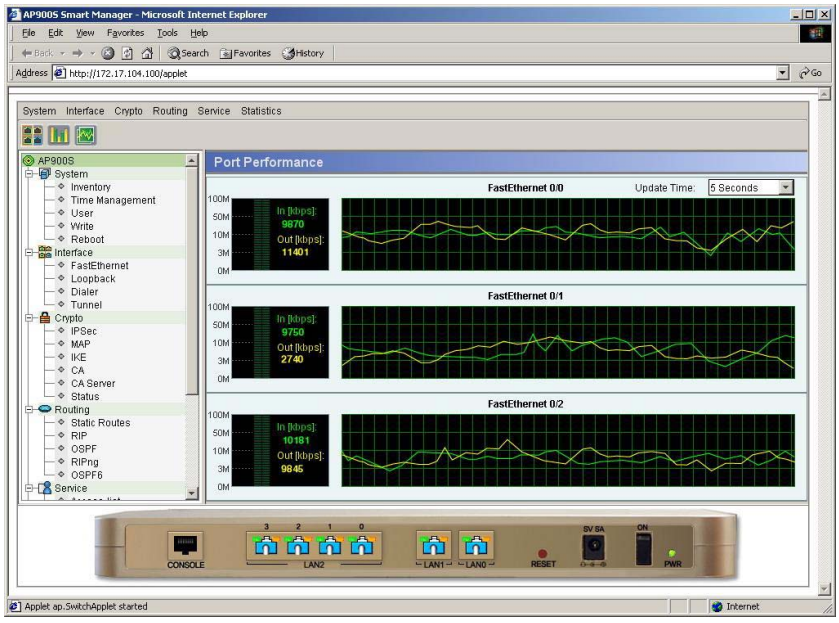
Smart Manager

Operation Guide for AP900S

Release 1.00

August, 2004



AddPac Technology Co., Ltd.

2/ 3F, Jeong-Am Bldg, Kangnam-Gu,

Seoul, Korea, Zip 135-080

Phone +82 2 568-3848

Fax +82 2 568-3847

E-mail : info@addpac.com

http://www.addpac.com

[CONTENTS]

Chapter 1. AP900S Introduction 16

SecureFinder AP900S Introduction **16**

SecureFinder AP900S Product Overview **16**

AP900S Main features 17

AP900S Hardware Specification **18**

AP900S Software functions **19**

AP900S Figure **21**

Chapter 2. Smart Manager Connection 22

Smart Manager Introduction **22**

Smart Manager Feature Highlights **22**

Hardware Requirement for Smart Manager **23**

Java 2 Runtime Environment v1.4.2 Download **24**

Java 2 Runtime Environment v1.4.2 Installation **28**

Smart Manager Access **31**

Chapter 3. Smart Manager Menus 34

Smart Manager Screen Elements **34**

How to Use Shortcut Icons **42**

System Menu **47**

Inventory 47

Time Management 48

User Management 50

Write 56

Reboot 57

System Popup Menu 58

Interface Menus **63**

FastEthernet 63

Loopback 100

Dialer 110

Tunnel 127

Interface Popup Menu 134

Crypto Menu **136**

IPSec 136

MAP 144

IKE 161

CA..... 172
CA Server 174
Status 179
Routing Menu 180
Static Routes 180
RIP 191
OSPF 202
RIPng 218
OSPF6 226
Service menu 235
Access-List 235
DHCP 251
ARP 259
DNS 262
SNMP 266
Misc 271
Statistics Menu 274
System Performance 274
Port Performance 275
Port Statistics 277
AP900S control method on the front panel 279
Introducing the front ports of AP900s 279
Checking list for Smart Manager connection failure 283
IPSec related technical term 284

[Table of Figures]

(Figure1-1) SecureFinder AP900S의 network diagram 17
(Figure1-2) SecureFinder AP900S Front 21
(Figure1-3) SecureFinder AP900S Rear 21
(Figure2-1) Select Java 2 Platform Standard Edition 24
(Figure2-2) Select J2SE Windows 25
(Figure2-3) License Agreement for J2SE 25
(Figure2-4) Java 2 Runtime Environment, SE v1.4.2_01 downlaod 26
(Figure2-5) File Download Dialog Box 26
(Figure2-6) Downloading the file 27
(Figure2-7) Java 2 Runtime Environment – License 28
(Figure2-8) Select Java 2 Setup Type 29
(Figure2-9) Java 2 installation processing 29
(Figure2-10) Java 2 Runtime installation completion 30
(Figure2-11) Web Management System access 31
(Figure2-12) Web Management System Login 31
(Figure2-13) Initial window of Web Management System 32
(Figure2-14) Java Applet security warning page 32
(Figure2-15) Java Applet Login 33
(Figure2-16) Smart Manager main page window 33
(Figure3-1) Smart Manager Elements Page 34
(Figure3-2) Pull Down Menu – system 35
(Figure3-3) Pull Down Menu – system -> Inventory 35
(Figure3-4) Pull Down menu –> FastEthernet 36
(Figure3-5) Pull Down menu – FastEthernet page 36
(Figure3-6) Pulll Down menu –> Crypto -> IPSec 37
(Figure3-7) Pull Down menu – IPSec Config page 37
(Figure3-8) Pull Down Menu –>Routing-> Static Routes 38
(Figure3-9) Pull Down Menu– Static Routes page 38
(Figure3-10) Pull Down Menu –>Service-> Access-list 39
(Figure3-11) Pull Down Menu – Access-list page 39
(Figure3-12) Pull Down menu –>Statistics-> System Performance 40
(Figure3-13) Pull Down Menu – System Performance page 40
(Figure3-15) FastEthernet icon 43
(Figure3-16) FastEthernet page 43
(Figure3-17) Port Performance Icon 44
(Figure3-18) Port Performance History Shortcut Icon 44

(Figure3-19) Port Statistics Icon 45
(Figure3-20) Port Statistics page 45
(Figure3-21) Tree menu of AP900S 46
(Figure3-22) System-Inventory 47
(Figure3-23) Time Management window 48
(Figure3-24) Time Management Elements 49
(Figure3-25) User Management main window 50
(Figure3-26) Configuring User Management elements 51
(Figure3-27) Input User Management ID 52
(Figure3-28) Select User Management Password Type 52
(Figure3-29) Enter User Management Password 53
(Figure3-30) User Management –new ID 53
(Figure3-31) User Management-select user ID 54
(Figure3-32) Select User Management Delete Row 54
(Figure3-33) User Management user ID deleted 55
(Figure3-34) Write menu page 56
(Figure3-35) System Reboot main page 57
(Figure3-36) System Popup Menu page 58
(Figure3-37) System Version Info page 59
(Figure3-38) System Running-Config page 60
(Figure3-39) System Startup-Config page 61
(Figure3-40) System User Info page 62
(Figure3-41) FastEthernet Main page 63
(Figure3-42) FastEthernet Interface Link Status Info 64
(Figure3-43) Interface IPv4 Info 65
(Figure3-44) Interface IPv4 RIP Info 66
(Figure3-45) Interface IPv4 OSPF Info 67
(Figure3-46) Interface IPv6 Info 69
(Figure3-47) Interface IPv6 OSPFv3 Info 70
(Figure3-48) Interface Crypto Info 71
(Figure3-49) Select Fast Ethernet 0/1 72
(Figure3-50) Input Fast Ethernet 0/1 Description 72
(Figure3-51) Select Fast Ethernet 0/1 Link Speed 73
(Figure3-52) Select Fast Ethernet 0/1 Link Duplex 73
(Figure3-53) Input Fast Ethernet PPPoE Dialer 74
(Figure3-54) Input Fast Ethernet Fixed IP Address 74
(Figure3-55) Input Fast Ethernet Fixed IP Address 75
(Figure3-56) Change Fast Ethernet MTU 75
(Figure3-57) Select Fast Ethernet Access Filter Inbound 76

(Figure3-58) Select Fast Ethernet Access Filter Outbound 76
(Figure3-59) Checking Fast Ethernet IPv4 value 77
(Figure3-60) Select Fast Ethernet IPv4 Routing RIP 78
(Figure3-61) Select Fast Ethernet RIP Send Version 78
(Figure3-62) Select Fast Ethernet RIP Receive Version 79
(Figure3-63) Select Fast Ethernet RIP Split-Horizon 79
(Figure3-64) Select RIP Authentication Method 80
(Figure3-65) Input MD5 Password String 80
(Figure3-66) Input MD5 KeyChain 81
(Figure3-67) Check RIP configuration setting 81
(Figure3-68) Select Fast Ethernet IPv4 Routing OSPF 82
(Figure3-69) Input OSPF Interface Cost 82
(Figure3-70) Input OSPF Interface Priority 83
(Figure3-71) Input OSPF Hello Interval 83
(Figure3-72) Input OSPF Dead Interval 84
(Figure3-73) Input OSPF Retransmit Interval 84
(Figure3-74) Input OSPF Transmit Delay 85
(Figure3-75) Select OSPF Network Type 85
(Figure3-76) Select OSPF Authentication Method 86
(Figure3-77) Input Message Digest Key ID 86
(Figure3-78) Input Message Digest Password 87
(Figure3-79) OSPF configuration setting verify 87
(Figure3-80) Select Fast Ethernet IPv6 88
(Figure3-81) Input IPv6 Address 88
(Figure3-82) Select IPv6 Access Filter Inbound 89
(Figure3-83) Select IPv6 Access Filter Outbound 89
(Figure3-84) Adding IPv6 Address & Access Filter verify 90
(Figure3-85) Delete IPv6 Address 90
(Figure3-86) Verifying IPv6 Address delete 91
(Figure3-87) Select IPv6 OSPFv3 92
(Figure3-88) Input OSPFv3 Cost 92
(Figure3-89) Input OSPFv3 Interface Priority 93
(Figure3-90) Input OSPFv3 Hello Interval 93
(Figure3-91) Input OSPFv3 Dead Interval 94
(Figure3-92) Input OSPFv3 Retransmit Interval 94
(Figure3-93) Input OSPFv3 Transmit Delay 95
(Figure3-94) Input OSPFv3 Instance ID 95
(Figure3-95) Input OSPFv3 Prefix-List 96
(Figure3-96) OSPFv3 Passive Interface check 96

(Figure3-97) Verify OSPFv3 settings 97
(Figure3-98) Select Fast Ethernet Crypto 98
(Figure3-99) Select Fast Ethernet Crypto Map 98
(Figure3-100) Verify Interface Crypto Map 99
(Figure3-101) Loopback initial page 100
(Figure3-102) Network (including Loopback Interface) Example 101
(Figure3-103) Loopback Interface page 102
(Figure3-104) Loopback IPv4 Main page 103
(Figure3-105) Loopback Interface Crypto Info 104
(Figure3-106) Add Loopback1 Interface 105
(Figure3-107) Input Loopback1 Interface Description 105
(Figure3-108) Input IPv4 Address 106
(Figure3-109) Input Subnet Mask of IPv4 Address 106
(Figure3-110) Input IPv4 MTU 107
(Figure3-111) Input IPv6 Address 107
(Figure3-112) Input IPv6 MTU 108
(Figure3-113) Loopback1 Interface verify page 108
(Figure3-114) Delete Loopback1 Interface 109
(Figure3-115) Loopback1 Interface delete verify. 109
(Figure3-116) Dialer main page 110
(Figure3-117) Dialer Interface elements 111
(Figure3-118) Dialer IPv4 Address elements 112
(Figure3-119) Authentication method for PPP Session creation 113
(Figure3-120) Dialer PAP Configuration 114
(Figure3-121) Dialer CHAP Configuratoin 115
(Figure3)-122 Dialer LCP Configuration 116
(Figure3-123) Dialer IPCP Configuration 117
(Figure3-124) Dialer IPv6CP configuration 118
(Figure3-125 Create Dialer1 Interface) 119
(Figure3-126) Input Description 120
(Figure3-127) Select Encapsulation 121
(Figure3-128) Alter Administrative Link State 121
(Figure3-129) Select Negotiated via PPP 122
(Figure3-130) Check Authentication 122
(Figure3-131) Check PAP Callin 123
(Figure3-132) Input PAP Username 123
(Figure3-133) Input PAP User Password 124
(Figure3-134) Check LCP ACFC 124
(Figure3-135) Check LCP PFC 125

(Figure3-136) Check IPCP DNS Request, Default Router 125
(Figure3-138) Tunnel main page 127
(Figure3-139) Tunnel Interface example Network Diagram 1 128
(Figure3-140) Tunnel Interface example Network Diagram 2 128
(Figure3-141) Tunnel main page 129
(Figure3-142) Input Tunnel Interface Name 130
(Figure3-143) Input Tunnel Interface Description 130
(Figure3-144) Select Tunnel Mode 131
(Figure3-145) Input Tunnel Interface IP Address 131
(Figure3-146) Input Tunnel Interface Destination IP Address 132
(Figure3-147) Input Tx Packet ToS 132
(Figure3-148) Input Tx Packet TTL 133
(Figure3-149) Tunnel Interface creation 133
(Figure3-150) Interface Popup Menu Main page. 134
(Figure3-151) Interface Info page 135
(Figure3-152) Stages of realizing IPSec 136
(Figure3-153) Crypto IPSec Main page 137
(Figure3-154) IPSec Menu 138
(Figure3-155) Transport Mode and Tunnel Mode 139
(Figure3-156) ESP Packet structure 139
(Figure3-157) AH Packet Structure 140
(Figure3-158) Input IPSec Transform-set name 141
(Figure3-159) Select IPSec Transform-set Mode 141
(Figure3-160) IPSec Authentication main page 142
(Figure3-161) Select IPSec Encryption 142
(Figure3-162) Select IPSec Data Compression 143
(Figure3-163) Root Parameters configuration page 143
(Figure3-164) Crypto MAP main page 144
(Figure3-165) IPSec-ISAKMP Menu 145
(Figure3-166) IPSec-Manual menu page 147
(Figure3-167) Input IPSec-ISAKMP Name 149
(Figure3-168) Input IPSec-ISAKMP S/N 149
(Figure3-169) Input IPSec-ISAKMP Peer Address 150
(Figure3-170) Input IPSec-ISAKMP Match Address 150
(Figure3-171) Input IPSec-ISAKMP Transform-set 151
(Figure3-172) Select IPSec-ISAKMP Diffie-Hellman Group 151
(Figure3-173) Input IPSec-ISAKMP SA Lifetime 152
(Figure3-174) Input IPSec-Manual Name 153
(Figure3-175) Input IPSec-Manual S/N 153

(Figure3-176) Input IPSec-Manual Peer Address 154
(Figure3-177) Input IPSec-Manual Match Address..... 154
(Figure3-178) Input IPSec-Manual Transform-set 155
(Figure3-179) Select IPSec-Manual Protocol in..... 155
(Figure3-180) Input IPSec-Manual Spi in..... 156
(Figure3-181) Input IPSec-Manual Cipher-key in 156
(Figure3-182) Input IPSec-Manual Auth-key in..... 157
(Figure3-183) Select IPSec-Manual Protocol out..... 157
(Figure3-184) Input IPSec-Manual Spi out..... 158
(Figure3-185) Input IPSec-Manual Cipher-key out 158
(Figure3-186) Input IPSec-Manual Cipher-key out 159
(Figure3-187) Input IPSec-Manual Auth-key out..... 159
(Figure3-188) Verify IPSec-Manual settings..... 160
(Figure3-189) IKE Policy Main page..... 161
(Figure3-190) IKE Policy Menu 162
(Figure3-191) Input IKE Policy Priority 163
(Figure3-192) Select IKE Policy Authentication Method 163
(Figure3-193) Select IKE Policy Encryption Algorithm..... 164
(Figure3-194) Select IKE Policy Hash Algorithm..... 164
(Figure3-195) Select IKE Policy Diffe-Hellman Group 165
(Figure3-196) Input IKE Policy Lifetime..... 165
(Figure3-197) IKE Key Menu 166
(Figure3-198) Select IKE Key Peer Type 167
(Figure3-199) Input IKE Key Peer IP Address 167
(Figure3-200) Input IKE Key Subnet mask..... 168
(Figure3-201) IKE Key Menu 168
(Figure3-202) IKE Key configuration verify 169
(Figure3-203) IKE Key Peer Menu page I..... 170
(Figure3-204) IKE Key Peer Menu page II..... 170
(Figure3-205) IPSec using certificate of CA Server..... 172
(Figure3-206) Crypto CA menu..... 173
(Figure3-207) Crypto CA Server main page 174
(Figure3-208) CA Server in AP900S Diagram 175
(Figure3-209) Crypto CA Server Menu..... 176
(Figure3-210) Crypto CA Server Enable Menu page..... 177
(Figure3-211) Crypto CA Server Enable input example 178
(Figure3-212) Crypto CA Server Request input example 178
(Figure3-213) Crypto Status Session page 179
(Figure3-214) Crypto Status Policy page 179

(Figure3-215) Static Routes Main page 180
(Figure3-216) IP version 4 Static Routes page 181
(Figure3-217) IP version 6 Static Routes page 182
(Figure3-218) Input IP version 4 Static Routes Destination IP Address 183
(Figure3-219) Input IP version 4 Static Routes Subnet Mask 183
(Figure3-220) Input IP version 4 Static Routes Gateway Address 184
(Figure3-221) Input IP version 4 Static Routes Distance 184
(Figure3-222) Verify IP version 4 Static Routes settings. 185
(Figure3-223) Select IP version 4 Static Route you want to delete 186
(Figure3-224) Delete IP version 4 Static Route 186
(Figure3-225) Verify IP version 4 Static Routes delete. 187
(Figure3-226) Input IP version 6 Static Routes Destination 188
(Figure3-227) Input IP version 6 Static Routes Gateway Address 188
(Figure3-228) Input IP version 6 Static Routes Distance 189
(Figure3-229) IP version 6 Static Routes configuration verify 189
(Figure3-230) Select Static Routes Pop menu 190
(Figure3-231) IP version 4 Static Routes Routing Table Verify 190
(Figure3-232) Routing RIP Main page 191
(Figure3-233) RIP Network Diagram 192
(Figure3-234) RIP General Main page 193
(Figure3-235) Input RIP Distance 194
(Figure3-236) Input RIP Version 194
(Figure3-237) Input RIP Update-Interval 195
(Figure3-238) Input RIP Routing-Timeout 195
(Figure3-239) Input RIP Garbage-Collection 196
(Figure3-240) RIP Network Main page 197
(Figure3-241) Add RIP Network Address 197
(Figure3-242) Input RIP Network Subnet Mask 198
(Figure3-243) New RIP Network verify 198
(Figure3-244) RIP Redistribution Main page 199
(Figure3-245) RIP Pop menu page 200
(Figure3-246) RIP Info Page 200
(Figure3-247) RIP Database Page 201
(Figure3-248) Routing OSPF Main page 202
(Figure3-249) OSPF Network Diagram 203
(Figure3-250) OSPF General main page 204
(Figure3-251) Input OSPF General Distance 205
(Figure3-252) Input OSPF General Inter-area Distance 205
(Figure3-253) Input OSPF General Intra-area Distance 206

(Figure3-254) Input OSPF General External Distance 206
(Figure3-255) Input OSPF General Router-ID 207
(Figure3-256) OSPF Network Page 208
(Figure3-257) Add a new OSPF Network Address 208
(Figure3-258) Input OSPF Network Subnet mask 209
(Figure3-259) Input OSPF Network Area-ID 209
(Figure3-260) OSPF Network verification page 210
(Figure3-261) OSPF Area page 211
(Figure3-262) Input OSPF Area 212
(Figure3-263) Select OSPF Area authentication method 212
(Figure3-264) Input OSPF Area Default Cost 213
(Figure3-265) OSPF Redistribution page 214
(Figure3-266) OSPF Pop Menu page 215
(Figure3-267) OSPF Routing Table page 215
(Figure3-268) OSPF Info page 216
(Figure3-269) OSPF Routing Info page 216
(Figure3-270) OSPF Interface Info page 217
(Figure3-271) OSPF Database Info page 217
(Figure3-272) Routing RIPng Main page 218
(Figure3-273) RIPng General Menu page 219
(Figure3-274) Input RIPng General Distance 220
(Figure3-275) Input RIPng General Update-Interval 220
(Figure3-276) Input RIPng General Routing-Timeout 221
(Figure3-277) Input RIPng General Garage-Collection 221
(Figure3-278) RIPng General Configuration verify 222
(Figure3-279) RIPng Prefix menu page 223
(Figure3-280) Input RIPng Prefix IPv6 223
(Figure3-281) Verify RIPng Prefix IPv6 224
(Figure3-282) RIPng Redistribution menu page 225
(Figure3-283) Routing OSPF6 Main page 226
(Figure3-284) OSPF6 General Menu page 227
(Figure3-285) Input OSPF6 General Distance 228
(Figure3-286) Input OSPF6 General Router-ID 228
(Figure3-287) Select OSPF6 Network 229
(Figure3-288) Input OSPF6 Network Interface 229
(Figure3-289) Input OSPF6 Network Area ID 230
(Figure3-290) OSPF6 Network configuration verify 230
(Figure3-291) OSPF6 Redistribution page 231
(Figure3-292) Routing Pop menu page 232

(Figure3-293) Working Routing Table page 232
(Figure3-294) Working Routing Table for IPv6 page 233
(Figure3-295) Connected Routing Table page 233
(Figure3-296) Connected Routing Table for IPv6 page 234
(Figure3-297) Access-List Main page 235
(Figure3-298) Access-List Network Diagram 236
(Figure3-299) Create Standard Access-List 237
(Figure3-300) Input Access-ID, Remark 237
(Figure3-301) Access-ID creation verify. 238
(Figure3-302) Select Insert Action 238
(Figure3-303) Select Action, Source Address Type 239
(Figure3-304) Input Source Address Range 239
(Figure3-305) Access-List creation verify 240
(Figure3-306) Select Extended Access-List Create Access-ID 241
(Figure3-307) Input Extended Access-List Access-ID, Remark 241
(Figure3-308) Select Extended Access-List Insert Action 242
(Figure3-309) Extended Access-List 242
(Figure3-310) Extended Access-List creation verify 243
(Figure3-311) Select Name Access-List Create Access-ID 244
(Figure3-312) Input Name Access-List Access-ID, Remark 244
(Figure3-313) Select Name Access-List Insert Action 245
(Figure3-315) Name Access-List Verify 246
(Figure3-316) Select IPv6 Extended Access-List Create Access-ID 247
(Figure3-317) Input IPv6 Extended Access-List Access-ID, Remark 247
(Figure3-318) IPv6 Select Extended Access-List Insert Action 248
(Figure3-319) Writing IPv6 Extended Access-List 248
(Figure3-320) IPv6 Extended Access-List creation 249
(Figure3-321) Access-List Pop Menu 250
(Figure3-322) IPv4 Access-List page 250
(Figure3-323) DHCP Main page 251
(Figure3-324) DHCP Diagram 1 252
(Figure3-325) DHCP Diagram 2 252
(Figure3-326) Select DHCP Add Pool 253
(Figure3-327) Input DHCP Pool Name 253
(Figure3-328) Select DHCP Add Network 254
(Figure3-329) Input DHCP IP Address Range 254
(Figure3-330) Input IP Address Range for DHCP Client 255
(Figure3-331) Move to DHCP Address Range box. 255
(Figure3-332) Input DHCP Default Router IP Address 256

(Figure3-333) DHCP Router IP List page 256
(Figure3-334) Input DHCP DNS IP Address 257
(Figure3-335) Select DHCP Lease Duration 257
(Figure3-336) addpac DHCP Pool configuration 258
(Figure3-337) DHCP Pool Option page 258
(Figure3-338) ARP Main page 259
(Figure3-339) Input Static ARP Entry IP Address 260
(Figure3-340) Input Static ARP Entry MAC Address 260
(Figure3-341) Select ARP Pop Menu ARP Info 261
(Figure3-342) ARP Info page 261
(Figure3-343) DNS Main page 262
(Figure3-344) DNS Service Diagram example 263
(Figure3-345) DNS input example 264
(Figure3-346) Input Host Name 265
(Figure3-347) Input Host IP Address 265
(Figure3-348) SNMP Main page 266
(Figure3-349) SNMP System Option Input example 267
(Figure3-350) SNMP Community String example 268
(Figure3-351) SNMP Trap Managers example 269
(Figure3-352) SNMP Trap Managers page 269
(Figure3-353) Telnet/SSH Menu page 271
(Figure3-354) FTP menu page 272
(Figure3-355) HTTP Menu page 273
(Figure3-357) Port Performance page 275
(Figure3-358) Port Statistics page 276
(Figure3-359) System Performance page 277
(Figure3-360) AP900S 279
(Figure3-361) AP900S Front 280
(Figure3-362) Execute AP900S Front Port Configuration 281
(Figure3-363) Execute AP900S Front Port Configuration 281
(Figure3-364) Execute AP900S Front Port Status 282
(Figure3-365) HTTP Server from CLI 283
(Figure3-366) Enable HTTP Server from CLI 283

< Table of Tables >

<Table 1-1> AP900S Hardware Specification 18
<Table 1-2> AP900S software functions 19
<Table 2-1> Hardware Requirements 23
<Table 2-2> Software Requirements 23
<Table 3-1> Smart Manager Main Page Elements and Descriptions 34
<Table 3-2> Pull Down menu elements 41
<Table 3-3> Shortcut Icons & Description 42
<Table 3-4> Tree Menu & Description 46
<Table 3-5> Inventory Fields 47
<Table 3-6> Time Management Elements and Description 49
<Table 3-7> User Management elements & Description 51
<Table 3-8> System Popup Menu Description 58
<Table 3-9> Interface Link Status Info Description 64
<Table 3-10> Interface IPv4 Info Description 65
<Table 3-11> Interface IPv4 RIP Info Description 66
<Table 3-12> Interface IPv4 OSPF Info Description 67
<Table 3-13> Interface IPv6 Info Description 69
<Table 3-14> Interface IPv6 OSPFv3 Info Description 70
<Table 3-15> Loopback Interface Description 102
<Table 3-16> Loopback IPv4 Description 103
<Table 3-17> Dialer Interface Description 111
<Table 3-18> Dialer IPv4 Address Description 112
<Table 3-19> Dialer Authentication Method Description 113
<Table 3-20> Dialer PAP Description 114
<Table 3-21> Dialer CHAP Description 115
<Table 3-22> Dialer LCP Description 116
<Table 3-23> Dialer IPCP Description 117
<Table 3-24> Dialer IPv6CP Description 118
<Table 3-25> Tunnel Description 129
<Table 3-26> IPSec Description 138
<Table 3-27> IPSec-ISAKMP Menu Description 145
<Table 3-28> IPSec-Manual menu Description 148
<Table 3-29> IKE Policy menu Discription 162
<Table 3-30> IKE Key Menu Description 166
<Table 3-31> IKE Key Description 171

<Table 3-32> Crypto CA Description 173
<Table 3-33> Crypto CA menu Description 176
<Table 3-34> Crypto CA Enable menu Description 177
<Table 3-35> IP version 4 Static Routes menu Description 181
<Table 3-36> IP version 6 Static Routes menu description 182
<Table 3-37> RIP General menu Description 193
<Table 3-38> RIP Redistribution Description 199
<Table 3-39> OSPF General Menu Description 204
<Table 3-40> OSPF General Menu Description 211
<Table 3-41> OSPF Redistribution menu Description 214
<Table 3-42> RIPng General Menu Description 219
<Table 3-43> RIPng Redistribution menu Description 225
<Table 3-44> OSPF6 General Menu Description 227
<Table 3-45> OSPF6 Redistribution menu Description 231
<Table 3-46> ARP Menu Description 259
<Table 3-47> DNS menu Description 262
<Table 3-48> SNMP System Option Description 267
<Table 3-49> SNMP Community String Description 268
<Table 3-50> SNMP Trap Parameter Description 270
<Table 3-51> Telnet/SSH Description 271
<Table 3-52> FTP Description 272
<Table 3-53> HTTP elements Description 273
<Table 3-54> Port Statistics Description 278
<Table 3-55> AP900S front Description 280
<Table 3-56> IPSec related technical terms 284

Chapter 1. AP900S Introduction

SecureFinder AP900S Introduction

SecureFinder AP900S is a residential embedded VPN gateway based on IPSec standard. SecureFinder AP900S is suitable for small companies which require a strong secure policy to have access to important applications such as CRM, ERP, and Groupware of its head office.

SecureFinder AP900S Product Overview

1. Smart VPN gateway with strong features

SecureFinder AP900S is suitable for companies requiring high-performance, multi-functional VPN services. It supports not only protocols such as PPPoE for XDSL, cable modem connection but also various routing protocols such as Static and IEEE 802.1Q VLAN Routing, RIP v1/v2, OSPF v2, BGP v4. This SecureFinder AP900S provides advanced services which residential VPN gateway has never provided before.

2. Adopt Hardware VPN accelerator

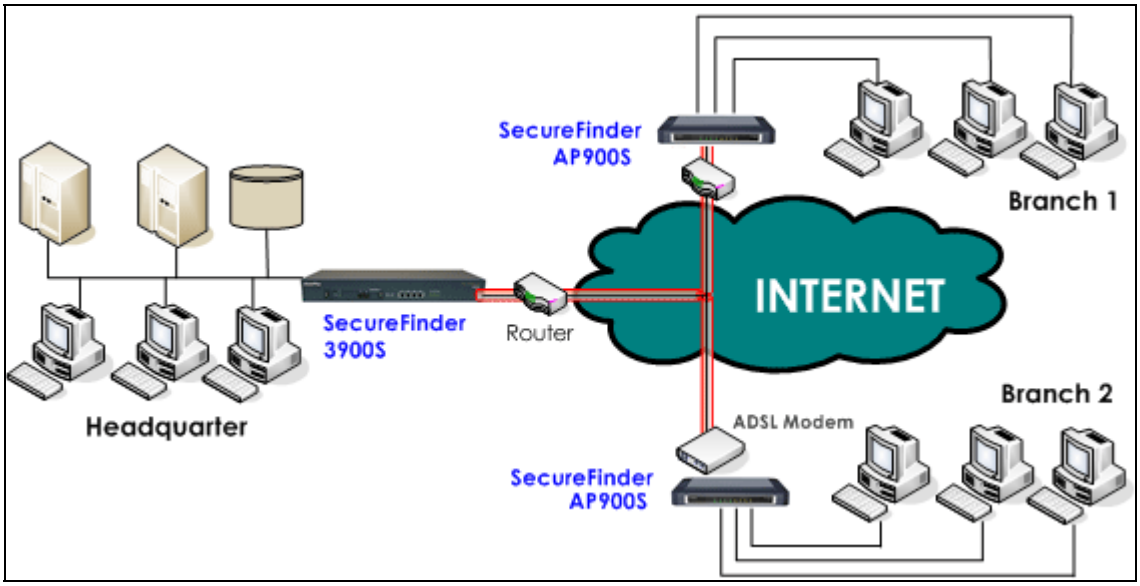
AP900S provides an optimized performance through hardware accelerator which is built in for VPN security. This controls network and system traffics enabling excellent VPN service. Based on AddPac's own embedded OS, APOS™, it delivers reliable VPN service and wide area network expansion service which can be adopted in any network environments. Also it is capable of using various algorithms such as DES, 3DES, AES so it is suitable for encryption algorithm and security policy.

3. The next-generation solution

Even for a small enterprise branch needs to have VPN gateway system for critical data applications, and secure VoIP calls from head office. It has to be prevented and protected by reliable security system such as VPN gateway. However, it is not easy for small business companies to realize secure data communication network and often unpredicted problems can be faced without IT expert. AP900S ensures network protection through the functions of VPN. It guarantees secure internet communications using embedded 4 ports 10/100Mbps hub which also has auto secure networking configuration function.

4. Streaming solution

Effective processing capability of streaming data such as video, audio(example, MP3) and VoIP application is one of the main considerations when it comes to choosing VPN system. SecureFinder AP900S offers excellent performance on processing multimedia data such as VoD, MP3 file, etc using QoS along with AddPac's own QoS features.



(Figure1-1) SecureFinder AP900S의 network diagram

AP900S Main features

- Residential VPN Gateway : embedded system type
- HW based security accelerator to reduce processing delay
- DMZ Zone for secure internet access such as Web, email etc
- Built in 4-Port Fast Ethernet Interface
- Authentication algorithm: MD5, SHA-1, HAS-160
- Encryption algorithm: DES, 3DES, AES etc
- Supports SSL/SSH communication functions
- Key managing : IKE Standard
- CA authentication : ID/Password, LDAP, X.509
- Flexible backup function using VRRP
- Embedded Advanced QoS features for multi-media application
- Real-time monitoring
- Supports Various routing service
- Various management services such as remote upgrade

AP900S Hardware Specification

<Table 1-1> AP900S Hardware Specification

Microprocessor	64bit RISC Microprocessor	
Memory	Flash Memory	8 Mbytes
	SDRAM Memory	64 Mbytes
	Boot Memory	512 Kbytes
Network Interface	2-Port 10/100Mbps Fast Ethernet Interface (RJ-45 interface) - Support Load Balancing - DMZ for Secure Web & E-mail Access - Creates a Public and Private Network Simultaneously	
	4-Port 10/100Mbps Fast Ethernet Interface for LAN - Support Auto Secure Service Configuration	
Console Port	1-Port RS-232C Console Interface(RJ-45 interface)	
Power	External Power, 110~220 VAC free voltage, 50/60Hz, 20Watt	
Operating Temperature	0 ~ 50 ℃ (32 ~ 122 ℉)	
Store Temperature	-40 ~ +85 ℃ (-40 ~ +185 ℉)	
Relative humidity	5 ~ 95 %	
Dimension	43 x 265 x 165 (mm, H x W x D)	

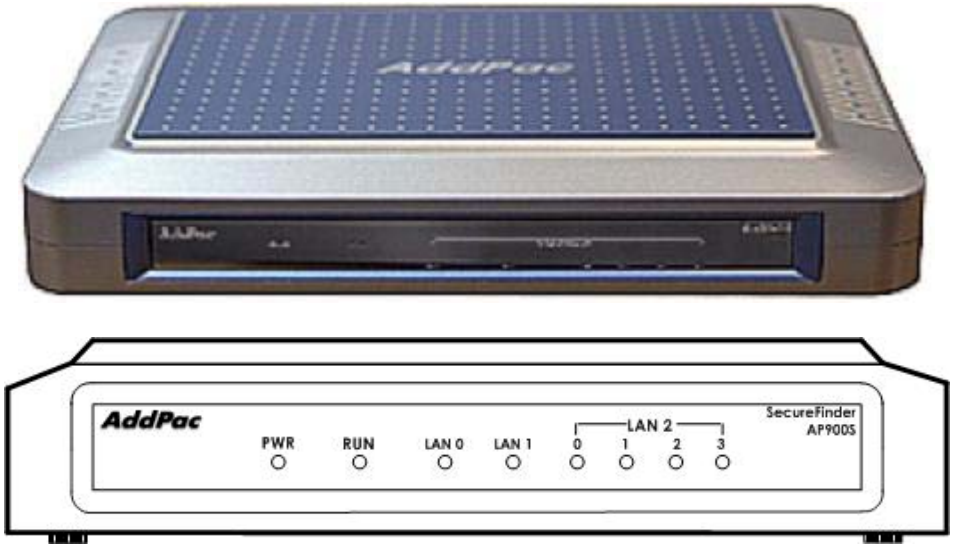
AP900S Software functions

<Table 1-2> AP900S software functions

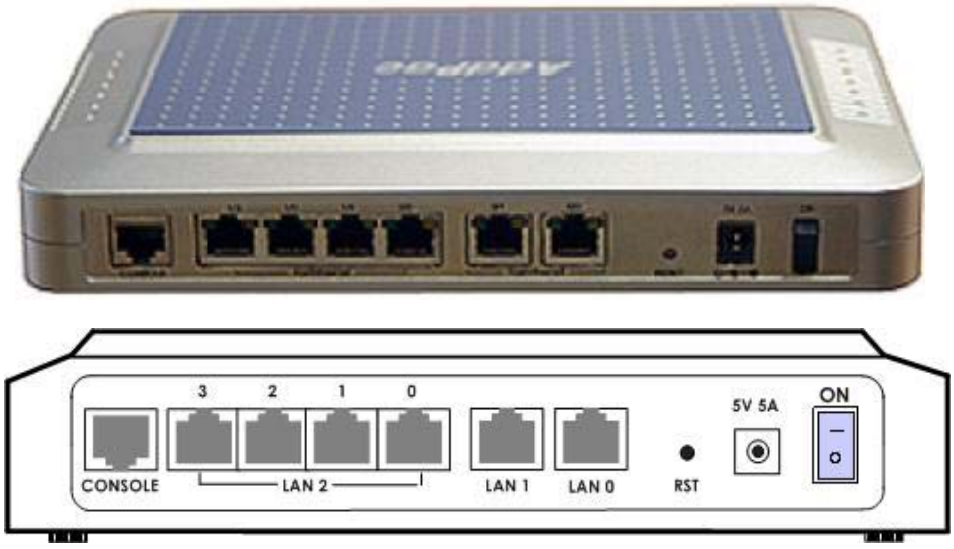
Network & Routing Protocol	Static and Default Routing
	RIP v1/v2, OSPF v2, BGP v4
	IEEE 802.1Q VLAN Routing
WAN Protocol	Point-to-Point over Ethernet Protocol (PPPoE) for ADSL Dynamic Host Configuration Protocol (DHCP) for Cable Modem
VPN function	Authentication Algorithm : MD5, SHA-1, HAS-160
	Key Management : IKE Standard
	CA Authentication : ID/Password, LDAP, X.509
	IP Authentication Header (AH)
	IP Encapsulation Security Payload (ESP)
	Authentication : PAP, CHAP, MS-CHAP, RADIUS
	Tunneling Protocol : PPTP, L2TP, IPSec
	IKE Encryption : DES, 3DES, AES, blowfish, cast
	IKE hash : MD5, SHA1
	IKE Authentication : Preshared-key, RSA-sig
	IKE Key Exchange : DH group 1(768), DH group 2(1024), DH group 5(1536)
	IKE lifetime : Second/Byte
	IKE Phase 1 : Main-mode, Aggressive-mode
	IKE Phase 2 : Quick-mode
	IPSec Protocol : AH(Authentication Header), ESP
	IPSec mode : Transport mode, Tunnel mode
	IPSec Encryption : DES, 3DES, AES, blowfish, cast, null
	IPSec Authentication : hmac-md5, hmac-sha1
	PFS : group1, group2, group5
	IPSec lifetime : Second/Byte
	Compression : LZS, deflate
	CA : CA Server, SCEP, OCSP
	VPN Tunnel Monitoring, Prevent Replay Attack
	NAT-Traversal : IPSEC Communication in NAT Environment with L2TP
Security	Supports IP Packet Filtering
	Supports IP Access-List

	User Authentication function (PAP, CHAP)
	Protocol Enable/Disable function
	Auto-disconnect function for Console, Telnet Session
	Multi-Level User Account Management function
Network management	Web based management feature: Java Based Manager
	Supports SSL/SSH communication
	Supports Standard SNMP Agent (MIB v1/2)
	Remote management using Console, Rlogin, Telnet
Additional services	Traffic Management feature
	Flexible backup using VRRP
	PAT(Port Address Translation)
	NAT(Network Address Translation)
	DHCP server and relay function
	CLI (Command Line Interface)
Other services	System monitoring and debugging function
	Back up for routing configuration data (FTP, TFTP)
	Remote upgrade of system software

AP900S Figure



(Figure1-2) SecureFinder AP900S Front



(Figure1-3) SecureFinder AP900S Rear

Chapter 2. Smart Manager Connection

Smart Manager Introduction

AddPac Smart Manager program is designed for easy control of SecureFinder AP900S. Even the first time users enable to easily access and configure AP900S via GUI (Graphic User Interface) without CLI(Command Line Interface).

Smart Manager Feature Highlights

- Java based Web Management
- Real time monitoring of Link status for each Port
- Assign IP address for managing
- User Account Management
- SNMP Agent setup
- Control two Fast Ethernet Port for WAN and four 10/100 Switch Hub Port for LAN application
- Control Crypto related function such as IPSec, IKE, CA
- Configuring Routing Protocol such as RIP, OSPF
- Standard/Extended/Name Access-List manage
- DHCP Pool writing function Using Wizard
- Maximum of 5 DNS Server/ DNS Host
- Telnet, SSH, FTP, HTTP Service control
- Detail View function for CPU, Memory capability.
- Real-time Performance Graph for each Ethernet Port
- Performance History Graph for each Ethernet Port
- Provide IPSec Performance Information Data

Hardware Requirement for Smart Manager

<Table 2-1> Hardware Requirements

CPU	Minimum Intel Pentium II 300Mhz or more
MEMORY	Minimum 128MB or more
Hard Disk	Minimum 10GB or more

<Table 2-2> Software Requirements

Operating System	MS Windows 2000 / XP / Server 2003
	Minimum Java 2 Runtime Environment SE v1.4.2
	Web browser : Microsoft Internet Explorer

Java 2 Runtime Environment v1.4.2 Download

To access to Smart Manager, Java Virtual Machine is required to execute Java applet on web browser. SUN distributes Java Virtual Machine with the name of J2RE (Java 2 Runtime Environment).

The J2RE version used in this guide is J2RE v1.4.2, the latest version. Visit at "http://java.sun.com/j2se/downloads.html" and download the program.
* J2SE is "Java 2 Platform Standard Edition," A type of the J2RE.

Step 1

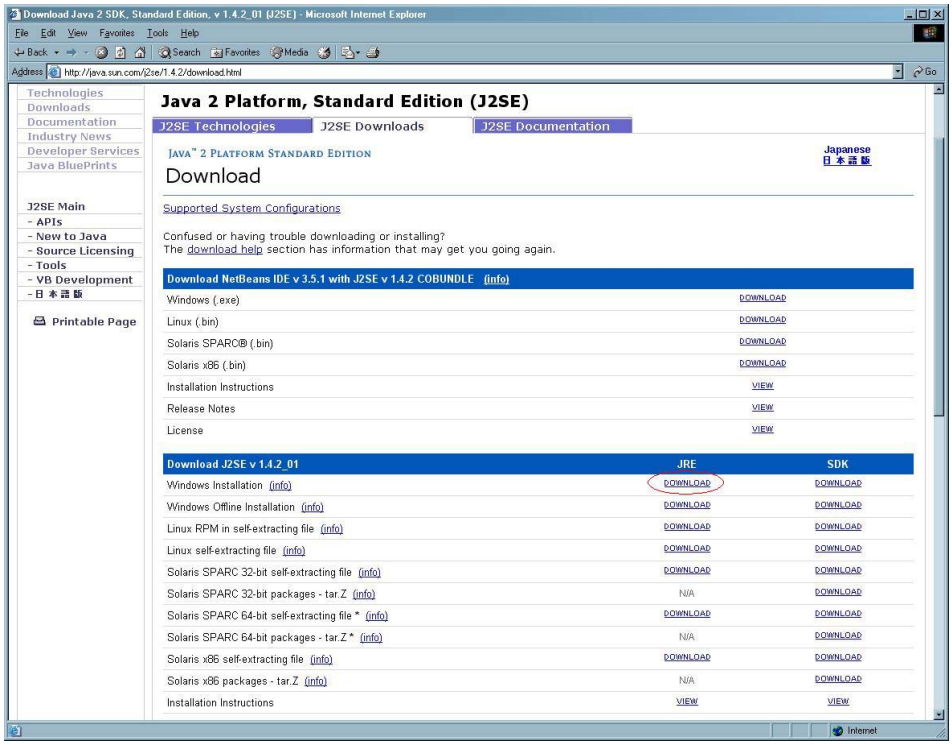
Select J2SE 1.4.2



(Figure2-1) Select Java 2 Platform Standard Edition

Step 2

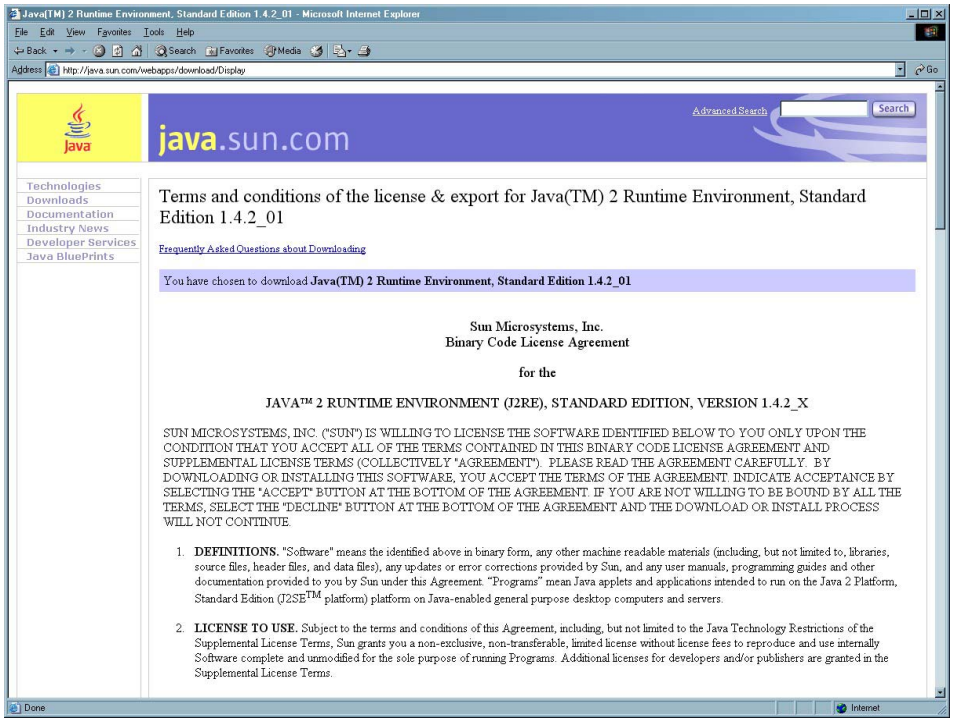
Select J2SE Windows.



(Figure2-2) Select J2SE Windows

Step 3

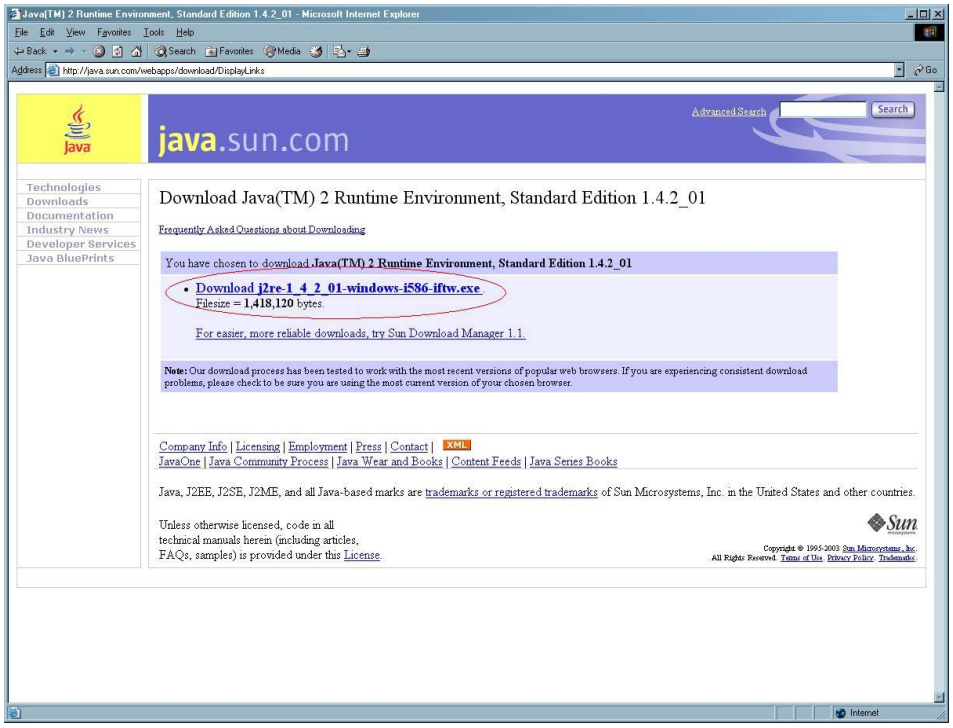
Carefully review "Terms and conditions of the license~" and select "agree."



(Figure2-3) License Agreement for J2SE

Step 4

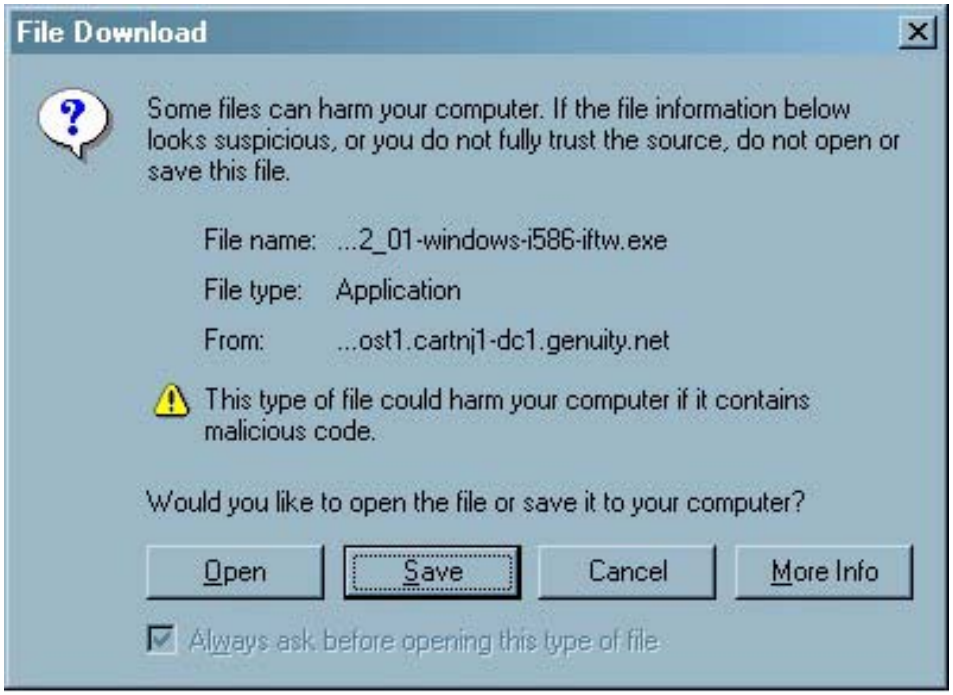
Download "Java 2 Runtime Environment, Standard Edition v1.4.2_01".



(Figure2-4) Java 2 Runtime Environment, SE v1.4.2_01 downlaod

Step 5

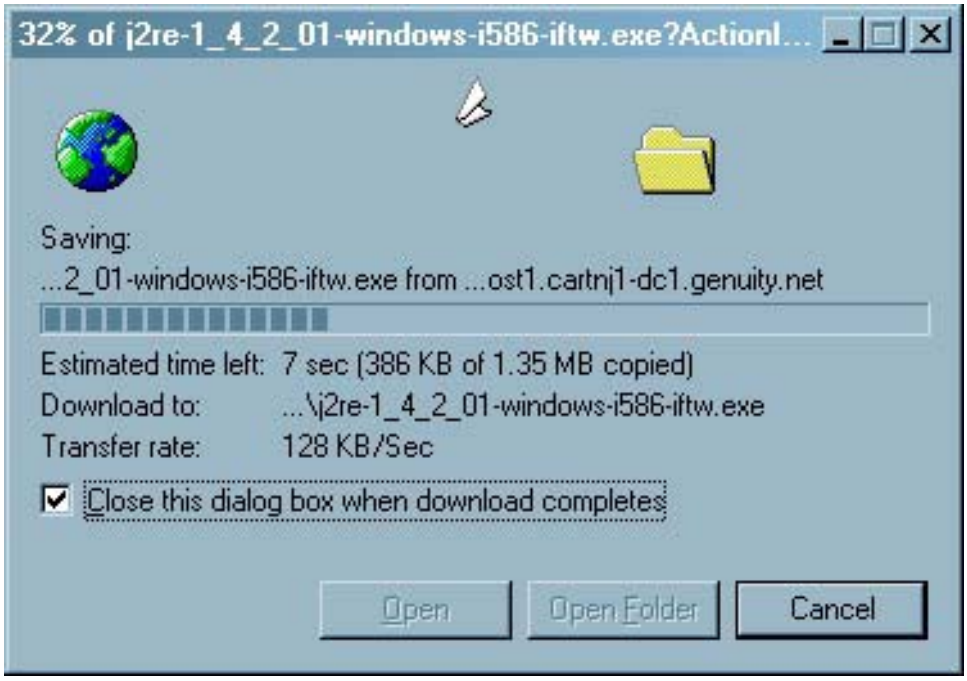
"File Download" dialog box appears. Click "Save" to save the program at the PC.



(Figure2-5) File Download Dialog Box

Step 6

Then the program is downloaded.



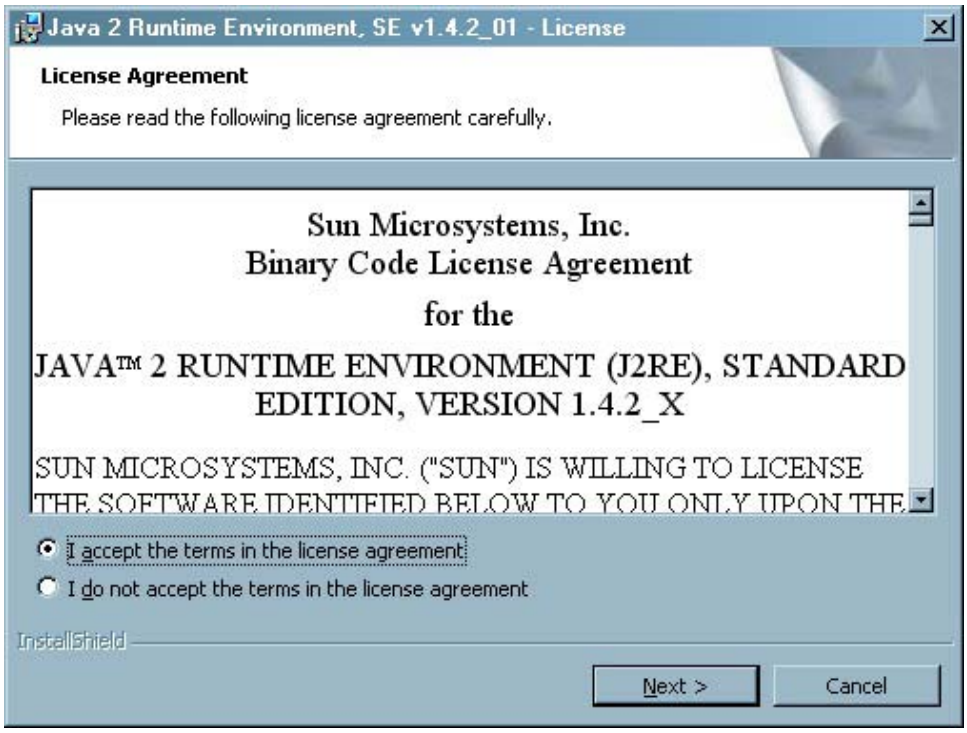
(Figure2-6) Downloading the file

Java 2 Runtime Environment v1.4.2 Installation

This part explains how to install "J2RE v 1.4.2" on the PC

Step 1

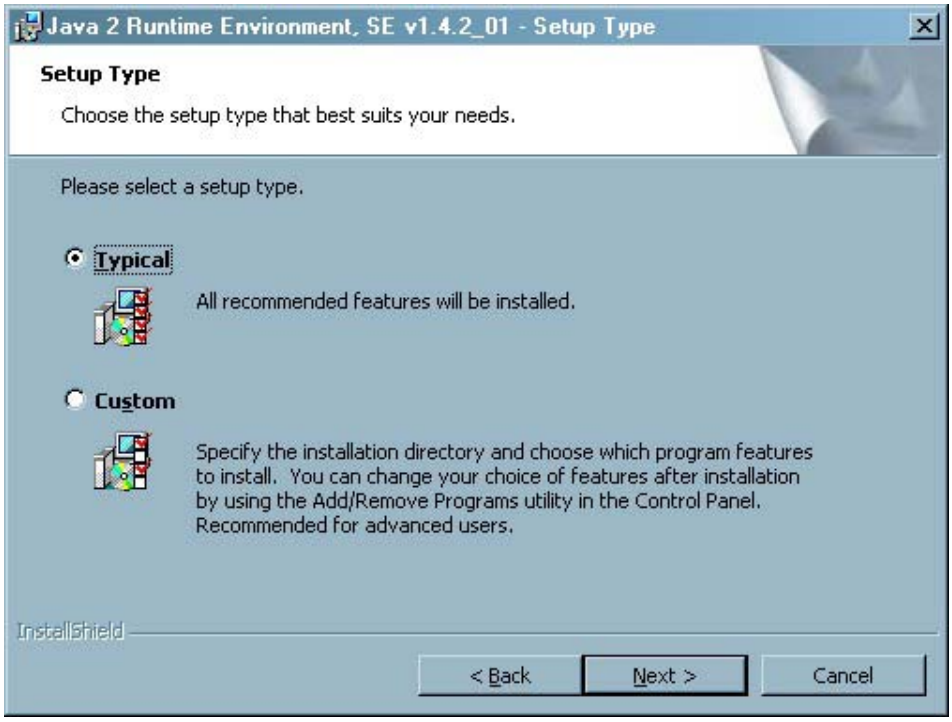
Execute "j2re-1_4_2_01-windows-i586-iftw.exe"file. Then the License Agreement appears. Review it carefully and select "I accept~." Then click "Next>" button to proceed.



(Figure2-7) Java 2 Runtime Environment – License

Step 2

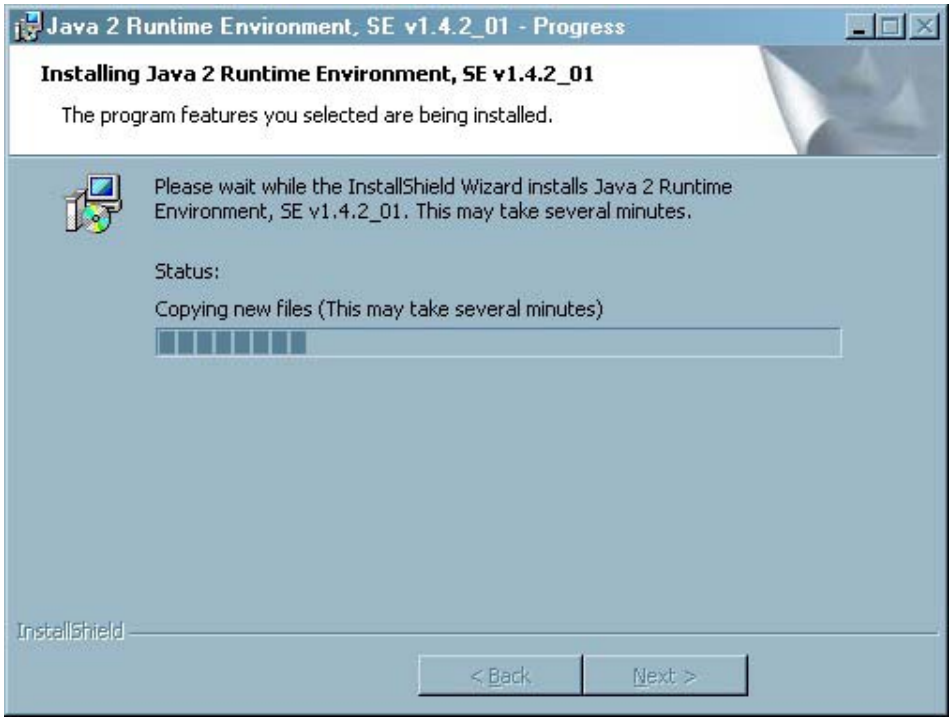
Select "Setup Type" as "Typical" and click "Next>" button.



(Figure2-8) Select Java 2 Setup Type

Step 3

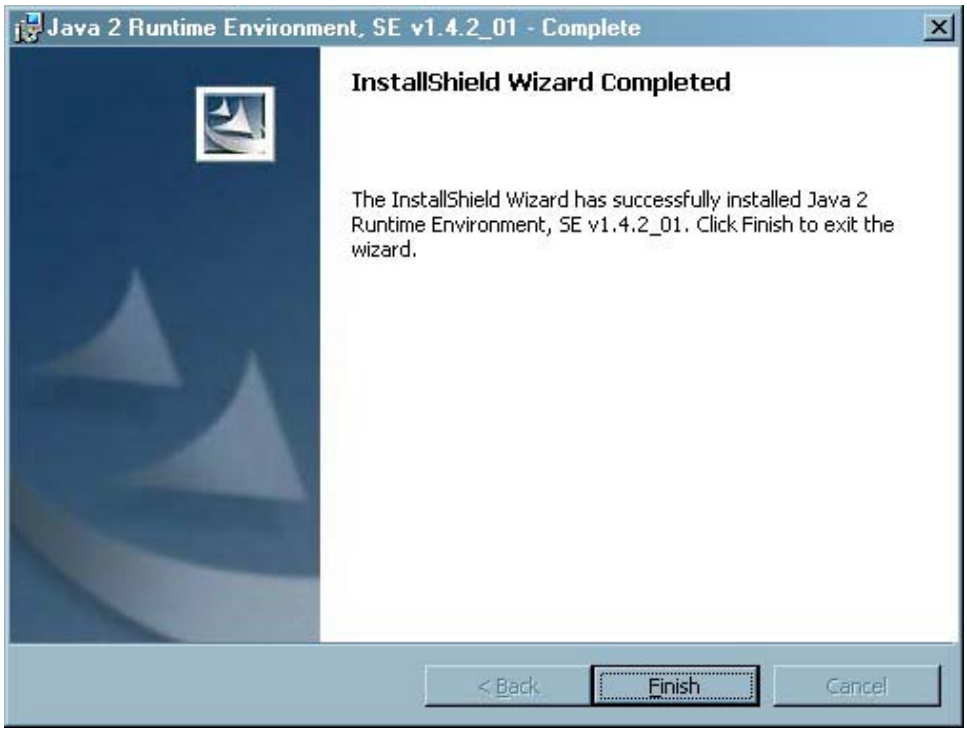
J2SE installation is on processing.



