disable the user. After receiving the payments User will be Active.
Auto disable	Is used for Automatic disable. For Example : if user package time is completed then user automatic disconnect from the server and if user again want to connect server then user should request to Administrator for renew package.

6.9.1.2Advanced User

STEP **Click on User Management in left side of main menu → click on user new icon → click on advanced user icon.**

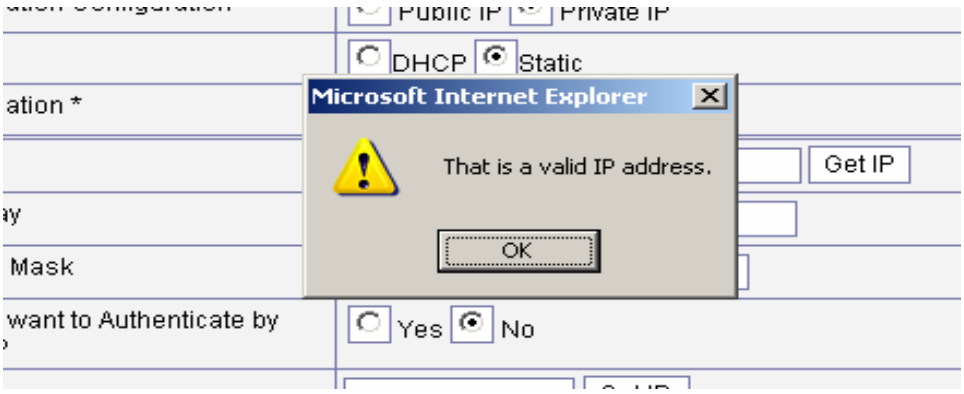
For creating new user you need to click on advanced user icon and enter the following details as



IP & Package

Server Type *	Master Server / Child Server
Package Name *	128Kb [Details]
Start Date	2006 03 31
End Date	2006 04 30
Grace Days	0
Authenticate User *	Yes / No
Disconnect Automatically *	Yes / No
Auto Disable	Yes / No
Status	Active / Disable
IP Allocation Configuration*	Public IP / Private IP
IP Type	DHCP / Static
IP Allocation *	Single / Multiple
IP *	192.168.10.200 Get IP
Gateway	192.168.20.1
Subnet Mask	255 255 255 255
Do you want to Authenticate by Mac Id?	Yes / No
Mac Id	Get ID

Next



New

Group Name *	user
Owner Name *	admin,a
First Name *	nitin
Last Name*	jain
Login ID *	nitin1
Password	nitin
Company Name	XS Infoways
Address	New Delhi
Phone No	011 23253236
Email	info@xsinfoways.com
Fax	011 23253236
Package Name *	128Kb
Status	Active
Server Type*	Child
IP Allocation Configuration*	Private
IP Allocation *	Single
No of IP's *	1
IP *	192.168.10.200
SubnetMask	255.255.255.255
Gateway	192.168.20.1
Netmask	32
IP Type	Static
Authenticate User *	Yes
Disconnect Automatically *	Yes
Do you want to Authenticate by MacID?	No
MAC ID	
Start Date	2006-03-31
End Date	2006-04-30 00:00:00
Auto Disable	No

Are you sure you want to create this User? Yes No

Authenticate User	Authenticate User option is used for authenticate the user with a valid username & password. For example: If select "Yes" then user has to enter Login ID & Password for

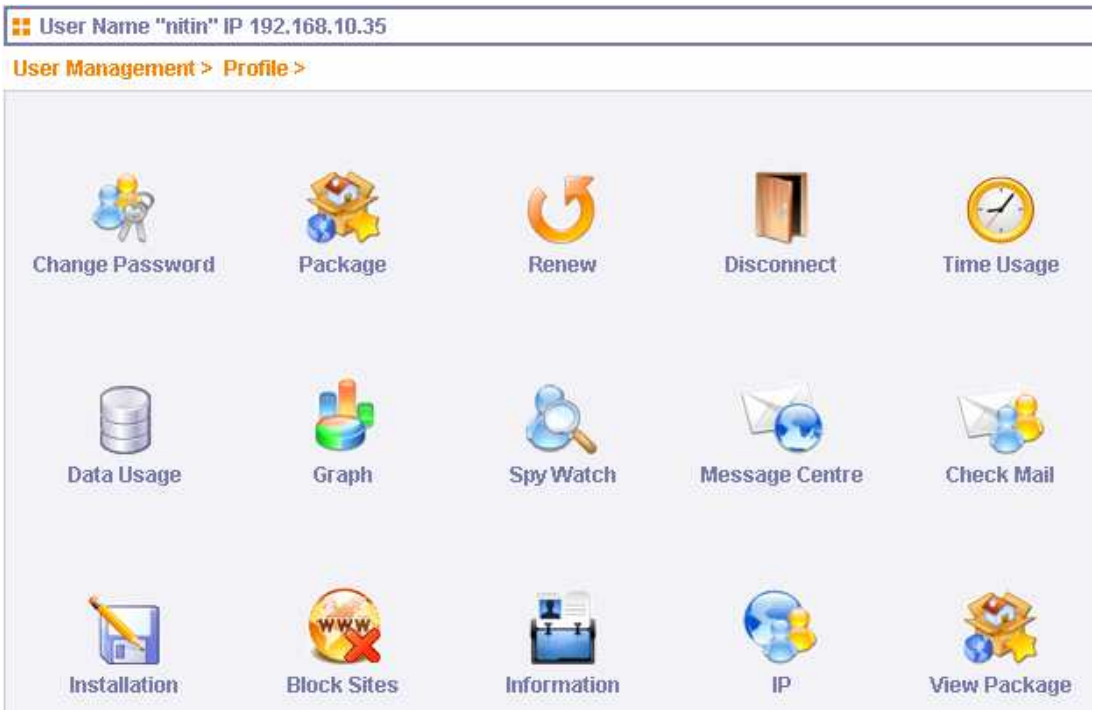
	Internet connection. IF “No” then user can directly connect Internet without verification of Login or Password.
Login / Password	Login ID & Password require for user authenticate.
IP	Every users on the Internet has IP Address no two machines has same IP Address. Administrator must specify IP Address to all users. This IP Address is allow you to connect with your SmartGuard server and access also Internet . Here you have an option of two types of IP **Public IP/Private IP.** Public IP is provided by your ISP for Internet connectivity. Private IP is assigned address for internal or private Network. IP address specify by clicking on GET IP. Its shows you available IP address. This IP Address is assigned to a user and required setting in User system which is mentioned in User panel(). IP Address must be entered. **Note:** After Clicking on GET IP Form if you do not receive any IP then insert users IP through **system > Manage User IP >Add IP**
Authenticate By MAC ID	MAC is LAN card physical address which is unique that no two cards have the same address. IP Address can be bind to MAC Address. If check box is selected, then user to which IP address is assigned cannot change his machine or network card. This restriction enhances security of users. Specify a Machine Name that can be used to identify the IP Address like name of an Area. If user change his/her LAN card then could not be able to access Internet.(Not allow to login users)
Active / Disable	Example : User Disable require for temporary

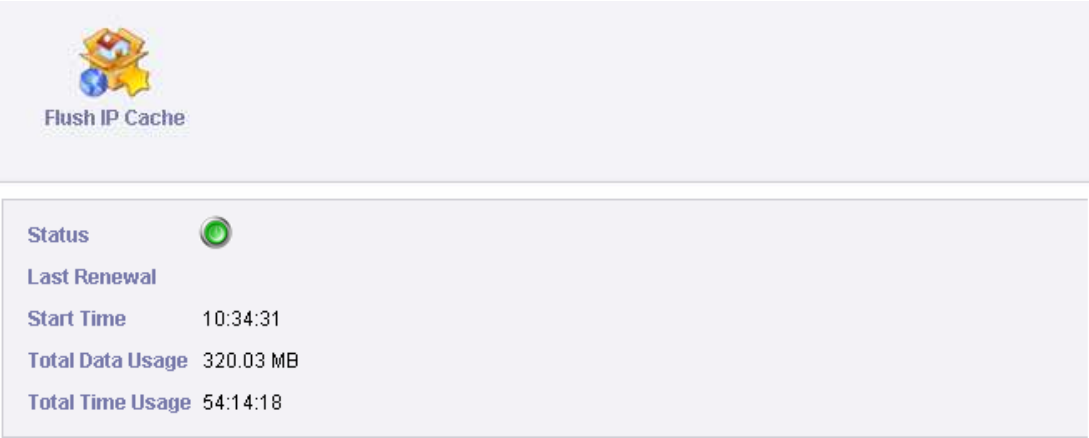
	because of Payment Delay or any other reason then Administrator has rights to temporary Disable the user. After receiving the payments User will be Active.
Auto disable	Is used for Automatic disable. For Example : if user package time is completed then user automatic disconnect from the server and if user again want to connect server then user should request to Administrator for renew package.

6.9.2 USER PROFILE

STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user.**

When you click on user name it will show you user profile as displayed below:

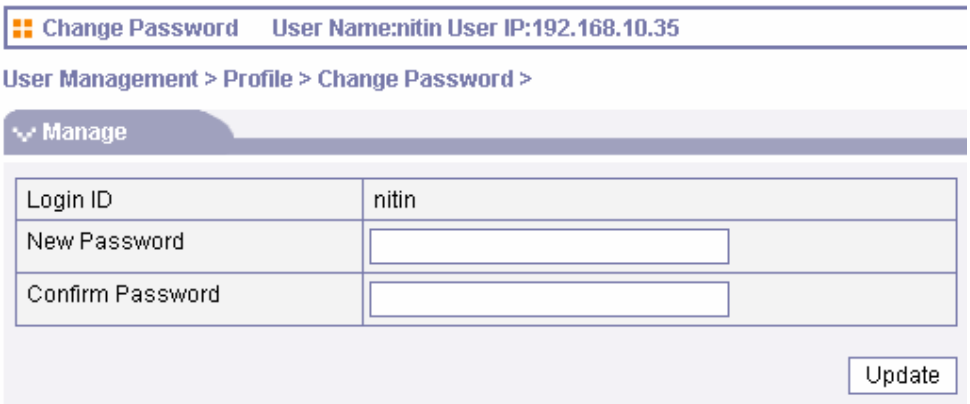




6.9.2.1 Change Password

STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select Change password icon.**

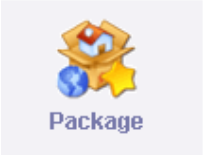
After click on change password icon following options will be displayed.



Enter the new password & conform it

Then Click on ok

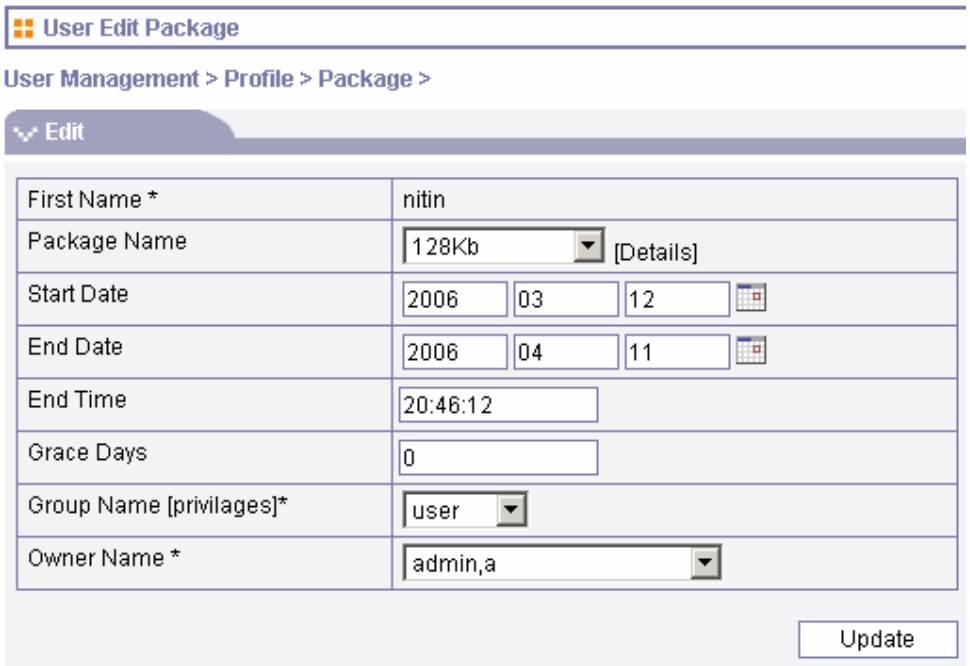
6.9.2.2 Package



STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select package icon.**

Administrator can view/modify the Package assigned, Start Date/End Date, End Time, and Group Name & Owner Name of a desired user.

After click on package icon following options will be displayed.



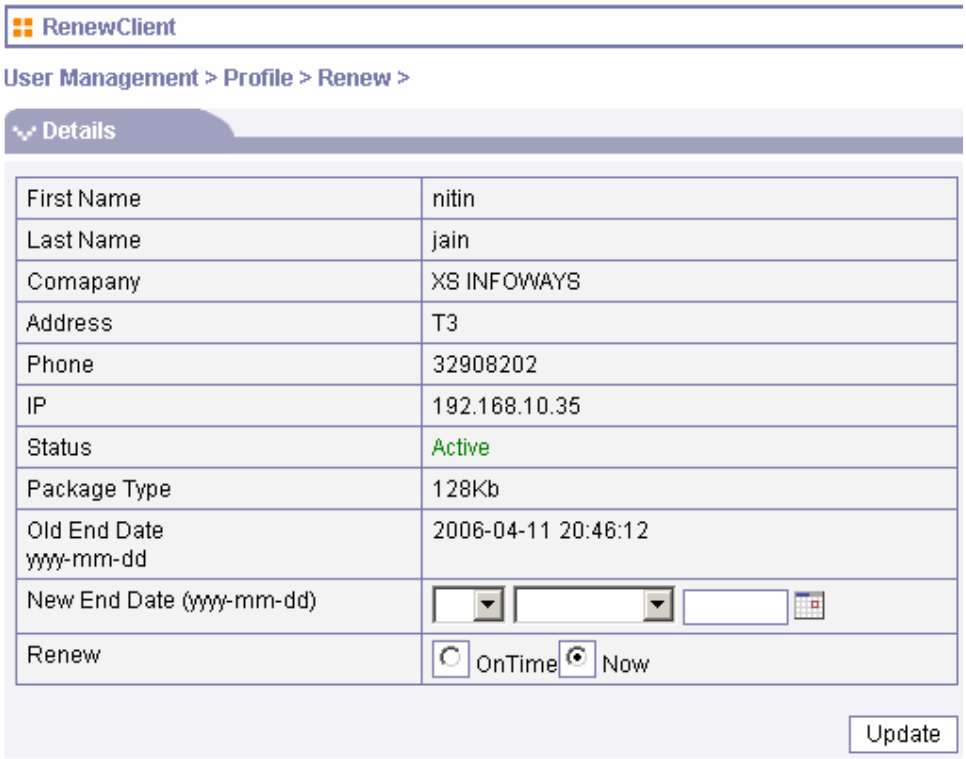
6.9.2.3 Renew User

STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select Renew icon.**

You can Renew Users from here. For Example If Users Package End Date comes. If user wants to continue the connection then renewal required.

After click on Renew icon following options will be displayed.

Here you enter new end date (Expiry Date) and Click on option On time or Now.



On Time/ Now	On Time means renew customer when renewal date comes. For example: If User paid in advance for renewal and user old package is valid. If we renew "now" then old time & days which is balance in user

	package will be zero and the user lost his/her old package usage. For that purpose you have to renew those client "Now" whose package (days& time) expired and if user package not expired then click on "On Time" which will renew user automatically when users package expire(days & time) will zero.

6.9.2.4 Disconnect

STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select Disconnect icon.**

You can disconnect all connected users or individual users.

After click on disconnect icon following message will be displayed.

When click on OK button user gets disconnected.

6.9.2.5 Time Usage

STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select time usage icon.**

You can view the Time-Usage for a particular user for a particular month by clicking on Submit Query.

User Management > Profile > Time Usage > Back

View

Select	April	2006	Submit Query

Start Date	Start Time	End Date	End Time	Total
--				0:0:0

After click on submit query button following list will be displayed.

Time Usage [nitin]

User Management > Profile > Time Usage > Back

View

Select	March	2006	Submit Query

Start Date	Start Time	End Date	End Time	Total
27-03-2006	09:58:22	2006-03-27	10:00:02	0:1:40
25-03-2006	10:09:39	2006-03-25	13:37:45	5:55:10
24-03-2006	10:22:43	2006-03-24	20:02:23	9:39:40
23-03-2006	10:27:26	2006-03-23	19:53:46	22:15:13
22-03-2006	11:42:19	2006-03-22	17:43:51	7:53:58
20-03-2006	18:41:01	2006-03-20	18:56:39	0:15:38
16-03-2006	11:25:59	2006-03-16	13:26:25	2:0:26
14-03-2006	11:27:47	2006-03-14	11:28:08	5:29:54
13-03-2006	11:35:29	2006-03-13	11:40:01	0:30:26
12-03-2006	20:47:48	2006-03-12	21:00:01	0:12:13

6.9.2.6 Data Usage

STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select data usage icon.**

The Data Usage for particular user for particular month can be viewed from **Submit Query** option.

smartguard

Data Usage [nitin Speed 128Kb/sec]

User Management > Profile > Data Usage >

View

Select	March	2006	Submit Query

On Date	Download Bandwidth	Upload Bandwidth	Total Bandwidth
	0 KBytes	0 KBytes	0 KBytes

After click on Submit Query button following list will be displayed.

Data Usage [nitin Speed 128Kb/sec]

User Management > Profile > Data Usage >

View

Select	March	2006	Submit Query

On Date	Download Bandwidth	Upload Bandwidth	Total Bandwidth
2006-03-12	83.62 KBytes	0 KBytes	83.62 KBytes
2006-03-13	1.27 MB	114.39 KBytes	1.38 MB
2006-03-14	5.45 MB	1.07 MB	6.52 MB
2006-03-16	9.2 MB	6.7 KBytes	9.21 MB
2006-03-20	5.12 MB	135.43 KBytes	5.26 MB
2006-03-22	17.66 MB	1.85 MB	19.5 MB
2006-03-23	115.71 MB	1.37 MB	117.08 MB
2006-03-24	18.95 MB	1.09 MB	20.04 MB
2006-03-25	56.58 MB	2.13 MB	58.71 MB
2006-03-27	51.71 MB	17.45 MB	69.16 MB
2006-03-28	24.81 MB	2.2 MB	27.01 MB

6.9.2.7 Graph

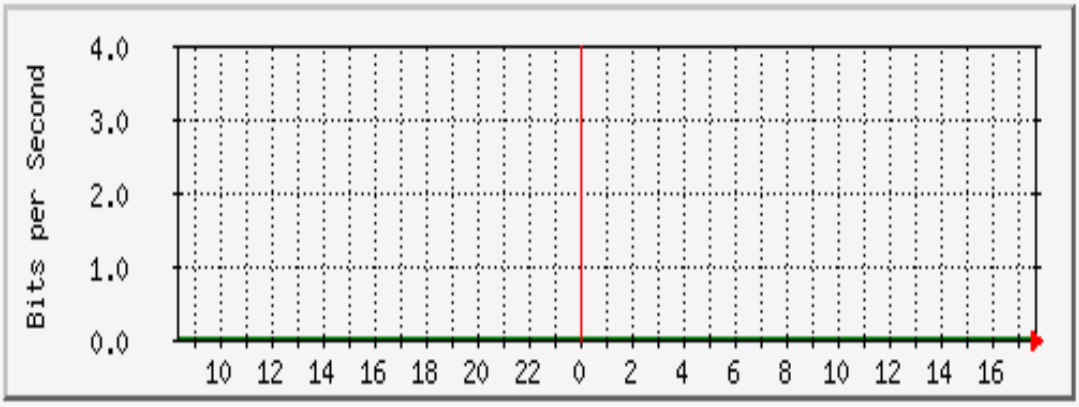
STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select Graph icon.**

The Upload/Download live Bandwidth Graph of Single User (192.168.10.35) is displayed here:

smartguard

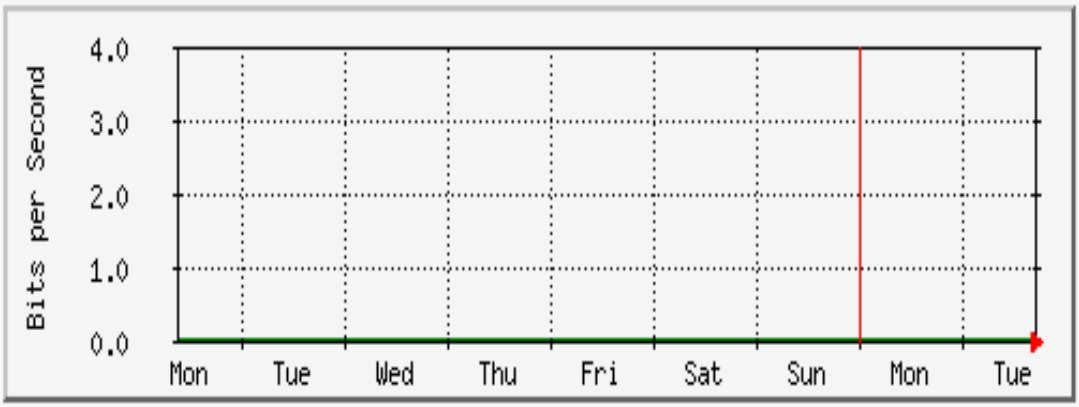
The statistics were last updated **Tuesday, 4 April 2006 at 17:40**,
at which time **'unknown'** had been up for **unknown**.

`Daily' Graph (5 Minute Average)

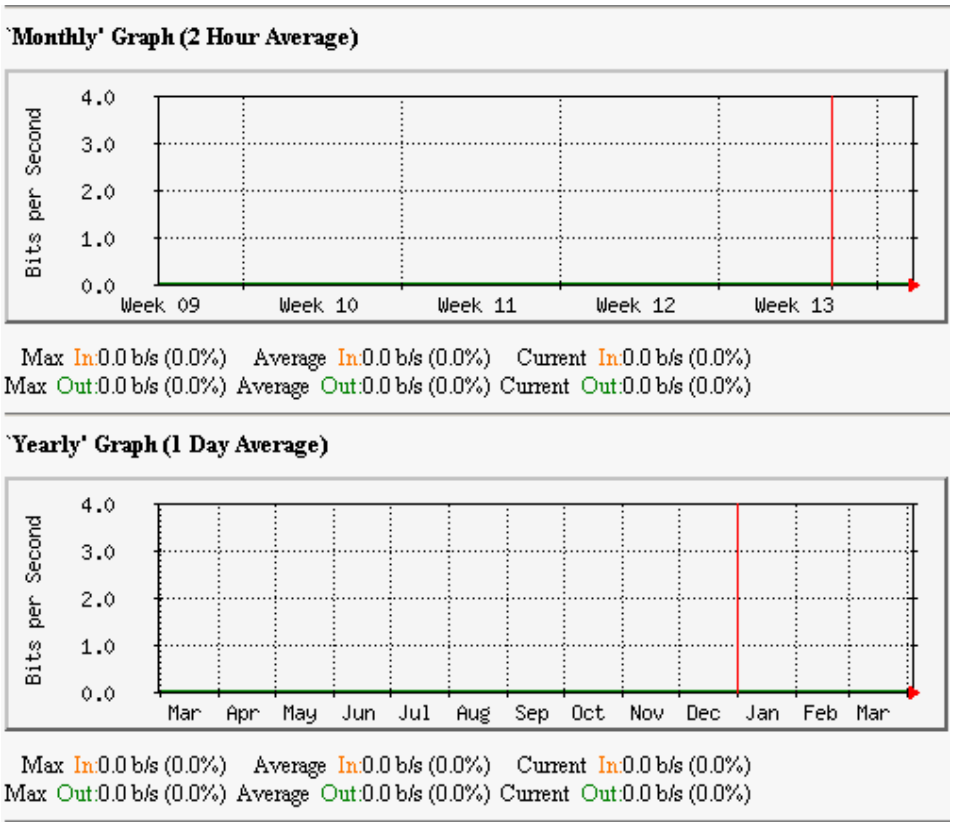


Max In:0.0 b/s (0.0%) Average In:0.0 b/s (0.0%) Current In:0.0 b/s (0.0%)
Max Out:0.0 b/s (0.0%) Average Out:0.0 b/s (0.0%) Current Out:0.0 b/s (0.0%)

`Weekly' Graph (30 Minute Average)



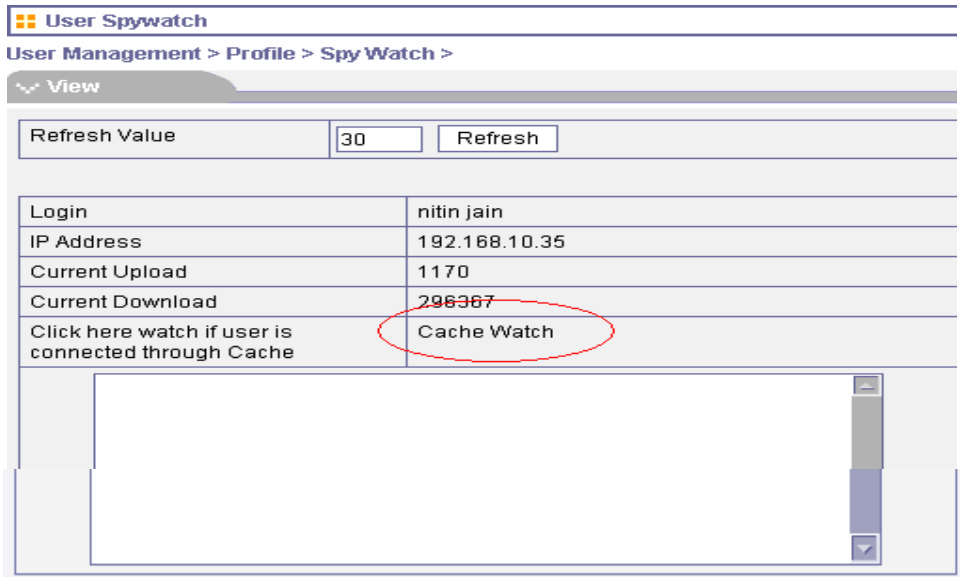
Max In:0.0 b/s (0.0%) Average In:0.0 b/s (0.0%) Current In:0.0 b/s (0.0%)
Max Out:0.0 b/s (0.0%) Average Out:0.0 b/s (0.0%) Current Out:0.0 b/s (0.0%)



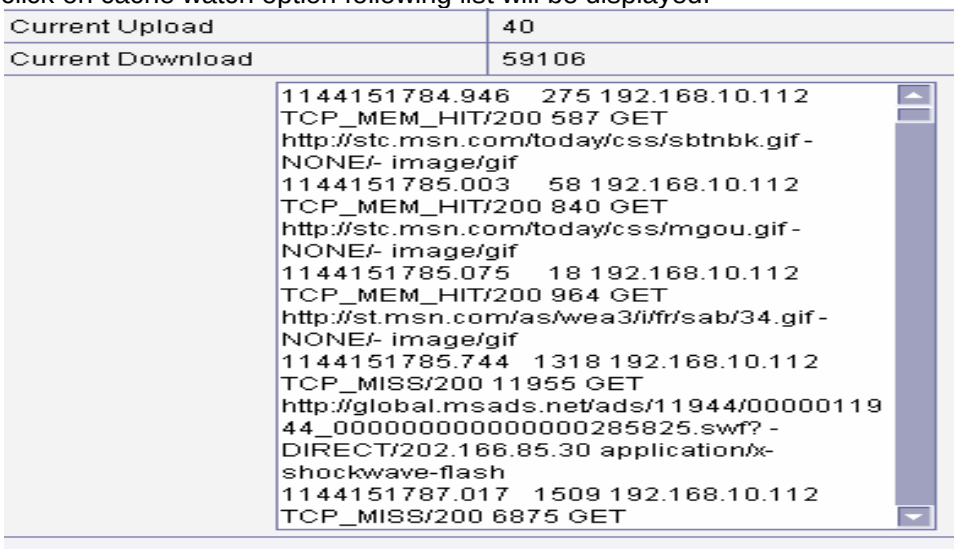
6.9.2.8 Spy Watch

STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select Spy watch icon.**

SmartGuard has facility of Watch the all connected users or individual users. You can watch user's actions. Users where connected in Internet, where browsing or more.



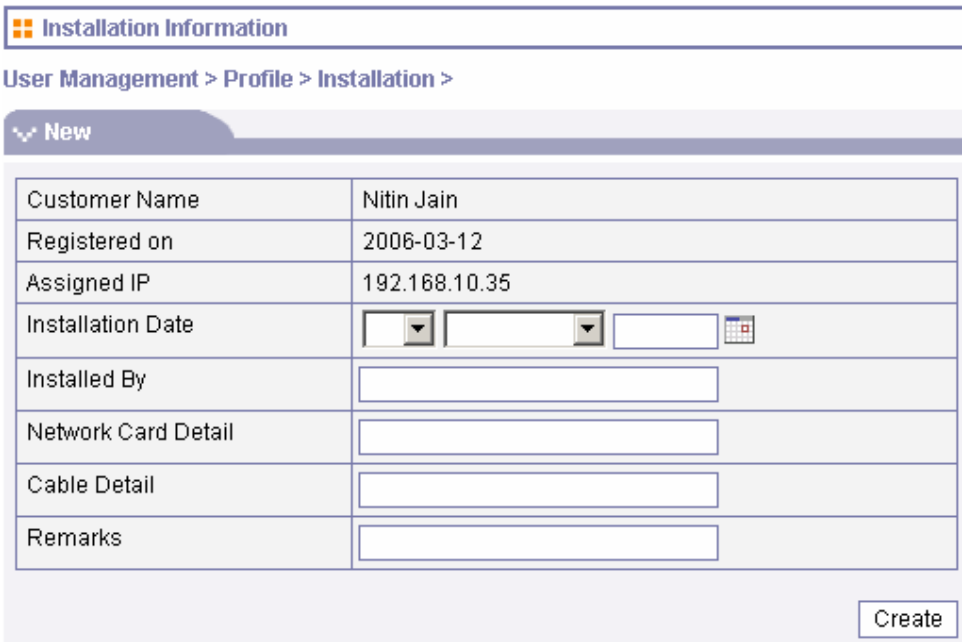
After click on cache watch option following list will be displayed.



6.9.2.9 Installation

STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select installation icon.**

The Installation information can be checked / modified for a user from here.



6.9.2.10 Information

STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select Information icon.**

The users Personal Information can be Viewed/Modified from here. When you click on information icon following list will be displayed.

User Edit

User Management > Profile > Information >

Edit

First Name *	nitin
Last Name *	jain
Company Name	XS INFOWAYS
Address	T3
Phone No	32908202
Email	nitin@xsinfoways.com
Fax	

Update

6.9.2.11 IP

STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select IP icon.**

The IP details of user can be Viewed/Modified from this option. When you click on IP option following options will be displayed.

Edit

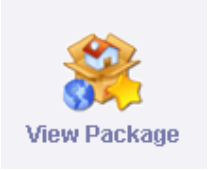
Status	Active Disable
IP Allocation Configuration*	Public IP Private IP
IP Type	DHCP Static
IP Allocation *	Single Multiple
No of IP 's	1
IP *	192.168.10.35 Get IP
Gateway	192.168.10.9
Subnet Mask	255 255 255 255
Netmask	32
Authenticate User *	Yes No
Disconnect Automatically *	Yes No
Do you want to Authenticate by MacID?	Yes No
MAC ID	0 Get ID
Auto Disable	Yes No

Update

Edit User Name:nitin User IP:192.168.10.35User IP configuration

User Management > Profile > IP >

6.9.2.12 View Package



STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select View package icon.**

The Package details for a user can be viewed from here. After click on view package icon following options will be displayed.

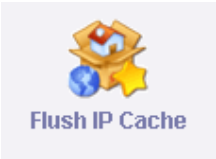
View Package

User Management > Profile > View Package >

View

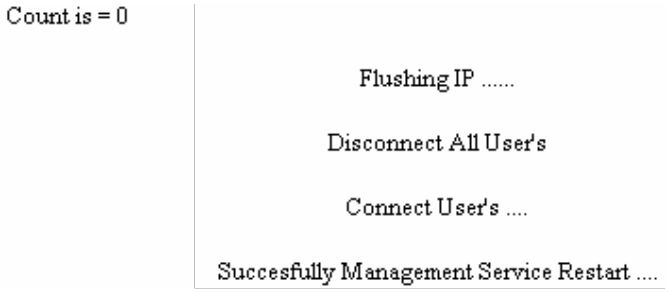
First Name *	nitin
Package Name	128Kb [Details]
Start Date	2006-03-12
End Date	2006-04-11 20:46:12
Group Name	user
Authenticate User	Yes
Disconnect Automatically	No
Auto Disable	Yes
Status	Yes
Disable Reason	

6.9.2.13 Flush IP Cache



STEP **Click on User Management in left side of main menu → click on user new icon → click on all users icon → then select first name of user → now select Flush IP cache icon.**

The Caching of Users IP is flushed from here.



6.9.3 VIEW ALL USERS

STEP **Click on User Management in left side of main menu → click on all users icon.**

When you click on all user icons following users list will be displayed.

smartguard

All User Show

User Management > All Users >

Total Users : 14 Online Users :11 Offline Users 3

Manage

Search | User IP | Search

Page 1

Status	First Name	Last Name	Login Id	IP	Download Speed(KBps)	Upload Speed (KBps)	Disconnect	Delete
	Admin	Don't Delet These Users	admin	10.0.0.3	0.0	0.0		
	Nitin	Jain	nitin	192.168.10.35	0.0	0.0		
	Nishant	Dubey	nishant	192.168.10.37	0.0	0.0		
	Deepak	Kumar	deepak	192.168.10.50	0.0	0.0		
	Manish	Kumar	manish	192.168.10.80	0.0	0.0		
	Yogender	Kumar	yogender	192.168.10.81	0.0	0.0		
	Rahul	Goel	rahul	192.168.10.88	0.0	0.0		
	Akshay	Chaudhary	akshay	192.168.10.101	0.0	0.0		
	Arun	Kumar	arun	192.168.10.111	0.0	0.0		
	Rajiv	Sharma	rajiv	192.168.10.112	0.0	0.0		
	Vipin	Sharma	vipin	192.168.10.120	0.0	0.0		

Delete

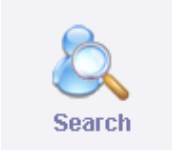
You can click on “Offline Users” or “Online Users” to see the details also.

It’s an online user

It’s an offline user

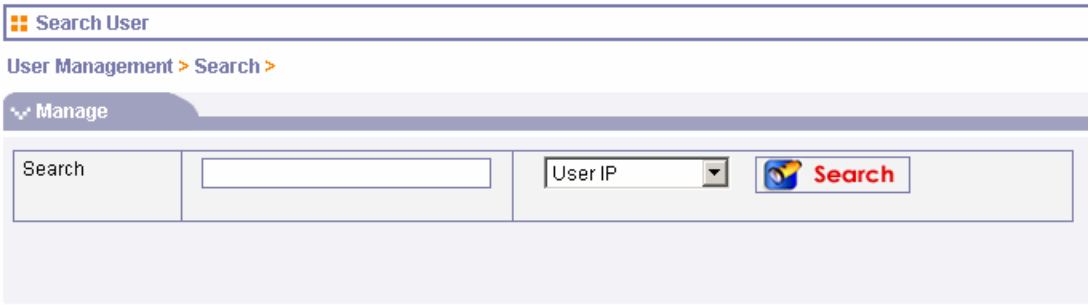
If you will click on this button the user will be disconnected.

6.9.4 SEARCH

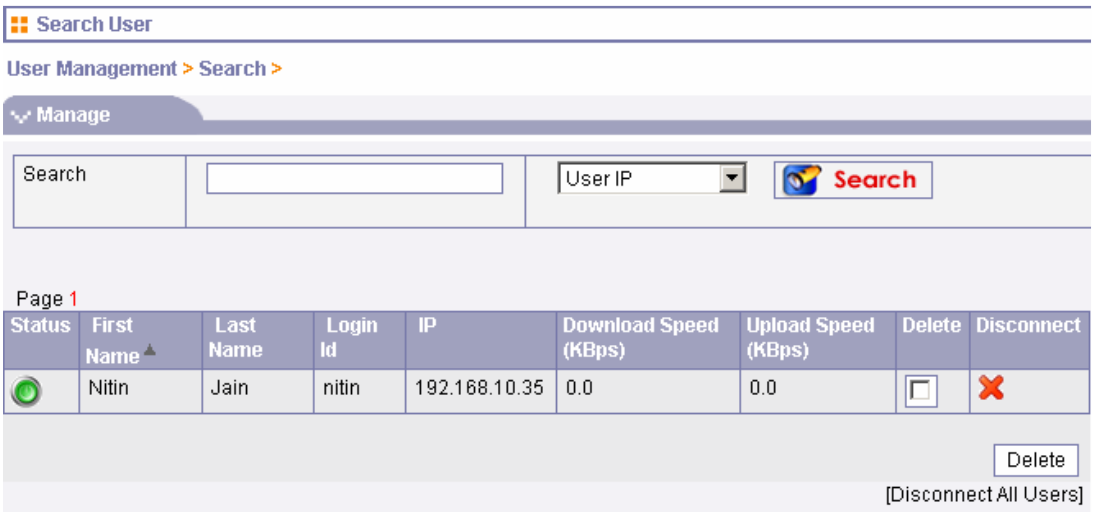


STEP **Click on User Management in left side of main menu → click on Search icon.**

User Management has an option of Search. Where you can search by User Name, Customer First Name, Last Name, Company Name, Mac ID, IP Address. When you click on search option following search window will be displayed.



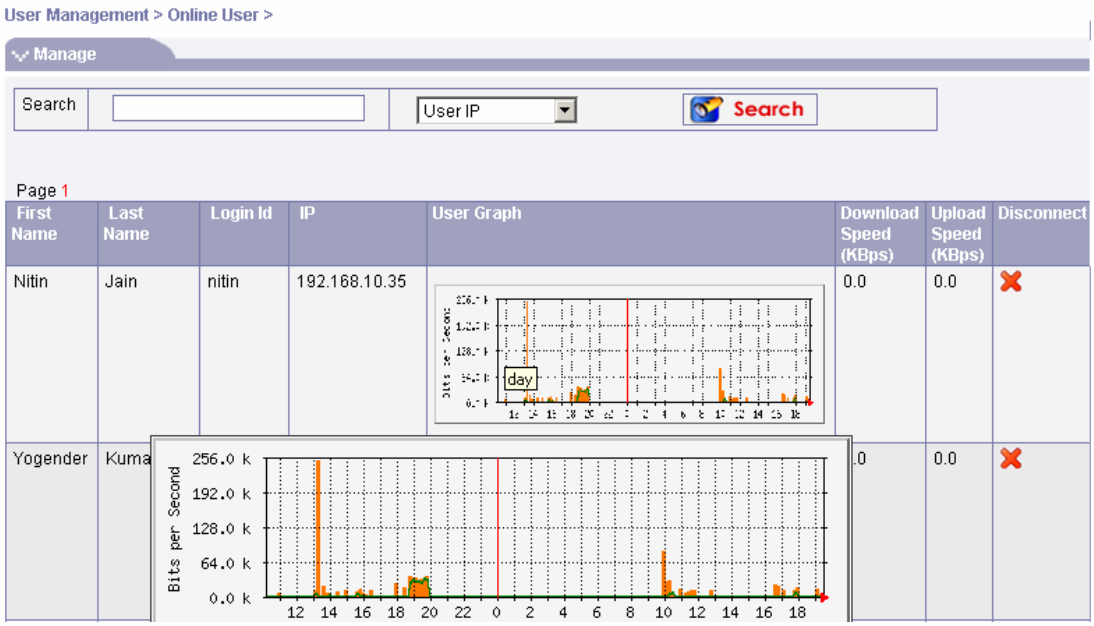
Type ip address of user and select user ip option after fill entries click on search button. When you click on search button following list will be displayed.



6.9.5 ONLINE USER

STEP **Click on User Management in left side of main menu → click on Online user icon.**

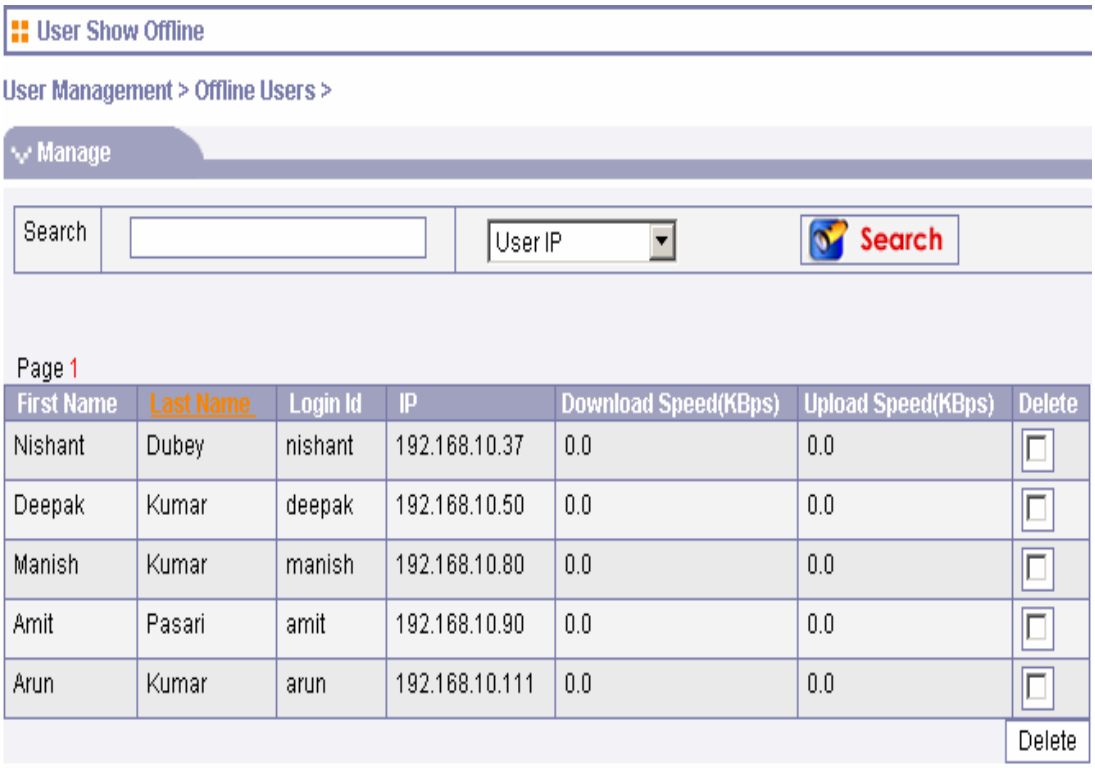
From this menu you can view the users who are currently online on server.
From here you can also search for the desired user by mentioning any of his detail.