(Figure2-9) Java 2 installation processing

Step 4

J2SE installation is completed. Click "Finish".

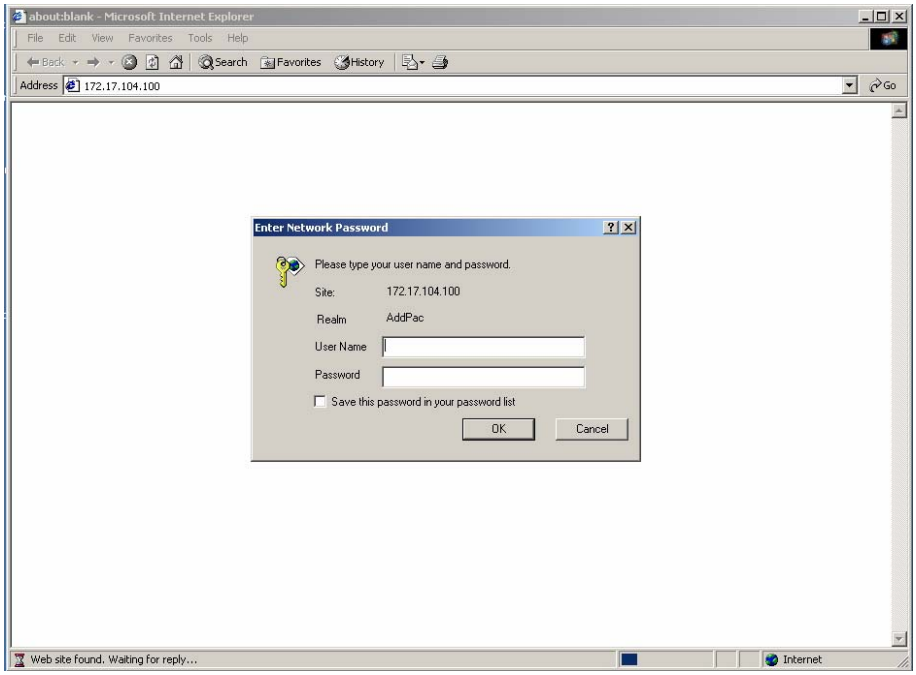


(Figure2-10) Java 2 Runtime installation completion

Smart Manager Access

Step 1

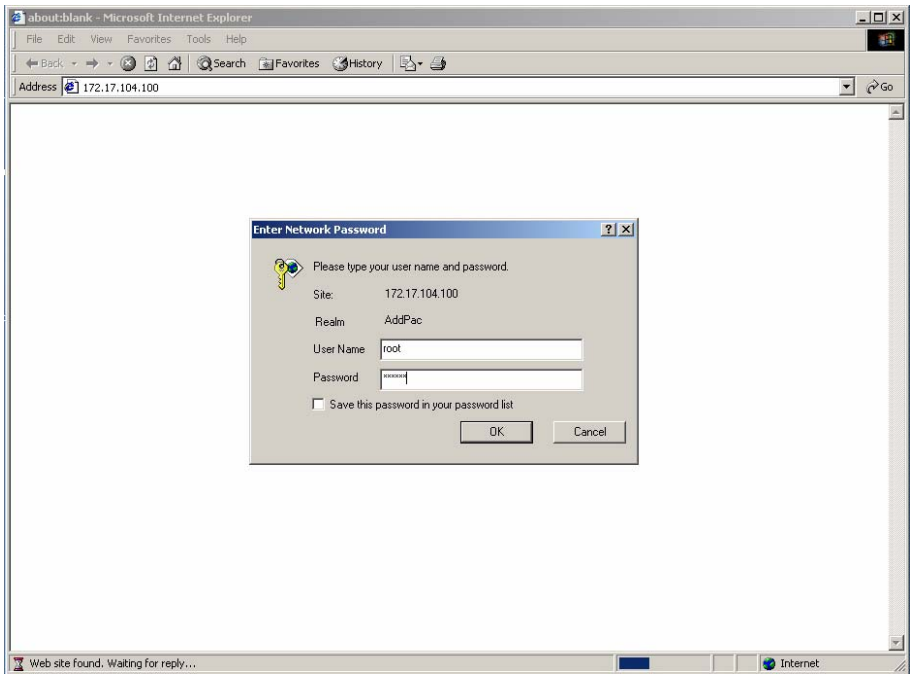
Enter IP address of AP900S at the address bar of the web browser.



(Figure2-11) Web Management System access

Step 2

Enter User Name ("root") and Password ("router"). Click "OK" button. The User Name and Password are changeable by users.



(Figure2-12) Web Management System Login

Step 3

Smart Management System window will be shown after login.

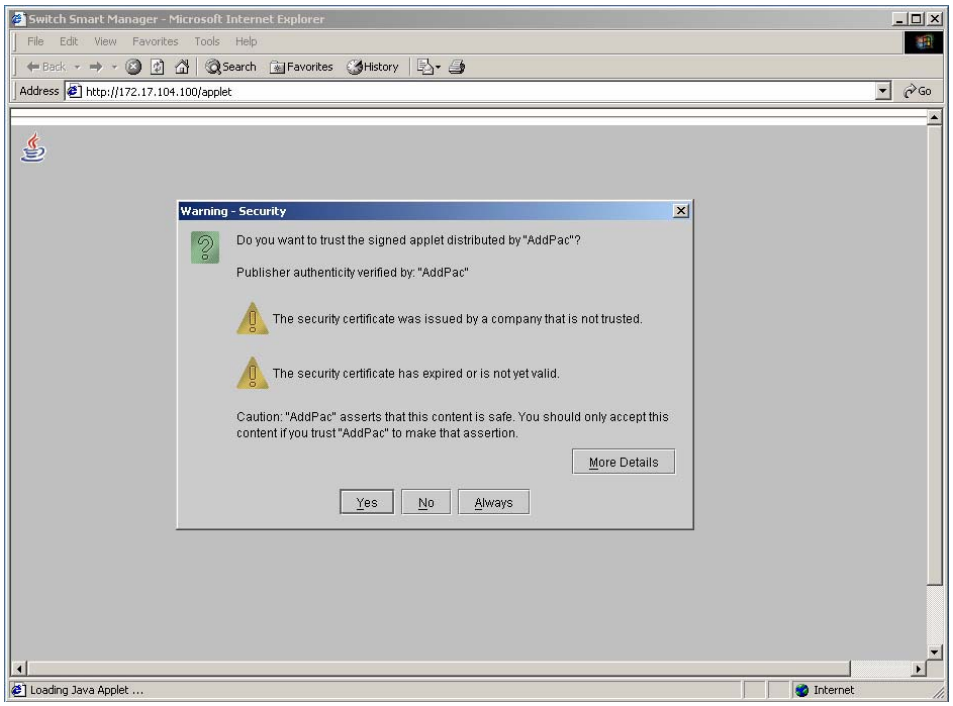
Select Smart Manager.



(Figure2-13) Initial window of Web Management System

Step 4

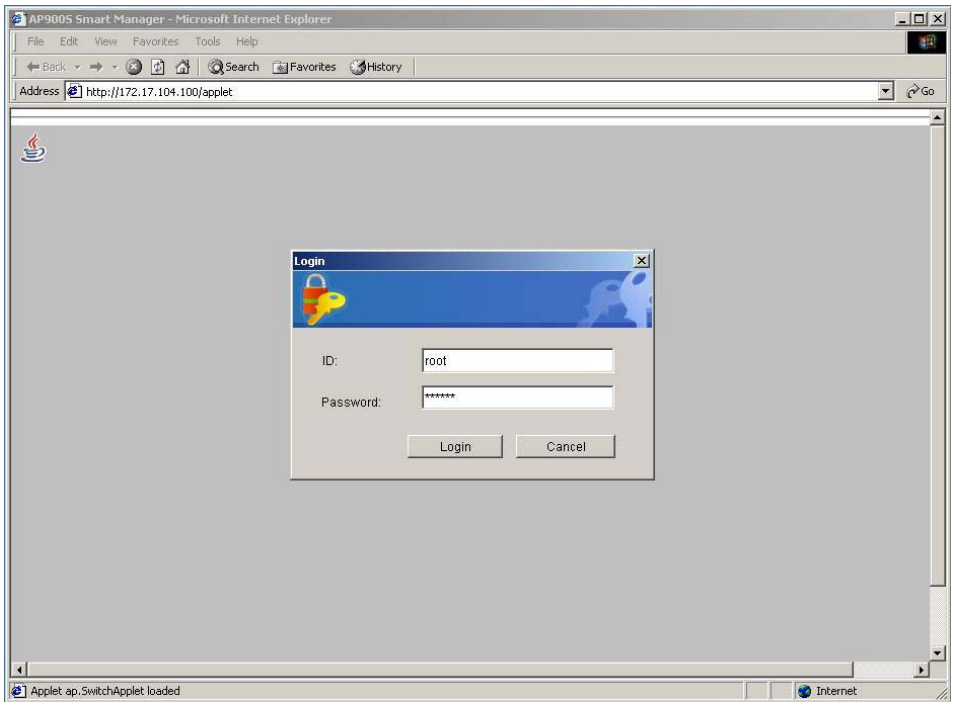
Java Applet is executed. Select "Yes" or "Always" for security.



(Figure2-14) Java Applet security warning page

Step 5

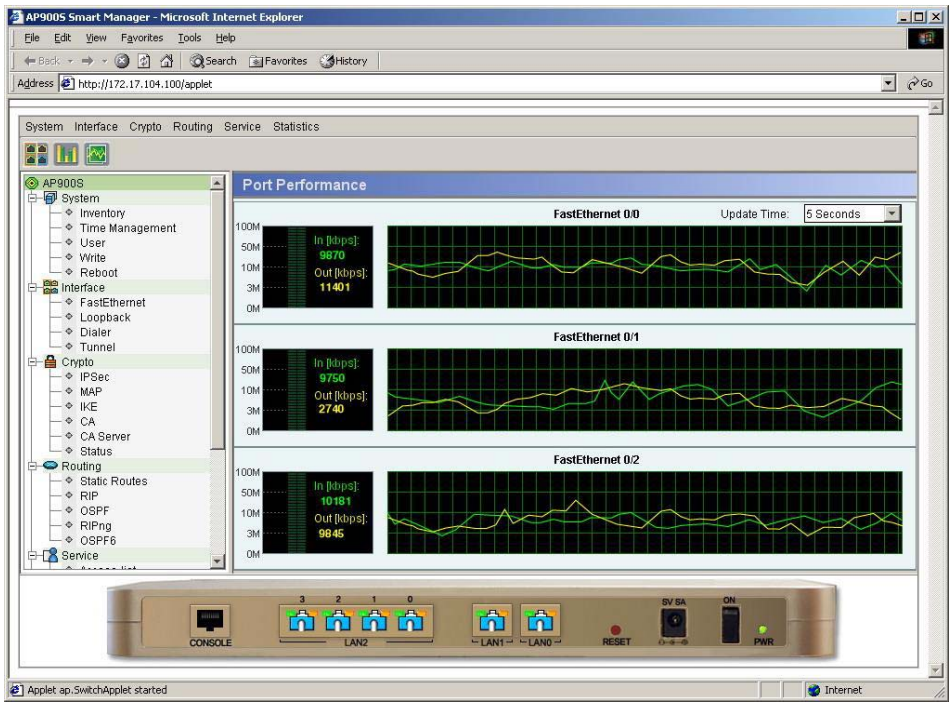
Login prompt for Smart Manager appears. Enter the same User ID and Password used for the web management system login.



(Figure2-15) Java Applet Login

Step 6

It moves to the main page for Smart Manager.

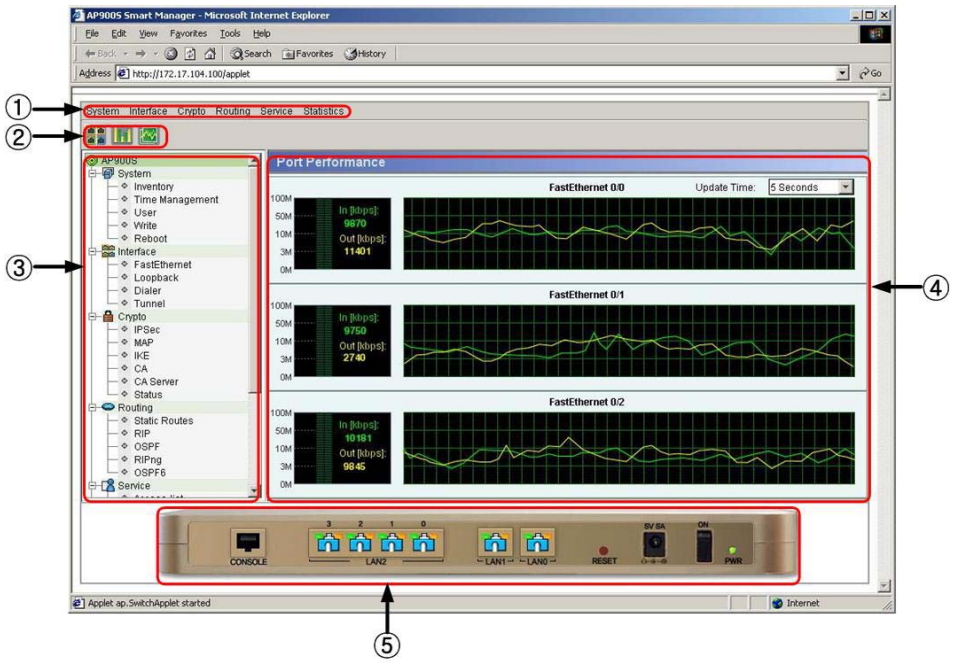


(Figure2-16) Smart Manager main page window

Chapter 3. Smart Manager Menus

Smart Manager Screen Elements

Smart Manager consists of 5 sections.



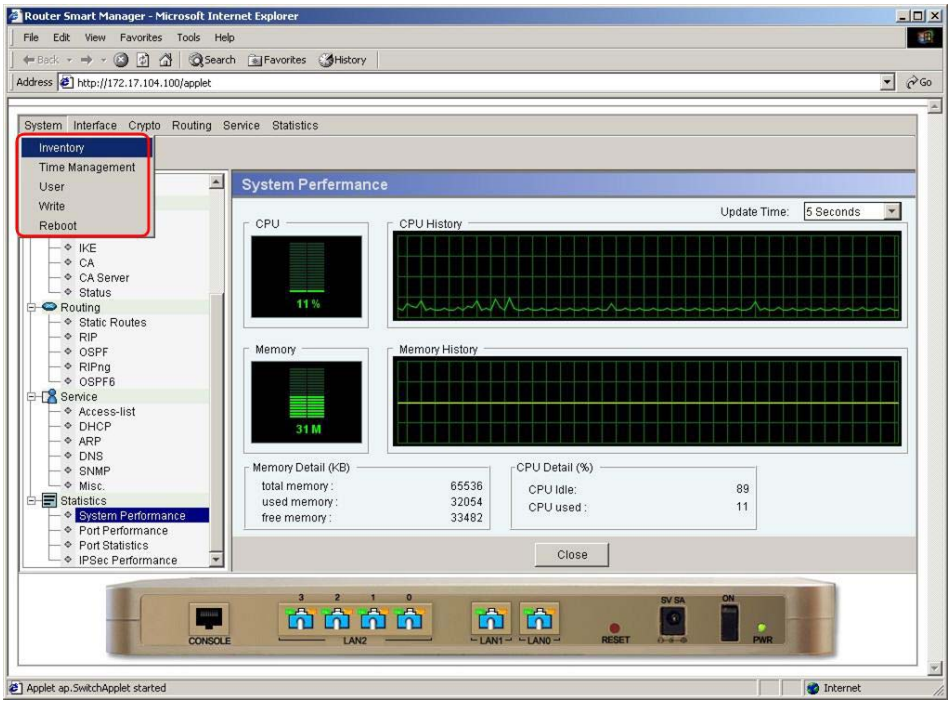
(Figure3-1) Smart Manager Elements Page

<Table 3-1> Smart Manager Main Page Elements and Descriptions

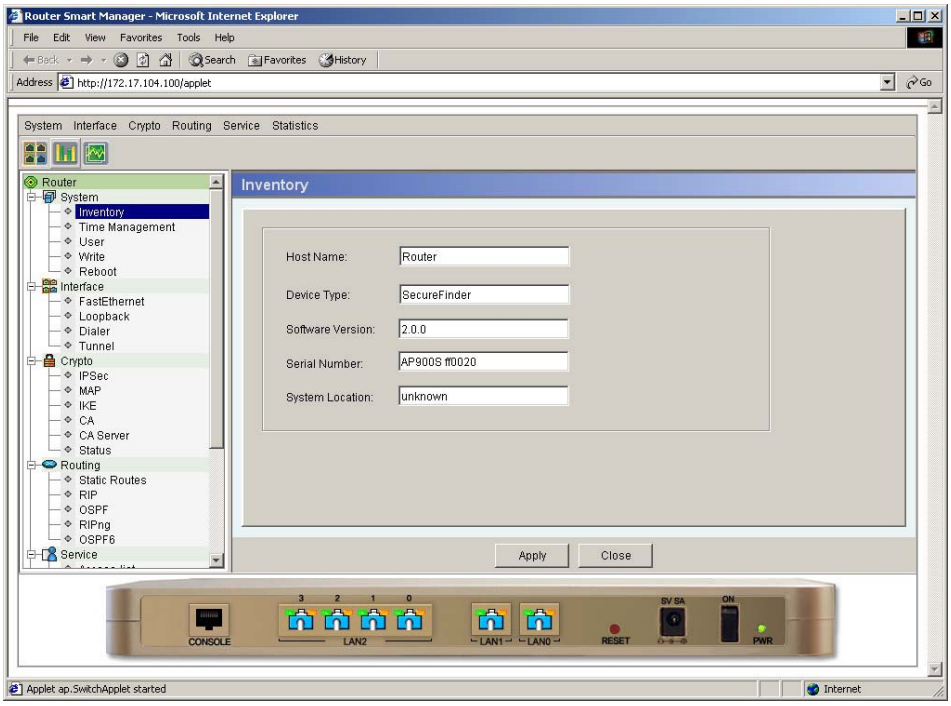
Sections	Description
①	Pull-down menu to access sub-menus of the Smart Manager. The menus are same as the tree type menu at ③.
②	Shortcut Icons for Port Performance, Port Configuration, management and Parametric Information.
③	Tree type menu for sub-menus of the Smart Manager
④	This shows the output window of ①~③
⑤	Real-time monitoring port link status of AP900S. With the mouse right-click, “Port Configuration”, “Port Status” can be selected.

How to Use Pull-down Menu

Click the desired menu from the menu bar, and then relevant sub-menus are displayed. Select the right category, and then further information is displayed on the main display area. Figure 3-2 shows the example of selecting Inventory under system menu.

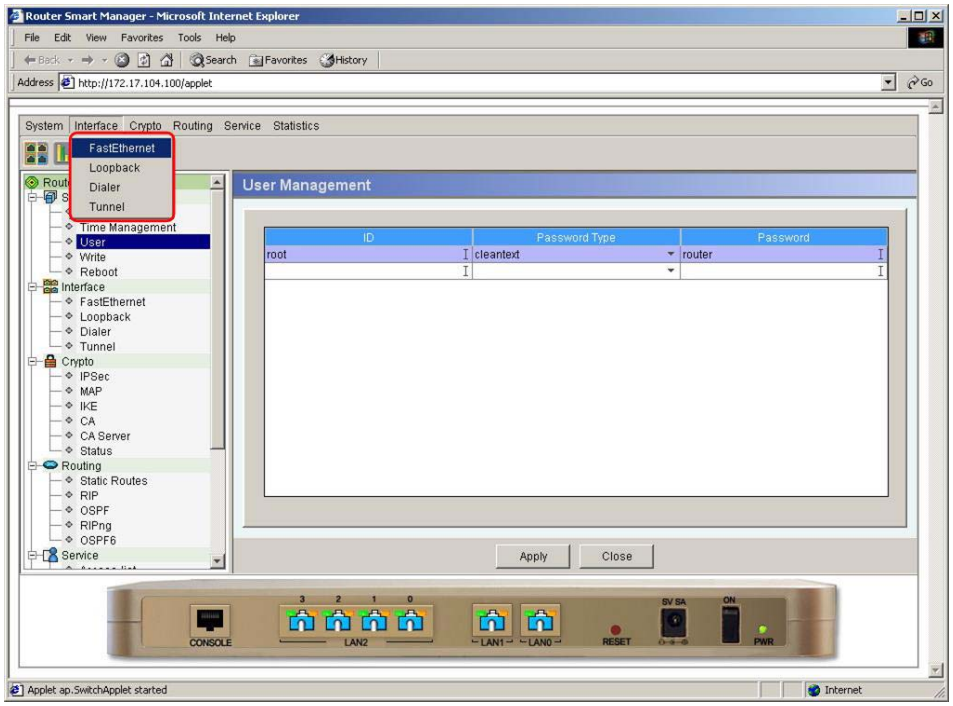


(Figure3-2) Pull Down Menu – system



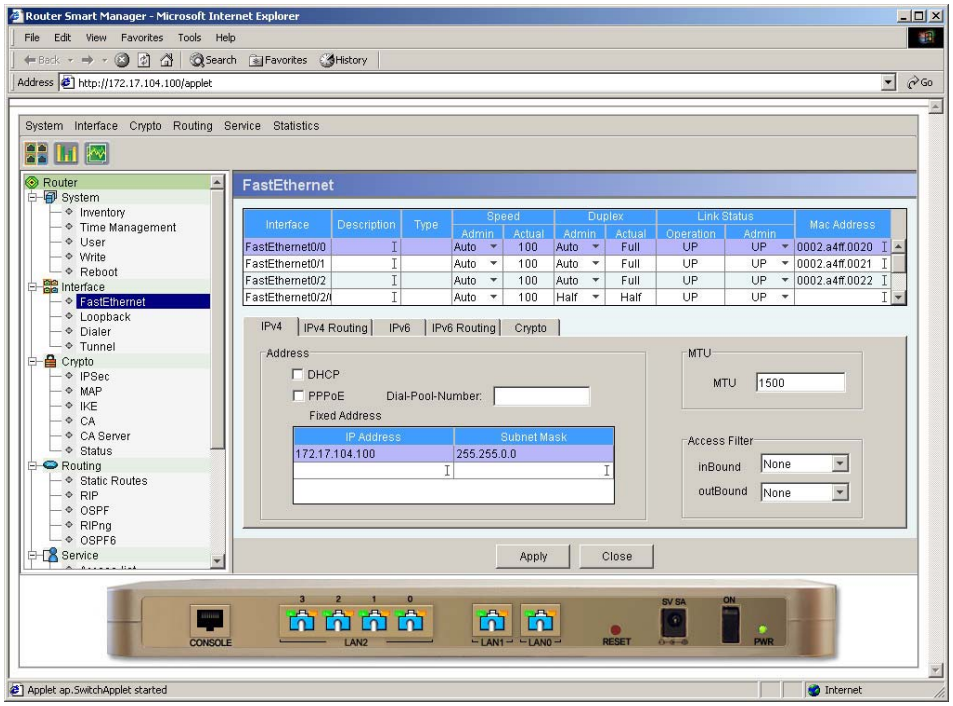
(Figure3-3) Pull Down Menu – system -> Inventory

At Figure 3-4, "FastEthernet" is selected from the pull-down menu.



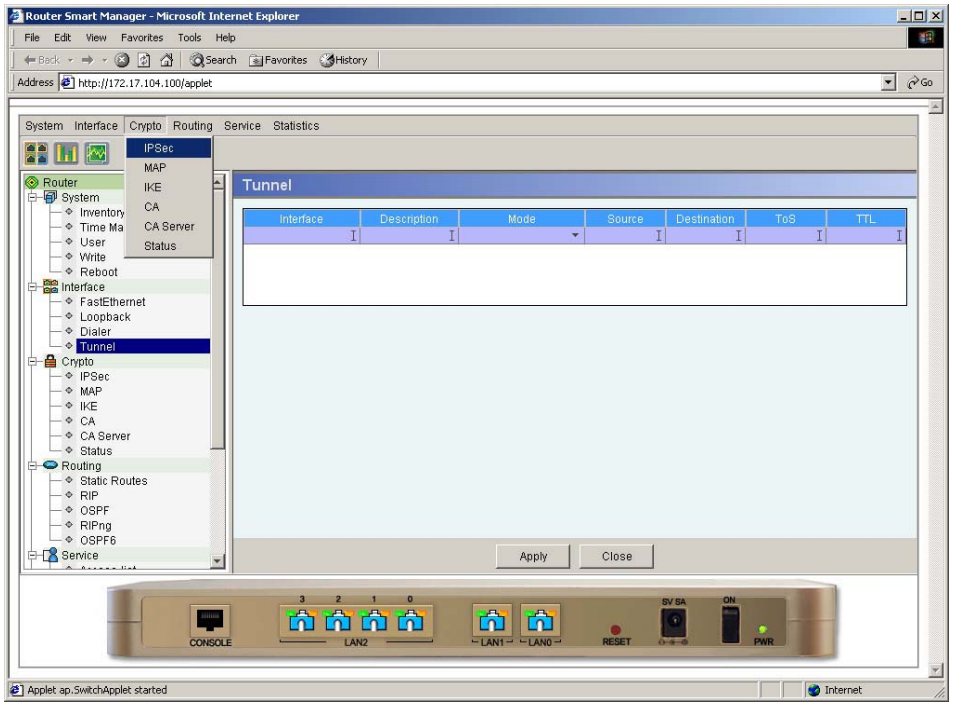
(Figure3-4) Pull Down menu –> FastEthernet

Figure 3-5 shows FastEthernet Page.



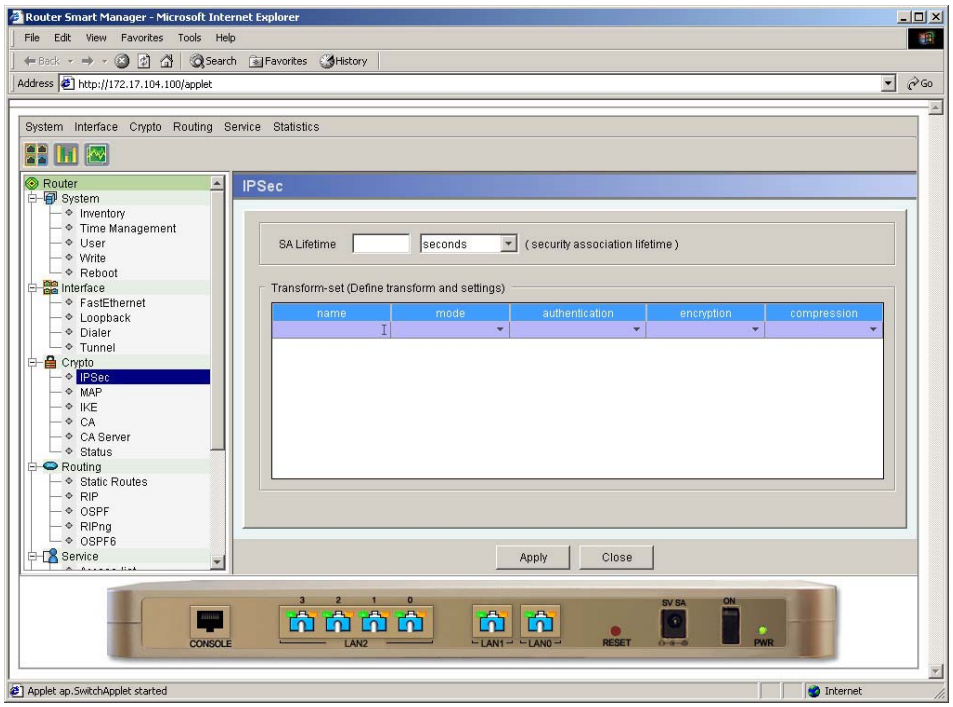
(Figure3-5) Pull Down menu – FastEthernet page

At Figure 3-6, "IPSec" is selected from pull-down menu.



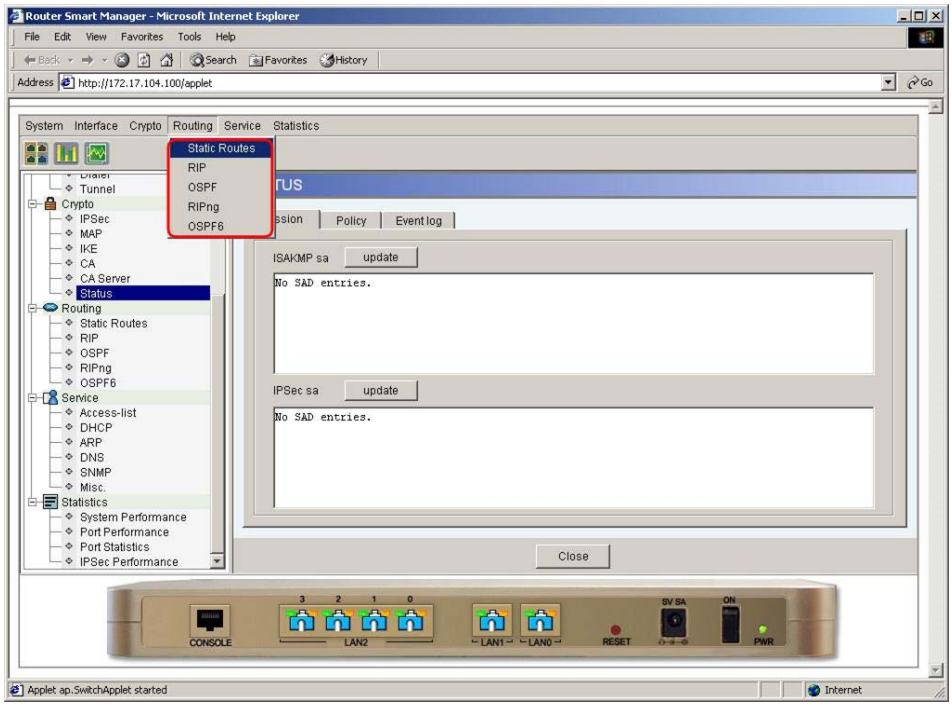
(Figure3-6) Pulll Down menu –> Crypto -> IPSec

Figure 3-7 shows IPSec Config page.

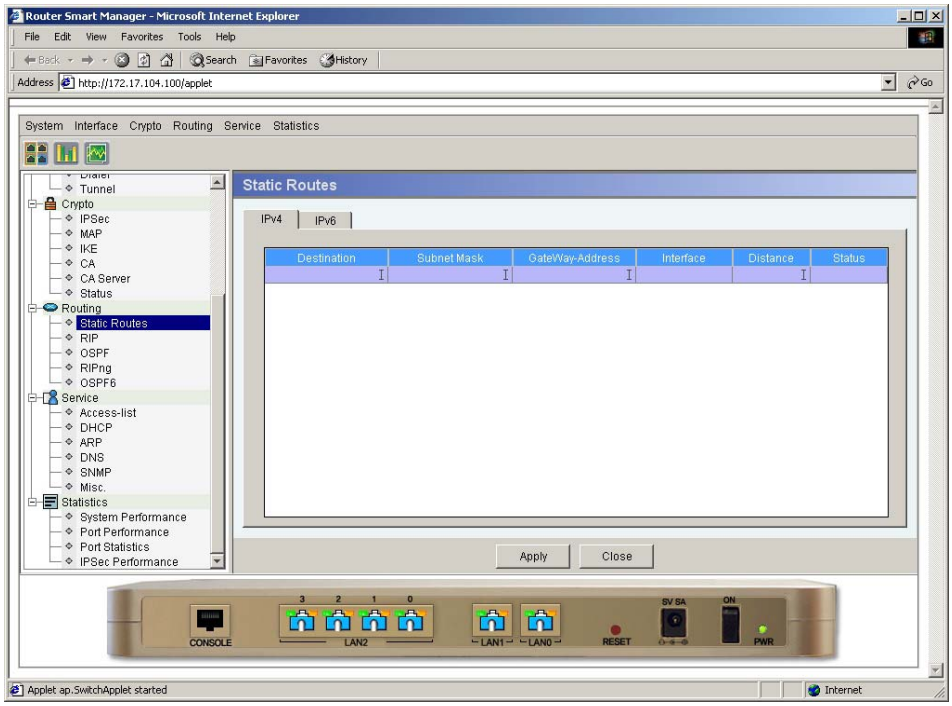


(Figure3-7) Pull Down menu – IPSec Config page

At Figure 3-8, "Static Routes" is selected from "Routing" of pull-down menu.

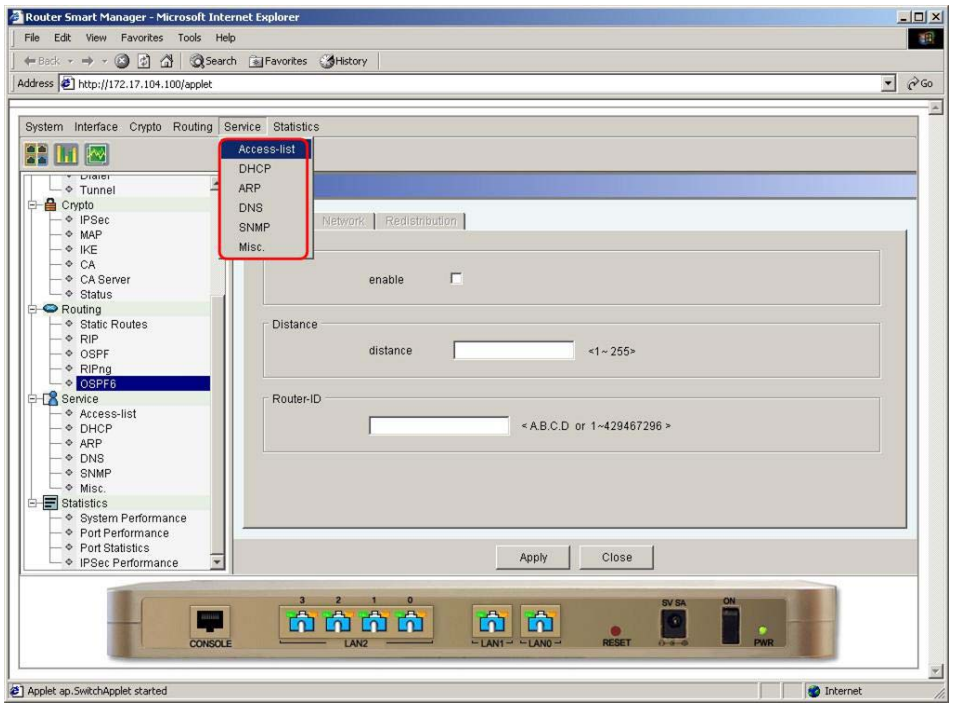


(Figure3-8) Pull Down Menu –>Routing-> Static Routes

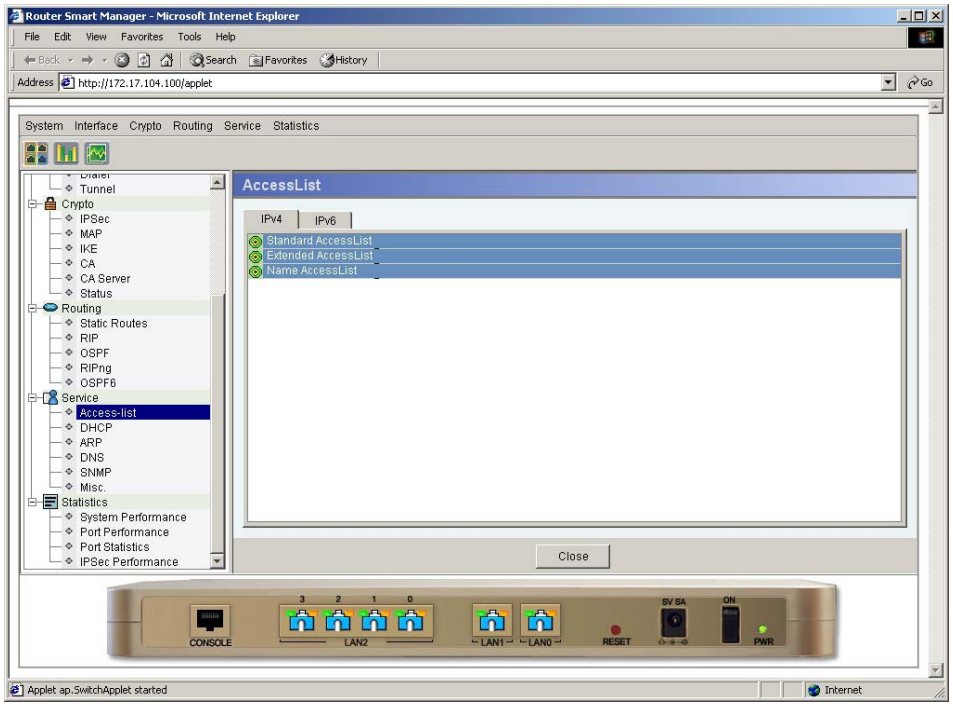


(Figure3-9) Pull Down Menu– Static Routes page

At the below Figure 3-10, "Access-list" is selected from "Service" of pull-down menu.

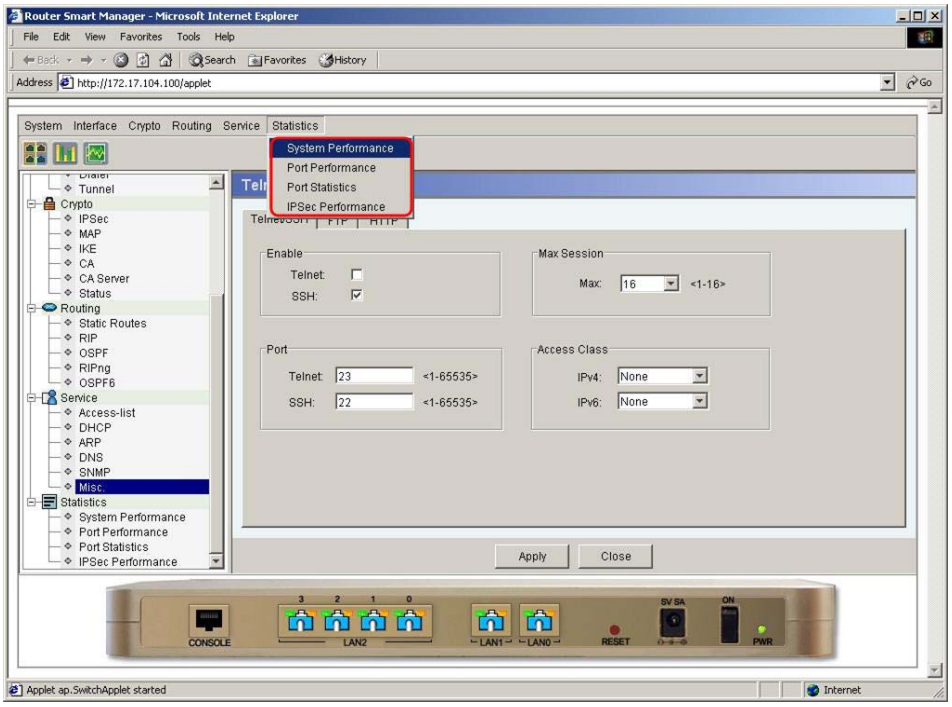


(Figure3-10) Pull Down Menu –>Service-> Access-list

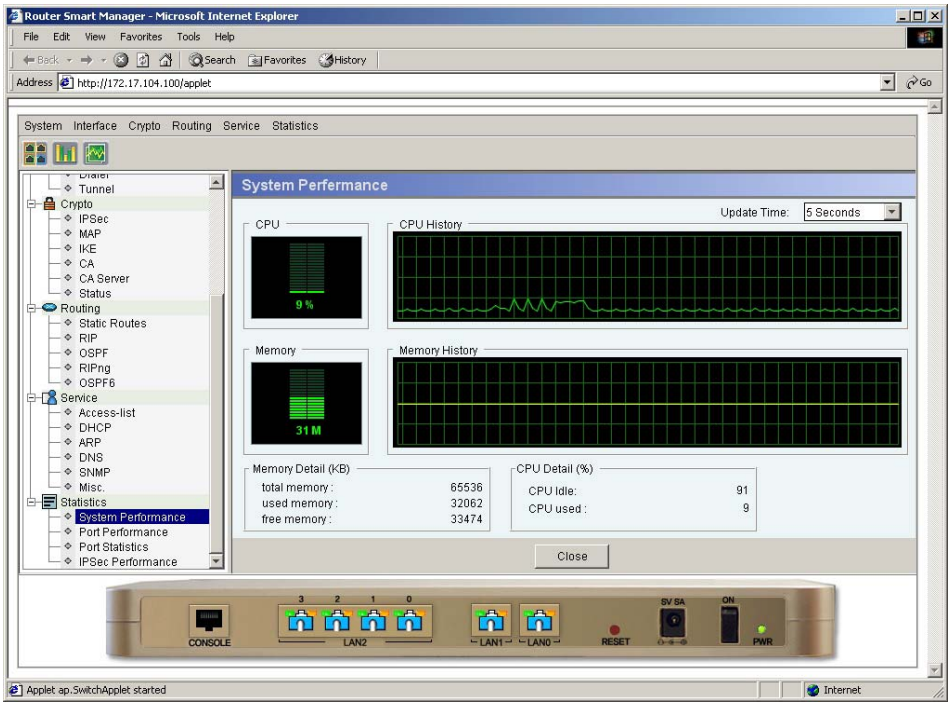


(Figure3-11) Pull Down Menu – Access-list page

At the below Figure 3-12, "System Performance" is selected from "Statistics" of pull-down menu.



(Figure3-12) Pull Down menu –>Statistics-> System Performance



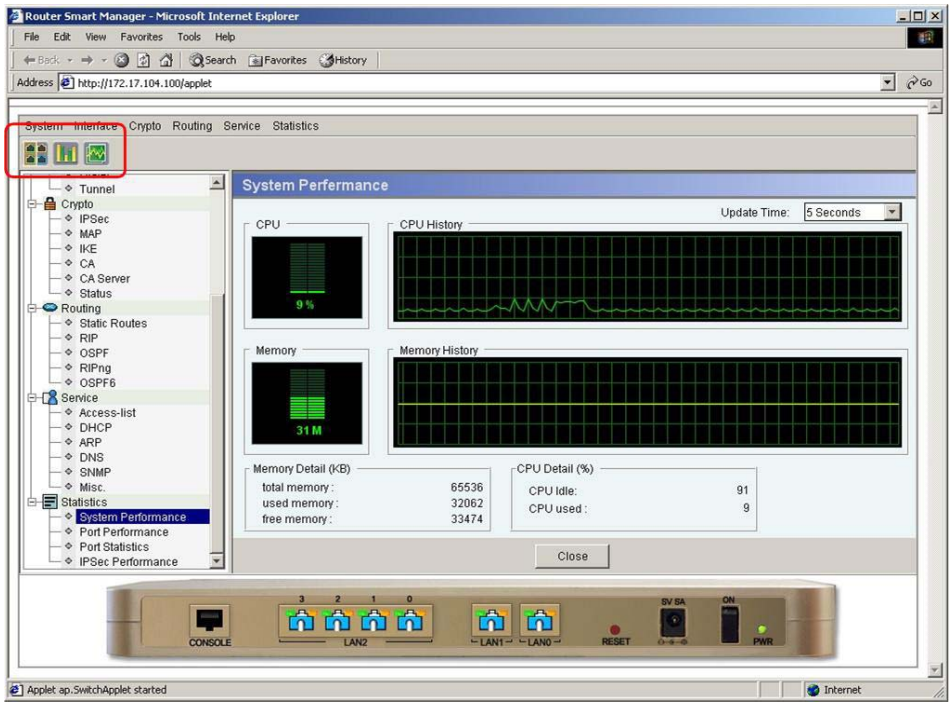
(Figure3-13) Pull Down Menu – System Performance page

<Table 3-2> Pull Down menu elements

Menu	Elements
System	Inventory
	Time Management
	User
	Write
	Reboot
Interface	FastEthernet
	Loopback
	Dialer
	Tunnel
Crypto	IPSec
	MAP
	IKE
	CA
	CA Server
	Status
Routing	Static Routes
	RIP
	OSPF
	RIPng
	OSPF6
Service	Access-List
	DHCP
	ARP
	DNS
	SNMP
	Misc.
Statistics	System Performance
	Port Performance
	Port Statistics
	IPSec Performance

How to Use Shortcut Icons

Frequently used configuration menus such as FastEthernet, Port Performance, Port Statistics are listed as shortcut icons under the pull-down menu bar.

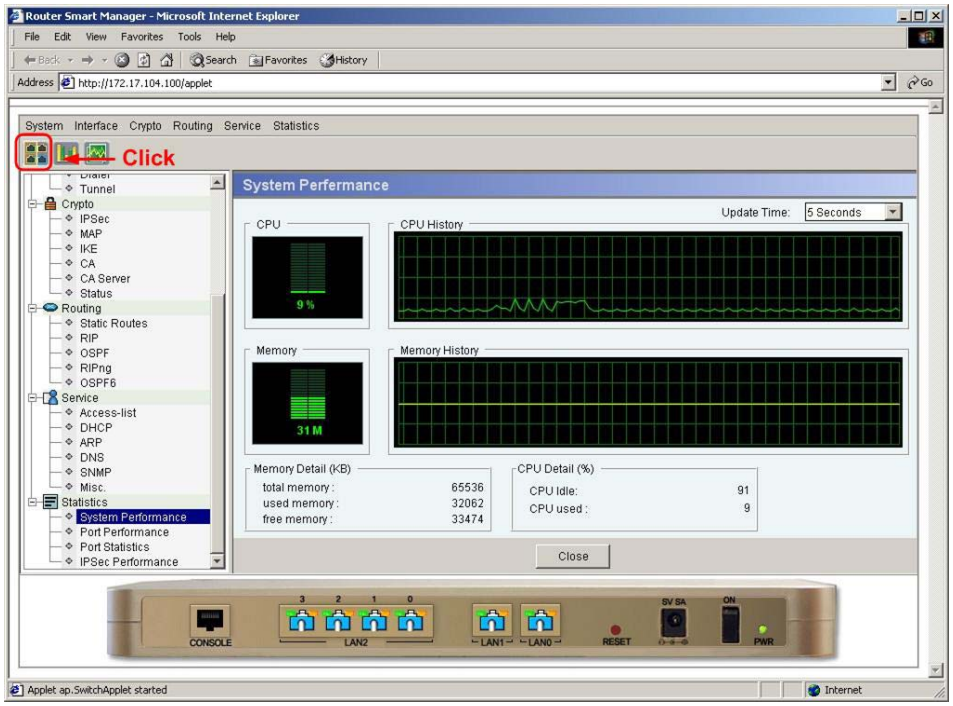


(Figure3-14) Shortcut Icons

<Table 3-3> Shortcut Icons & Description

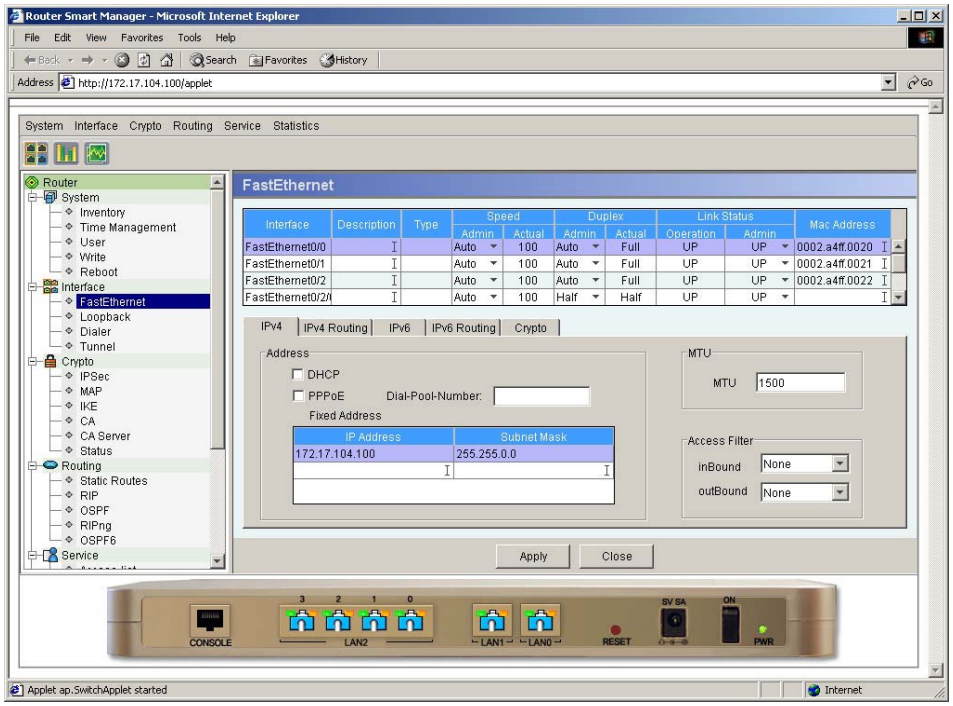
Icons	Description
	Move to FastEthernet menu
	Move to Port Performance menu
	Move to Port Statistics menu

Click  icon to go to FastEthernet page.



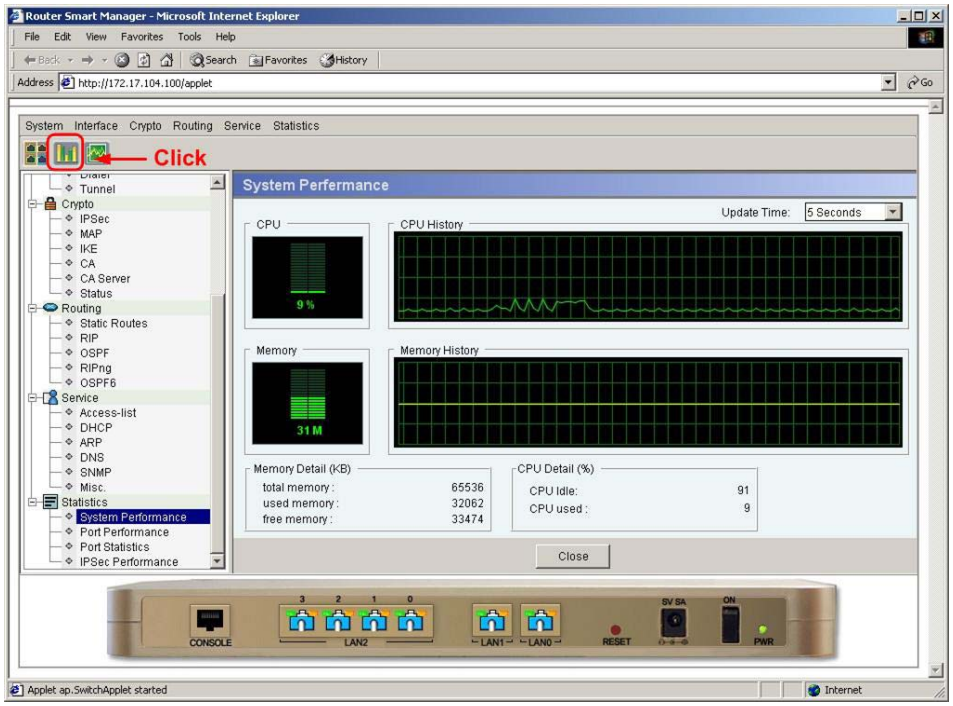
(Figure3-14) FastEthernet icon

Move to FastEthernet page



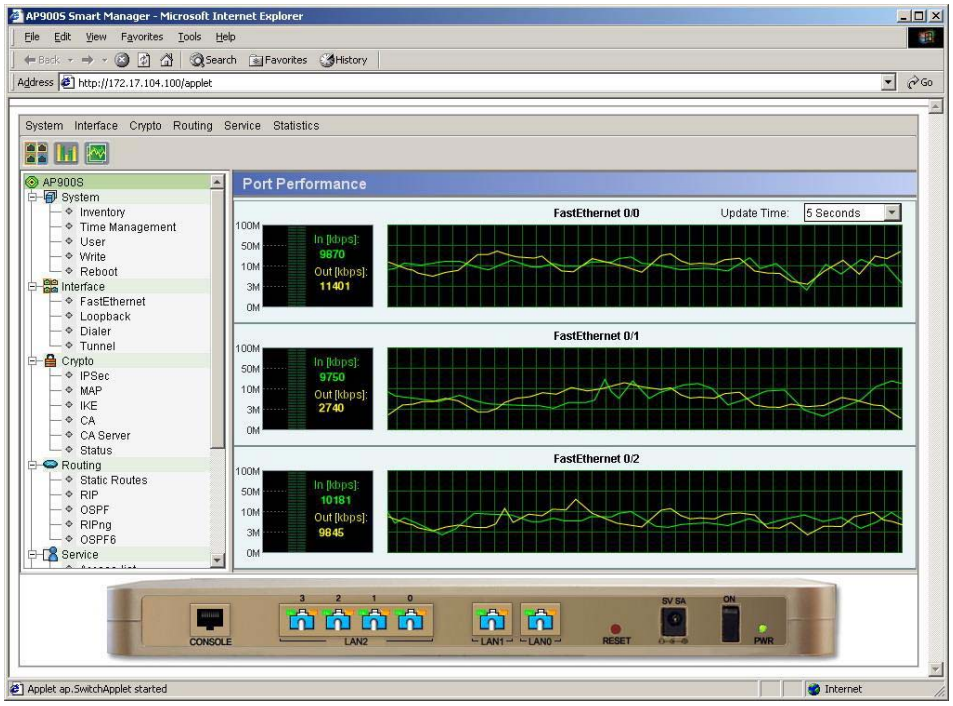
(Figure3-15) FastEthernet page

At Figure 3-17, Click  icon to go to Port Performance directly.



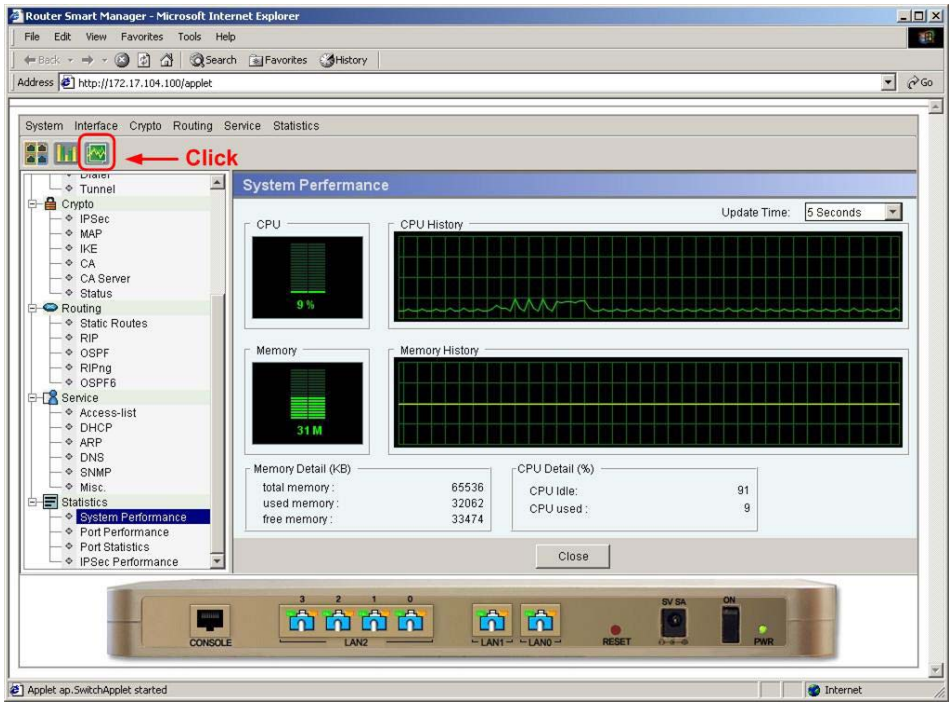
(Figure3-16) Port Performance Icon

Move to Port Performance.



(Figure3-17) Port Performance History Shortcut Icon

At Figure 3-19, Click  Icon to go to Port Statistics.



(Figure3-18) Port Statistics Icon

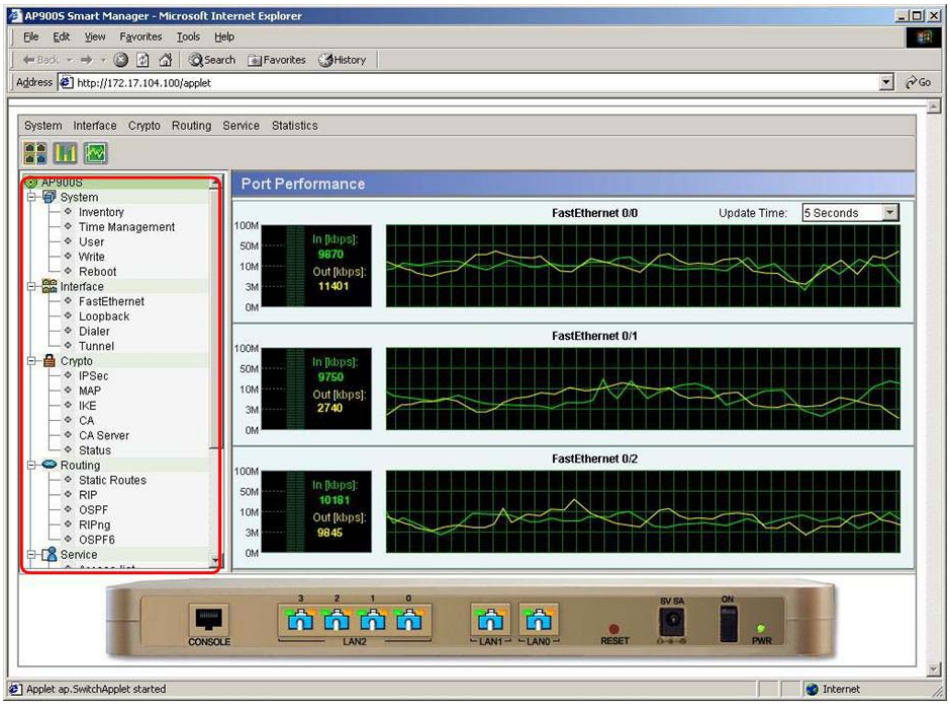
Move to Port Statistics page



(Figure3-19) Port Statistics page

How to Use Tree Menu

The users enable to control and access overall features of SecureFinder AP900S using the tree menu. This tree menu is divided by 6 parts and the detailed description is listed at the Table 3-4.



(Figure3-20) Tree menu of AP900S

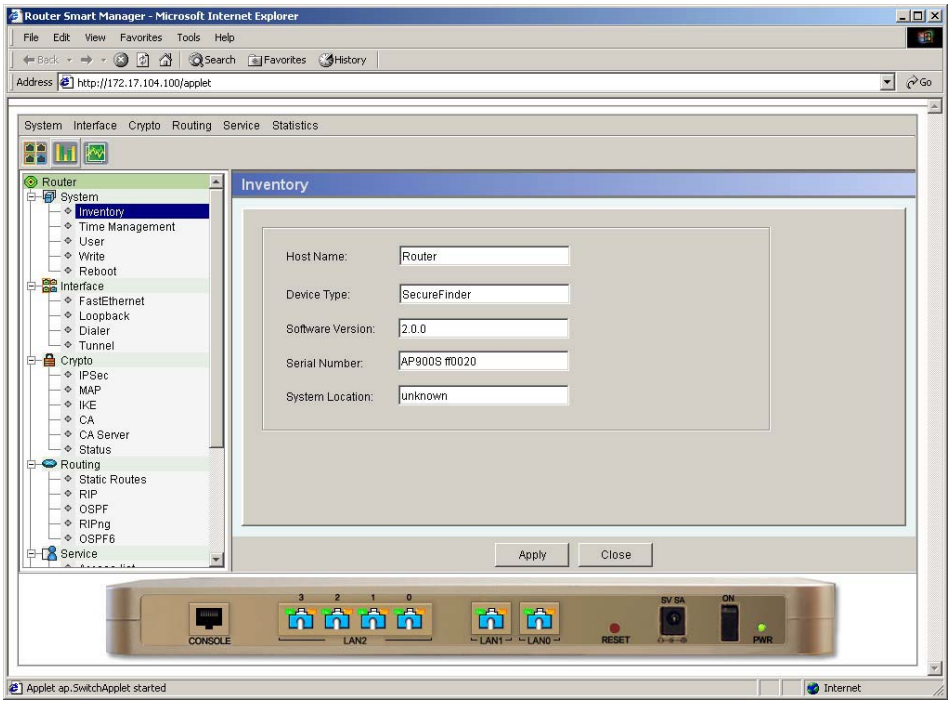
<Table 3-4> Tree Menu & Description

Menu	Description
System	Basic configuration parameters of AP900S. Time setup, User ID, Configuration Write and Reboot menus are included.
Interface	It controls Ethernet Interface functions of AP900S. It includes Dialer and IPv6 Tunnel configuration for PPP Session.
Crypto	It includes controlling VPN related function such as IPSec, Crypto Map, IKE, CA, CA Server etc.
Routing	It includes Routing Protocol related elements such as Static, RIP, OSPF etc.
Service	It includes Access-List, DHCP Pool, ARP, DNS, SNMP, Telnet, FTP etc.
Statistics	This menu shows the statistics and monitoring data such as System Performance, Port Performance, IPSec Performance etc.