6.9.6 OFFLINE USERS

STEP **Click on User Management in left side of main menu → click on offline users icon.**

From this menu you can view the users who are currently offline on server.



First Name	Last Name	Login Id	IP	Download Speed(KBps)	Upload Speed(KBps)	Delete
Nishant	Dubey	nishant	192.168.10.37	0.0	0.0	
Deepak	Kumar	deepak	192.168.10.50	0.0	0.0	
Manish	Kumar	manish	192.168.10.80	0.0	0.0	
Amit	Pasari	amit	192.168.10.90	0.0	0.0	
Arun	Kumar	arun	192.168.10.111	0.0	0.0	

Delete

smartguard

Chapter 8

DHCP Server

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

8.DHCP Server

Dynamic Host Control Protocol (DHCP) enables you to automatically assign reusable IP addresses to DHCP clients. The Cisco IOS DHCP Server feature is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the router to DHCP clients. If the Cisco IOS DHCP Server cannot satisfy a DHCP request from its own database, it can forward the request to one or more secondary DHCP servers defined by the network administrator.

1. **What Is DHCP?**

   DHCP (Dynamic Host Configuration Protocol) is a protocol that lets network administrators manage centrally and automate the assignment of IP (Internet Protocol) configurations on a computer network. When using the Internet's set of protocols (TCP/IP), in order for a computer system to communicate to another computer system it needs a unique IP address. Without DHCP, the IP address must be entered manually at each computer system. DHCP lets a network administrator supervise and distribute IP addresses from a central point. The purpose of DHCP is to provide the automatic (dynamic) allocation of IP client configurations for a specific time period (called a lease period) and to eliminate the work necessary to administer a large IP network.

2. **Who Created DHCP?**

   DHCP was created by the Dynamic Host Configuration Working Group of the Internet Engineering Task Force (IETF: a volunteer organization which defines protocols for use on the Internet). As such, its definition is recorded in an Internet RFC (standard) and the Internet Activities Board (IAB) is asserting its status as to Internet Standardization.

3. **Why Is DHCP Important?**

   When connected to a network, every computer must be assigned a unique address. However, when adding a machine to a network, the assignment and configuration of network (IP) addresses has required human action. The computer user had to request an address, and then the administrator would manually configure the machine. Mistakes in the configuration process are easy for novices to make, and can cause difficulties for both the administrator making the error as well as neighbors on the network. Also, when mobile computer users travel between sites, they have had to relive this process for each different site from which they connected to a network. In order to simplify the process of adding machines to a network and assigning unique IP addresses manually, there is a need to automate the task.

   The introduction of DHCP alleviated the problems associated with manually assigning TCP/IP client addresses. Network administrators have quickly appreciated the importance, flexibility and ease-of-use offered in DHCP.

4. **How Does DHCP Work?**

When a client needs to start up TCP/IP operations, it broadcasts a request for address information. The DHCP server receives the request, assigns a new address for a specific time period (called a lease period) and sends it to the client together with the other required configuration information. This information is acknowledged by the client, and used to set up its configuration. The DHCP server will not reallocate the address during the lease period and will attempt to return the same address every time the client requests an address. The client may extend its lease with subsequent requests, and may send a message to the server before the lease expires telling it that it no longer needs the address so it can be released and assigned to another client on the network.

5. **What Advantages Does DHCP Have Over Manual Configuration Methods?**

The use of DHCP is highly recommended and there are a number of obvious reasons why you should use it. As mentioned before, there are two ways you can configure client addresses on a computer network, either manually or automatically. Manual configuration requires the careful input of a unique IP address, subnet mask, default router address and a Domain Name Server address. In an ideal world, manually assigning client addresses should be relatively straight forward and error free. Unfortunately, we do not live in an ideal world; computers are frequently moved and new systems get added to a network. Also if a major network resource, such as a router (which interconnects networks) changes network addresses, this could mean changing EVERY system's configuration. For a network administrator this process can be time consuming, tedious and error prone. Problems can occur when manually setting up your client machines, so if you have the option to set-up your client machines automatically, please do, as it will save you time and a lot of headaches.

DHCP has several major advantages over manual configurations. Each computer gets its configuration from a "pool" of available numbers automatically for a specific time period (called a leasing period), meaning no wasted numbers. When a computer has finished with the address, it is released for another computer to use. Configuration information can be administered from a single point. Major network resource changes (e.g. a router changing address), requires only the DHCP server be updated with the new information, rather than every system.

6. **Can DHCP Provide Support For Mobile Users?**

Yes. The benefits of dynamic addressing are especially helpful in mobile computing environments where users frequently change locations. Mobile users simply plug-in their laptop to the network, and receive their required configuration automatically. When moving to a different network using a DHCP server, then the configuration will be supplied by that network's server. No manual reconfiguration is required at all.

7. **Are DHCP Servers Easy To Set-up And Administer?**

DHCP Servers offer completely centralized management of all TCP/IP client configurations, including IP address, gateway address and DNS address. DHCP servers are easy to administer and can be set-up in just a few minutes. Client addresses are assigned automatically unlike static set-up which requires the manual input of client addresses which can be a time consuming and tedious task.

8. **Are There Any Limitations That I Should Be Aware Of?**

Some machines on your network need to be at fixed addresses, for example servers and routers. The DHCP server you choose should be capable of assigning pre-allocated addresses to these specific machines.

You need to be able to assign a machine to run the DHCP server continually as it must be available at all times when clients need IP access.

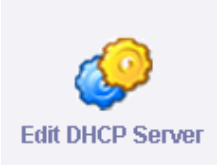
To avoid conflicts between addresses assigned by the DHCP server and those assigned manually, users should be discouraged, or preferably prevented, from reconfiguring their own IP addresses.

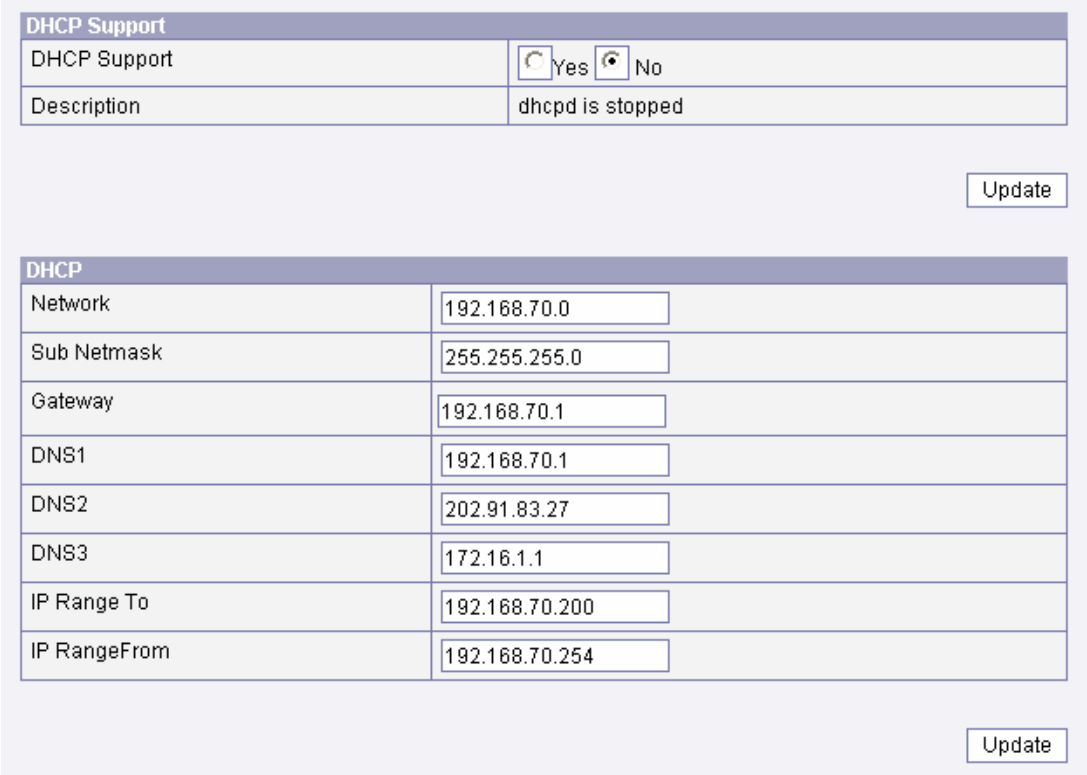
Some older operating systems do not support DHCP. If you have such systems you may be able to upgrade them. If this is not possible they may support the older BOOTP protocol, and a DHCP server can be chosen that will support this option.

For peace of mind, it is a good idea to decide what is important to you, which of the available DHCP servers is best suited to meet your specific requirements and always get a second opinion.

8.3 DHCP SERVER

8.3.1 Edit DHCP Server



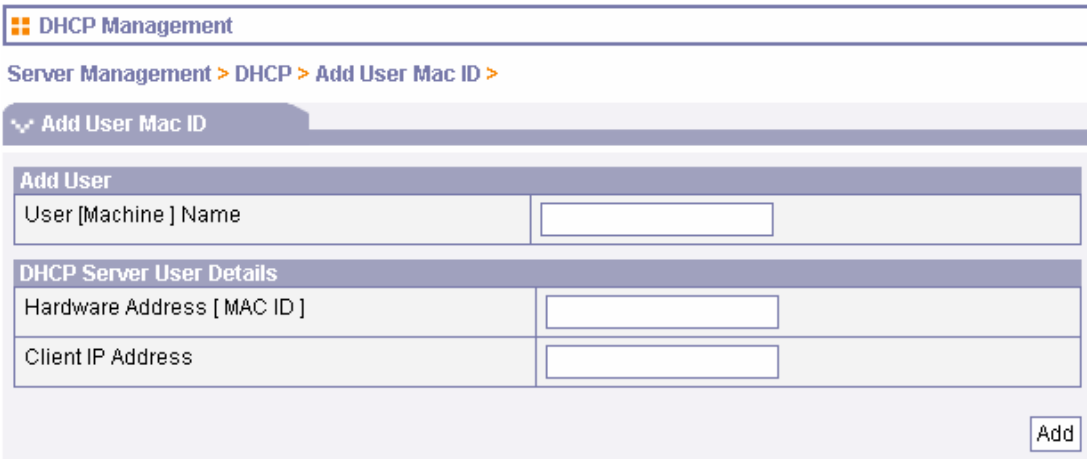


The DHCP server support can be disabled / enabled from this window.

Administrator just needs to define the IP range for DHCP Server and the other required network information in the respective fields.
By clicking on

8.3.2 Add User Mac ID

Update every entry done will be configured.



smartguard

Chapter 9

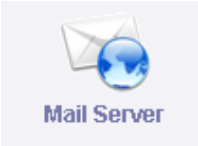
Mail Server

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

9.Mail Server

9.1 MAIL SERVER



Smart Guard – MailServer

E-mail is generally considered the most important service provided by the Internet, which makes servers that move and store mail a crucial piece of software.

SmartGuard has build in Mail server with POP3 & IMAP for incoming and SMTP for outgoing mail. It also provides webmail service just like hotmail for the users. SmartGuard's Mail Server is a versatile mail server capable of sending and receiving Internet e-mail on behalf of your users. Rather than each user sending and receiving e-mail directly to and from other ISPs.

Features Of SmartGuard Mail Servers are given below :
Linux Base Mail Server
Web mail
POP3 / IMAP
Unlimited Mail boxes
Anti-Spam
Anti-Virus
Mail Forwarding
Mail Auto responder

1. What is Email?

Electronic mail (email) is the term given to an electronic message, usually a form of simple text message, that a user types at a computer system and is transmitted over some form of computer network to another user, who can read it.

Email once consisted of a number of proprietary email systems. Originally these email systems could only send and receive email in an office where every person was equipped with the same software. With the expansion of the Internet, some manufacturers of these proprietary email systems introduced the capability of connecting to the Internet for the transfer of messages outside of the local network. This can take the form of a software interface that converts the local messages into a recognized standard form suitable for transfer over the Internet. These systems are more common in establishments that have used email for longer than most, and are renowned for minor problems with access to global

Internet email, (e.g. problems with sending or receiving attachments) however such problems are slowly disappearing.

Since the Internet has grown in popularity, proprietary systems have become less popular, with more businesses moving over to Internet standards for local network mail services. This has the advantages of usually being less expensive, simpler, no longer being tied to a particular vendor and allows the IT Manager to have a wider choice of email client applications, or different hardware platforms.

2. What are the benefits of Email?

Email has become one of the driving forces behind connecting businesses to the Internet. It offers fast, economical transfer of messages anywhere in the world. As local telephone calls are free in most parts of the US, messages destined to long-distance destinations become effectively free to send. Outside of the US, local calls tend to be chargeable, therefore the email system can reduce the telephone bill considerably.

The substantial cost-cutting associated with these facts have encouraged many businesses to invest in an implementation of email services.

Email has considerable benefits over traditional paper based memo's and postal systems:

Messages can be sent at any time across the world as easily as across the office, to a group of people or a single recipient, without the sender leaving their desk. Messages can be logged, ensuring some form of record is held, and messages are stored when the recipient is away from their desk.

The recipient can collect their mail when they want, from wherever they are. Mobile users can collect their mail whilst out visiting customers, or at other locations.

The person you are sending the message to gets it directly, without passing through any third party.

Environmentally friendly! Unless requested, email messages require no paper or resources other than storage space on a computer disk drive.

3. What is an email client?

An email client is an application that is used to read, write and send email. In simple terms it is the user interface to the email system.

The client usually consists of a combination of a simple text editor, address book, filing cabinet and communications module.

The text editor allows for the creation of the message itself, and usually includes simple spell checking and formatting facilities.

The ability to allow files or documents to be attached to the message is also available. For example a diagram or schematic could be attached to an email message, offering the recipient the chance to see a project's progress, and comment on it with a reply.

The address book allows the users to store commonly used email addresses in an easy to get at format, reducing the chance of addressing errors.

The filing cabinet allows for the storage of email messages, both sent and received, and usually gives some form of search function, allowing the easy retrieval of a desired message.

The final, but most important, section of the email client is the element that deals with the actual communication of email messages to and from an email server. How this actually occurs will be described later in this FAQ.

4. What is a mail server?

A mail server is an application that receives email from email clients or other mail servers. It is the workhorse of the email system.

A mail server usually consists of a storage area, a set of user definable rules, a list of users and a series of communication modules.

The storage area is where mail is stored for local users, and where messages that are in transit to another destination are temporarily stored. It usually takes the form of a simple database of information.

The user defined rules determine how the mail server should react when determining the destination of a specific message, or possibly react to the sender of the message. For example: specific email addresses can be barred, or certain users can be restricted to only sending messages within the company.

The list of users is a database of user accounts that the mail server recognizes and will deal with locally.

The communications modules are the components that actually handle the transfer of messages to and from other mail servers and email clients. Depending upon the requirements of the mail server there may be a number of different modules installed for use. What these modules do and how they communicate will be dealt with later in this FAQ.

A person, sometimes called a Postmaster, maintains the mail server and the list of user accounts that it supports.

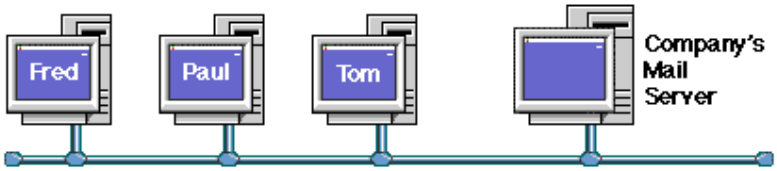
Most mail servers are designed to operate without any manual intervention during normal operation. They wait for a message to be sent to them and process it accordingly, or collect messages from other mail servers at predetermined intervals.

5. Email Basics - Overview of Email Services

The following examples will start with a fictional computer network, and will lead through the basics of how email functions, and it's relevance to the Internet. An example email system to illustrate the basics could be as follows:

a. **Simple office email system**

Email is required within a company, but not out to the rest of the world. A very simple email system could be installed and maintained, giving interoffice communications:

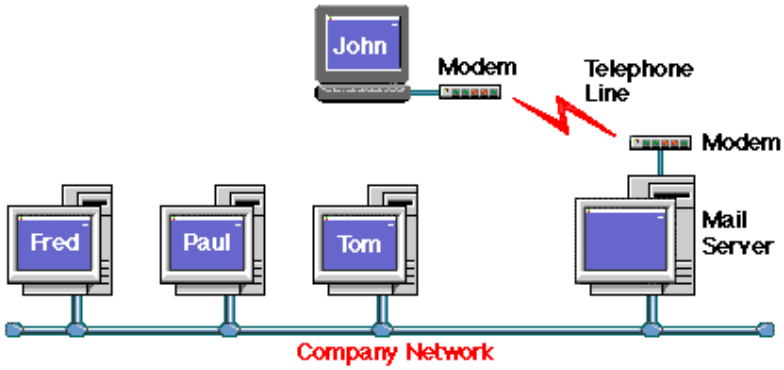


In the above example, the three workstations are connected to a computer network within a company office. If one user wishes to send email to another user, then the message is simply typed and sent to the mail server, addressed to the recipient using their email name, which would simply be the first name of a user, such as "Tom".

For example: if Fred wants to send a message to Tom, he types his message on his email client, addressing it to Tom. His email client then sends the message to the mail server, where it is stored for Tom. When Tom next checks to see if there is any mail for him, his email client will collect his messages and allow him to read them. Because this email system works only within the office, each recipient can be referred to using only their email name.

This system could easily be expanded to allow for remote users if some form of dial in support is added to the network using a modem (A modem is a device that sends computer signals down a telephone line, effectively making a telephone system a part of a computer network). This would increase the flexibility of the system enormously.

b. **Remote user with access to office email**

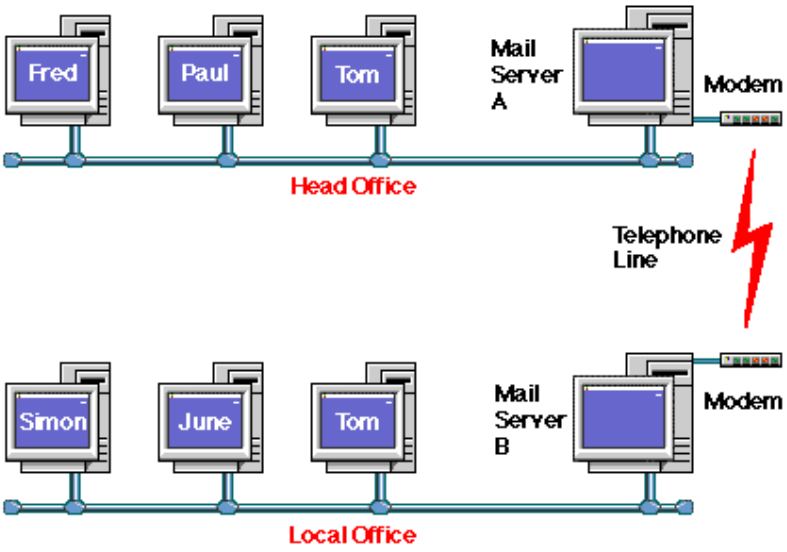


When John wants to send email to Paul, he types his message within his email client, then, when he wants it to, his email client dials into his company computer network using a modem and telephone line, sends his message to Paul, then collects any waiting messages for him. Once the messages have been collected, the modem disconnects from the phone line, and John can read any messages that were collected.

Because John's computer connected using the telephone lines, he can collect his mail from anywhere he can plug his modem into a telephone socket. If the company also had another remote user who also connected through the telephone network, then messages could also be transferred to them as easily as to one of the workstations in the office. The advantages and flexibility of an email system starts to become clearer when compared against traditional memo and telephone systems.

The next step is to allow email messages to be able to be sent to another office or company.

c. **Simple email between two offices**



This diagram shows a simple email system to give internal email between two offices, which are connected via a telephone line.

Mail is sent internally within an office using the same methods as discussed earlier, but as there are two separate sites, this adds an additional complication in addressing the recipient. As can be seen in the above diagram, there are two Toms available to send email to. How can you specify the correct Tom to send your message to? There are two ways:

1. Change Tom's email name to be something else. This usually is implemented by using the users second name or initial, such as "S" of the second name "Smith", so the second Tom's email name would be "Tom.S" (there is no actual standard way of implementing email names, other than trying to keep them short and easy to remember).

2. Refer to users at a separate office or site with an additional piece of information which defines their location, such as "local office." So to send mail to Tom at the Local Office, you would address his messages to "Tom@local.office". Notice the "@" symbol which is read as "at" and that there are no spaces allowed within an email name or address.

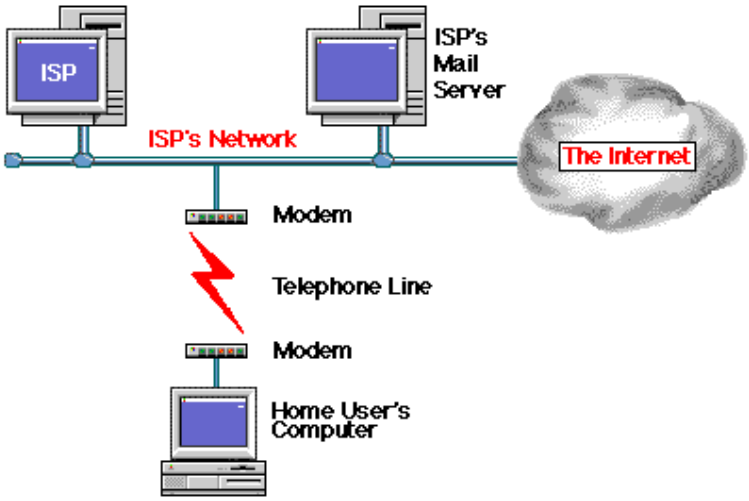
The second method is the preferred option as it allows for future expansion of the system, especially if there is the potential for a number of local offices. These

could be referred to as "Local.Office.A" "Local.Office.B" or possibly by location, such as "New.York.Office" and so forth. These addresses are known as "Domains" and simply give the location of the user who the message is destined for within the company. (Note that these are not "Internet Domains", but internal company ones).

Note that the telephone line would only be used intermittently, when mail was destined for the other office, and could also be used for remote users as well. Using a combination of the discussed options so far, it can be seen that a comprehensive company email system can be assembled without too many problems.

The options discussed so far only allow for internal email with a company or organisation. The next example is to allow for email access to the global Internet.

d. **A single user dialling into an Internet Service Provider (ISP)**



When a single user dials into the Internet via an Internet Service Provider (ISP) they are effectively dialling into the ISP's network in the same way as in the earlier example
Remote user with access to office email.

The only major difference is that the ISP's computer network is itself connected to the Internet, and may have a large number of modems to support their users.

The home users email is stored at the ISP's mail server in exactly the same way as within the simple company email system introduced above. The home user can connect to the ISP's network, send their messages and collect their waiting email, then disconnect.

The only complexity added is for the actual addressing of the Home user, and the recipients of the messages that the home user wants to send. Due to the Internet actually consisting of a large number of smaller networks, much like the ones shown in
Simple email between two offices, an email address needs to be specific in

defining the recipients Domain. Can you imagine how many "Toms" exist on the Internet!

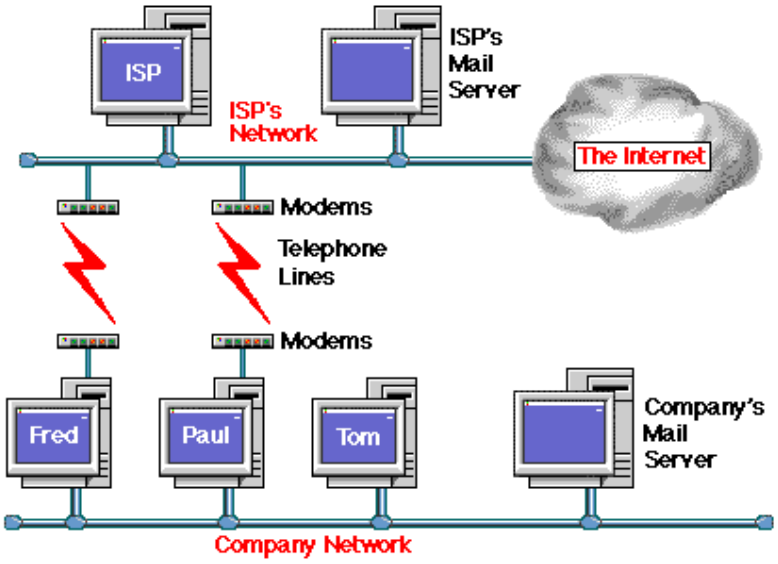
This brings us back to the subject of "Domains".

Each network connected to the Internet has a Domain name associated with it, to ensure email --and other traffic-- gets directed to the right recipient. In the above diagram the ISP would have their own domain name, which points any email destined for a user in their domain to their mail server.

So, for example, if the ISP is called "Provider" and the domain that they own on the Internet could be called "provider.com" (We'll go into more details on the domain name later in this FAQ) then all email to the home user is directed to "home.user@provider.com" which will result in the mail being stored on the ISP's mail server, ready to collect by the home user email client.

A single office user could also use the same system to collect and send mail using an ISP, but this would not have any direct relationship, or link, to the internal email systems that have already been discussed.

e. **A number of users on a network dialling in to an ISP**



In this example Fred and Paul have two email addresses: One for internal mail within a company, and one for Internet email. This can sometimes occur if most of the email that a user reads or sends is internal within a company network, yet the user wants access to global Internet email. Each user would have an email account on both the company mail server and the ISP's mail server.

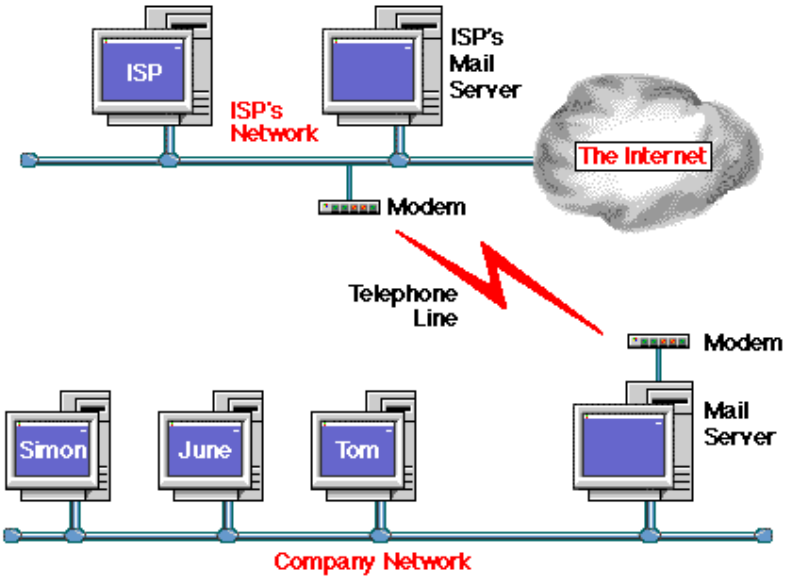
An Internet email user can contact Fred and Paul using email directly. However if an Internet user wanted to send a message to Tom, then they could not without having to send it to either Fred or Paul and asking them to forward the message.

This arrangement allows for company email within the confines of the office network, but gives Internet email facilities to users who need them, in this case Fred and Paul. If Tom wanted to send email to an Internet address, rather than within the confines of the company, then he would have to ask either Fred or Paul to send it on his behalf.

Note that there may not actually be individual modems for all users, but some form of modem sharing may occur.

If there were more than two Internet email users, then connecting the office network mail server --rather than individual machines--to the Internet would probably be more efficient and flexible. Tom would then have been able to send his email message to another company himself, rather than asking another user to do it for him.

f. **A company network connected to an ISP**



In this example the company network is connected to the ISP's network by modem.

This adds the additional complication that the email addresses within the company network must be of a form that other users on the Internet can use. As the company network is connected to the Internet through an ISP, then the company could use the "Internet Domain" of the ISP for addressing their own email -- which means that each user could be addressed in the form "user@company.provider.com" (note that this is one possible method of addressing: each service provider may have their own way of addressing individual companies) or they could register their own Internet Domain. This would mean that a user is addressed as "user@company.com" where "company.com" is the Internet domain registered.

When Fred, Paul or Tom want to send email to a recipient on the Internet, they send the message in the same way as sending it internally within the office, but also must specify the "Domain" of the person they are trying to contact within the email address.

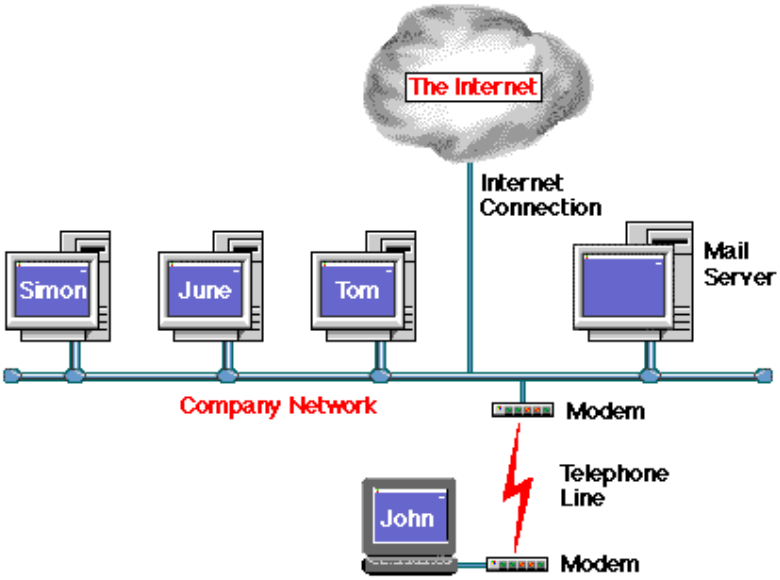
For example, if Tom wants to send a message to "Fred" who is an email user within another company in the US, then he would address the mail message to "Fred@thecompany.com" where "thecompany.com" is the domain for the company where Fred is based. (Domains will be discussed more fully later in this FAQ).

With this arrangement the company mail server sends and collects email on behalf of the office network users. The users themselves never actually connect to the Internet.

This allows the local Company Network and telephone connection to be used efficiently with the most flexibility.

Used in conjunction with dial-in remote users to the company network, as discussed earlier, this system would allow for remote users to have access to global Internet email when dialling in to the Company Network.

g. **A Company Network connected to the Internet**



This gives all the flexibility of internal email within the company, but also allows Internet access for remote users to the company mail server for collecting and sending messages. The Internet connection would have to be full time in order to implement this arrangement.

Note that the actual physical "Internet Connection" could be one of a number of different connection methods, depending upon the potential traffic requirements

to and from the Internet. Also some form of Firewall protection would be a sensible option. (A Firewall allows specified traffic through it, preventing unauthorised access both into the company network, and out onto the Internet).

Remote users could access the company network either via a direct dialled connection, or via the Internet. Also local dial-in users could access the Internet through the Internet Connection, effectively turning the Company into a private ISP!

h. **More on Domain Names**

Domains were introduced earlier, with the examples "Local.Office.A" ,"Local.Office.B" or "New.York.Office." which would allow the easy addressing of users within a department. Taking the "New.York.Office" as an example, it is fine for use internally within a company, but does not give enough information to be used on the Internet.

As can be seen, these domain names are suitable for internal use within a company, but as there are potentially a large number of company with a New York Office, this cannot be used on its own. This description is simply not sufficient for Internet Email, which has to give an unique address for every user.

The way to expand on this would be to add the company name to the domain:

So the example "New.York.Office" could become "ny.office.company.com" which would be fine for addressing Internet email, as it would give a legal usable address, for example:

Tom, based at the Company New York Office, would be addressed to on the Internet as "tom@ny.office.company.com." This gives full information on how to address a message to Tom, with no chance of it going to the wrong person.

If you are wondering what the "com" part of the domain name is for, it simply specifies the type of domain, or the location of the network that the domain is referring to. This section of the domain name is referred to as the "top level" of the domain.

"com" specifies "COMmercial organisation", and tends to refer to an American company, although other non-US companies also have "com" top levels to their domain.

Some examples of these are: apple.com, microsoft.com or pepsi.com

A few other possible variations of "Top Level" domains are:

GOV Government
ORG Non-Profit Organisation
EDU Educational Establishment

Please note that recently a number of new top level domains have been made available, but are not get in general use. A few of the new domains are: firm, store, web, arts, rec, info, nom.

Other endings available give the country of the network, in two letter format. A few examples are:

UK United Kingdom
JP Japan
GM Gambia
AQ Antarctica

Note that top level domains, normally outside the of the US, are sometimes combined and that "co." (referring to "Company") is usually also added before the country, for example:

open.gov.uk government office in the United Kingdom.
nissan.co.jp The Nissan Car company in Japan.

6. What is an Email address?

An example email address looks like this:

This address is made up of two parts:

Email account	This is a particular users email account name that, in this case, the SmartGuard.com mail server can deal with.
Domain name	This is a name that a company has registered so that they can use it on the Internet. Other examples are: apple.com, or microsoft.com.

If a person or company has not registered their own domain name then they may be using their Internet Service Provider's (ISP) domain name, for example: netcom.com, or aol.com. This is usually a less expensive option than registering your own domain name, but does mean that you have to use your ISP's domain name all the time.

In the above example "SmartGuard.com" is the domain name that has been registered so that SmartGuard can use it on the Internet.

7. How does email get from one email client to another email client?

a. Fred wants to send an email message to joe@acompany.com. The email client on Fred's machine sends the message to the email server.

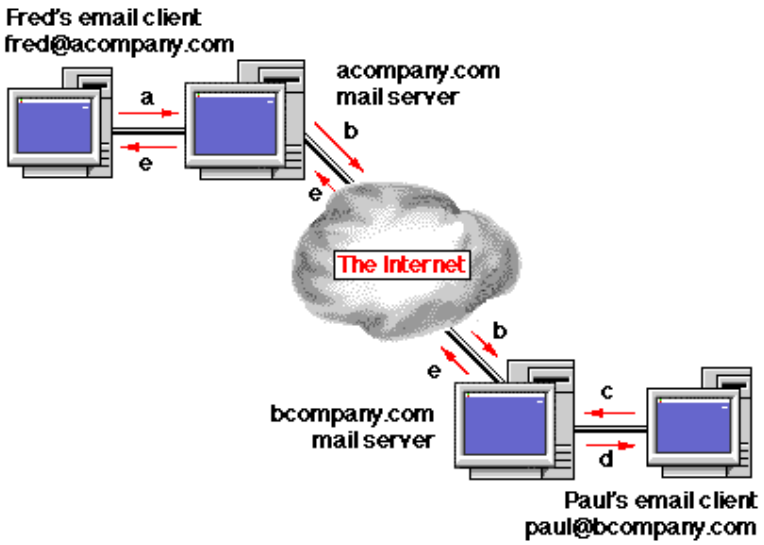
The mail server checks to see if it has an account with the user name "Joe." If this account exists then the message is stored, ready for Joe to collect. If there is not an account for Joe, the message is returned, with an explanation that Joe does not have an account, so the message could not be delivered.

b. Joe checks his email at a later time. Joe's email client asks the email server if there is any mail for Joe.

c. As there is mail waiting for Joe--from Fred-- the email client downloads the waiting message from the mail server. Joe can then read the email message and reply to Fred, if he wants, using his email client.

d. If Fred had sent mail to "tom@acompany.com", instead of "Joe@acompany.com" and Tom did not have an email account created on the mail server, Fred would receive a message back telling him that Tom did not have an email account, so his message could not be delivered.

8. How does email get from one email client to another when they are at different locations?



Fred wants to send an email message across the world to "paul@bcompany.com"

a. He creates his email message with his email client, which sends the message to the acompany.com mail server.

b. The mail server compares the domain name of the destination email address (i.e. bcompany.com) with the domain name it has been told to look after (i.e. acompany.com). These domain names are different, therefore the acompany.com mail server will send the message to the mail server that looks after email for the bcompany.com domain. (How it finds the bcompany.com mail server will be dealt with in Part two of this FAQ)

c. Paul checks his email at a later time. His email client asks his email server if there is any mail for Paul.

d. As there is mail waiting for Paul --from Fred-- the email client downloads the waiting message from the mail server. Paul can then read the email message and reply to Fred, if he wants, using his email client.

e. If Fred had sent mail to "tom@bcompany.com", instead of "Paul@bcompany.com" and Tom did not have an email account created on bcompany.com's mail server, Fred would receive a message back telling him that Tom did not have an email account on the bcompany.com mail server, so his message could not be delivered.

9. But what happens when a destination mail server cannot be found by the sending mail server?

If the destination mail server cannot be found or is extremely busy, a number of different things can happen:

If the sending mail server cannot find any information *at all* regarding the destination, then the message is returned to sender, stating the reason for failure. This usually means that the message had an incorrectly spelt email address.

If the sending mail server can find information regarding the domain it is trying to contact, but cannot actually contact the mail server that maintains the destination domain, it will hold the message for a specified time, before trying again. If it has tried to send the same message a number of times without success, then it will return the message to the sender, warning that it had tried a number of times, but failed.

This can happen if the destination mail server is unavailable for some reason, (such as on a part time connection) or has crashed.

To assist against this type of problem, it is possible for more than one mail server to look after a domain. If the first mail server cannot be found, then a second machine can be specified to accept mail on it's behalf. If this mail server cannot be found then a third mail server can be specified, and so forth. If no mail server at all can be found to contact, then the sending mail server will wait for a specified time before trying again.

Some larger organizations can have 10 or more mail servers looking after their domain, each passing mail to the final destination mail server.

This method also makes allowances for when a mail server is extremely busy, as can be the case with large ISP's mail servers which can process many thousands of messages an hour.

1. What is Spam?
The term Spam refers to unsolicited, unwanted, inappropriate bulk email, Usenet postings and MUD/IRC monologs. For the purposes of this discussion, we will use the term Spam primarily in reference to email, which is what it is generally understood to mean when used in connection with the Internet. Spam is often referred to as Unsolicited Bulk Mail (UBM), Excessive Multi-Posting (EMP), Unsolicited Commercial email (UCE), spam mail, bulk email or just junk mail.

2. When is Spam Spam?
Exactly where to draw the line between Spam and legitimate email or spam free bulk email is not as obvious as it may seem. To some, any and all email that does not come from an approved source is Spam. According to Mail Abuse Prevention System (MAPS) http://www.mail-abuse.org/:

An electronic message is "spam" IF: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; AND (3) the transmission

and reception of the message appears to the recipient to give a disproportionate benefit to the sender.

MAPS' definition of Spam goes on to say that whether the email is relevant, or whether the benefit to the sender is disproportionate is up to the recipient and not open to discussion. If this is the case, then Spam isn't Spam until the recipient decides it is. However, point (2) above really only makes sense when interpreted in the context of bulk email sent to subscribers. As often as not, the first email you ever send to someone has not been "authorised" since you have never exchanged emails. Further, MAPS goes to considerable length to define "strong terms and conditions prohibiting [email users] from engaging in abusive email practices". These terms and conditions deal exclusively with bulk email sent to lists of addressees. In other words, they want their users to send spam free bulk email. This underlines the generally accepted principle that for Spam to really be Spam, it has to be bulk email. This definition is reinforced by Henry Neeman's "Why Spam is Bad" - a thoroughly enlightening read. Mr Neeman explains to a particularly dense group of spammers, entirely in single syllable words that "Spam is the same thing lots and lots of times."

To learn more about how to stop spam mail and block junk email with a junk email filter or anti spam program, read on.

3. Where does the term "Spam" come from?

The prevailing theory is that the term refers to a classic skit by Monty Python's Flying Circus. In the skit a couple in a restaurant tries in vain to order something that does not have SPAM in it. As the waitress lists endless dishes, all of them containing increasing amounts of SPAM, a group of Vikings in the corner begin to sing "spam, spam, spam, spam…" until all useful information is drowned out. But where did the connection between unwanted SPAM and unwanted Spam come from?

It did not start with email. The term has it roots, in relation to the Internet, in the late 1980s or early 1990s in Multi-User Dungeons (MUD) and Multi-User Shared Hallucinations (MUSH). MUDs and MUSHes are online, real-time, interactive, text-based virtual environments. According to one source, a MUSH user programmed a macro key to type "spam spam spam…" in a MUSH until his connection was terminated by a SysAdmin. He was subsequently referred to as "the !*%@ who spammed us" by other members. From MUDs and MUSHes the term Spam began to be used to describe Excessive Multi-Posting (EMP) on Usenet groups. Usenet "news" groups are forums where "authors" can "publish articles" to be read by other users and subsequently discussed. Not much of what gets "published" could ever be considered "news" by any reasonable standard of measure, but the original term is still used today. Under normal circumstances a user would post a message to one or to a small number of relevant newsgroups, asking questions or airing opinions. By using software to automate the process of posting, it became possible to post the same message to thousands of newsgroups ensuring a readership in the hundreds of thousands or even millions.

The very first Spam email was sent on 1 May 1978 by a Digital Equipment Corp. sales rep advertising a computer equipment demonstration. An attempt was made to send this email to all of the Arpanet users on the west coast of the US. The reaction on the part of the recipients was not unlike what you may expect

today. Remember that Arpanet was a military project and commercial use was not acceptable. At the time, there was no such thing as an email Spam filter to stop Spam mail because there was no Spam. In April 1994, the Phoenix law firm, Canter and Siegel, advertised their services by posting a message to several thousand newsgroups. This was probably the first automated large scale commercial use of Spam, and was the incident that popularised the term, which up until then had been exclusively part of the arcane vocabulary of Multi-User Dungeons.

4. Why do people send spam?
Spam is the electronic equivalent of junk mail. People send Spam in order to sell products and services or to promote an email scam. Some Spam is purely ideological, sent by purveyors of thought. The bulk of Spam is intended, however, to draw traffic to web sites or to sell sex and money making schemes. Unlike junk mail in your physical mailbox, Spam does not abait if it is unsuccessful. When marketing departments send junk mail at considerable expense, without success, they generally cease, or try a different sales pitch. Spam on the other hand can be entirely unsuccessful, but the large number of wannabe spammers waiting in the wings ensures that we will continue to receive lots of it.

Spammers go to considerable effort to thwart recipients' attempts to stop spam email. They specifically design their emails to bypass your email spam filter.

5. How can I tell who the spam is from?
Normally you cannot. Spam control can become very sophisticated. More experienced users can look at the email "headers" to find the origin of the message but frequently the spammer will set up a one-time email account purely to initiate the spam email shot. When the email shot is finished, the account is closed. At other times, the spammer will forge headers making it difficult or impossible to trace the origin of the Spam, so finding the original sender will very often prove fruitless. Spam protection and junk email prevention require more subtle measures than just finding the culprit.