System Menu

Inventory

"Inventory" offers the brief information of AP900S.



(Figure3-21) System-Inventory

<Table 3-5> Inventory Fields

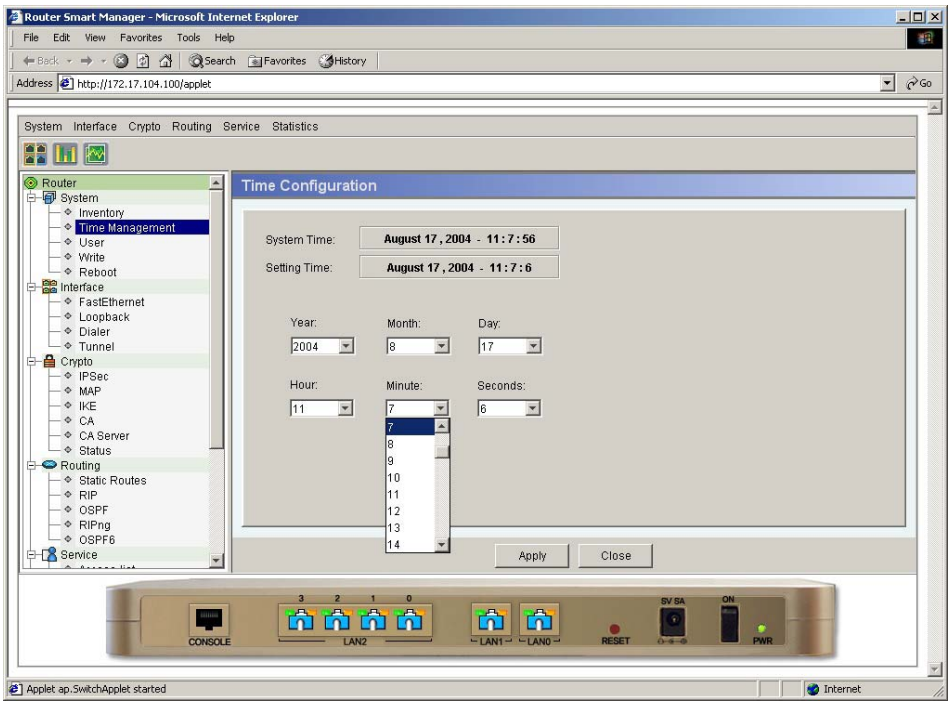
Field	Description
Host Name	The Host Name of AP900S. The user enables to change it from the SNMP Management Page.
Device Type	The Device Type of AP900S. It is set to "SecureFinder" as default.
Software Version	APOS Version of AP900S
Serial Number	MAC Address of AP900S
System Location	The System Location information from SNMP Management page.

Time Management

Time Management changes the system time of SecureFinder AP900S.

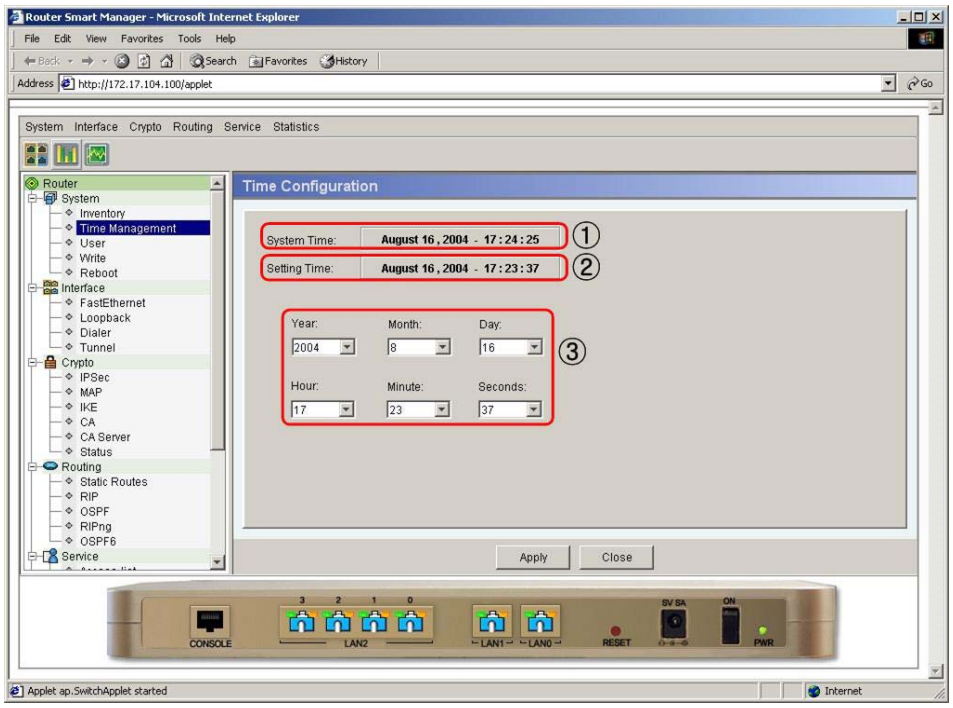
With each pull-down menu, users enable to change year, month, day, and hour. Click "Apply" button to save the changed values.

Figure 3-23 shows the example of changing Minutes using the pull down menu.



(Figure3-22) Time Management window

The Time Management elements are described below.



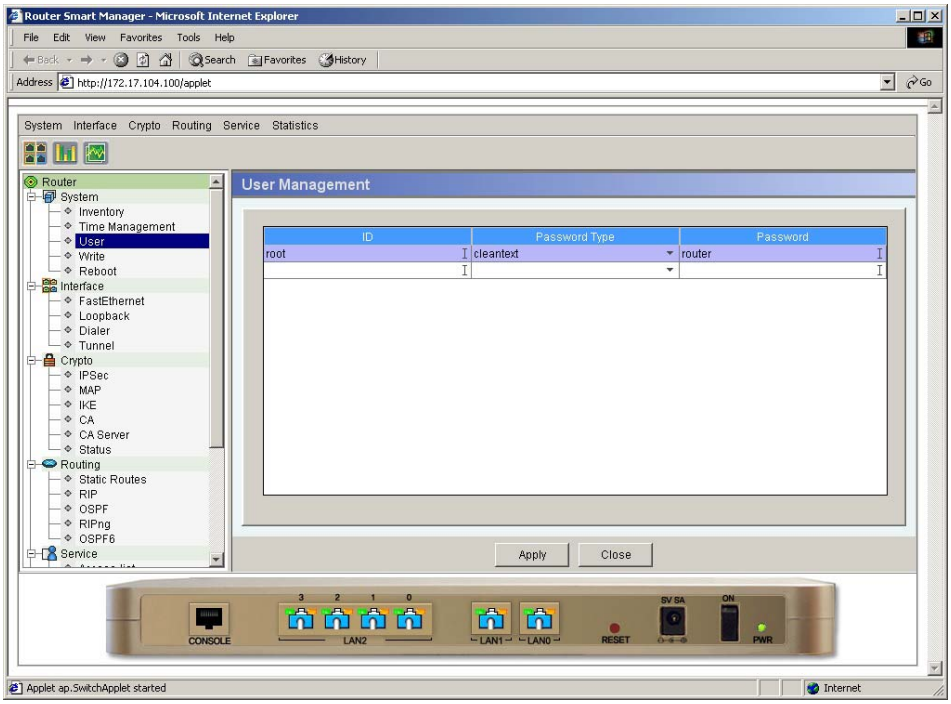
(Figure3-23) Time Management Elements

<Table 3-6> Time Management Elements and Description

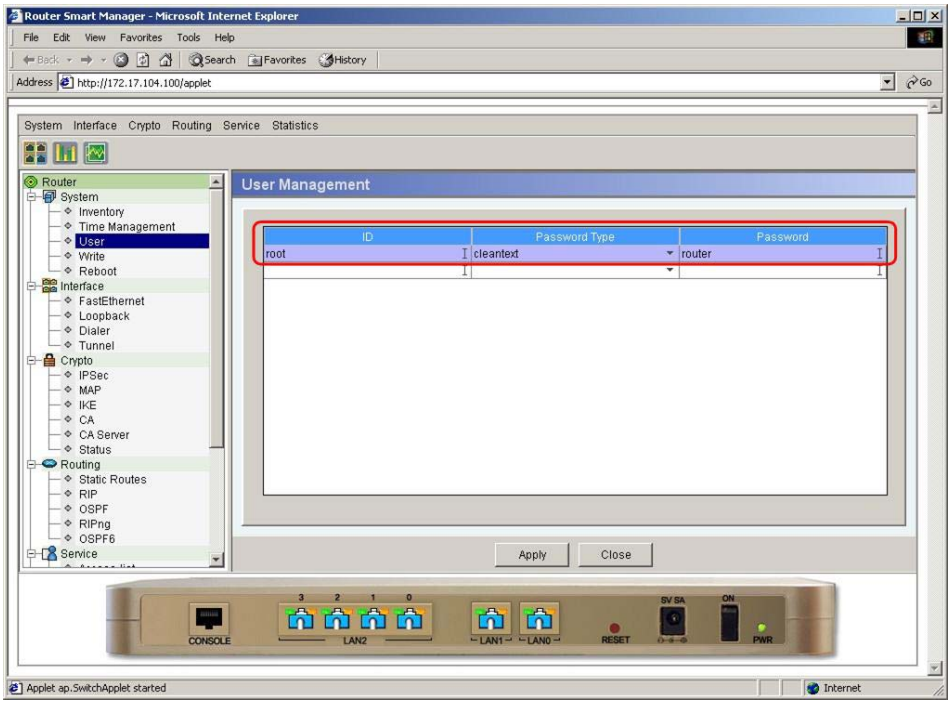
Element	Description
① System Time	The current system time of AP900S.
② Setting Time	When a user sets the time in ③bars, it will show the time in this field. The system time is set by user. The default time is synchronized with the time of PC.
③ Year, Month, Day, Hour, Minute, Seconds	Set the year, month, day, hour, minute and seconds with the pull-down menu.

User Management

It configures User Management elements of AP900S. Use this User Management menu when you want to add other user IDs besides “root”.



(Figure3-24) User Management main window

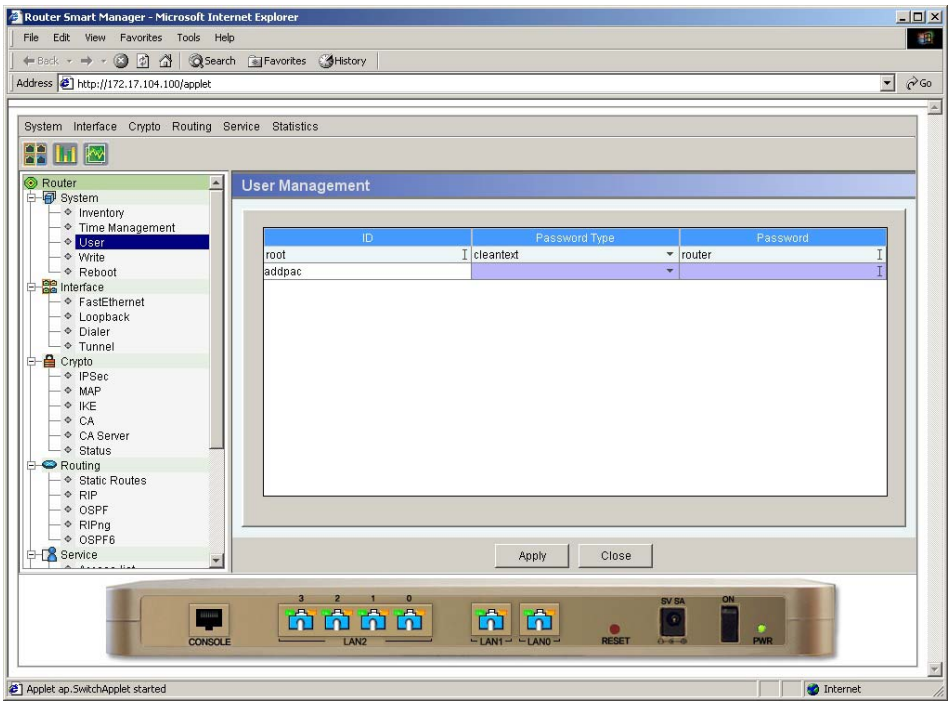


(Figure3-25) Configuring User Management elements

<Table 3-7> User Management elements & Description

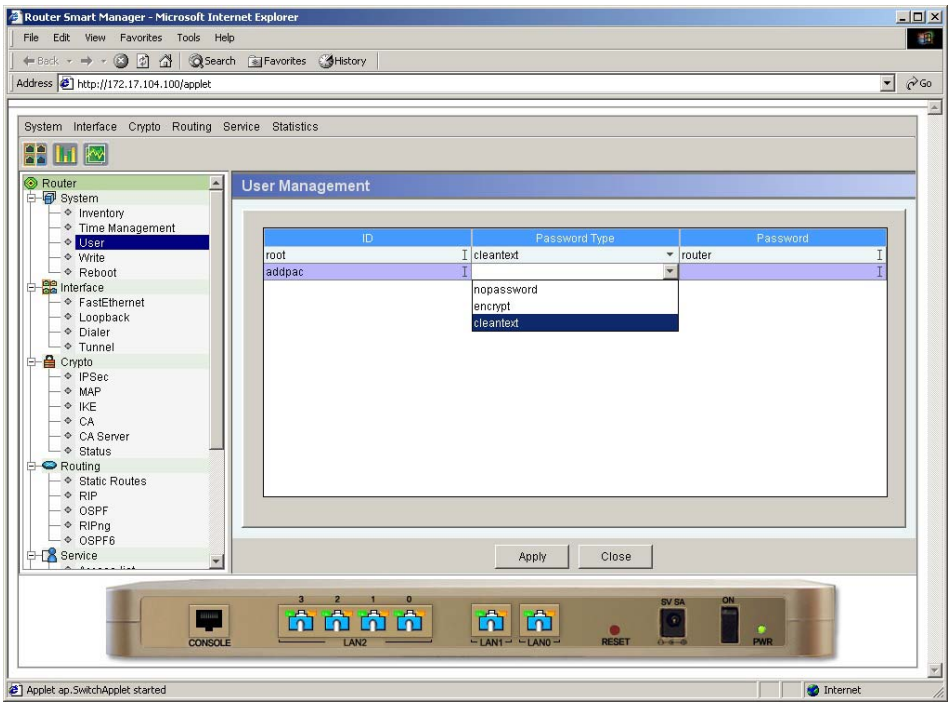
Elements	Description
ID	Define user ID.
Password Type	Define password type on Smart Manager. "Nopassword" is when you do not use Password, "Encrypt" is when the password is shown as an encryption and "Cleartext" is when password is shown without encryption.
Password	Define Password for specific ID.

Figure 3-27 shows an example of adding user ID/Password/PasswordType: as (“addpac”/”router”/”ClearText”).
First, double click on blank ID field then enter “addpac”



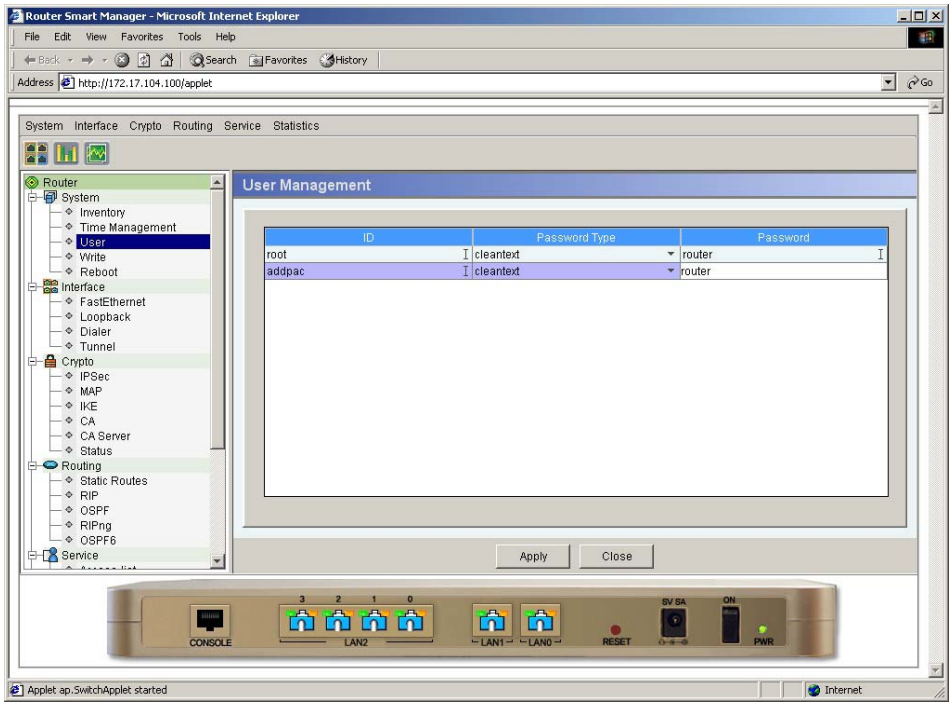
(Figure3-26) Input User Management ID

Set Password Type to “ClearText”



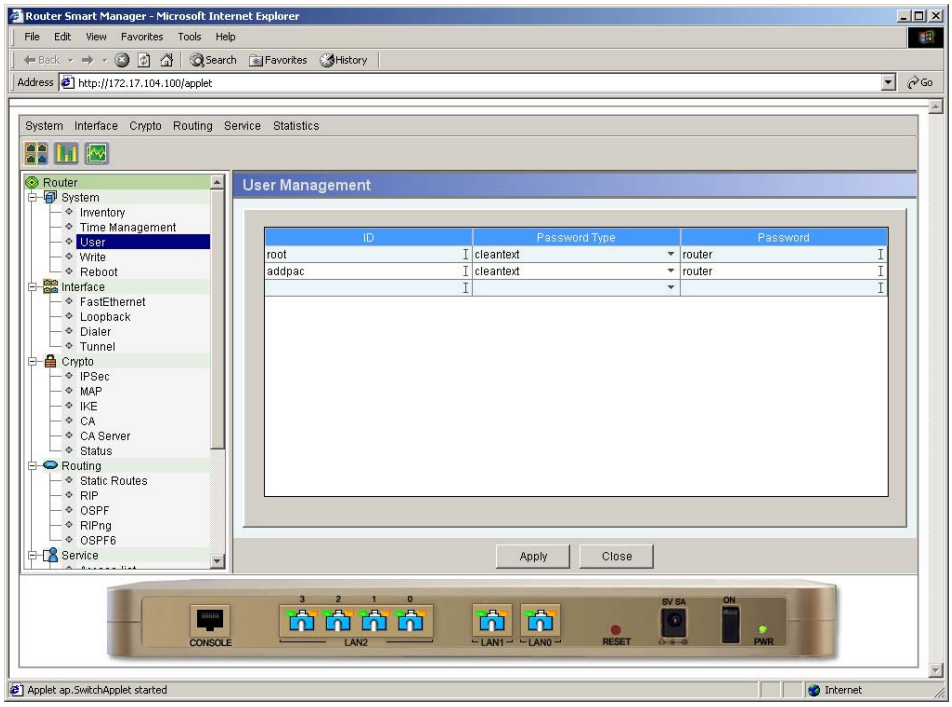
(Figure3-27) Select User Management Password Type

Input “router” in Password field, then Click Enter.



(Figure3-28) Enter User Management Password

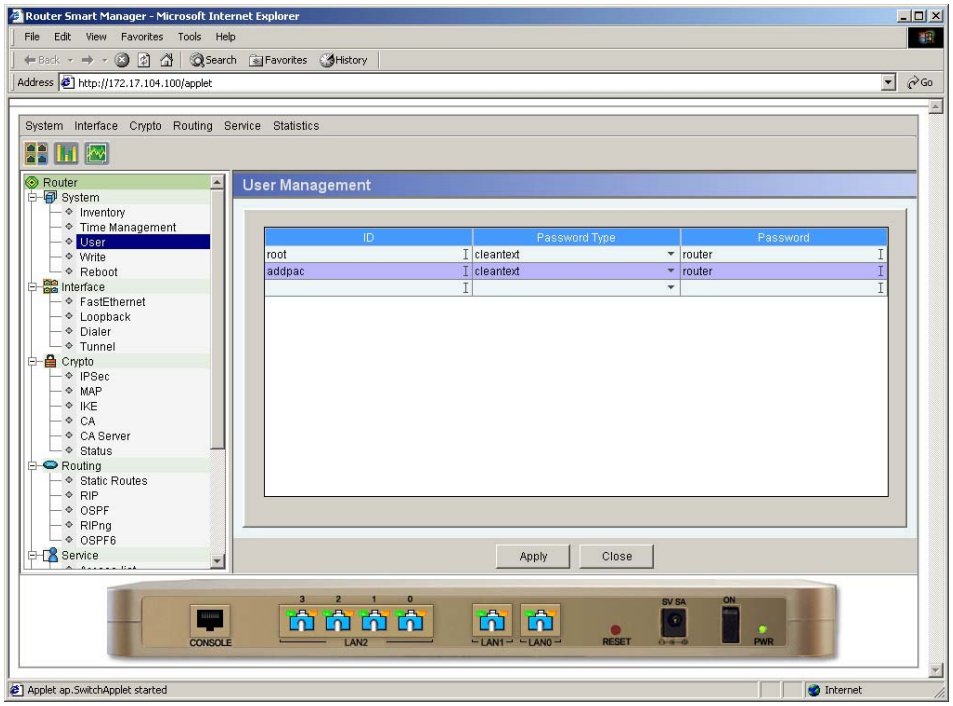
At Figure 3-30, new User IDs are shown.



(Figure3-29) User Management –new ID

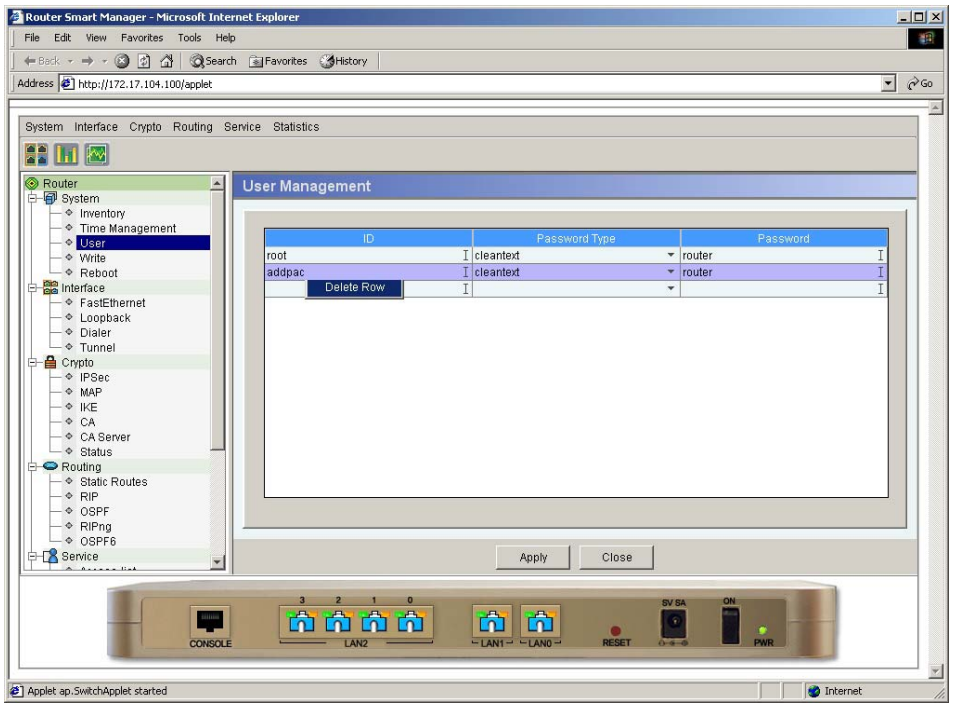
Figure 3-31 shows how to delete user ID "addpac".

Select the ID you want to delete with a mouse.



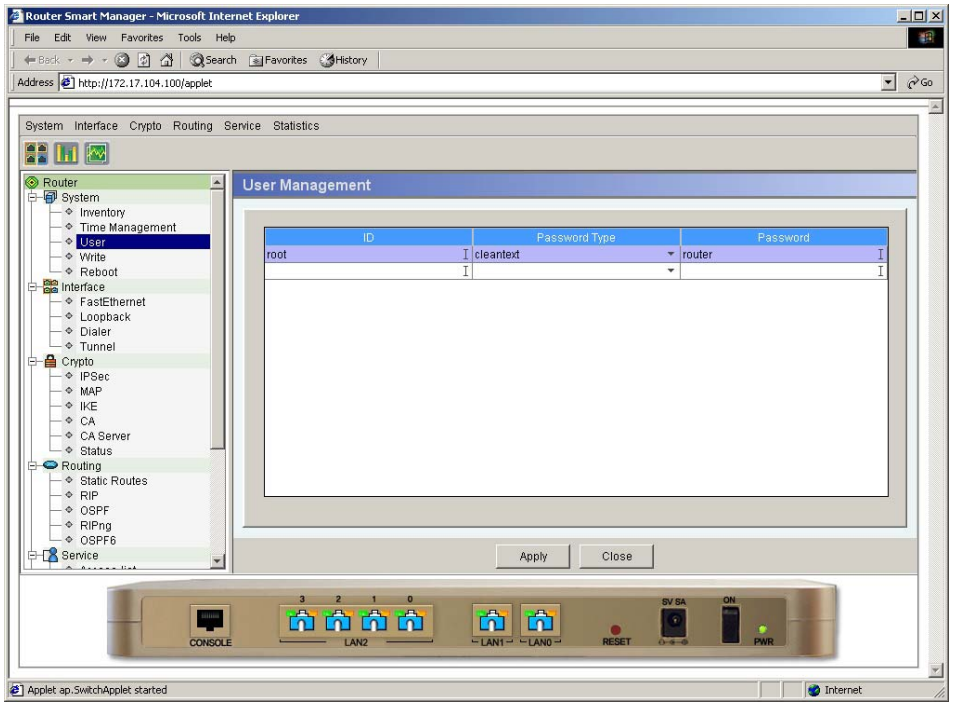
(Figure3-30) User Management-select user ID

Select "Delete Row" by clicking right side of the mouse.



(Figure3-31) Select User Management Delete Row

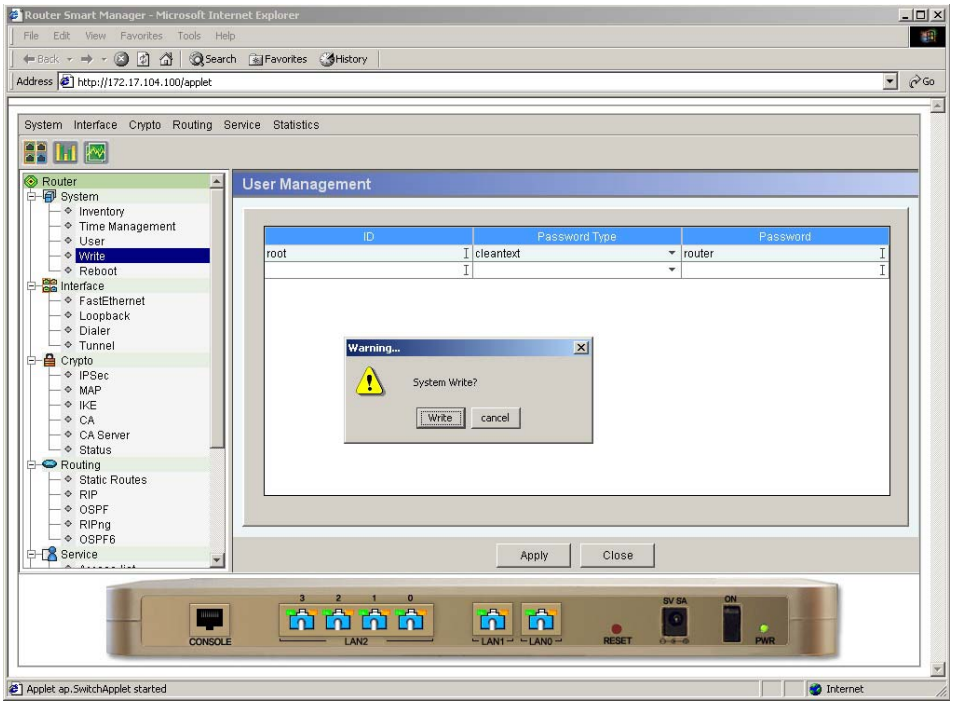
At Figure 3-33, Use ID "addpac" is deleted.



(Figure3-32) User Management user ID deleted

Write

The changed parameter values of System, Interface, Crypto, Routing, Service, Statistics menus are stored in the volatile main memory, SDRAM temporarily. Make sure to save the values permanently using Write command. Otherwise, the new values are lost when AP900S power is turned off.

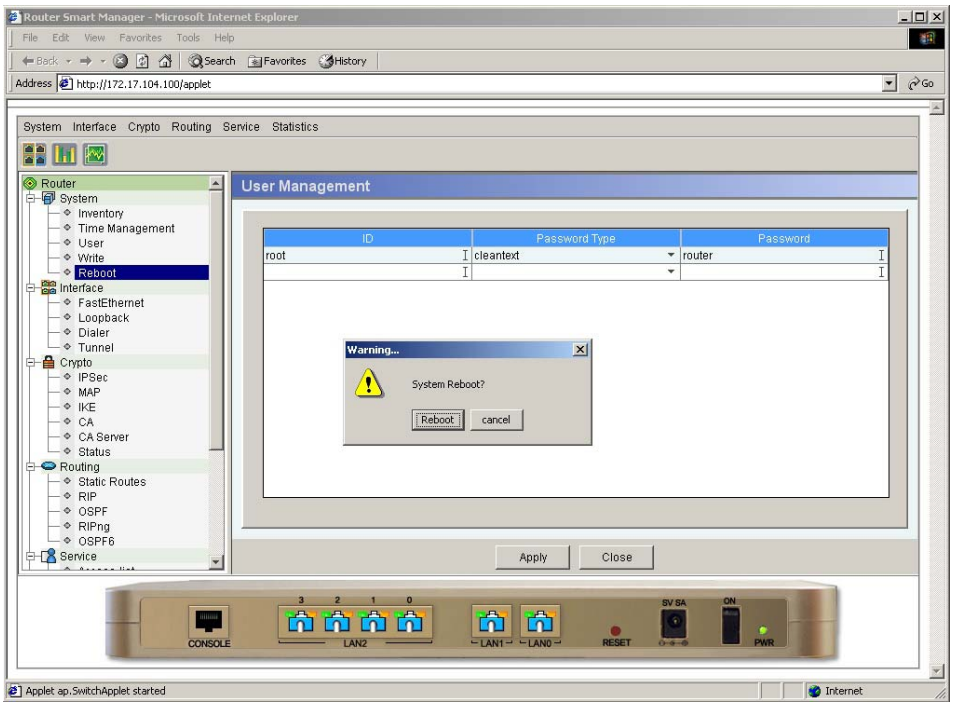


(Figure3-33) Write menu page

Reboot

Use “Reboot” when an operator wants to re-start the system without power down(cold start).

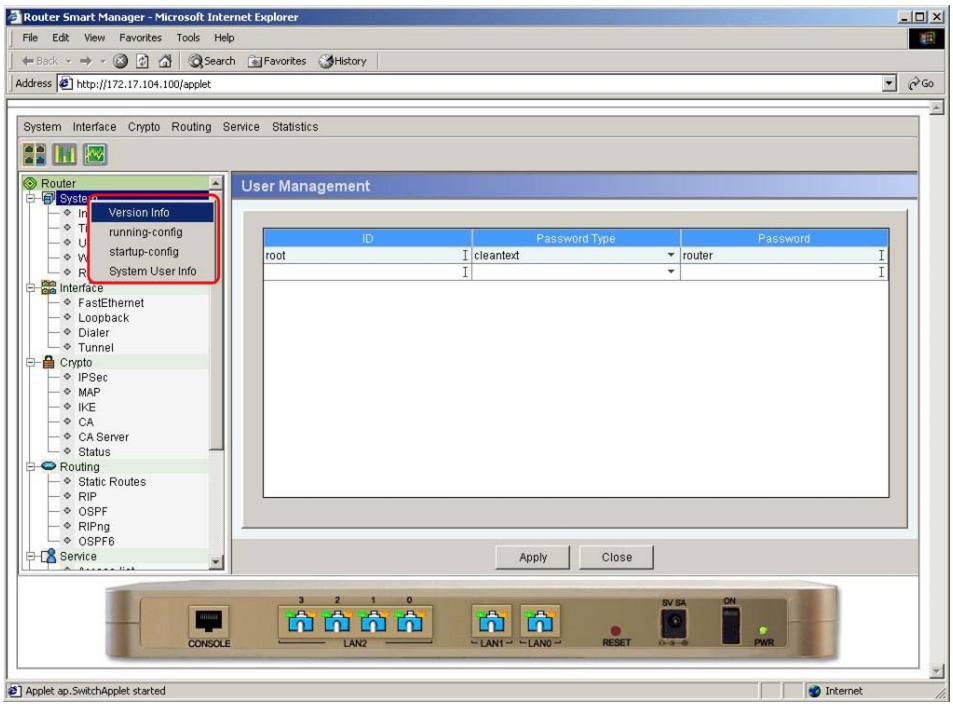
Caution: Smart Manager can be stopped for a while when reboot is executed.



(Figure3-34) System Reboot main page

System Popup Menu

To use Popup Menu, Select System and click on right side of mouse. This menu consists of APOS Version Info, Running-Configuration, Startup-configuration, and System User Info of AP900S. Click on each element to see the more information.

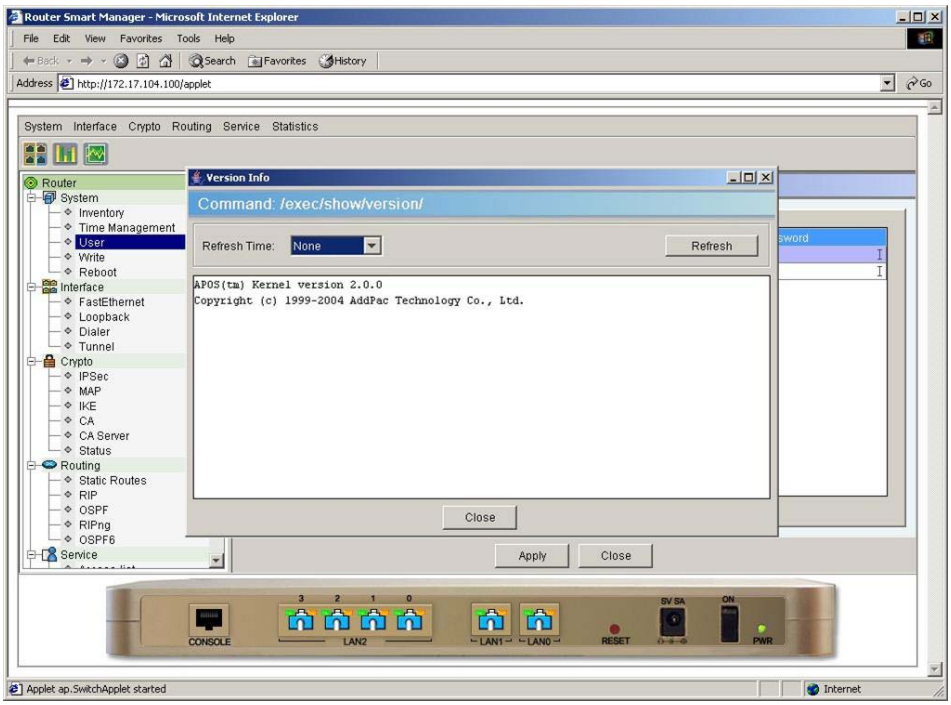


(Figure3-35) System Popup Menu page

<Table 3-8> System Popup Menu Description

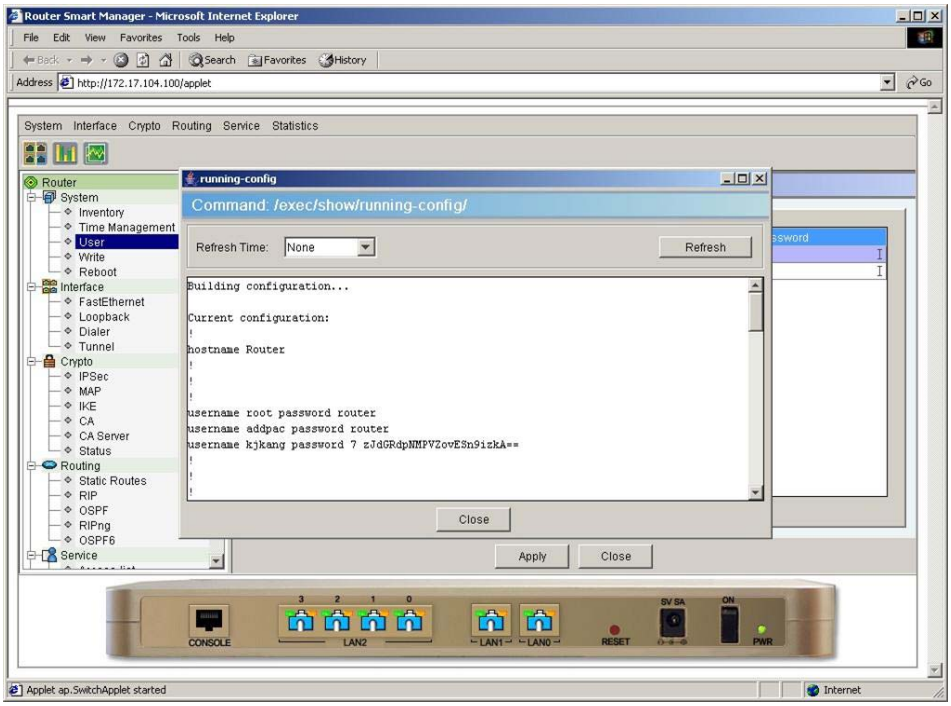
Elements	Description
Version Info	APOS Version Info of AP900S
Running-Config	Running-Configuration on main memory
Startup-Config	Startup-Configuration information
System User Info	User Account information

Figure 3-37 is “Version Info” page. Refresh Time can take 3 to 5 sec or click “Refresh” button to see the information right away. Version Info of AP900S is the same Version of APOS.



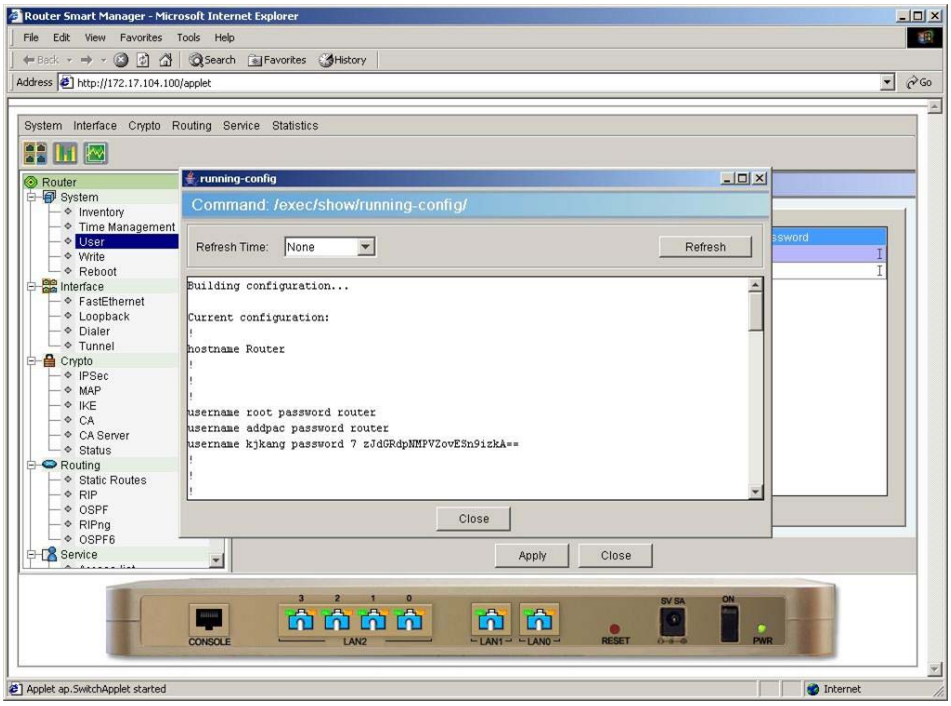
(Figure3-36) System Version Info page

Figure 3-38 is Running-Config page. Refresh Time can take 3 to 5 sec or click on “Refresh” button to see the information right away. Running-Config is configuration of current AP900S memory and it controls operations of AP900S.



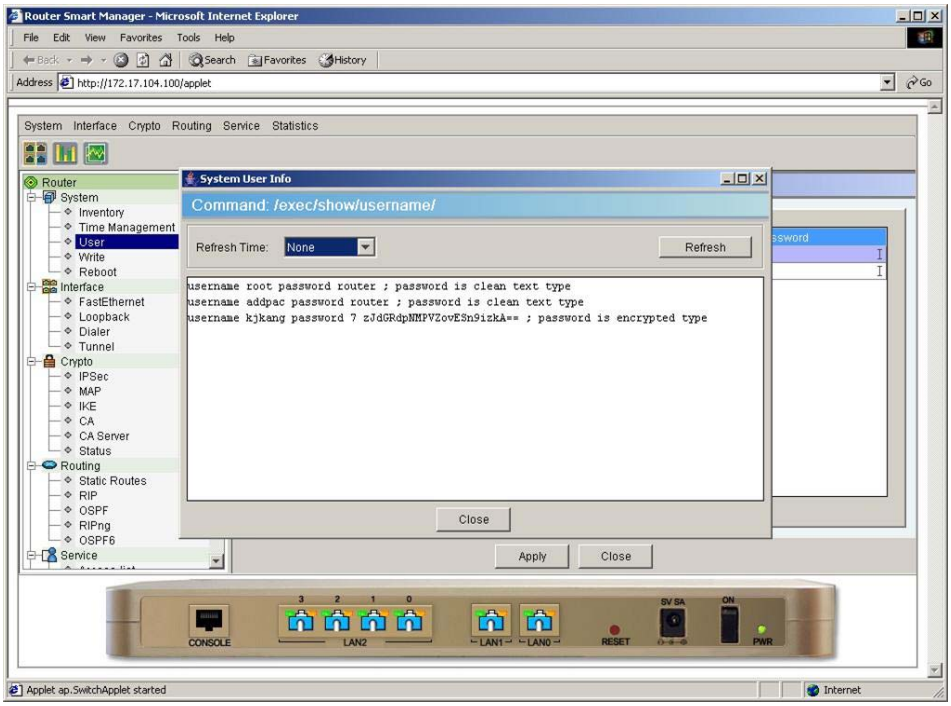
(Figure3-37) System Running-Config page

Figure 3-39 is Startup-Config page. Refresh Time can take 3 to 5 sec or click on “Refresh” button to see the information right away. Startup-Config is configuration info which is saved in non-volatile flash memory. It is read when initial start up of AP900S, so it is irrelevant with operation of current AP900S.



(Figure3-38) System Startup-Config page

Figure 3-40 is System User Info page. Refresh Time can take 3 to 5 sec or click on “Refresh” button to see the information right away. System User Info shows the information of new ID which is created from User Management.



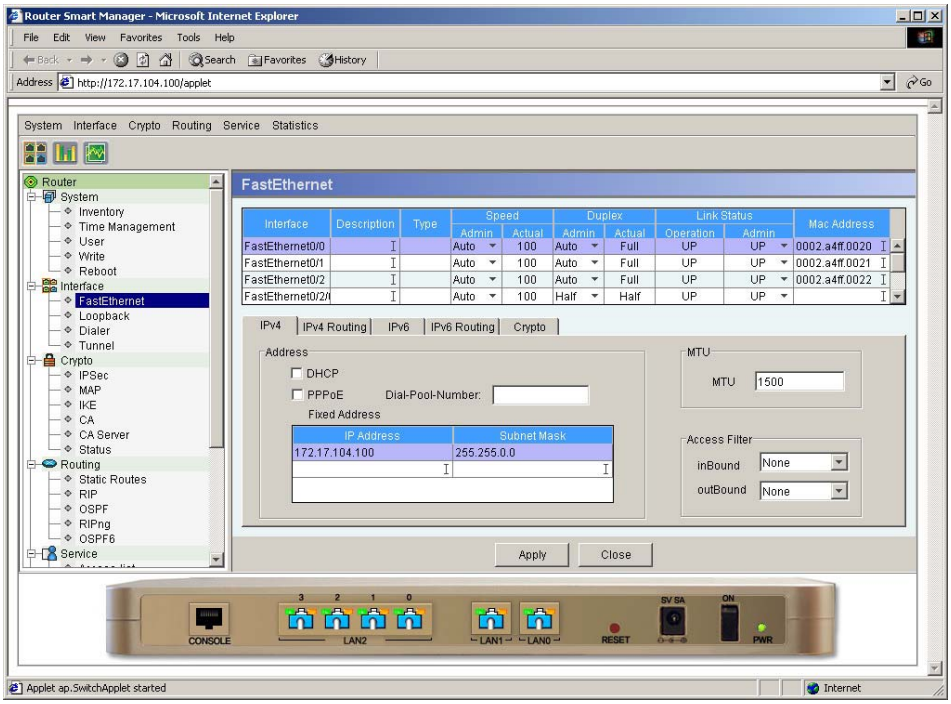
(Figure3-39) System User Info page

Interface Menus

Interface menu consists of FastEthernet, Loopback, Dialer and Tunnel. Operator enables to change settings for all interfaces of AP900S and apply created values from Crypto, Routing, Service, and Statistics to Interface.

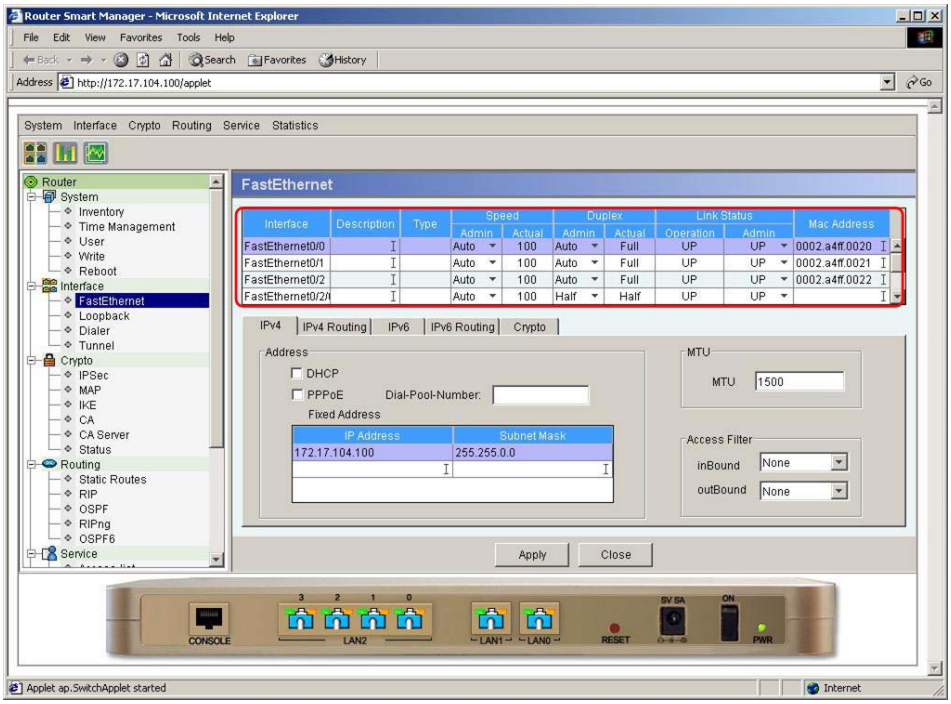
FastEthernet

FastEthernet menu not only enable controlling and link status monitoring of all AP900S interfaces but also configures parameter settings for Routing Protocol, IPv6, Crypto, and Access-List. The operator can change parameter setting values for each interface.



(Figure3-40) FastEthernet Main page

Figure 3-42 is Link Status Info of each interface.

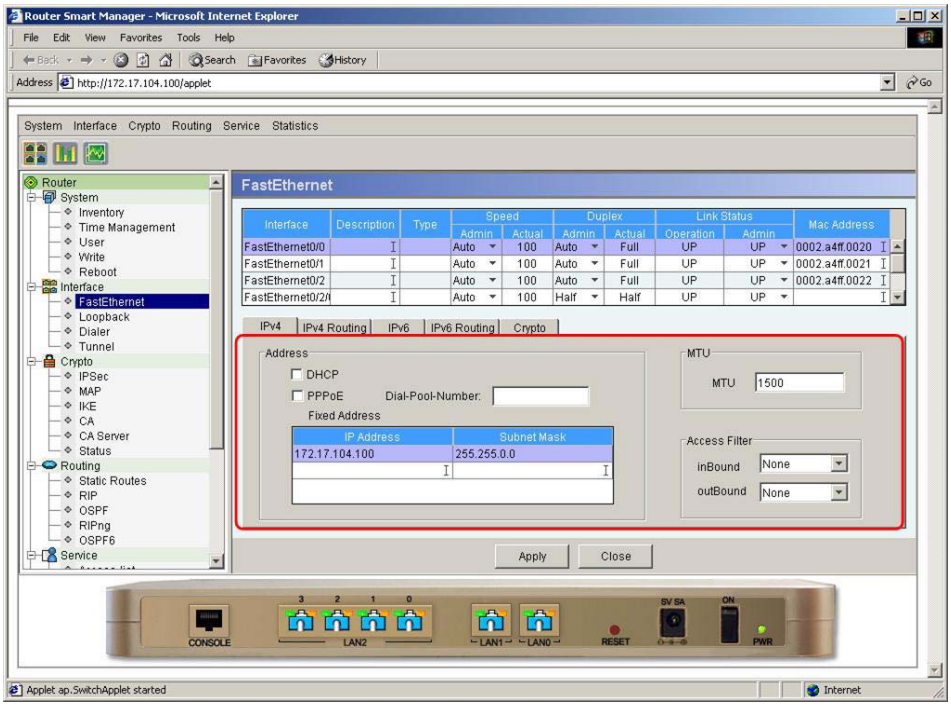


(Figure3-41) FastEthernet Interface Link Status Info

<Table 3-9> Interface Link Status Info Description

Elements	Description
Interface	Shows Ethernet Interface of AP900S
Description	Shows Comment field
Speed	Link Speed of interface. Operator can choose one among 10Mbps, 100Mbps or Auto Negotiation. User can check actual Link Speed on the system.
Duplex	Duplex Mode of Interface. Operator can choose one from Half Duplex, Full Duplex or Auto Negotiation. Actual Duplex Mode can be checked on the system.
Link Status	Link Status of interface. It can be used to shutdown interfaces by user. Actual Link up/down can be checked on operation field.
MAC Address	Shows MAC address of interface

Figure 3-43 shows IPv4 Info of each interface.

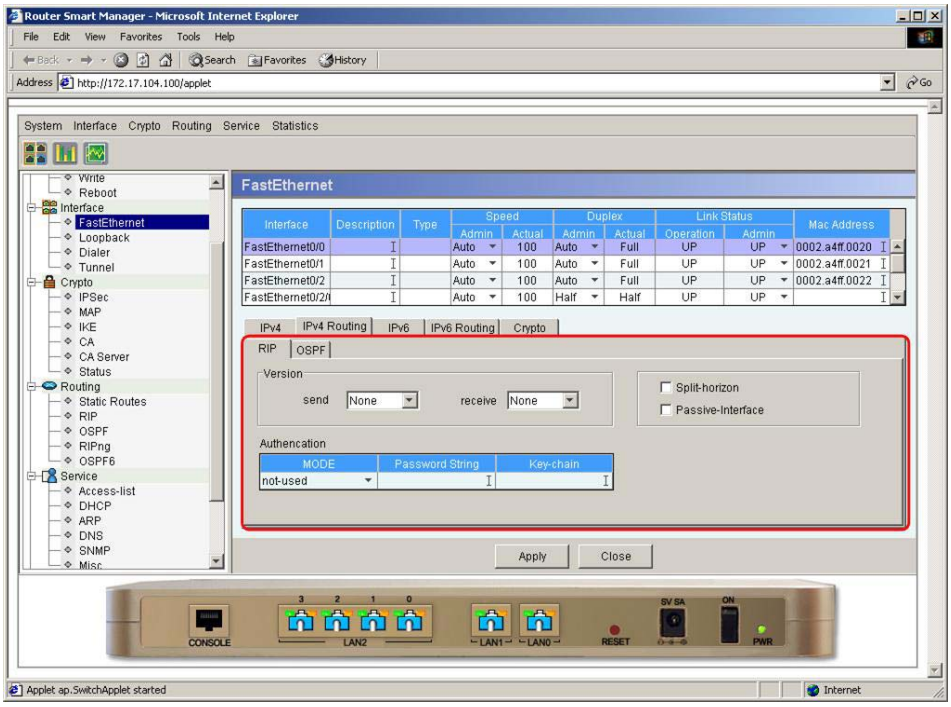


(Figure3-42) Interface IPv4 Info

<Table 3-10> Interface IPv4 Info Description

Elements	Description
DHCP	Set Interface to DHCP Client
PPPoE	Set Interface to PPPoE Client
Dial-Pool Number	Assign Dialer. Dialer includes authentication method for PPP Session, user ID info. User has to enter per-written Dialer.
IP Address/ Subnet mask	Enter fixed IP Address to interface.
MTU	MTU(maximum transmission unit), it limits maximum size of packet. Default value is 1500 Bytes.
Access Filter	It is used in Service menu to apply Access-List to interface.

Figure 3-44 shows IPv4 RIP Information of each interface.

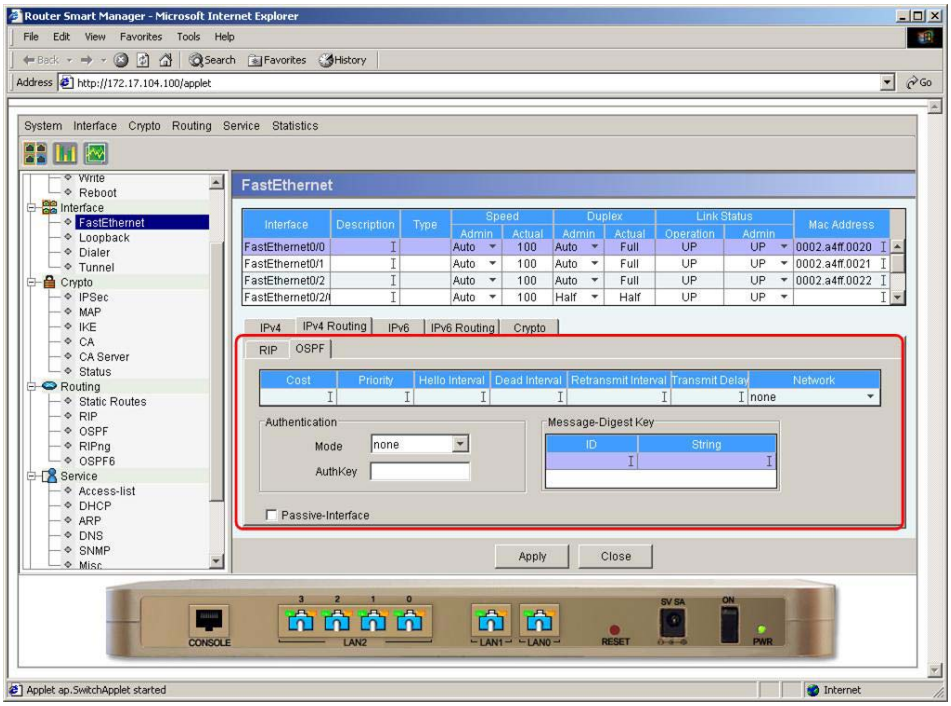


(Figure3-43) Interface IPv4 RIP Info

<Table 3-11> Interface IPv4 RIP Info Description

Elements	Description
Version Send/ Receive	It decides RIP Version which is used for exchanging RIP Routing Table. Generally RIP Version2 is used, and when it is necessary, send/receive Version can be set differently.
Split-Horizon	Split-Horizon is to prevent Loop phenomenon caused by unreachable network when using RIP as Routing Protocol.
Passive-Interface	Only to receive RIP Routing Table.
Authentication Mode	When there is no authentication : Not-used, When using text authentication: Simple-Text When using MD5 for password encryption : md5
Password String	Enter password when using Simple-Text and MD5.
Key-Chain	Input the KEY value for using MD5 algorithm.

Figure 3-45 shows IPv4 OSPF Information of each interface.



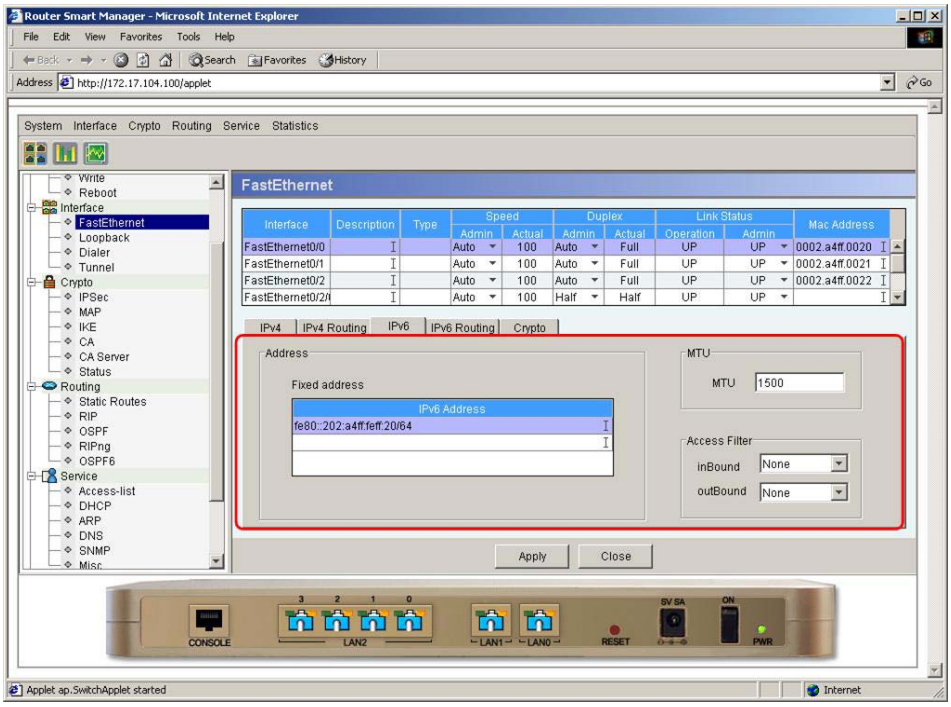
(Figure3-44) Interface IPv4 OSPF Info

<Table 3-12> Interface IPv4 OSPF Info Description

Elements	Description
Cost	Input the cost of interface which is used for comparing path between destinations. Lower Cost has high priority.
Priority	It decides Priority of interface. This is used when deciding Designated Router.
Hello Interval	It decides transfer interval of Hello Packet which checks the status of peer interface.
Dead Interval	It decides waiting time after declaring Dead status on peer Interface.
Retransmit Interval	It decides re-transmit interval when Link State Advertisement Packet is lost.
Transmit Delay	It decides transfer delay for Link State Advertisement Packet.
Network	It configures the network interface.
Authentication Mode	When there is no authentication : Not-used, when using text authentication: Simple-Text when using MD5 for password encryption : md5

Auth Key	Input the key value when Simple-Text is used.
Message-Digest Key	Input ID and String value when MD5 algorithm is used.
Passive-Interface	It is used to receive OSPF Routing Table from a specific interface.

Figure 3-46 shows IPv6 Info of interface.