6. How do spammers get my email address?
Through many means. Some companies you may have had dealings with sell their mailing lists to third parties, spammers included. Spammers also use "robots" to scour the Internet and harvest any email addresses that they find. If you post to newsgroups you are also at risk of spammers picking up your email address and sending you junk email. To get adequate spam protection and get rid of Spam, you really need more than one email address. This is an essential element of proper Spam control.

7. If I unsubscribe won't it get rid of spam?
If you didn't have to subscribe to get it, there is little chance that unsubscribing will get rid of Spam. Professional spammers (something about those two words in the same phrase doesn't seem right, but I digress…) use this trick to validate their email address list. They buy or steal lists sometimes containing millions of email addresses. Large percentages of these addresses may be invalid. By unsubscribing to the list, you are informing the spammer that your email address is a good one, and may be sold on to other spammers. Be prepared for more Spam, from many more sources. A better alternative would be to try blocking Spam, or to bounce Spam email using specialized email software.

8. Isn't Spam illegal?
Clearly Spam is illegal if it promotes an illegal product or service. However, spam legislation is pending in the US and in Europe that would make the mere act of sending unsolicited commercial email illegal in the absence of an existing business relationship. The Coalition Against Unsolicited Commercial email (CAUCE) applauds the tough proposed European legislation, but opposes the proposed US anti spam legislation which it considers weak and ineffective at stopping spam. Bill S 630 would establish UCE as a legitimate practice. The onus would be upon the recipient to "opt out" of the mailing list by unsubscribing. In the event of non-compliance on the part of the spammer, it would be up to the ISP to trace them and take action (most end-users lack the sophistication to trace an email back to a physical real-world company or individual). Fines of up to $10 per illegal Spam would be levied. The CAUCE argues that since the Federal Trade Commission (FTC) is the only enforcing body, given the large number of Spam emails it is unlikely that any serious enforcement would ever take place. CAUCE takes the position that the recipient's email resources are private property and likens UCE to placing advertising billboards on their property at no charge.

Proposed European legislation is much tougher and many believe it would help get rid of Spam. It will require prior consent from the recipient before receiving unsolicited commercial electronic communications including SMS, fax and email. The directive has already been published in the Official Journal of the Economic and Monetary Union and is expected to be implemented in member states by 31 October 2003.

9. How big of a problem is spam?
Big. Spam is a big problem first of all because it is symptomatic of inefficient, parasitical businesses. The Nobel Prize winning economist Ronald Coace in what is now known as the Coace Theorem postulated that an inefficient business (one that cannot bear the cost of its own activities) is dangerous to the economy, because to function, it must spread the cost of its activities across a large number of victims. The Coace Theorem cuts close to home where Spam is concerned. Any business that needs to send Spam emails to survive is not a viable business. The benefit to the spammer is disproportionate to the cost borne by the spammer, which is next to nil. More importantly, the cost of Spam removal to the victims is totally disproportionate to the benefit to the spammer. In a free market economy such a grossly inefficient process should cease when property rights are enforced (i.e. the cost is borne by the the party who incurs them).

Spam is a big problem because property rights are difficult or impossible to enforce which makes it hard to get rid of Spam. From the 1800s through the mid 1960s industrials considered it their right to produce and pollute with impunity. The economy could not run without their products. They could not afford to not pollute. It took over two decades of lobbying to move government and industry to another point of view. Yet these were reasonable businesses, with physical assets in the countries of their victims and subject to their legal systems. Consider the spammers in contrast. Any physical assets they may have are irrelevant to their activity, which incidentally, has no borders. They are not subject to the legal systems of their victims. If they become subject to legislation attempting to stop Spam they can find a more favourable environment in another

country. The immediate effect of the new European legislation will be to force the spammers offshore rather than to stop junk email. There will be less Spam coming from European countries, but there will not necessarily be any less Spam.

Spam is a big problem because of the shared resources it consumes. Internet Service Providers (ISPs) allow you to surf the Internet, and deliver your email to your email software usually for a flat monthly fee. They must, in turn, purchase bandwidth (the technical term for their own connection to the Internet). The more users they have, the more bandwidth they need. If they have very large numbers of users they may need to purchase additional servers to manage email. These costs are offset by the added revenues of a larger user base. Spam however, increases their need for bandwidth, and increases the load on their email servers with no added revenue to compensate. The added cost must be passed on to the customers, the victims of spammers trespassing on their private cyberproperty. Some very large email servers have been shut down due to Spam overload for extended periods depriving hundreds of thousands of paying customers of their emails. One leading ISP processes about 30 million email messages a day, 30% of which are Spam. The problem of Spam has reached proportions where it threatens the viability of email and of the Internet itself.

Spam is a big problem because of the private resources it consumes. Many business people spend up to fifteen minutes per day reading and deleting their Spam emails. A company with 100 knowledge workers earning an average of $40,000 per year each spending ten minutes per day deleting Spam would experience an added burden of $80,000 per year. This cost would be passed on to Internet users and non-users alike as they purchase products from this company at their local department store.

Spam is a big problem because of number of victims it involves. According to META Group, 5-15% of corporate email is Spam. This is expected to grow to to 15-30% in the near term. This means that the average medium-sized company receives 20,000 Spam emails per day. Taking the above example a little further, if 10 million people each lose 5 minutes a day deleting Spam, in terms of productivity, this could cost the global economy over $4 billion annually, not counting wasted bandwidth, CPU time and network administration time and tools. Based on these assumptions, the global cost of Spam may well be over $5 billion annually.

10. What are DNS blacklists?

DNS blacklists are lists of domains that are known to originate Spam. Many anti-spam software programs use these lists to control Spam by refusing any email that originates from one of these domains. DNS blacklists are usually maintained by anti-spam organizations or by individuals with an intense dislike for Spam. The difficulty with DNS blacklists is the need for objectivity in deciding when to blacklist a domain. In order to know that a domain is producing Spam, the offence must be reported. Reporting Spam without any anti-abuse mechanism in place, however, leaves nothing to stop people from getting servers added to a DNS blacklist out of malice. The obvious solution would be to require a minimum number of reported incidents before blacklisting a server. This proves equally unsatisfactory however as a measure to stop Spam mail. Anyone who manages large mailing lists knows that a small percentage of people who subscribe

subsequently accuse the sender of spamming them when they receive their email. Naturally, a company that sends out millions of legitimate commercial emails will receive more accusations of Spam than one that sends out a smaller amount of spam free bulk email.

The real solution lies in good management. A system administrator that knows about Spam, that knows who the large legitimate bulk mailers are and responds rapidly to complaints from unjustly blacklisted domains will ultimately provide a useful service to the Internet community at large. There are some well-managed DNS blacklists on the Internet and these can be a useful addition to the feature set of anti spam software. Below is a short list of the better known sites:
Realtime Blackhole List
Spam Cop
Spews.org
Open Relay Data Base
Monkeys.com
Rfc-ignorant.org

11. What is an open relay?
Anyone who has travelled a lot has experienced the following: You check into your hotel. You connect to the Internet using the Ethernet socket in your hotel room. You try to send an email to the office, and your email client refuses saying "relaying denied". What happened? Suppose your email address is you@foo.bar. Your regular email server, which may be named mail.foo.bar, knows all of the IP addresses of all of the machines connected to the Internet via the foo.bar domain. Should the mail.foo.bar forward email coming from another domain than foo.bar, this is referred to as "relaying". Most ISPs do not allow relaying of email from untrusted domains, indeed from any domains but their own. Your laptop computer was using an IP address allocated by your hotel's DHCP server. Mail.foo.bar did not recognize this IP address, and refused to relay. There are a lot of poorly configured email servers however, that will let anyone use them to send email. An open mail relay becomes a channel for Spam, virtually "hijacked" by unscrupulous spammers who send large numbers of emails through them until they are discovered and banned, and move on to another open relay. Early versions of certain email servers did not stop spam email , but defaulted to open relaying when set up, so that there are many open relays available to spammers today. Recent versions of most email server products default to denying relaying in order to block junk email.

12. How can I stop Spam email?
There are a number of things you can do to stop Spam email. Which ones suit you best will depend upon your needs, the type of email you generally receive, whether you have complete control over your email account, the number of legitimate correspondents you may have and how long you tend to keep them.

Scenario A.
Joe runs a small business. He regularly exchanges emails with about 50 business contacts. He also uses the Internet extensively to order goods or information, to book events and travel and to make new business contacts on newsgroups. Currently, over one half of his email is Spam. He can delete it fairly quickly, but it gets on his nerves. The first thing Joe can do to get rid of

Spam is change his email address and inform his regular colleagues. Next, he can get a second, web-based email address at no charge from one of the many providers of this type of service. He can use his web email address when entering information into online forms or when dealing with any untrusted third party, knowing that this is the address that will be likely to get more Spam. When it starts to get too much Spam, he can simply change it without having to inform anyone. Lastly, Joe can use the Spam filters in his email client software to filter out any obvious Spam that manages to get through. Optionally he can use dedicated anti Spam software to block Spam.

Scenario B.
Annette works in the customer service department of a large organization. Unlike Joe, Annette receives large numbers of legitimate emails from people with whom she has had no previous contact. It would not be feasible for Annette to change her email address and inform all of her correspondents. Furthermore, all of the email addresses in Annette's organization have the same format: firstname.lastname@organization.tld. Annette receives over one hundred emails per day, of which typically sixty are Spam. Annette needs to talk to her email administrator to discuss the problem, which plagues many of her co-workers as well. The ideal long-term solution for Annette's organization would be to install a server based anti Spam software with rules that can be modified for users and groups of users. Email users in Annette's service may have slightly different needs than users in human resources or in the legal department. In the meantime, Annette can probably lower her Spam workload substantially without filtering out legitimate customer email. By using the filters in her email client to examine the sender email addresses and subject fields of the Spam she receives, she can quickly identify keywords that will enable her to filter out most of the obnoxious Spam messages. This is not a good long-term solution, but will help her to cope until her email administrator implements something better.

Scenario C.
Jean is head of IT in a middle school. She wants her students to use the Internet for research, become fluent in IT and be able to receive emails from legitimate sources. She already has a web content filtering system in place, but has no means to ensure that students do not receive inappropriate emails. Unlike Annette's organization, which would rather let the odd Spam message get through than accidentally prevent legitimate customer emails from reaching their destination, Jean's school cannot allow any inappropriate email to reach the students, even if this means blocking the odd legitimate message. Jean needs a server based solution that meets the following requirements: a) it must filter all email regardless of what email server it came from, b) it must quarantine suspect emails, allowing authorised personnel to flag individual mails as legitimate and c) it must have a variable threshold allowing the administrator to increase the level of severity in the

event that marginal but bad emails actually reach their recipients.

There are many ways to stop Spam. One or several may be right for you. This will depend on a variety of factors as the above scenarios suggest.

13. How does an email Spam filter work?
For most email users, using an email Spam filter to get rid of Spam is the only viable alternative to manually sifting through large numbers of junk email every day.

There are different kinds of filters:
User defined filters are included in most email clients today. With these filters you can forward email to different mailboxes depending on headers or contents. For example, you would put email from each of your friends into a mailbox named after them. You can also use these same filters to forward email to the trash if the origin or contents are suspicious. To do this you need to carefully look at any Spam emails you receive. Try to notice common characteristics, recurring patterns in senders' email addresses, dubious claims in the subject line and so on. You will soon find that Spam filtering using a small number of rules can eliminate a large number of Spam emails.

Header filters are more sophisticated. They look at the email headers to see if they are forged. Email headers contain information in addition to the recipient, sender and subject fields displayed on your screen. They also contain information regarding the servers that were used in delivering your email (the relay chain). Many spammers do not want to be traced. They put false information in the email headers to prevent people from contacting them directly. Some anti spam programs can detect forged headers which are a sure indication that the email is Spam. Not all Spam has forged headers though, so this filter by itself is not sufficient.

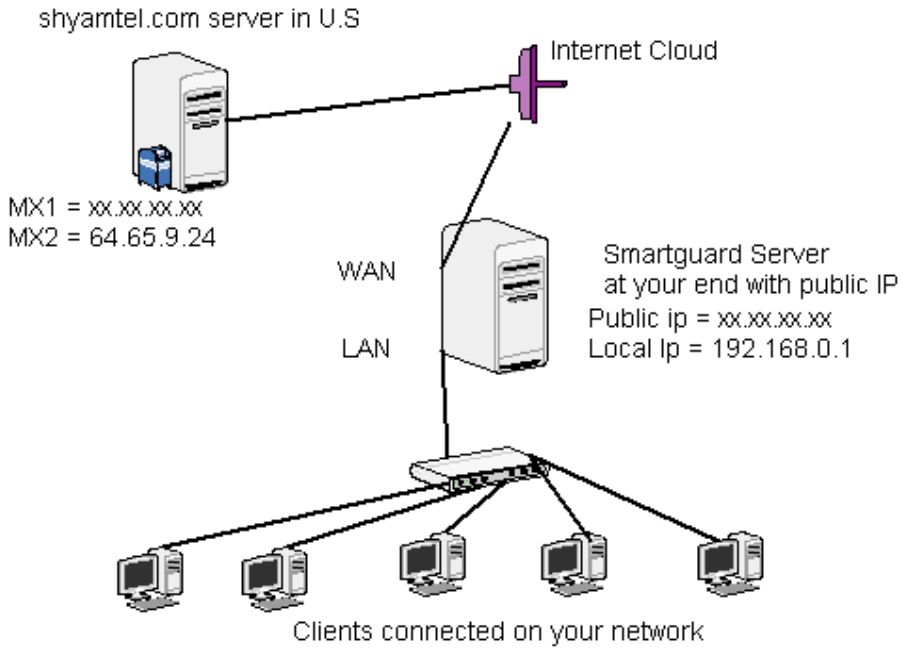
Language filters simply filter out any email that is not in your native tongue. It only filters out foreign language Spam, which is not a major problem today, unless the foreign language in question is English. In future, languages other than English are expected to make up an increasingly large percentage of Internet communications. If you do not expect to get emails in another language, this may be a quick and easy way to eliminate some portion of your Spam.

Content filters scan the text of an email and use fuzzy logic to give a weighted opinion as to whether the email is Spam. They can be highly effective, but can also occasionally filter out newsletters and other bulk email that may appear to be Spam. This can usually be overridden by explicitly authorizing email from domains you subscribe to.

Permission filters block all email that does not come from an authorized source. Typically the first time you send an email to a person using a permission filter you will receive an auto-response inviting you to visit a web page and enter some information. Your email then becomes authorized and any future emails you send will be accepted. This is not suitable for all users, but very effective for those that choose to use it, as long as the auto-response email is not blocked by the Spam filter of the initial sender!

14. I want to send Spam free bulk email. How can I be sure my recipients won't think I'm sending Spam?

Not all bulk email is Spam. Many responsible organizations send Spam free bulk email regularly to their customers, and subscribers. In efforts to stop Spam email, many recipients use specialised email software to block junk email, which has the undesired effect of filtering out legitimate Spam free bulk email. What is more frustrating to the email sender is to receive Spam reports from DNS blacklist holders stating that they are sending Spam when in fact they are sending legitimate Spam free bulk email. Many people subscribe to so many lists, they cannot remember what they subscribed to. If an email looks like Spam, they report it without taking a closer look to determine what it is.



All Traffic coming to WAN port will be filtered and then will be passed to LAN and vice versa . ALL Spam and virus will be filtered at smartguard server and then traffic will be send to individual users.

PROPOSED SOLUTION FOR SHYAM TELECOM

SmartGuard virus scanner is a complete e-mail security system designed for use on e-mail gateways. It protects against viruses, and detects attacks against e-mail client packages (Outlook, Eudora). It can also detect almost all unsolicited commercial e-mail (spam) passing through it and respond to all incidents in a wide variety of ways.

Not only can it scan for known viruses, but it can also protect against unknown viruses hidden inside e-mail attachments by refusing entry to attachments whose filenames match any given pattern. This can include generic patterns that trap filenames attempting to hide the true filename extension (e.g. ".txt.vbs").

Attachments containing viruses that can be disinfected (e.g. word processor macro viruses) are automatically disinfected and sent on to their original destination.

Smartguard Webmail Features For Users:

* Auto Login
* Multiple Languages/Multiple Charsets
* Strong MIME Message Capability
* Full Content Search
* Draft Folder Support
* Confirm Reading Support
* Spelling Check Support
* vCard compliant Addressbook
* POP3 Support
* Mail Filter Support
* AntiSpam Support through SpamAssassin (http://www.spamassassin.org)
* AntiVirus Support through ClamAV (http://www.clamav.net)
* Calendar with Reminder/Notification Support
* Webdisk Support
* HTTP Compression

For System:

* Fast Folder Access
* Efficient Message Movement
* Smaller Memory Footprint
* Graceful File Lock
* Various Authentication Modules
* PAM support
* Remote SMTP Relaying
* Virtual Hosting
* User Alias
* Pure Virtual User Support
* Per User Capability Configuration

Spam Protection
Smartguard's Spam Protection application detects and blocks unsolicited emails.

It uses multiple detection methods to pinpoint spam types while minimizing "false positives".

It performs a series of tests and assigns a "spam score" to each message indicating the probability that the message is unsolicited. Messages whose score exceeds thresholds set by the administrator are dropped, returned to the sender, passed to the recipient with a warning, or quarantined.

Accurate Identification of Spam
Smartguard's Spam Protection utilizes nine methods to pierce the disguises used by professional spammers:

Sender Address Verification: Messages are tested to determine if they come from legitimate email addresses.
Realtime Blackhole Lists (RBLs) and spam databases: Email addresses are checked against databases of known spammers.
Header Analysis: The header section of emails are checked for false or altered information and addresses with invalid characters.
Body Analysis (Heuristics): Words and word patterns typical of spam are identified.
SPF record checking: Rejects emails coming from a false “Mail From” address.
URL Scanning: URLs within emails are checked against a database of known spam URLs.
Greylisting: Unknown mail BATV Reverse Path Signing: Blocks emails from being “bounced back” to an email server unless they really originated there. servers are asked to resend messages before they are accepted.
Whitelist and Blacklist: The administrator can list email sources known to be legitimate and illegitimate
The results of all tests are incorporated in a “spam score” that indicates the probability that the message is unsolicited.

Management Control
Administrators can tune Smartguard’s spam filter to balance stringent blocking against the risk of missing legitimate messages. Options include:
Enabling or disabling tests.
Taking actions based on “spam score” thresholds.
Specifying that suspect messages should be:
Dropped
Rejected and error notice returned to the sender
Passed through to the recipient with a warning In addition, a digest of blocked messages can be sent to each user daily. If the user sees an email that was incorrectly blocked, he or she can click on a link and receive the email automatically.

Performance and Simplicity
Smartguard’s Content Filtering FrameworkTM integrates spam protection with the firewall and virus scanning into a single extensible system. This improves performance and simplifies ongoing management:

Quarantined for later evaluation and disposition

Performing spam testing, virus scanning and packet filtering on the same system eliminates delays vectoring files to separate systems.
Local whitelists, blacklists and network configurations can be entered just once and shared by all of Smartguard’s security applications.
Reports track statistics on email messages processed, their size and spam score, and the number of viruses found.

Working with the Email Server

Smartguard Security Gateway software can add headers to email messages so that a recipient email application can take specific actions, such as sending suspicious email messages to a “spam” folder on an email user’s desktop. Information added to email headers can include:

A spam flag
The "spam score"
Expression match (flag that the message contains suspicious text)
RBL warning (flag that the message comes from a domain identified in a Realtime Blackhole List)

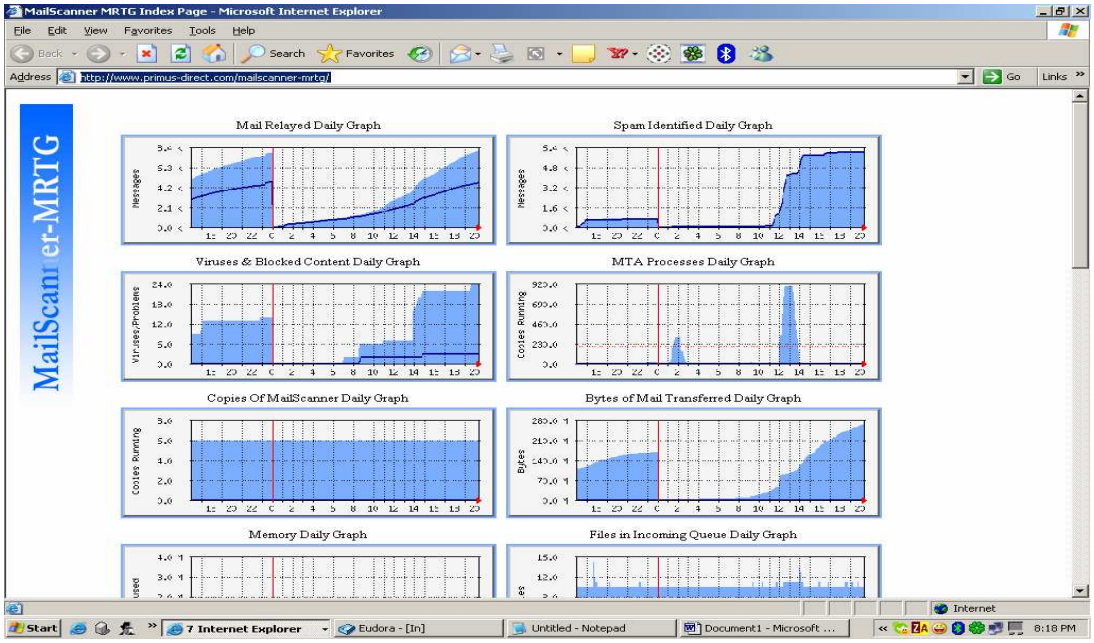
SmartGuard virus scanner is a complete e-mail security system designed for use on e-mail gateways. It protects against viruses, and detects attacks against e-mail client packages (Outlook, Eudora). It can also detect almost all unsolicited commercial e-mail (spam) passing through it and respond to all incidents in a wide variety of ways.

Not only can it scan for known viruses, but it can also protect against unknown viruses hidden inside e-mail attachments by refusing entry to attachments whose filenames match any given pattern. This can include generic patterns that trap filenames attempting to hide the true filename extension (e.g. ".txt.vbs").

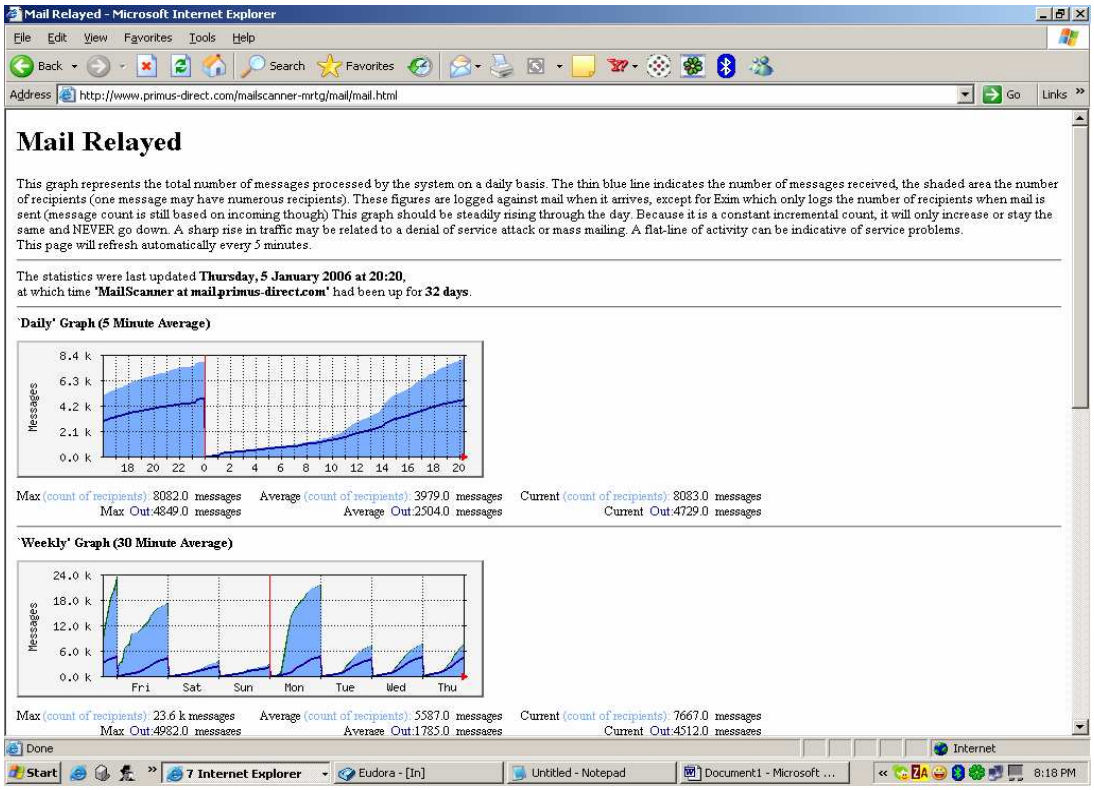
Attachments containing viruses that can be disinfected (e.g. word processor macro viruses) are automatically disinfected and sent on to their original destination.

a. Based on Gateway Level (FTP, SMTP, POP3 & Spam Control)
b. Based on Concurrent Connection to Internet
c. Scanning on HTTP (Requires Customization)
d. Detection should be relevant, continues & real-time
e. Detailed reporting
f. Third Party solution should be able to integrate on same server (supports)

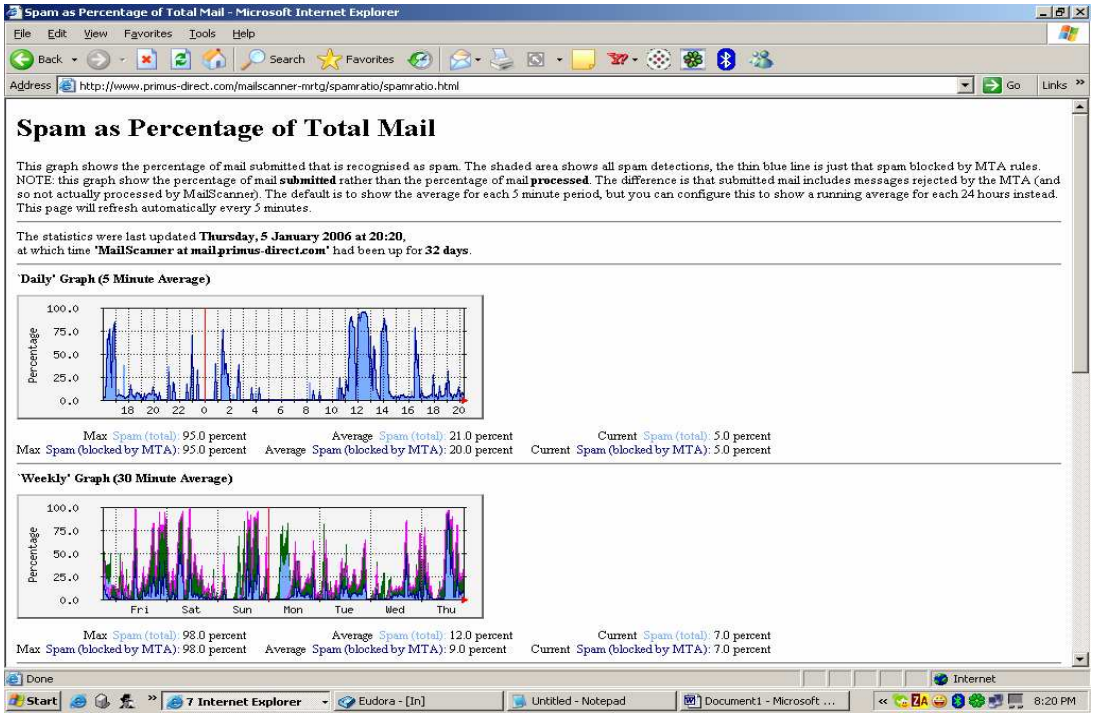
SmartGuard Admin Panel Screen Shot



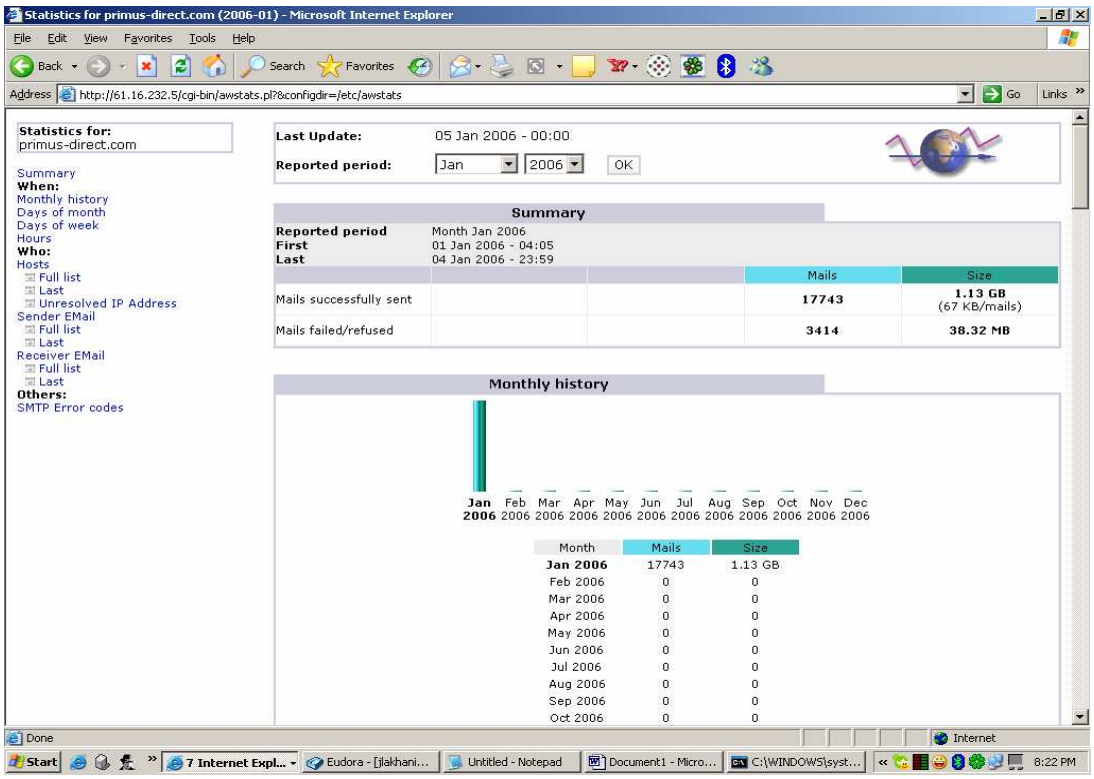
SmartGuard MRTG – Mail Graph Screen Shot -


Mail Relayed - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.primus-direct.com/mailscanner-mrtg/mail/mail.html
Mail Relayed
This graph represents the total number of messages processed by the system on a daily basis. The thin blue line indicates the number of messages received, the shaded area the number of recipients (one message may have numerous recipients). These figures are logged against mail when it arrives, except for Exim which only logs the number of recipients when mail is sent (message count is still based on incoming though) This graph should be steadily rising through the day. Because it is a constant incremental count, it will only increase or stay the same and NEVER go down. A sharp rise in traffic may be related to a denial of service attack or mass mailing. A flat-line of activity can be indicative of service problems.
This page will refresh automatically every 5 minutes.
The statistics were last updated Thursday, 5 January 2006 at 20:20,
at which time 'MailScanner at mail.primus-direct.com' had been up for 32 days.
'Daily' Graph (5 Minute Average)
Messages
8.4 k
6.3 k
4.2 k
2.1 k
0.0 k
18 20 22 0 2 4 6 8 10 12 14 16 18 20
Max (count of recipients): 8082.0 messages Average (count of recipients): 3979.0 messages Current (count of recipients): 8083.0 messages
Max Out:4849.0 messages Average Out:2504.0 messages Current Out:4729.0 messages
'Weekly' Graph (30 Minute Average)
Messages
24.0 k
18.0 k
12.0 k
6.0 k
0.0 k
Fri Sat Sun Mon Tue Wed Thu
Max (count of recipients): 23.6 k messages Average (count of recipients): 5587.0 messages Current (count of recipients): 7667.0 messages
Max Out:4982.0 messages Average Out:1785.0 messages Current Out:4512.0 messages
Done
Internet
Start
7 Internet Explorer
Eudora - [In]
Untitled - Notepad
Document1 - Microsoft ...
8:18 PM

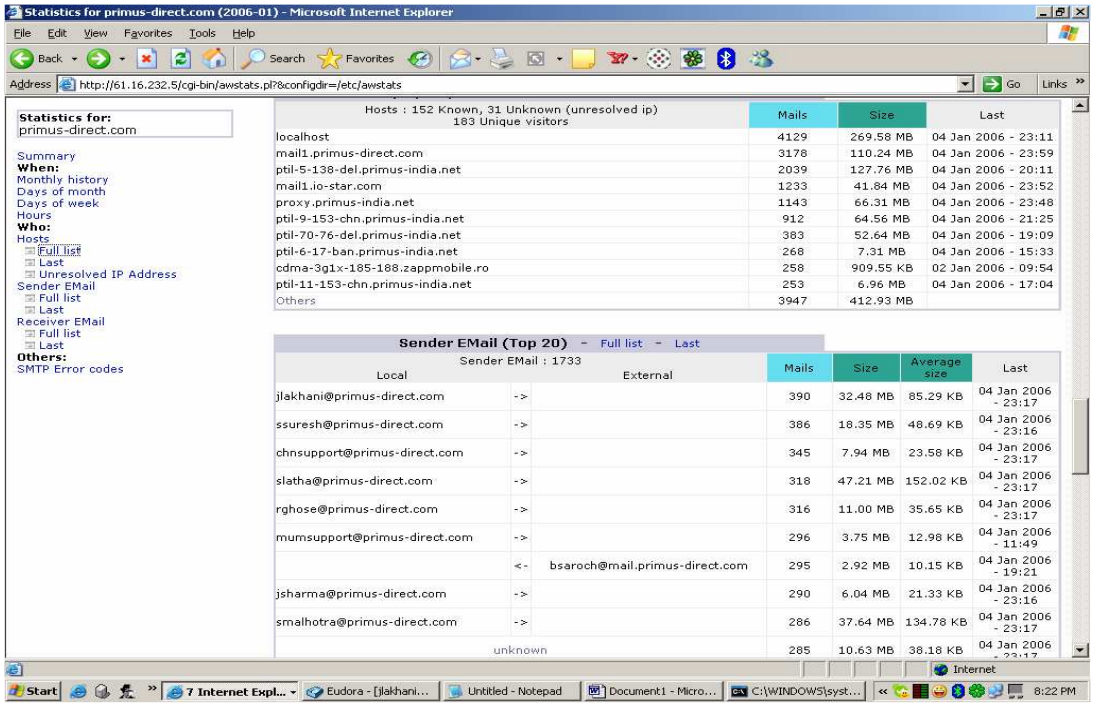
Screen Shot –


Spam as Percentage of Total Mail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.primus-direct.com/mailscanner-mrtg/spamratio/spamratio.html
Spam as Percentage of Total Mail
This graph shows the percentage of mail submitted that is recognised as spam. The shaded area shows all spam detections, the thin blue line is just that spam blocked by MTA rules.
NOTE: this graph show the percentage of mail submitted rather than the percentage of mail processed. The difference is that submitted mail includes messages rejected by the MTA (and so not actually processed by MailScanner). The default is to show the average for each 5 minute period, but you can configure this to show a running average for each 24 hours instead.
This page will refresh automatically every 5 minutes.
The statistics were last updated Thursday, 5 January 2006 at 20:20,
at which time 'MailScanner at mail.primus-direct.com' had been up for 32 days.
'Daily' Graph (5 Minute Average)
Percentage
100.0
75.0
50.0
25.0
0.0
18 20 22 0 2 4 6 8 10 12 14 16 18 20
Max Spam (total): 95.0 percent Average Spam (total): 21.0 percent Current Spam (total): 5.0 percent
Max Spam (blocked by MTA): 95.0 percent Average Spam (blocked by MTA): 20.0 percent Current Spam (blocked by MTA): 5.0 percent
'Weekly' Graph (30 Minute Average)
Percentage
100.0
75.0
50.0
25.0
0.0
Fri Sat Sun Mon Tue Wed Thu
Max Spam (total): 98.0 percent Average Spam (total): 12.0 percent Current Spam (total): 7.0 percent
Max Spam (blocked by MTA): 98.0 percent Average Spam (blocked by MTA): 9.0 percent Current Spam (blocked by MTA): 7.0 percent
Done
Internet
Start
7 Internet Explorer
Eudora - [In]
Untitled - Notepad
Document1 - Microsoft ...
8:20 PM

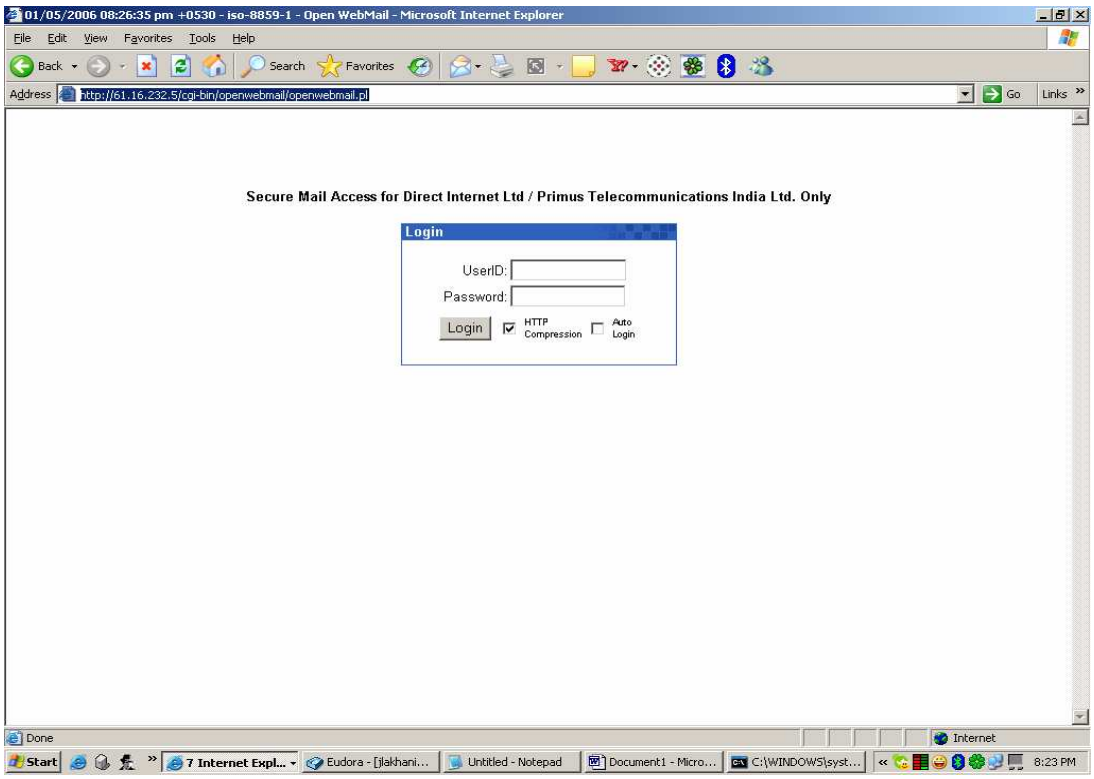
SmartGuard – Mail Stats & Graph Screen Shot -



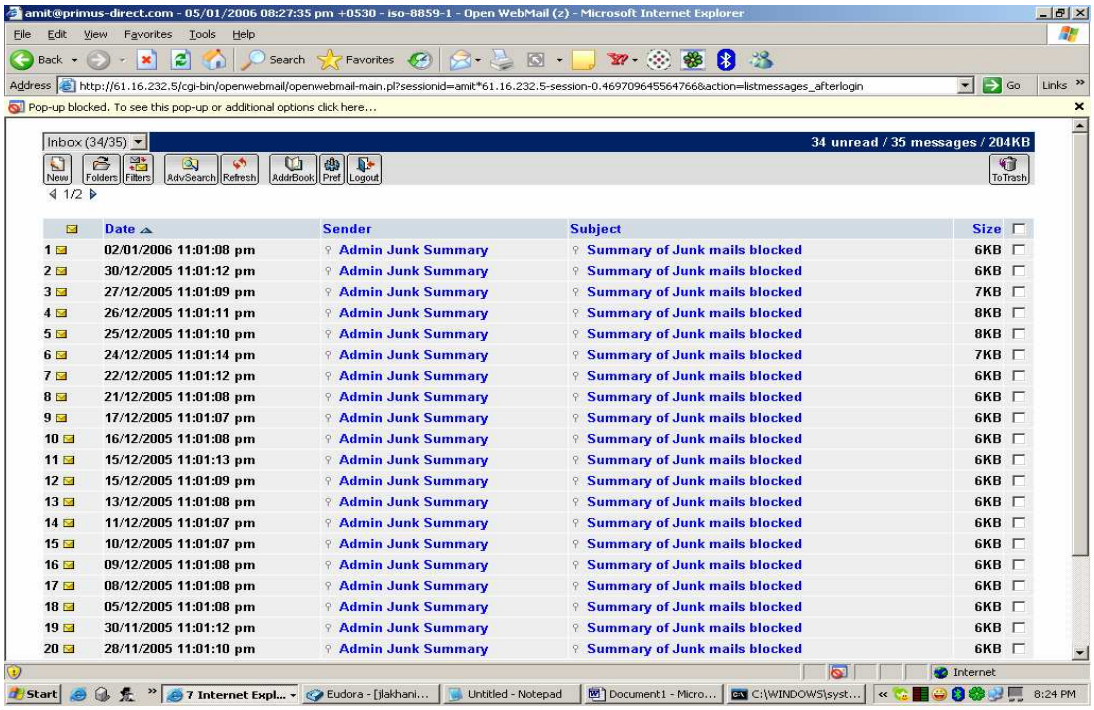
Screen Shot -



SmartGuard WebMail Screen Shot -

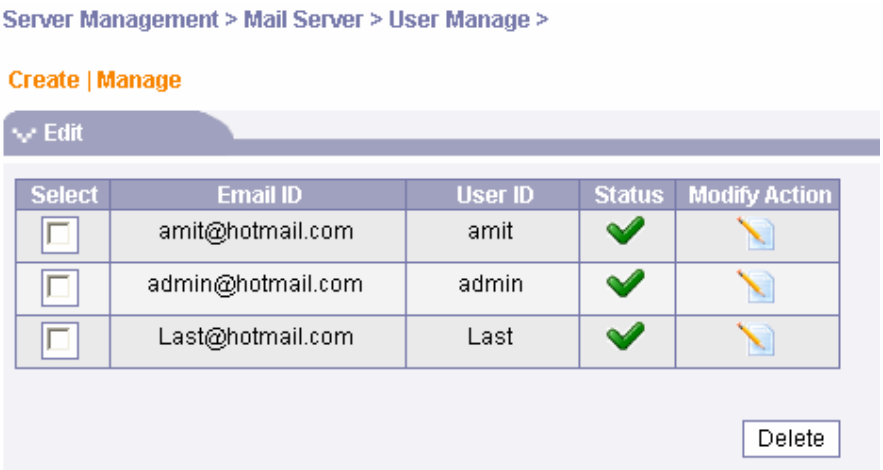


Screen Shot –



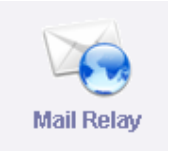
9.2.1 User Manage

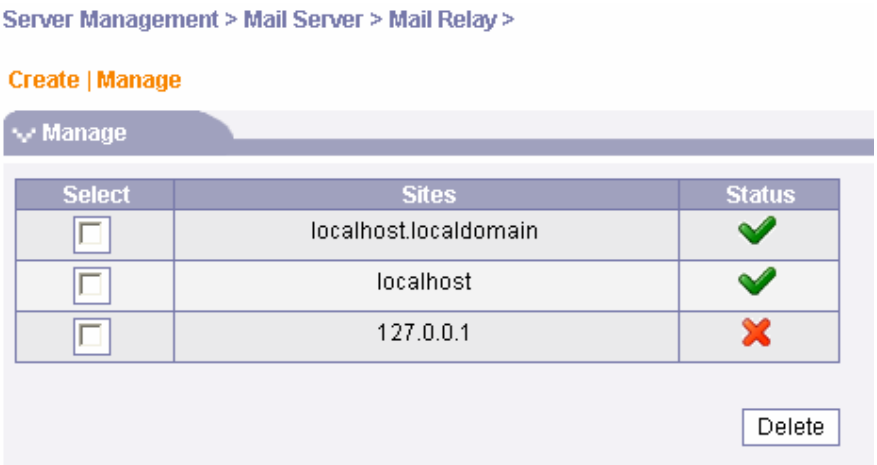
At this page administrator can view the status of mail users and also create , edit and delete the mail accounts.