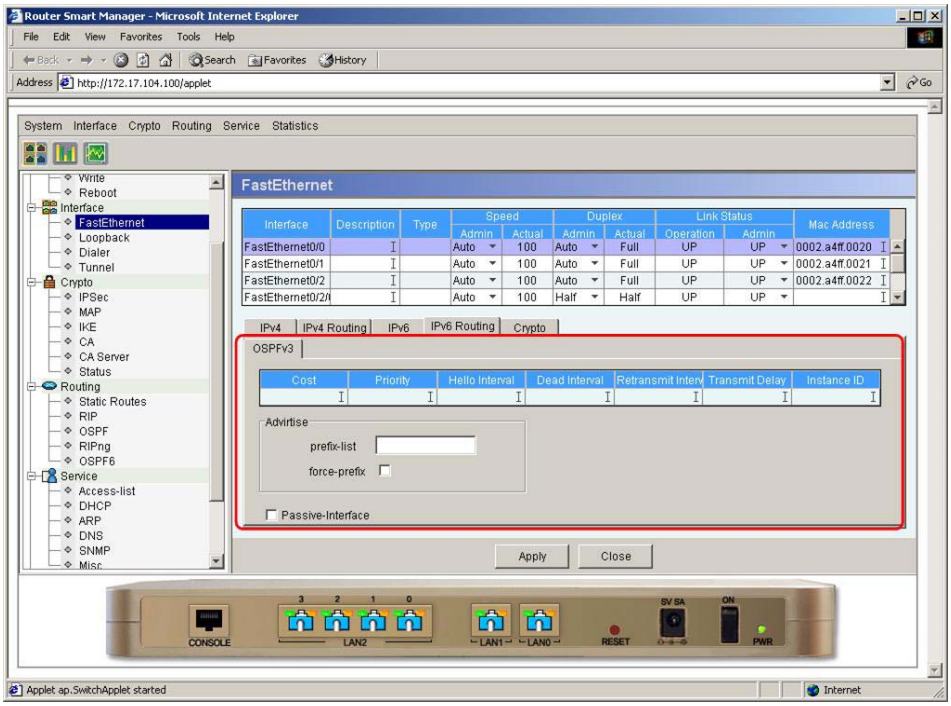


(Figure3-45) Interface IPv6 Info

<Table 3-13> Interface IPv6 Info Description

Elements	Description
Fixed IP Address	Input 128 bit Fixed IPv6 Address.
MTU	Maximum Transmission Unit, maximum size of Packet.
Access Filter InBound	It is used to apply Access-List to interface. Inbound is used for filtering receiving packet.
Access Filter OutBound	It is used to apply Access-List to interface. Outbound is used for filtering sending packet.

Figure 3-47 shows IPv6 Routing Information of interface. This is about IPv6 OSPFv3.



(Figure3-46) Interface IPv6 OSPFv3 Info

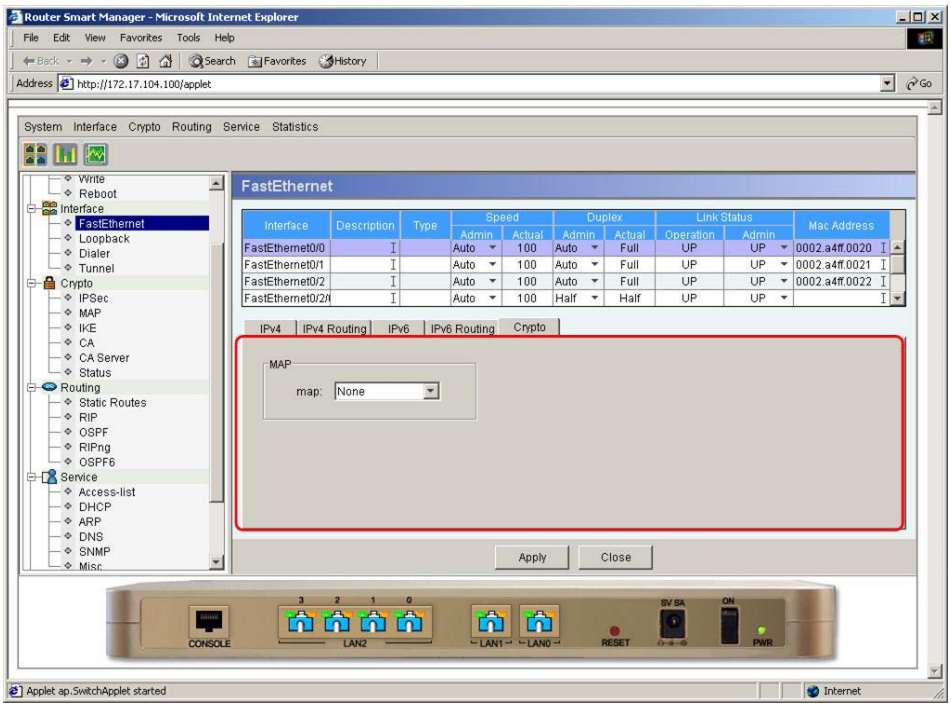
<Table 3-14> Interface IPv6 OSPFv3 Info Description

Elements	Description
Cost	Input the cost of interface which used for comparing path between OSPF to destiny. Lower Cost has high priority.
Priority	It decides Priority of interface. This is used when deciding Designated Router.
Hello Interval	It decides transfer interval of Hello Packet which checks the status of peer interface
Dead Interval	It decides waiting time after declaring Dead status on peer Interface.
Retransmit Interval	It decides re-transmit interval when Link State Advertisement Packet is lost.
Transmit Delay	It decides transfer delay for Link State Advertisement Packet.
Instance ID	Input Instance ID which is used for exchanging OSPF Routing Table.

Advertise Prefix-list	It is to prevent or to accept specific network information when exchanging OSPF Routing Table. Prefix-list has to be pre-written to apply.
Force-Prefix	Even if Interface is Loopback, or Point-to-Point, Prefix-List is forced to be applied.
Passive-Interface	It is used when receiving OSPF Routing Table in a specific interface.

Figure 3-48 shows Crypto Information of interface

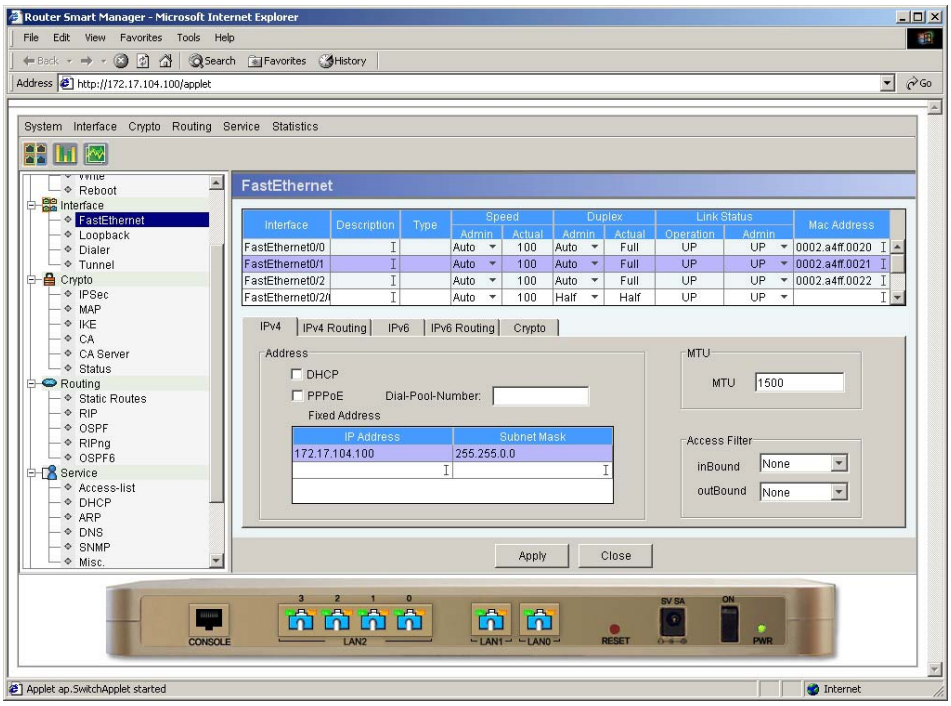
It is used when Crypto Map, which is created from Crypto menu, is applied to the interface. Select the Map using scroll bar.



(Figure3-47) Interface Crypto Info

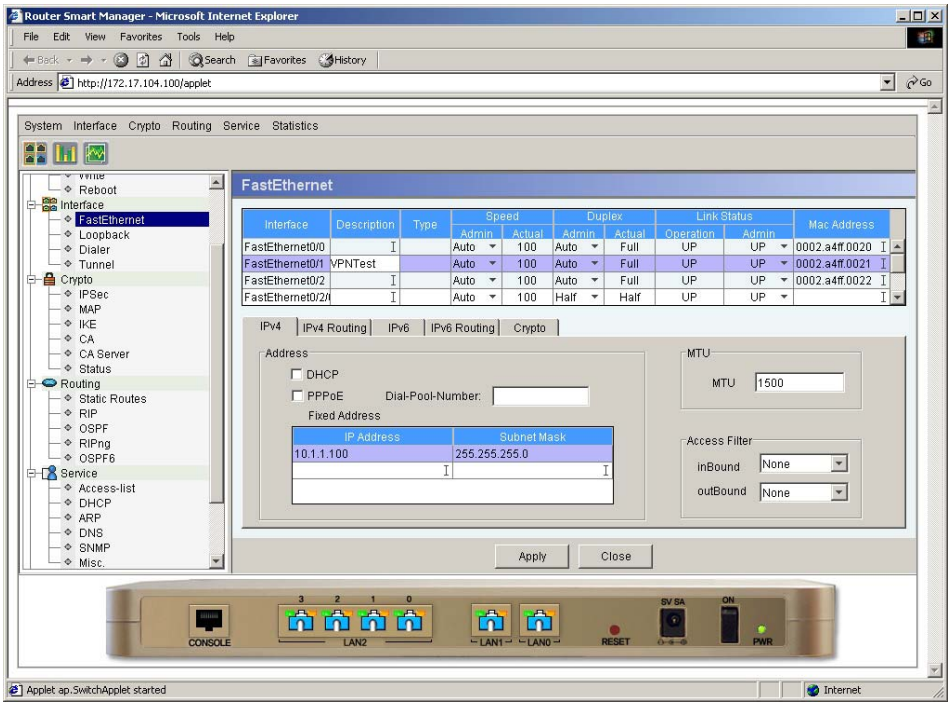
Figure 3-49 shows configuration after selecting Fast Ethernet 0/1

First, Select Fast Ethernet 0/1



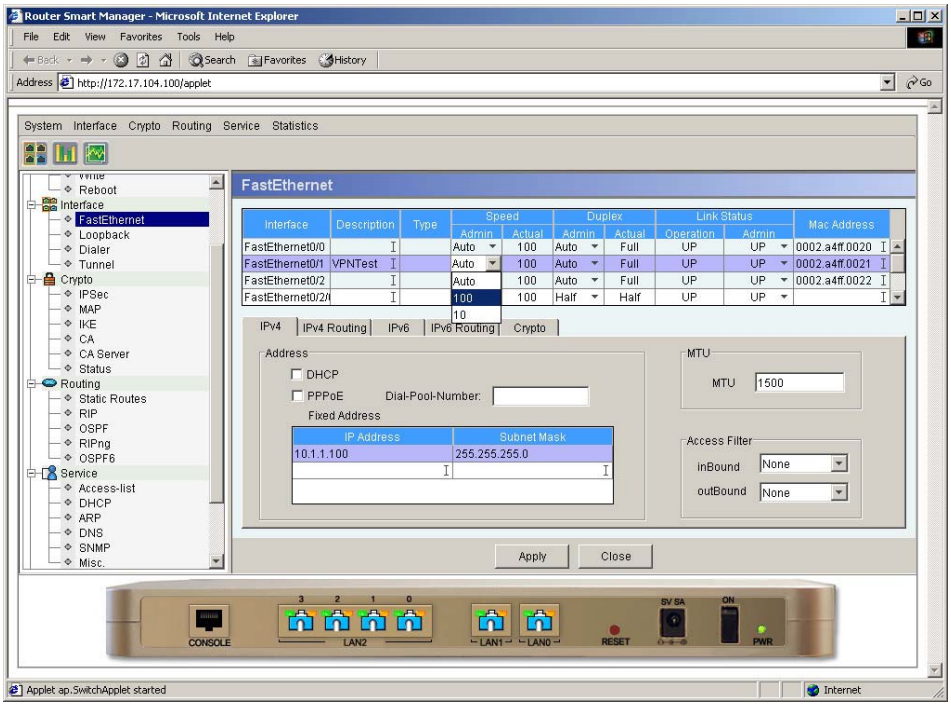
(Figure3-48) Select Fast Ethernet 0/1

Double click Description field. Input “VPNTest”.



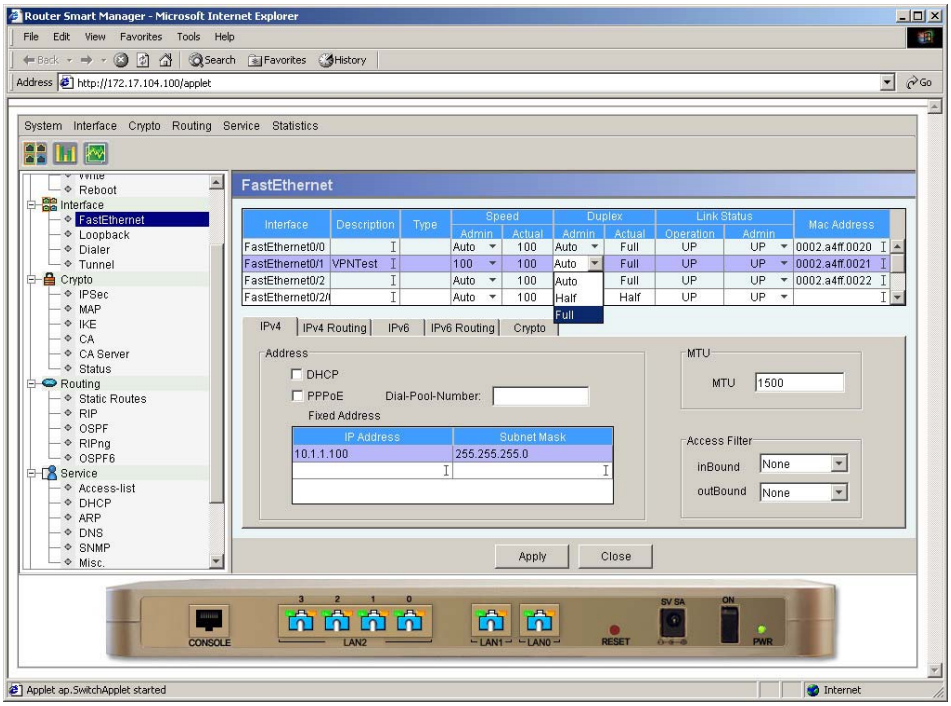
(Figure3-49) Input Fast Ethernet 0/1 Description

Select 100Mbps in Link Speed field.



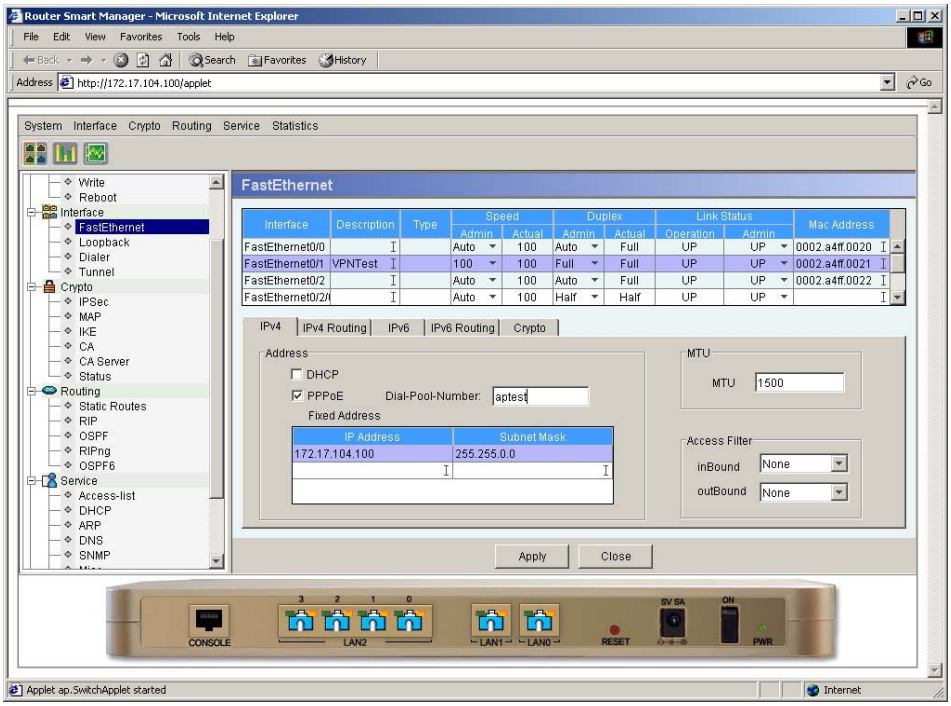
(Figure3-50) Select Fast Ethernet 0/1 Link Speed

Select Full Duplex in Link Duplex field.



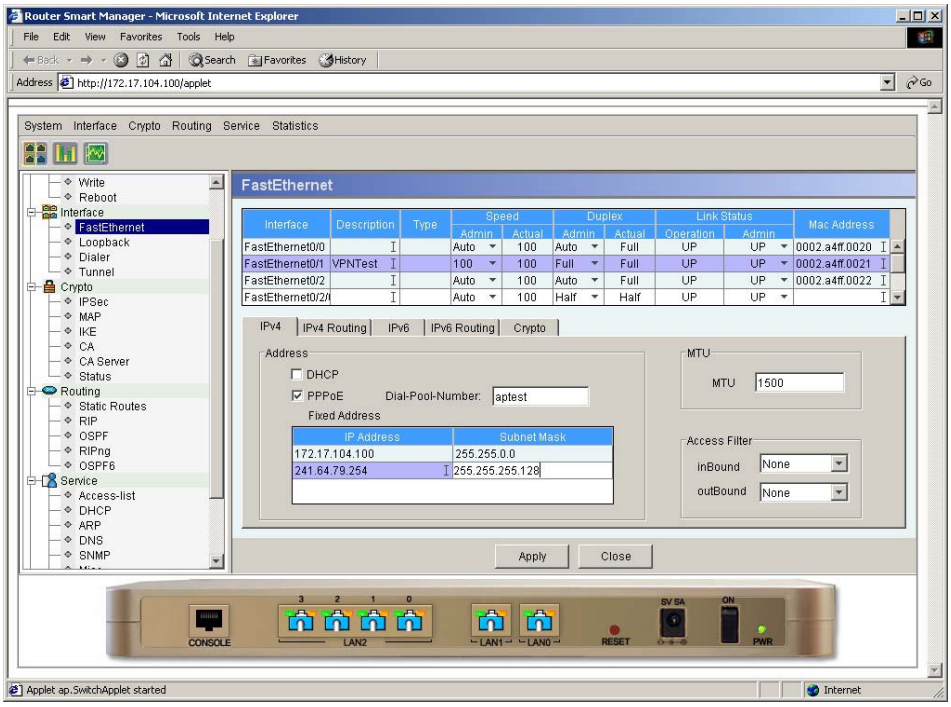
(Figure3-51) Select Fast Ethernet 0/1 Link Duplex

Check PPPoE to use appropriate interface as PPPoE Client. Then enter Dial-Pool Number. In this Figure, input "aptest" for Dialer.



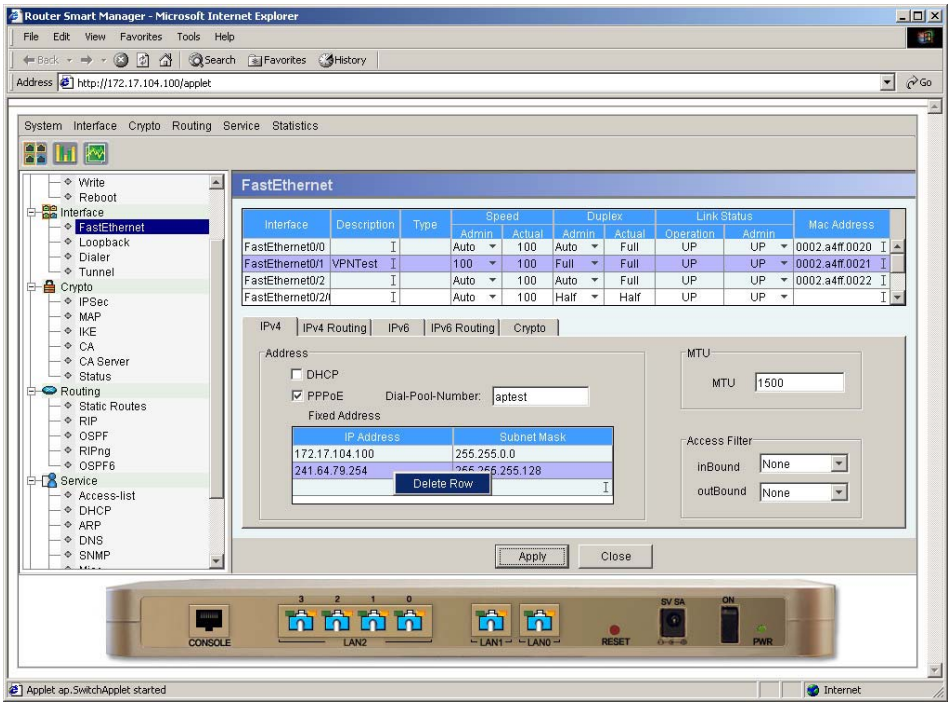
(Figure3-52) Input Fast Ethernet PPPoE Dialer

To add IP Address in the interface, input the IP Address in Fixed Address field.



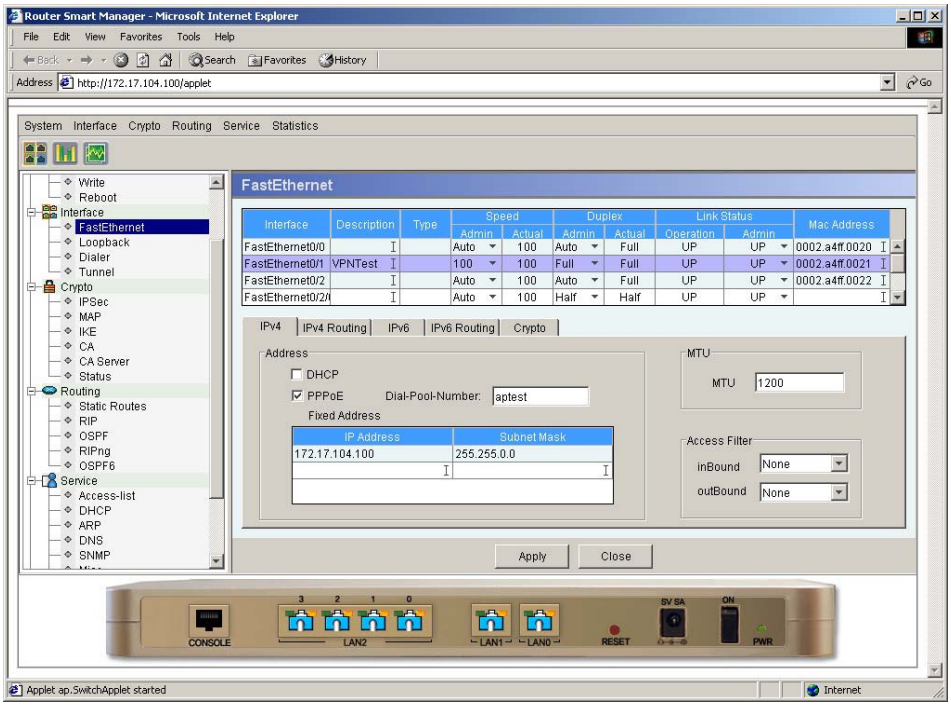
(Figure3-53) Input Fast Ethernet Fixed IP Address

To delete IP Address in interface, Select “Delete Row” by clicking right side of mouse then, delete IP Address.



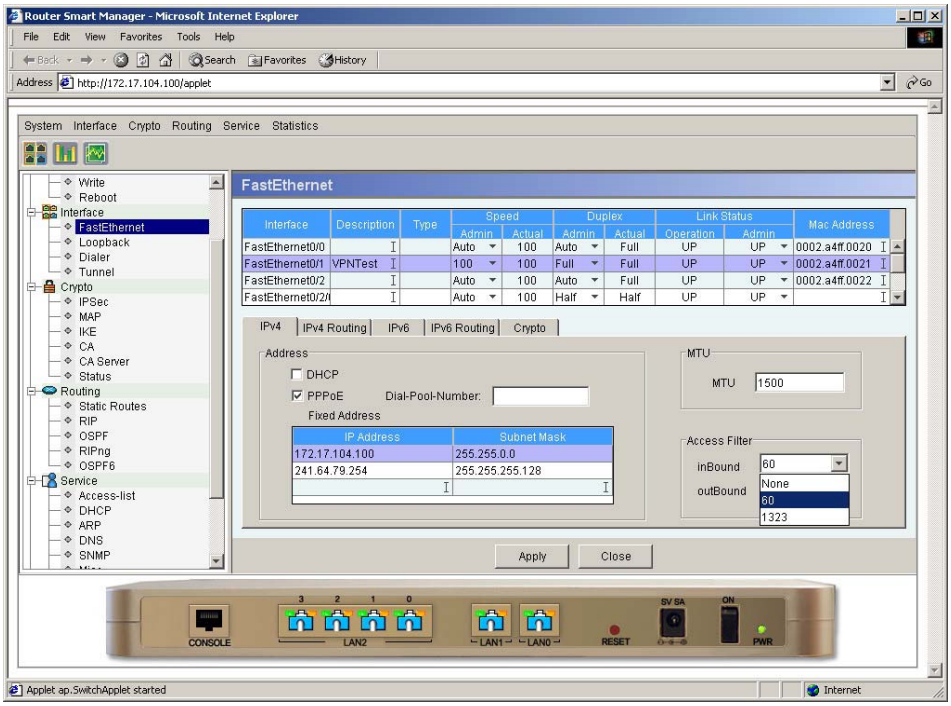
(Figure3-54) Input Fast Ethernet Fixed IP Address

Change the value of MTU(Maximum Transmission Unit) to 1024.



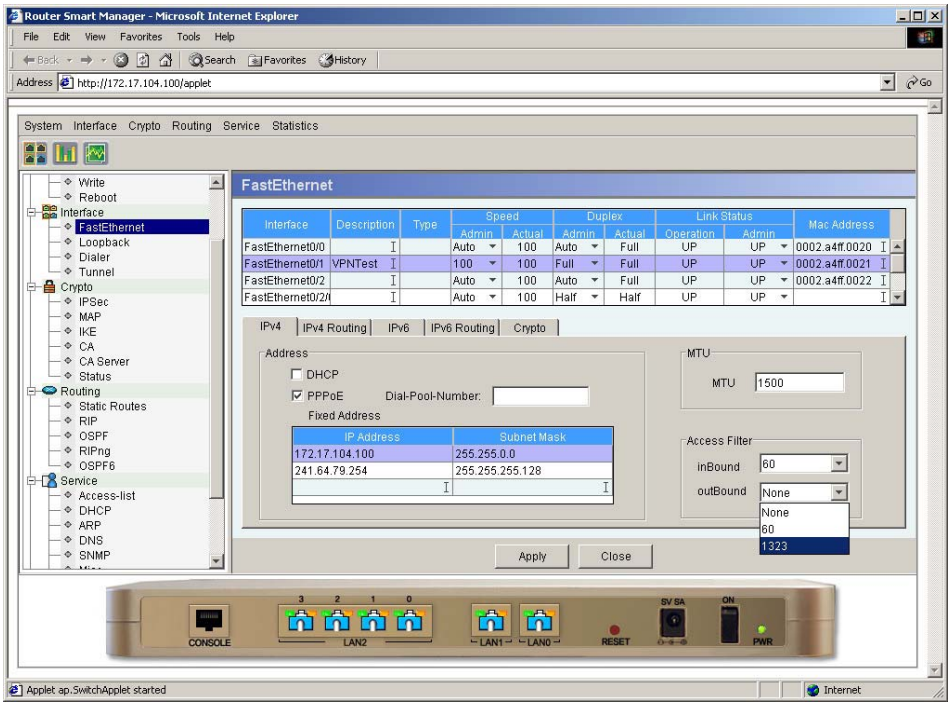
(Figure3-55) Change Fast Ethernet MTU

Select “Access-List 60” for Access Filter Inbound.



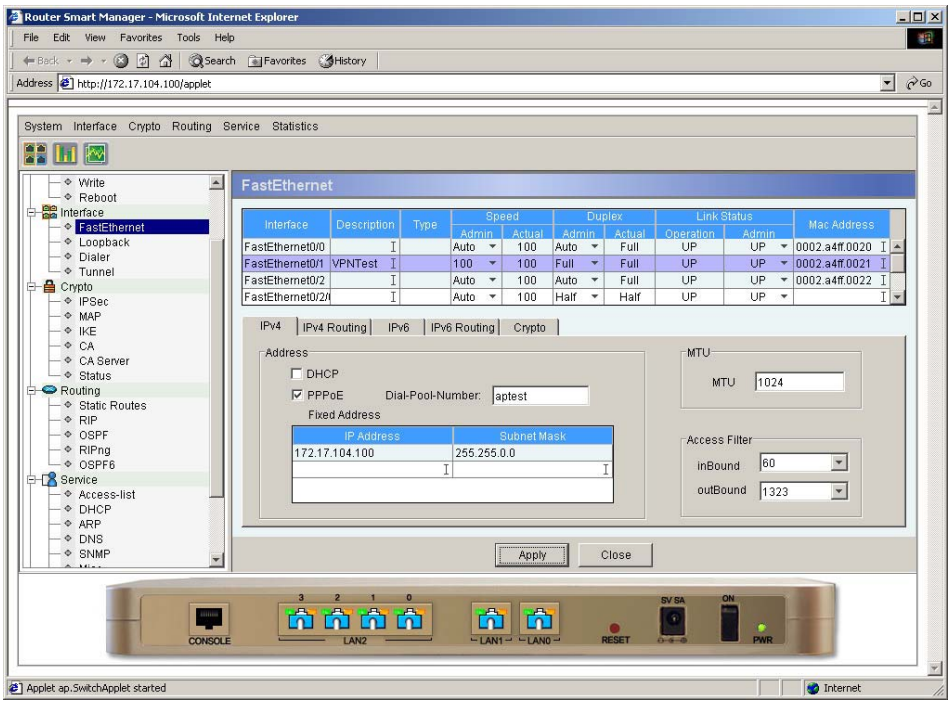
(Figure3-56) Select Fast Ethernet Access Filter Inbound

Select “Access-List 1323” for Access Filter Outbound.



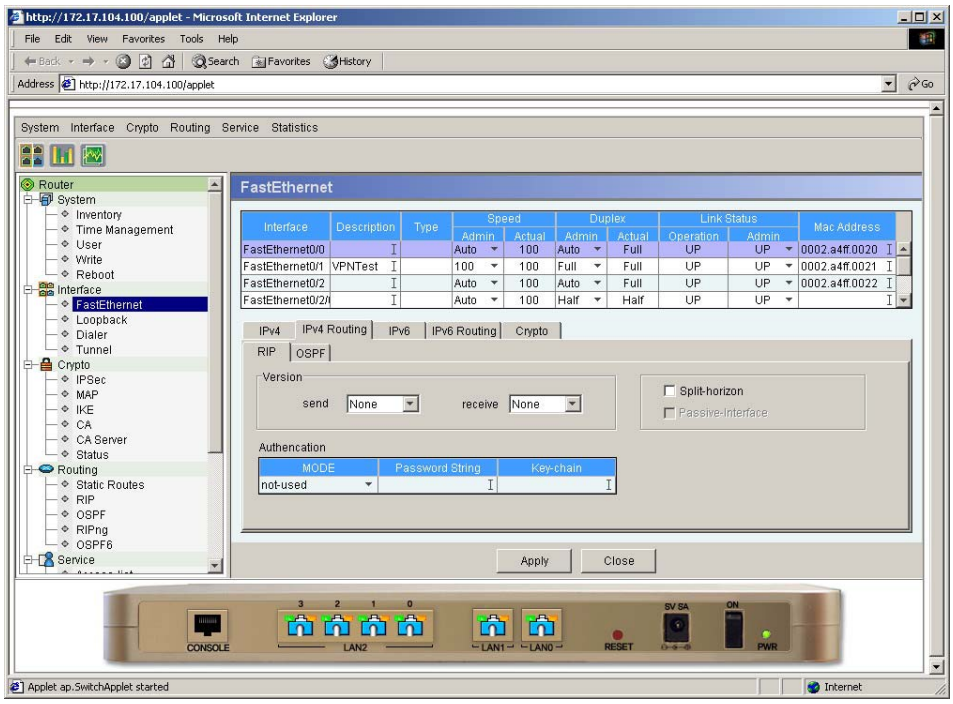
(Figure3-57) Select Fast Ethernet Access Filter Outbound

Figure 3-59 will be shown by clicking “Apply”.



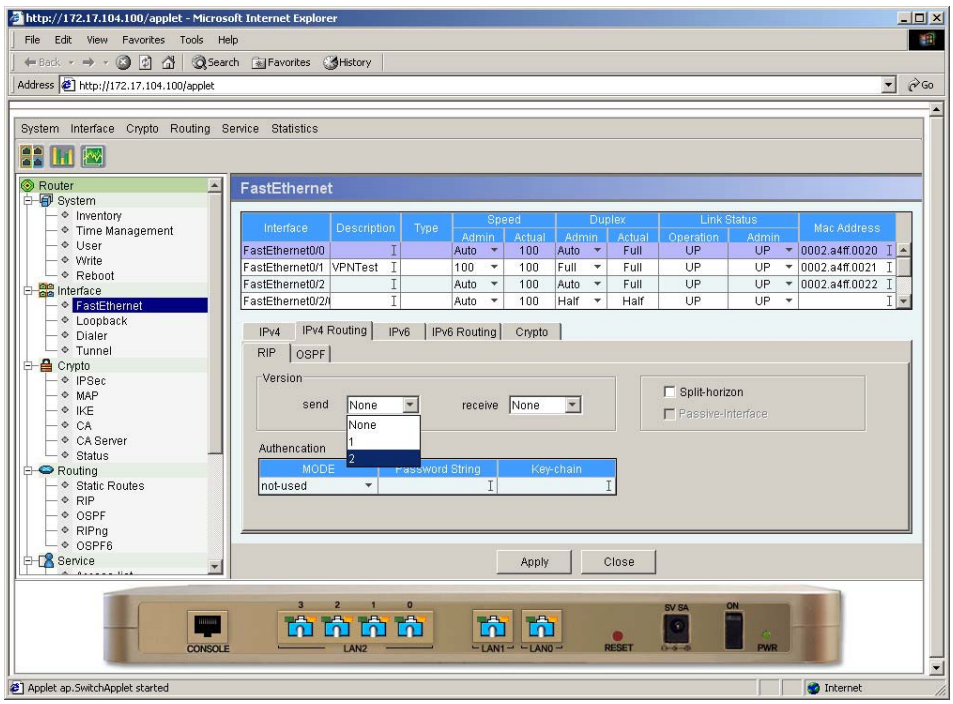
(Figure3-58) Checking Fast Ethernet IPv4 value

Figure 3-60 shows how to change configuration settings for Fast Ethernet 0/1 RIP. Select Fast Ethernet 0/1 -> select IPv4 Routing RIP.



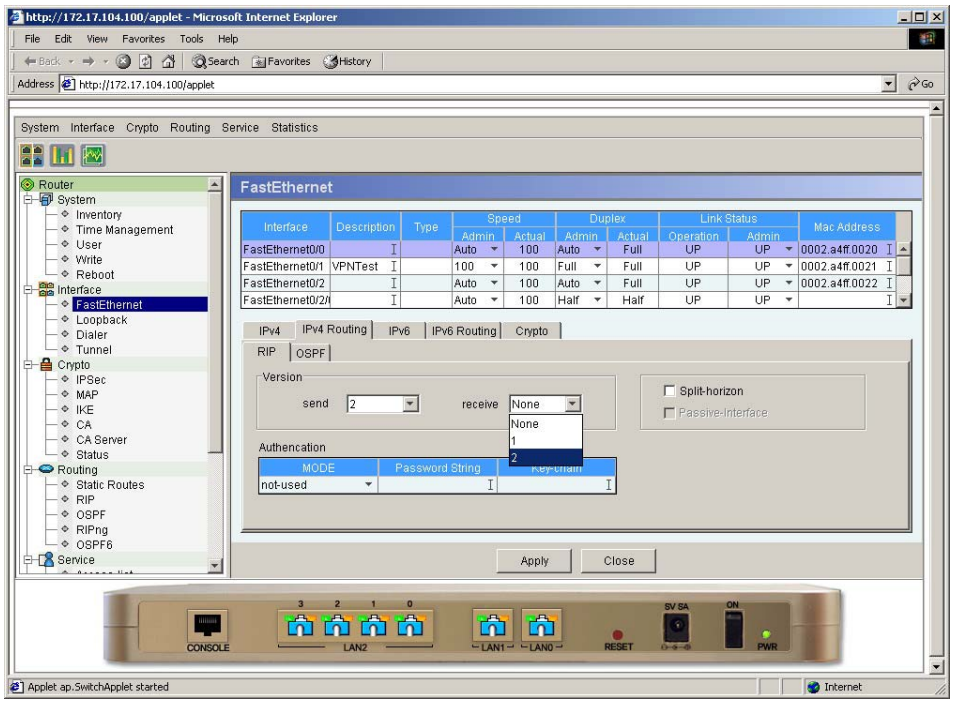
(Figure3-59) Select Fast Ethernet IPv4 Routing RIP

Select Version of RIP Routing Table to send.



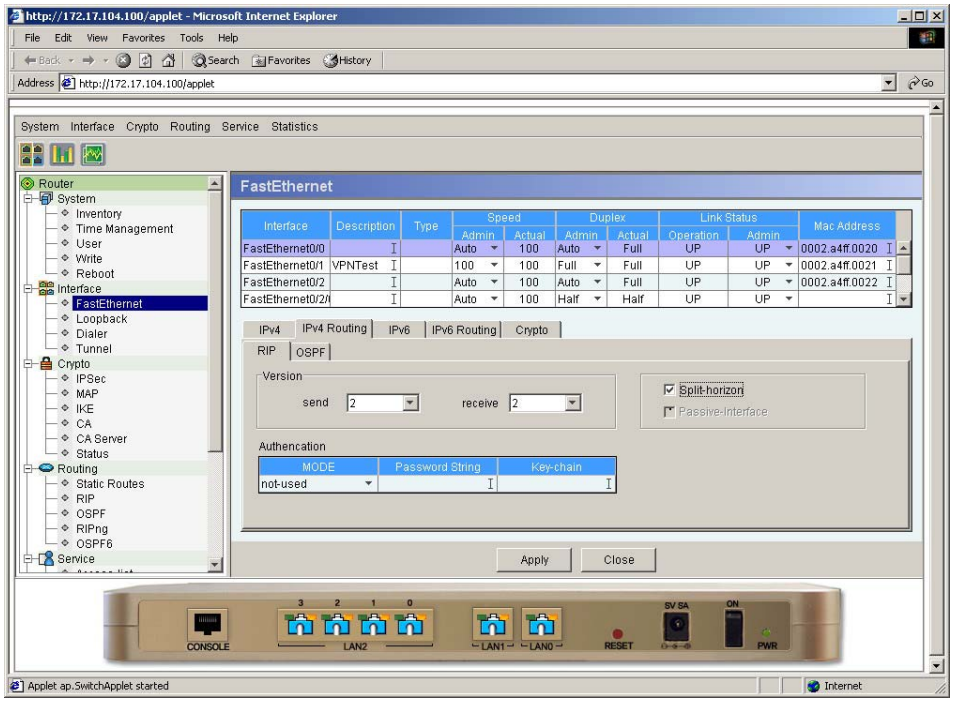
(Figure3-60) Select Fast Ethernet RIP Send Version

Select Version of RIP Routing Table to receive.



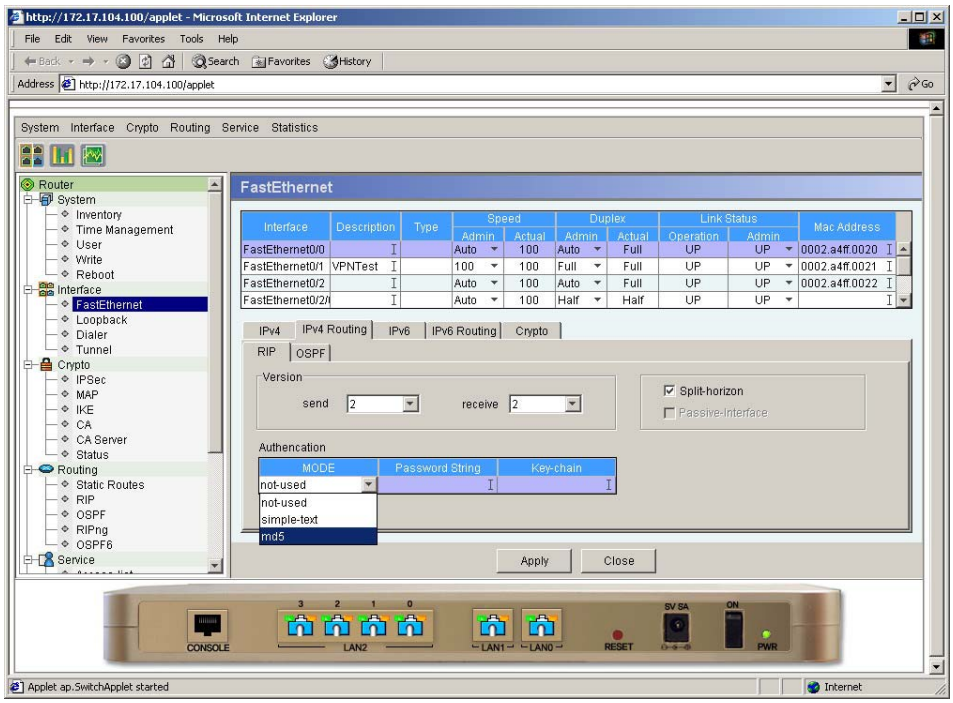
(Figure3-61) Select Fast Ethernet RIP Receive Version

Check Split-Horizon to prevent Loop phenomenon when RIP Routing.



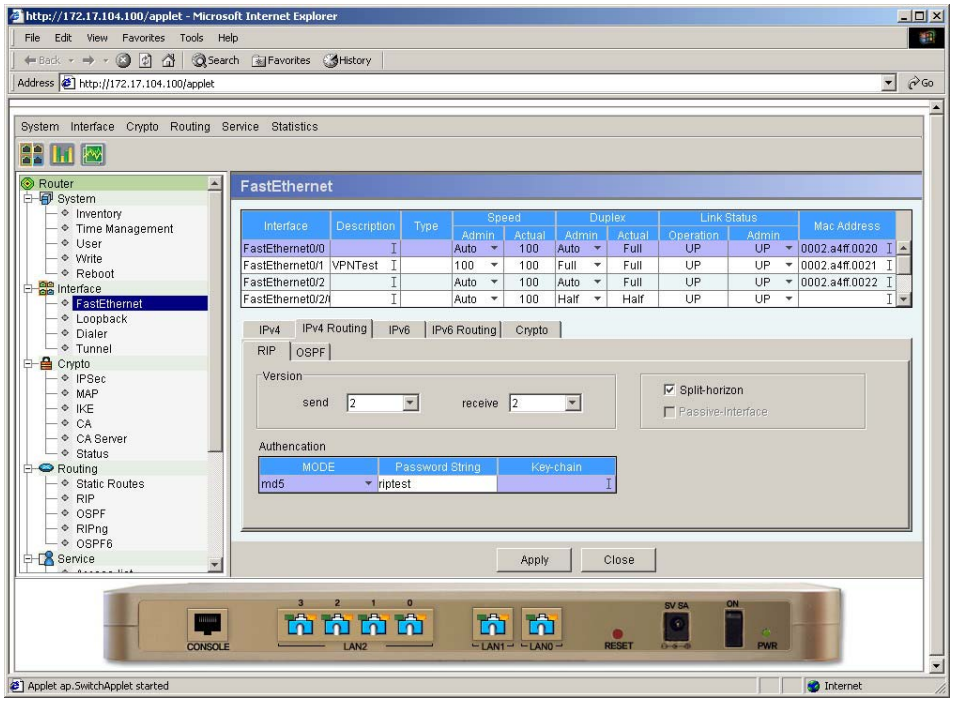
(Figure3-62) Select Fast Ethernet RIP Split-Horizon

Select MD5 for authentication when exchange Routing Table.



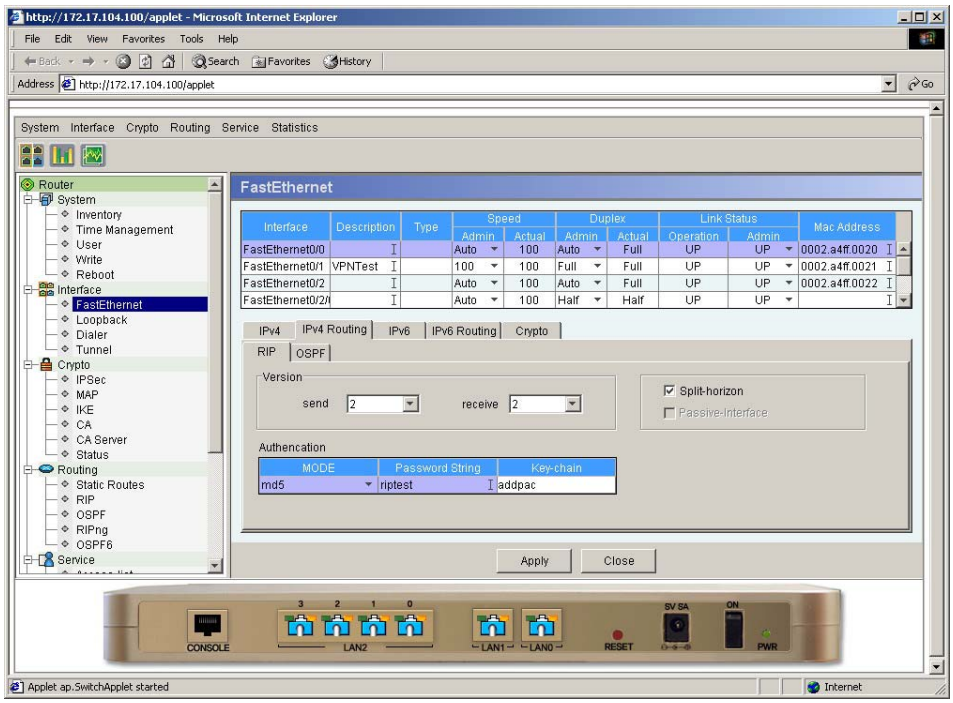
(Figure3-63) Select RIP Authentication Method

Input "riptest" for MD5 Password.



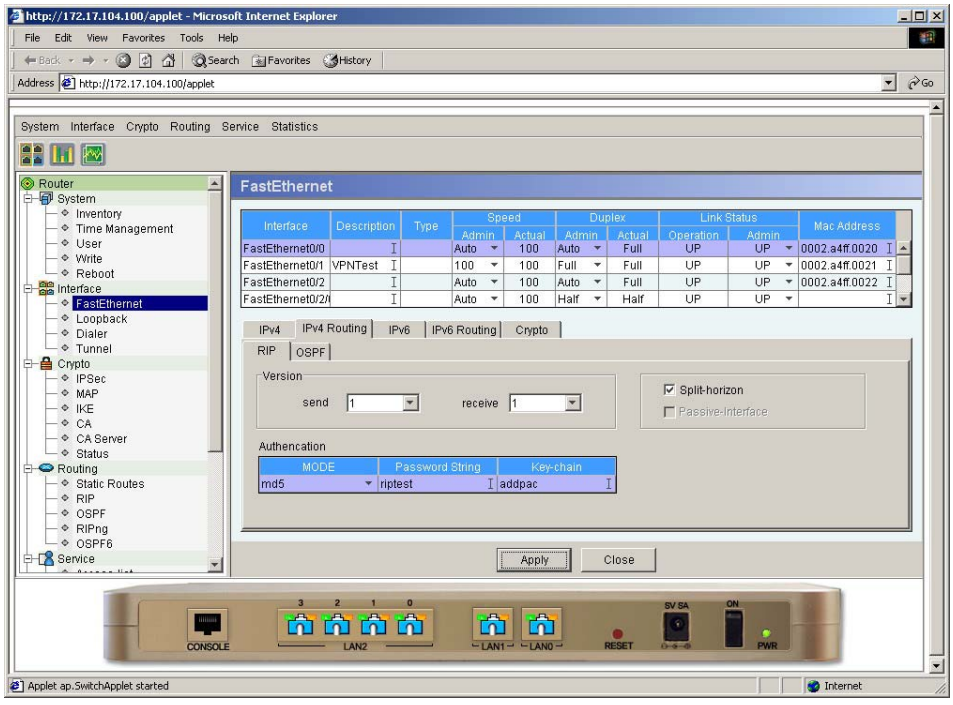
(Figure3-64) Input MD5 Password String

Input the key value "addpac" when using Password as MD5 algorithm.



(Figure3-65) Input MD5 KeyChain

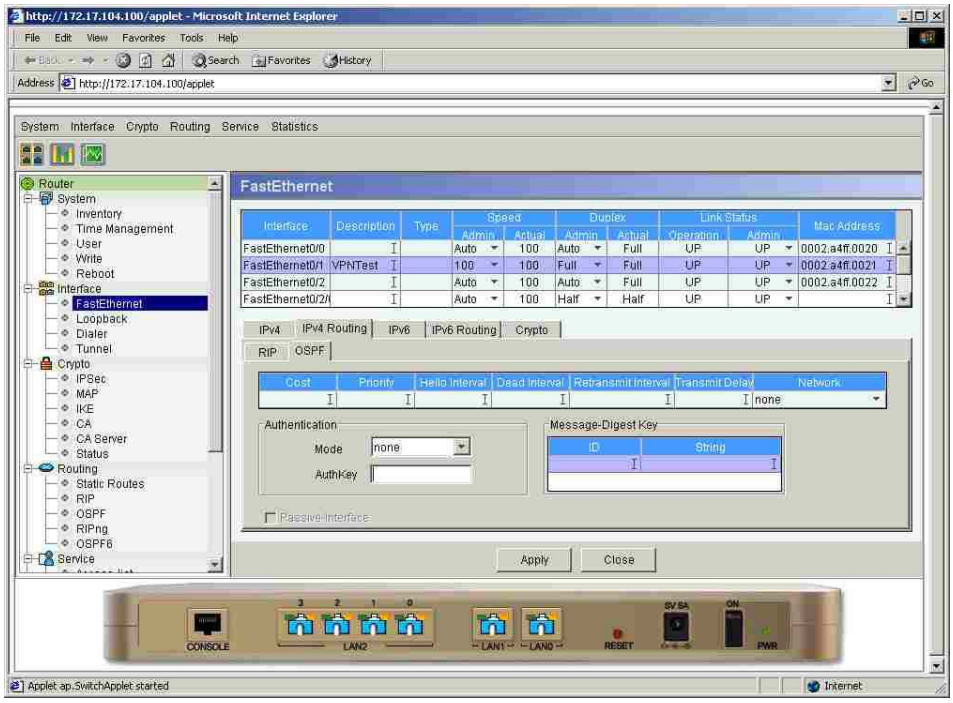
Click "Apply" to see



(Figure3-66) Check RIP configuration setting

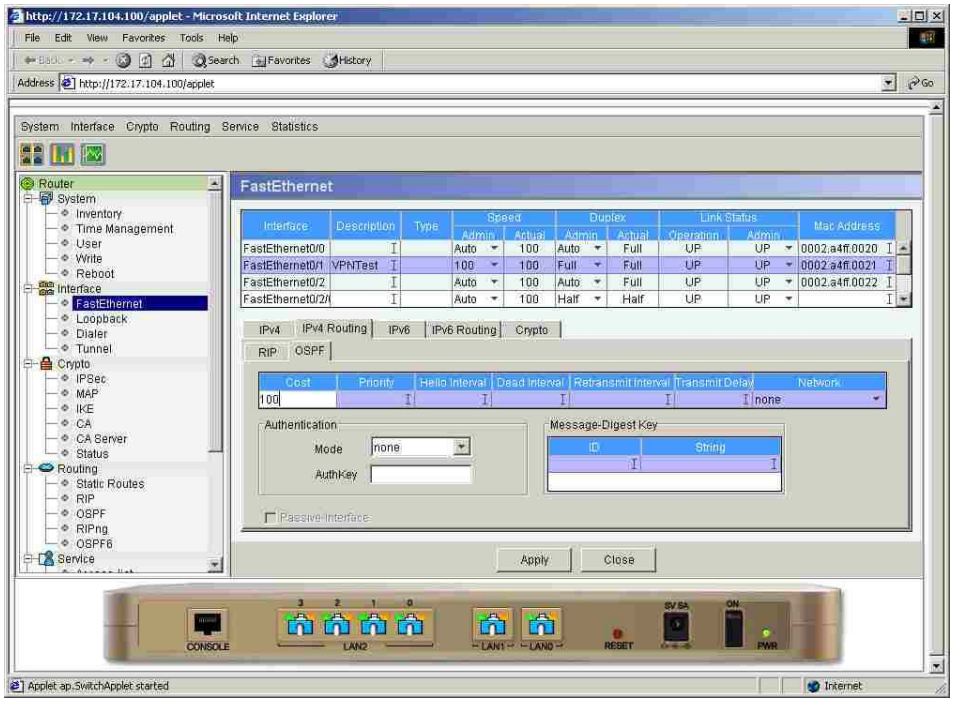
Figure 3-68 shows how to change configuration settings for OSPF of Fast Ethernet 0/1.

Select FastEthernet 0/1-> Select OSPF on IPv4 Routing.



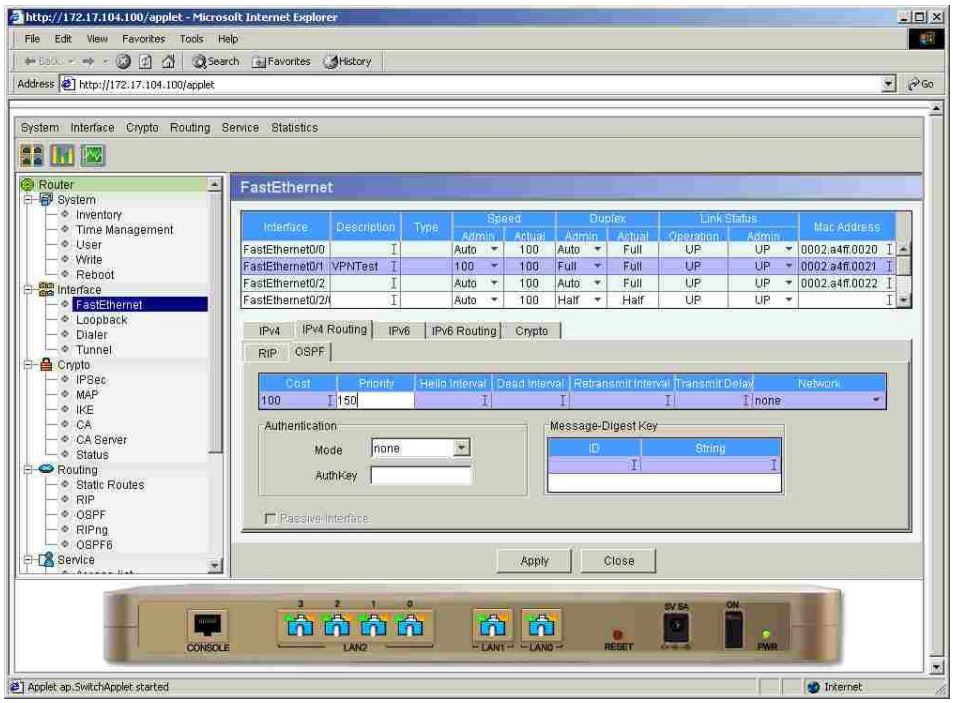
(Figure3-67) Select Fast Ethernet IPv4 Routing OSPF

Input Cost “100” of the Interface.



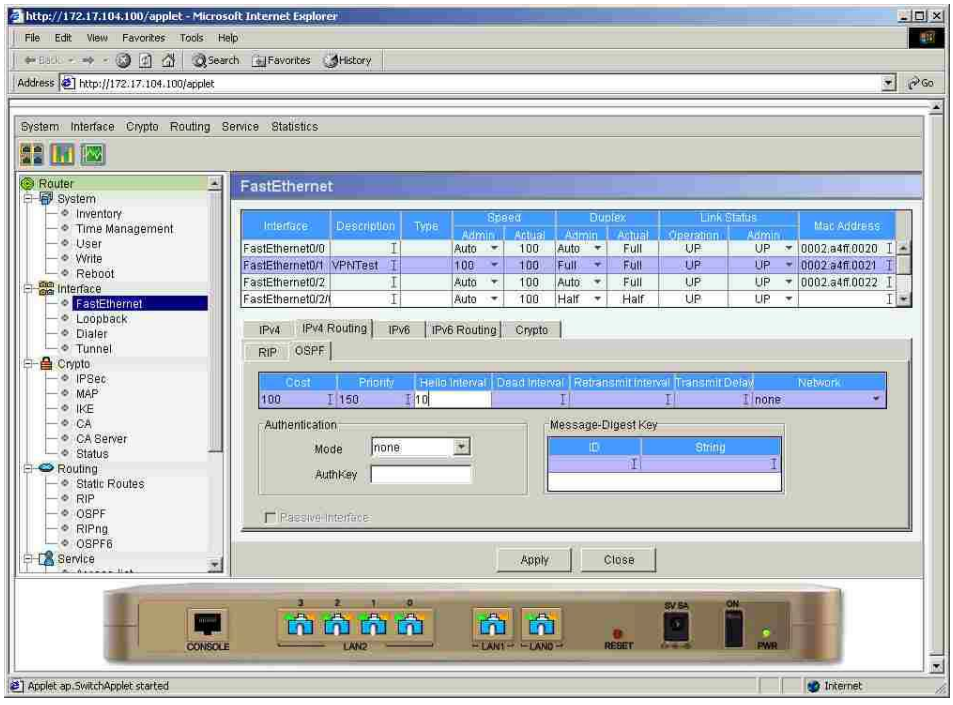
(Figure3-68) Input OSPF Interface Cost

Input Priority “150” to decide “Designed Router”



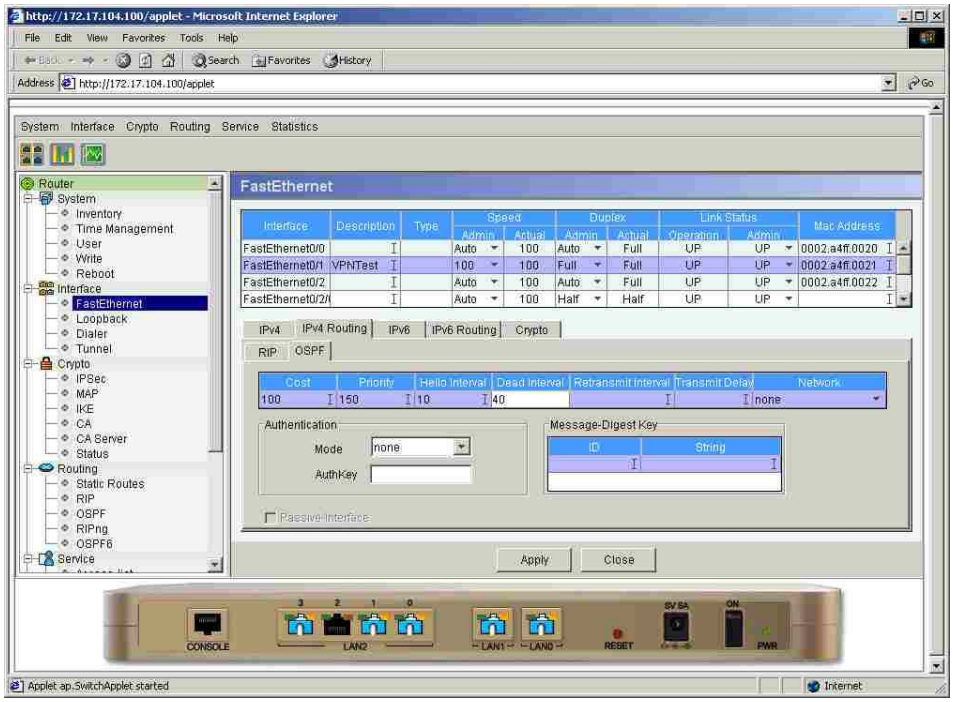
(Figure3-69) Input OSPF Interface Priority

Input “10” for OSPF Hello Packet transfer interval.