Create user page

9.2.2 Mail Relay





Administrator can manage and set the Mail Relay at this page.
Create relay page

9.2.3 Spam Configuration

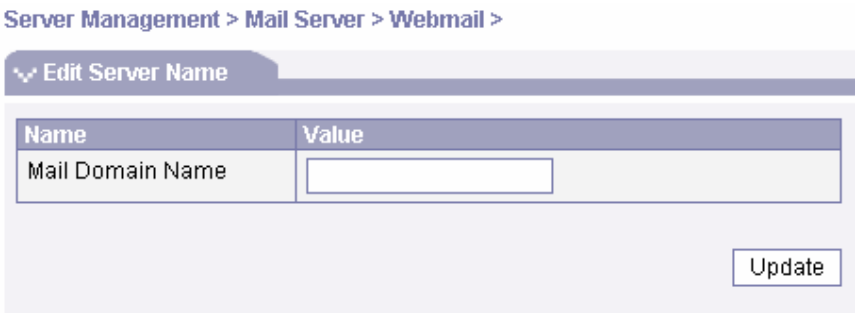
Server Management > Mail Server > Spam Configuration >

Spam Configuration

Name	Value
Quarantine Virus Infections	(•) Enable ( ) Disable
Quarantine Silent Viruses	(•) Enable ( ) Disable
Quarantine Whole Message	( ) Enable (•) Disable
Quarantine Whole Message As Queue Files	( ) Enable (•) Disable
Detailed Spam Report	(•) Enable ( ) Disable
Include Scores In SpamAssassin Report	(•) Enable ( ) Disable
Notify Senders	(•) Enable ( ) Disable
Notify Senders Of Viruses	( ) Enable (•) Disable
Send Notices	(•) Enable ( ) Disable
Notices To Admin Email Id	postmaster
Spam Checks	(•) Enable ( ) Disable
Spam Lists To Reach High Score	3
Required SpamAssassin Score	6

Administrator can do all the spam configurations from here on its server. All the virus definitions, Spams, Quarantines can be done with a single click from this window.

9.2.4 Web mail

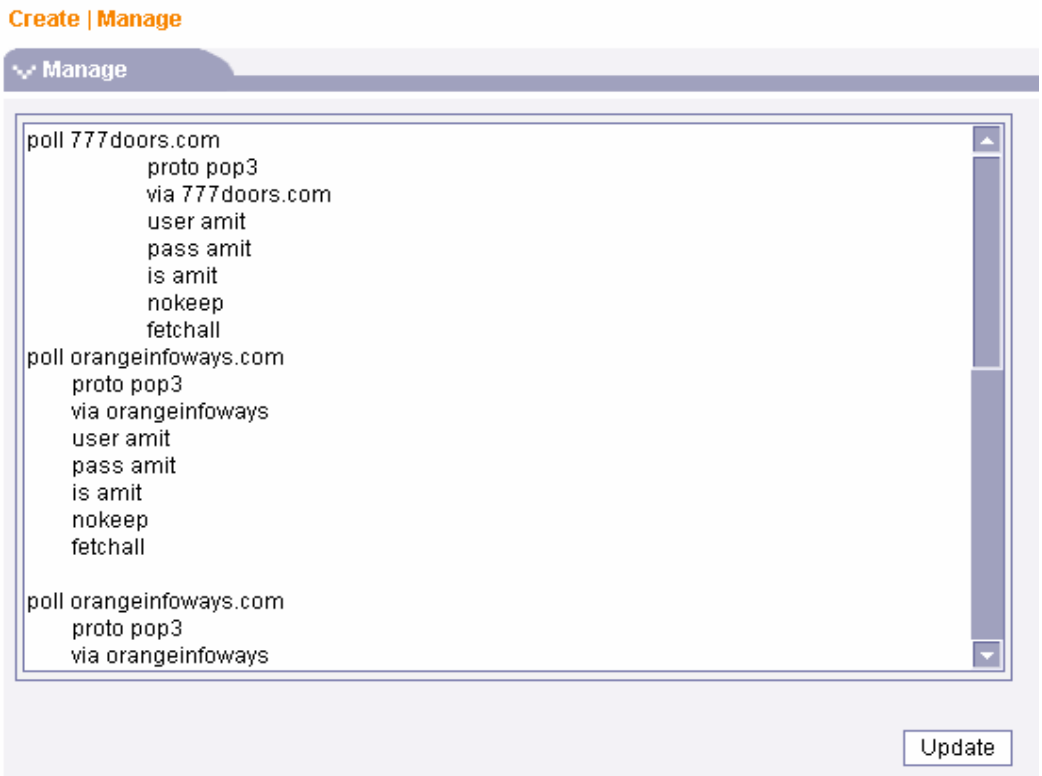


Administrator can Define & Update the Mail Domain Name from this window.

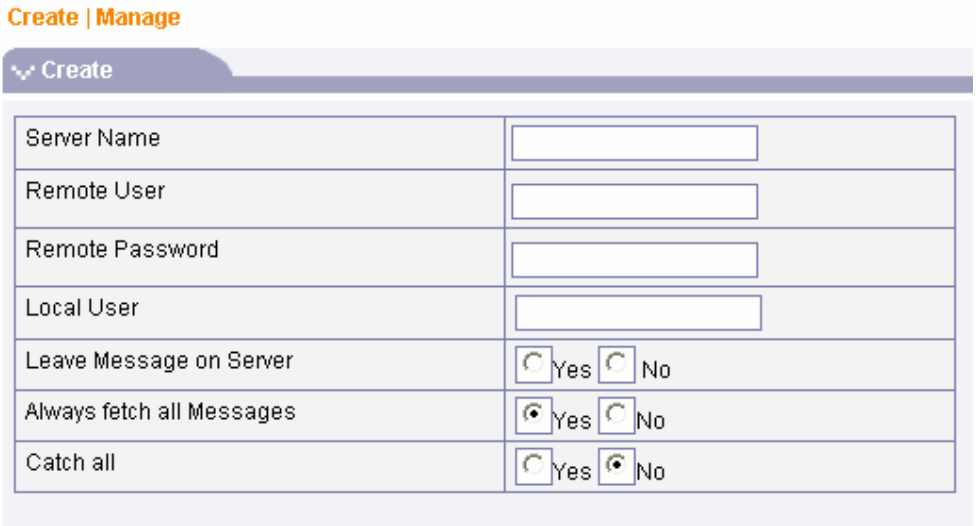
9.2.5 Domain Map

Administrator can do the Domain Mapping & Update it from this utility window

9.4 FETCHMAIL SERVER



What to update picture Create Fetch mail



Administrator can create a Fetchmail server by entering all the details in the respective fields. And click on create.

After the page is refreshed Fetchmail server is ready to fetch mails.

No option is there for automatic startup.

smartguard

Chapter 10

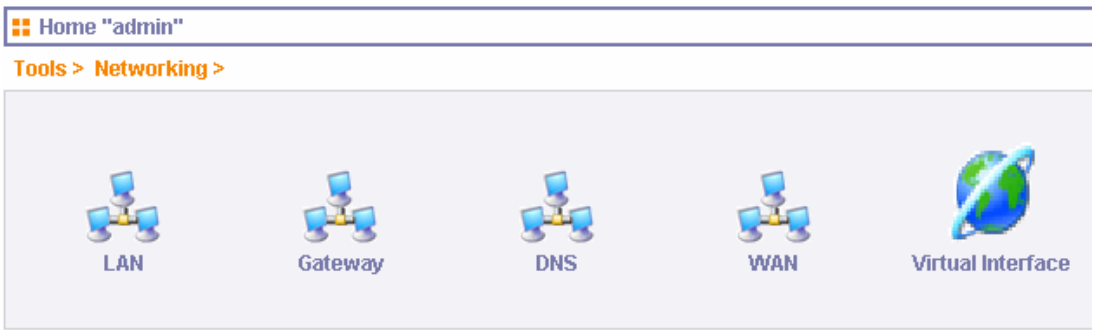
Load Balancing /Multiple ISP /Failover

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

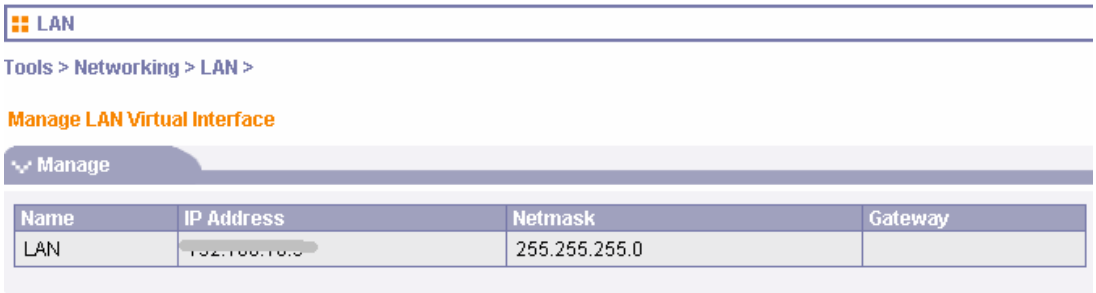
10.3 NETWORKING

STEP **Click on Tools option in left side of main menu → click on networking icon.**



10.3.1 LAN

STEP **Click on Tools option in left side of main menu → click on networking icon → then click on LAN icon.**



LAN ip edit

Manage LAN Virtual Interface

Manage

Name	IP Address	Netmask	Gateway
LAN	192.168.10.9	255.255.255.0	

After click on LAN name for edit following details will be displayed.

Edit

Name	LAN
IP Address	172.16.1.1
Sub Netmask	255.255.255.0
Gateway	

Update

10.3.2 GATEWAY

STEP **Click on Tools option in left side of main menu → click on networking icon → then click on Gateway icon.**

Default Gateway

Tools > Networking > Gateway >

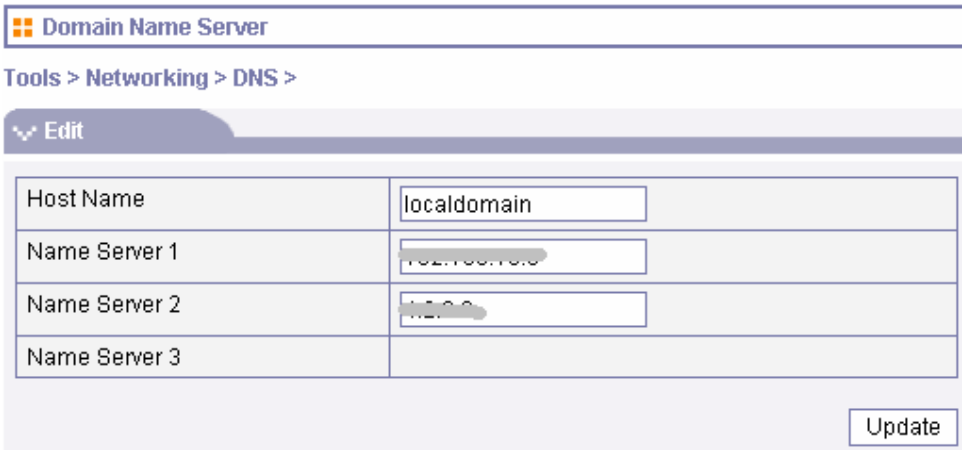
Edit

Networking(eg: Yes/no)	yes
Hostname (eg : localhost.localdomain)	localhost.localdomain
Gateway (eg : 203.195.149.201)	[redacted]

Update

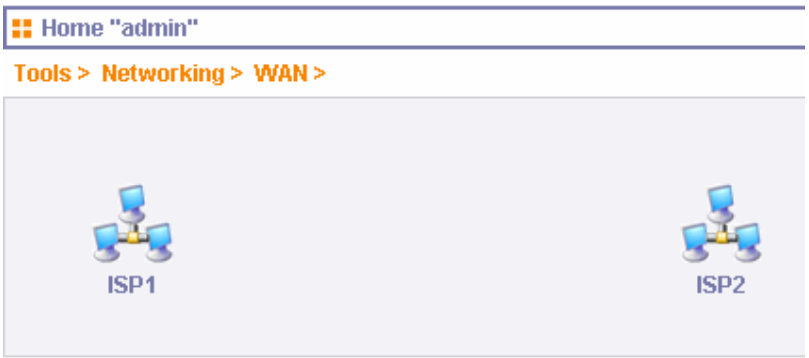
10.3.3 DNS

STEP **Click on Tools option in left side of main menu → click on networking icon → then click on DNS icon.**



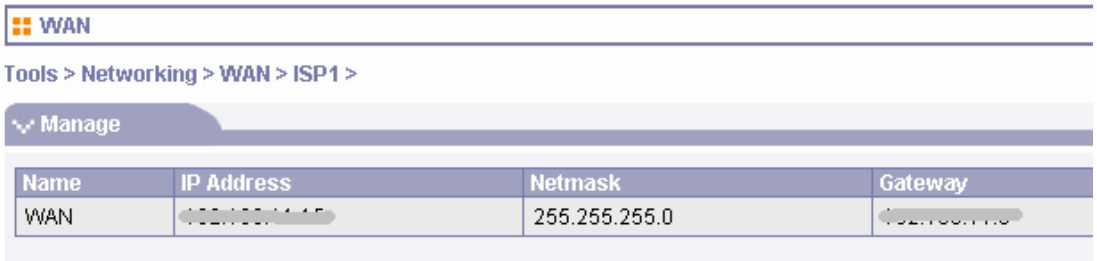
10.3.4 WAN

STEP **Click on Tools option in left side of main menu → click on networking icon → then click on WAN icon.**



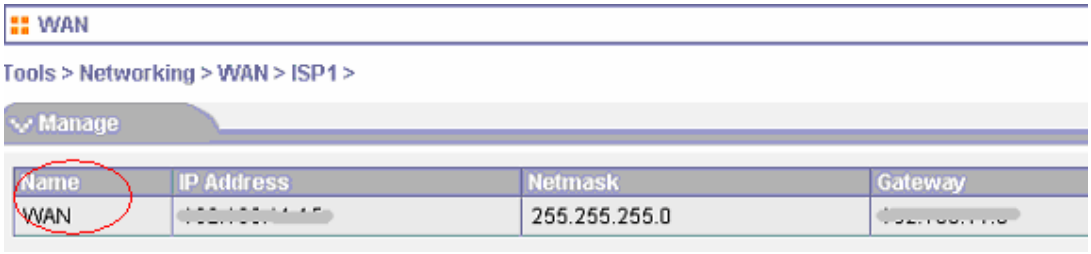
10.3.4.1 ISP 1

STEP **Click on Tools option in left side of main menu → click on networking icon → click on WAN icon → then click on ISP 1 icon.**

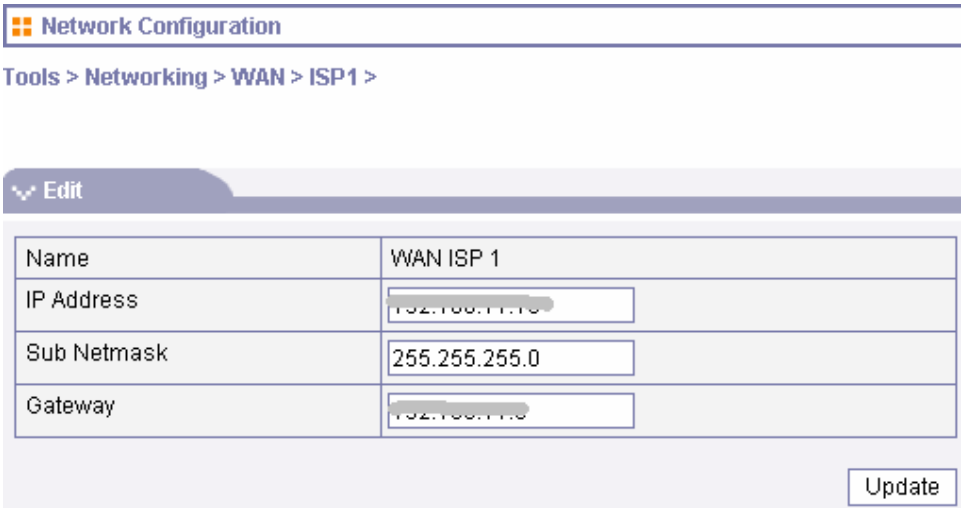


Change ISP1 Settings

STEP **Click on Tools option in left side of main menu → click on networking icon → click on WAN icon → then click on ISP 1 icon → click on WAN option.**



After click on WAN option for edit following option will be displayed.



10.3 NETWORKING

STEP **Click on Tools option in left side of main menu → click on networking icon → click on Virtual interface icon.**

What is bandwidth aggregation?

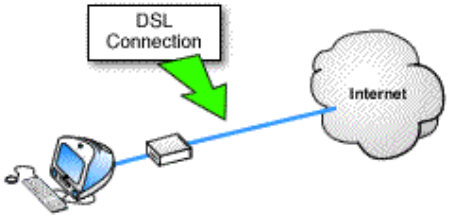


Figure 1: User connected via 256K DSL connection.
For many users broadband connections are either too expensive or simply unavailable.

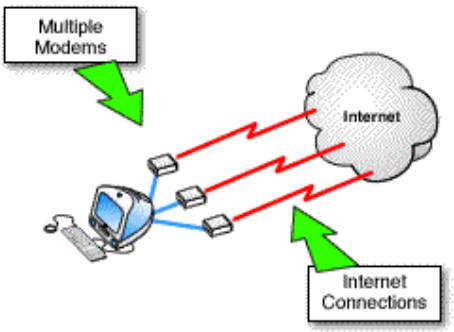


Figure 2: Multiple 56K connections between User and ISP.
The use of multiple modems to achieve aggregate bandwidth equivalent to broadband solutions is both available and affordable to most users today.

The amount of time it takes to download web pages or other information from the Internet depends on a number of factors including Internet access bandwidth limitations, ISP performance restrictions, general Internet congestion and remote host response time. Often, the weakest link in this chain is the bandwidth between your computer and the Internet, also known as Internet access bandwidth. To many Internet users, increasing this bandwidth involves getting a broader bandwidth connection, sometimes at considerable expense. If no low cost broadband alternative is available in your area, the only way forward from a 56Kbps modem is ISDN or leased line. Both of these alternatives can be very costly.

It is possible however to have more than one connection between your computer and the Internet, and to combine them to accumulate bandwidth. Techniques that accomplish this task are collectively referred to in this document as "bandwidth aggregation". Although bandwidth aggregation may occur in many different contexts, the scope of this document is limited to the aggregation of Internet access bandwidth. Two techniques will be examined in detail, Multilink and Connection Teaming.

2. What is bonding?

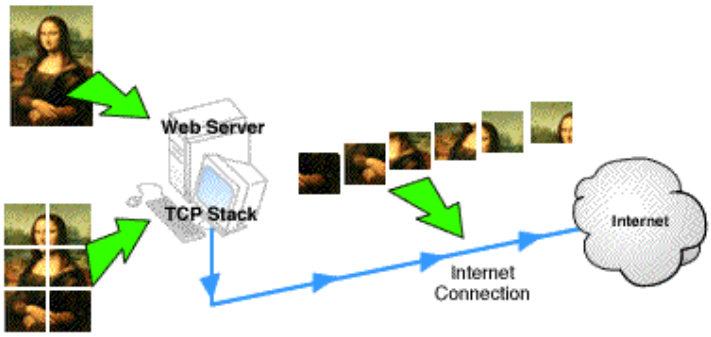


Figure 3: Data Packets.
Data is broken up into manageable packets for Internet delivery.

Multiple bonded connections behave like a single connection. Suppose for example that a web server sends an image to a web browser. This image would be broken up into several packets by the server operating system because a single packet would be much too large for routers and network components to handle.

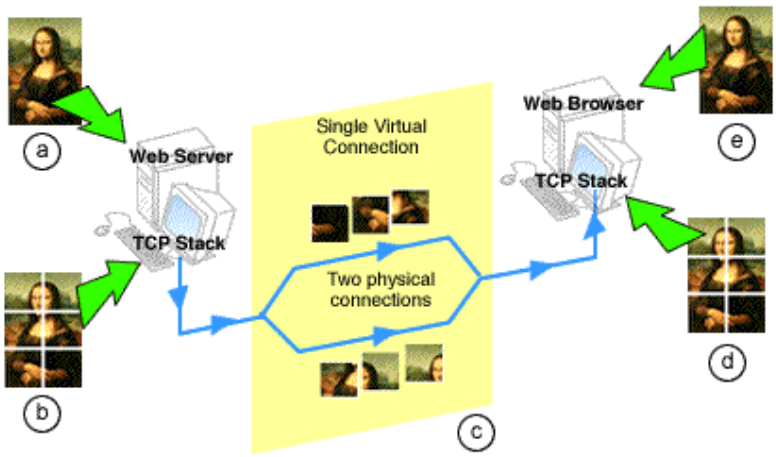


Figure 4: Component links are bonded.
a) Web server sends image to web browser.
b) TCP stack on web server computer breaks data into packets for delivery.
c) Packets are delivered to web browser over bonded link.
d) TCP stack on web browser computer reassembles packets into image.
e) Web browser displays image.

If part of the route between the server and the browser were composed of bonded multiple links, the packets that made up the image could alternately travel over one or the other of the component links. Neither the web server nor the web browser would be aware of this. From a functional point of view there is only one link. The component links are said to be bonded.

3. What is PPP Multilink?

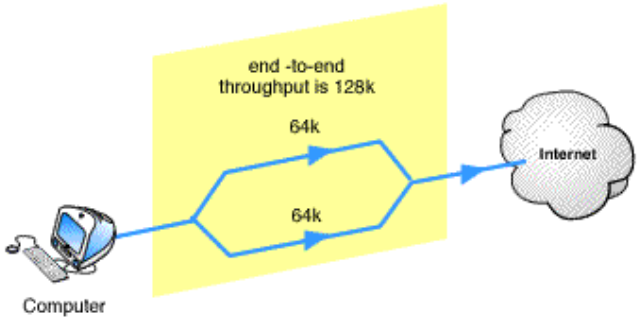


Figure 5: PPP Multilink.
PPP Multilink can give you aggregate bandwidth equal to the sum of the individual physical connections.

The PPP Multilink Protocol (MP) is an extended version of PPP (Point to Point Protocol). It has the ability to bond two or more simultaneous parallel connections. The resulting virtual connection has bandwidth equal to the sum of the separate connections.

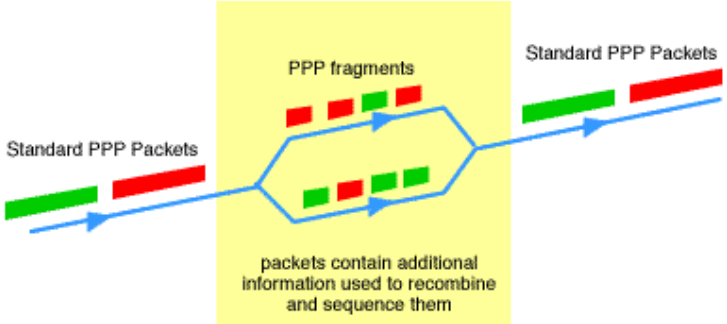


Figure 6: Recombination of PPP Packets.
PPP Packets contain information used to recombine and sequence them.

MP may fragment the packets if needed to meet the MTU (Maximum Transmit Unit) value, or alternatively send whole packets over the available links. MP transmits each individual packet or fragment along the first available link, along with extra information to enable the receiving end to recombine the fragments into a single packet for onward routing.

MP is a form of bandwidth aggregation that involves bonding. It is a non-proprietary TCP/IP standard defined in RFC 1990.

4. How does PPP Multilink work?

PPP Multilink splits a single PPP connection into two separate physical links, then recombines them in the correct sequence. To accomplish this it is necessary to have an MP compliant hardware device or software program at either end of the link. The functions performed by MP are as follows:

- originating MP receives packets
- optionally fragments them
- determines which is the next available link
- adds a PPP Multilink header containing sequencing and other information
- forwards packet or packet fragments over available links
- receiving MP receives packets or packet fragment
- removes MP header
- reconstitutes fragments into whole packets
- forwards packets to IP address

The result is a smooth distribution of traffic over available links even when they vary considerably in capacity or when available bandwidth fluctuates greatly.

5. What are the limitations of PPP Multilink?

Because PPP Multilink uses bonding, all the bonded links must originate and terminate on the same pair of endpoints so that they can split and recombine the data streams. Both the endpoints must use PPP Multilink.

In plain terms, this means that to use Mulitilink PPP, your ISP must have hardware or software that supports Multilink for the type of connection you are using and must offer this service to their subscribers. Not all connection types are supported. You may be using MP over a particular type of modem but your ISP may not have the corresponding hardware. Most ISDN enabled ISPs offer MP to bond the two B channels. Many offer bonding of V.90 modems as well. If you wish to bond any other connection type such as DSL, this can be done with very expensive hardware routing solutions, but these are not within the reach of most end users, and few ISPs support them.

To the best of our knowledge at the time of this writing, the majority of ISPs do not have any support for PPP Multilink with any type of connection other than ISDN.

6. What are the advantages of PPP Multilink?

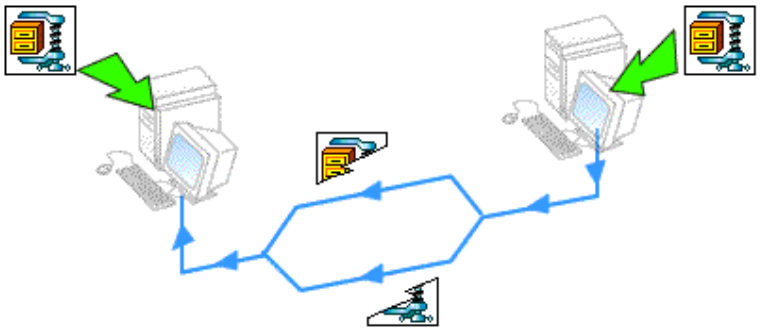


Figure 7: Protocols with a single connection will benefit from Multilink Transparency.

The major advantage of PPP Multilink is that it is a public standard, and therefore offers interoperability among vendors, in theory at least. It also has the benefit that even a single TCP/IP connection, for example an FTP download, can take advantage of multiple links. If you download a file over a PPP Multilink connection with two identical bonded links, the file will download twice as fast. Neither the FTP client nor the server will be aware that there is a Multilink connection in the middle. Similarly, any protocol that requires a single connection between host and client, such as terminal emulation, will benefit from bandwidth aggregation offered by Multilink because of this transparency.

7. What is Connection Teaming?

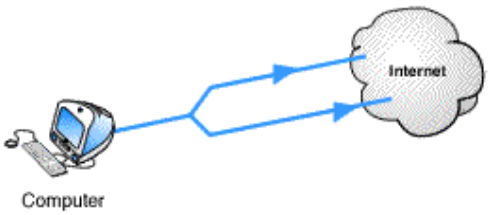


Figure 8: PPP Multilink and Connection Teaming.
Unlike PPP Multilink, Connection Teaming links are not terminated on pairs of end points.

Connection Teaming is a form of bandwidth aggregation that does not bond links. It sets up and maintains individual TCP/IP sessions along multiple links using standard protocols. A Connection Teaming server between the LAN and the Internet receives requests from LAN clients and forwards them along the next available connection. LAN browsers and other clients do not need to know which connection is used to forward their requests to the Internet. Unlike bonded links, however, individual requests are not split across multiple links then recombined again. Each request must follow one of the available data paths.

8. How does Connection Teaming work?

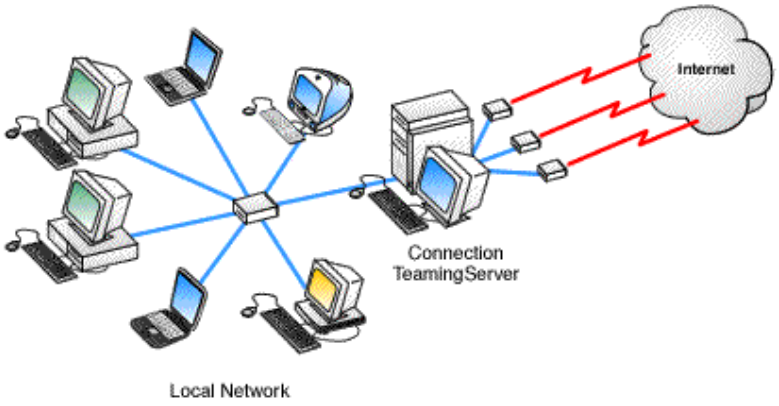


Figure 9: Connection Teaming creates a significant increase in effective throughput.

A Connection Teaming server is situated on the user's LAN, as part of the routing software between the user and the Internet. When a TCP session is opened, the server uses the link with the lowest amount of traffic. The many HTTP, FTP or other TCP sessions that are opened by LAN computers are distributed to all of the available connections this way. The result is a relatively even distribution of Internet traffic across the available links, and a significant increase in effective throughput.

9. What are the limitations of Connection Teaming?

The primary limitation of Connection Teaming comes from the fact that it does not split up individual requests. A single user downloading a large file will not experience any improvement with Connection Teaming. Some teaming solutions do allow FTP delivery over multiple links. This would not apply however, to a single large graphic delivered via HTTP.

10. What are the advantages of Connection Teaming?

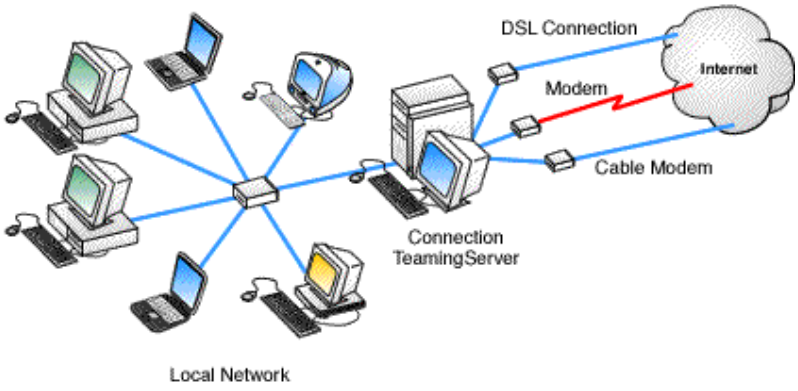


Figure 10: Connection Teaming allows a combination of cable modems, DSL and older modems.

Connection Teaming can use different connection technologies. It is possible combine older modems with your current ones, and to combine analog modems with DSL, or cable modems.

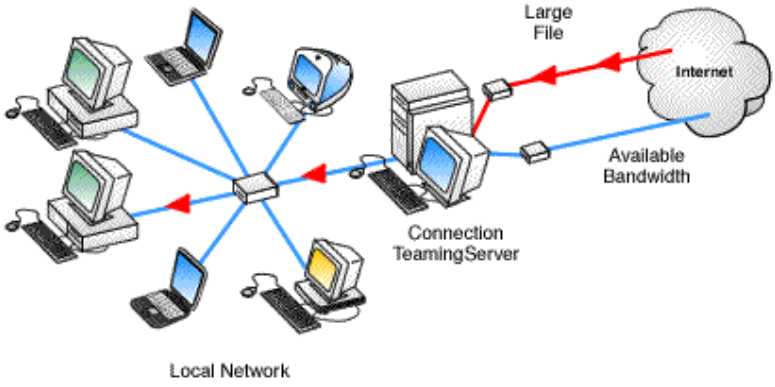


Figure 11: Connection Teaming can share the load when there are multiple concurrent TCP/IP connections.

Connection Teaming is an effective way to share load whenever there are multiple concurrent TCP/IP connections. For example, if one user sets up an FTP download connection it can only use one of the links, but this leaves the other links available for other user connections.

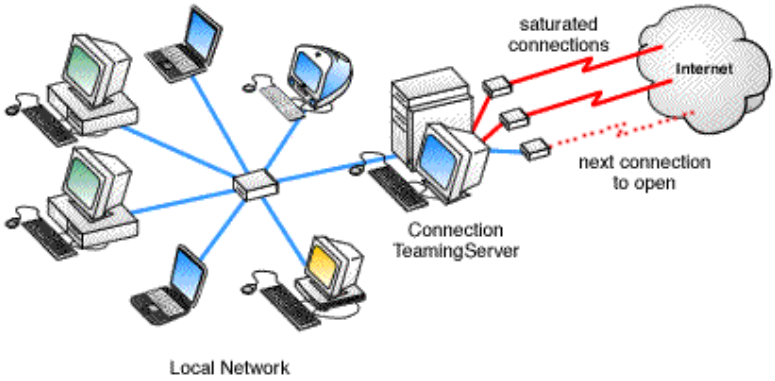


Figure 12: Connection Teaming can open additional connections on demand.

Connection Teaming can open additional connections on demand, for example when saturation of existing open bandwidth reaches 80%, or when a specific route is solicited.

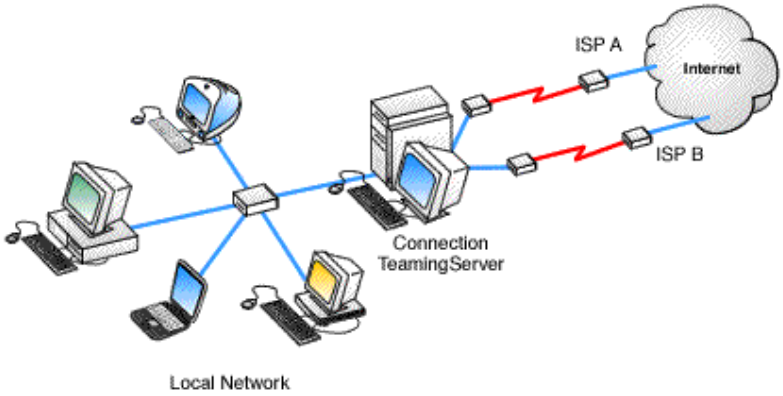


Figure 13: Each link behaves like a separate Internet Connection.

Connection teaming allows the teamed links to connect to separate Internet access points, or to separate ISPs. It is therefore not necessary to find a compliant ISP. Each link behaves like a separate, independent Internet connection, so the upstream service providers do not need to know that your system is using teaming, nor do they require any special protocol or subscription options.

11. Is Connection Teaming worthwhile for a single Internet user?

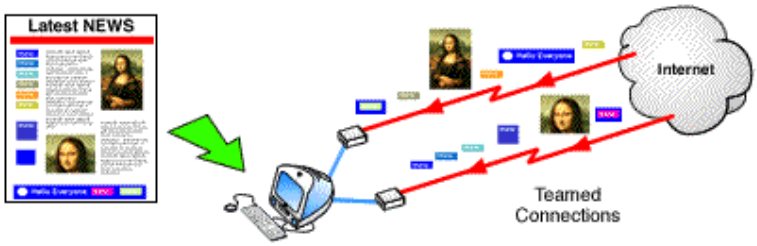


Figure 14: Delivering individual page elements over Teamed Connections.

Possibly.

Web pages are composed of dozens of individual graphical items. Each of these items involves a separate HTTP request. Each request can be delivered over a separate link. Therefore, it is possible a single user browsing the Web will experience performance gains through the use of Connection Teaming, but this depends on the sites you visit, the types of connections to the Internet you are using and your ISP.

Please be aware that a product such as the SmartGuard InterGate is designed for a network of machines, i.e. multiple people accessing the Internet at the same time rather than just one machine.

smartguard

Chapter 11

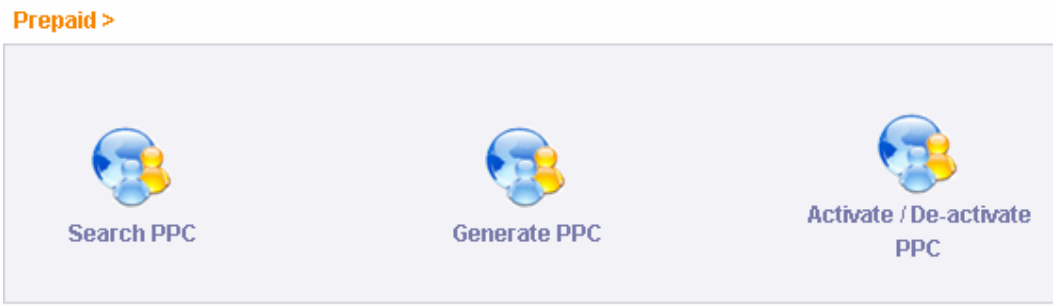
Pre-Paid Coupons (PPC)

XS Infoways
the invincible technology

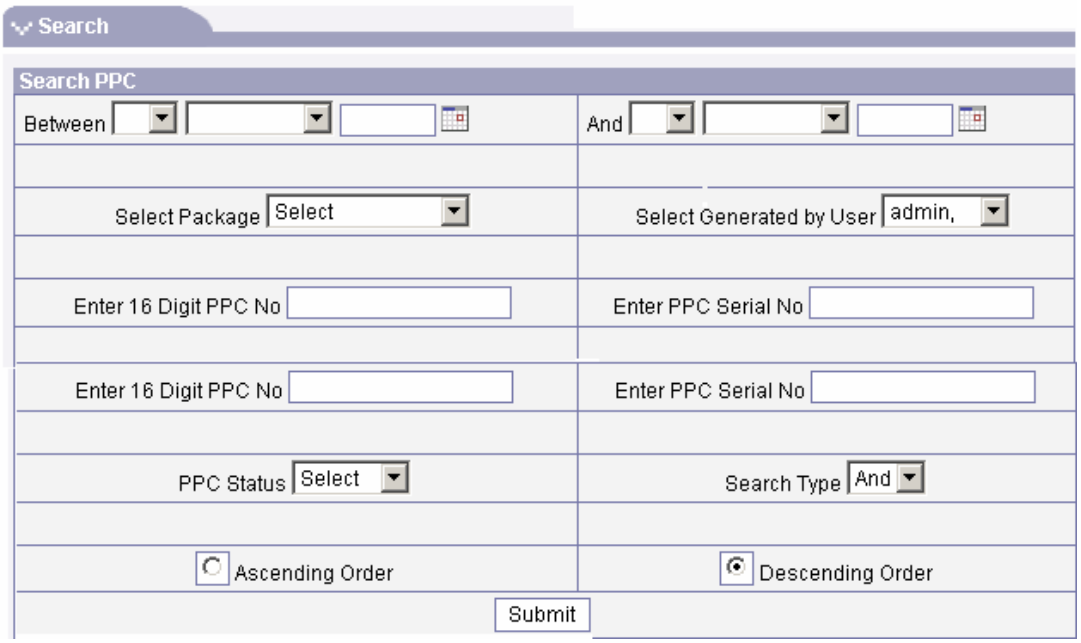
ver. **4.0.4**
Updated:06/27/2006

11. Pre Paid Coupons

All the PPC`s configurations will be done by the reseller from this menu.



Search PPC



From this menu Reseller can search the desired PPC by mentioning specific time duration , Package , User Who Generated PPC , PPC Number , PPC status , Search PPC and Submitting it.

Generate PPC

Prepaid > Generate PPC >

View Logs

Package Name	Used PPC	Un - Used PPC	Total PPC
32Kbps NIGHT	0	0	0
32kbps home	0	0	0
64Kbps	6	0	9
1 hour	7	0	7
56 bandwidth pol	0	0	0

From this PPC list reseller can monitor Package Wise Used, Unused and Total number of PPC`s

Generate PPC

Generate PPC for Package	Number of ID
32Kbps NIGHT / Charges - 2400 INR [Details]	

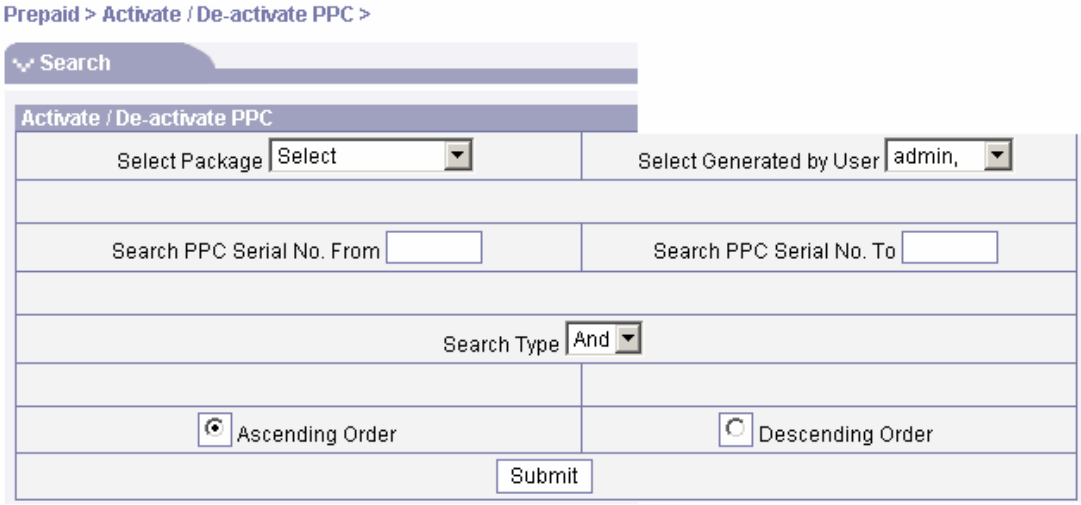
Balance	Amount
Total Payment	711 INR
Total Invoice	837 INR
Credit Note	44 INR
Debit Note	56 INR
Credit Limit	500 INR
Current Balance	-138 INR
Available Credit Limit	406 INR

Generate PPC

From this Menu reseller can generate the number of PPC`s depending upon the current balance & available credit limit.

***Note:* Reseller will not be able to generate PPC`s in case no advance payment is made to ISP or there is no balance or credit limit available for it.**

Activate/De-activate PPC



From this menu Reseller can Deactivate/activate the earlier generated pre-paid coupons (PPC`s)

smartguard

Chapter 12

Tools

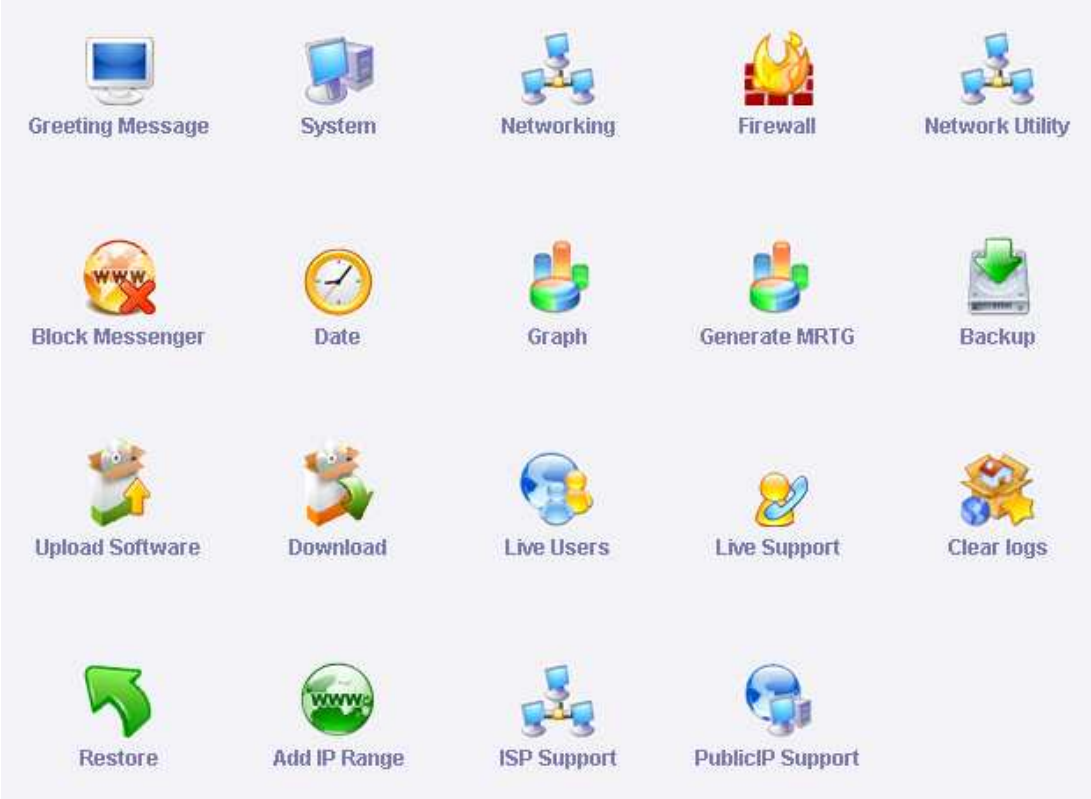
XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

12. TOOLS

STEP **Click on Tools option in left side of main menu.**

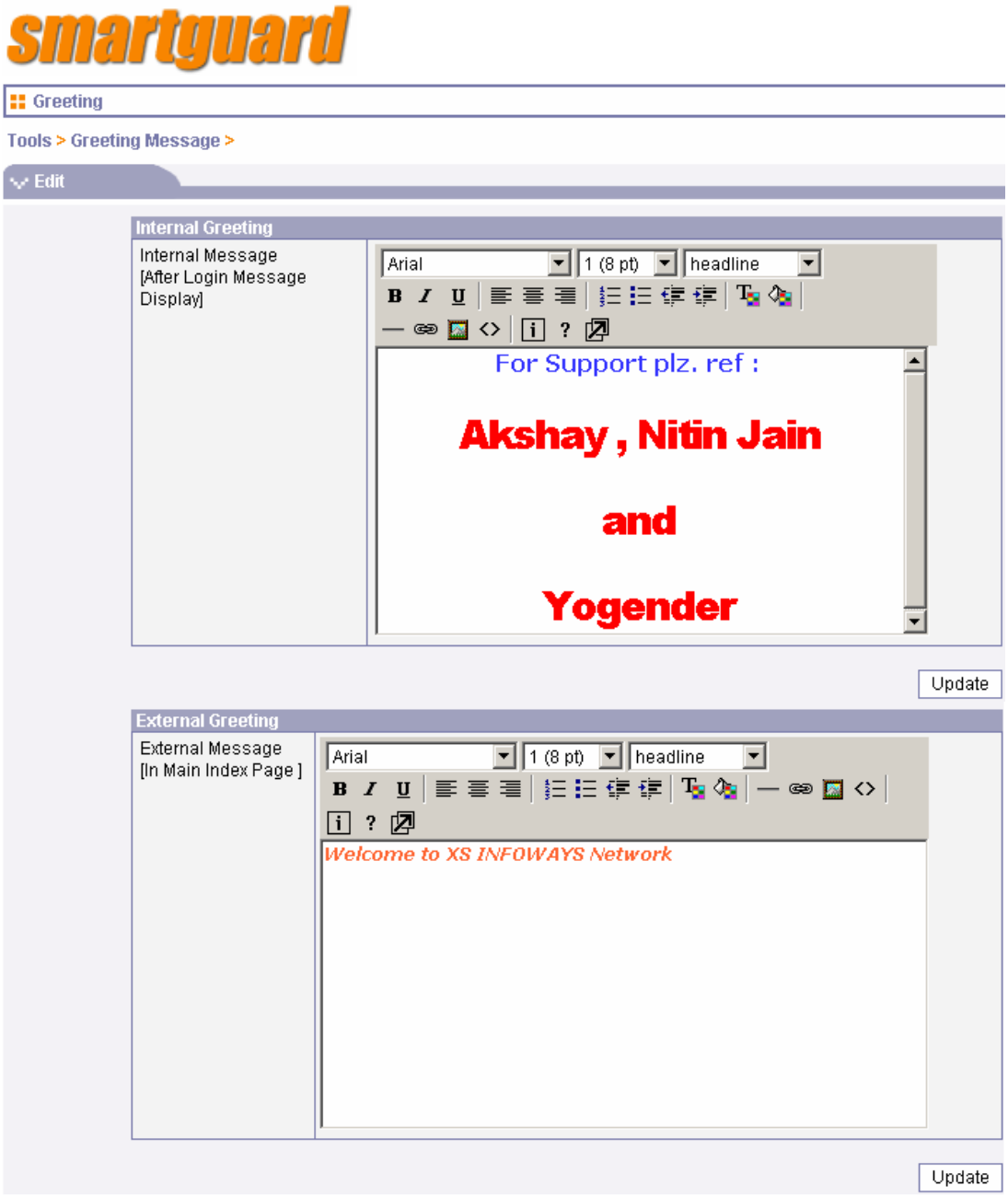
When you click on Tools it will show you options as displayed below:



12.1 GREETING MESSAGE

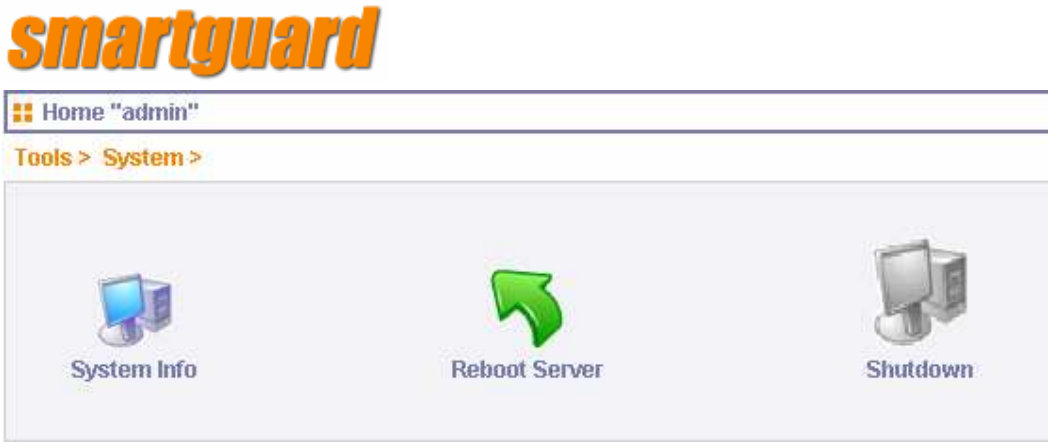
STEP **Click on Tools option in left side of main menu → click on greeting message icon.**

If you want to change login message then click on greeting message option.



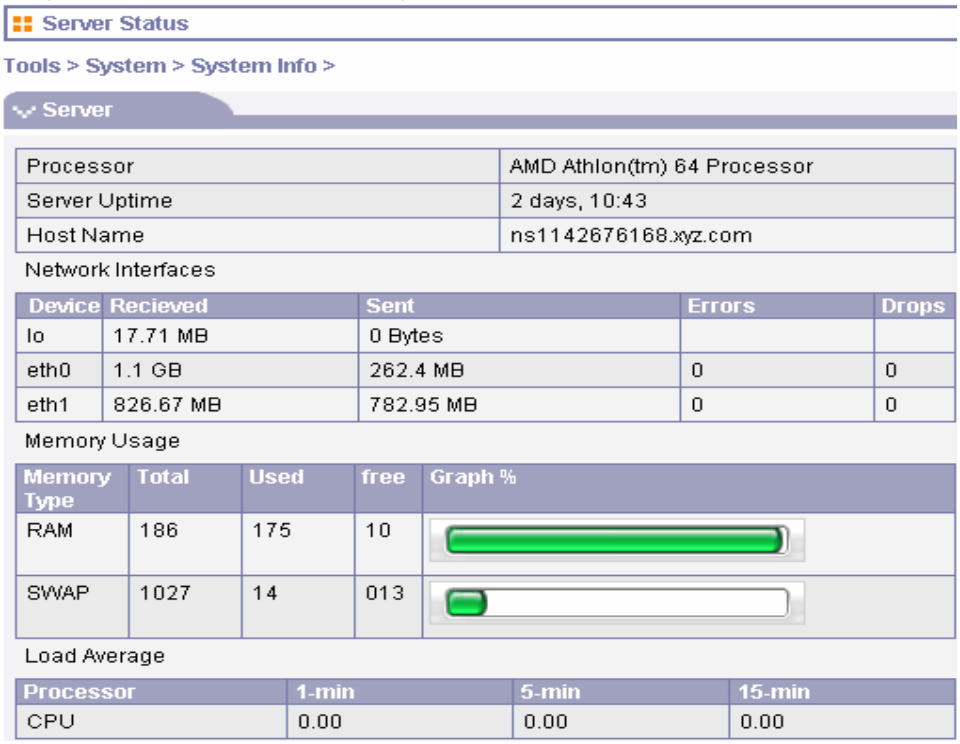
12.2 SYSTEM

STEP **Click on Tools option in left side of main menu → click on System icon.**



12.2.1 System Info

STEP **Click on Tools option in left side of main menu → click on System icon → click on system info.**



Processor	AMD Athlon(tm) 64 Processor
Server Uptime	2 days, 10:43
Host Name	ns1142676168.xyz.com

Network Interfaces

Device	Recieved	Sent	Errors	Drops
lo	17.71 MB	0 Bytes		
eth0	1.1 GB	262.4 MB	0	0
eth1	826.67 MB	782.95 MB	0	0

Memory Usage

Memory Type	Total	Used	free	Graph %
RAM	186	175	10	
SWAP	1027	14	013	

Load Average

Processor	1-min	5-min	15-min
CPU	0.00	0.00	0.00

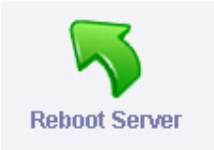
Mounts

Mount Point	Size	Available	Used	Used %	Graph %
/dev/sda2	72G	66G	2.6G	4%	
/dev/sda1	190M	172M	8.4M	5%	
none	94M	94M	0	0%	
/dev/sda5	1012M	921M	40M	5%	

Server Status

Server Name	Status	Stop	Restart
squid			
httpd			
dhcpd			
MailScanner			
mysql			

12.2.2 Reboot Server



STEP **Click on Tools option in left side of main menu → click on System icon → click on Reboot server icon.**

Reboot
Click this icon system restart now.

12.2.3 Shutdown

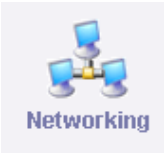
STEP **Click on Tools option in left side of main menu → click on System icon → click on shutdown icon.**

Shutdown

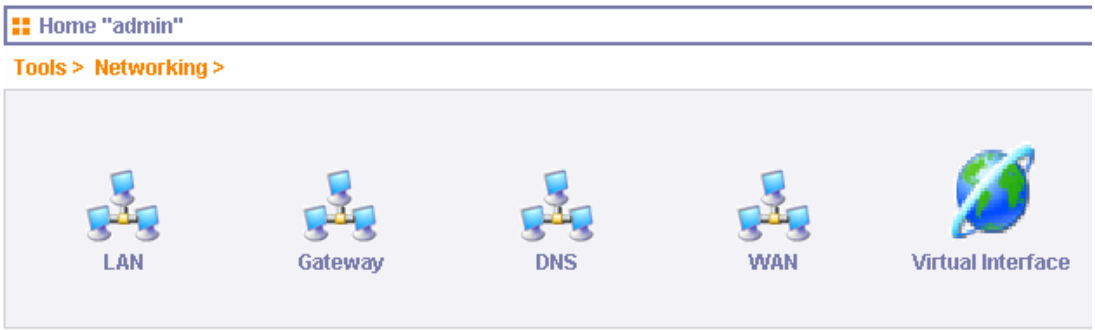
Click this icon system shutdown now.

Networking

12.3 NETWORKING

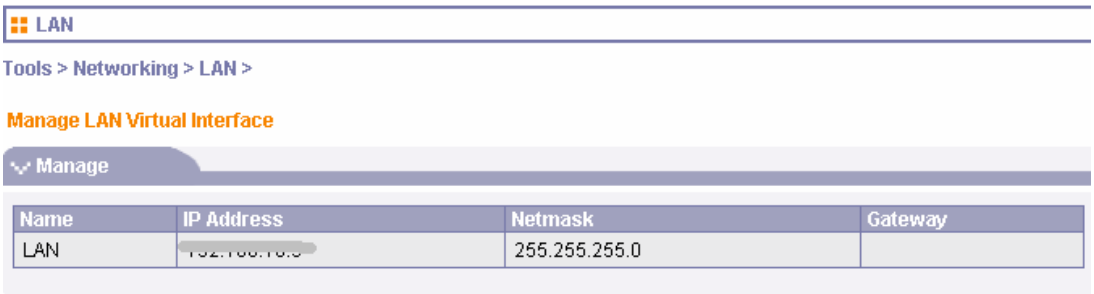


STEP **Click on Tools option in left side of main menu → click on networking icon.**



12.3.1 LAN

STEP **Click on Tools option in left side of main menu → click on networking icon → then click on LAN icon.**



LAN ip edit

Manage LAN Virtual Interface

Manage

Name	IP Address	Netmask	Gateway
LAN	192.168.10.9	255.255.255.0	

After click on LAN name for edit following details will be displayed.

Edit

Name	LAN
IP Address	172.16.1.1
Sub Netmask	255.255.255.0
Gateway	

Update

12.3.2 GATEWAY

STEP **Click on Tools option in left side of main menu → click on networking icon → then click on Gateway icon.**

Default Gateway

Tools > Networking > Gateway >

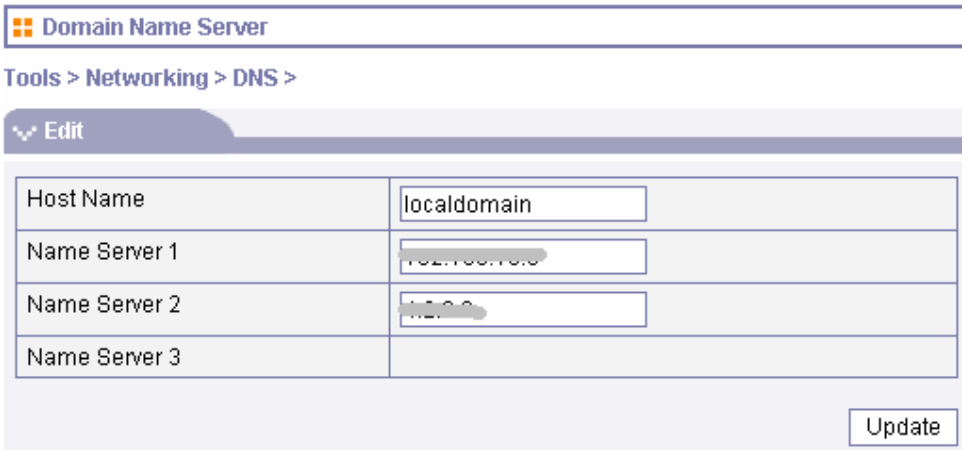
Edit

Networking(eg: Yes/no)	yes
Hostname (eg : localhost.localdomain)	localhost.localdomain
Gateway (eg : 203.195.149.201)	[redacted]

Update

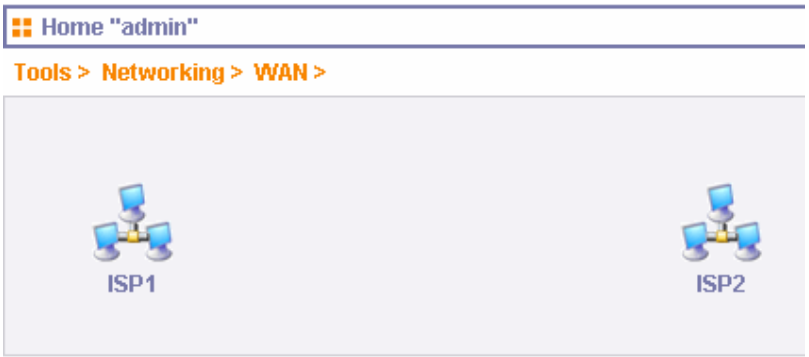
12.3.3 DNS

STEP **Click on Tools option in left side of main menu → click on networking icon → then click on DNS icon.**



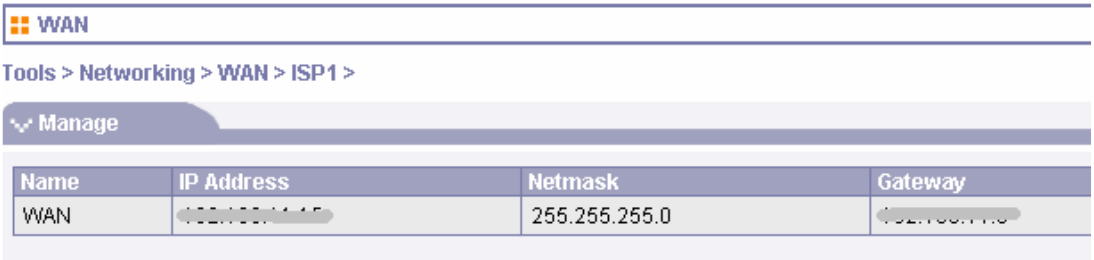
12.3.4 WAN

STEP **Click on Tools option in left side of main menu → click on networking icon → then click on WAN icon.**



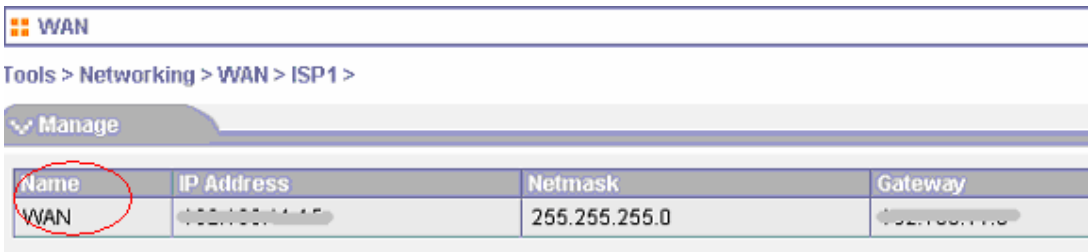
12.3.4.1 ISP 1

STEP **Click on Tools option in left side of main menu → click on networking icon → click on WAN icon → then click on ISP 1 icon.**

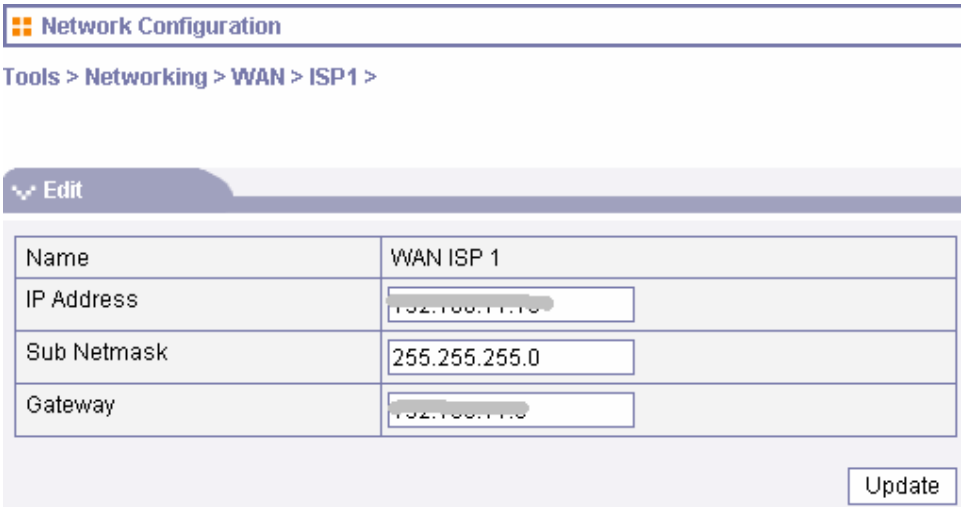


Change ISP1 Settings

STEP **Click on Tools option in left side of main menu → click on networking icon → click on WAN icon → then click on ISP 1 icon → click on WAN option.**



After click on WAN option for edit following option will be displayed.

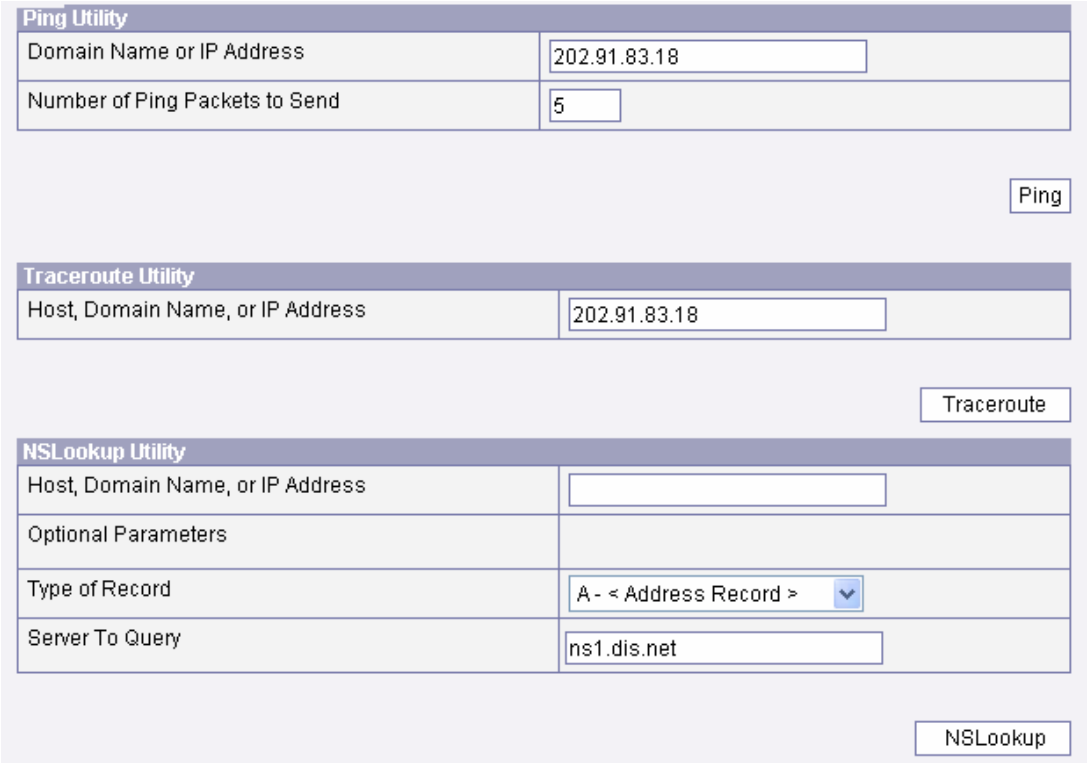


12.3.5 VIRTUAL INTERFACE

STEP **Click on Tools option in left side of main menu → click on networking icon → click on Virtual interface icon.**

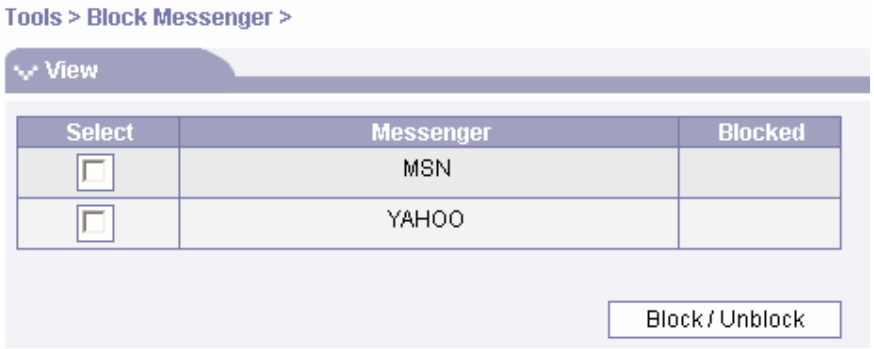
12.5 NETWORK UTILITIES

STEP **Click on Tools option in left side of main menu → click on Network utility icon.**

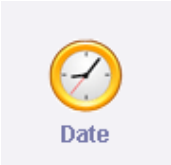


12.6 BLOCK MESSENGER

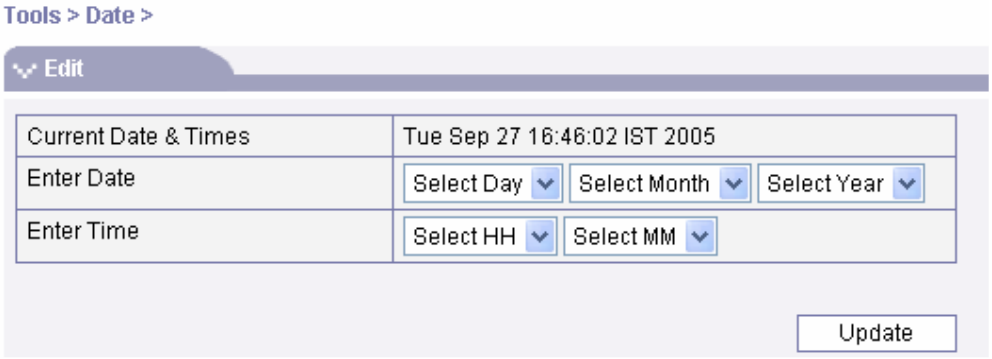
STEP **Click on Tools option in left side of main menu → click on Block messenger icon.**



12.7 TIME



STEP **Click on Tools option in left side of main menu → click on Date icon.**



smartguard

Chapter 13

Server Management

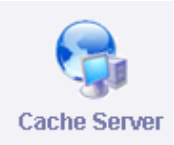
XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

13. SERVER MANAGEMENT

On clicking on server management administrator will be directed to the following page:

13.1 CACHE SERVER



Cache (pronounced kash) is a collection of data duplicating original values stored elsewhere , where the original data are expensive (usually in terms of Access Time/ Bandwidth Consumption) to fetch or compute relative to reading the cache. Once the data are stored in the cache, future use can be made by accessing the cached copy rather than refetching or recomputing the original data, so that the average access time is lower.

SMARTGUARD CACHING ENGINE caches web documents accessed providing plus points to an enterprise as :

* Reduced Bandwidth Consumption (cached page fetched locally)
* Speedy Downloads
* Reduced Requests to web hence less load on network.

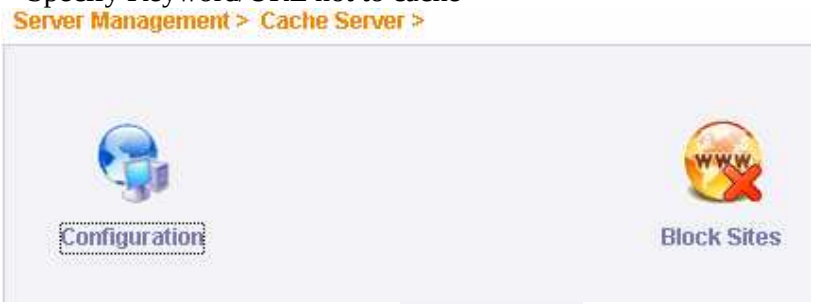
In Smartguard Caching Engine Web documents retrieved may be stored (cached) for a time so that they can be conveniently accessed if further requests are made for them. The issue of whether the most up-to-date copy of the file is retrieved is handled by the caching program which initially makes a brief check and compares the date of the file at its original location with that of the copy in the cache. If the date of the cached file is the same as the original, then the cached copy is used.

Smartguard maintain a cache of retrieved documents and this cache is used for retrievals where possible. In addition, the user may configure particular request to point to a

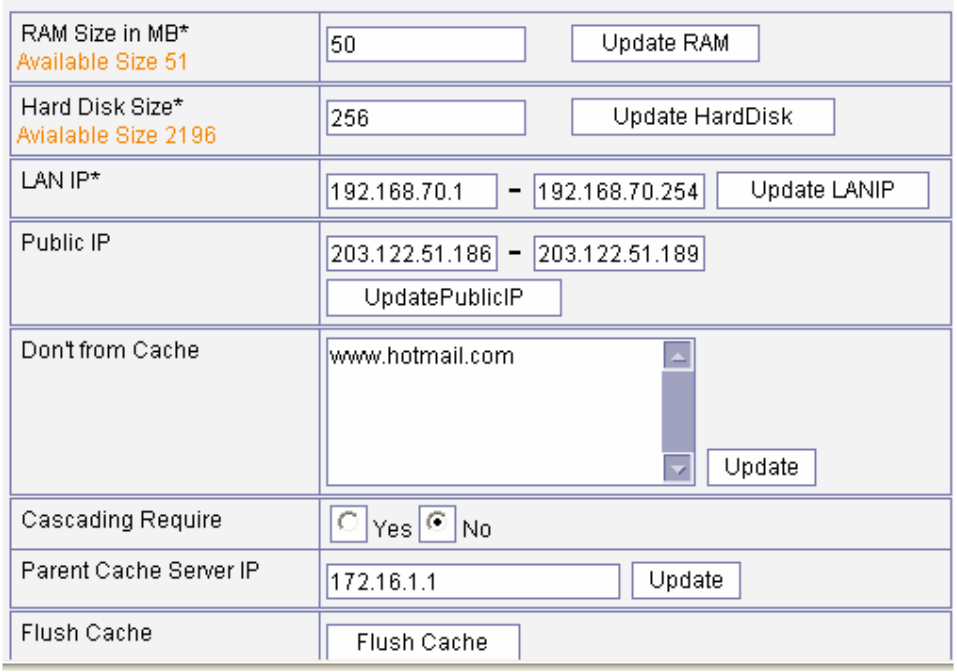
caching server or request should go directly to the web. The caching server would supply the files from its cache if they were current, or pass on the request to the originating server if they were not.

SmartGuard caches all sites visited by Subscribers locally in to the server's hard drive. Caching not only serve the pages faster but also saves expensive Bandwidth. Caching can be configured at the package level, so it is possible for the administrator to bypass caching server for some Subscribers. SmartGuard Cache Server Administrator can also

- Modify Cache Memory and Hard Drive Space
- Specify Keyword/URL not to cache



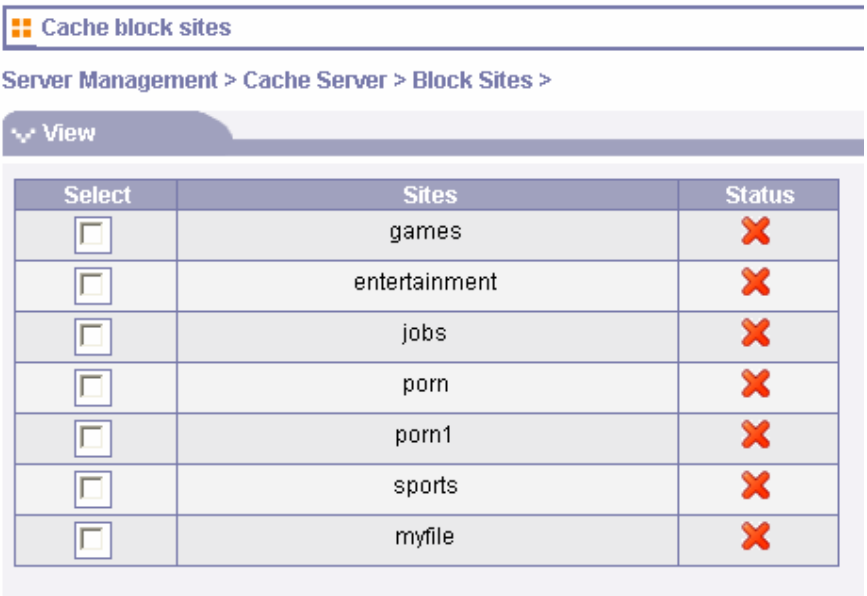
13.1.1 Configuration



Administrator can update and edit Cache Ram, HDD Size, LAN IP series, Public IP series and all other configurations.

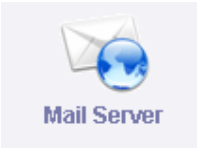
13.1.2 Block Sites

Administrator can select the various groups for blocking sites as mentioned in the menu given below. Administrator just needs to click the specific group and mention the list of sites it wants to get blocked / Unblocked.



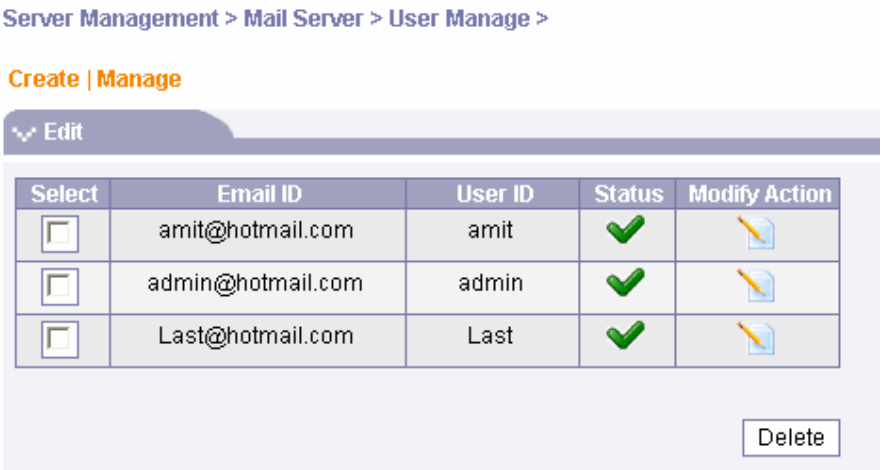
Select	Sites	Status
	games	
	entertainment	
	jobs	
	porn	
	porn1	
	sports	
	myfile	

13.2 MAIL SERVER



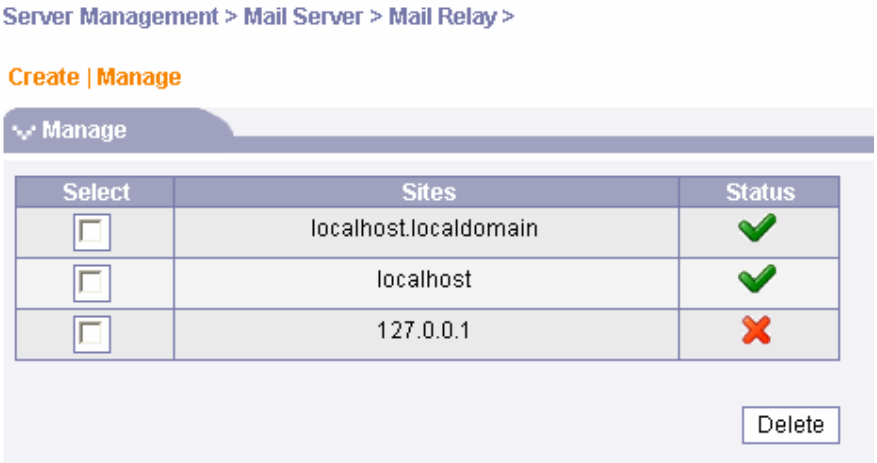
13.2.1 User Manage

At this page administrator can view the status of mail users and also create , edit and delete the mail accounts.



Create user page

13.2.2 Mail Relay



Administrator can manage and set the Mail Relay at this page.
Create relay page

13.2.3 Spam Configuration

Server Management > Mail Server > Spam Configuration >

Spam Configuration

Name	Value
Quarantine Virus Infections	(•) Enable ( ) Disable
Quarantine Silent Viruses	(•) Enable ( ) Disable
Quarantine Whole Message	( ) Enable (•) Disable
Quarantine Whole Message As Queue Files	( ) Enable (•) Disable
Detailed Spam Report	(•) Enable ( ) Disable
Include Scores In SpamAssassin Report	(•) Enable ( ) Disable
Notify Senders	(•) Enable ( ) Disable
Notify Senders Of Viruses	( ) Enable (•) Disable
Send Notices	(•) Enable ( ) Disable
Notices To Admin Email Id	postmaster
Spam Checks	(•) Enable ( ) Disable
Spam Lists To Reach High Score	3
Required SpamAssassin Score	6

Administrator can do all the spam configurations from here on its server. All the virus definitions, Spams, Quarantines can be done with a single click from this window.

13.2.4 Web mail

Server Management > Mail Server > Webmail >

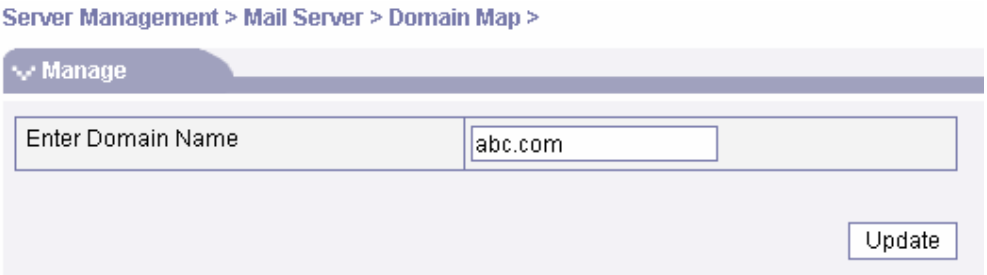
Edit Server Name

Name	Value
Mail Domain Name	

Update

Administrator can Define & Update the Mail Domain Name from this window.

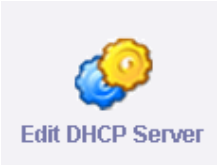
13.2.5 Domain Map



Administrator can do the Domain Mapping & Update it from this utility window

13.3 DHCP SERVER

13.3.1 Edit DHCP Server



DHCP Support	
DHCP Support	Yes No
Description	dhcpd is stopped

Update

DHCP	
Network	192.168.70.0
Sub Netmask	255.255.255.0
Gateway	192.168.70.1
DNS1	192.168.70.1
DNS2	202.91.83.27
DNS3	172.16.1.1
IP Range To	192.168.70.200
IP RangeFrom	192.168.70.254

Update

The DHCP server support can be disabled / enabled from this window.

Administrator just needs to define the IP range for DHCP Server and the other required network information in the respective fields.
By clicking on Update every entry done will be configured.