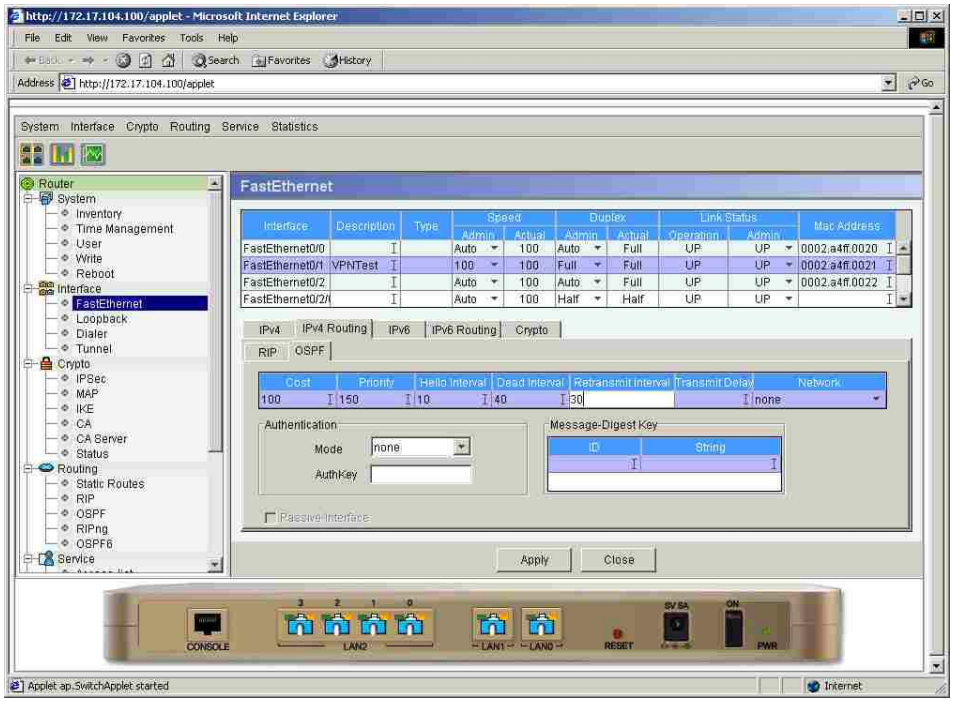
(Figure3-70) Input OSPF Hello Interval

Input “40” for Dead Interval of OSPF. Dead Interval is usually set 4 times more than Hello Interval.



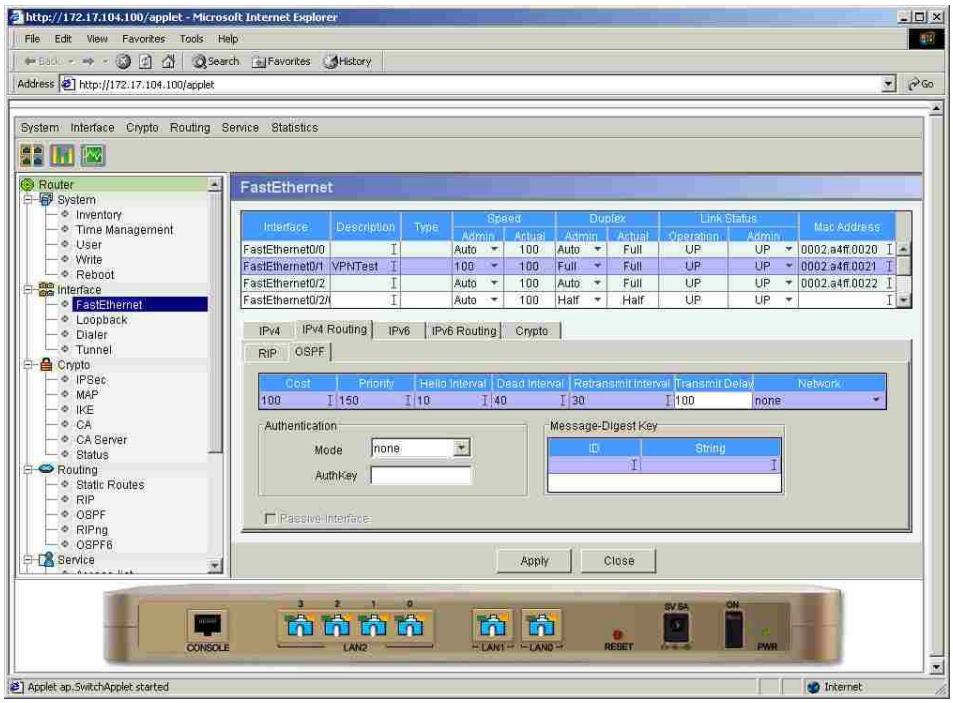
(Figure3-71) Input OSPF Dead Interval

Input “30” value for Retransmit Interval of Advertisement Packet.



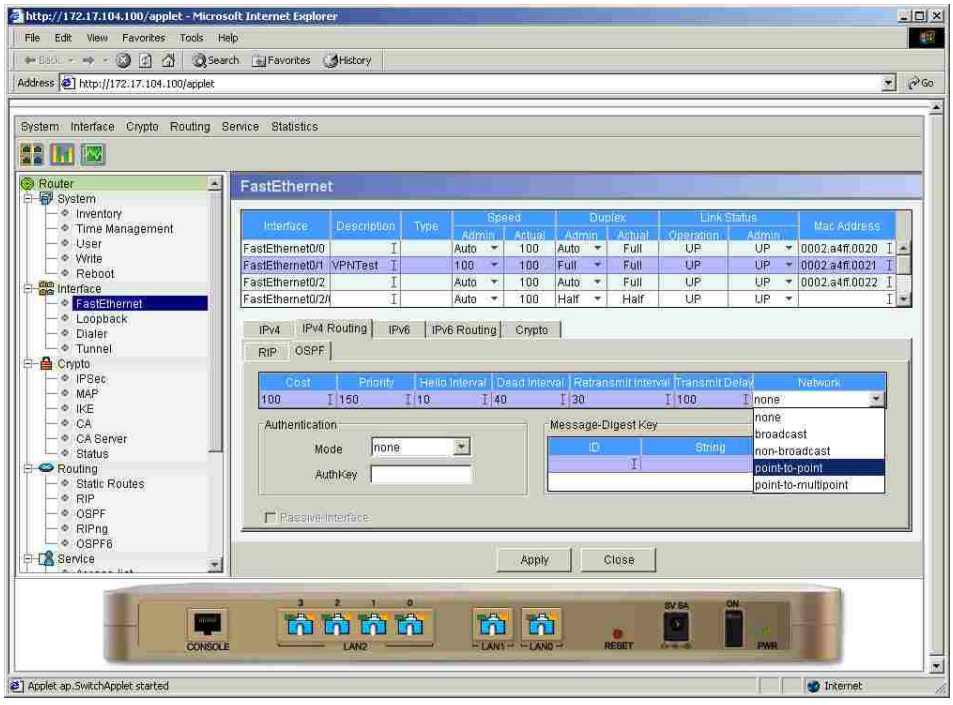
(Figure3-72) Input OSPF Retransmit Interval

Input “100” for Transmit Delay of Link State Packet.



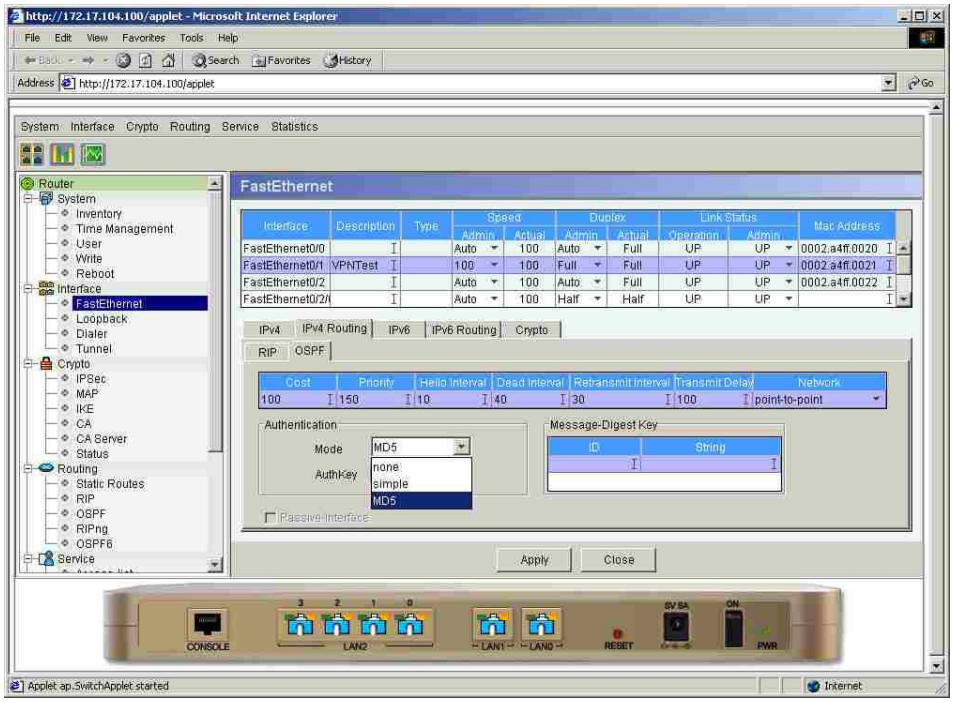
(Figure3-73) Input OSPF Transmit Delay

Select Network Type of Interface – “Point-to-Point”.



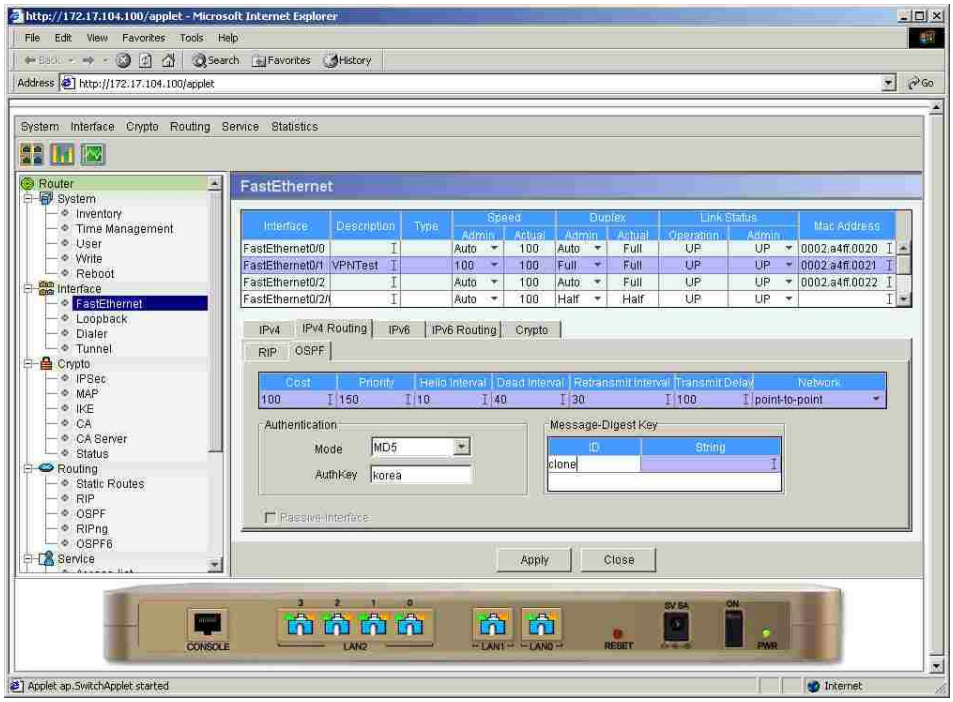
(Figure3-74) Select OSPF Network Type

Select Authentication method for exchanging Routing Table. It is “MD5” in below Figure.



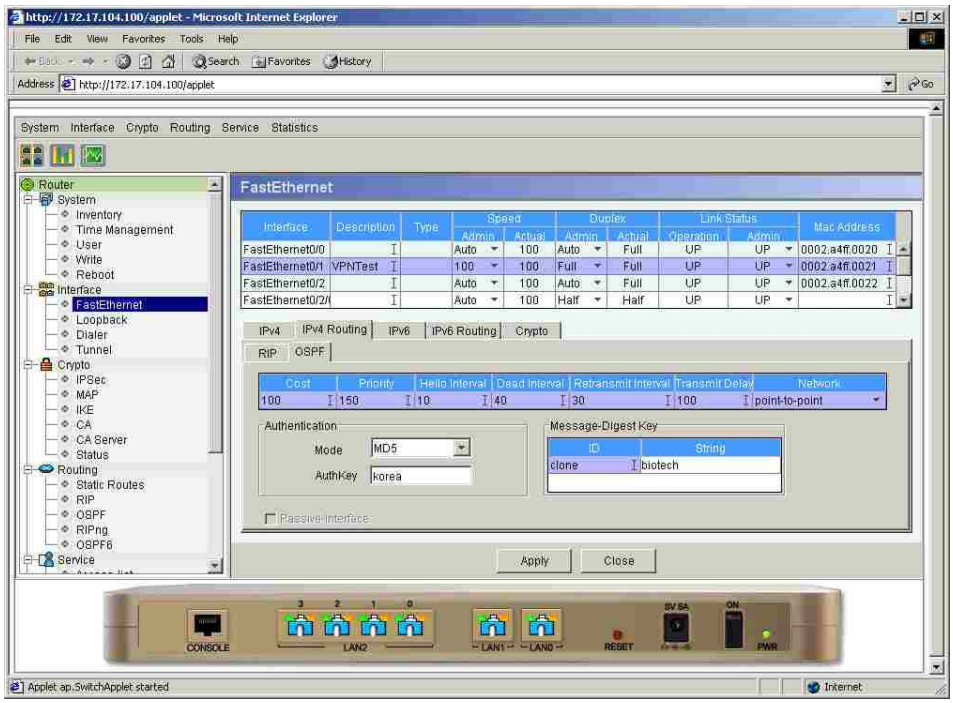
(Figure3-75) Select OSPF Authentication Method

Input ID value for MD5 authentication. Auth-Key is used for SimpleText authentication.



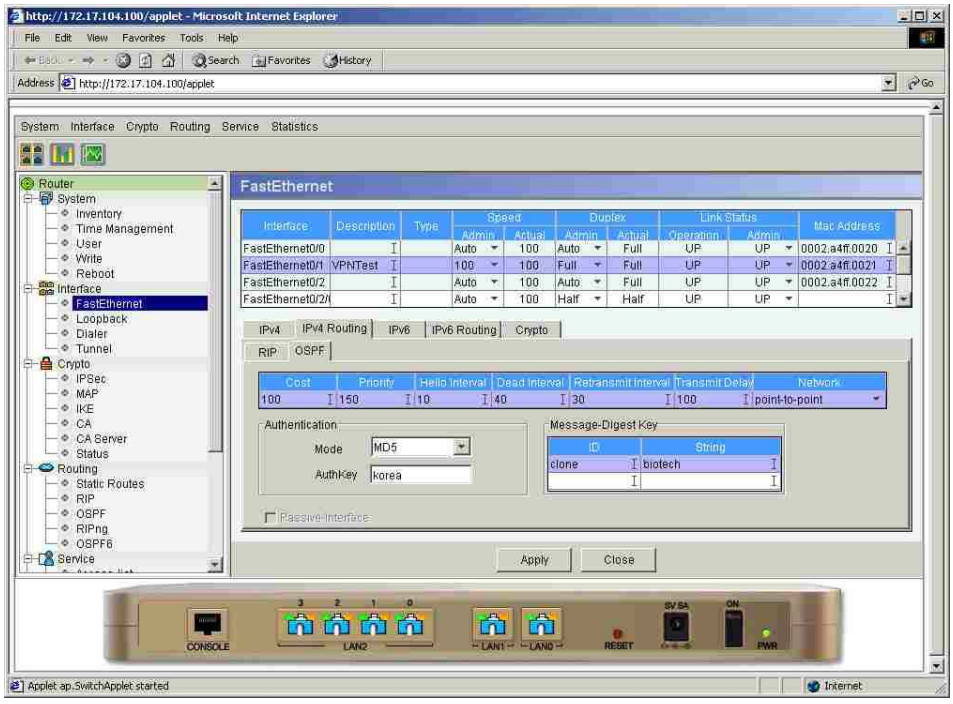
(Figure3-76) Input Message Digest Key ID

Input the password for MD5 authentication in the String field.



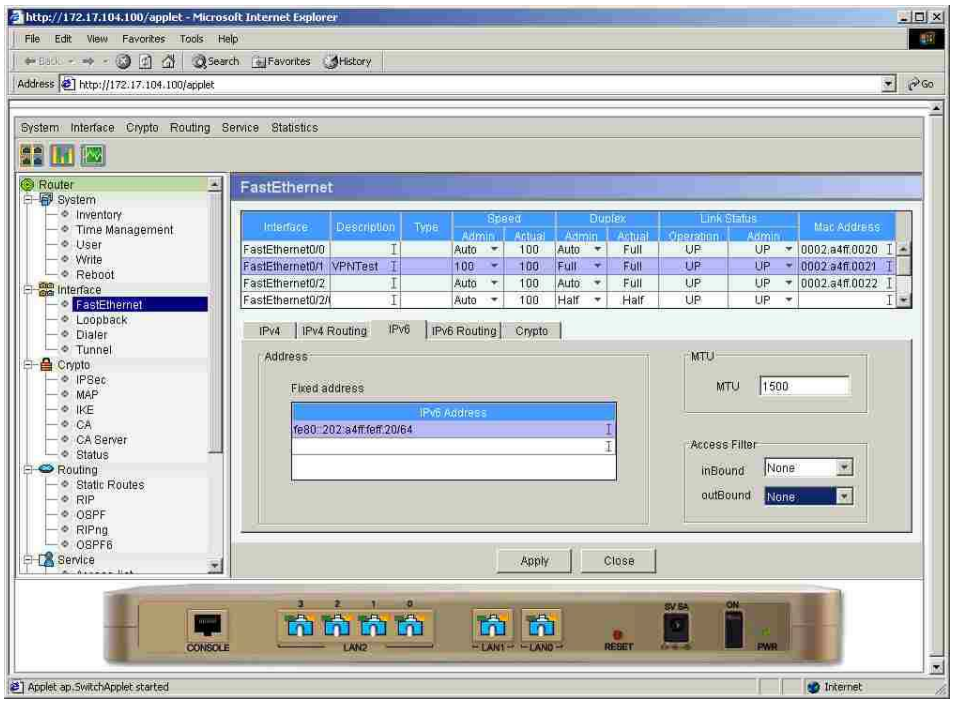
(Figure3-77) Input Message Digest Password

Click “Apply” to verify.



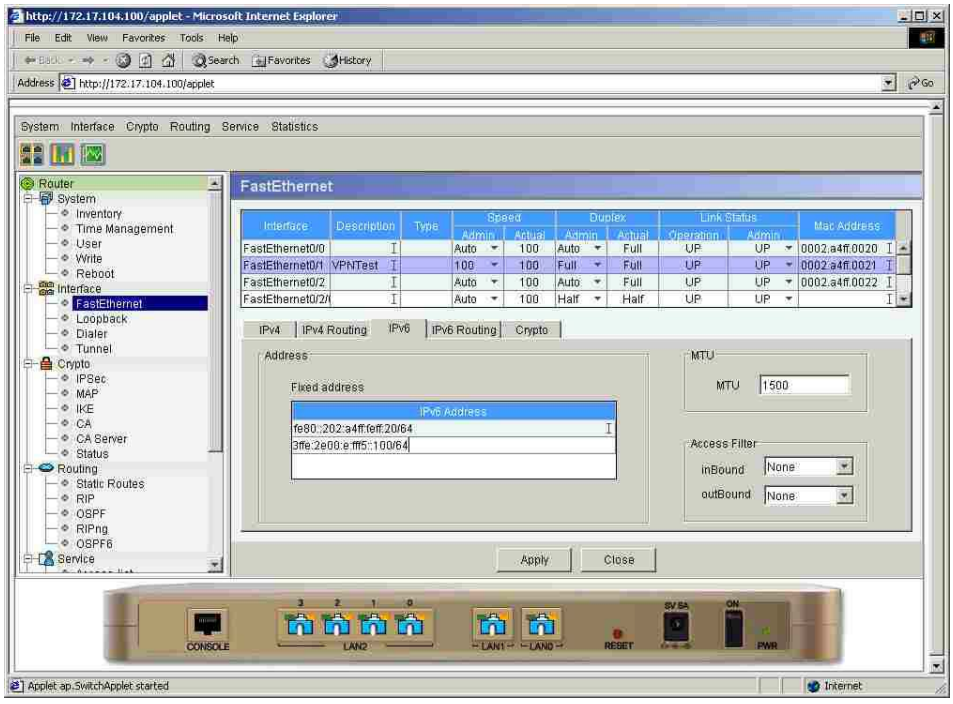
(Figure3-78) OSPF configuration setting verify

Figure 3-80 shows how to input IPv6 Address on Fast Ethernet 0/1.



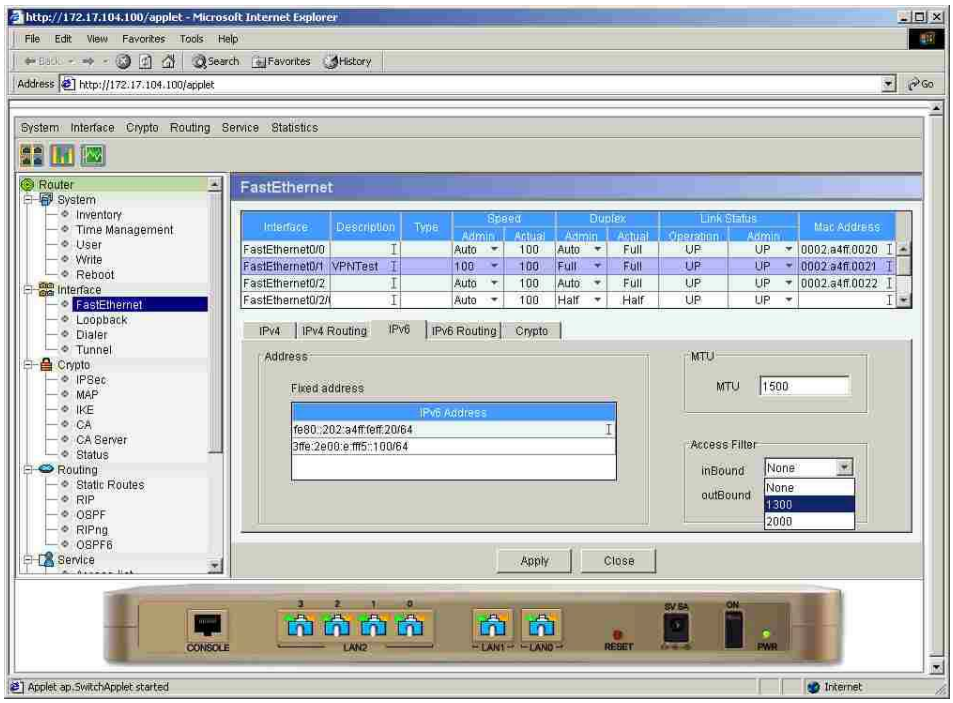
(Figure3-79) Select Fast Ethernet IPv6

Input the new IPv6 Address “3ffe:2e00:e:fff5::100/64”.



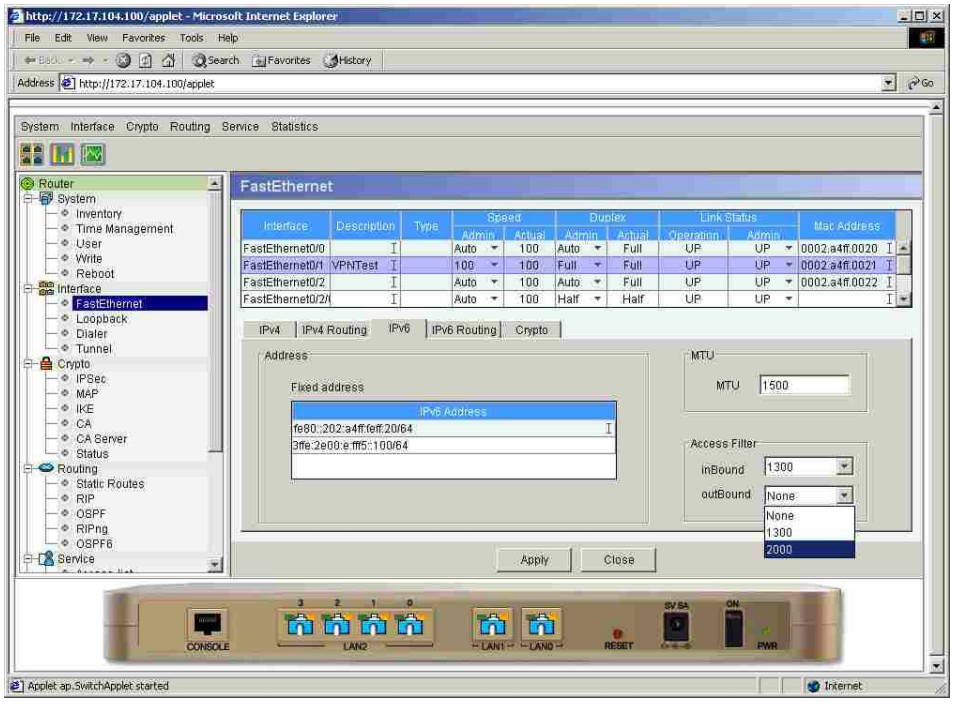
(Figure3-80) Input IPv6 Address

Select “Access-List 1300” in Access Filter Inbound.



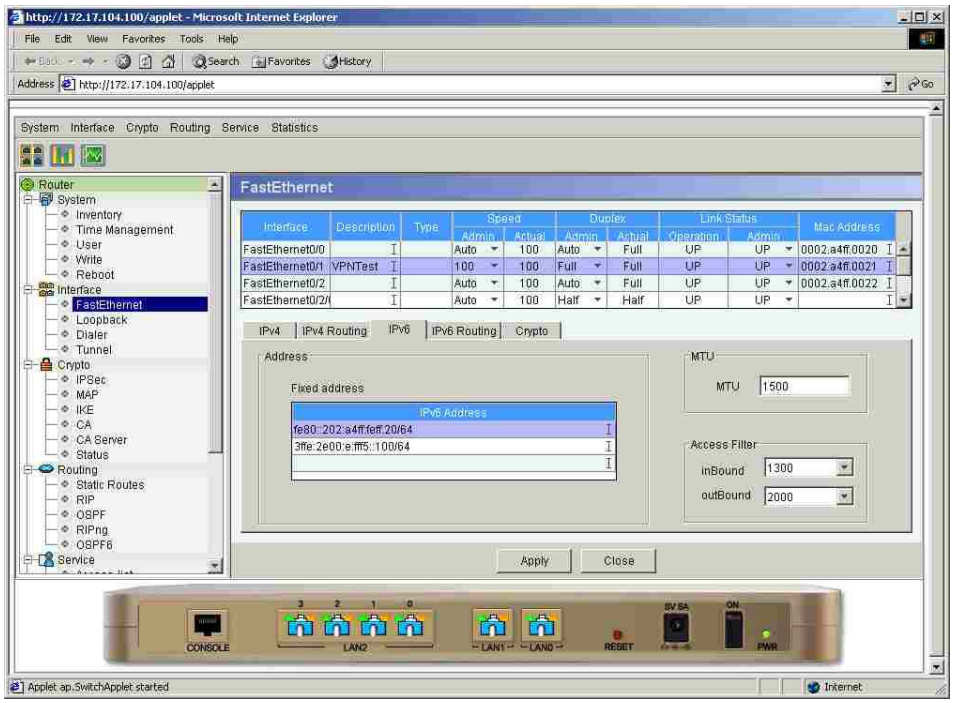
(Figure3-81) Select IPv6 Access Filter Inbound

Select “Access-List 2000” in Access Filter outbound Access Filter.



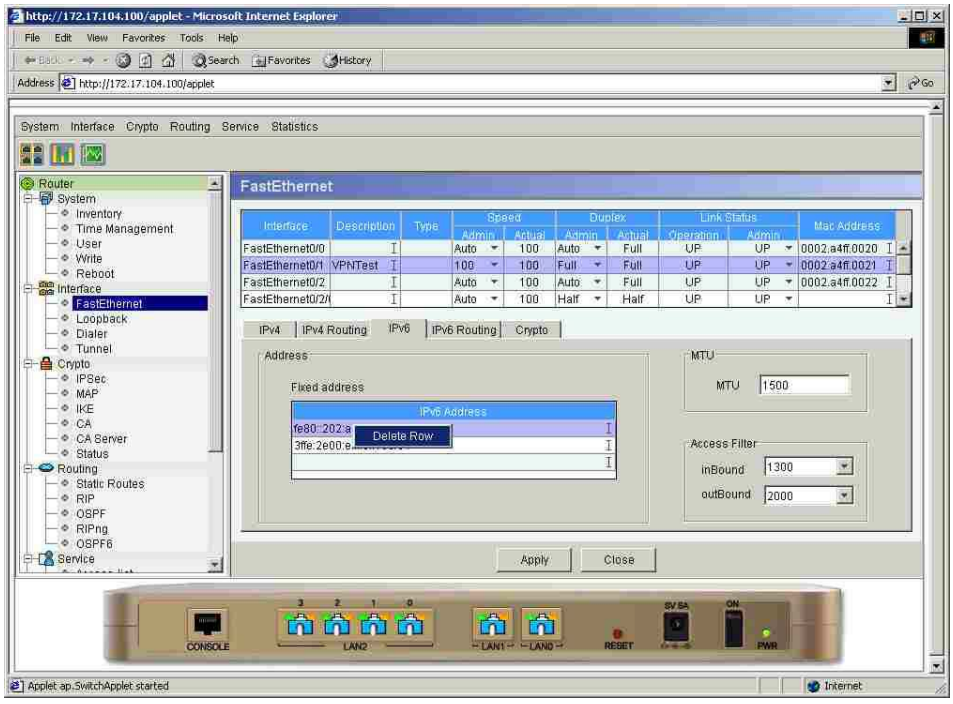
(Figure3-82) Select IPv6 Access Filter Outbound

Click “Apply” to verify



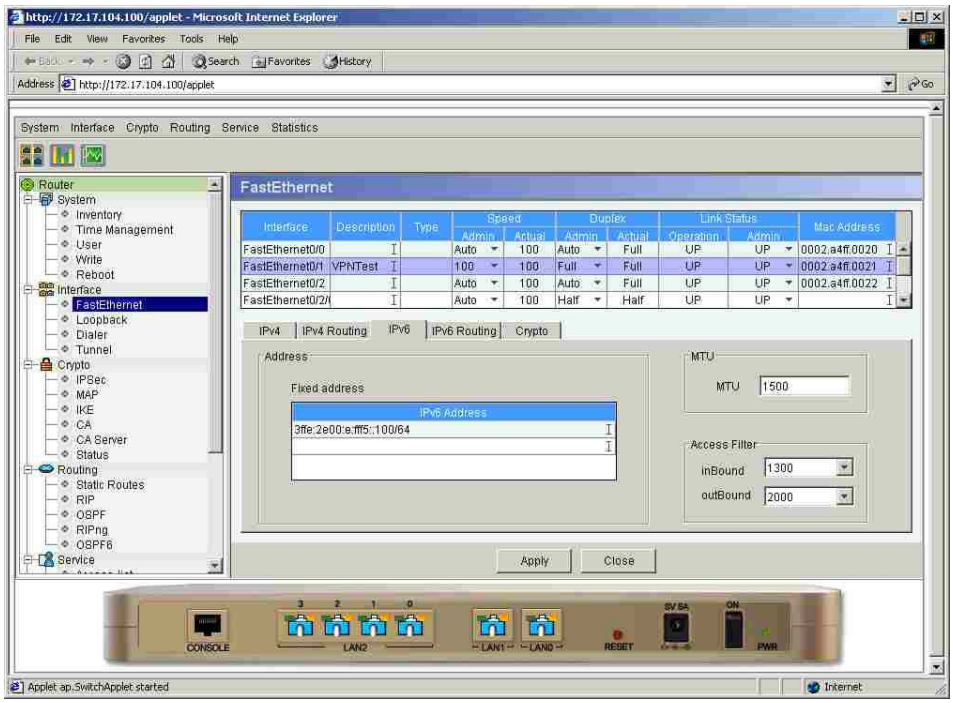
(Figure3-83) Adding IPv6 Address & Access Filter verify

To delete IPv6 Address, Select IPv6 Address-> Select “Delete Row” by clicking right side of mouse.



(Figure3-84) Delete IPv6 Address

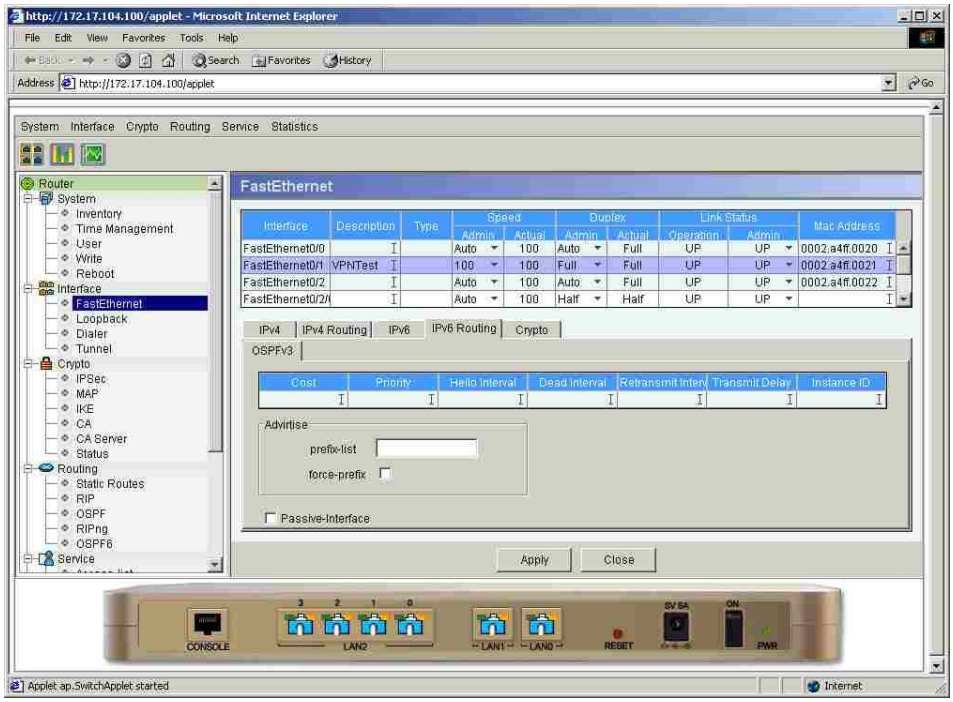
Click “Apply” to verify



(Figure3-85) Verifying IPv6 Address delete

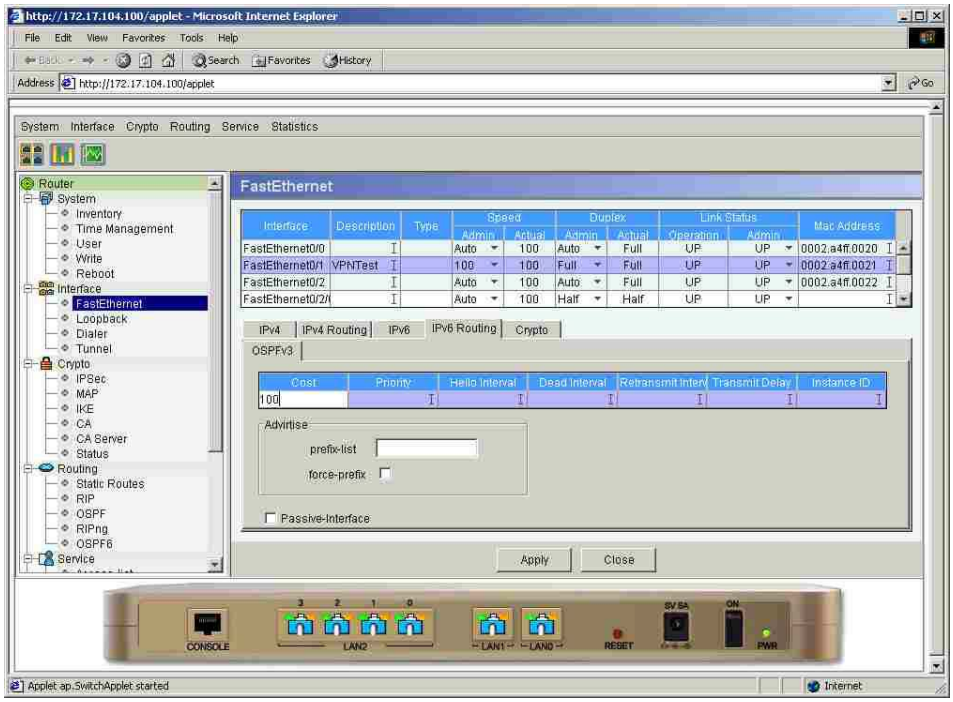
Figure 3-87 shows how to configure IPv6 Routing Protocol, OSPFv3.

Select "OSPFv3" of IPv6 Routing.



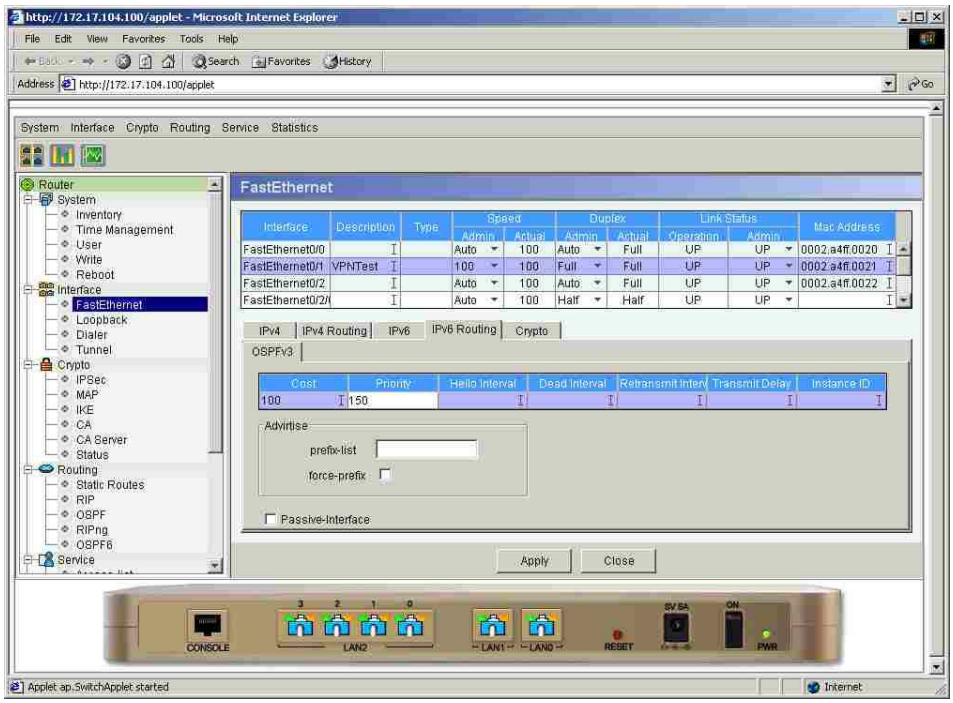
(Figure3-86) Select IPv6 OSPFv3

Input "100" for OSPFv3 Cost



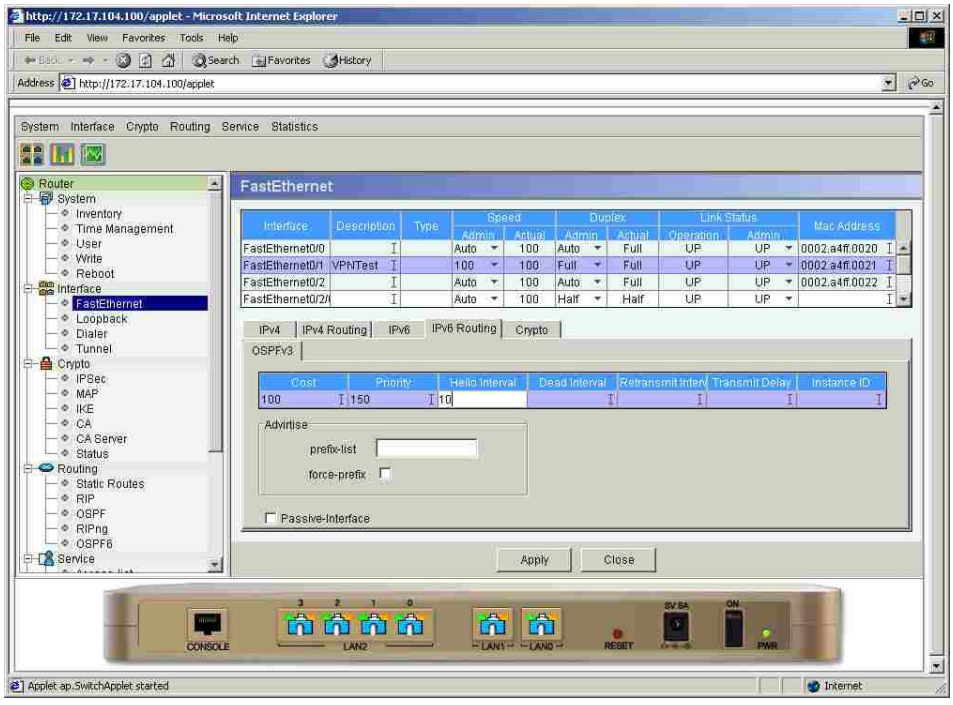
(Figure3-87) Input OSPFv3 Cost

Input “150” for OSPFv3 Interface Priority



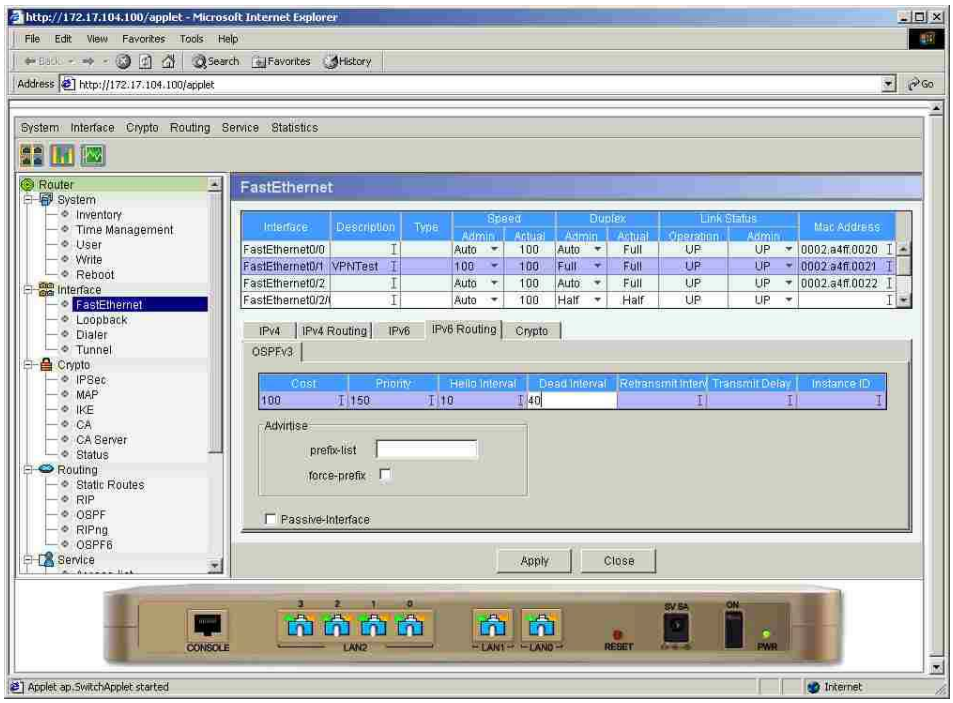
(Figure3-88) Input OSPFv3 Interface Priority

Input “10” for OSPFv3 Hello Packet transmit interval.



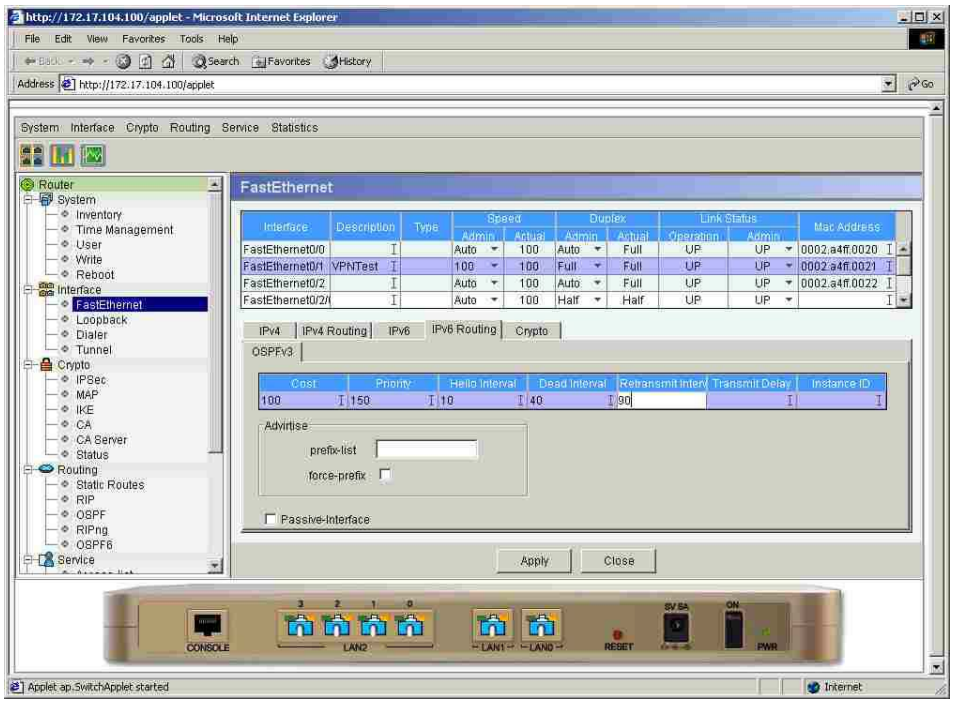
(Figure3-89) Input OSPFv3 Hello Interval

Input “40” for OSPFv3 Dead Interval parameter.



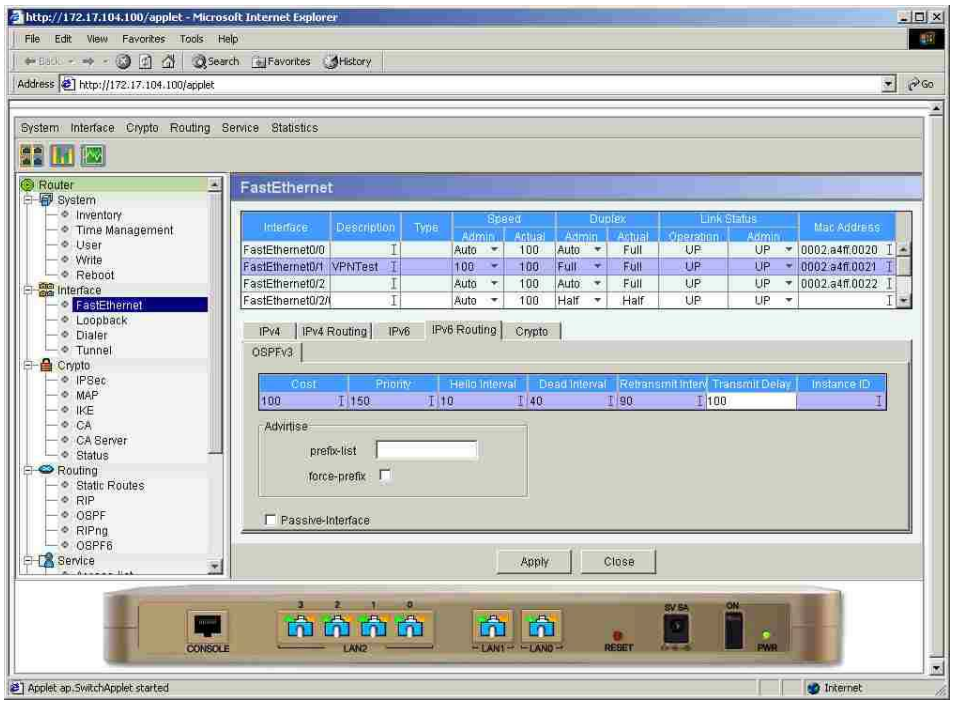
(Figure3-90) Input OSPFv3 Dead Interval

Input “90” for Advertisement Packet Retransmit interval parameter.



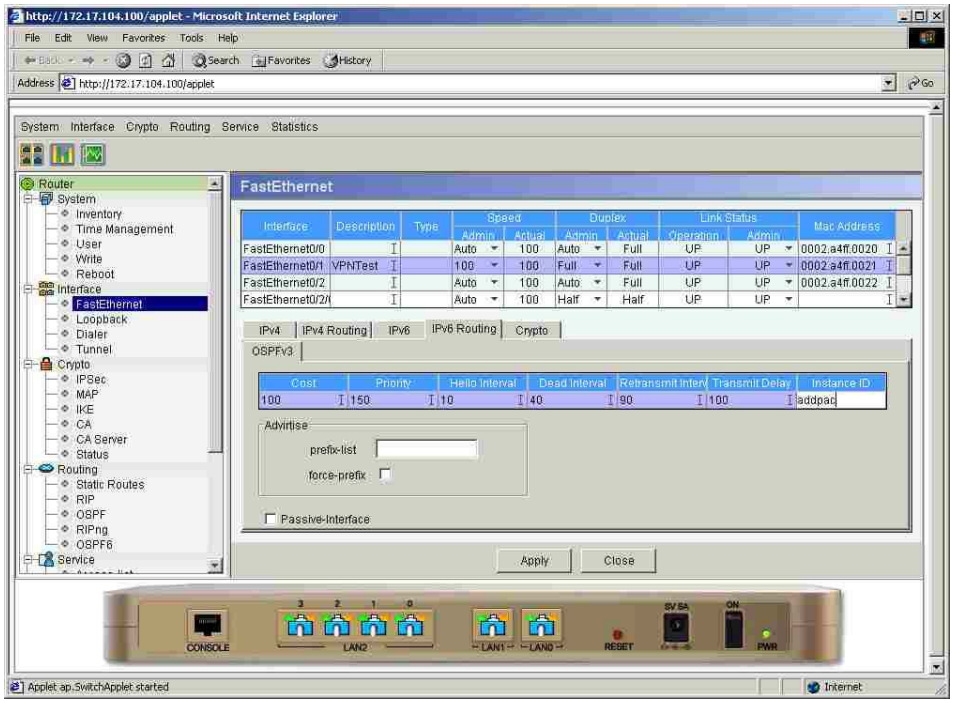
(Figure3-91) Input OSPFv3 Retransmit Interval

Input “100” for Transmit Delay of Link State Packet.



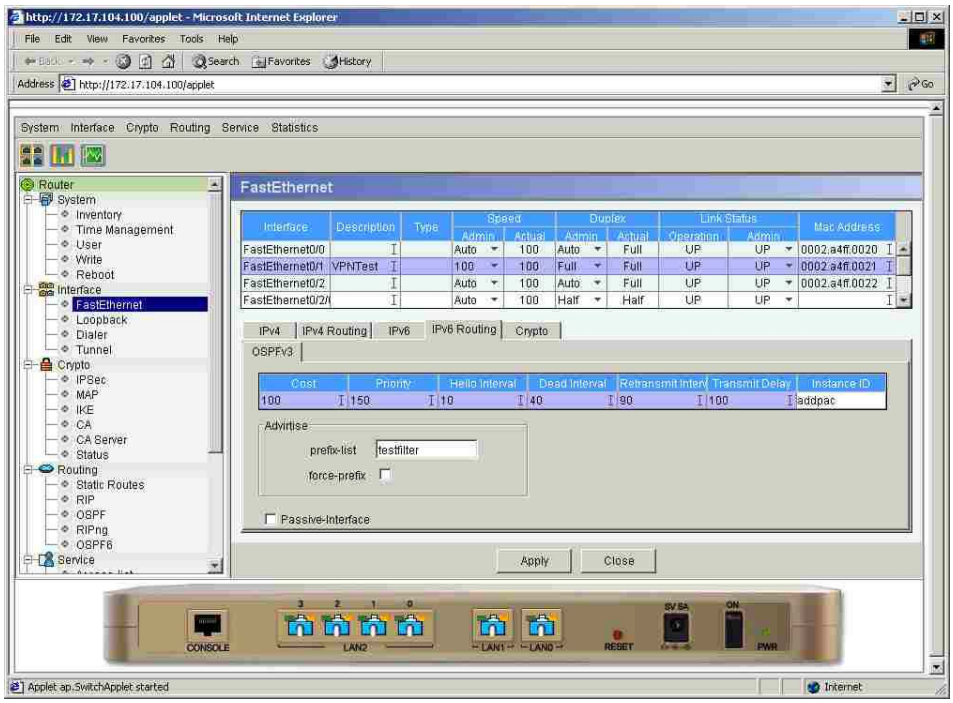
(Figure3-92) Input OSPFv3 Transmit Delay

Input “addpac” for OSPFv3 Instance ID parameter.



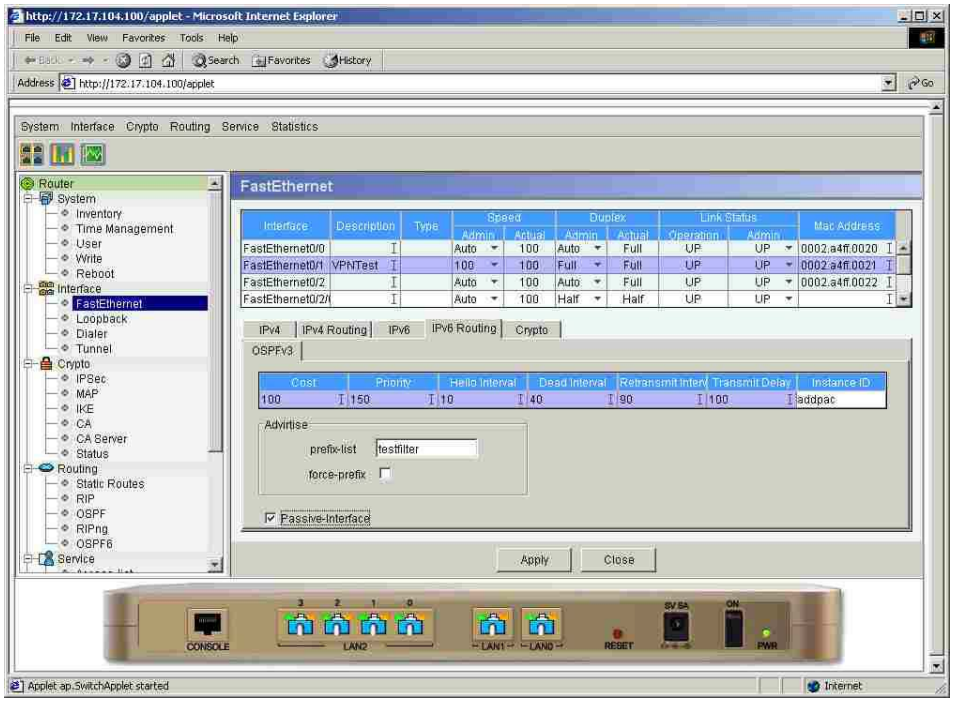
(Figure3-93) Input OSPFv3 Instance ID

Input Prefix-List “testfilter” to filter information of specific network.



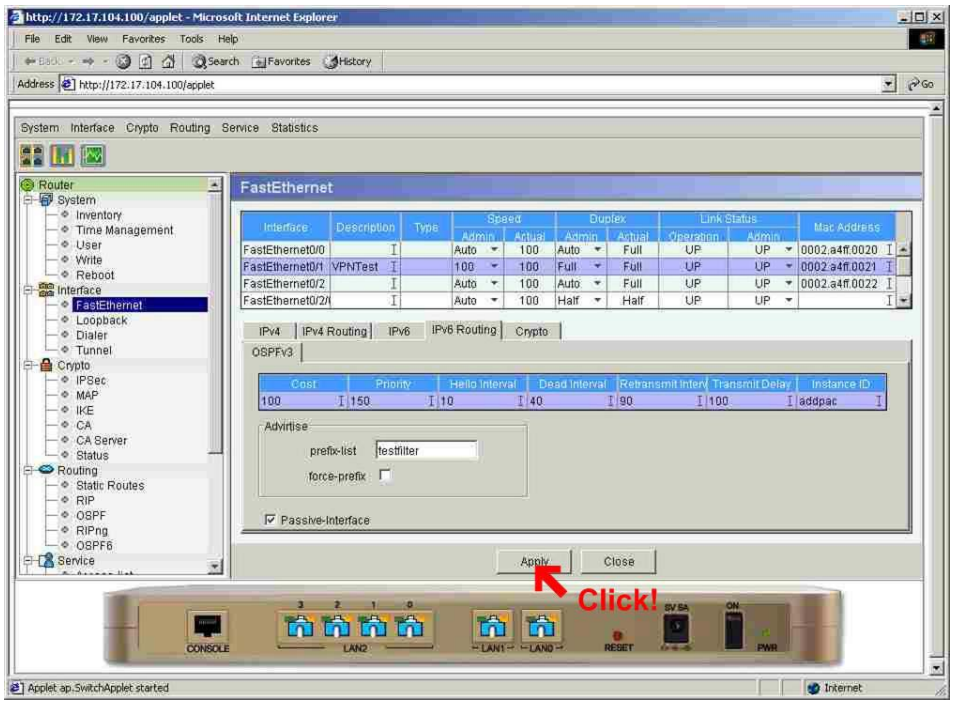
(Figure3-94) Input OSPFv3 Prefix-List

Check Passive-Interface to only receive OSPFv3 Routing Table



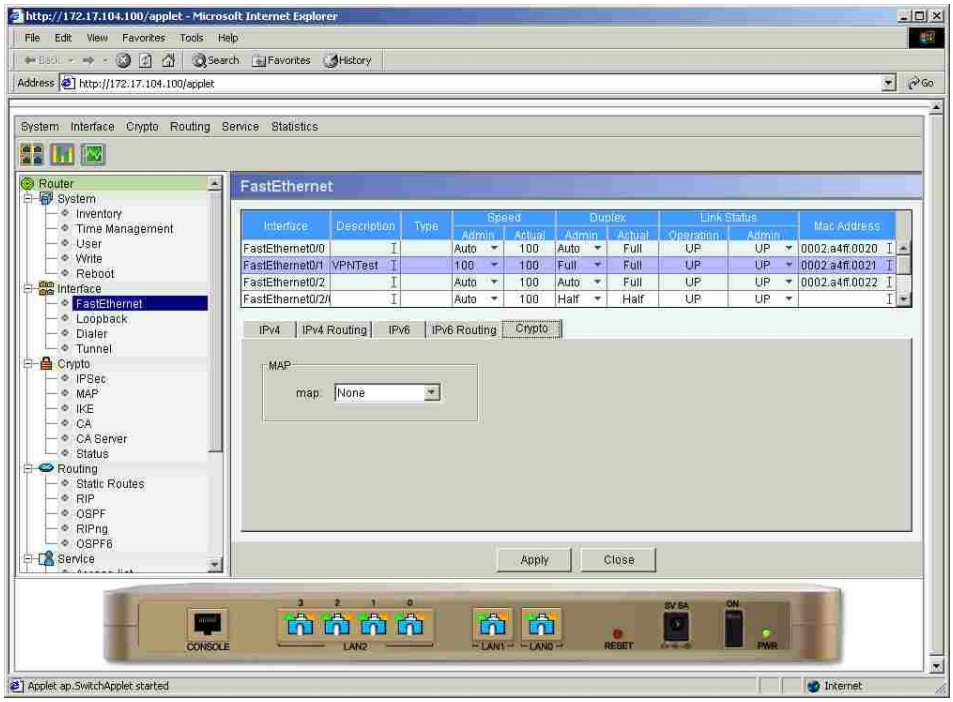
(Figure3-95) OSPFv3 Passive Interface check

Click “Apply” to verify



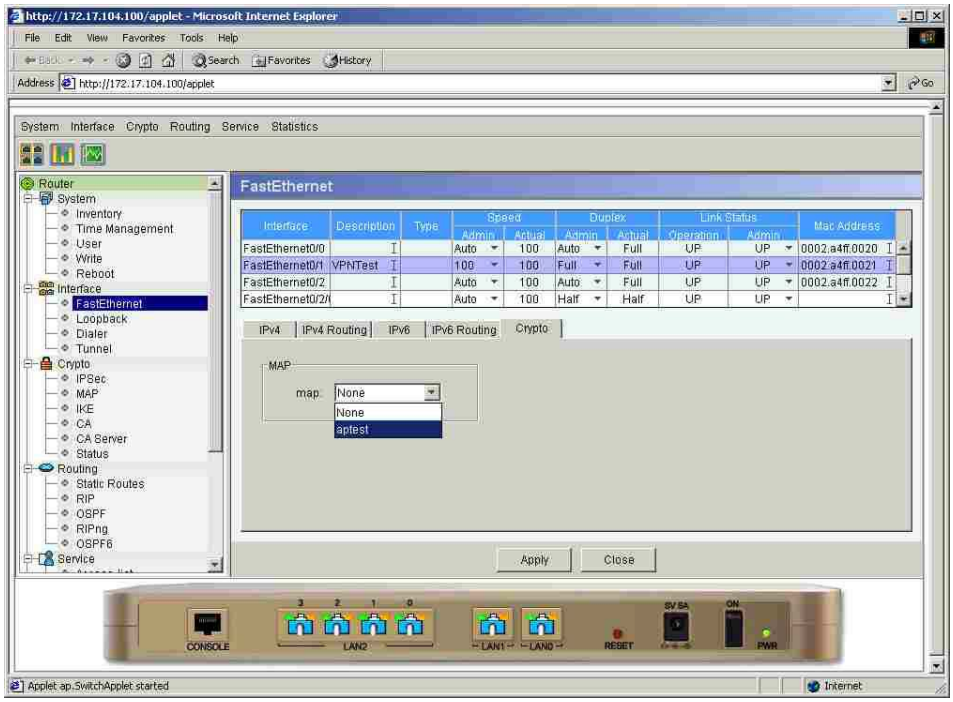
(Figure3-96) Verify OSPFv3 settings

Figure 3-98 shows the example of applying Crypto Map to Fast Ethernet 0/1. The user has to select pre-created Map from Crypto menu.