13.3.2 Add User Mac ID

DHCP Management

Server Management > DHCP > Add User Mac ID >

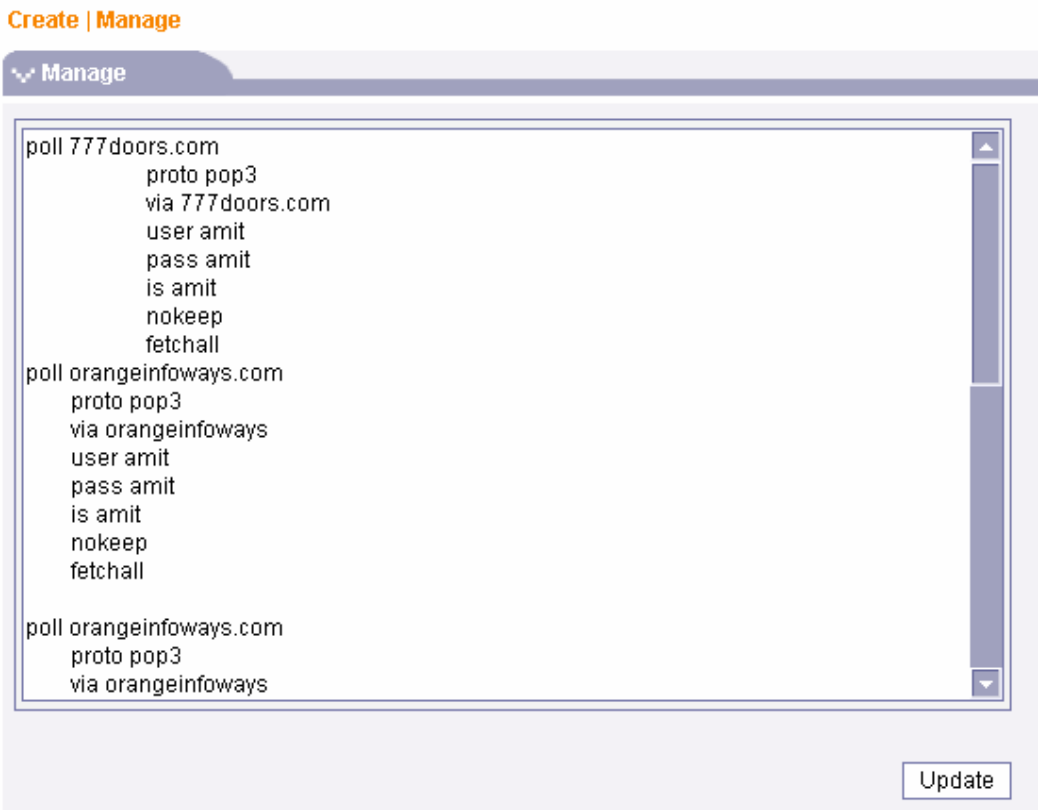
Add User Mac ID

Add User	
User [Machine] Name	

DHCP Server User Details	
Hardware Address [MAC ID]	
Client IP Address	

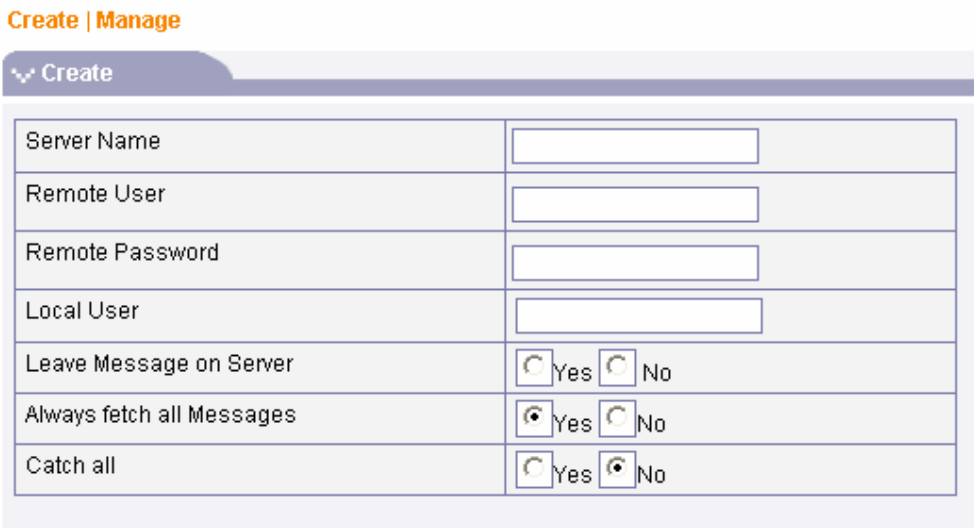
Add

13.4 FETCHMAIL SERVER



What to update picture

Create Fetch mail



Administrator can create a Fetchmail server by entering all the details in the respective fields. And click on create.
After the page is refreshed Fetchmail server is ready to fetch mails.

No option is there for automatic startup.

smartguard

Chapter 14

Services

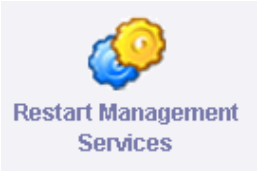
XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

14. SERVICES

In this menu administrator has two options:

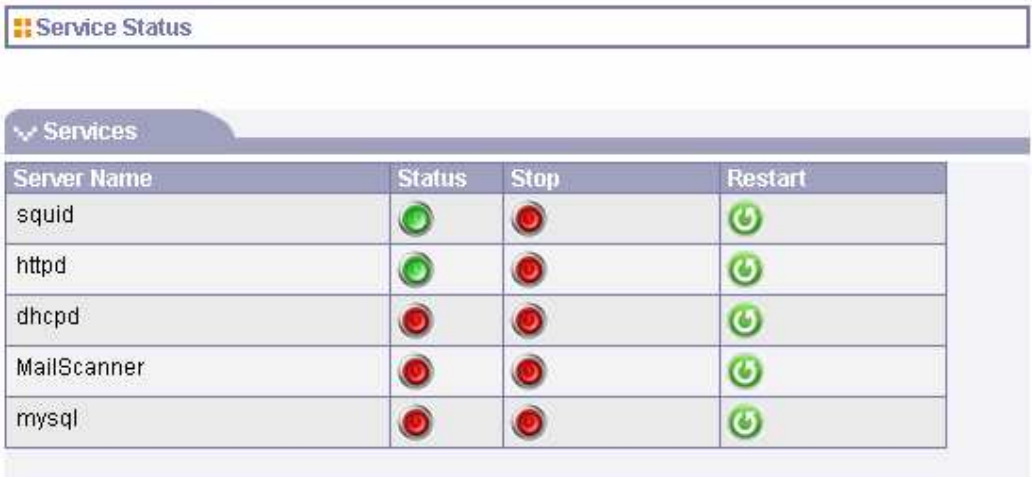
14.1 RESTART MANAGEMENT SERVICES



On clicking this icon all the management services currently running on server will get restarted.

14.2 SERVICES STATUS

You can view the status of management services from here and administrator can also restart or stop any service at a single click as shown in figure



smartguard

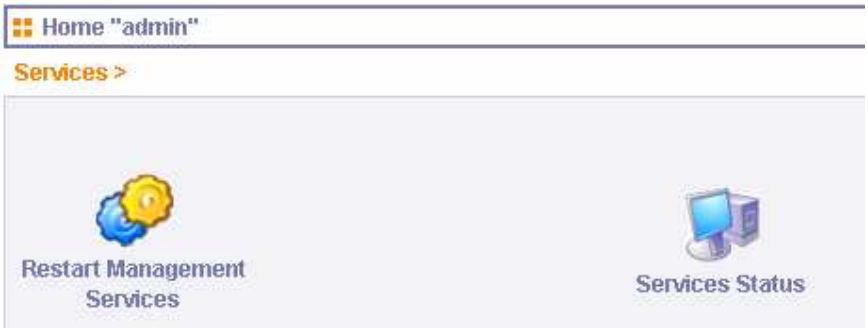
Chapter 15

Restore and Backup

XS Infoways
the invincible technology

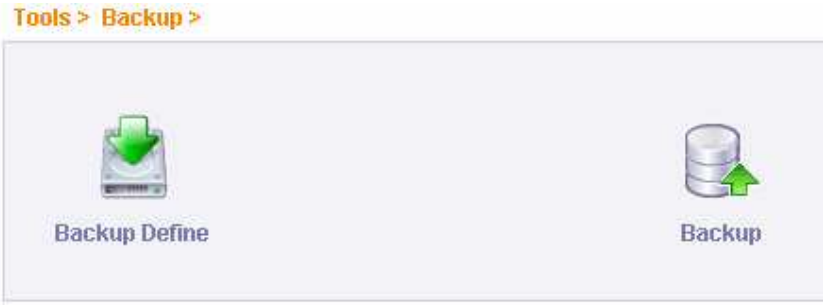
ver. **4.0.4**
Updated:06/27/2006

15. Backup And Restore



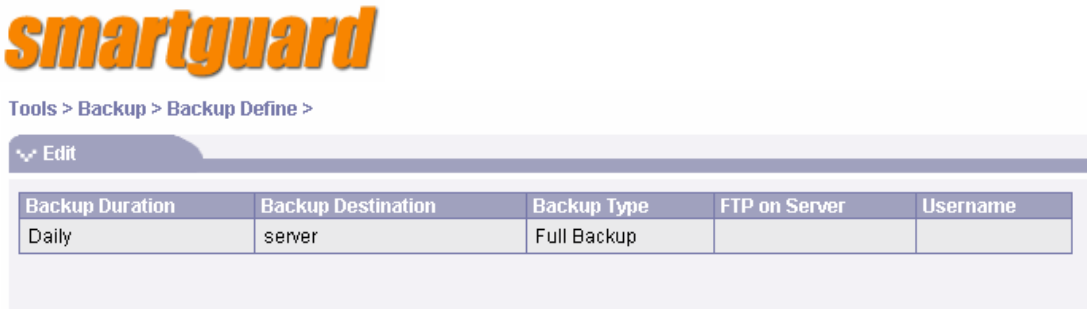
15.1BACKUP

STEP **Click on Tools option in left side of main menu → click on Backup icon.**

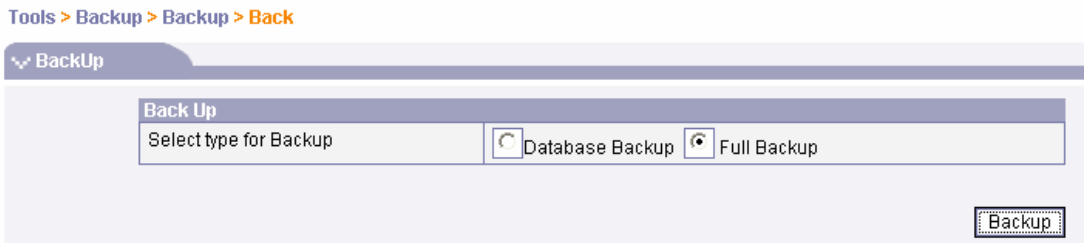


15.1 BACKUP DEFINE

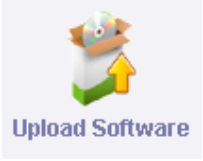
STEP **Click on Tools option in left side of main menu → click on Backup icon → click on Backup define icon.**



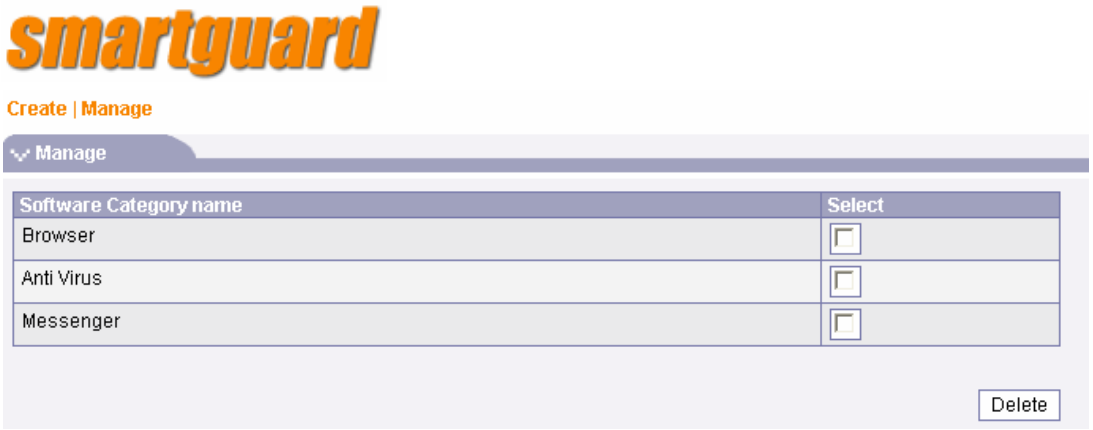
15.2 BACKUP



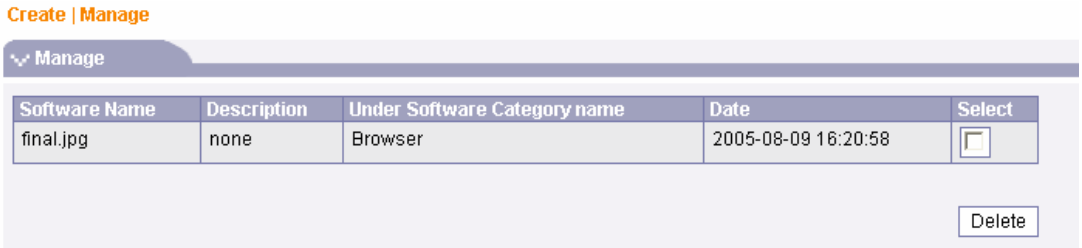
15.3 UPLOAD SOFTWARE



15.4 SOFTWARE CATEGORY



15.5 UPLOAD SOFTWARE



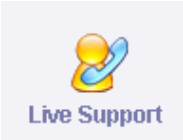
15.6 DOWNLOAD SOFTWARE

View

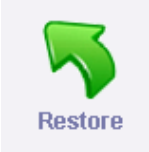
File Name	Size	Download	Delete
31_08_05.tar	9840640 Bytes		
fullbackup.tar.gz	192473 Bytes		
01_09_05.tar	10895360 Bytes		
03_09_05.tar	5416960 Bytes		
04_09_05.tar	8611840 Bytes		
05_09_05.tar	1515520 Bytes		
08_09_05.tar	9984000 Bytes		
09_09_05.tar	870400 Bytes		
10_09_05.tar	14131200 Bytes		
12_09_05.tar	11325440 Bytes		

15.7 LIVE USERS

15.8 LIVE SUPPORT

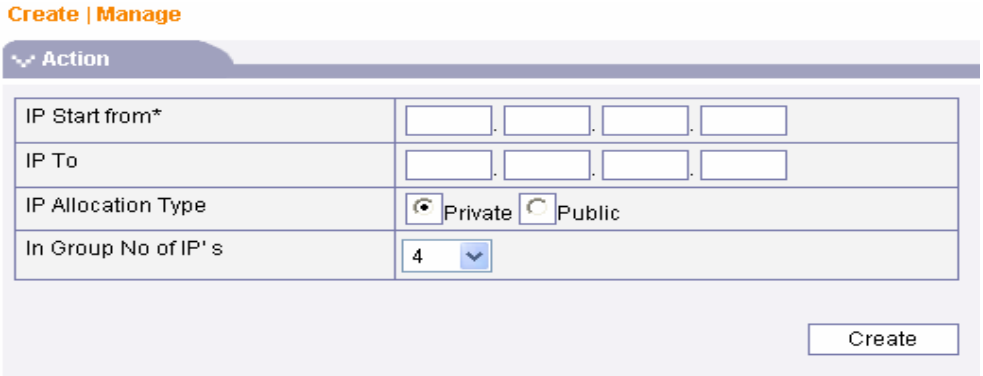


15.9 RESTORE

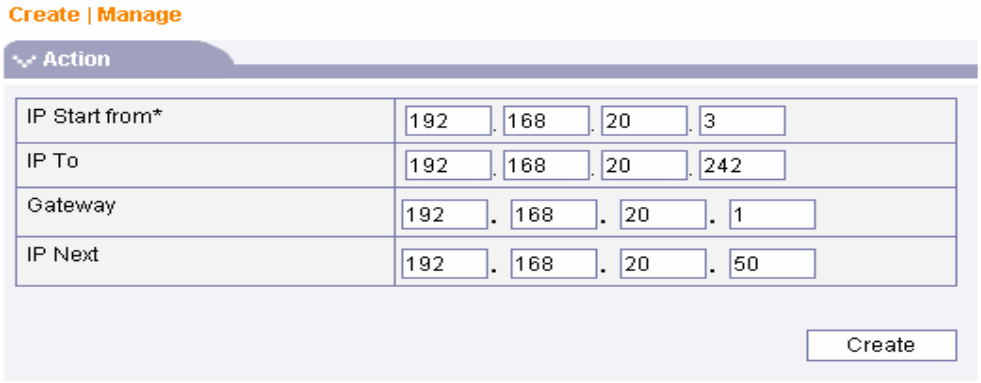


15.10 ADD IP RANGE

15.11 MULTIPLE IP



15.12 SINGLE IP



ISP Support

Tools > PublicIP Support >

Edit

Public IP Support	Yes No
Description	Pulic IP Support no

Update

Tools > ISP Support >

Edit

Mutilple ISP Support	Yes
ISP 1 Priority [192.168.10.10]	1
ISP 2 Priority [not enabled]	1
Description :	Mutiple ISP Support

Update

15.13 PUBLIC IP SUPPORT

smartguard
Tools > PublicIP Support >
Edit
Public IP Support
Yes
No
Description
Pulic IP Support no
Update
Tools > Restore >
Restore
Restore
Upload File
Browse...
Restore
show/hide

smartguard

Chapter 16

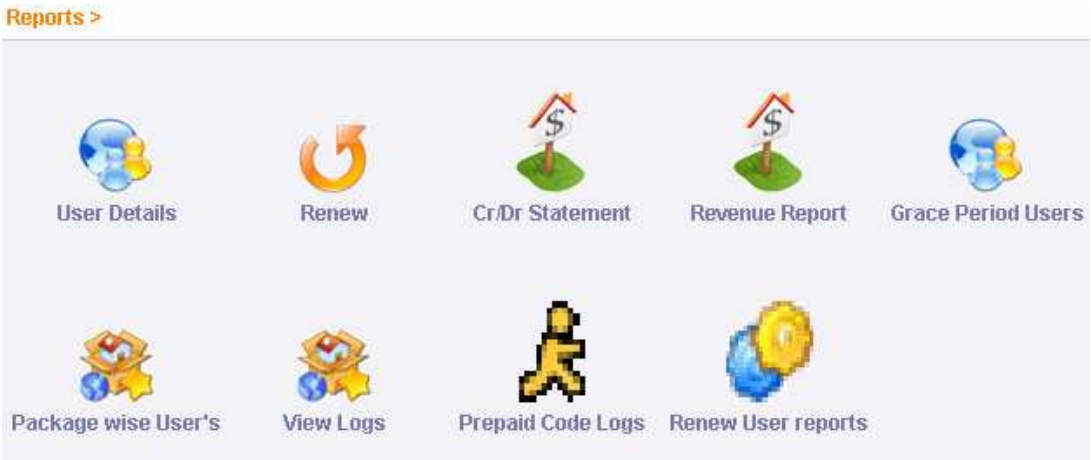
Reports

XS Infoways
the invincible technology

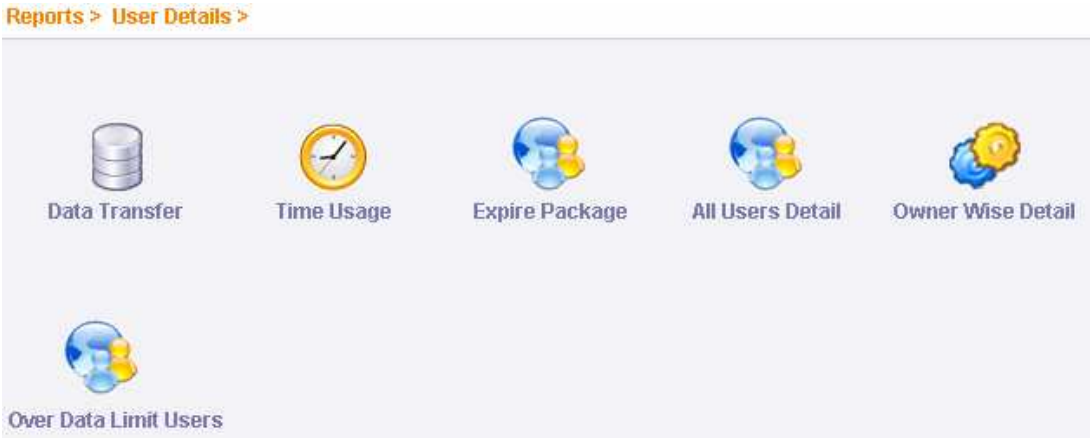
ver. **4.0.4**
Updated:06/27/2006

16. REPORTS

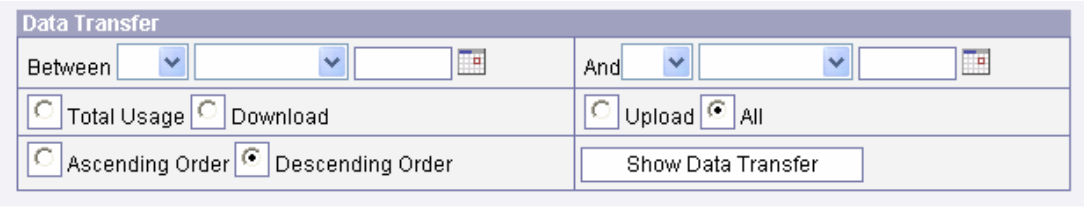
When administrator clicks on this option in the main menu following page is displayed.



16.1 USER DETAILS

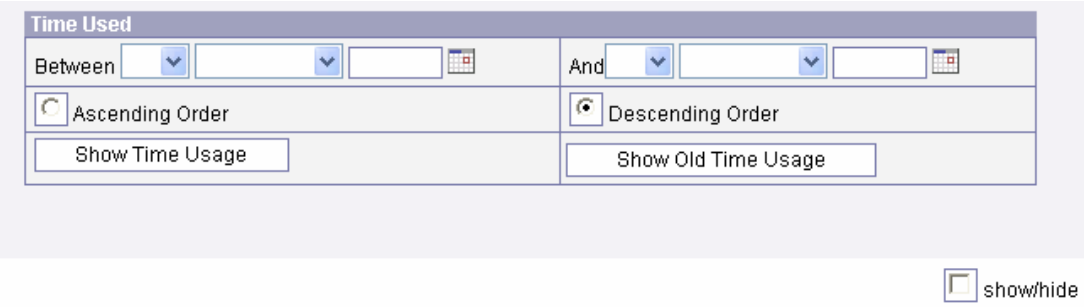


16.1.1 Data Transfer



From here administrator can view the data transfer in ascending/descending order for the specific user for the specific period of time.

16.1.2 Time Usage



From here administrator can view the time usage in ascending/descending order for the specific user for the specific period of time.

16.1.3 Expire Package

Page 1

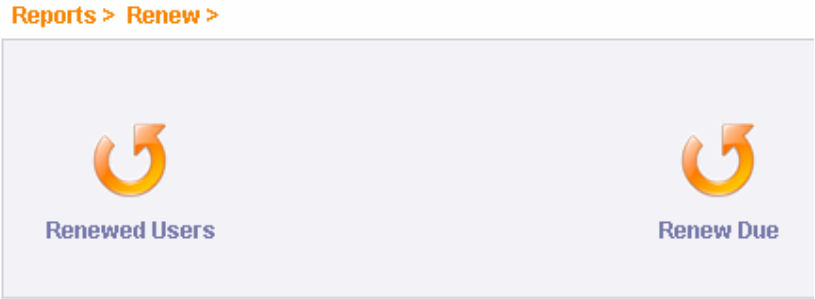
User IP	Customer Name	Company	Start Date	End Date	Grace Days	Renew
192.168.60.11	Super Admin don't delete these users	Super Admin	2005-06-24	2005-07-24 00:00:00		Renew
10.0.0.56	admin Don't delet these users	a	2005-03-08	2005-09-21 00:00:00		Renew

From this menu option administrator can view the start date, end date, grace days and also renew the specific package for the specific user.

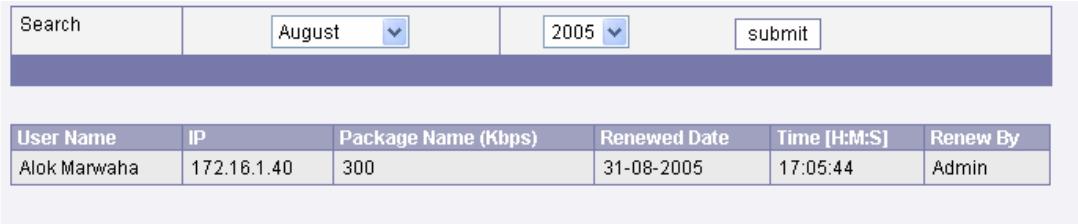
16.1.4 User Details

Sr No	Name	Address	Phone	Status	IP	IP Configuration Type	Package	Auto disconnect	Package Rate	Expiry Date
1	Admin Don't Delet These Users	a	11		10.0.0.56	STATIC	64 Kbps	✗	15.45	2005-09-21 00:00:00
2	Super Admin Don't Delete These Users	delhi	delhi		192.168.60.11	STATIC	32kbps	✗	2400	2005-07-24 00:00:00
3	Reseller Clinton	234 halley road	23432434		192.168.70.125	STATIC	64 Kbps	✗	15.45	2005-10-01 12:52:16
4	11 Yogener				192.168.70.109	STATIC	1 hour package	✓	100	2005-09-28 00:00:00
5	22 22				192.168.20.150	STATIC	64 Kbps	✓	15.45	2005-10-11 10:25:29
6	33 Singh				192.168.70.110	STATIC	64 Kbps	✓	15.45	2005-10-15 16:32:01

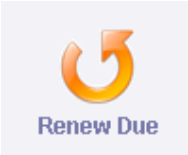
16.2 RENEW



16.2.1 Renewed Users



16.2.2 Renew Due



Enter Days	5	Submit

Page

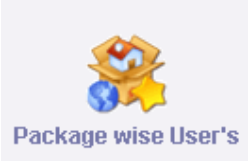
User IP	Customer Name	Company	Start Date	End Date	Grace Days	Renew
192.168.90.101	test user testing		2005-09-13	2005-10-13 17:10:14	0	Renew
172.16.1.35	UPDESCO -	-Academics	2005-01-18	2005-12-30 00:00:00		Renew
172.16.4.7	Video Test	t	2004-12-29	2005-12-30 00:00:00		Renew
172.16.1.72	Umang Bagla	The Web Artists	2005-01-26	2005-12-31 00:00:00		Renew
172.16.1.19	Carlton Hotel Mr.Rahul	Carlton Hotel	2005-01-16	2005-12-31 00:00:00		Renew
172.16.1.30	Shahid -	-	2005-01-16	2005-12-31 00:00:00		Renew
172.16.10.17	OP Tripathi -	-	2005-03-11	2005-12-31 00:00:00		Renew

16.3 CR/DR STATEMENT

16.4 REVENUE REPORT

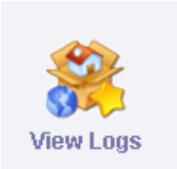
16.5 GRACE PERIOD USERS

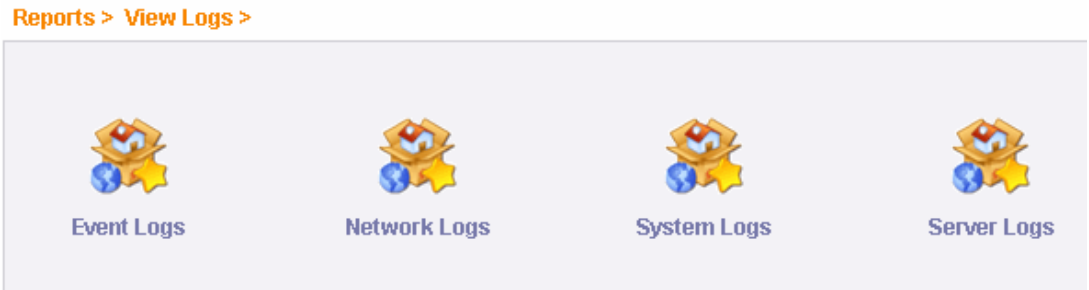
16.6 PACKAGE WISE USERS



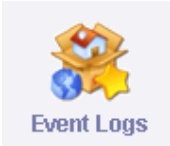
Package Name	Active Users	Disable Users	Total Users	Upload	Download	Total Bandwidth
25 Hours 30 Days	1	0	1	0 Bytes	232.58 KB	232.58 KB
Unlimited Access	0	0	0	0 Bytes	0 Bytes	0 Bytes
1200	116	0	116	12.65 GB	78.99 GB	91.63 GB
600	166	0	166	17.38 GB	75.87 GB	93.26 GB
300	127	0	127	9.99 GB	28.24 GB	38.23 GB
64kbps	2	0	2	166.76 MB	1.09 GB	1.25 GB
128kbps	4	0	4	236.45 MB	2.56 GB	2.79 GB
512	0	0	0	0 Bytes	0 Bytes	0 Bytes
256kbps	0	0	0	0 Bytes	0 Bytes	0 Bytes
512 Burstable	3	0	3	186.89 MB	323.58 MB	510.47 MB
night [d (64)]	0	0	0	0 Bytes	0 Bytes	0 Bytes
Night [g(512)]	0	0	0	0 Bytes	0 Bytes	0 Bytes
Night [e(128)]	0	0	0	0 Bytes	0 Bytes	0 Bytes
1GB 256kbps	4	0	4	351.43 MB	1.16 GB	1.5 GB
2 GB [512]	3	0	3	111.09 MB	254.47 MB	365.56 MB
x	0	0	0	0 Bytes	0 Bytes	0 Bytes
Special A	0	0	0	0 Bytes	0 Bytes	0 Bytes
Special C	0	0	0	0 Bytes	0 Bytes	0 Bytes

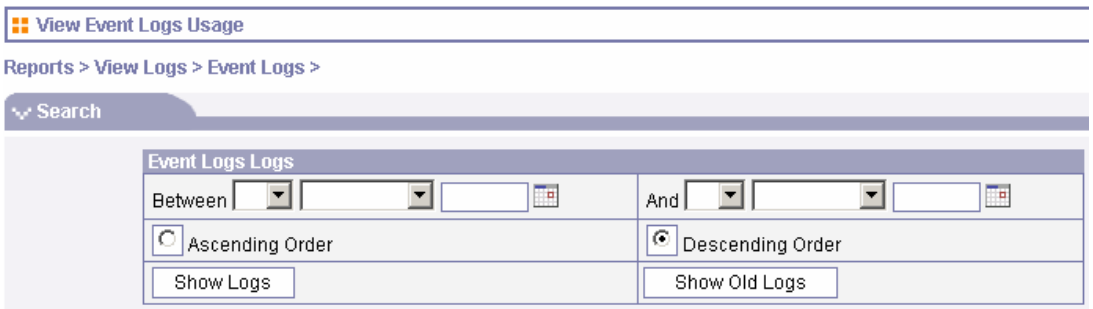
16.7 VIEW LOGS





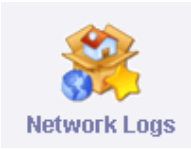
16.7.1 Event Logs





Date/Time	Log Type	Message	Action By	IP
26/09/2005 11:31:23	Package Changed	600 Package changed for user mull (package_id Modified From 128kbps To 600 ,)	admin	61.246.128.11
26/09/2005 12:12:05	User IP Edited	User Name:E-Solutions User IP:172.16.1.59 IP Edited (mac_id Modified From 00:02:44:29:5A:26 To 00:08:A1:53:B2:E1 , status Modified From Disable To Active , mac_authenticate Modified From 1 To 0 ,)	admin	61.246.128.11
26/09/2005 16:37:58	New User Created	raza User Created User IP 172.16.10.119 Netmask 32 Gateway 172.16.10.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 16:40:45	User IP Edited	User Name:Aamir User IP:172.16.10.119 IP Edited (status Modified From Disable To Active , user_ip Modified From 172.16.10.119 To 172.16.1.51 , gateway Modified From 172.16.10.1 To 172.16.1.1 ,)	admin	61.246.128.11
26/09/2005 16:42:33	New User Created	meraj User Created User IP 172.16.1.46 Netmask 32 Gateway 172.16.1.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 17:49:41	Package Changed	512 Package changed for user jaya (package_id Modified From 600 To 512 ,)	admin	172.16.1.242
26/09/2005 17:53:01	Package Changed	600 Package changed for user jaya (package_id Modified From 512 To 600 ,)	admin	172.16.1.242
26/09/2005 17:59:22	New User Created	neeraj User Created User IP 172.16.10.119 Netmask 32 Gateway 172.16.10.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 22:22:43	Pool Management Edited	Pool Management Edited (pool_bandwidth Modified From 320 To 384 ,)	admin	61.246.128.18

16.7.2 Network Logs



View Network Logs Usage

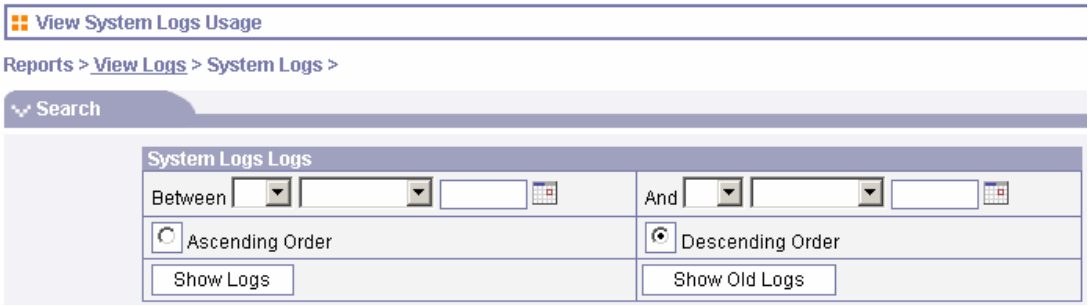
Reports > View Logs > Network Logs >

Search

Network Logs Logs	
Between	And
Ascending Order	Descending Order
Show Logs	Show Old Logs

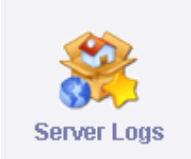
Date/Time	Log Type	Message	Action By	IP
26/09/2005 11:31:23	Package Changed	600 Package changed for user null (package_id Modified From 128kbps To 600 ,)	admin	61.246.128.11
26/09/2005 12:12:05	User IP Edited	User Name:E-Solutions User IP:172.16.1.59 IP Edited (mac_id Modified From 00:02:44:29:5A:26 To 00:08:A1:53:B2:E1 , status Modified From Disable To Active , mac_authenticate Modified From 1 To 0 ,)	admin	61.246.128.11
26/09/2005 16:37:58	New User Created	raza User Created User IP 172.16.10.119 Netmask 32 Gateway 172.16.10.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 16:40:45	User IP Edited	User Name:Aamir User IP:172.16.10.119 IP Edited (status Modified From Disable To Active , user_ip Modified From 172.16.10.119 To 172.16.1.51 , gateway Modified From 172.16.10.1 To 172.16.1.1 ,)	admin	61.246.128.11
26/09/2005 16:42:33	New User Created	meraj User Created User IP 172.16.1.46 Netmask 32 Gateway 172.16.1.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 17:49:41	Package Changed	512 Package changed for user jaya (package_id Modified From 600 To 512 ,)	admin	172.16.1.242
26/09/2005 17:53:01	Package Changed	600 Package changed for user jaya (package_id Modified From 512 To 600 ,)	admin	172.16.1.242
26/09/2005 17:59:22	New User Created	neeraj User Created User IP 172.16.10.119 Netmask 32 Gateway 172.16.10.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 22:22:43	Pool Management Edited	Pool Management Edited (pool_bandwidth Modified From 320 To 384 ,)	admin	61.246.128.18

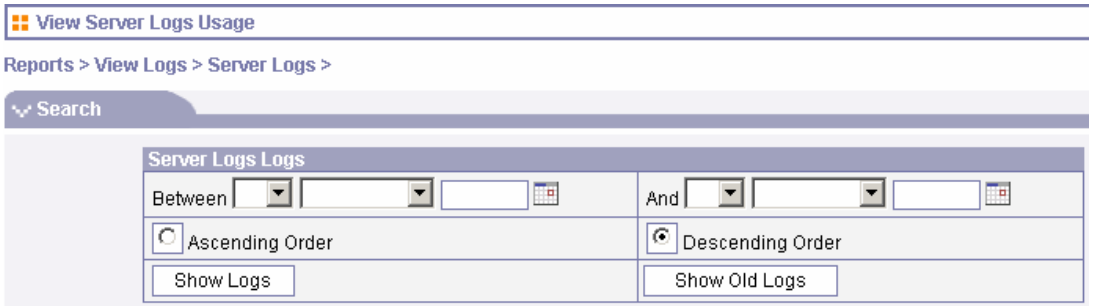
16.7.3 System Logs



Date/Time	Log Type	Message	Action By	IP
26/09/2005 11:31:23	Package Changed	600 Package changed for user null (package_id Modified From 128kbps To 600 ,)	admin	61.246.128.11
26/09/2005 12:12:05	User IP Edited	User Name:E-Solutions User IP:172.16.1.59 IP Edited (mac_id Modified From 00:02:44:29:5A:26 To 00:08:A1:53:B2:E1 , status Modified From Disable To Active , mac_authenticate Modified From 1 To 0 ,)	admin	61.246.128.11
26/09/2005 16:37:58	New User Created	raza User Created User IP 172.16.10.119 Netmask 32 Gateway 172.16.10.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 16:40:45	User IP Edited	User Name:Aamir User IP:172.16.10.119 IP Edited (status Modified From Disable To Active , user_ip Modified From 172.16.10.119 To 172.16.1.51 , gateway Modified From 172.16.10.1 To 172.16.1.1 ,)	admin	61.246.128.11
26/09/2005 16:42:33	New User Created	meraj User Created User IP 172.16.1.46 Netmask 32 Gateway 172.16.1.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 17:49:41	Package Changed	512 Package changed for user jaya (package_id Modified From 600 To 512 ,)	admin	172.16.1.242
26/09/2005 17:53:01	Package Changed	600 Package changed for user jaya (package_id Modified From 512 To 600 ,)	admin	172.16.1.242
26/09/2005 17:59:22	New User Created	neeraj User Created User IP 172.16.10.119 Netmask 32 Gateway 172.16.10.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 22:22:43	Pool Management Edited	Pool Management Edited (pool_bandwidth Modified From 320 To 384 ,)	admin	61.246.128.18

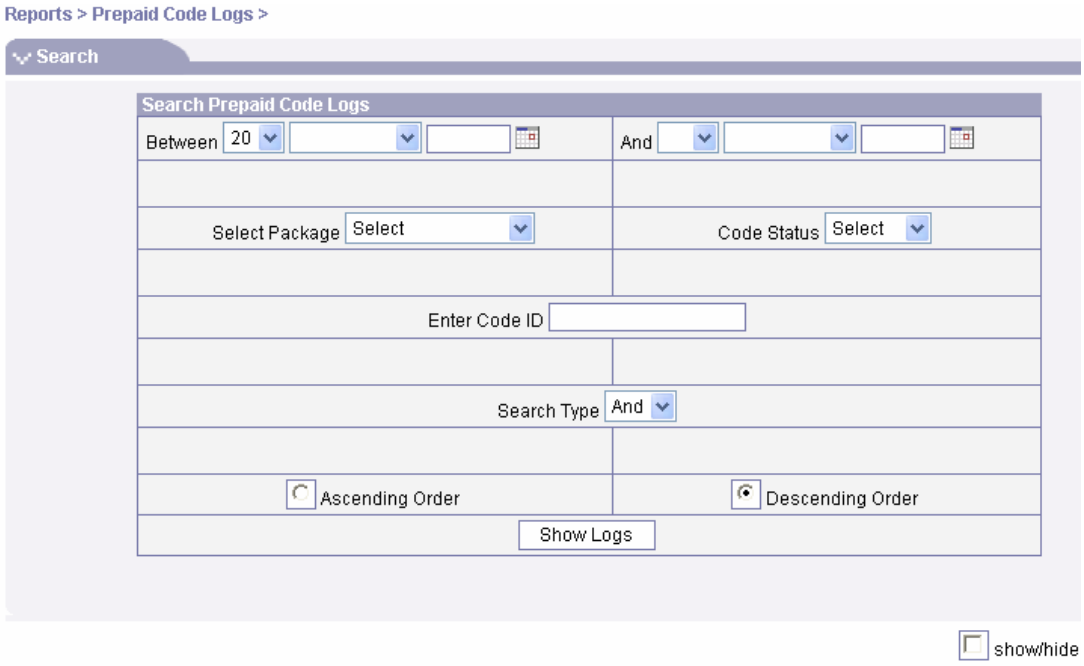
16.7.4 Server Logs



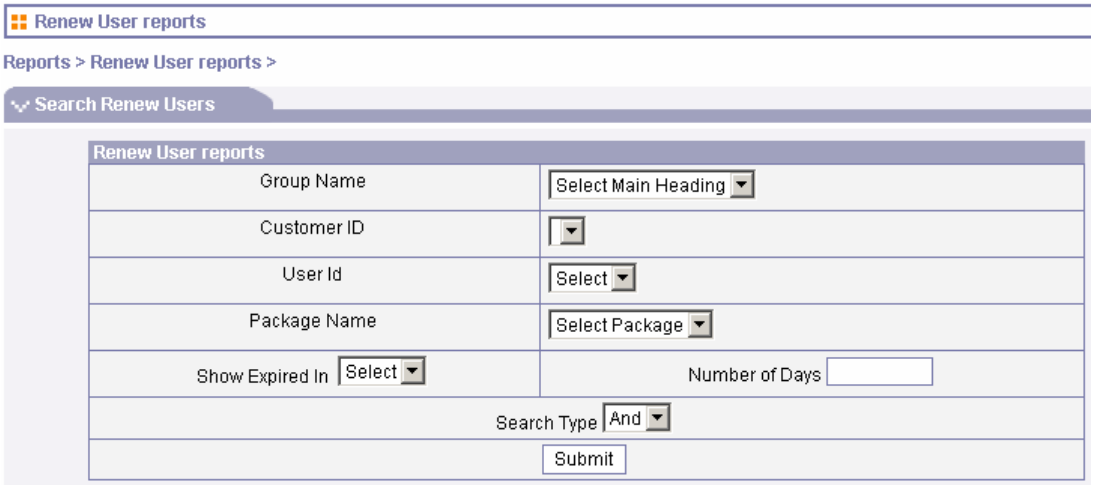


Date/Time	Log Type	Message	Action By	IP
26/09/2005 11:31:23	Package Changed	600 Package changed for user null (package_id Modified From 128kbps To 600 ,)	admin	61.246.128.11
26/09/2005 12:12:05	User IP Edited	User Name:E-Solutions User IP:172.16.1.59 IP Edited (mac_id Modified From 00:02:44:29:5A:26 To 00:08:A1:53:B2:E1 , status Modified From Disable To Active , mac_authenticate Modified From 1 To 0 ,)	admin	61.246.128.11
26/09/2005 16:37:58	New User Created	raza User Created User IP 172.16.10.119 Netmask 32 Gateway 172.16.10.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 16:40:45	User IP Edited	User Name:Aamir User IP:172.16.10.119 IP Edited (status Modified From Disable To Active , user_ip Modified From 172.16.10.119 To 172.16.1.51 , gateway Modified From 172.16.10.1 To 172.16.1.1 ,)	admin	61.246.128.11
26/09/2005 16:42:33	New User Created	meraj User Created User IP 172.16.1.46 Netmask 32 Gateway 172.16.1.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 17:49:41	Package Changed	512 Package changed for user jaya (package_id Modified From 600 To 512 ,)	admin	172.16.1.242
26/09/2005 17:53:01	Package Changed	600 Package changed for user jaya (package_id Modified From 512 To 600 ,)	admin	172.16.1.242
26/09/2005 17:59:22	New User Created	neeraj User Created User IP 172.16.10.119 Netmask 32 Gateway 172.16.10.1 STATIC and graph created	admin	61.246.128.11
26/09/2005 22:22:43	Pool Management Edited	Pool Management Edited (pool_bandwidth Modified From 320 To 384 ,)	admin	61.246.128.18

16.8 PREPAID CODE LOGS



16.9 RENEW USER REPORTS

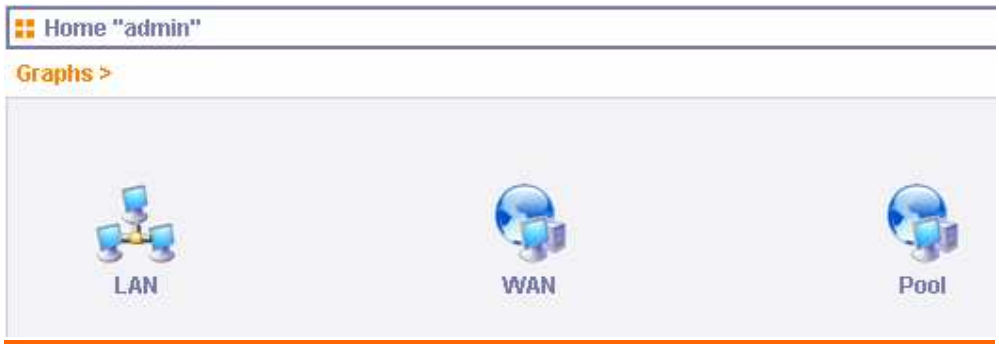


Chapter 17

Graphs

17. GRAPHS

If administrator wants to view the LAN, WAN & POOL Graphs. Then Click on graphs option.