(Figure3-97) Select Fast Ethernet Crypto

Select Map "aptest"



(Figure3-98) Select Fast Ethernet Crypto Map

Click “Apply” to verify.

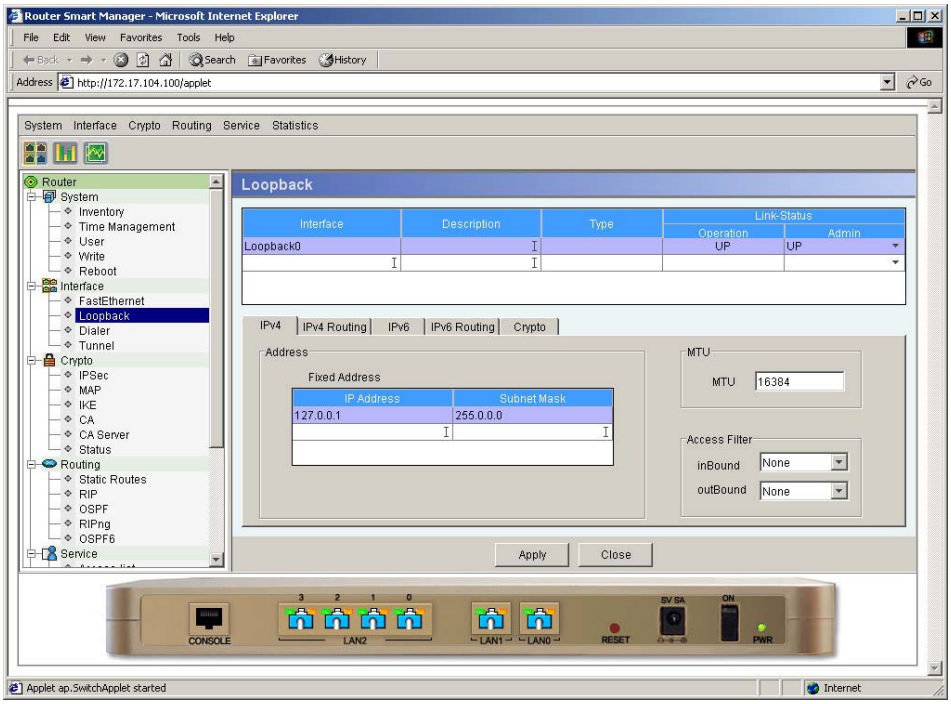


(Figure3-99) Verify Interface Crypto Map

Loopback

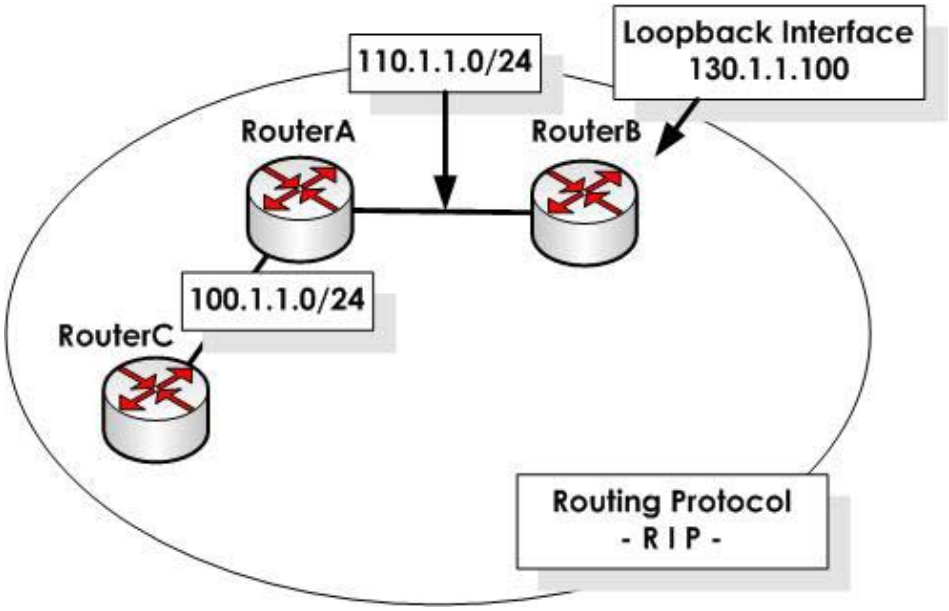
Loopback Interface is not physical Interface. It is logical interface placed inside of Gateway. Therefore, it is unable to have direct communication with other hosts using physical interface. To communicate with other hosts, Routing Protocols such as Static Routing, RIP are necessary for packets exchange. Generally, Loopback Interface is used for testing Routing Protocols.

Figure 3-101 shows the initial page of Loopback



(Figure3-100) Loopback initial page

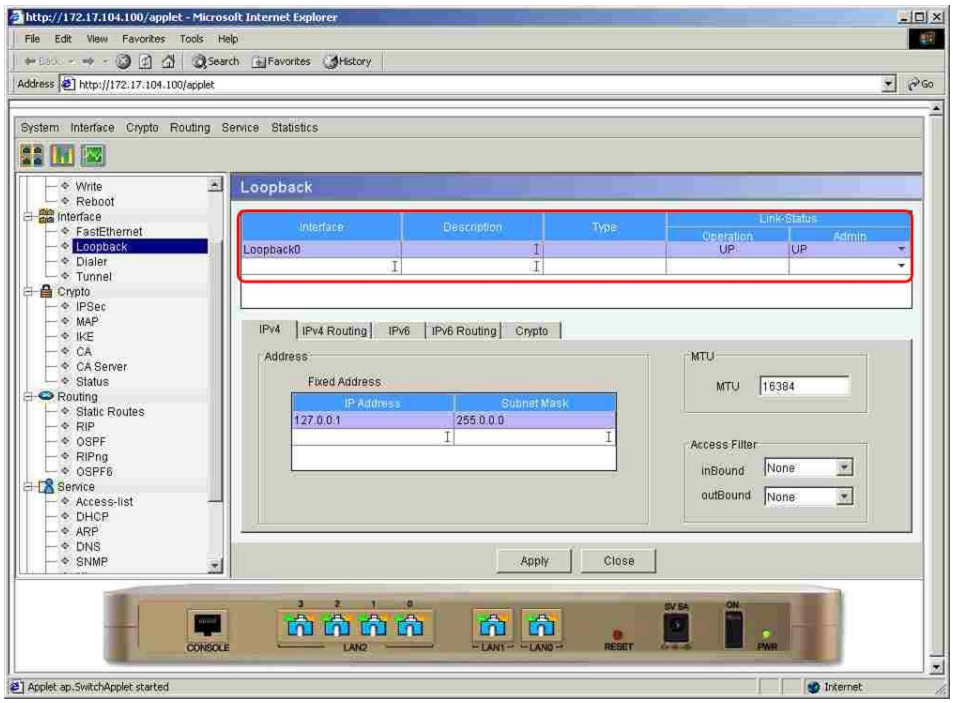
Figure 3-102 shows the network which includes Loopback Interface and uses RIP as Routing Protocol.



(Figure3-101) Network (including Loopback Interface) Example

RouterC has information on “100.1.1.0” Network, RouterA has info on “100.1.1.0”, “110.1.1.0” Network, and RouterB has info on “110.1.1.0”, “130.1.1.0” Network. Once RIP is started, Router A, B, C shares information on every network. Loopback Interface is not physically exists however, network can be configured using interfaces inside of the router. Also there is no physical Link Up/Down in Loopback Interface so it is easier to test Routing Protocol or Routing performance without configuring complicating network diagram.

Figure 3-103 shows Loopback Interface menu.

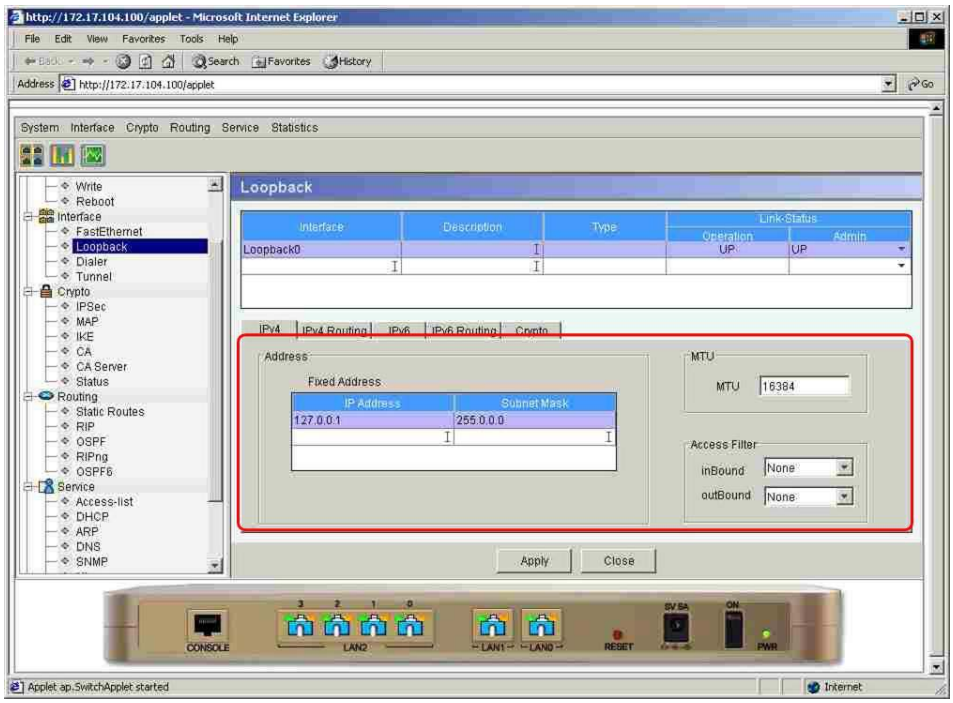


(Figure3-102) Loopback Interface page

<Table 3-15> Loopback Interface Description

Elements	Description
Interface	It is a Loopback Interface. The user can create total 32 of Loopback Interface.
Description	Comments Field
Type	Interface Type
Link Status	Link Status of Loopback Interface & shutdown

Figure 3-104 shows Loopback Interface, IPv4 menu



(Figure3-103) Loopback IPv4 Main page

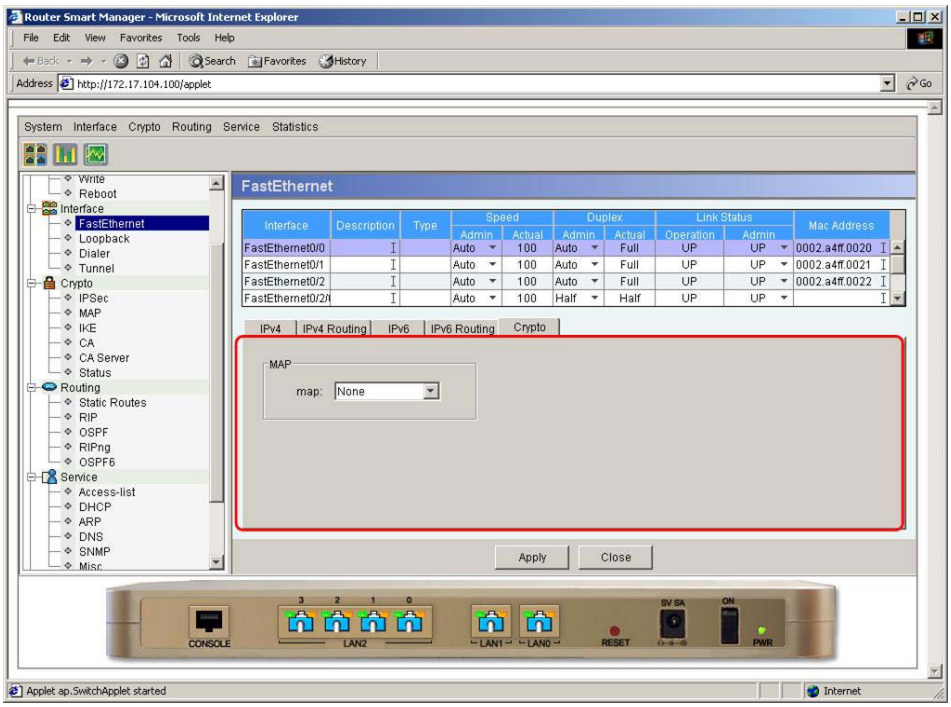
<Table 3-16> Loopback IPv4 Description

Elements	Description
IP Address	IP Address of Loopback Interface
Subnet Mask	Subnet Mask for appropriate IP Address of Loopback Interface
MTU	Maximum Transmission Unit. Default value is 16384 Bytes.
Access Filter InBound	To apply Access-List. Access Filter Inbound is used for filtering received packets.
Access Filter OutBound	To apply Access-List. Access Filter Outbound is used for filtering sending packets.

IPv4, IPv6, IPv4 and IPv6 Routing Protocol menu of Loopback Interface is the same as menu in FastEthernet. Please refer to FastEthernet menu description.

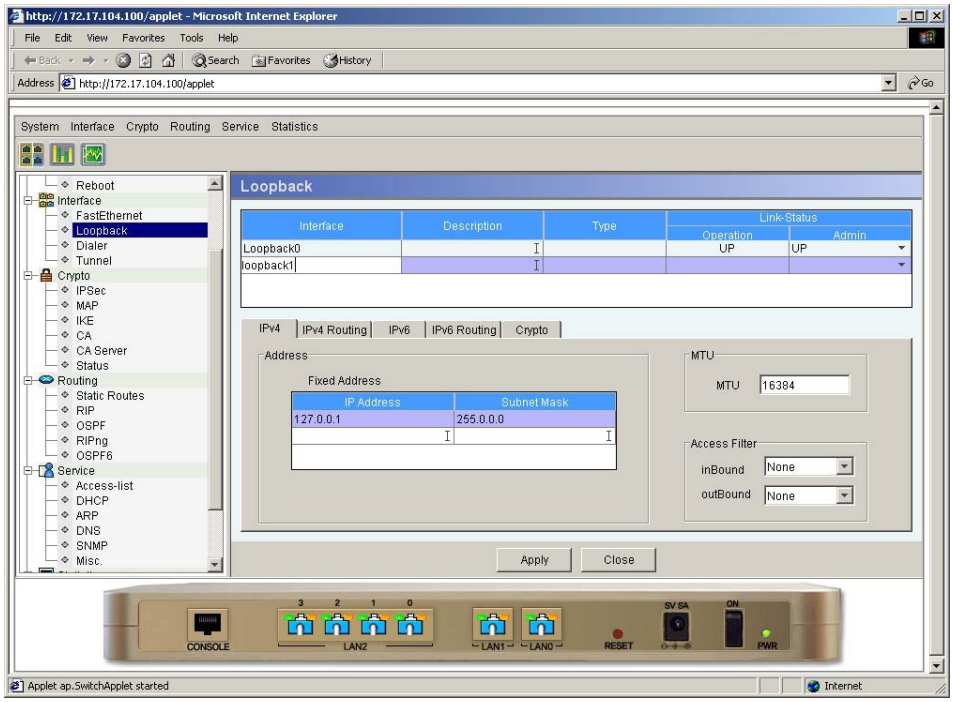
Figure 3-105 shows Crypto Info of Loopback Interface.

Crypto Map form Crypto Menu is applied to a specific Interface. Select a Map using scroll bar.



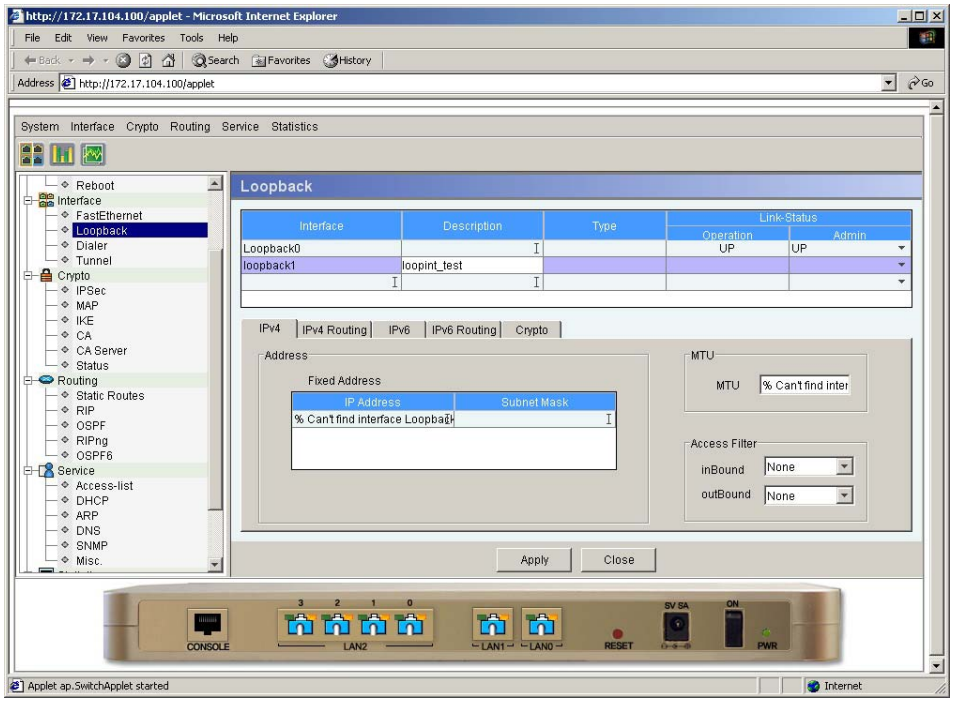
(Figure3-104) Loopback Interface Crypto Info

Figure 3-106 shows how to add Loopback1 Interface for IPv4 and IPv6 Address. Select Loopback Interface1 with a mouse.



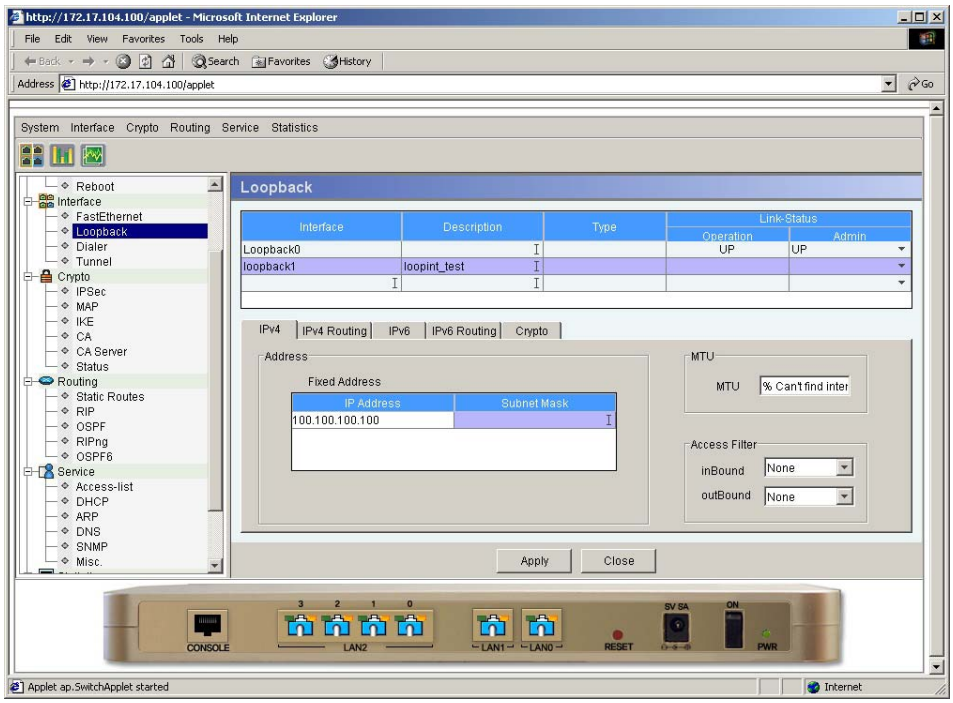
(Figure3-105) Add Loopback1 Interface

Brief comment on Loopback1 Interface.



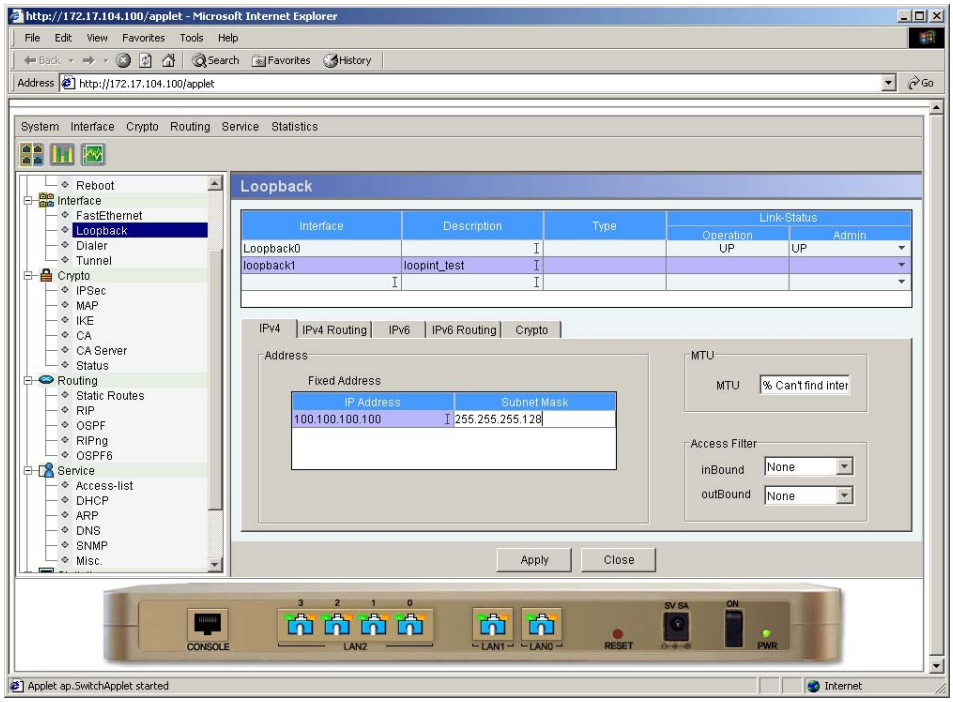
(Figure3-106) Input Loopback1 Interface Description

Input “100.100.100.100” IP Address for IPv4.



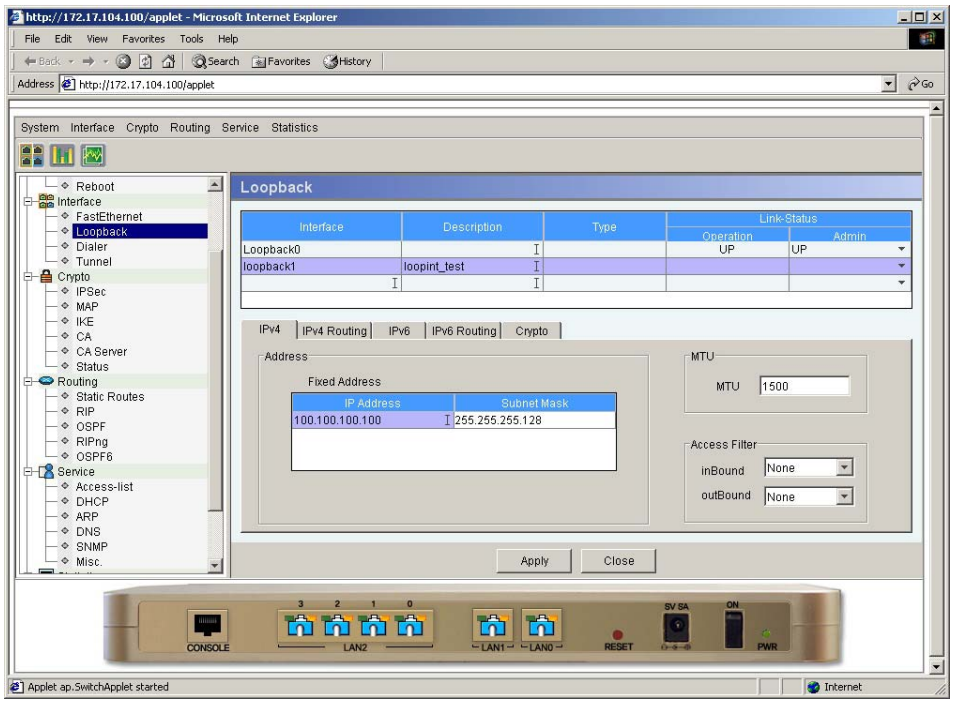
(Figure3-107) Input IPv4 Address

Input “255.255.255.128” Subnet Mask for the IP Address.



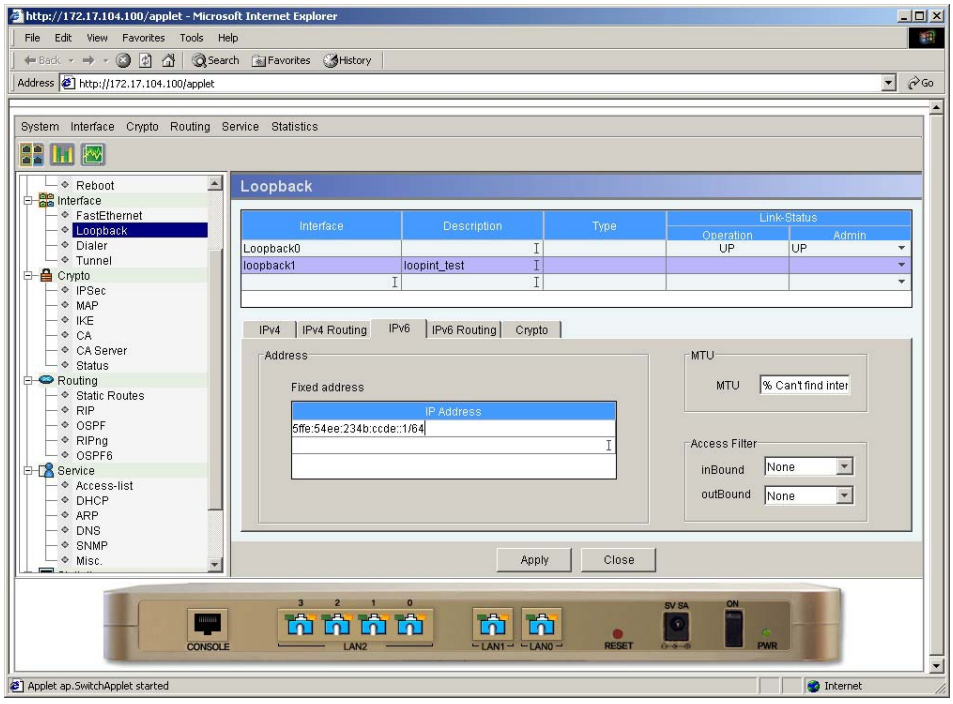
(Figure3-108) Input Subnet Mask of IPv4 Address

Input “1500” for MTU value.



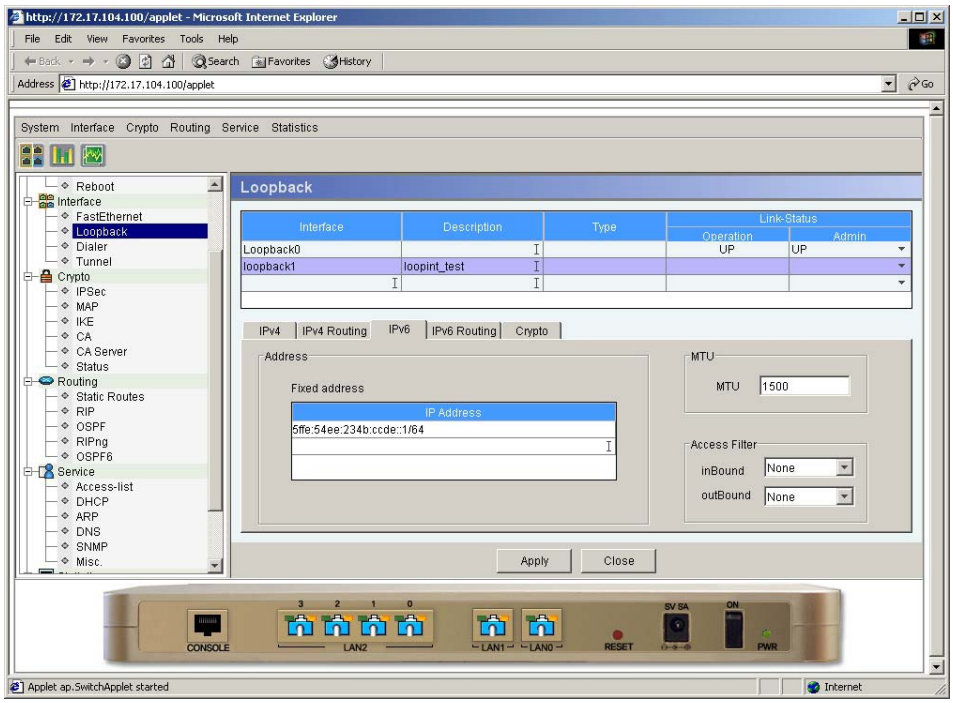
(Figure3-109) Input IPv4 MTU

Move to IPv6 then, input IPv6 Address.



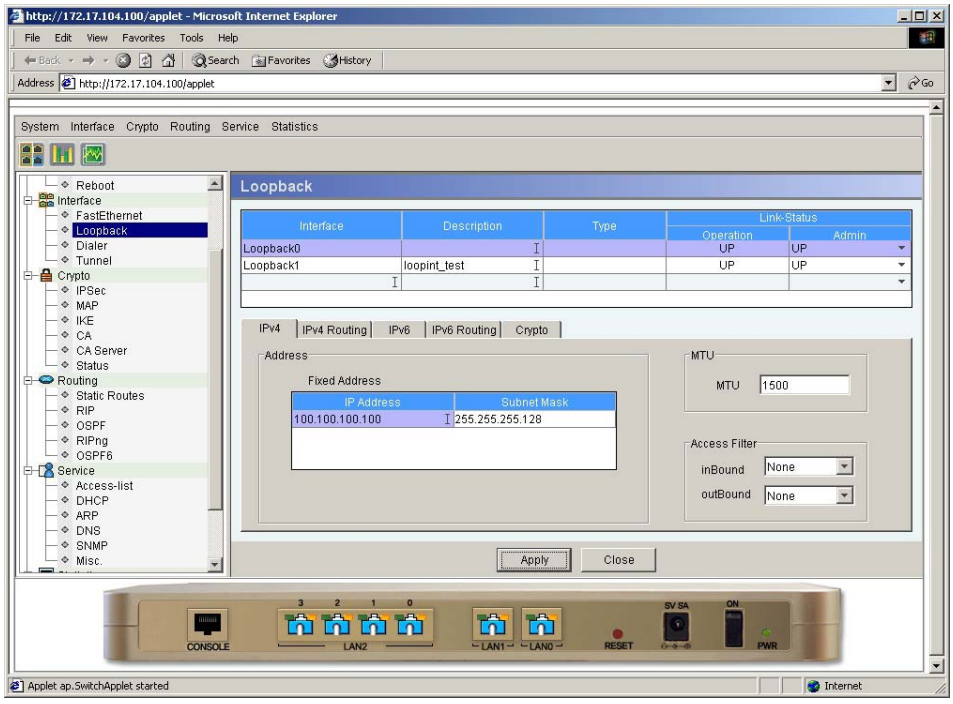
(Figure3-110) Input IPv6 Address

Input “1500” for MTU value.



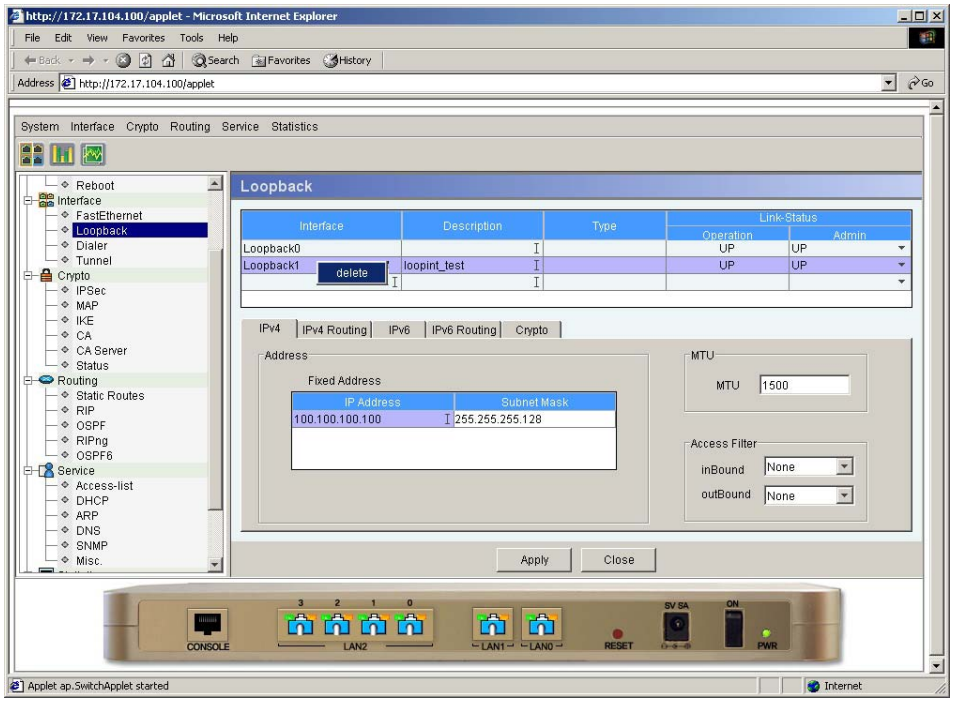
(Figure3-111) Input IPv6 MTU

Click “Apply” to verify.



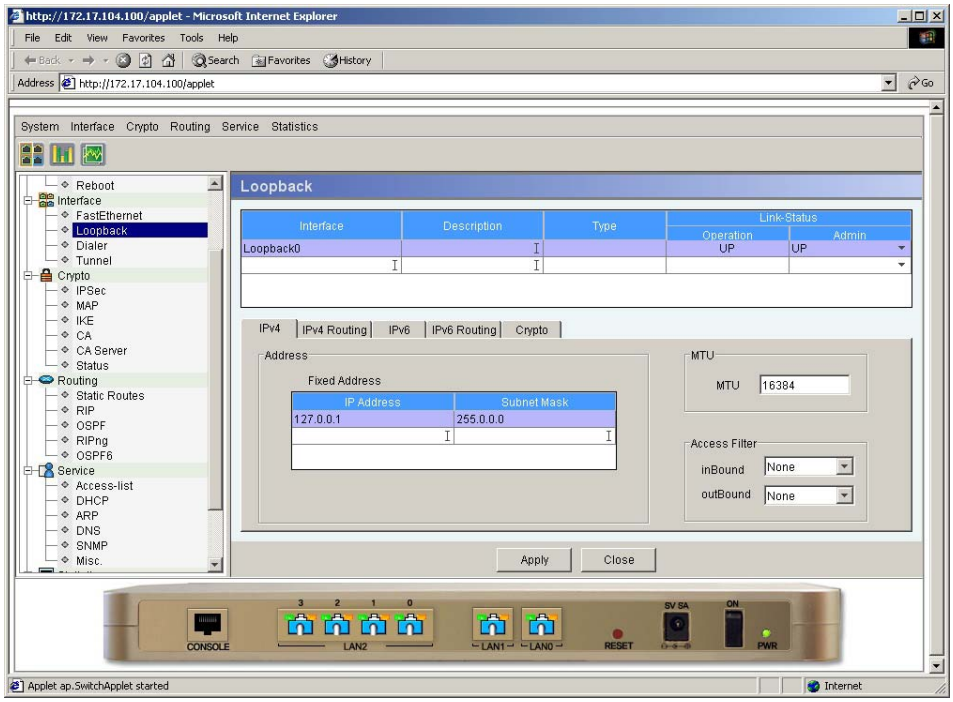
(Figure3-112) Loopback1 Interface verify page

To delete Loopback1 Interface, Select Interface then select “Delete” by clicking right side of mouse.



(Figure3-113) Delete Loopback1 Interface

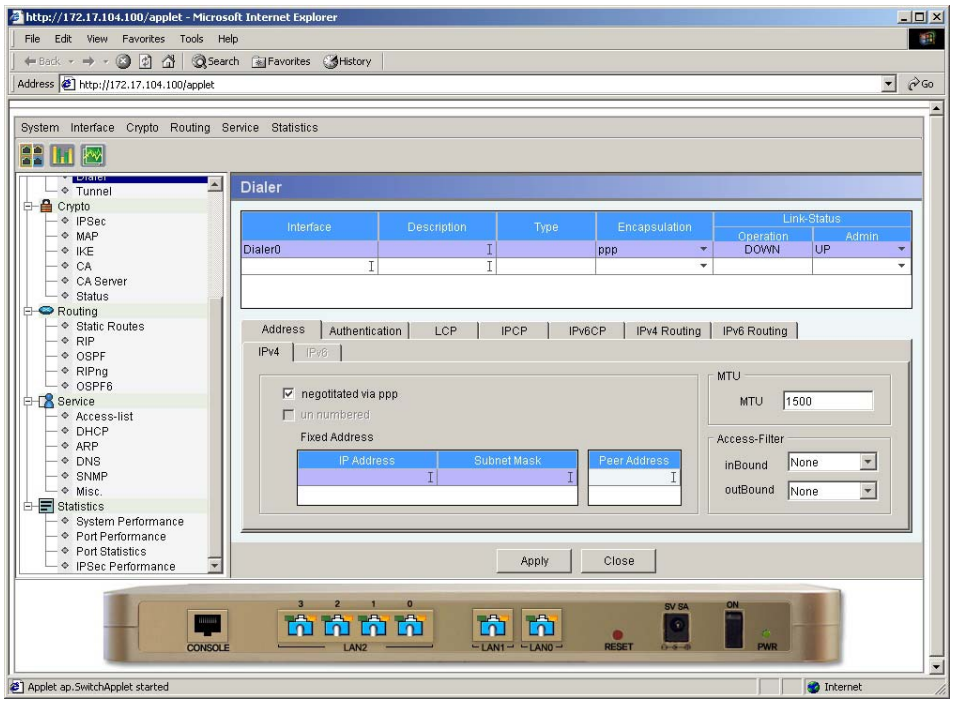
Click “Apply” to verify.



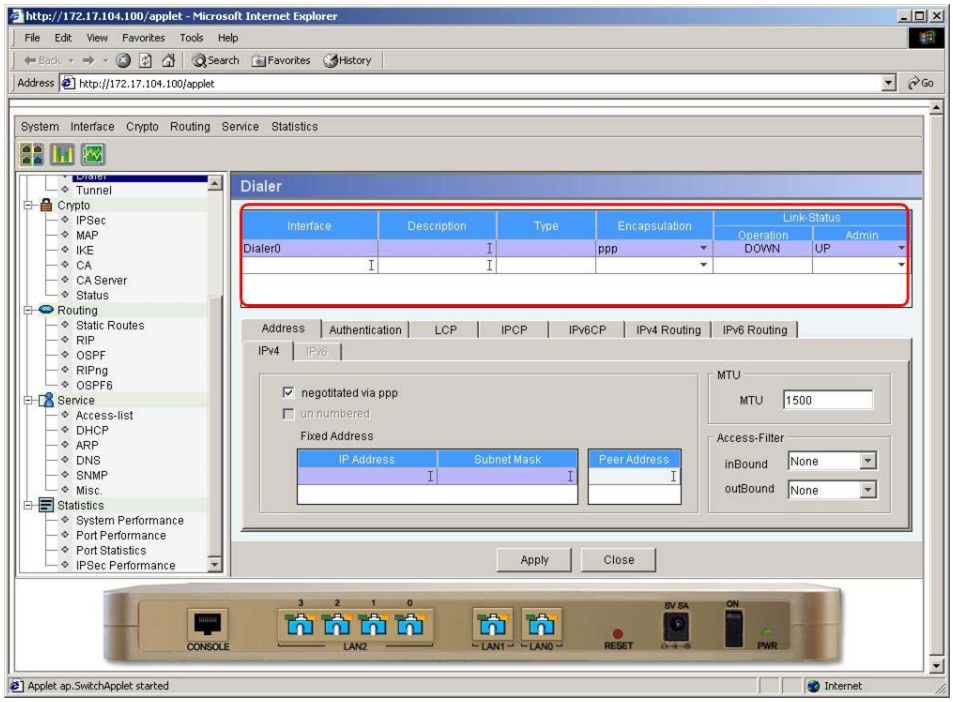
(Figure3-114) Loopback1 Interface delete verify.

Dialer

Dialer is a virtual interface which includes elements for PPP Session. The user has to define authentication for PPP Session, rules to access IP address and protocols for Link control. Also the virtual interface from Dialer has to be applied on Ethernet Interface to use.



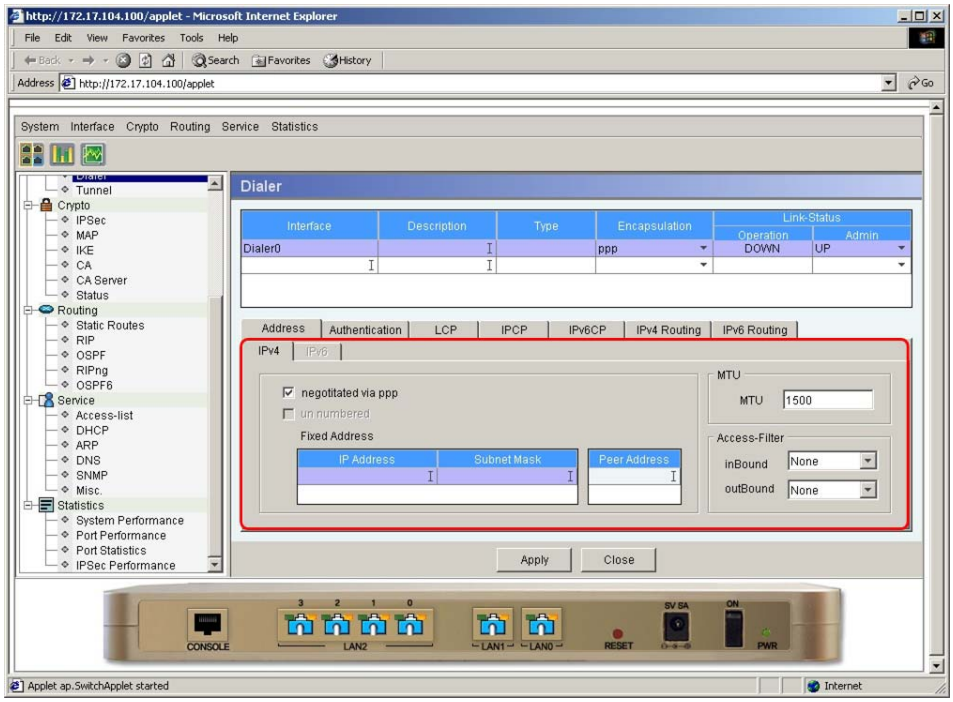
(Figure3-115) Dialer main page



(Figure3-116) Dialer Interface elements

<Table 3-17> Dialer Interface Description

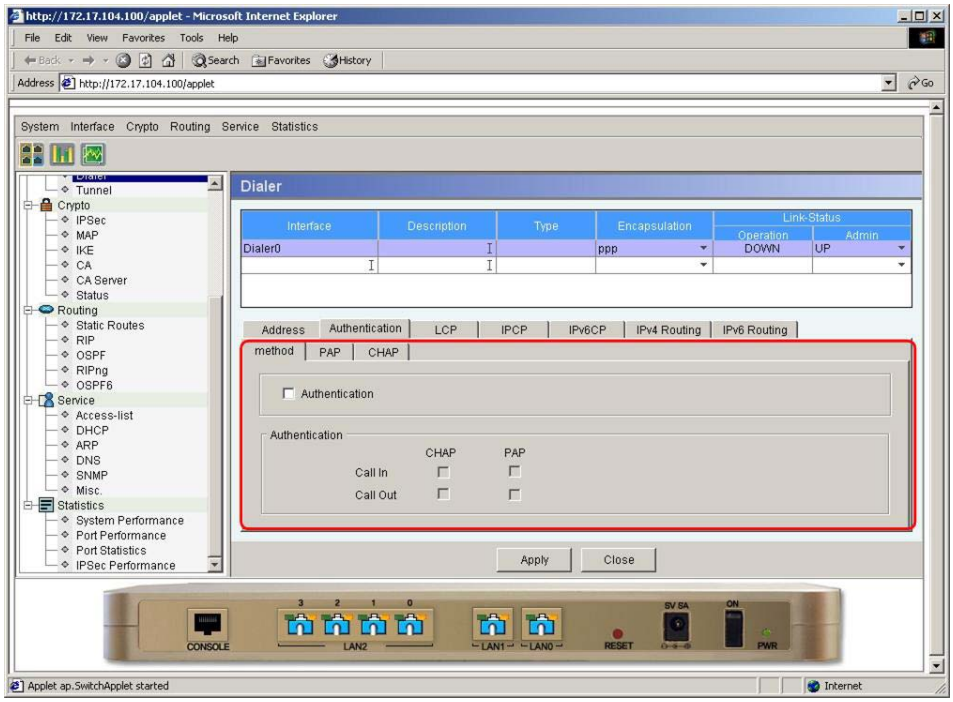
Elements	Description
Interface	This is Dialer Interface. You can create maximum 32 of Dialer Interfaces.
Description	Comments on Dialer Interface.
Type	Interface Type
Encapsulation	Encapsulation method of Link Protocol. PPP or Null can be used.
Link Status	Monitoring Link Status & controlling Shutdown



(Figure3-117) Dialer IPv4 Address elements

<Table 3-18> Dialer IPv4 Address Description

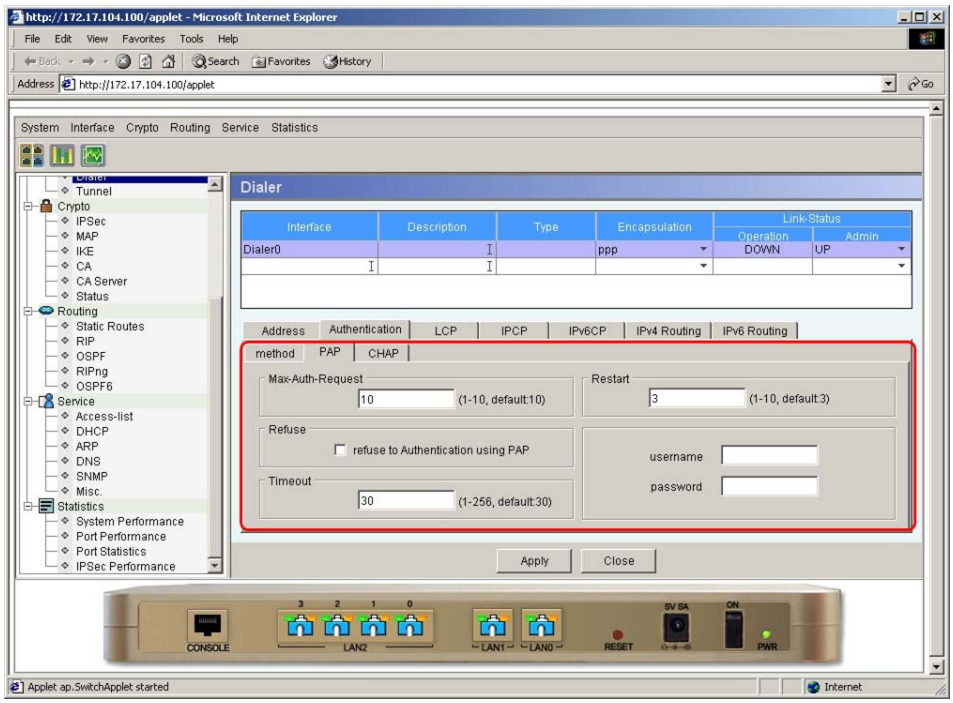
Elements	Description
Negotiated via PPP	To get IP Address from Peer via PPP Session
Unnumbered	This is not only for one specific IP Address, it is for using every IP Address.
Fixed Address	Input fixed IP Address. Not PPP Client.
Peer Address	It decides IP Address for peer when creating PPP Session.
MTU	Maximum Transmission Unit
Access Filter	To realize Packet Filter using Access-List.



(Figure3-118) Authentication method for PPP Session creation

<Table 3-19> Dialer Authentication Method Description

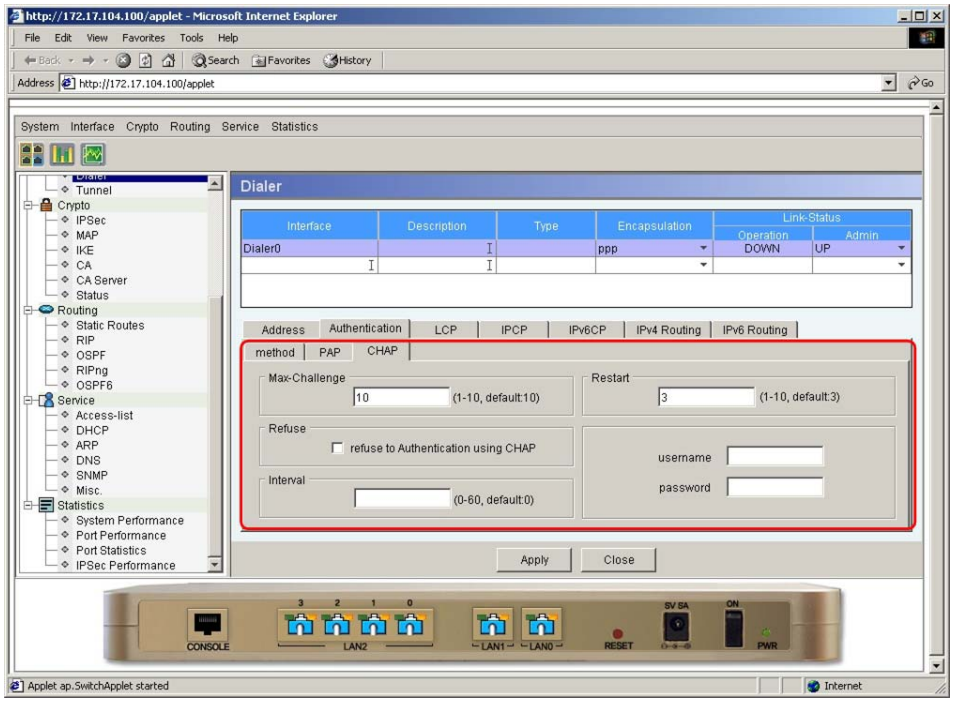
Elements	Description
Authentication	It decides whether authentication is needed or not for PPP Session.
Unnumbered	This is not only for one specific IP Address; it is for using every IP Address.
Fixed Address	Input fixed IP Address. Not PPP Client.
Peer Address	It decides IP Address for peer when creating PPP Session.
Callin[Chap|Pap]	Set PPP to Callin, it choose PAP and CHAP.
Callout[Chap|Pap]	Set PPP to Callout, it choose PAP and CHAP.



(Figure3-119) Dialer PAP Configuration

<Table 3-20> Dialer PAP Description

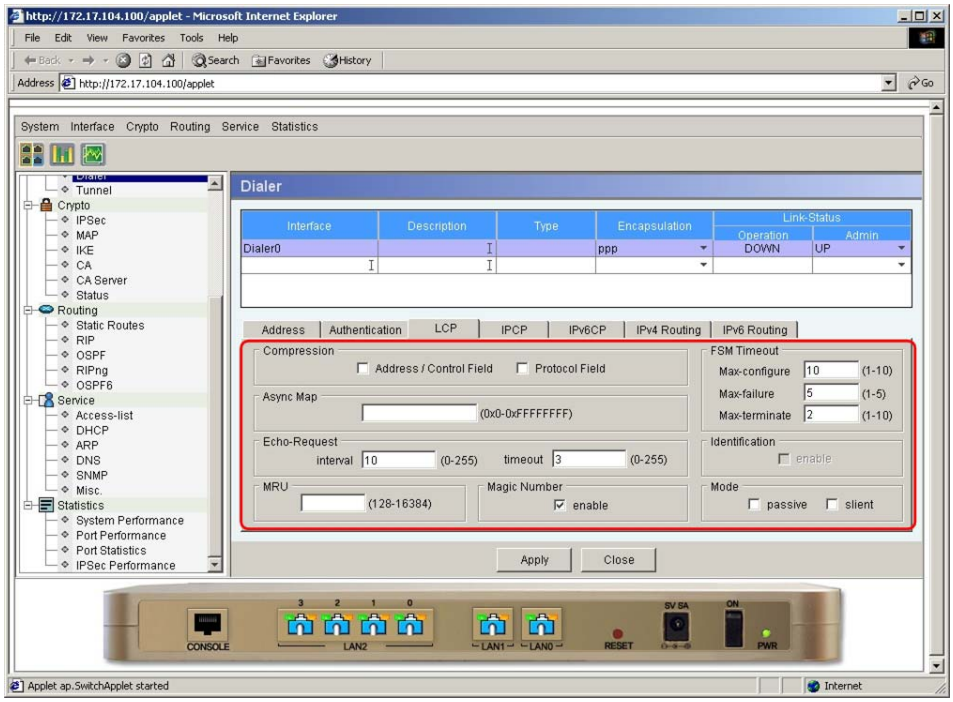
Elements	Description
Max-Auth-Request	It sets the maximum number of requesting time for authentication. PPP Session will be terminated after the requesting time is over. The default requesting number is “10”.
Restart	It sets the waiting time from peer after requesting PAP authentication. The default time is 3 sec.
Refuse	It is to refuse authentication when authentication is set to Callin.
Timeout	It restricts requesting time for PAP authentication. Default time is 30 sec.
Username	Input user name for PAP authentication.
Password	Input password for PAP authentication.



(Figure3-120) Dialer CHAP Configuratoin

<Table 3-21> Dialer CHAP Description

Elements	Description
Max-Auth-Request	It sets the maximum number of requesting time for authentication. PPP Session will be terminated after the requesting time. The default requesting number is “10”.
Restart	It sets the waiting time from peer after requesting CHAP authentication. The default time is 3 sec.
Refuse	It is to refuse authentication when authentication is set to Callin.
Timeout	It restricts requesting time for CHAP authentication. Default time is 30 sec.
Username	Input user name for CHAP authentication.
Password	Input password for CHAP authentication.

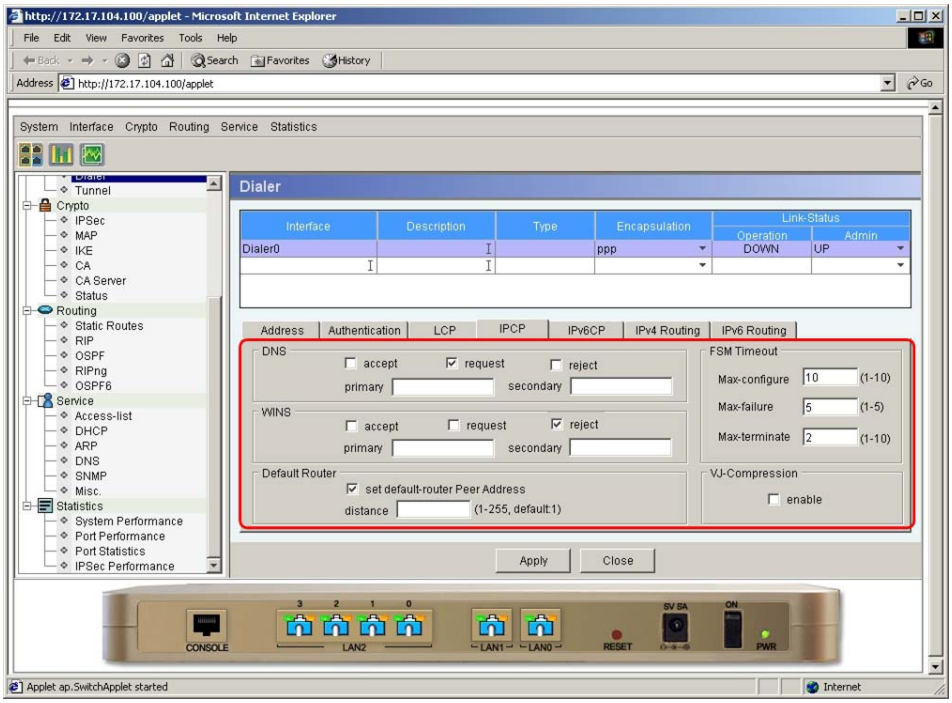


(Figure3)-121 Dialer LCP Configuration

<Table 3-22> Dialer LCP Description

Elements	Description
Compression	It is a Compression on Address, Controls field of PPP Packet and Protocol field.
Async Map	Input Async Map in LCP level.
FSM Timeout [Max-ConFigure]	Maximum transmit number of Configuration Request. Default number is “10”.
FSM Timeout [Max-Failure]	Restrict the number of Configuration. Default number is “5”.
FSM Timeout [Max-Terminate]	Restrict the number of Terminate Request. Default number is “2”.
Echo-Request Interval	Set transmit interval of Echo Request to check peer via PPP Session. Default is “10” sec.
Echo-Request Timeout	It restricts waiting time for Echo-Repeat after sending Echo-Request. Default time is “3” sec.
Identification	LCP Identification options.
MRU	It restricts Maximum Received Packet Size for PPP Negotiation.

Magic Number	To use LCP Magic Number. Default is “Enable”.
Mode	To use Passive Silent mode. Default is “Disable”.

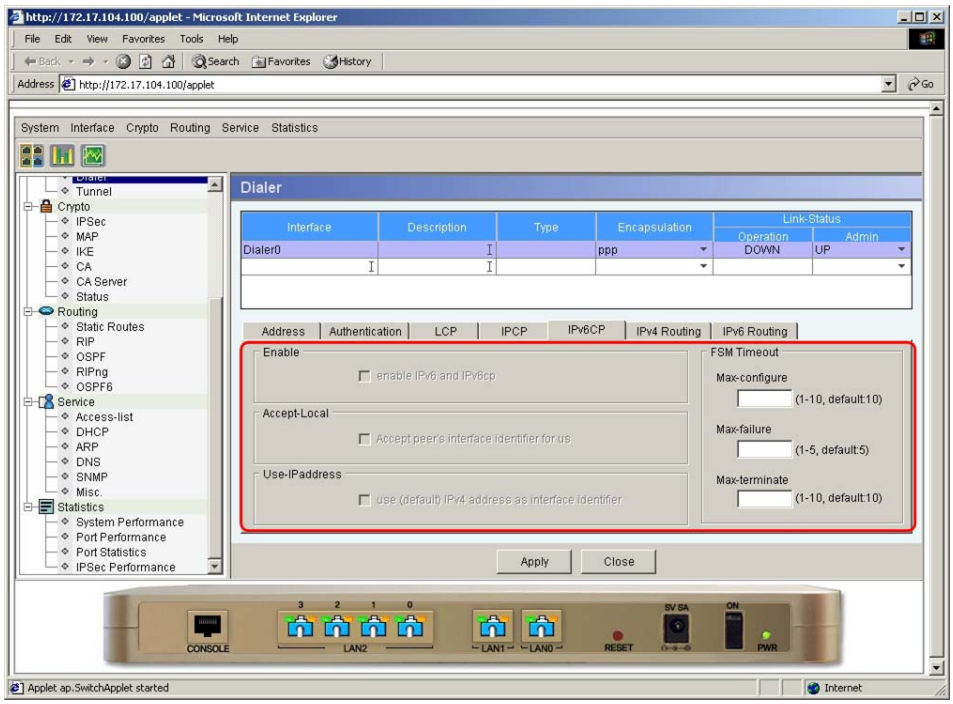


(Figure3-122) Dialer IPCP Configuration

<Table 3-23> Dialer IPCP Description

Elements	Description
DNS	It is used to get DNS information from PPP Server. Accept is to receive DNS info. Request is to request DNS info. Reject is to ignore DNS info from PPP Server. The user can input DNS addresses in Primary/Secondary field. Default value is “Request”.
WINS	It is used to get WINS information from PPP Server. Accept is to receive WINS info. Request is to request WINS info. Reject is to ignore WINS info from PPP Server. The user can input WINS addresses in Primary/Secondary field. Default value is “Reject” .
Default-router	Set IP Address of peer to Default-router.
FSM Timeout [Max-Configure]	Restricts Maximum transmit number of Configuration Request. Default number is “10”.
FSM Timeout [Max-Failure]	Restricts the number of IPCP operation. Default number is “5”.

FSM Timeout [Max-Terminate]	Restricts maximum transmit number of Terminate Request. Default number is “2”.
VJ Compression	To use VJ Compression



(Figure3-123) Dialer IPv6CP configuration

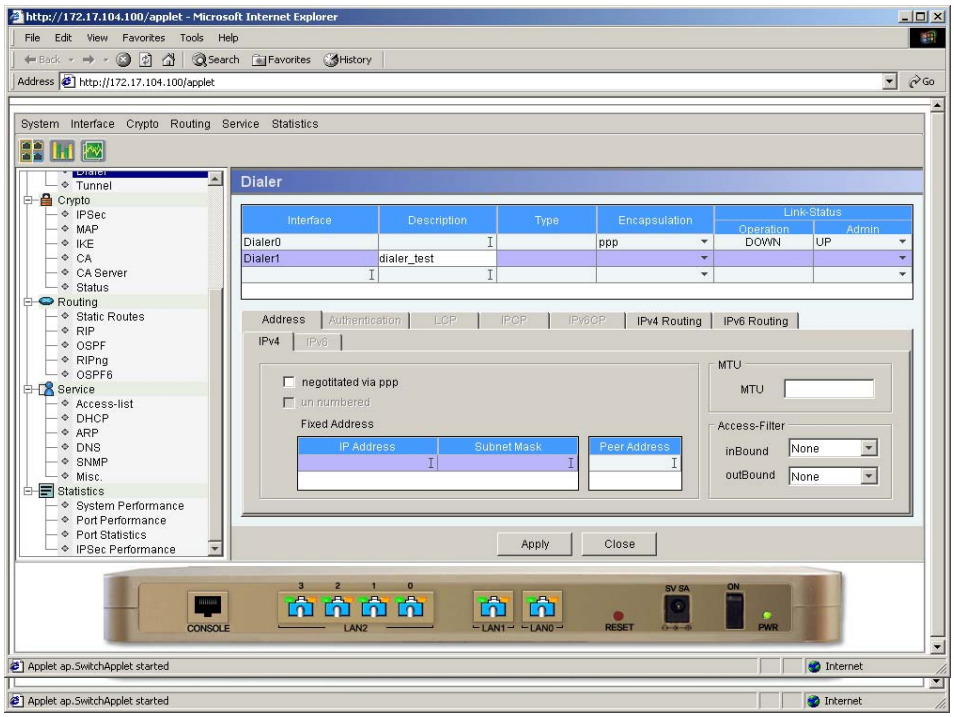
<Table 3-24> Dialer IPv6CP Description

Elements	Description
Enable IPv6 and IPv6CP	Enable of disable IPv6, IPv6CP on virtual Interface.
Accept-Local	It decides whether to recognize Interface Identifier of peer.
Use-IP Address	Config Identifier of interface as “Default-router”.
FSM Timeout [Max-ConFigure]	It sets the maximum transmit number of Configuration Request. Default number is “10”.
FSM Timeout [Max-Failure]	It sets the number of IPv6CP operation. Default number is “5”.
FSM Timeout [Max-Terminate]	It sets the maximum transmit number of Terminate Request. Default number is “2”.

Configuration setting for Dialer IPv4 Routing Protocol (RIP, OSPF), IPv6 Routing Protocol (RIPng, OSPFv3) is the same as Routing Protocol configuration setting of FastEthernet. Please refer to Routing Protocol configuration of FastEthernet.

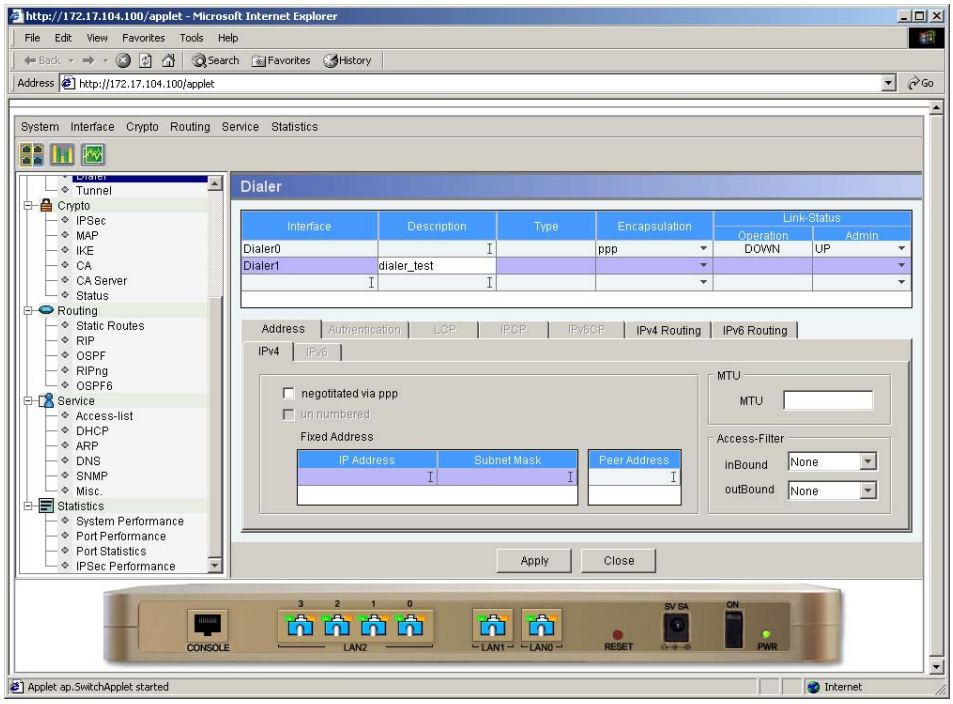
Figure 3-125 shows how to create and delete Dialer Interface.

First, Input “Dialer1” in Interface field.



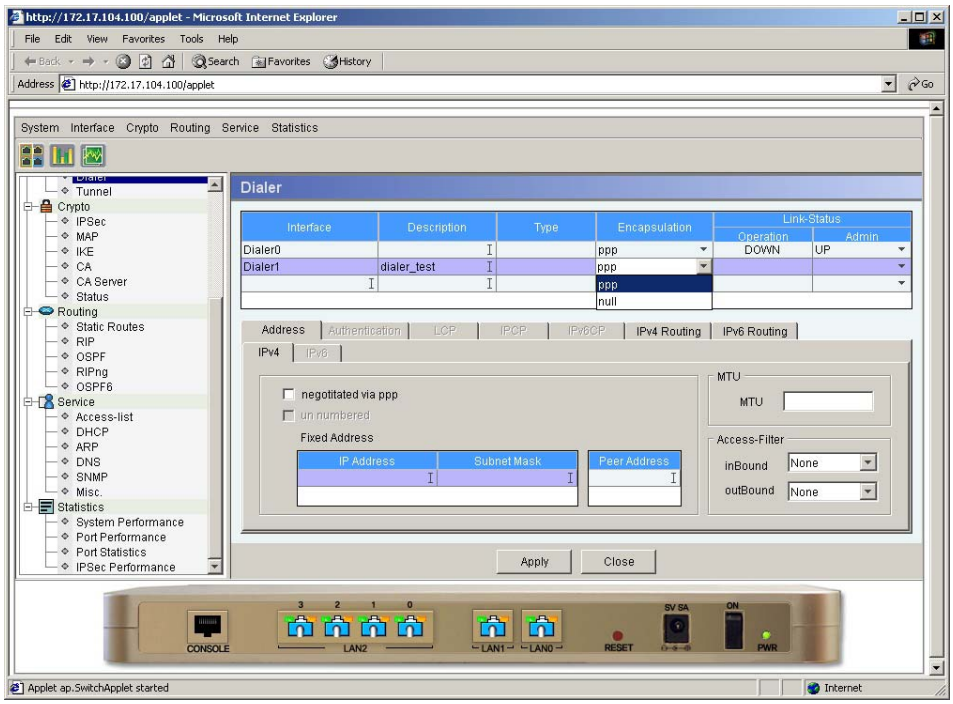
(Figure3-124 Create Dialer1 Interface)

Input “dialer_test” in Description field for brief comment.



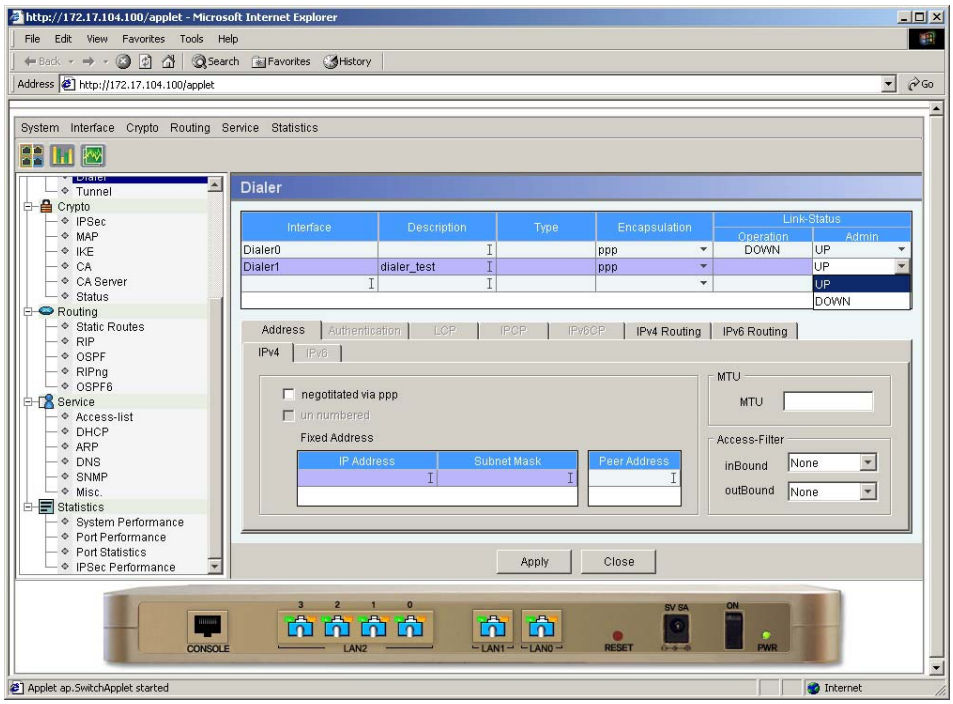
(Figure3-125) Input Description

Set Encapsulation to PPP.



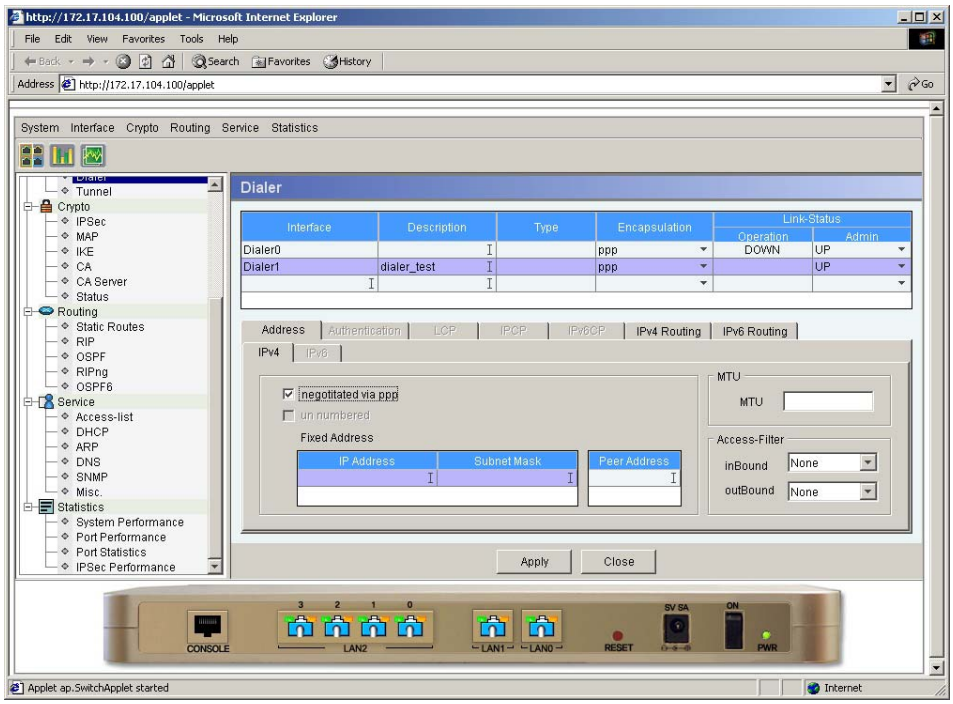
(Figure3-126) Select Encapsulation

Set Administrative Link State of Interface to “Up”.



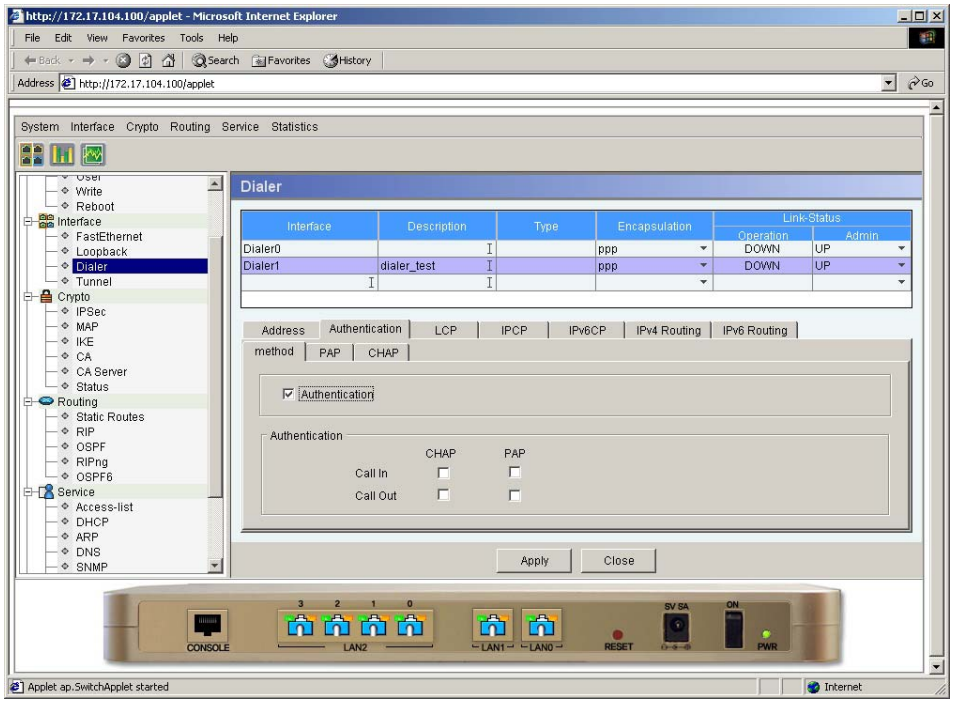
(Figure3-127) Alter Administrative Link State

Select Negotiated via ppp for PPP Session.



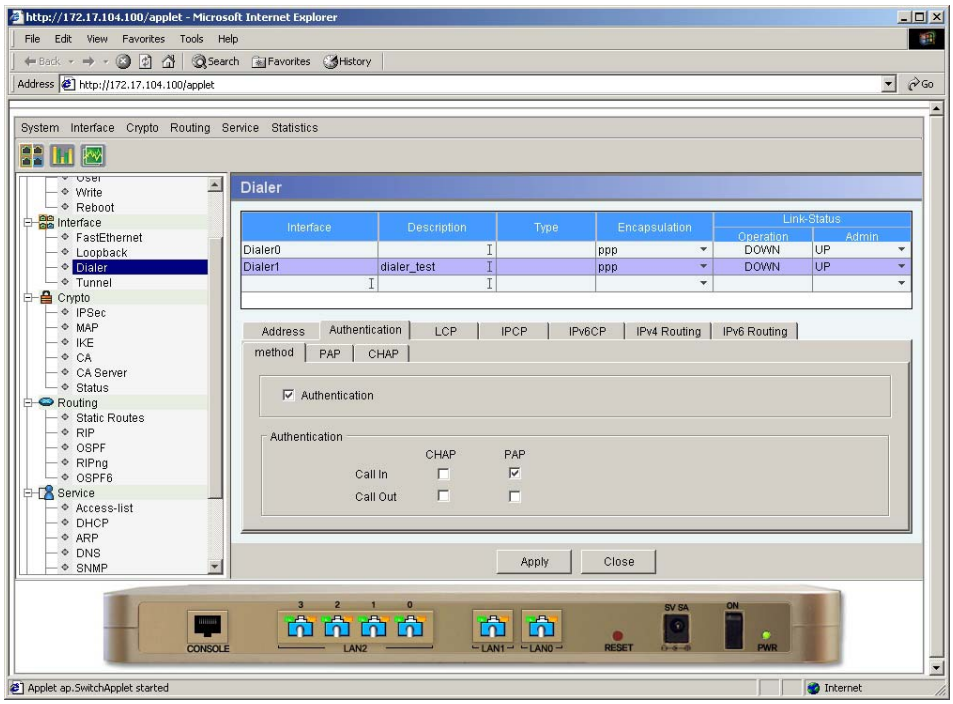
(Figure3-128) Select Negotiated via PPP

Check "Authentication" for PPP Session Authentication.



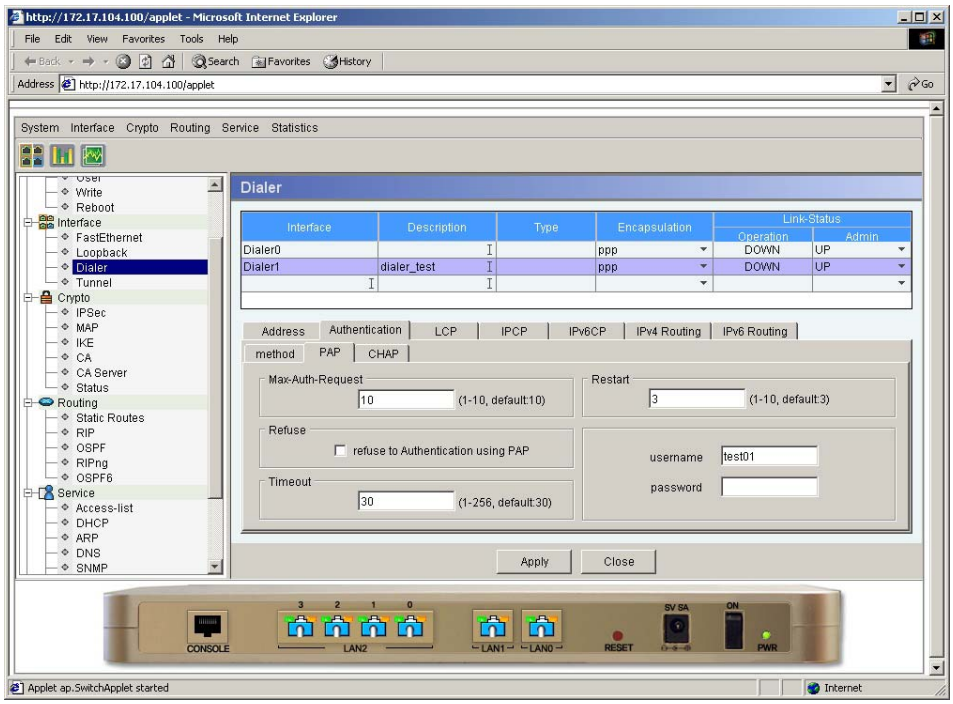
(Figure3-129) Check Authentication

Check general PPP Session authentication method, PAP Callin.



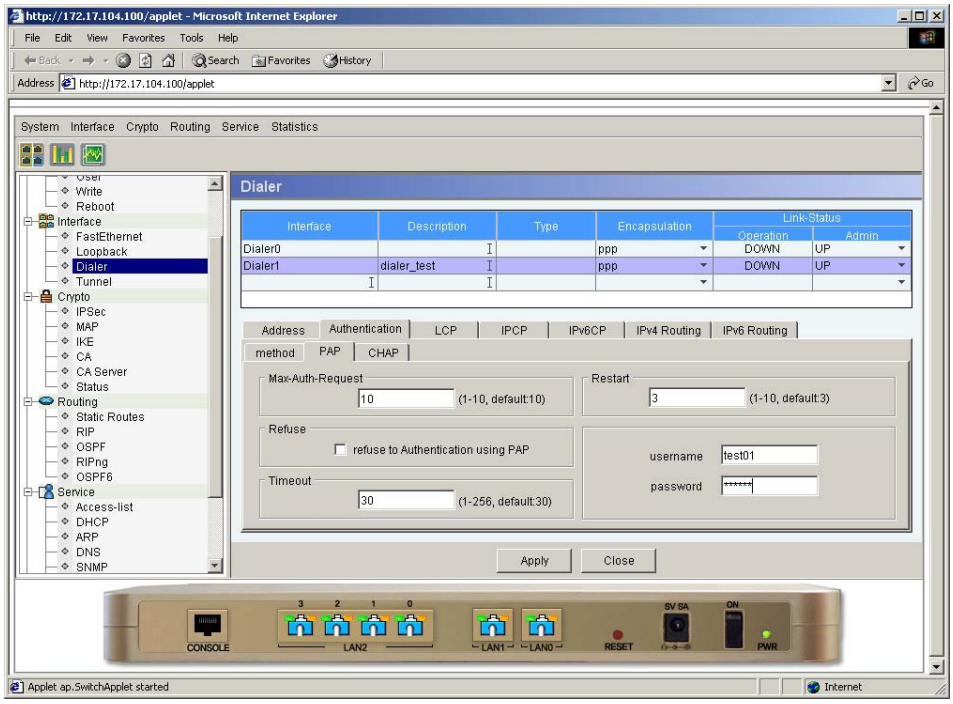
(Figure3-130) Check PAP Callin

Input Username “test01” for PAP authentication.



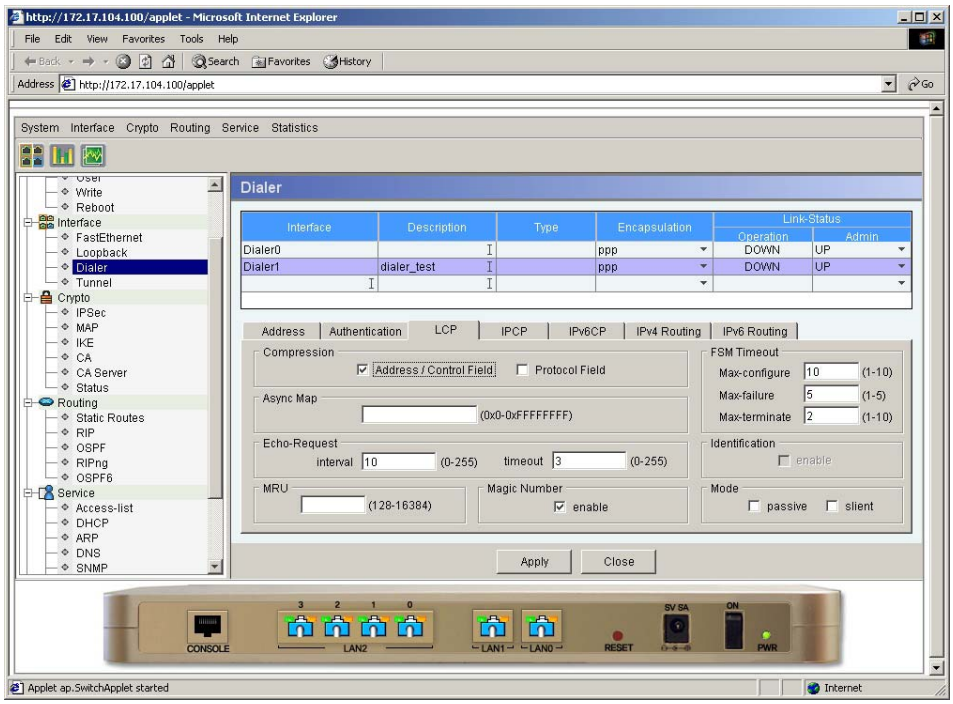
(Figure3-131) Input PAP Username

Input PAP Password “test01”. It will be shown as “*” on the screen for security.



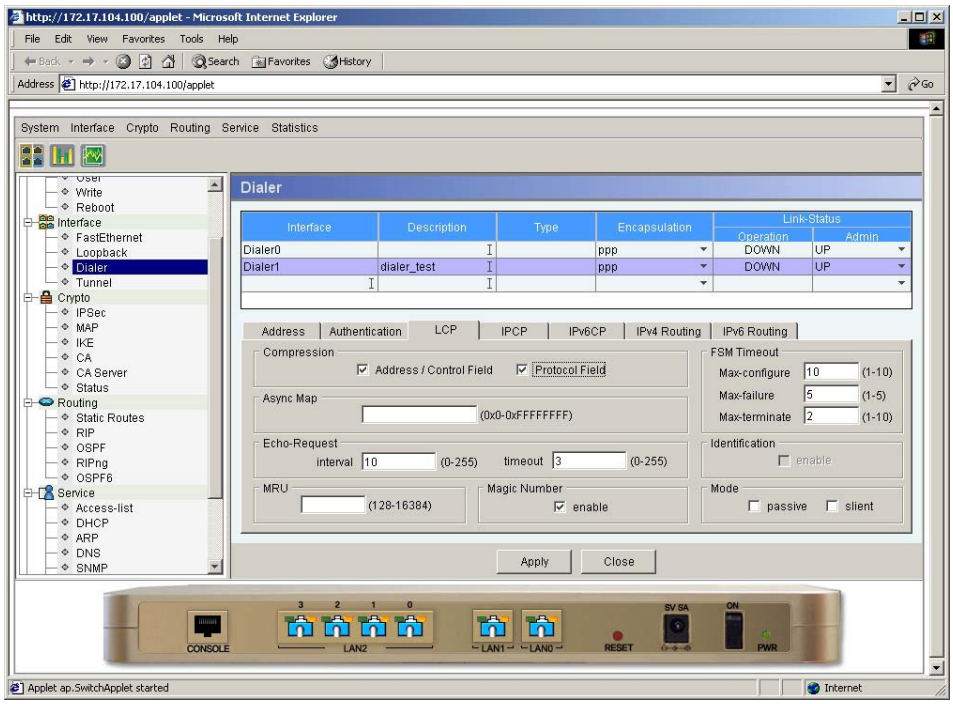
(Figure3-132) Input PAP User Password

Check on LCP Address/Control Field Compression



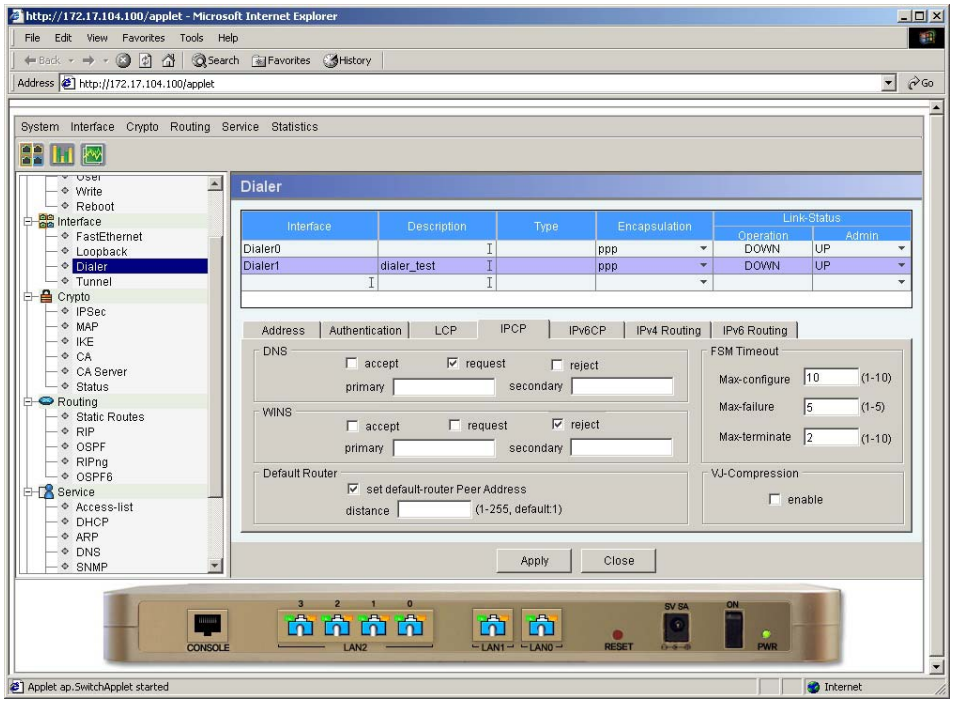
(Figure3-133) Check LCP ACFC

Check LCP Protocol Field Compression.



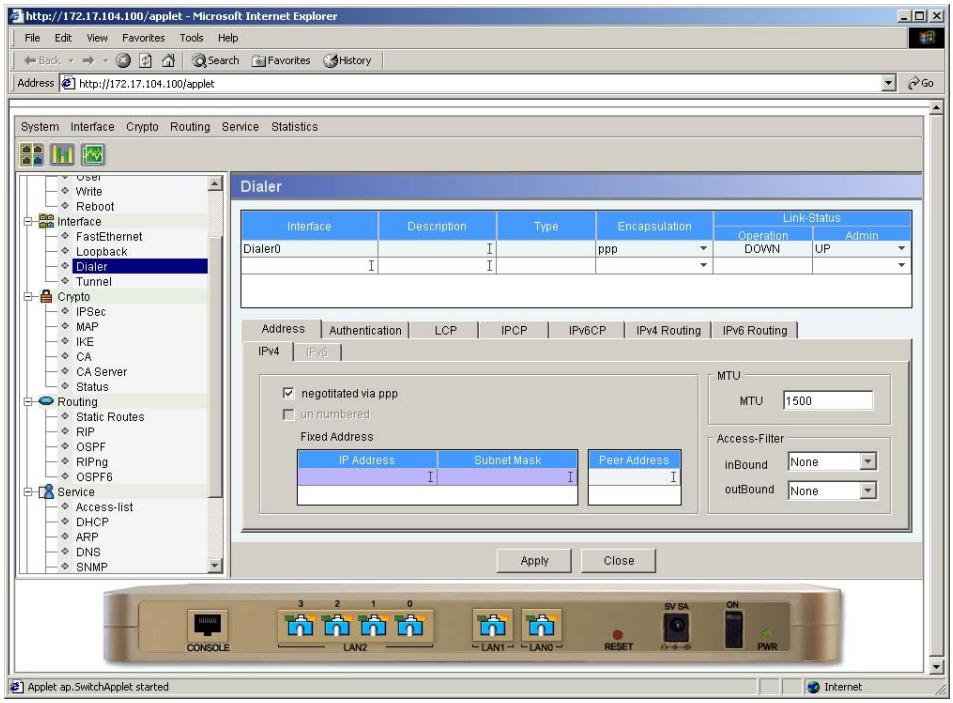
(Figure3-134) Check LCP PFC

Check DNS Request and Default Router to be able to receive information from Peer.



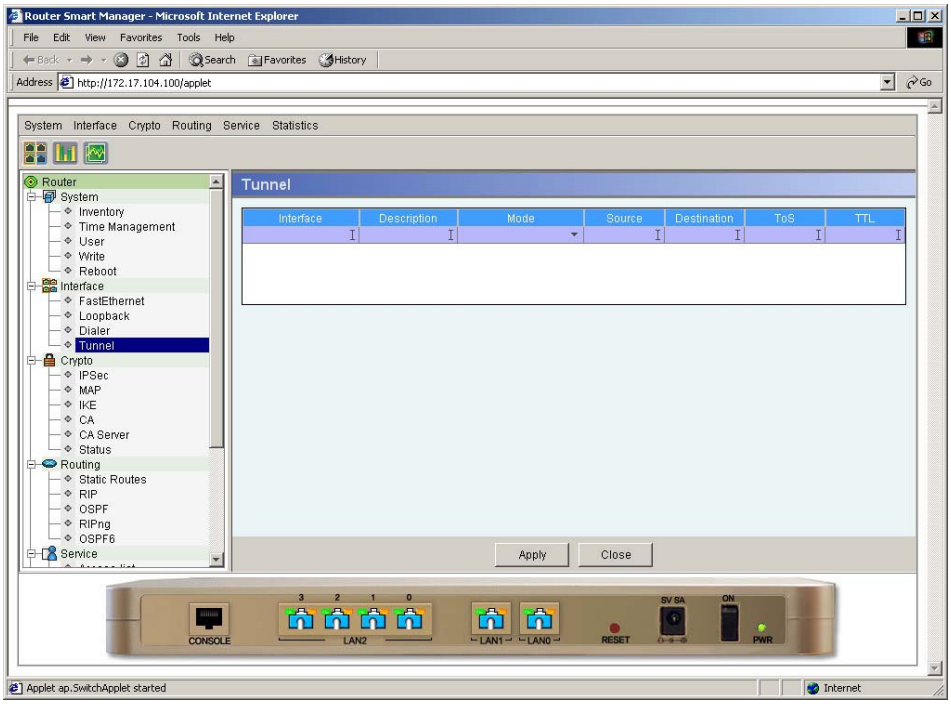
(Figure3-135) Check IPCP DNS Request, Default Router

To delete a specific Dialer Interface, select the interface you want to delete, click on right side of the mouse to delete.



Tunnel

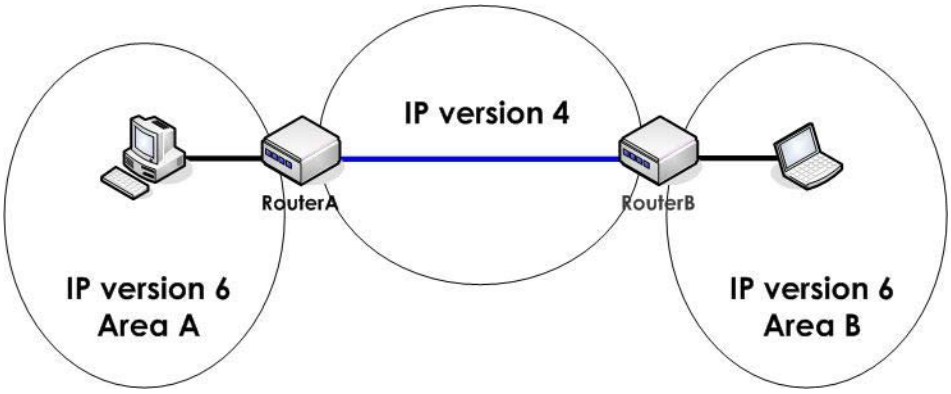
Tunnel Interface is necessary for IPv4 and IPv6 communication. For example, there is LAN A and LAN B configured with IPv6. And they need to go through IPv4 area for end-to-end IPv6 Communication. Tunnel Interface enables to communicate between LAN A and LAN B.



(Figure3-136) Tunnel main page

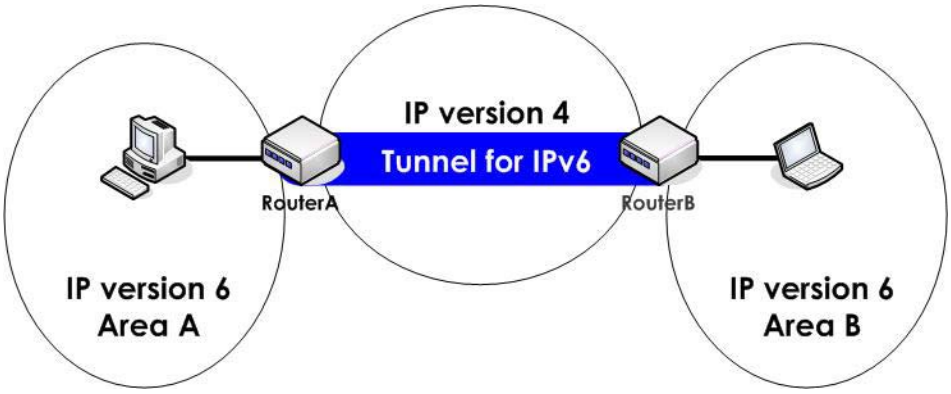
Figure 3-139 is an example of Tunnel Interface.

Router A and B is configured with IP version 4 network, so hosts from Area A and Area B are not able to communicate each other. It is because of Router A and Router B can not implement normal Routing.

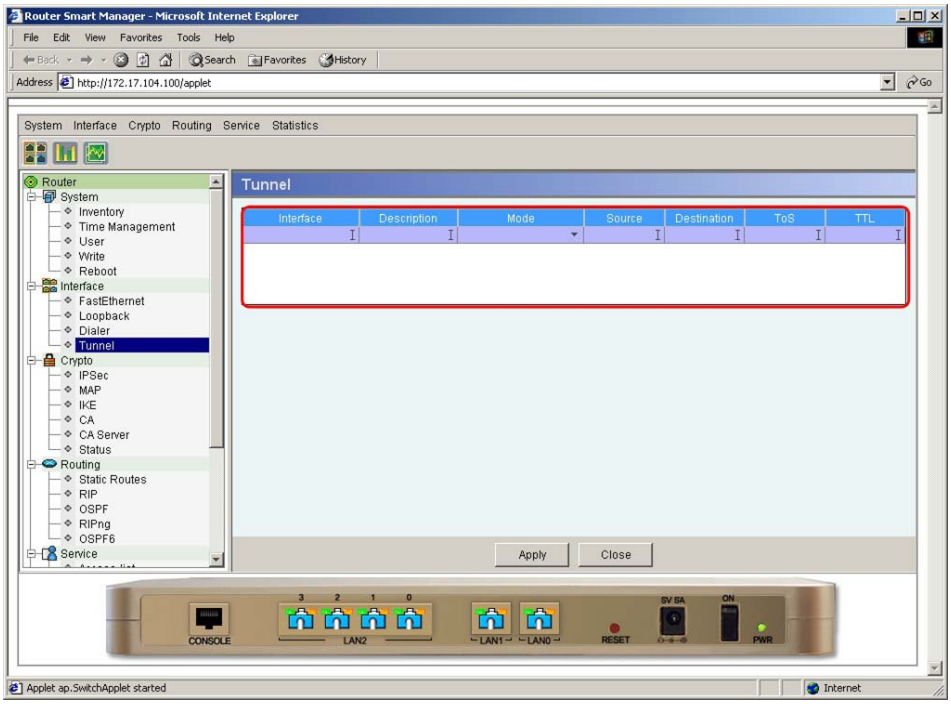


(Figure3-137) Tunnel Interface example Network Diagram 1

However, through Tunnel Interface, Router A and Router B create logical tunnel between Area A and Area B. So hosts from these two areas can send and receive IP version 6 datagram.



(Figure3-138) Tunnel Interface example Network Diagram 2



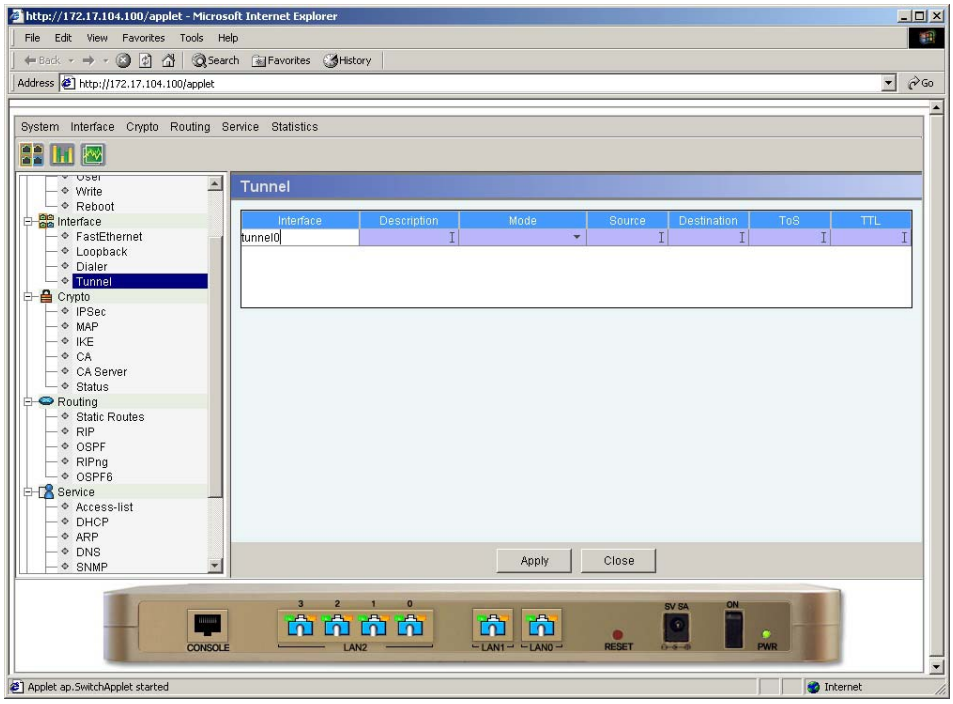
(Figure3-139) Tunnel main page

<Table 3-25> Tunnel Description

Elements	Description
Interface	The name of Tunnel Interface
Description	Brief comments
Mode	Select one from ipip, ipv6ip or none mode.
Source	Input IP Address of Local Interface.
Destination	Input Interface IP Address of Peer system.
ToS	Type of Service. It is used for changing ToS field value of sending Packet. Default value is “0”.
TTL	It decides TTL field value of Sending Packet. Default value is 30 Hop.

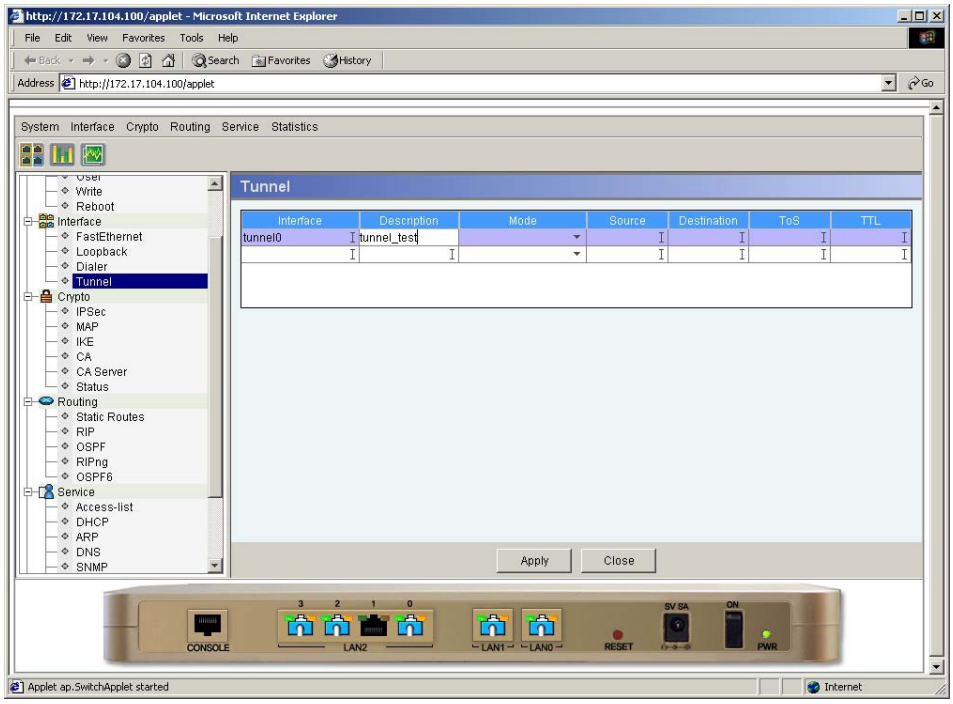
Figure 3-142 shows how to add Tunnel Interface.

Input “tunnel0” by clicking Interface field.



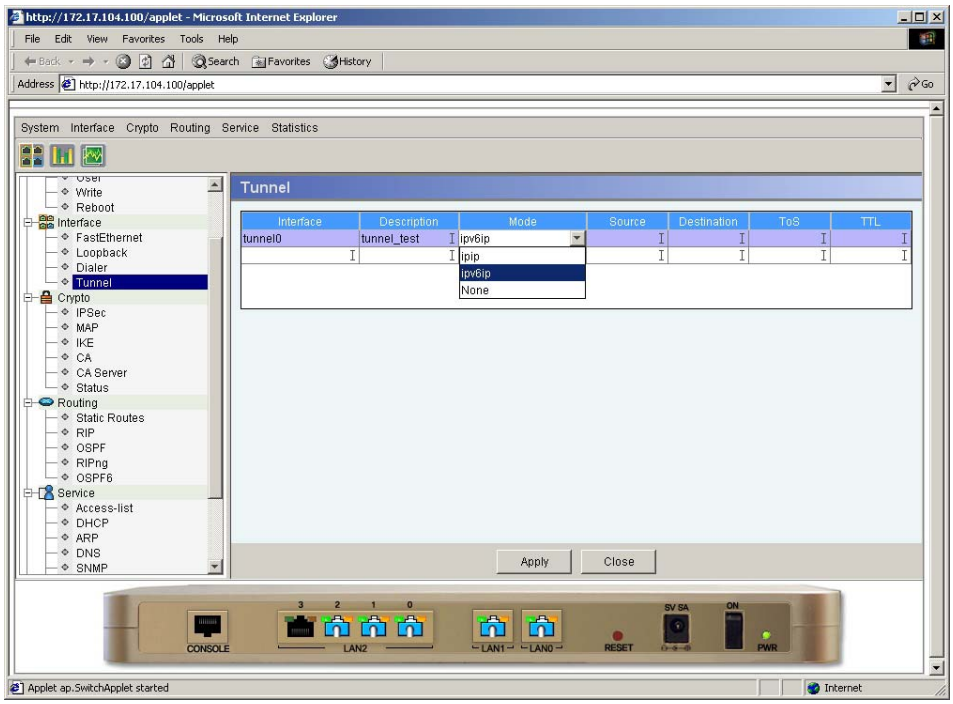
(Figure3-140) Input Tunnel Interface Name

Input “tunnel_test” in Description field.



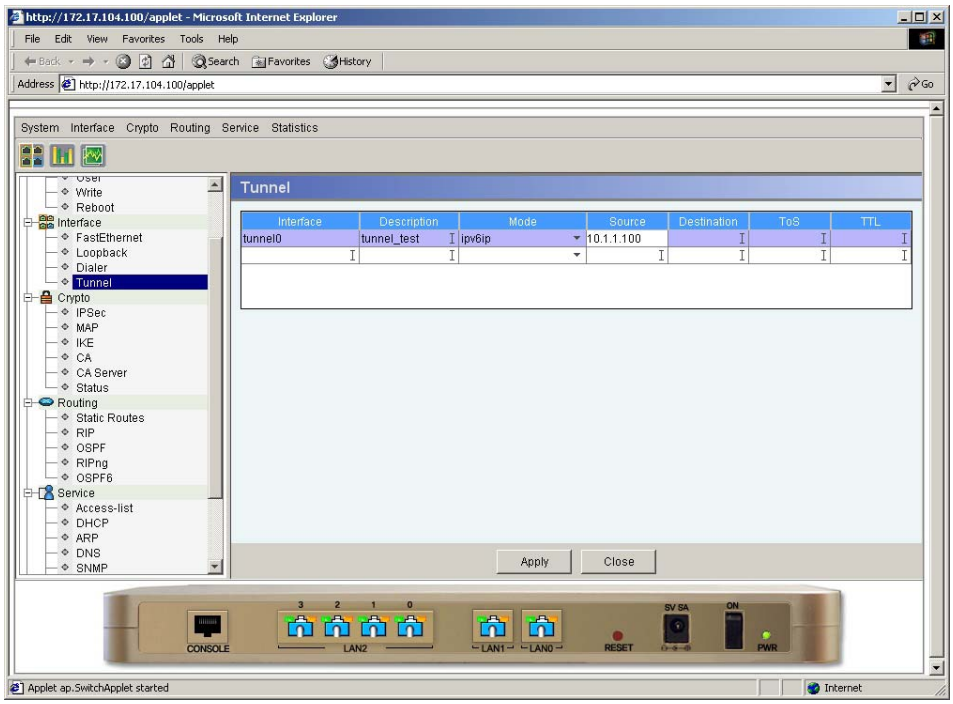
(Figure3-141) Input Tunnel Interface Description

Select “ipv6ip” Mode to create IPv6 → IPv4 Tunnel Interface.



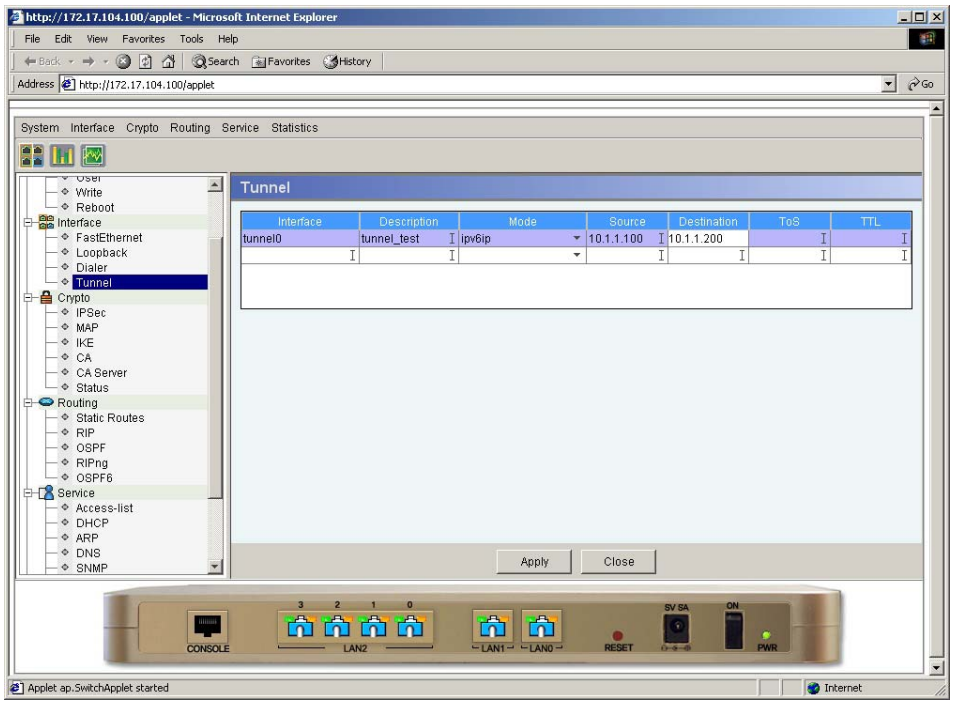
(Figure3-142) Select Tunnel Mode

Input IP Address of Local Interface in Source field.



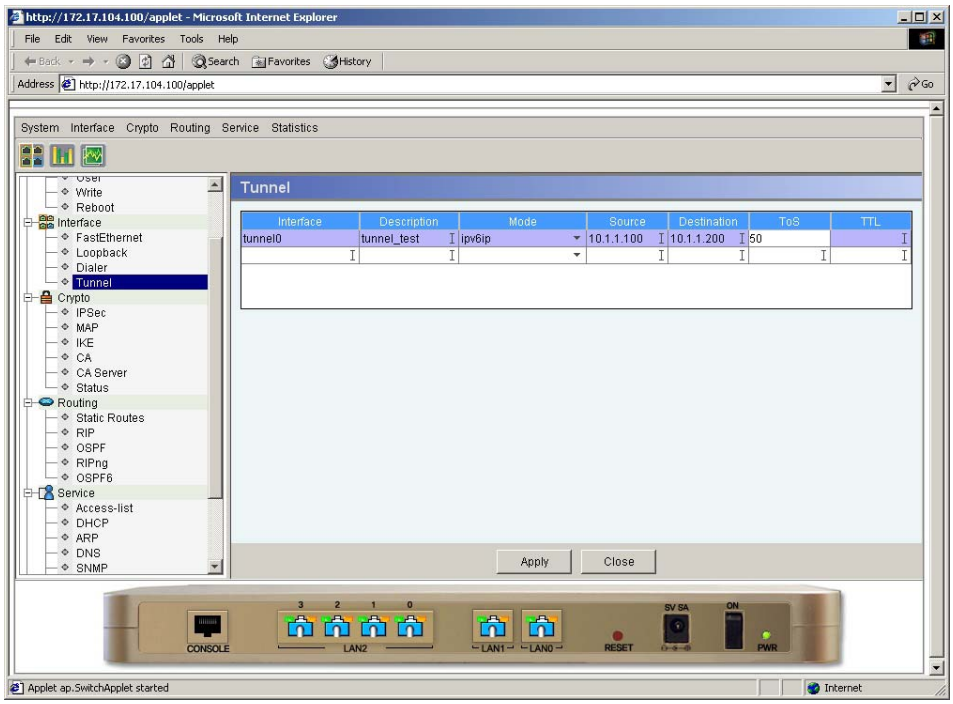
(Figure3-143) Input Tunnel Interface IP Address

Input Peer IP Address in Destination field.



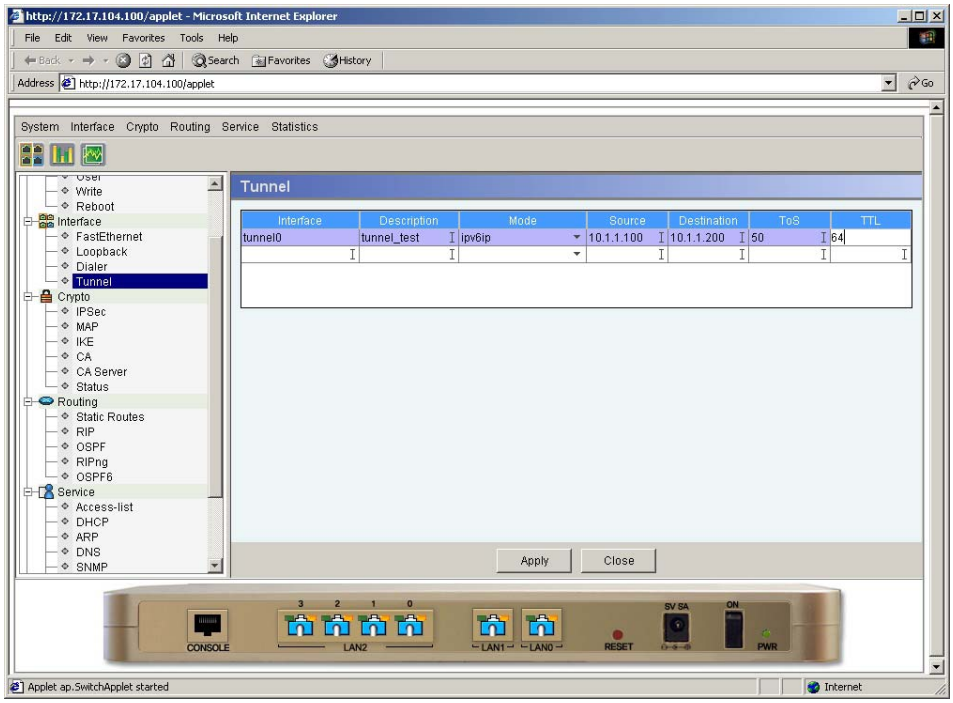
(Figure3-144) Input Tunnel Interface Destination IP Address

Input “50” for ToS field of sending packet via Tunnel Interface.



(Figure3-145) Input Tx Packet ToS

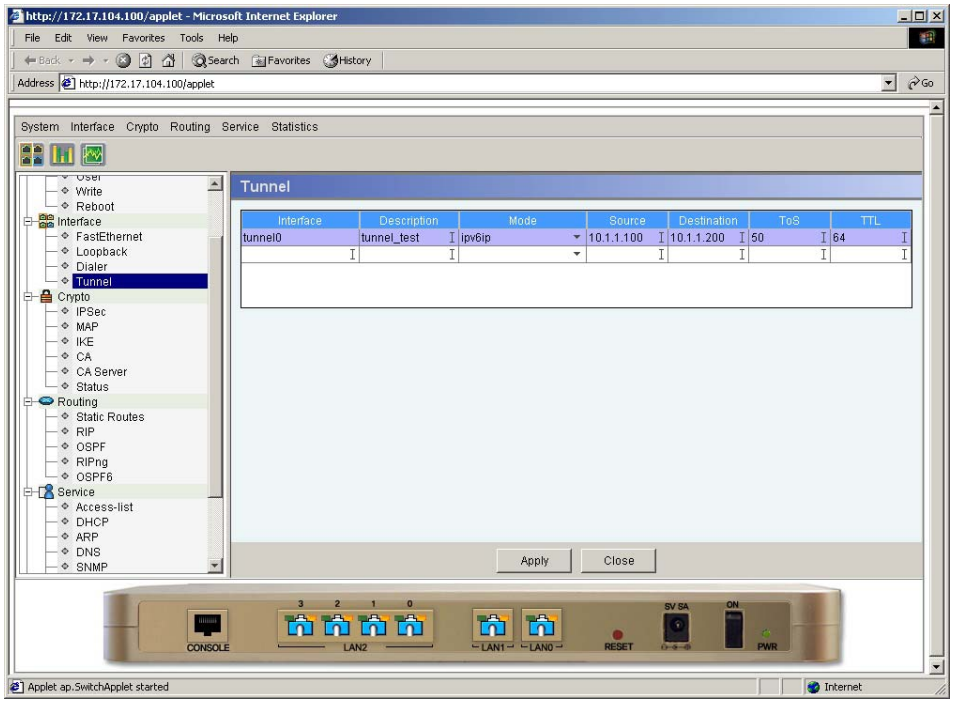
Input “64” for TTL field of sending packet via Tunnel Interface.



(Figure3-146) Input Tx Packet TTL

Click “Apply” to verify.

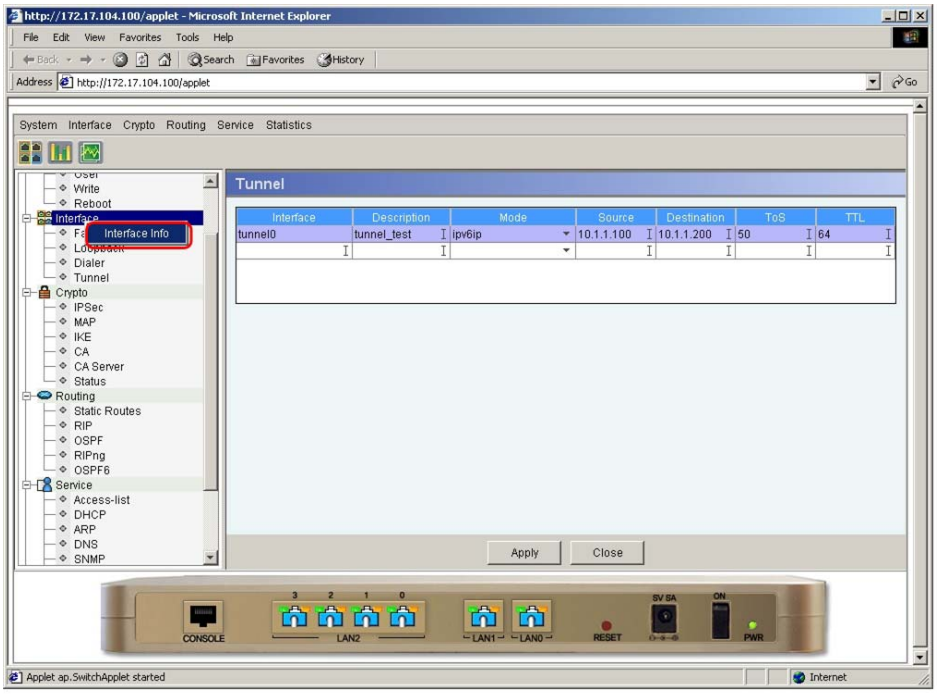
To delete Tunnel Interface, Select the interface you want to delete then click “Delete” on the right side of mouse.