17.1 LAN

You can view the daily, weekly, monthly and yearly average graphs of incoming and outgoing traffic through LAN network.

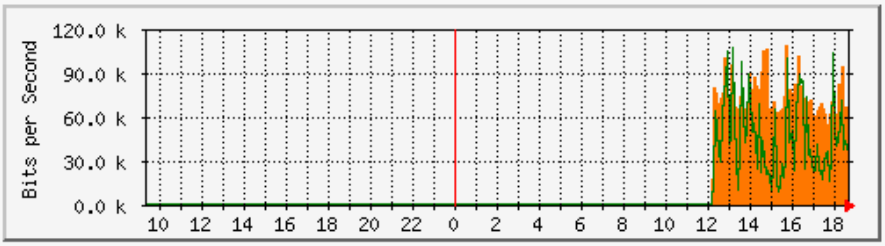
smartguard

Traffic Analysis for 3 -- ns1142676168.xyz.com

System: ns1142676168.xyz.com in Unknown
Maintainer: root@localhost
Description: eth1
ifType: ethernetCsmacd (6)
ifName:
Max Speed: 12.5 MBytes/s
Ip: 192.168.10.9 ()

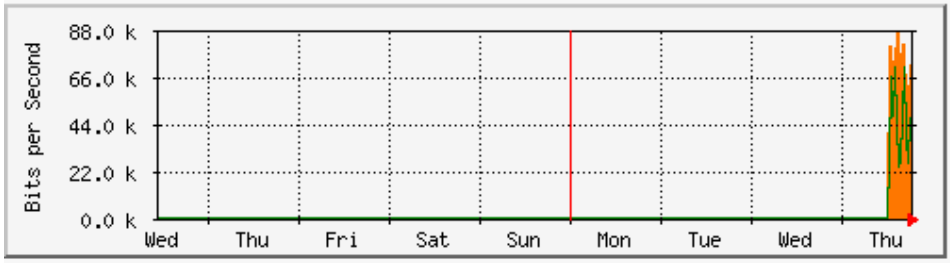
The statistics were last updated **Thursday, 30 March 2006 at 18:40**, at which time **'ns1142676168.xyz.com'** had been up for **6:39:45**.

`Daily' Graph (5 Minute Average)



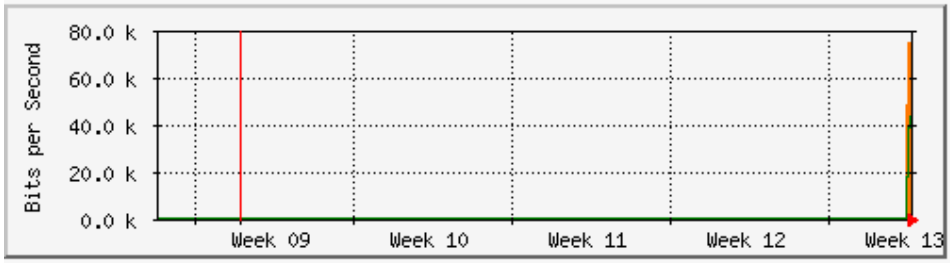
Max In:109.5 kb/s (0.1%) Average In:72.6 kb/s (0.1%) Current In:56.2 kb/s (0.1%)
Max Out:107.9 kb/s (0.1%) Average Out:46.4 kb/s (0.0%) Current Out:41.1 kb/s (0.0%)

`Weekly' Graph (30 Minute Average)

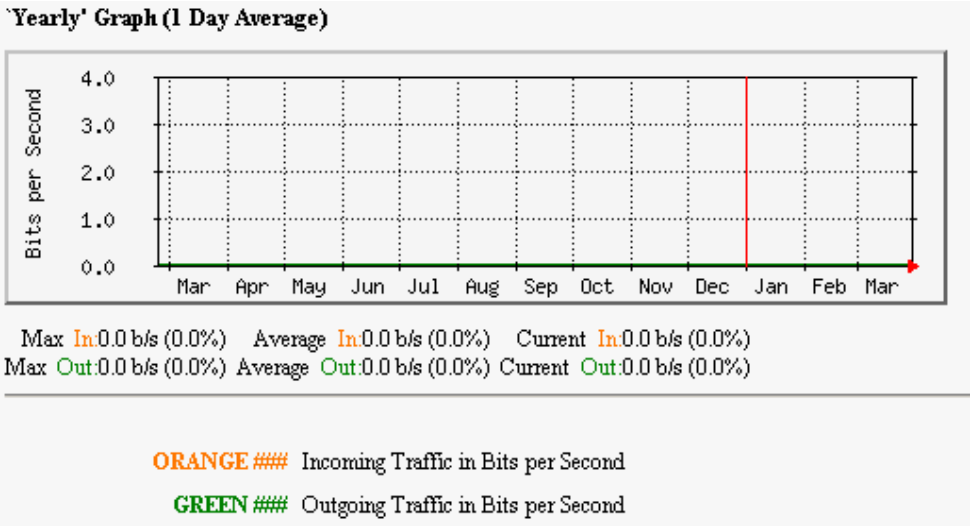


Max In:87.3 kb/s (0.1%) Average In:71.0 kb/s (0.1%) Current In:72.7 kb/s (0.1%)
Max Out:70.7 kb/s (0.1%) Average Out:45.4 kb/s (0.0%) Current Out:49.0 kb/s (0.0%)

`Monthly' Graph (2 Hour Average)

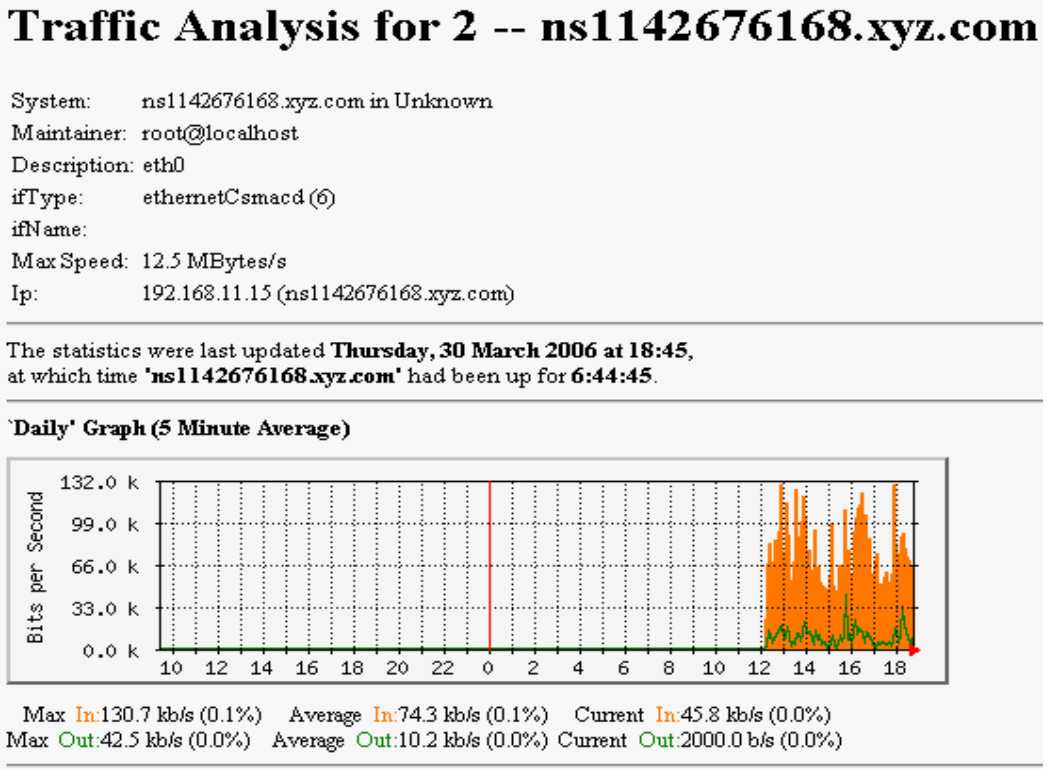


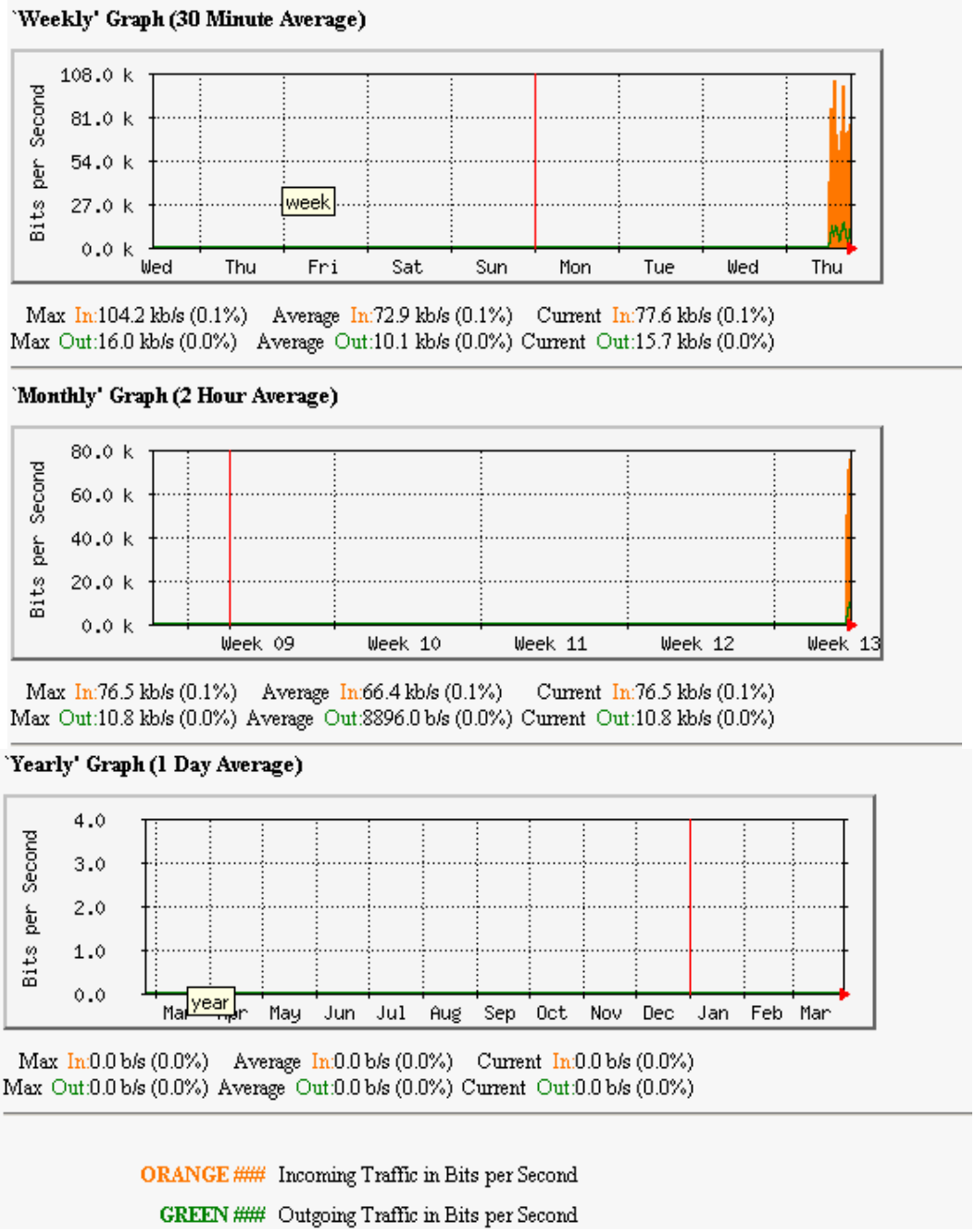
Max In:75.6 kb/s (0.1%) Average In:65.8 kb/s (0.1%) Current In:72.8 kb/s (0.1%)
Max Out:46.0 kb/s (0.0%) Average Out:41.3 kb/s (0.0%) Current Out:46.0 kb/s (0.0%)



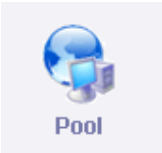
17.2 WAN

You can view the daily, weekly,monthly and yearly average graphs of incoming and outgoing traffic through the wan network from here.




`Weekly' Graph (30 Minute Average)
Bits per Second
108.0 k
81.0 k
54.0 k
27.0 k
0.0 k
week
Wed Thu Fri Sat Sun Mon Tue Wed Thu
Max In:104.2 kb/s (0.1%) Average In:72.9 kb/s (0.1%) Current In:77.6 kb/s (0.1%)
Max Out:16.0 kb/s (0.0%) Average Out:10.1 kb/s (0.0%) Current Out:15.7 kb/s (0.0%)
`Monthly' Graph (2 Hour Average)
Bits per Second
80.0 k
60.0 k
40.0 k
20.0 k
0.0 k
Week 09 Week 10 Week 11 Week 12 Week 13
Max In:76.5 kb/s (0.1%) Average In:66.4 kb/s (0.1%) Current In:76.5 kb/s (0.1%)
Max Out:10.8 kb/s (0.0%) Average Out:8896.0 b/s (0.0%) Current Out:10.8 kb/s (0.0%)
`Yearly' Graph (1 Day Average)
Bits per Second
4.0
3.0
2.0
1.0
0.0
year
May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar
Max In:0.0 b/s (0.0%) Average In:0.0 b/s (0.0%) Current In:0.0 b/s (0.0%)
Max Out:0.0 b/s (0.0%) Average Out:0.0 b/s (0.0%) Current Out:0.0 b/s (0.0%)
ORANGE ### Incoming Traffic in Bits per Second
GREEN ### Outgoing Traffic in Bits per Second

17.3 POOL


Pool

smartguard

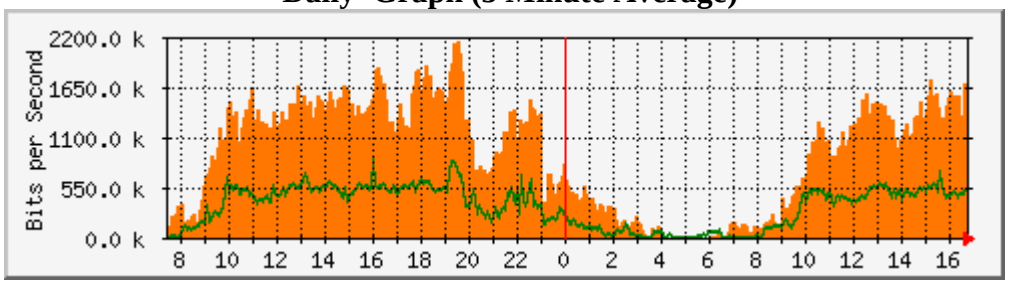
You can view the daily, weekly, monthly and yearly average graphs of incoming and outgoing traffic through individual pools from here.

Traffic Analysis for 2 -- ns1142676168.xyz.com

System: ns1142676168.xyz.com in Unknown
Maintainer: root@localhost
Description: eth0
ifType: ethernetCsmacd (6)
ifName:
Max Speed: 12.5 MBytes/s
Ip: 192.168.11.15 (ns1142676168.xyz.com)

The statistics were last updated **Tuesday, 27 September 2005 at 16:46**,
at which time **'ns1125988099.xyz.com'** had been up for **17:37:14**.

`Daily' Graph (5 Minute Average)



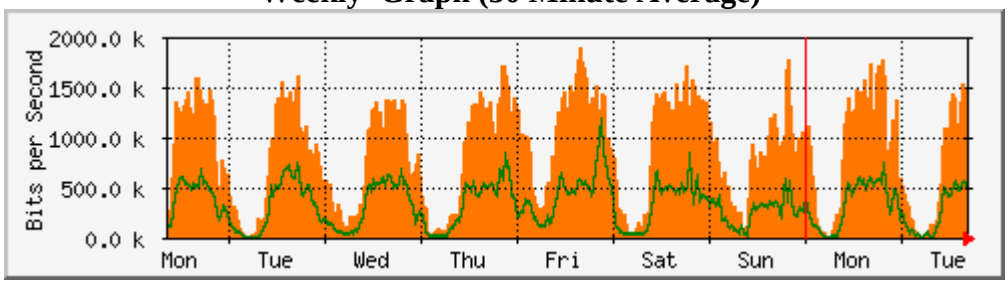
Max In:2175.1 kb/s (21.8%) Average In:911.7 kb/s (9.1%) Current In:1663.2 kb/s (16.6%)
Max Out: 870.6 kb/s (8.7%) Average Out:349.4 kb/s (3.5%) Current Out: 544.1 kb/s (5.4%)

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

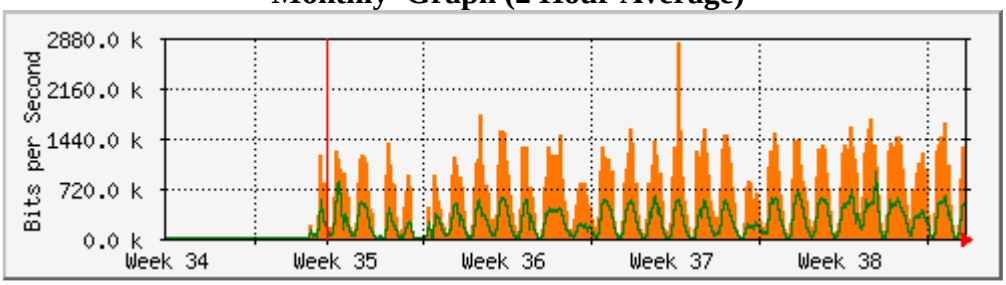
smartguard

`Weekly' Graph (30 Minute Average)



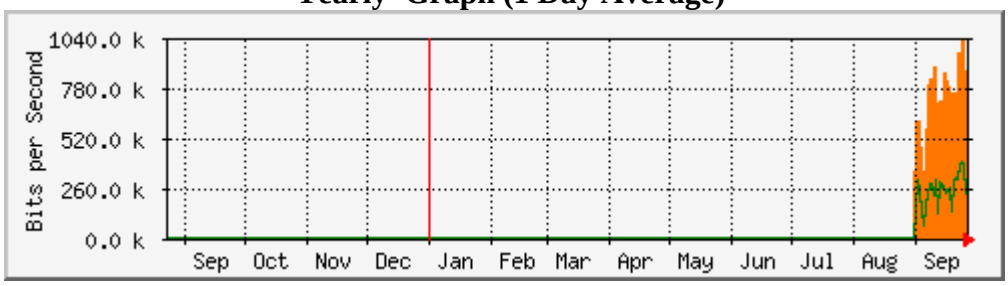
Max In:1906.1 kb/s (19.1%) Average In:865.4 kb/s (8.7%) Current In:1495.7 kb/s (15.0%)
Max Out:1190.4 kb/s (11.9%) Average Out:338.1 kb/s (3.4%) Current Out: 490.8 kb/s (4.9%)

`Monthly' Graph (2 Hour Average)



Max In:2844.3 kb/s (28.4%) Average In:695.0 kb/s (6.9%) Current In:1298.8 kb/s (13.0%)
Max Out: 968.1 kb/s (9.7%) Average Out:259.6 kb/s (2.6%) Current Out: 518.6 kb/s (5.2%)

`Yearly' Graph (1 Day Average)



Max In:1030.0 kb/s (10.3%) Average In:671.3 kb/s (6.7%) Current In:880.4 kb/s (8.8%)
Max Out: 404.8 kb/s (4.0%) Average Out:250.2 kb/s (2.5%) Current Out:327.3 kb/s (3.3%)

ORANGE ### Incoming Traffic in Bits per Second

GREEN ### Outgoing Traffic in Bits per Second

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

smartguard

Chapter 18

Downloads

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

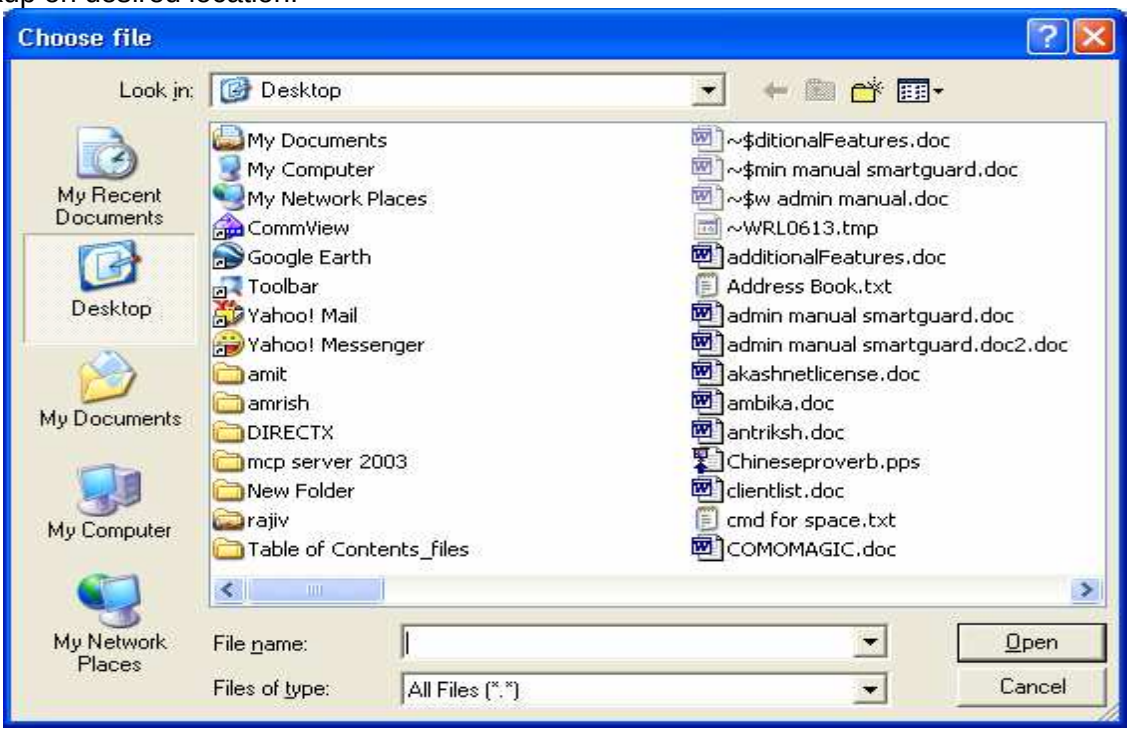
18. DOWNLOADS

From this option administrator can download the backups taken on server (Database, Full Backup, Defined backups) on a local machine.

View

File Name	Size	Download	Delete
31_08_05.tar	9840640 Bytes		
fullbackup.tar.gz	192473 Bytes		
01_09_05.tar	10895360 Bytes		
03_09_05.tar	5416960 Bytes		
04_09_05.tar	8611840 Bytes		
05_09_05.tar	1515520 Bytes		
08_09_05.tar	9984000 Bytes		
09_09_05.tar	870400 Bytes		
10_09_05.tar	14131200 Bytes		
12_09_05.tar	11325440 Bytes		

After clicking on download you would be directed to this page and you can download desired backup on desired location.



smartguard

Chapter 19

FAQ's

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

19. FAQ

SOLUTIONS WITH REASONS TO SMARTGUARD ERRORS

a) Gateway not defined on lan machine.
Ping not coming.
Load average high on server.
Low space on harddisk
System out of ram.

Solution: give the command
service httpd restart

b) Gateway not defined on lan machine.
Ping not coming.
Load average high on server.
Low space on harddisk
System out of ram.
Mysql error

Solution : give the command
service httpd restart
service squid restart
service mysqld restart

c} automatically backup at 1:00 clock in night put mysql service down

check by the command at root
tail -100 /var/log/mysqld.log
solution:
log in thru webmin interface
go to servers option
now go to crond jobs
stop the automatically backup option
click on save.

d) capping not done properly
capping not done proprly at isp end
problem in link
virus attack or broadcast in network.

solution: make one main pool and give restrictions on the particular users.

e) increase cache ram and harddisk size.

f) increare the physical ram on system

g) check by pitstop utility website.
Make the pools logically correct.

h) giv the package through cache.
Put the possible links to be blocked in the myfile in the website blocking option in system.
Give the messenger.php in the atrtup og nettshield.

i) giv the proper most possible and urls in the myfile to block the related links and sites.

j) giv the fsck command at riit i.e. # fsck /dev/(hda1,hdb1,hdc1,hdd1) –y

k) go to the menu by:
cd /var/www/html
sh menu.sh
now repair database by pressing 10

give the command at root as # service mysqld restart

l) problem with dns and squid.conf file. Someone has modified contents of that file thru vi editor.
Change the dns entries at lan pc.

m) double rule on the user
login the user disc onnect it and login again.
n) give the server restart and flush the cache once.
o) Stop the bandwith calculation from the text menu.
p) Username and password at email server and fetchmail server do not match.
Delete and create the account in emal server for the particular user.

q) Delete and create the account in emal server for the particular user.
Check pop3 server and smtp server to be correct.

r) these are attachments with spam..
flush the cache or give it a restart.

s) give the proper port number in the firewall option to block webcam service.
t) Change the dns for that user and restart that lan pc.
u) Flush the cache and restart the cache server through text menu.
v) Disconnect and reconnect the user and u wil be able to open it.
Set the default page of internet explorer to indexmain.php.
w) problem at lan , check the cable hub or switch connections.
Restart the switch.
x) ip already already connected at server.
y) Delete the list of ip form the system options at panel.
z) ip already already connected at server.
Delete the list of ip form the system options at panel.

smartguard

Chapter 20

Glossary

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

20. GLOSSARY

1. **What is a Cable Network?**

   Cable Networks began in the USA over thirty years ago to provide TV access to locations that had difficulty in receiving TV signals transmitted by normal transmission towers. This included many inner city locations where TV reception was poor due to interference from buildings. In addition, geographical conditions around some towns, and cities (such as mountains) made it impractical for each building to have its own tall costly aerial. From a practical point of view, it was also more efficient to have a TV signal 'delivered' to a central location in a building or a community and then passed to individual TV sets than to have each TV set connected to its own external aerial.

   Cable Companies were formed that normally obtained a license or franchise for a specific geographic location and sold access for a monthly subscription. Initially Cable Companies rebroadcast signals from the major TV networks and did not provide any of their own content.

   The communications industry is an ever changing and fast moving industry so it was not long before Cable Companies began offering their own content and special content, often provided at a premium price (such as movie channels or sports channels).

   At this juncture in our explanation, its worth emphasizing two points that will be elaborated on in more detail later.

   Firstly, although Cable Companies had central distribution points, they also ran a unique connection directly into each house, apartment or office (as in the case of a telephone line). Secondly, the cable connection was intended to deliver TV signals which by their nature, require high bandwidth (more on this later).

2. **What does a TV cable system have to do with the Internet?**

   As Cable Companies began to proliferate and expand, they began to recognize that they could provide services in addition to TV signals. Many began to offer telephone services which of course they were able to do relatively easily because they already had a connection running into premises. In this respect they were competing with traditional telephone companies who also had a connection into premises. The recent spectacular growth of the Internet offers Cable Companies a further

opportunity, particularly since they can connect a user to the Internet at much faster speed. As anyone who has used the Internet knows, the faster the speed of access, the more useful and enjoyable the experience. Conversely, slow access can discourage frequent use and even deter it. Some Cable Companies spotted the (now) obvious opportunity if (1) they could provide Internet access and (2) if they could provide faster speed.

3. **Why is access via a Cable Company faster?**

   Cable Companies by their very nature set up cabling and networks to provide TV signals which required far more signal throughput (bandwidth) to be communicated. Modern Cable Networks use fiber-optic cabling directly into the premises which cabling is theoretically capable of delivering vast amounts of data. On the other hand, most telephone subscribers have old 'copper cable' connecting them to their telephone company's high speed network.

   (Note: Not all Cable Company connections use fiber-optic cabling. Some older ones use coaxial cabling which, although superior to 'copper wire' telephone cabling, does not provide the same throughput as fiber-optic.)

4. **Why has it taken cable companies so long to provide Internet access?**

   Cable Companies can provide Internet access in two ways - either by a 'telephone dial-up type' of service or by a new high speed connection. Since they are able to provide telephone lines, their subscribers can usually use tradition connection devices such as modems or ISDN. This however is normally not much improvement over normal telephone dial-up access.

   Cable companies had several problems to solve before being able to use their high bandwidth capability and offer high speed Internet access. The first issue to be dealt with was that cable networks were initially designed to deliver signals (i.e. TV) to subscribers and were usually not designed to receive data (as they would if they were providing Internet access). To solve this they would have to change equipment at both the subscriber end of the cable and at their own end of the cable. At the subscriber end they would have to provide a new device called a 'cable modem' while at their own end (called the 'head-end') they would have to change equipment to be able to receive data from the subscriber. They would also have to arrange for their head-end switch to be connected to the Internet backbone itself.

   One problem was that many cable networks used differing technologies and there were no industry standards for either cable modems or head-end switches. Cable companies and their industry associations have been working together over the past several years and standards are now being established. As a result of the standards, cable modems will be able to be manufactured in significant quantities

(since they will work with different cable companies' systems) and the cost will be reduced to that approximating a 'normal' telephone modem.

(Note: Some cable companies are working out interim systems that deliver Internet data to subscribers via the cable and receive the data from the subscriber via a telephone-modem. More on this later.)

There are also some commercial reasons for the delay in cable companies offering Internet access. Almost everybody, cable companies included, has been surprised by the rate of growth of the Internet and the demand for access. In addition to solving technical problems, cable companies had to determine if it was commercially viable to provide access. Since many telephone-modem Internet Service Providers (ISPs) charge flat rates of $15.00 - $25.00 per month for unlimited access, cable companies had to determine what they could charge for their higher bandwidth access, what number of subscribers would take up the option and if the revenue received would offset their costs.

A number of cable companies have been running limited trial systems providing Internet access during 1996 and 1997 and it appears that most trials have been successful from both the subscriber and the cable company point of view.

5. **Can everyone have Internet access via Cable Services?**

Unfortunately cable networks are not universally available. Due to the very nature of cable systems' requiring underground wiring they are very expensive to set up and are most appropriate to highly populated locations. Cable networks do however continue to grow and the new telephone and Internet access sources of revenue should encourage expansion.

In addition, not all cable companies are offering Internet access yet and many that do are continuing to do so on a limited or trial basis. It has been estimated that in the USA and Canada, cable modem service will be commercially available to 9 million homes by the end of 1997. This represents 9 percent of all homes with cable available to them. It is further estimated that there are currently 100,000 cable subscribers in the USA and Canada using cable networks for their Internet access and that this will grow to 200,000 by mid-1998 and to 1 million by mid-1999.

6. **How do I get connected to a Cable Network for Internet access?**

You have already started researching the subject online by reading this Q&A and might like to continue your research online. If you are already connected to a cable system for television, you will only have to determine if your cable operator offers Internet access and what their rates are. If you are not yet connected to a cable system you will have to determine if cable connection is available to you and if you

are able to purchase Internet access only, or if you are obliged to take TV subscriptions as well.

7. **Do I need a separate cable for each service?**

   No, your Cable Company will put a junction box in your home or office. Your computer, telephone and Internet access will all be routed through this single connection.

8. **How do I access the Internet using the Cable Network?**

   There are two options available for accessing the Internet through a cable network. The first is to use the dial-up telephone services provided by your Cable Company in conjunction with a modem or ISDN adapter. The second is to use a Cable modem. Each of these options is discussed in more detail below.

9. **How do I use the telephone services for Internet access?**

   Using the standard dial-up services, the only involvement of your Cable Company is their provision of a telephone or ISDN line to you. You then choose your Internet Service Provider (ISP) as well as the connection equipment such as modem or ISDN terminal adapter. When you choose your ISP, they will require a service agreement, separate from your Cable contract. Using you cable provider to provide access this way will not however give you high speed access. For high speed access, you will need a Cable Modem.

10. **What is a Cable Modem?**

    A Cable modem is a device at the subscriber end of a cable that allows a computer to be connected to the Internet through an existing Cable network connection. Unlike a dial-up connection, it does not require a phone line. Now that standards for Cable Modems have been agreed, their cost will decrease and they will be more readily available. A cable modem works in a similar manner to a standard modem in that it takes a signal from the computer and converts it for transmission over the cable network. There are two major differences between a cable modem and other modem/ISDN devices. The first is that a cable modem attaches to your computer through an Ethernet Network Interface Card ('NIC'). The second and more significant difference is that the bandwidth available to cable modems is far in excess of that of a dial-up modem or ISDN.

11. **How do I get a Cable Modem?**

    When you obtain Internet access from your Cable Company, they will normally provide you with a Cable Modem that has been tested to work with their network.

They will also normally provide you with any other hardware and software to get you connected to the Internet. Some Cable Companies include the cost of the Cable Modem in the monthly subscription charge and some will have a one-time charge. In any event, their cost is now about the same as for a high speed modem.

12. **How does a Cable Modem's speed compare with other connection methods?**

As with many communication systems, there are both theoretical and 'Real World' performance statistics. Comparisons are further confused by the fact that not all Cable Companies provide the same Internet access speeds. At the end of this Part The real-world speed of Cable Modem access is probably more than 60 times that of a 33.6 k modem, probably more than 30 times that of a one of the new X2/56k modems and probably more than 15 times that of a two channel 128k ISDN connection.

Put another way, Cable Modem access can be as fast or faster than having a leased line T1 connection or put still another way - its fast! Most people that have used it are very enthusiastic and would do almost anything rather than revert to dial-up connection.

13. **What is the theoretical performance of a Cable Modem?**

A cable modem is theoretically capable of receiving data at 30Mbps which, if it were achieved in the real world, would be 892 times the throughput of a standard 33.6k modem. It is unlikely that Cable Companies would either want to provide this throughput or be technically able to do so in a real world situation.

14. **What is the real-world performance?**

The theoretical performance of a Cable Modem is based upon all other devices being able to work at the same speed and performance as the Cable Modem. However, in a similar way that a standard 10Mbps Ethernet connection reduces to a 4Mbps, so too will the performance of a Cable Modem connection.

In addition, the Cable network itself will suffer the same problems of Internet performance as any other Internet Service Provider (ISP). Although performance to services on the cable network itself can be amazingly fast, access to 'the outside world' will be slowed down by the performance of other connections on the way.

If you connect to a remote Internet site that itself has a connection speed equivalent to a T1 connection (1.5Mbps), then that is as fast as the data can be served to you, no matter how fast your receiving equipment is.

15. **What is the point of having all this bandwidth available?**

The bottom line is that having high speed cable modem access to the Internet will ensure that any data coming down to your computer will be by the fastest possible means. Your connection will not become the bottleneck. This really comes into its own where multiple sites and multiple sessions are being used, in other words, when you want to do more than one thing at a time on the Internet.

For example, a file transfer (FTP) will use as much of the connection speed (bandwidth) as is possible. With a modem or even an ISDN connection this means that using other services such as web browsing can become extremely slow. A Cable Modem is able to cope with the file transfer and the browsing and still have plenty of bandwidth available. The cable modem will also make connecting more than one computer (a LAN) to the Internet even more practical (more on this later).

Using Cable Access also means that in your community, serviced by the same Cable Company, you could use the cable network to share files with neighbors and have local information services at your fingertips.

16. **How should I choose between what type of connection to use?**

The decision to use either a Cable Modem or a dial up service depends upon the facilities offered by your Cable Company when compared against another ISP. For many people, the Cable Company as an ISP or a third party ISP is able to offer a similar level of service.

The following are a few considerations when deciding, who to use to provide your Internet access:

What Internet services do you want to use, such as email, web browsing, file transfers, etc.?
How much does the Internet account cost per month?
Are there costs for making a phone call to your ISP?
Does your ISP have any additional charges?
Does each service offer you sufficient email addresses?
Are you able to get personal web space?
Do you require additional phone lines to be installed?
Can the ISP be accessed through a local call?

Considerations might be the number of mailboxes that you are allowed, the amount of personal web space, is your Internet Service a flat fee or is it a scalable charge depending upon the amount of data you transfer and the services you require.

Firstly, it is a good idea to decide what is important to you, then which of the available providers is best suited to deliver those services.

17. **How much does it cost?**

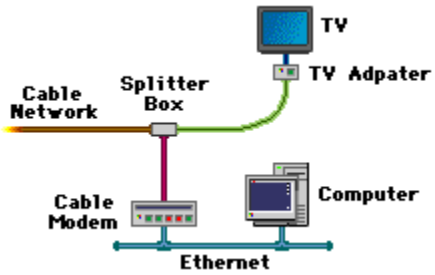
The cost of the Cable Modem for Internet Access is very reasonable, especially with the greater bandwidth available. The service costs tend to be only slightly more than the monthly charge for a dial-up 33.6 modem connection to an Internet Service Provider (ISP).

The table below shows the typical first year costs when comparing a Cable Modem, 33.6 modem and ISDN for Internet access.

Prices shown are averages drawn from various services and may vary in your area. Plan Dependant is where ISP's may have their own scale of charges for access time.

18. **How does a Cable Modem actually work?**

Your Cable Company supplies you with a connection to your home which in turn is connected to a splitter box. One spur from the splitter box is connected to your TV, through a TV Adapter, the other being connected to your Cable Modem, which in turn is connected to your computer through an Ethernet connection. The diagram below illustrates a typical installation.



19. **How does the Cable Modem physically attach to my computer?**

The most common method for Cable Modems to be attached to your computer is by using an Ethernet connection utilizing 10baseT cables. (10baseT is also referred to as Twisted Pair or UTP.) This uses a cable that is similar to a telephone cable with a small plastic connector at either end. One end connects to the Cable Modem, the other connects to your computer's Ethernet card.

20. **What is a Telco Return Cable Modem service?**

Telco Return (sometimes also referred to as TR or Telephone Return) is a system used by some cable company ISP's to provide Internet access. This system uses separate send and receive paths.

21. **What if I have more than one computer?**

If you wanted to connect several computers at a location to the Internet using traditional one-by-one methods, your costs would increase exponentially. For each computer, you would require an individual modem / ISDN, separate telephone lines, separate ISP accounts, etc. Clearly this is inefficient and impractical. Alternately you could use a dedicated hardware router obtain a business account from your ISP. This alternative requires technical skills (hardware routers are not for the faint hearted) and the business ISP account may be costly.

Fortunately there is a an easy-to-use cost-effective alternative using the SmartGuard InterGate. With its Network Address Translation feature, multiple users can simultaneously share one ordinary ISP account and one connection to the Internet.

The combination of the SmartGuard InterGate and a cable modem is ideal in a number of scenarios where Internet access is required by more than one computer, whether at school, at home or in businesses.

22. **What's the downside of using Cable access?**

The popular expression *"if something looks too good to be true, it probably is !"* is a warning to us all to exercise caution before enthusiastically embracing new technologies. On the surface, access to the Internet via cable networks appears to be the solution for all those who have suffered from slow access via dial-up modems. If, as is often the case, it is your method of accessing the Internet that is the bottleneck, then access via a cable modem will remove that bottleneck. It is worth remembering however that some popular sites and the wider Internet connections are often the bottlenecks, and in those cases, delays will still occur. The analogy of cars on a Freeway is appropriate. If you have a high performance car and there is not much traffic on the Freeway, you will be able to have unimpeded high speed travel (not that any of our readers would speed of course). If however the highway is clogged with other cars, it really doesn't matter what the performance or speed of your car is. You will only be able to go as fast as the slowest cars.

Another issue worth raising is somewhat of a technical one and it involves security. Cable modems connected to the head-end equipment at the cable company approximate the situation of your computer being connected to a LAN hub. When using a single Ethernet card, this results in other people on your branch of the network (perhaps as many as 500) being able to 'see' data passing to your computer. Unless you have some type of sharing or server active on your computer this will not normally represent any risk or danger. For total peace of mind you can use a Firewall product such as the SmartGuard InterGate which can be configured to insure that your computer or other computers on your LAN are not at risk.

23. **What's the bottom line? What does SmartGuard recommend?**

SmartGuard does not sell cable modems or access to the Internet via cable systems. Furthermore, our products can be used with any type of Internet connection, be it modem dial-up, ISDN, T1, or cable modem. In other words, we are neutral on the subject of how people connect to the Internet (but will admit to being biased to encouraging them to do so in some way).

From our tests, from feedback we have received from users, from the recent progress made by the cable companies and from what we have read, it would appear that accessing the Internet via cable systems using cable modems is an option that is definitely worth considering for users who have it available to them.

1. What is wireless networking?

   The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. The current buzzword however generally refers to wireless LANs. This technology, fuelled by the emergence of cross-vendor industry standards such as IEEE 802.11, has produced a number of affordable wireless solutions that are growing in popularity with business and schools as well as sophisticated applications where network wiring is impossible, such as in warehousing or point-of-sale handheld equipment.

2. What is a wireless network made up of?

   There are two kinds of wireless networks:

a. An ad-hoc, or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. (This is called "bridging")

   Figure 1: Ad-Hoc or Peer-to Peer Networking.
   Each computer with a wireless interface can communicate directly with all of the others.

b. A wireless network can also use an access point, or base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect (or "bridge") the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity.

There are two types of access points:

i. Dedicated hardware access points (HAP) such as Lucent's WaveLAN, Apple's Airport Base Station or WebGear's AviatorPRO. Hardware access points offer comprehensive support of most wireless features, but check your requirements carefully.

ii. Software Access Points which run on a computer equipped with a wireless network interface card as used in an ad-hoc or peer-to-peer wireless network. The SmartGuard suites are software routers that can be used as a basic Software Access Point, and include features not commonly found in hardware solutions, such as Direct PPPoE support and extensive configuration flexibility, but may not offer the full range of wireless features defined in the 802.11 standard.

With appropriate networking software support, users on the wireless LAN can share files and printers located on the wired LAN and vice versa. SmartGuard's solutions support file sharing using TCP/IP.

Figure 2: Hardware Access Point.
Wireless connected computers using a Hardware Access Point.

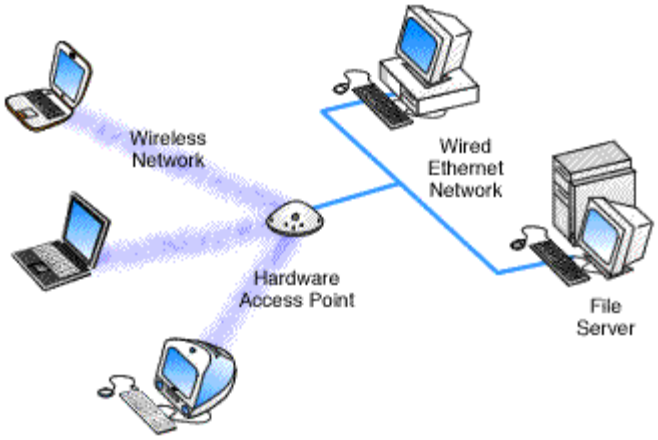
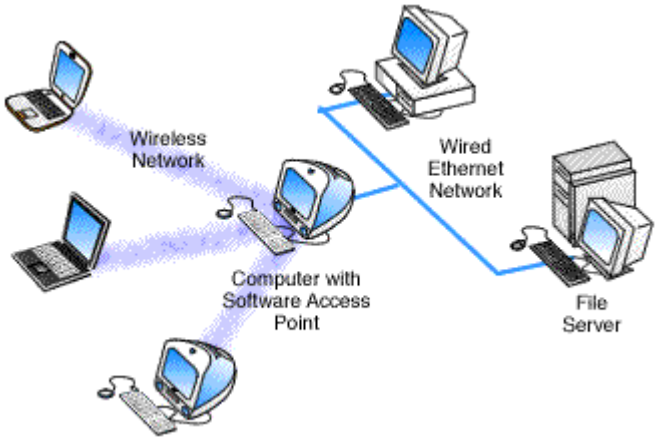


Figure 3: Software Access Point.
Wireless connected computers using a Software Access Point.



3. What is IEEE 802.11?

   Wireless networking hardware requires the use of underlying technology that deals with radio frequencies as well as data transmission. The most widely used standard is 802.11 produced by the Institute of Electrical and Electronic Engineers (IEEE). This is a standard defining all aspects of Radio Frequency Wireless networking.

4. Can I mix wireless equipment from different vendors?

   Because most wireless networking hardware vendors support the 802.11 standard they can inter operate. However, we recommend verification as the standard is a fairly recent one, and does specify two different methods for wireless communications; Frequency Hopping (FH) and Direct Sequence Spread Spectrum (DSSS or DS), which are not interoperable.

   When purchasing wireless networking hardware from separate vendors be sure to obtain guarantees from the vendors that the hardware will interoperate and follows the standards.

   Within a short time we expect all new wireless cards, like ethernet cards, to become inexpensive, ubiquitous and totally interoperable.

   Also of note is that the latest version of the standard defines 11mbps and 5.5mbps networking, with support for the older standard 1mbps and 2mbps speeds. This provides some compatibility with different or older equipment. Note that this new standard covers DS-type Networks, not FH types.

   Software access points such as InterGate which uses the wireless interface of the host computer should have no compatibility issues with third party wireless hardware, as long as standards are followed. Typically wireless hardware is identified to the software as a network interface, and therefore can be used in the same way as any other network card.

5. If my computer is connected to a wireless LAN, can it communicate with computers on a wired LAN as well?

To do this you will need some sort of bridge between the wireless and wired network. This can be accomplished either with a hardware access point or a software access point. Hardware access points are available with various types of network interfaces, such as Ethernet or Token Ring, but typically require extra hardware to be purchased if your networking requirements change.

If networking requirements go beyond just interconnecting a wired network network to a small wireless network, a software access point may be the best solution.

A software access point does not limit the type or number of network interfaces you use. It may also allow considerable flexibility in providing access to different network types, such as different types of Ethernet, Wireless and Token Ring networks. Such connections are only limited by the number of slots or interfaces in the computer used for this task.

Further to this the software access point may include significant additional features such as shared Internet access, web caching or content filtering, providing significant benefits to users and administrators.

6. What is the range of a wireless network?

   Each access point has a finite range within which a wireless connection can be maintained between the client computer and the access point. The actual distance varies depending upon the environment; manufacturers typically state both indoor and outdoor ranges to give a reasonable indication of reliable performance. Also it should be noted that when operating at the limits of range the performance may drop, as the quality of connection deteriorates and the system compensates.

   Typical indoor ranges are 150-300 feet, but can be shorter if the building construction interferes with radio transmissions. Longer ranges are possible, but performance will degrade with distance.

   Outdoor ranges are quoted up to 1000 feet, but again this depends upon the environment.

   There are ways to extend the basic operating range of Wireless communications, by using more than a single access point or using a wireless relay /extension point.

7. How many wireless networked computers can use a single access point?

   This depends upon the manufacturer. Some hardware access points have a recommended limit of 10, with other more expensive access points supporting up to 100 wireless connections. Using more computers than recommended will cause performance and reliability to suffer.

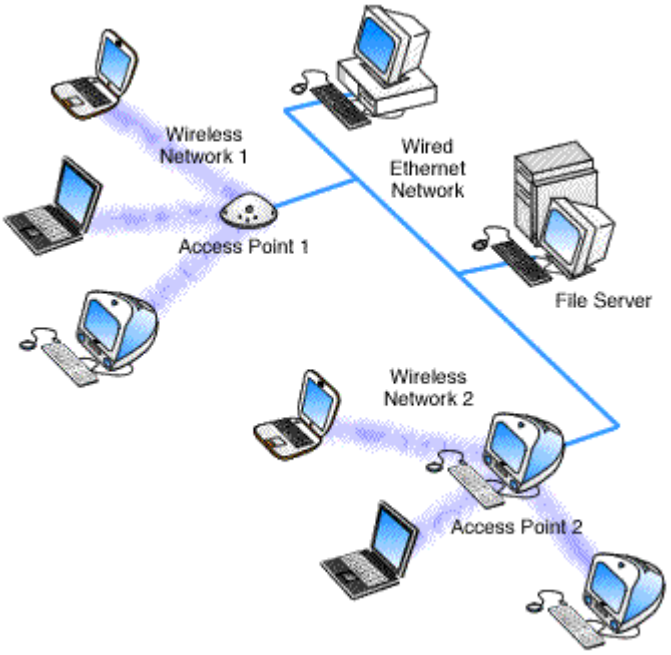
   Software access points may also impose user limitations, but this depends upon the specific software, and the host computer's ability to process the required information.

8. Can I have more than one access point?

   Yes, multiple access points can be connected to a wired LAN, or sometimes even to a second wireless LAN if the access point supports this.

In most cases, separate access points are interconnected via a wired LAN, providing wireless connectivity in specific areas such as offices or classrooms, but connected to a main wired LAN for access to network resources, such as file servers.

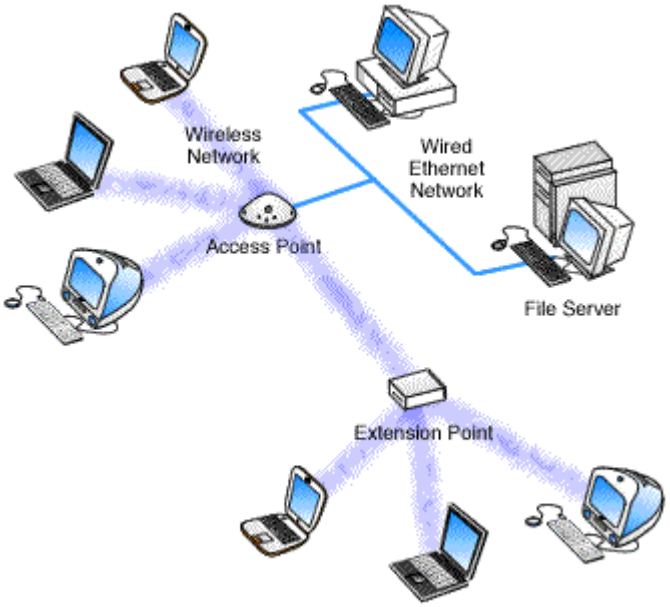
Figure 4: Multiple Access Points.
Wireless connected computers using Multiple Access Points.



If a single area is too large to be covered by a single access point, then multiple access points or extension points can be used. -- Note that an "extension point" is not defined in the wireless standard, but have been developed by some manufacturers. When using multiple access points, each access point wireless area should overlap its neighbors. This provides a seamless area for users to move around in using a feature called "roaming. " (See the next question for an explanation of Roaming)

Some manufacturers produce extension points, which act as wireless relays, extending the range of a single access point. Multiple extension points can be strung together to provide wireless access to far away locations from the central access point.

Figure 5: Extension Point.
Wireless connected computers using an Access Point with an Extension Point.

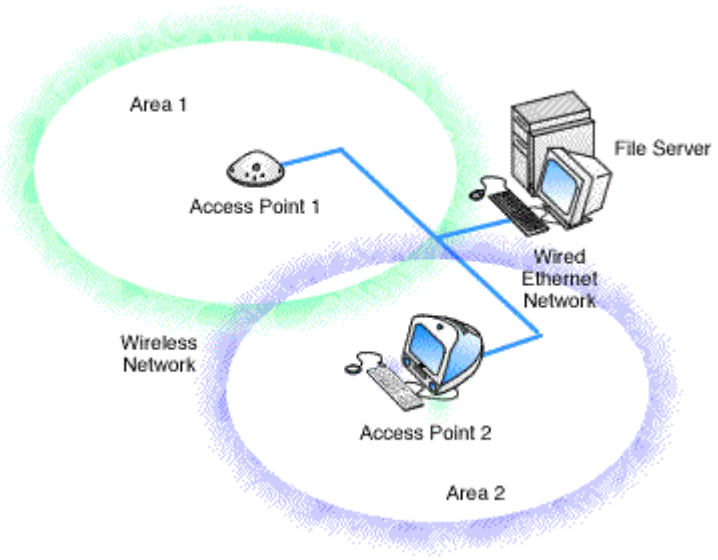


9. What is Roaming?

A wireless computer can "roam" from one access point to another, with the software and hardware maintaining a steady network connection by monitoring the signal strength from in-range access points and locking on to the one with the best quality. Usually this is completely transparent to the user; they are not aware that a different access point is being used from area to area. Some access point configurations require security authentication when swapping access points, usually in the form of a password dialog box.

Access points are required to have overlapping wireless areas to achieve this as can be seen in the following diagram:

Figure 6: Roaming.
A user can move from Area 1 to Area 2 transparently. The Wireless networking hardware automatically swaps to the Access Point with the best signal.

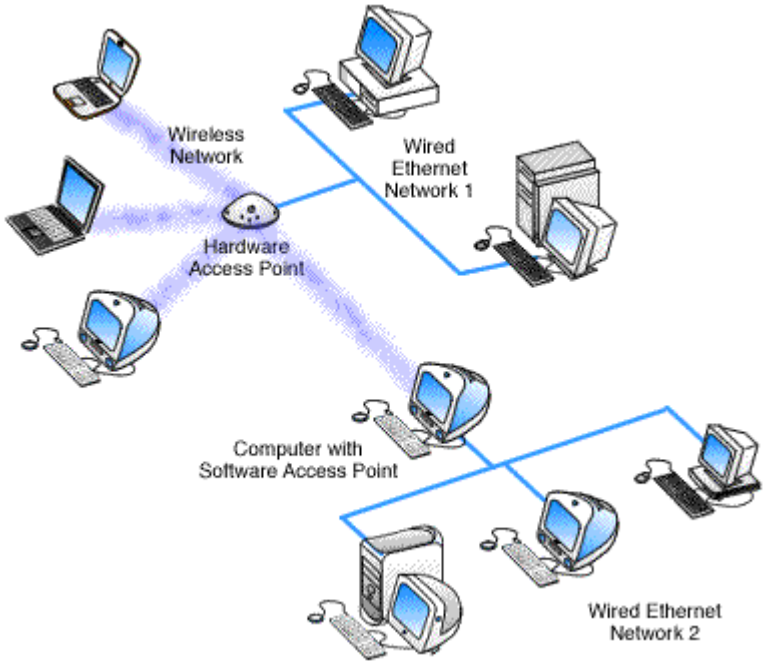


Not all access points are capable of being configured to support roaming. Also of note is that any access points for a single vendor should be used when implementing roaming, as there is no official standard for this feature.

10. Can I use a wireless network to interconnect two LANs?

Yes. Wireless networking offers a cost-effective solution to users with difficult physical installations such as campuses, hospitals or businesses with more than one location in immediate proximity but separated by public thoroughfare. This type of installation requires two access points. Each access point acts as a bridge or router connecting its own LAN to the wireless connection. The wireless connection allows the two access points to communicate with each other, and therefore interconnect the two LAN's.

Figure 7: LAN to LAN Wireless Communications
A Hardware Access Point providing wireless connectivity to local computers and a software access point. The software access point provides Wired Ethernet network 2 computers access to Wired Network 1.



Note that not all hardware access points have the ability to directly interconnect to another hardware access point, and that the subject of interconnecting LAN's over wireless connections is a large and complex one, and is beyond the scope of this introduction.

11. Is it true that wireless networking is only good for laptop computers?

    Although wireless networking offers obvious benefits to users of laptops who move from location to location throughout the day, there are benefits for users of fixed position computers as well:

    Many schools and businesses have unsuitable building layouts or walls that cannot be wired for various reasons making it difficult or impossible to build a wired network. Wireless networking in these environments is a very cost effective alternative also providing future flexibility.

    In cases where a small number of computers are separated from a main network a wireless link may be more cost effective than network cabling although the latter is perfectly feasible.

    Temporary wireless LANs can easily be created for exhibitions, school or business projects, all without any trailing cabling.

12. What about security?

    Wireless communications obviously provide potential security issues, as an intruder does not need physical access to the traditional wired network in order to gain access to data communications. However, 802.11 wireless communications cannot be received --much less decoded-- by simple scanners, short wave receivers etc. This has led to the common misconception that wireless communications cannot be eavesdropped at all. However, eavesdropping is possible using specialist equipment.

To protect against any potential security issues, 802.11 wireless communications have a function called WEP (Wired Equivalent Privacy), a form of encryption which provides privacy comparable to that of a traditional wired network. If the wireless network has information that should be secure then WEP should be used, ensuring the data is protected at traditional wired network levels.

Also it should be noted that traditional Virtual Private Networking (VPN) techniques will work over wireless networks in the same way as traditional wired networks.

Section Two - Wireless Networking and the Internet

13. How can I use a wireless network to share an Internet connection?

Once you realise that wireless cards are analogous to ethernet cards and that empty space is analogous to ethernet cabling, the answer to this question becomes clear. To share an Internet connection across a LAN you need two things:

- an Internet sharing hardware device or software program
- a LAN

If your LAN is wireless, the same criteria apply. You need a hardware or software access point and a wireless LAN. Any computer equipped with a wireless network card running suitable Internet sharing software can be used as a software access point. A number of vendors offer hardware access points.

A hardware access point may provide Internet Sharing capabilities to Wired LAN computers, but does not usually provide much flexibility beyond very simple configurations.

Figure 8: Software Access Point.
Wireless connected computers using a Software Access Point for shared Internet access.

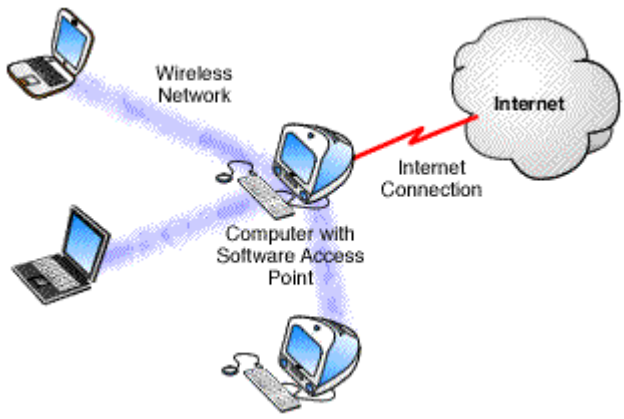
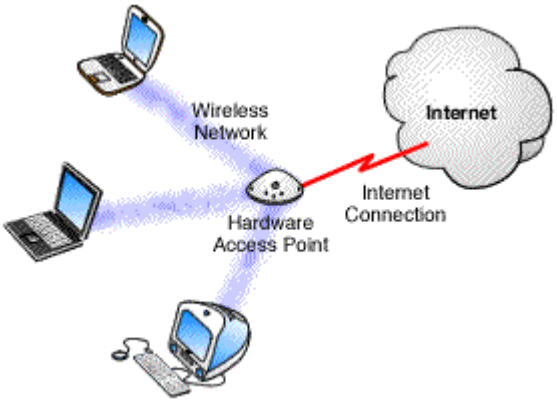


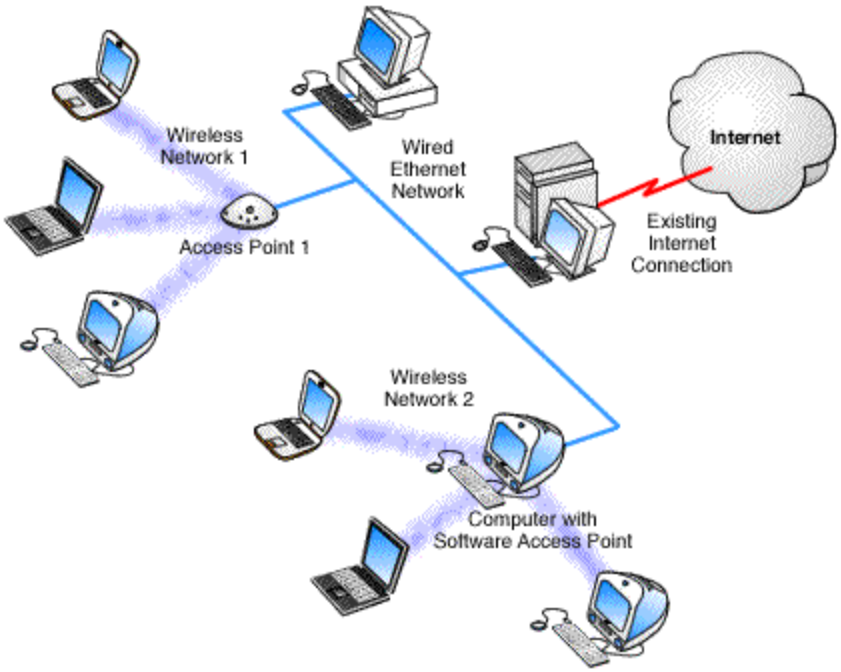
Figure 9: Hardware Access Point.
Wireless connected computers using a Hardware Access Point for shared Internet access.



14. If I have more than one hardware access point, how can I share a single Internet connection?

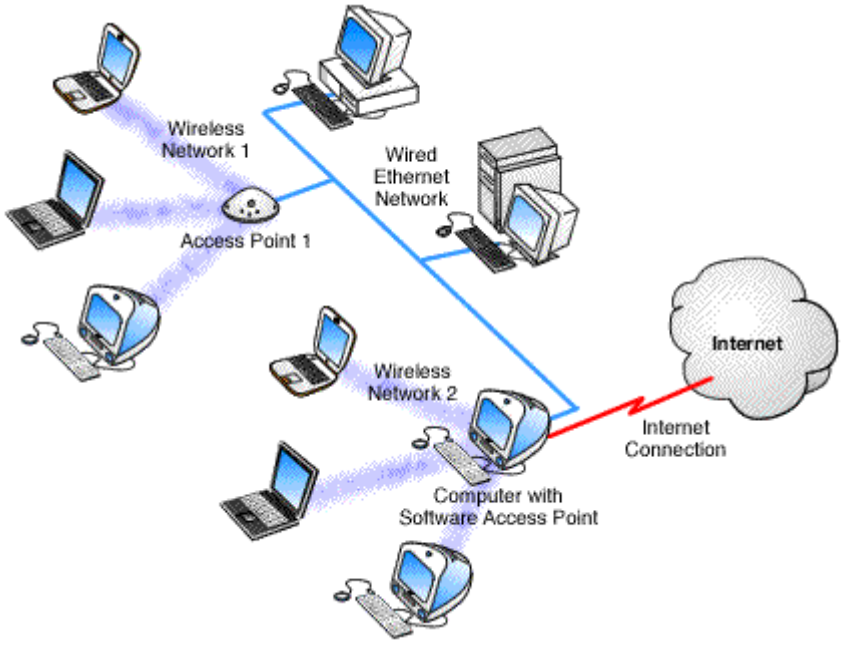
    If an existing wired LAN already has an Internet connection, then the hardware access points simply connect to your LAN and allow wireless computers to access the existing Internet connection in the same way as wired LAN computers.

    Figure 10: Multiple Access Points.
    Wireless connected computers using Multiple Access Points.



If there is no existing Internet connection, then this depends on the access point:

Figure 11: Software Access Point sharing one Internet connection.
Wireless connected computers using Multiple Access Points. All wired and wireless computers access the Internet through a single software access point.



If an access point provides some form of Internet sharing itself, then having multiple such access points connected to a wired LAN may require some special configuration, or possibly may require an additional Internet sharing device or software program.

15. If I use a wireless network to connect to the Internet does my ISP need a wireless network too?

    If you use a wireless network to connect to the Internet, the wireless part only concerns your LAN. The communications link from your LAN to your Internet service provider (ISP) would be identical whether or not you had a wireless network. For example, if you connected an ethernet network to the Internet via a 56K modem, when you upgraded your network to use wireless, you would still use the same 56K modem to connect to the Internet.

16. Can networking software identify a wireless computer in the same way it can identify an ethernet computer on the network?

    Wireless cards look just like ethernet cards to your network drivers. In fact, wireless networking cards have unique MAC hardware addresses that are formatted like ethernet hardware addresses allocated from the same standards organization.

1. **What is DSL?**

DSL refers to a class of technology used to obtain more bandwidth over existing copper telephone cabling running between a customer's premises and a Telco's Central Office. DSL allows simultaneous voice and high-speed data services such as super fast Internet access over a single pair of copper telephone wires. There are several variations of 'DSL' that include:

ADSL -Asymmetric Digital Subscriber Line
R-ADSL -Rate-Adaptive Digital Subscriber Line
HDSL -High Bit-Rate Digital Subscriber Line
VDSL -Very High Bit-Rate Digital Subscriber Line
SDSL -Symmetric Digital Subscriber Line

As the saying goes, 'there is no such thing as a free lunch' and a Telco must make compromises between costs, distance, speeds, reliability, equipment, etc when implementing or offering 'DSL' services. Each variation of 'DSL' reflects the different compromises made by Telco's when deciding how far and how fast data can flow on a particular kind of subscriber line.

2. **What's special about DSL?**

The cables connecting most households to the phone network are mainly simple twisted pair copper wires, which have only been able to carry analogue traffic. Modem speeds have gradually increased through the use of various compression and other techniques, but at today's fastest (56 kbit/s) they are approaching the theoretical limit for this technology.

DSL technology enables much higher speeds across the twisted pair lines from the Central Office to the home, school or business. Speeds up to 2 Megabits per second are achievable in some areas - 30 or more times faster than today's fastest modems. This means that some consumers and tele-workers will be able to use applications that need these higher speeds even if high performance (fibre) cable networks are not available in their location.

3. **What is PPPoE?**

PPPoE stands for Point to Point Protocol over Ethernet. PPP is usually used over serial communications like dial-up modem connections. Many DSL Internet service providers now use PPP over Ethernet because of its added login and security features. A whole Q&A document is dedicated to PPPoE here

4. **What is a DSL modem?**

a DSL "modem" is a device that is placed at either end of the copper phone line to allow a computer (or LAN) to be connected to the Internet through a DSL connection. Unlike a dial up connection, it usually does not require a dedicated phone line (a POTS splitter box enables the line to be shared simultaneously). DSL is considered to be the next generation

of modem technology. Although DSL modems resemble conventional analogue modems they provide much higher throughput.

5. **How does DSL compare to access using normal (analogue) modems, Cable modems and ISDN?**

Analogue modems allow digital data to flow over the Telco's existing analogue network by performing a digital to analogue conversion for transmission onto the network and vice versa on the receiving end. The only necessity for analogue modems is that each end of the call must have a compatible modem. This makes analogue modem connections the most ubiquitous form of data communications available today. However, analogue modems are limited by the Telco's voice bandwidth service. Current analogue modems are struggling to achieve rates of only 56 kbit/s over those networks.

Cable modems are capable of very high speed throughput (bandwidth) and are used when accessing the Internet across a television cable company's network (usually fibre). However access via cable modem from a cable company is normally structured in a way that has a group of users sharing a 'node' in a specific area. The more subscribers in that area, the less bandwidth is available to each. So although the cable modem itself can handle high throughput, the bandwidth available to a user may be less.

ISDN is a Telco technology that provides digital service across existing telephone copper wiring typically in increments of 64 Kbit/s channels. ISDN has been around for many years, but its popularity in the USA is only now beginning to increase as a result of limitations of analogue modems and the rise of Internet usage. Roll-out of this service by most Telcos in the USA has been slow due to high costs, lack of standards and low acceptance rate by consumers. [Note: ISDN is widespread throughout a number of other countries including Germany, France and the UK].

DSL are also Telco technologies but unlike ISDN they appear to be gaining widespread Telco approval. Backed by the Telcos, they appear the candidates to provide next generation high bandwidth services to the home, school or business using the existing telephone cabling infrastructure. DSL technology puts a high speed digital link on the copper telephone line, and routes it directly to a packet switching data network for efficient wide area transmission, bypassing the voice network. DSL modems use digital coding techniques to squeeze up to 99% more capacity out of a copper telephone line without interfering with regular phone services. That means you could be simultaneously talking on the phone or sending a fax - while accessing web pages on the Internet.

6. **What are the main benefits of connecting to the Internet via DSL?**

DSL can provide virtually instantaneous transmission of voice, data and video over ordinary copper phone lines. A DSL connection can eliminate the frustrating delays associated when waiting to download information and graphics from the Internet. It provides residential subscribers with a cost effective uninterrupted high speed Internet connection. For schools, businesses and branch offices, DSL provides fast access to mission-critical information on corporate Intranet servers and the Internet. Another significant benefit is that a DSL

connection is always on-line (like a LAN connection) with no waiting time for dialling or connecting.

7. **Why has it taken Telephone companies so long to deploy DSL?**

There are many reasons that affect the speed and ubiquity of actual deployment. Factors such as the level of an installed ISDN base, the existence of cable competition, the state of the existing local loop (distance between the central office and service user) architecture, the level of Internet access, content provision, and pricing, as well as individual Telco's strategies will create different conditions for DSL deployment on a region-by-region basis.

Though wide-scale commercial deployments have begun, there is still work to be done before DSL can be deployed to the consumer mass market. The Universal ADSL Working Group (UAWG) has agreed to establish a standard for interoperability in order to simplify DSL installation and facilitate retail solutions for the consumer mass market. Members of the group include Microsoft, Intel, Compaq, Ameritech, Bell Atlantic, Bell South, GTE, SBC Communications, Sprint and U S West. Other companies participating in the group include communications and chip companies such as Texas Instruments, Rockwell, Alcatel Telecom, Ariel Corporation, Ericsson Telecom AB, GlobeSpan Technologies and Nortel.

8. **Can everyone have Internet access via DSL services?**

Unfortunately DSL services are not yet universally available. DSL is being implemented in several metropolitan areas, but interoperability issues have to be resolved before DSL is fully implemented. Other factors also affect the rate of implementation. The cost of building the DSL infrastructure from the existing Telco's switching networks is expensive and may impact other revenue sources. Another consideration is whether the user is within a usable distance from the Central Office switching station. DSL networks do however continue to grow and the new telephone and Internet access sources of revenue should encourage expansion.

In addition, not all Telco's are offering Internet access yet and many that do are continuing to do so on a limited or trial basis.

Bell South has already begun to roll out its DSL service in major metropolitan markets in Louisiana, Georgia, Alabama, Florida, and North Carolina. In 1999, the company will extend service to another 23 markets. GTE's DSL service is now available in the following states: California, Florida, Hawaii, Illinois, Indiana, Kentucky, North Carolina, Oregon, Texas, Washington, Michigan, Ohio, Virginia, Missouri, Pennsylvania, and Wisconsin. Bell Atlantic's DSL service now is available in selected Washington, D.C., Pittsburgh, Philadelphia and New Jersey metropolitan areas. New York and Boston will be among the markets added early in 1999. US West's roll out of their DSL service is expected to reach over 400,000 customers in the Phoenix area by the end of 1999.

ISP's slow deployment of DSL has made it difficult to predict how widely the services will be available. The Yankee Group Inc. expects 300,000 DSL lines to be installed by year-end and 1.78 million by the year 2000. Similarly, TeleChoice Inc. forecasts 1 million lines by the turn of the century. (A year ago, however, TeleChoice estimated 5 million DSL lines by 2000).

Many industry analysts predict that throughout 1999 DSL services will be deployed on a larger scale and made available to the consumer mass market. If you are interested in access to the Internet via DSL but are unsure whether its available in your area, call your Telco or ISP and ask them about their DSL plans.

9. **When will DSL be available to the rest of the world?**

In other markets such as Germany and the Scandinavian countries, large Telco's have made public commitments to DSL deployment. However in most industrialised markets, DSL deployment is currently limited to trials. This is presently the case in Japan, New Zealand, Australia, Switzerland, Belgium, the UK, Netherlands, France, Italy, Spain, Taiwan, and Korea. (Trials and/or limited deployment are also occurring in some developing countries, e.g. Brazil, China.)

10. **How do I get connected to the Internet via DSL?**

If you are already connected to an ISP for Internet access, you will only have to determine if your ISP supports DSL technology and what their rates are. If you are not yet connected to the Internet, you will have to determine which ISP is available to you, if you are able to purchase Internet access only, if you are obligated to buy or rent the connection equipment, such as modems, routers or splitters from your ISP or if you can purchase them separately. The technology is changing rapidly, but the important thing is to ensure your equipment matches the provider's equipment.

11. **Do I need a separate telephone line for the DSL service?**

This will depend upon your present set-up and the type of DSL service that is being installed. If you are using ADSL, your Telco or DSL ISP will put a POTS splitter box in your home or office to separate the voice and data traffic coming through on the same line. Your computer, telephone and Internet access will all be routed through this single connection. If you are using SDSL, a separate phone line may need to be installed for your DSL connection in addition to your normal telephone line.

12. **What is the theoretical performance of DSL?**

As mentioned previously, there are different types of DSL services. They are:

ADSL -Asymmetric Digital Subscriber Line
R-ADSL -Rate-Adaptive Digital Subscriber Line
HDSL -High Bit-Rate Digital Subscriber Line
VDSL -Very High Bit-Rate Digital Subscriber Line
SDSL -Symmetric Digital Subscriber Line

Here is a simple table for you to see the theoretical performances of the different types of DSL services. As you can see the theoretical performance of some DSL services are quite comparable to T1 and E1 speeds that are usually more appropriate in Universities and corporate environments. Note however that many users of high speed connectivity often purchase subsets (i.e. lesser) bandwidth than the theoretical maximum.

Connection	Maximum Transfer Rate	Distance Limitations Using 24-Gauge Wire
56 K Analogue Modem	56 kbit/s	None
ISDN	Up to 128 Kbps (Multilink PPP)	3.4 miles / 5.4 Km
Cable Modem	10-30 Mbit/s Downstream 128 kbit/s to 10 Mbit/s Upstream (Shared bandwidth)	30 miles / 48 Km over coaxial cable
ADSL	1.5 - 8 Mbit/s Downstream Up to 1.544 Mbit/s Upstream	3.4 miles / 5.4 Km
HDSL	T1 - 1.544 Mbit/s (2 wire pairs) E1 - 2.048 Mbit/s (3 wire pairs)	2.2 miles / 3.6 Km 3.4 miles / 5.4 Km
SDSL	T1 - 1.544 Mbit/s E1 - 2.048 Mbit/s	2 miles / 3 Km
VDSL	13 - 52 Mbit/s Downstream 1.5 - 2.3 Mbit/s Upstream Up to 34 Mbit/s if symmetric	1,000 ft/304 m 4,500 ft/1371 m depending on speed
R-ADSL	1.5 - 8 Mbit/s Downstream Up to 1.544 Mbit/s Upstream	3.4 miles / 5.4 Km

13. **What is the real-world performance of DSL?**

One factor which affects the performance of DSL services is distance from the Telco Central Office to the home, school or business which the DSL line is connected to. In the table above you will see a column for distance. This represents the maximum distance at which you would see the bandwidth listed for that service. The further away you are from the Central Office, the lower the perceived speed.

14. **How do I determine how far I am from my Central Office?**

Your ISP or Telco should be able to calculate this information for you in airline and/or wire feet. The closer you are to your Central Office, the higher the speeds you can achieve using DSL. This will also determine the type of DSL service available to you.

15. **What equipment do I need to get connected to the Internet?**

The hardware required to make DSL work is effectively a DSL modem (in your home or office). It is possible to lease your DSL modem directly from your Telco or DSL ISP to ensure complete compatibility with their network equipment.

There are two other pieces of equipment you'll need on your end to make your DSL modem work: a computer, and an interface card such as an Ethernet 10base T card.

16. **How does the DSL line physically attach to my computer?**

The DSL modem is plugged into the telephone line and the ethernet cable connected to the DSL modem is plugged into the back of a computer, into a router or into a ethernet hub to distribute the access to other computers. A router requires a single IP address for itself, supplied by the ISP. The router then connects to an ethernet network utilising ethernet cables. If the modem is plugged directly into your computer, a specially wired cable called a "crossover cable"(which can be purchased for around $5.00) has to be used. DSL modems can also be an internal PCI card which accept the DSL line directly.

17. **What if I have more than one computer?**

If you wanted to connect several computers at one location to the Internet using traditional one-by-one methods each computer system would require an individual modem/ISDN Terminal Adapter, separate telephone lines, separate ISP accounts, etc. Alternatively you could use a dedicated hardware router and obtain a business account from your ISP. These usually require hardware updates above and beyond the initial cost. This alternative also requires technical skills (hardware routers are not for the faint hearted) and the business ISP account may be costly.

A SmartGuard solution is an easy-to-use cost-effective alternative. It will allow multiple users on a local network to simultaneously share one ordinary ISP account and one DSL connection to the Internet.

The combination of a SmartGuard solution and a DSL modem is ideal in a number of scenarios where Internet access is required by more than one computer, whether at home, school or in business.

18. **What is the set-up process?**

Your Telco or ISP should be able to run engineering tests on your lines which will determine what speeds are available to you. Decide on a cost/speed package. Get a due date from your ISP (usually within 10 to 30 days). Before the due date the lines up to your home, school or business will be provisioned for DSL. The hardware will be brought to you or sent to you by the due date. On the due date technicians will come to your home or business to 'turn up' the circuit (so that you can use the DSL service). Before this day you should square away the details of your account with your ISP with regard to a regular dial-up account, DNS, IP addresses, and billing.

19. **Does DSL provide regular phone service also?**

Some Telco's provide POTS service on the DSL line. This means that you get a POTS splitter box that lets you plug a telephone, fax machine, regular modem, or answering machine into the DSL line in addition to the DSL modem. Simultaneous use of POTS service does not 'eat

into' DSL bandwidth. However, some Telco's do not offer the capability of running POTS on their DSL lines and will install a new line to be used only for the DSL service.

20. **Can I convert my existing line to DSL or do I need a new line?**

In many cases you can convert an existing line to a DSL line. However, the best path to take would be to call your local Telco or ISP for further information.

21. **Can I convert an ISDN line to DSL?**

ISDN lines can, in most cases, be converted to DSL.

22. **How much does it cost?**

It varies. DSL service availability is still in the early stages, but pricing in some areas has been very aggressive. There are charges for the line and hardware and also for the Internet access. Check with your Telco or ISP to find out about pricing.

23. **How am I billed?**

This will depend on your ISP. Some will bill you directly for all costs associated with your DSL lines. Others will charge only for Internet access and you will receive a separate bill from your Telco for their services.

24. **How should I choose between what type of connection to use?**

The decision to use either DSL or a dial up service depends upon the facilities offered by your Telco or DSL ISP when compared against another ISP offering a dial up service.

The following are a few considerations when deciding what type of connection to use and who to use to provide your Internet access.

- What Internet services do you want to use, such as email, web browsing, file transfers, etc.?
- How much does the Internet account cost per month?
- Are there costs for making a phone call to your ISP?
- Does your ISP have any additional charges?
- Does each service offer you sufficient email addresses?
- Are you able to get personal web space?
- Do you require additional phone lines to be installed?
- Can the ISP be accessed through a local call?

Considerations might be the number of mailboxes that you are allowed, the amount of personal web space, is your Internet Service a flat fee or is it a scalable charge depending upon the amount of data you transfer and the services you require.

Firstly, it is a good idea to decide what is important to you, then, which of the available providers is best suited to deliver those services.

24. **What is the point of having all this bandwidth available?**

Initially this service was designed with business in mind. It was meant for remote Local Area Networks to be able to act seamlessly as one network. It was also designed for the person working from the home office to have rapid access to the network in order to maximise their productivity and time. The benefits of having this service are obvious. These services allow the home office/small office user the capability of accessing network servers (i.e. WWW, mail, FTP, etc.) without being restricted by the long access and transfer times imposed by ordinary analogue modem and ISDN lines.

25. **What is "Splitterless" DSL Technology?**

As mentioned previously a POTS splitter box divides the standard telephone line so it can carry voice and data simultaneously. "Splitterless" DSL technology (also referred to as DSL-Lite) does not require an on-site installation (as no box needs to be installed). "Splitterless" DSL achieves that division with software rather than hardware.

26. **Can I convert from my existing DSL service to "Splitterless" DSL?**

Standard DSL technology is convertible to "splitterless" technology. Telco's are expected to offer "splitterless" DSL to all is existing and future subscribers when it becomes widely available throughout 1999. If you are interested in "splitterless" DSL call your Telco or DSL ISP fore more information.

27. **What's the downside of using DSL?**

There is a cost to a Telco associated with deploying DSL but it is small compared with the cost of digging up roads to install cable. The cost of DSL is expected to drop once the new "splitterless" technology (DSL-Lite) becomes widely available. There are also limits to the distance over which DSL can be used, so that the user needs to be within a maximum distance of the Central Office.

28. **What's the bottom line? What does SmartGuard recommend?**

SmartGuard does not sell DSL or access to the Internet via DSL modems. Furthermore, our products can be used with any type of Internet connection, be it modem dial-up, ISDN, T1, DSL or cable modem. In other words, we are neutral on the subject of how people connect to the Internet (but will admit to being biased to encouraging them to do so in some way).

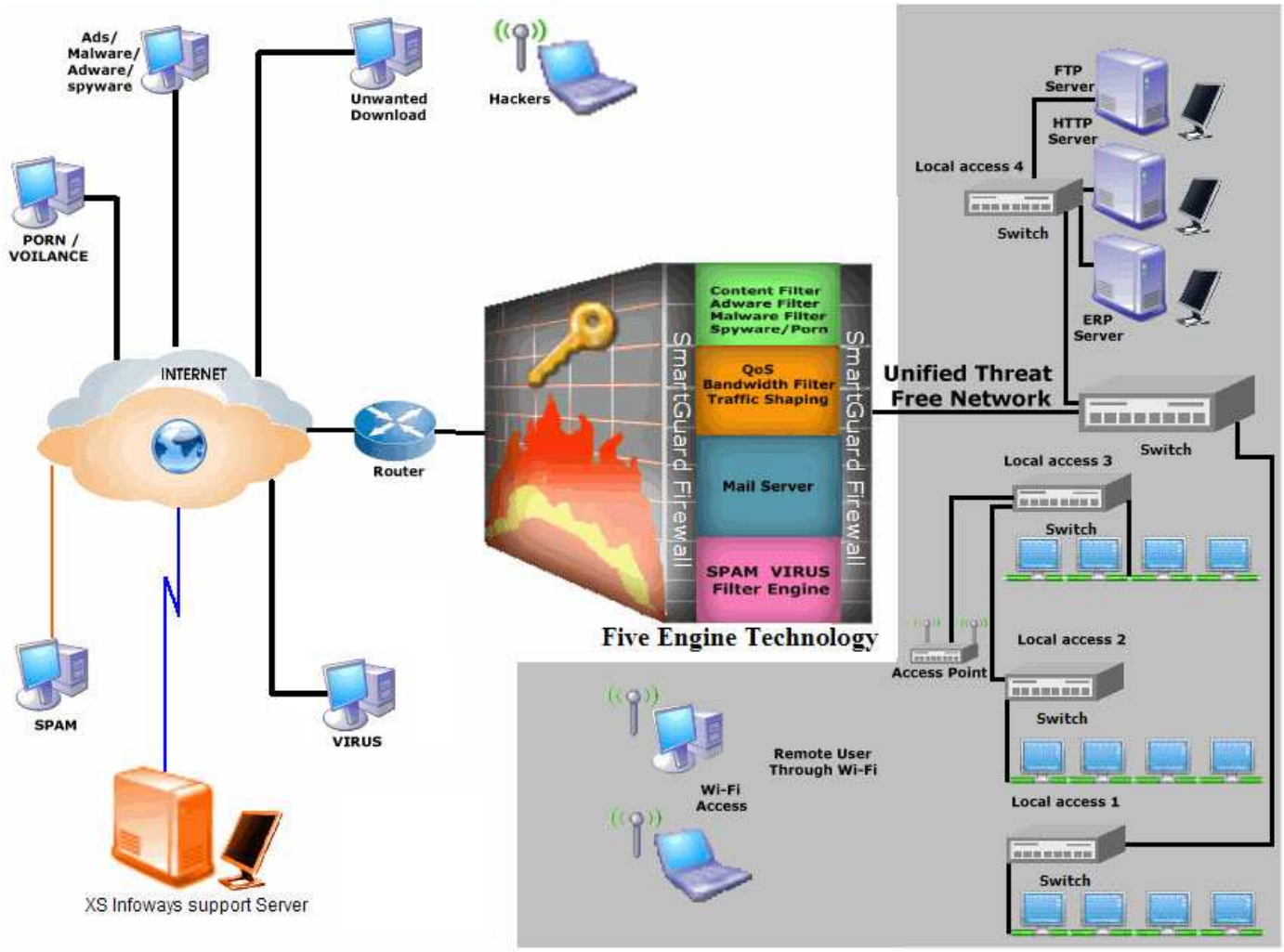
From our tests and customer feedback, plus the recent progress made by phone companies and Internet Service Providers, accessing the Internet via ADSL is an option that is definitely worth considering for users who have it available to them.

smartguard

Chapter 21

Real Life Scenarios And Case Studies

XS Infoways
the invincible technology

ver. **4.0.4**
Updated:06/27/2006

21. REAL LIFE SCENARIOS AND CASE STUDIES