(Figure3-147) Tunnel Interface creation

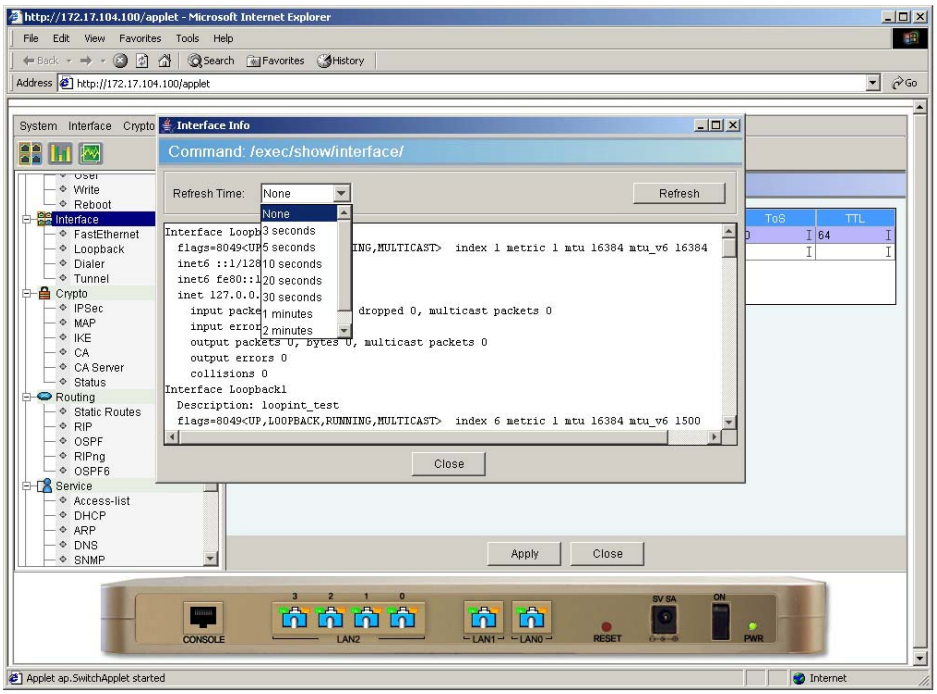
Interface Popup Menu

Select Interface, then click right side of the mouse to use Popup Menu. Popup Menu of Interface is Interface Information. Use a mouse to see the detail info for each element.



(Figure3-148) Interface Popup Menu Main page.

Refresh Time for Interface Info can take 3 sec to 5 sec. Click Refresh button run directly. Information for each Interface includes Interface Metric, MTU, IP Address, MAC Address, Tx/Rx Packet Count etc.



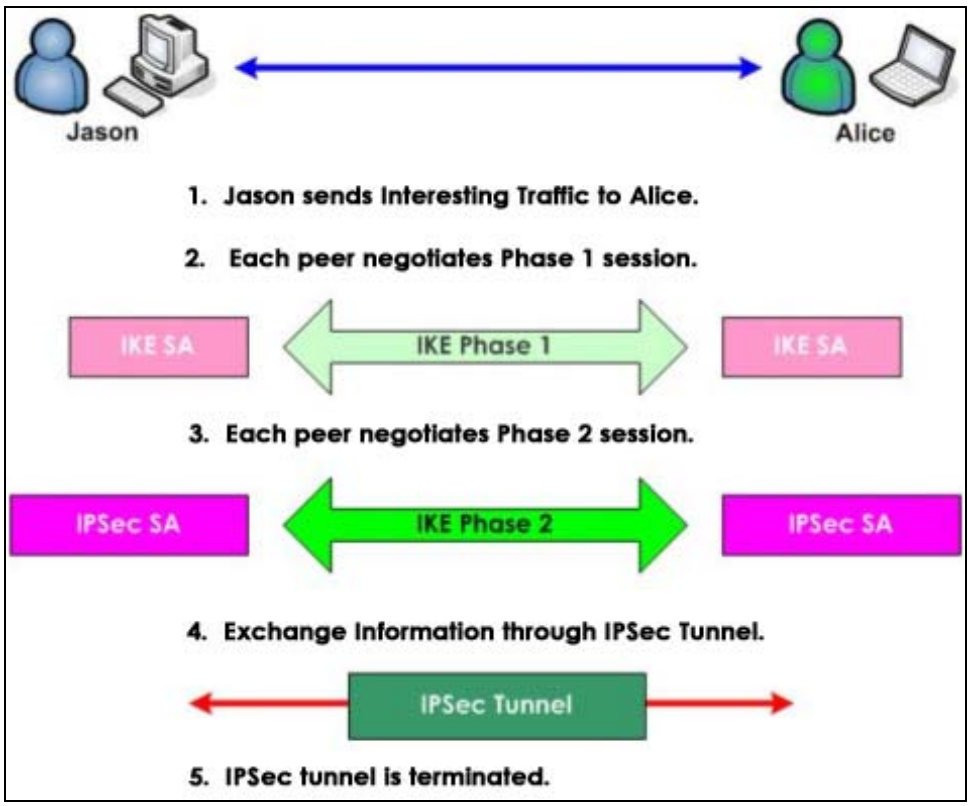
(Figure3-149) Interface Info page

Crypto Menu

IPSec

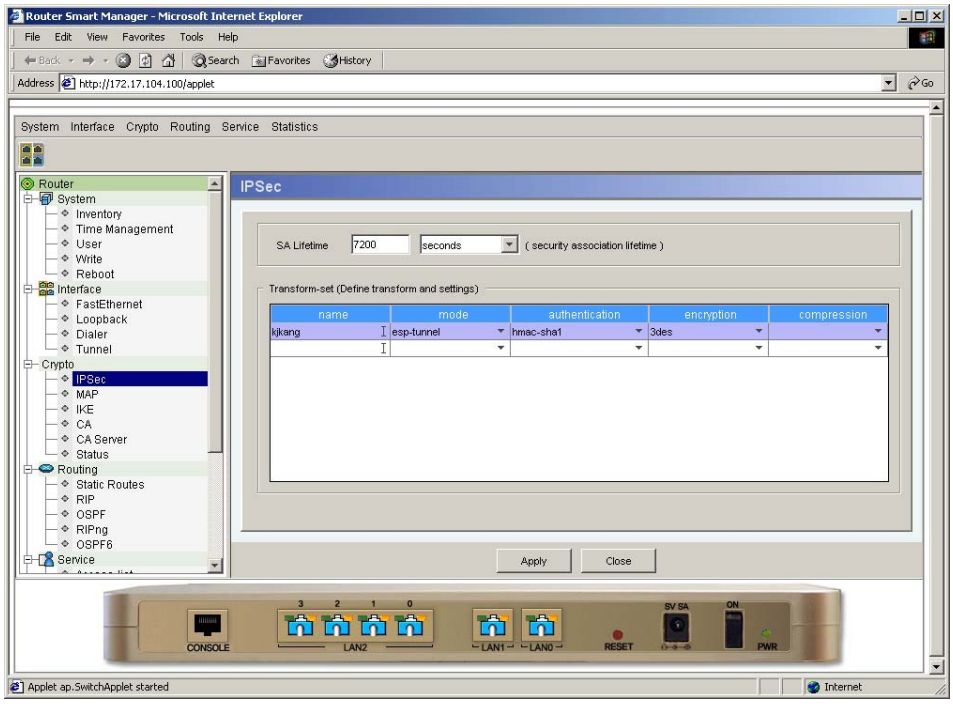
IPSec supports secure communication between the end-to-end terminals. It provides security protocols based on IP layer.

Figure 3-152 shows stages of realizing IPSec.



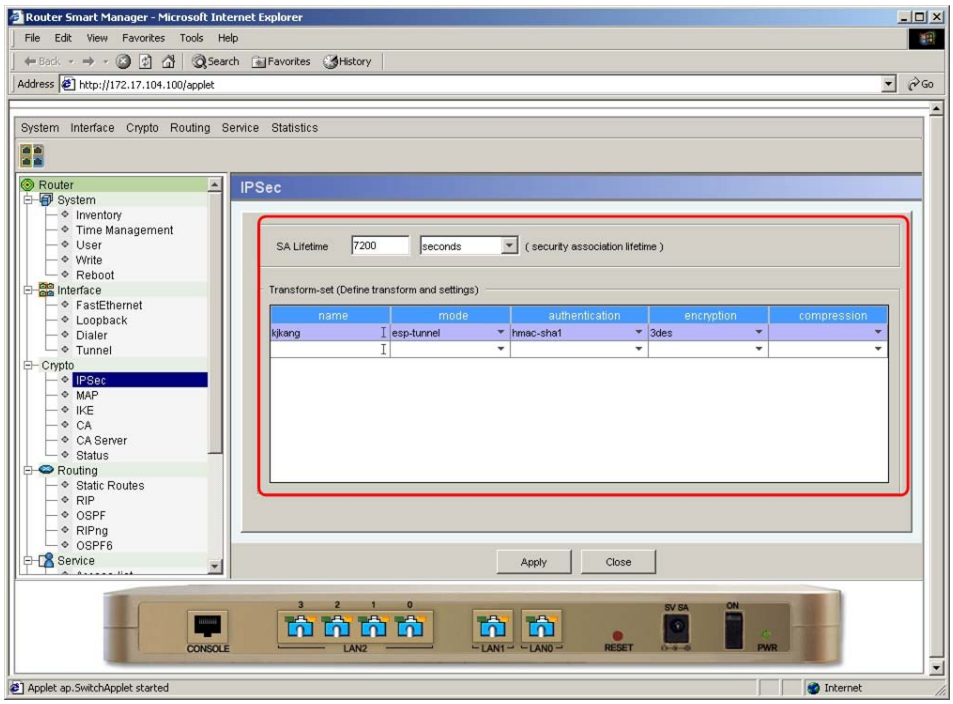
(Figure3-150) Stages of realizing IPSec

The user can define IPSec Mode, Authentication, Data Encryption, Data Compression etc on IPSec menu.



(Figure3-151) Crypto IPSec Main page

<Table 3-26> shows each element of IPSec menu.



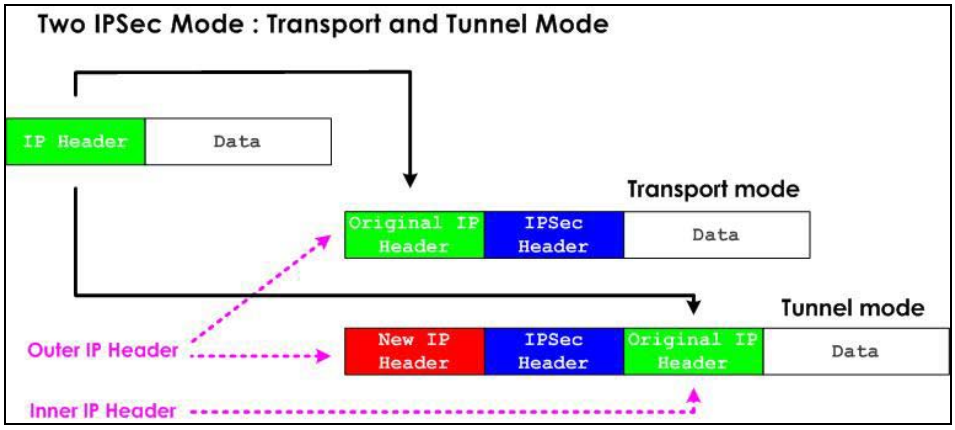
(Figure3-152) IPSec Menu

<Table 3-26> IPSec Description

Elements	Description
SA Lifetime	Lifetime of Security Association. Time or data traffic can be choosed.
Name	The name of Transform-set.
Mode	Select IPSec Mode. Choose one from esp-tunnel, esp-transport, ah-tunnel, ah-transport.
Authentication	Select authentication algorithm. Choose one from hmac-md5, hmac-sha1.
Encryption	Select Encryption algorithm. Choose one from 3des, blowfish, cast, des, null, rijndael.
Compression	Select data compression algorithm. Choose one from deflate, lzs.

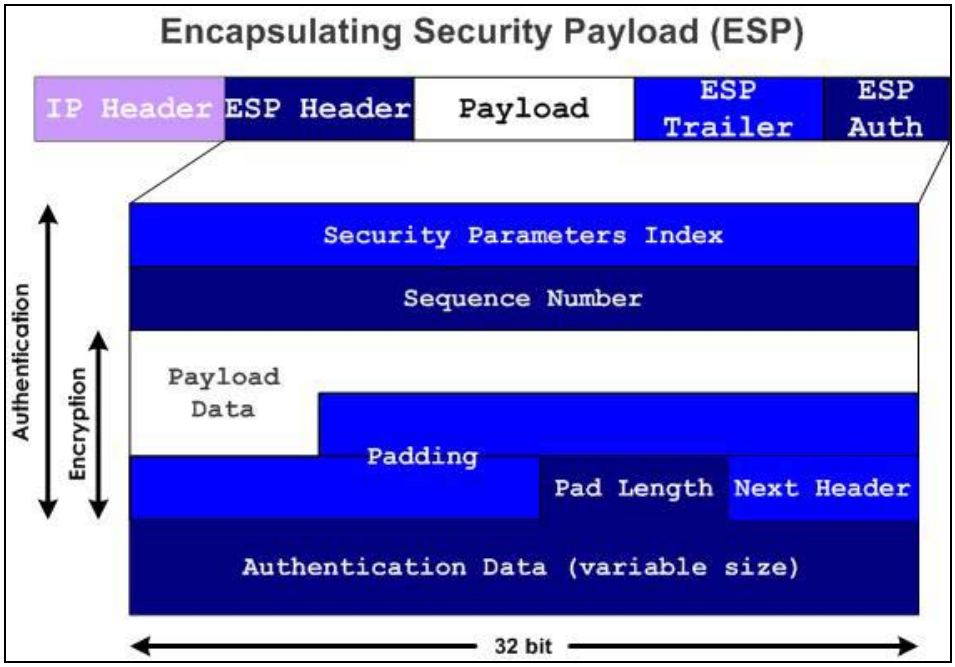
Figure 3-155 shows the difference between Transport Mode and Tunnel Mode.

Source IP Address and Destination IP Address are not changing on Transport Mode. IP Address for IPSec communication is added on Tunnel Mode.



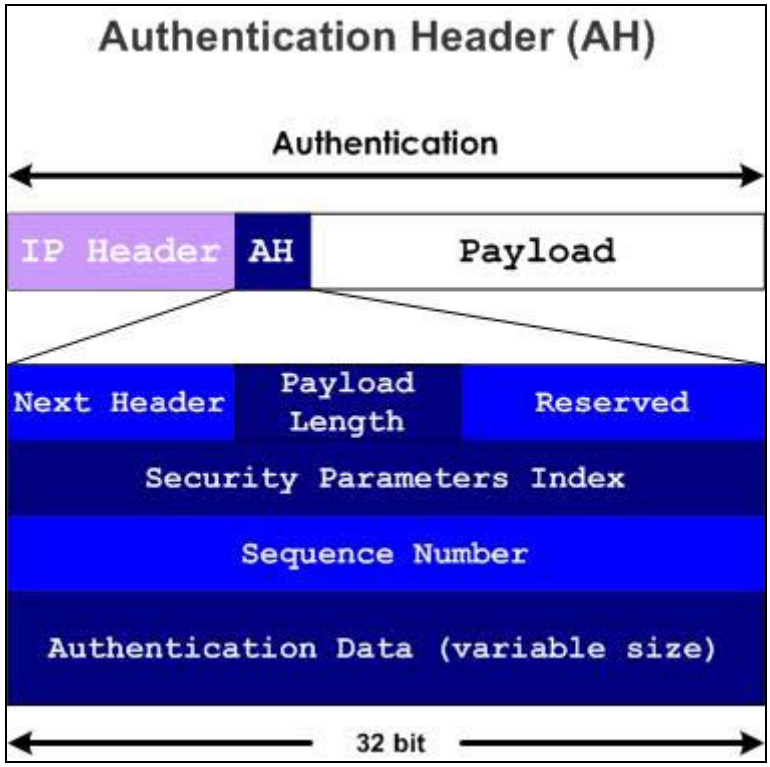
(Figure3-153) Transport Mode and Tunnel Mode

Figure 3-156 shows the structure of ESP Packet.



(Figure3-154) ESP Packet structure

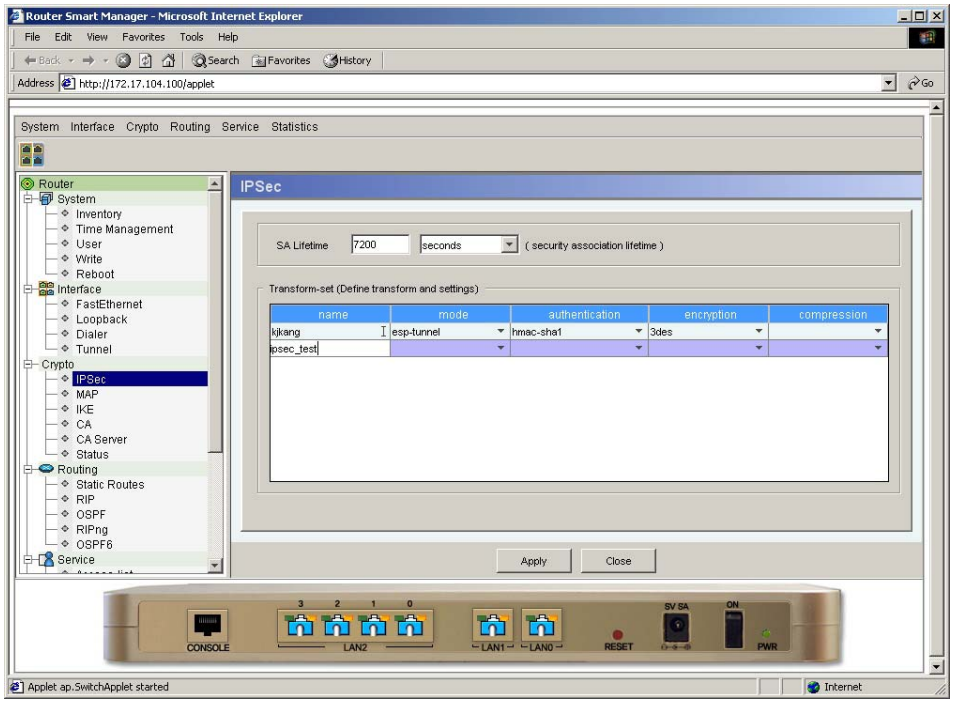
Figure 3-157 shows AH Packet structure.



(Figure3-155) AH Packet Structure

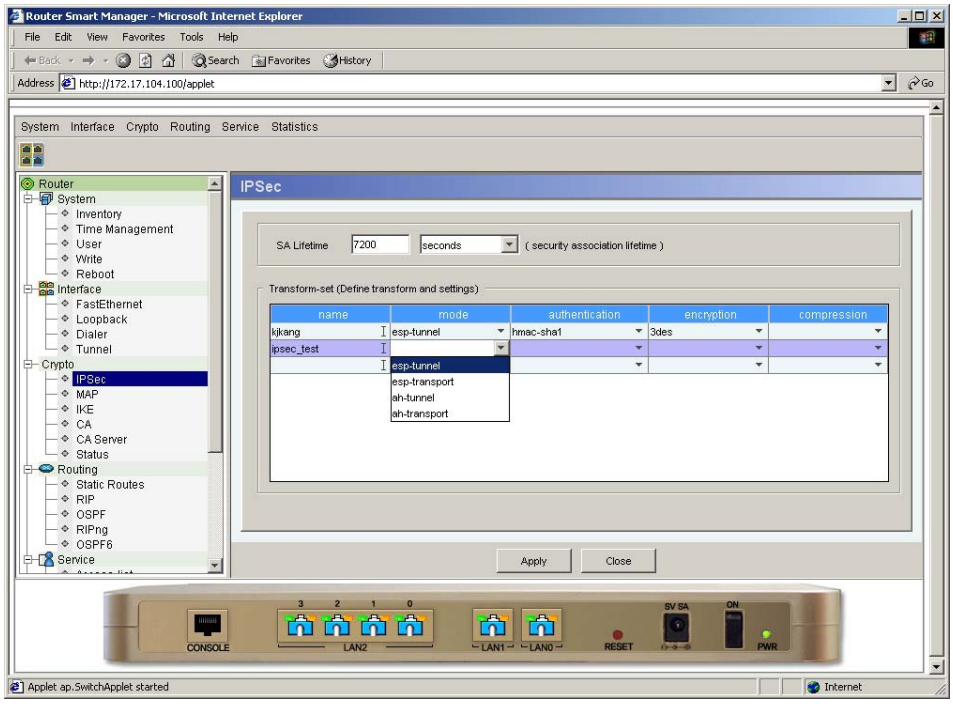
Figure 3-158 shows how to make IPSec Transform-set.

First, Input “ipsec_test” in the name field. You can make your own name. However, any spaces are not allowed in the name field.



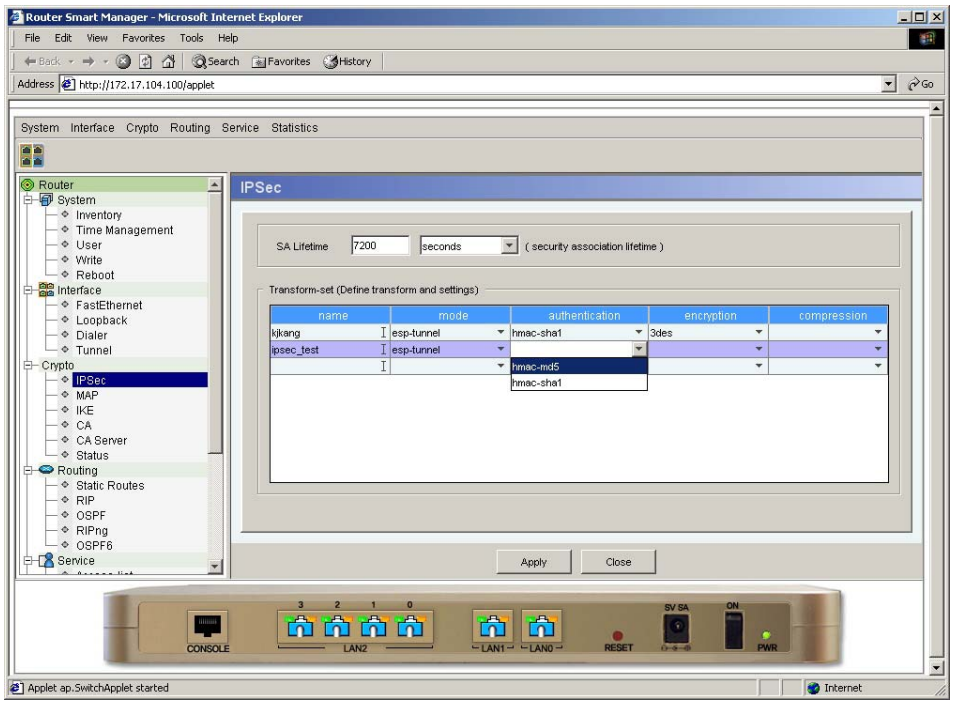
(Figure3-156) Input IPSec Transform-set name

Select “esp-tunnel” for IPSec Mode.



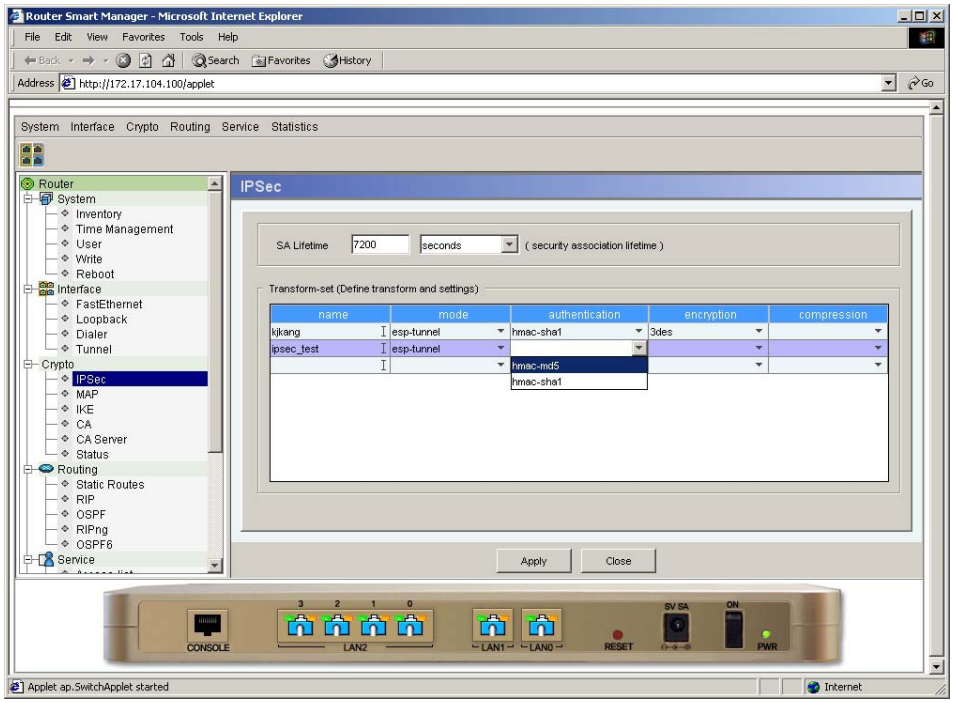
(Figure3-157) Select IPSec Transform-set Mode

Select “hmac-md5” for Data authentication algorithm.



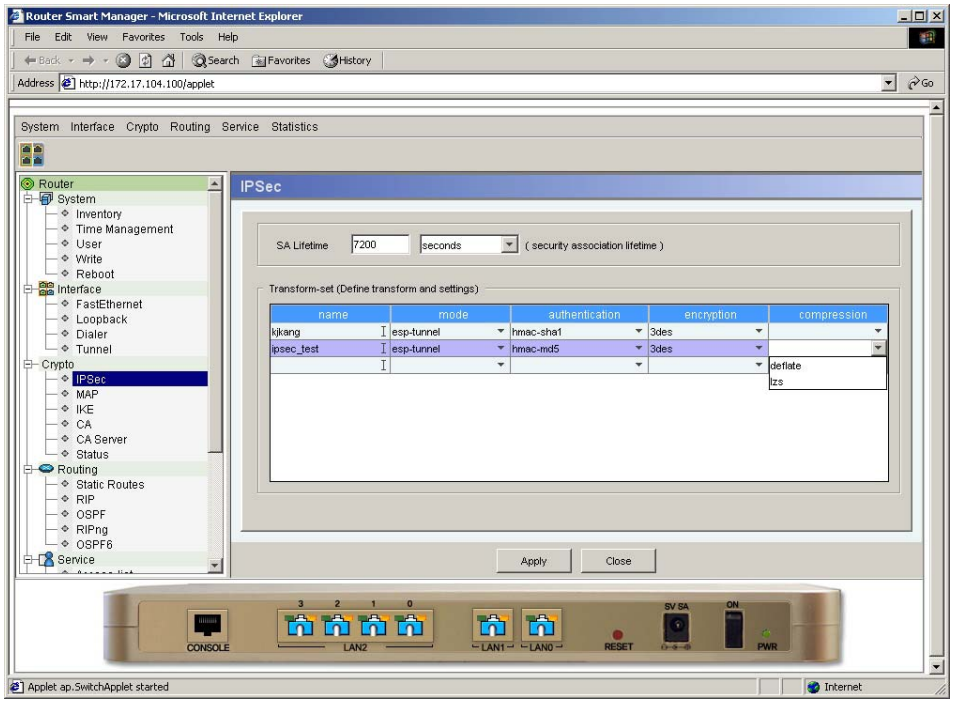
(Figure3-158) IPSec Authentication main page

Select “3des” for data encryption.



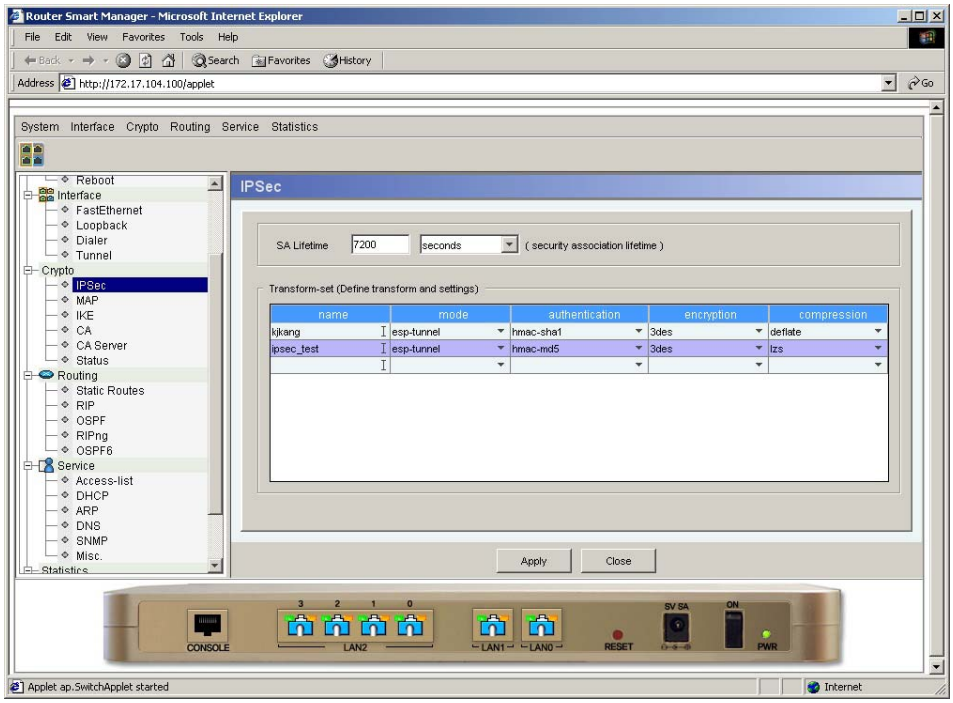
(Figure3-159) Select IPSec Encryption

Select “lzs” for data compression algorithm.



(Figure3-160) Select IPSec Data Compression

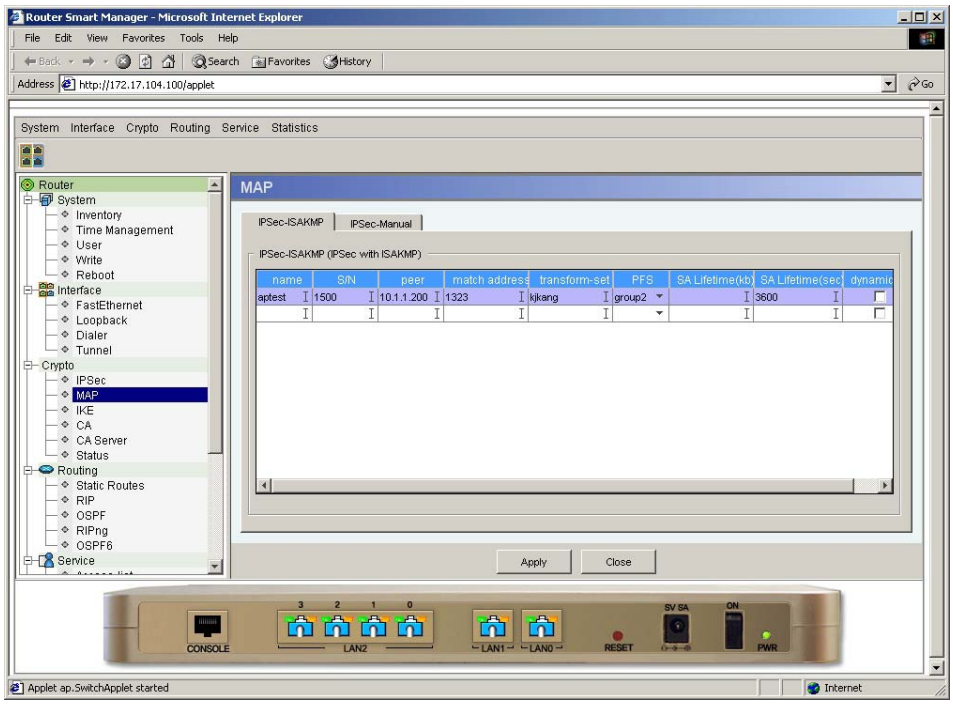
Click “Apply” to verify. Figure 3-163 will be shown.



(Figure3-161) Root Parameters configuration page

MAP

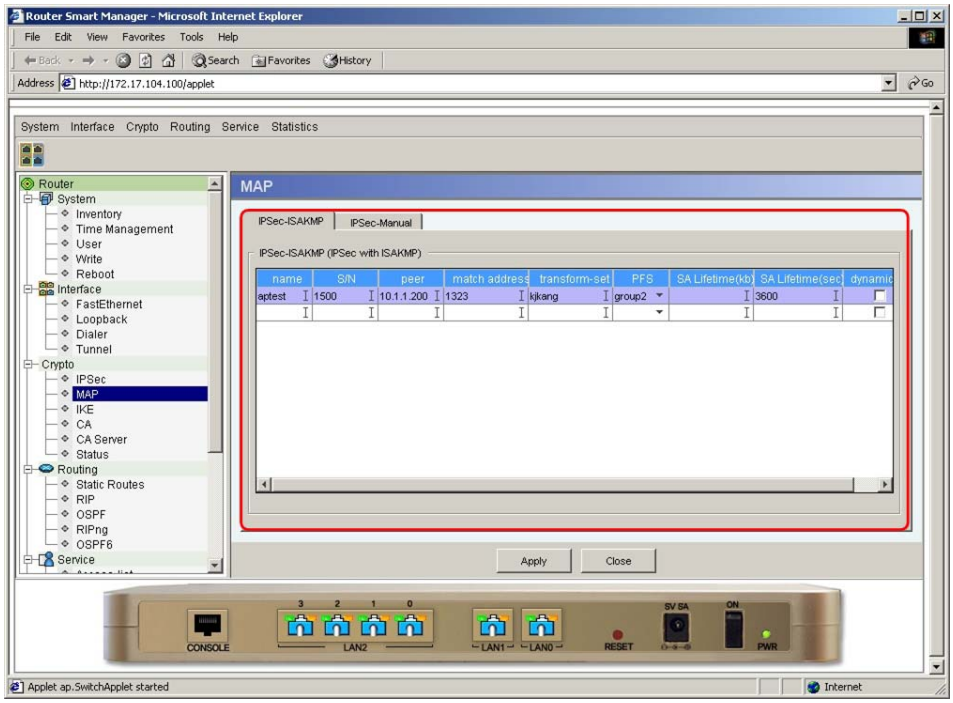
Virtual network can not be configured only with Transform-set from IPSec menu. You need to create a Map using Transform-set. The user can define session options for configuring virtual network.



(Figure3-162) Crypto MAP main page

There are two ways of creating Map. One is to use IKE Key creation algorithm and the other one is manually inputting the Key Values. The later one delivers high speed in data exchange than using IKE when configuring VPN. However, in the later one, if any one of the Key values is not matched with the other, problems can occur. So you need to be very careful on this.

<Table 3-27> shows IPSec-ISAKMP menu description.



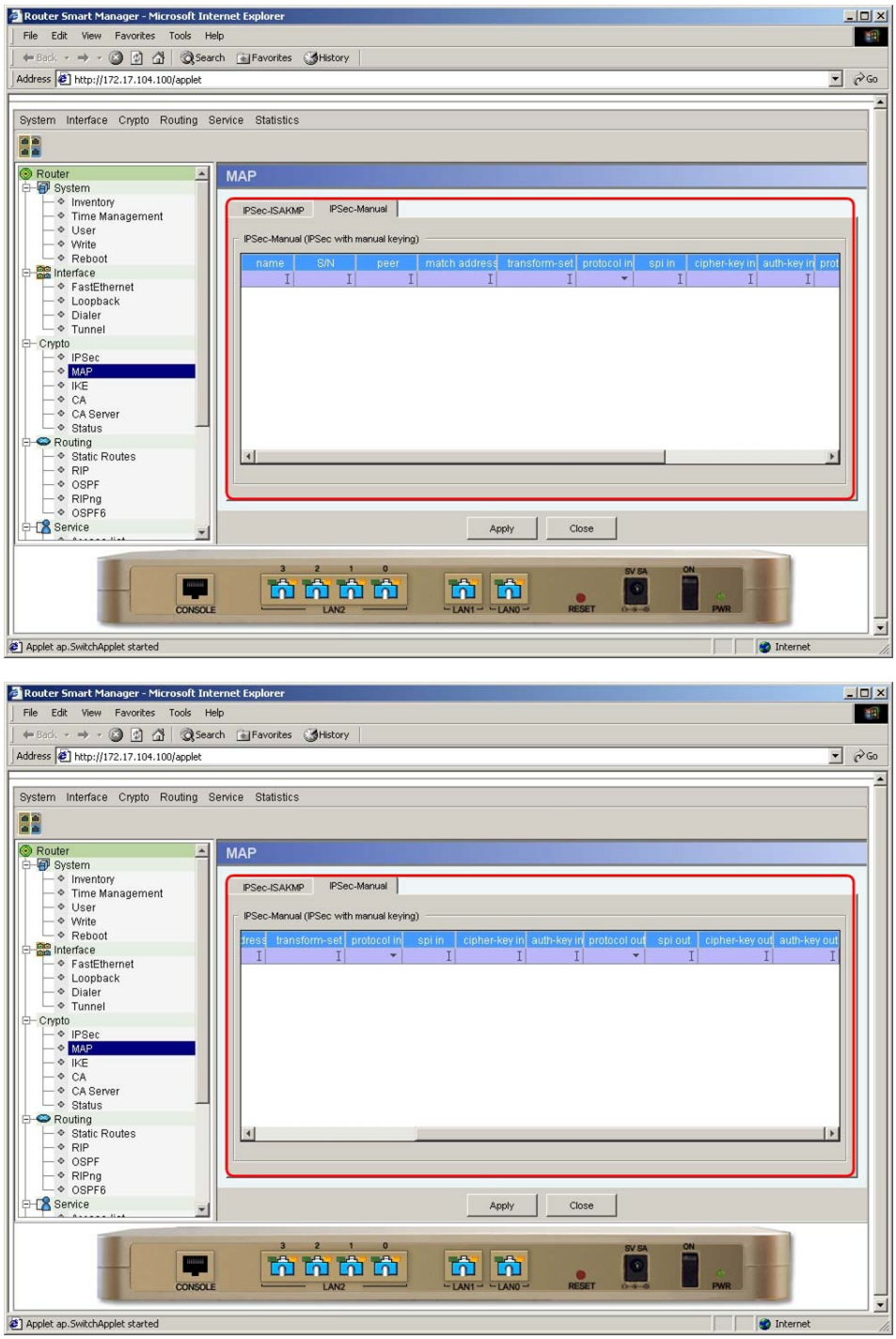
(Figure3-163) IPSec-ISAKMP Menu

<Table 3-27> IPSec-ISAKMP Menu Description

Elements	Description
Name	Define name of the Map
S/N	Sequence Number. It gives priority among many maps.
Peer	Input IP Address of Peer Interface.
Match Address	Input tag number of Access-List. When Map is applied to the Interface, only Packets in Access-List are secured by IPSec Transform-set.
Transform-set	Input Transform-set from IPSec menu.
PFS	Define Diffie-Hellman group. Diffie-Hellman group is an algorithm about creation of public key/private key.

	There are 3 groups (Group1, 2, 5). Group1 is the fastest but with less complexity of encryption and Group5 has excellent algorithm complexity but with slow speed. Therefore Gruop2 is recommended.
SA Lifetime (Kilobytes)	The unit is "Kilobytes"
SA Lifetime (Seconds)	Set Life time of Configured Map. The unit is "Seconds"
Dynamic	On Aggressive Mode, Peer which uses Fixed IP Address checks Dynamic Field.

<Table 3-28> shows IPSec-Manual menu.

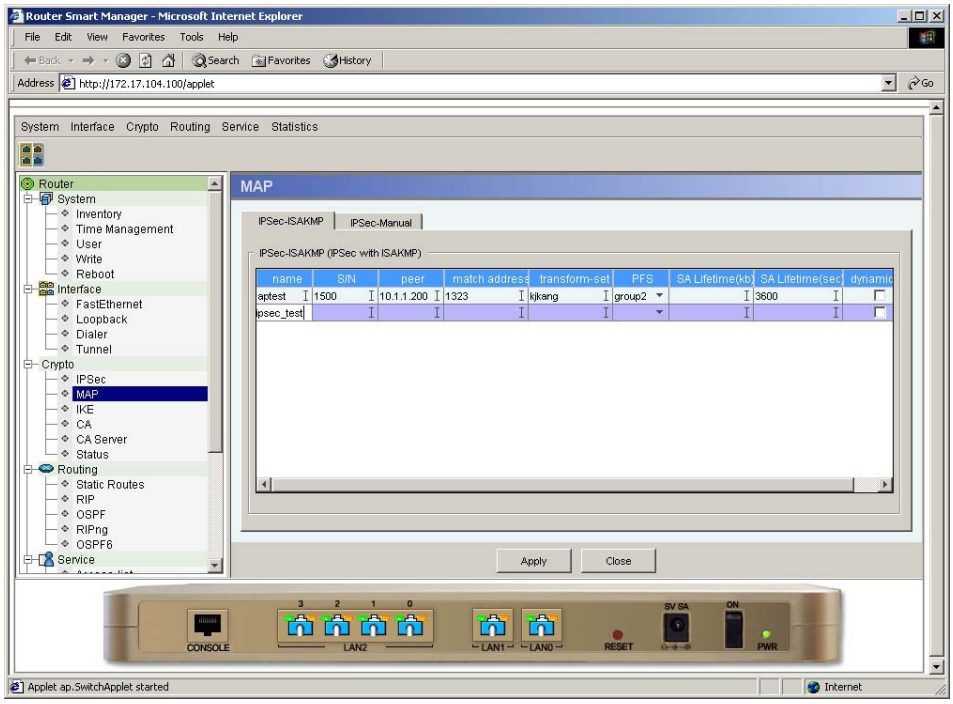


(Figure3-164) IPSec-Manual menu page

<Table 3-28> IPSec-Manual menu Description

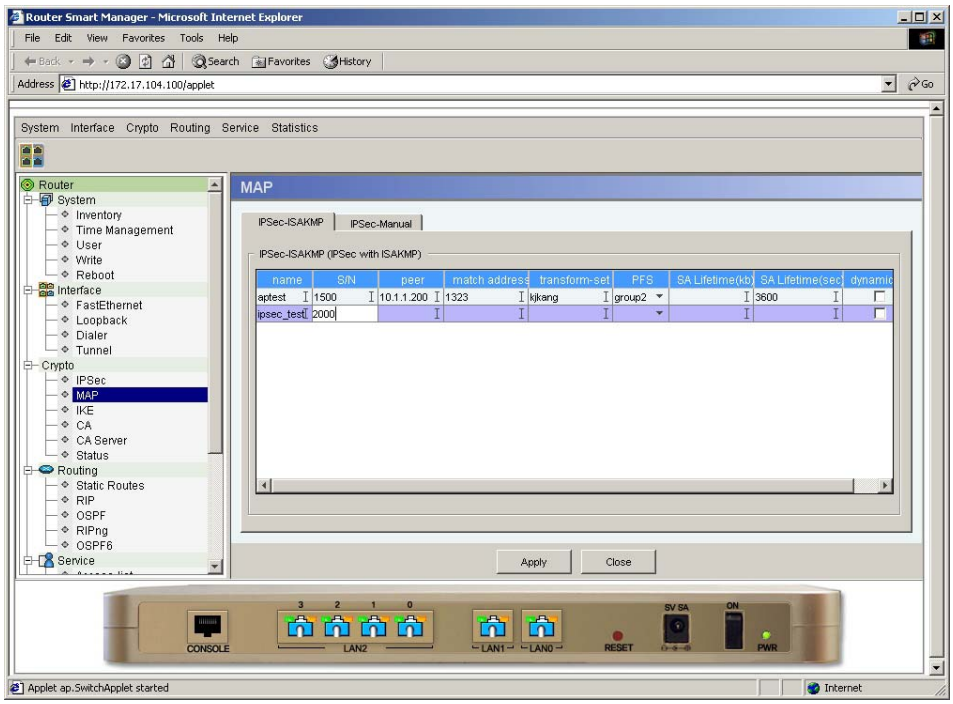
Elements	Description
Name	Define name of the Map
S/N	Sequence Number. It gives priority when there are many maps.
Peer	Input IP Address of Peer Interface
Match Address	Input tag number of Access-List. When Map is applied to Interface, only Packets in Access-List are secured by IPSec Transform-set.
Transform-set	Input Transform-set from IPSec menu.
Protocol in	Define IPSec Protocol for receiving. Select "esp" for esp, "ah" for ah for defined protocols in Transform-set.
Spi in	Defines Security Parameter Index value when receiving. Spi sets the values for opposite Peer. If the Spi value of Peer A is 1000, then the Spi value of PeerB has to be 1000 as well. Also user can define its own value in between 256~4294967295.
Cipher-key in	Defines (16 decimal format) session key for receiving. Select key value from authentication on Transform-set, authentication algorithm. DES : 8 Bytes, 3DES : 24Bytes, AES : 16 Bytes
Auth-key in	When "esp" and "ah" is used together, Input the authentication key value for sending.
Protocol out	Define IPSec Protocol for sending. Select "esp" for esp, "ah" for ah for defined protocols in Transform-set.
Spi out	Security Parameter Index when sending. Spi sets the values for opposite Peer. If the Spi value of Peer A is 1000, then the Spi value of PeerB has to be 1000 as well. Also user can define its own value in between 256~4294967295.
Cipher-key out	Defines (16 decimal format) session key for sending. Select key value from authentication on Transform-set, authentication algorithm. DES : 8 Bytes, 3DES : 24Bytes, AES : 16 Bytes
Auth-key out	When "esp" and "ah" is used together, Input the authentication key value for receiving.

Figure 3-167 shows how to create the map with a name of “ipsec_test”. First, Input “ipsec_test” in the name field.



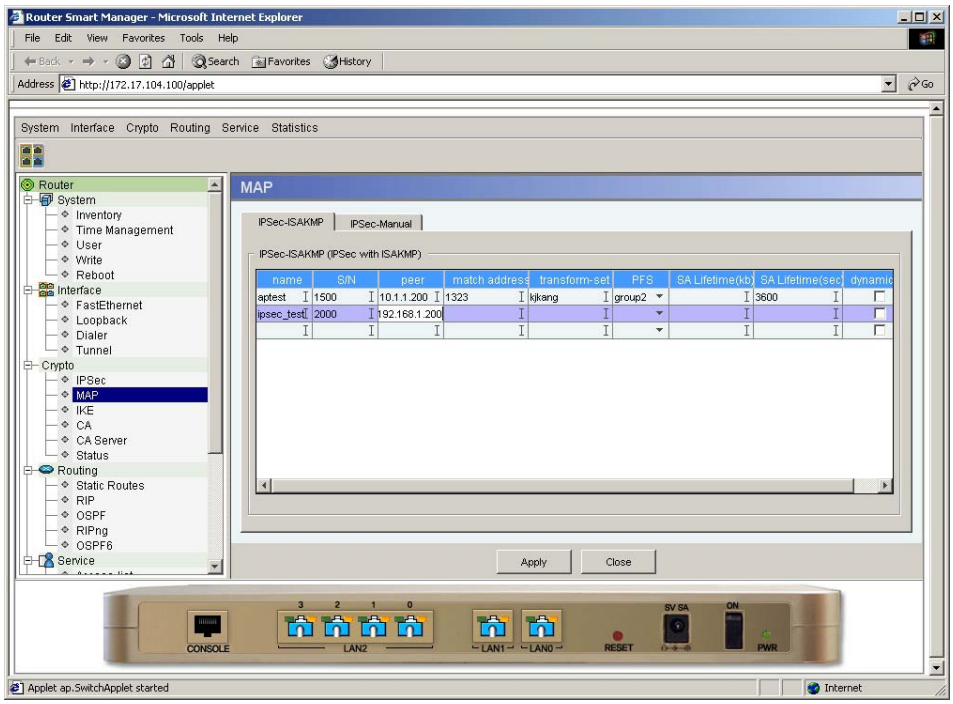
(Figure3-165) Input IPSec-ISAKMP Name

Input “2000” for Sequence Number.



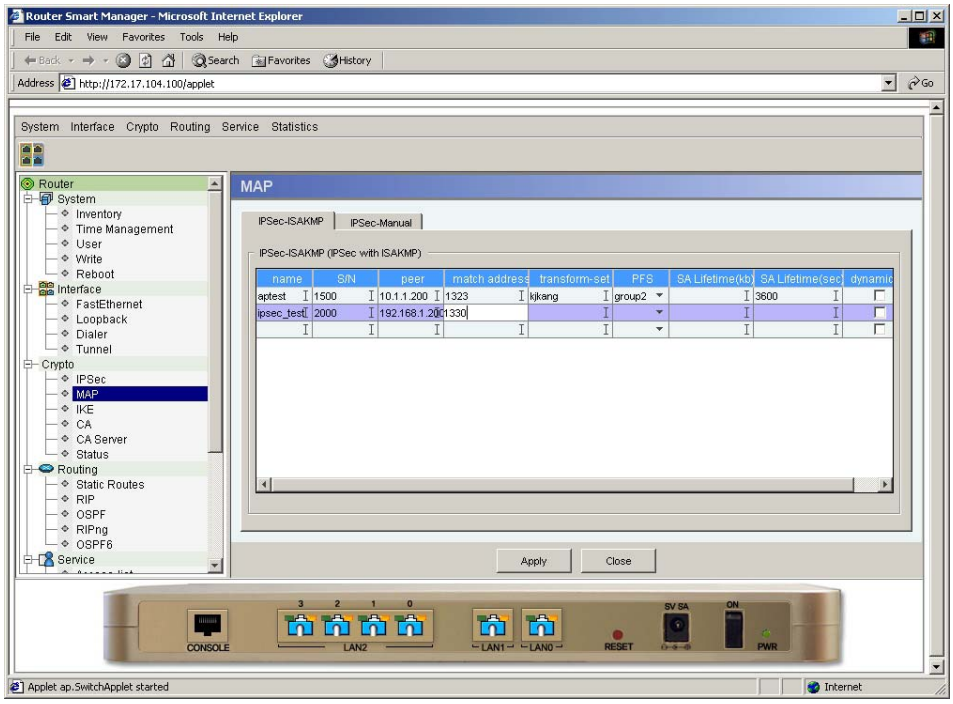
(Figure3-166) Input IPSec-ISAKMP S/N

Input “192.168.1.200” for IP Address of Peer Interface.



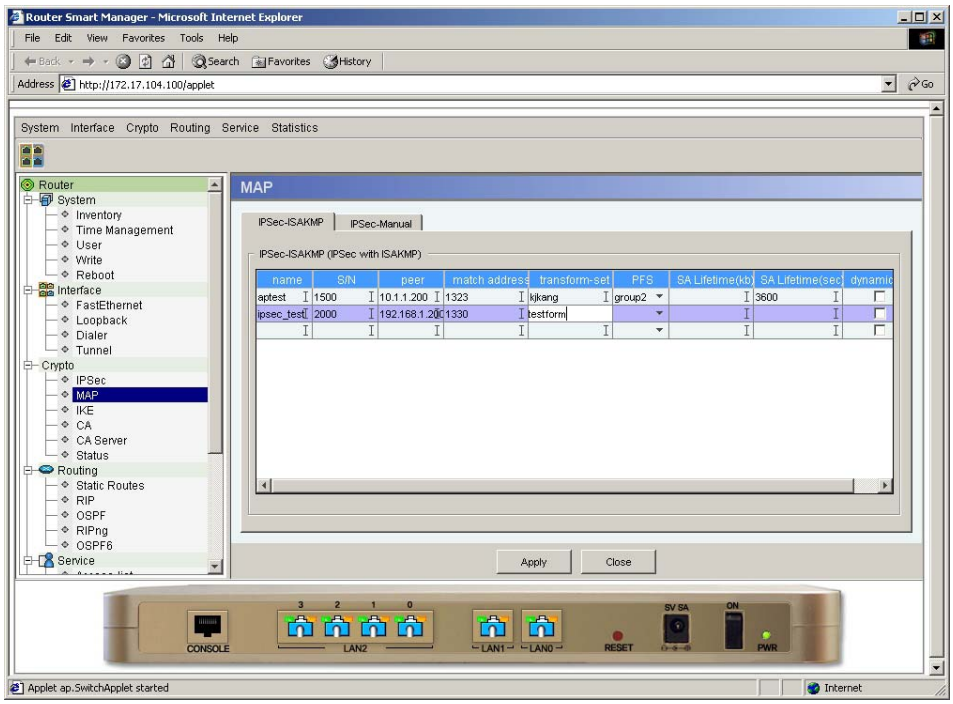
(Figure3-167) Input IPSec-ISAKMP Peer Address

Input “1300” for tag number of Access-List which has secured packet information.



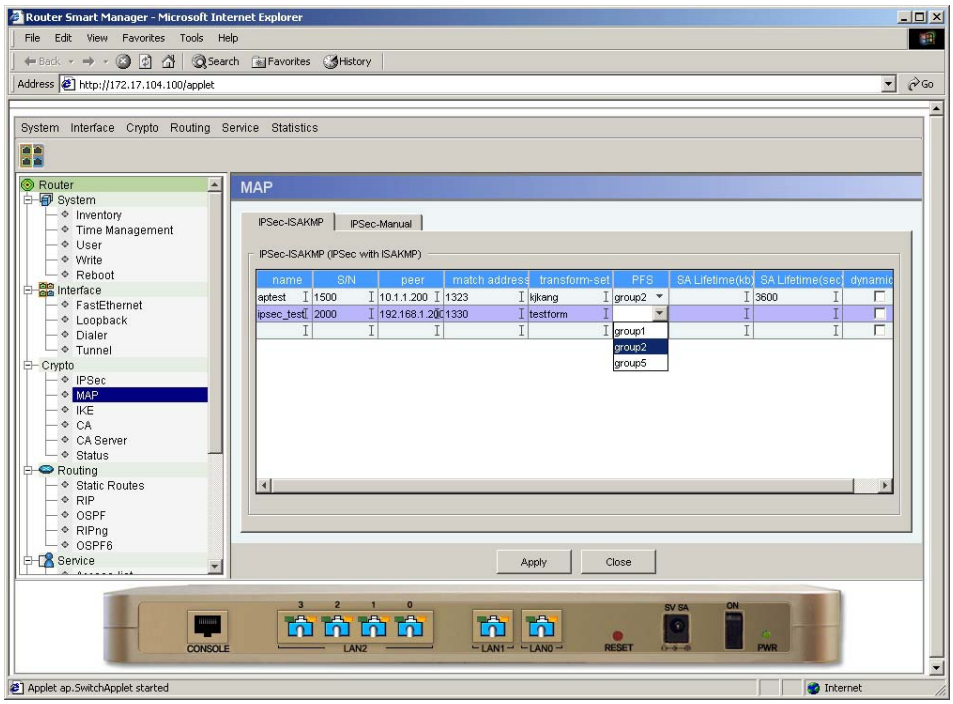
(Figure3-168) Input IPSec-ISAKMP Match Address

Input Transform-set "testform" which is created from IPSec.



(Figure3-169) Input IPSec-ISAKMP Transform-set

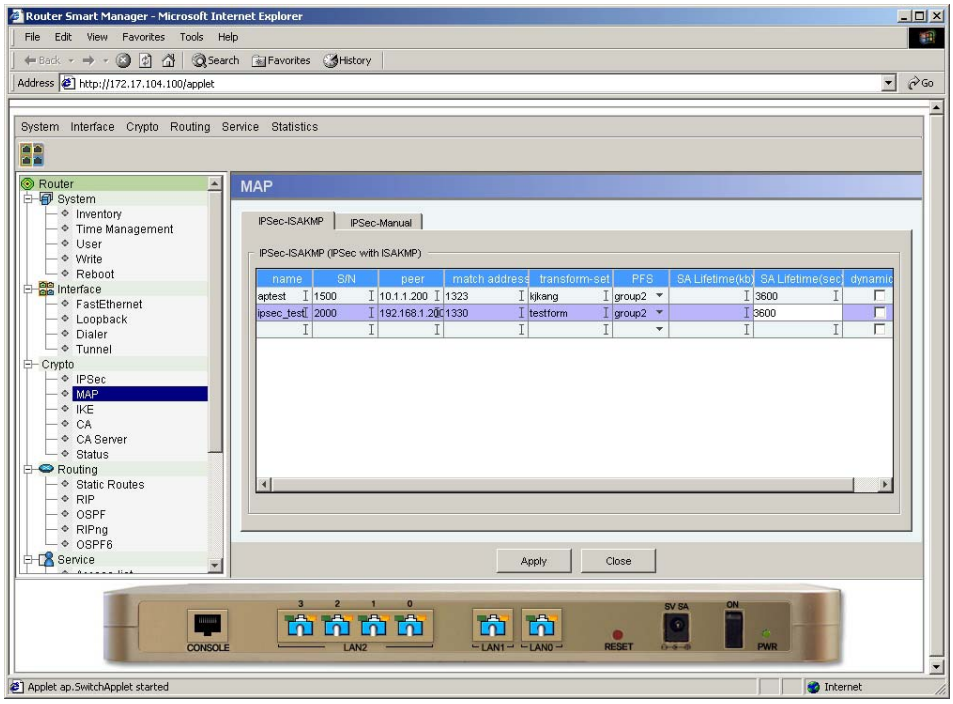
Select Diffie-Hellman Group "2"



(Figure3-170) Select IPSec-ISAKMP Diffie-Hellman Group

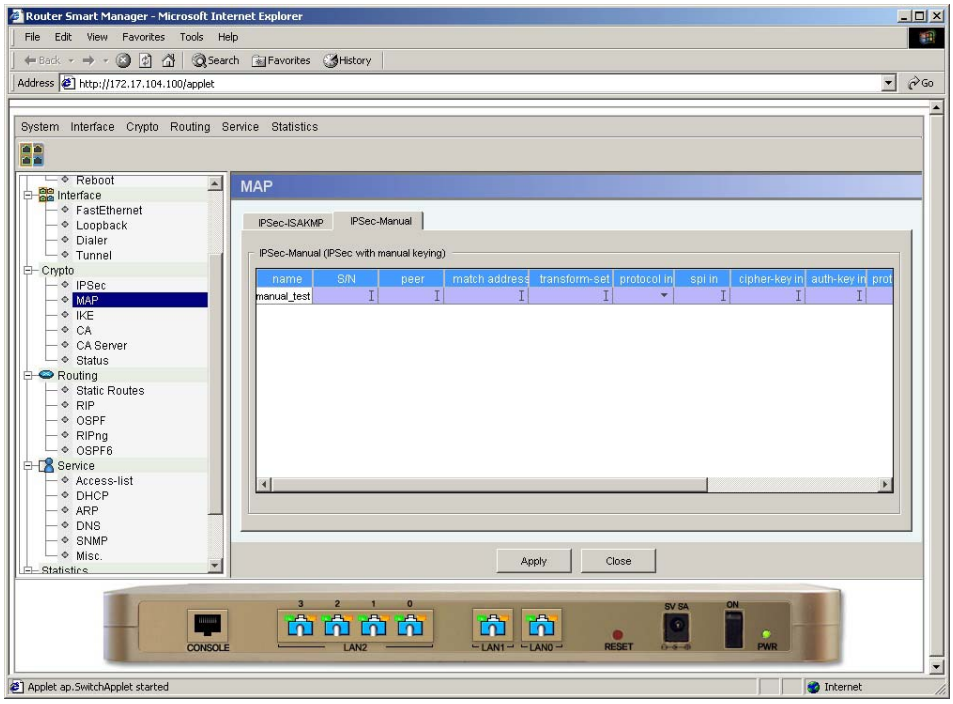
Set SA Lifetime to 3600 second.

Click “Apply” to create a Map named “ipsec_test”.



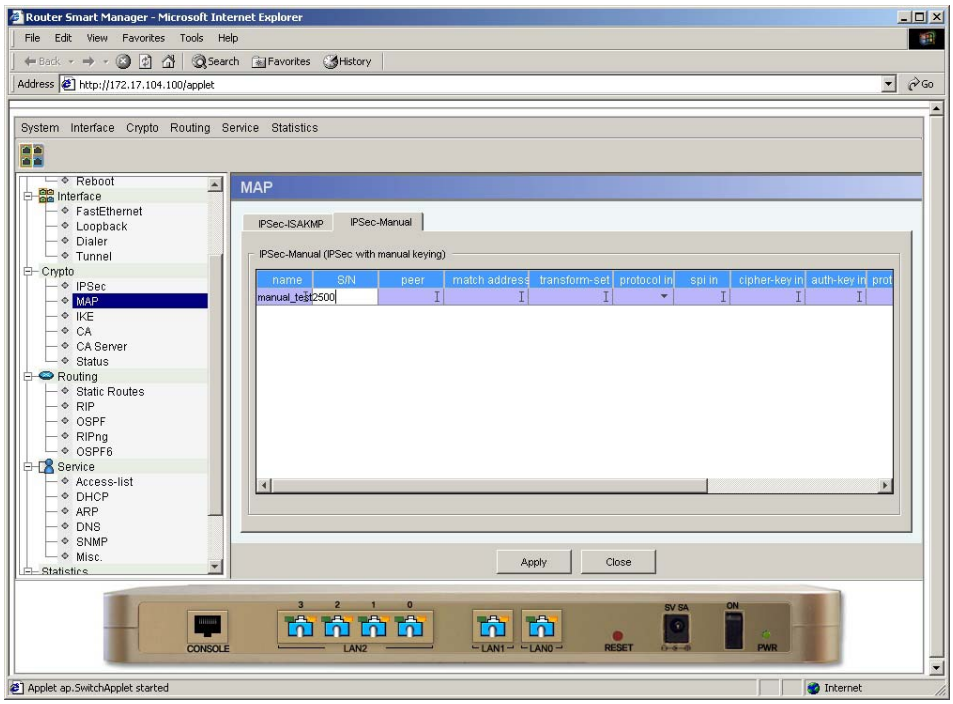
(Figure3-171) Input IPSec-ISAKMP SA Lifetime

Figure 3-174 shows how to create a Map named “manual_test” using IPSec-Manual menu. Input “manual_test” in the name field..



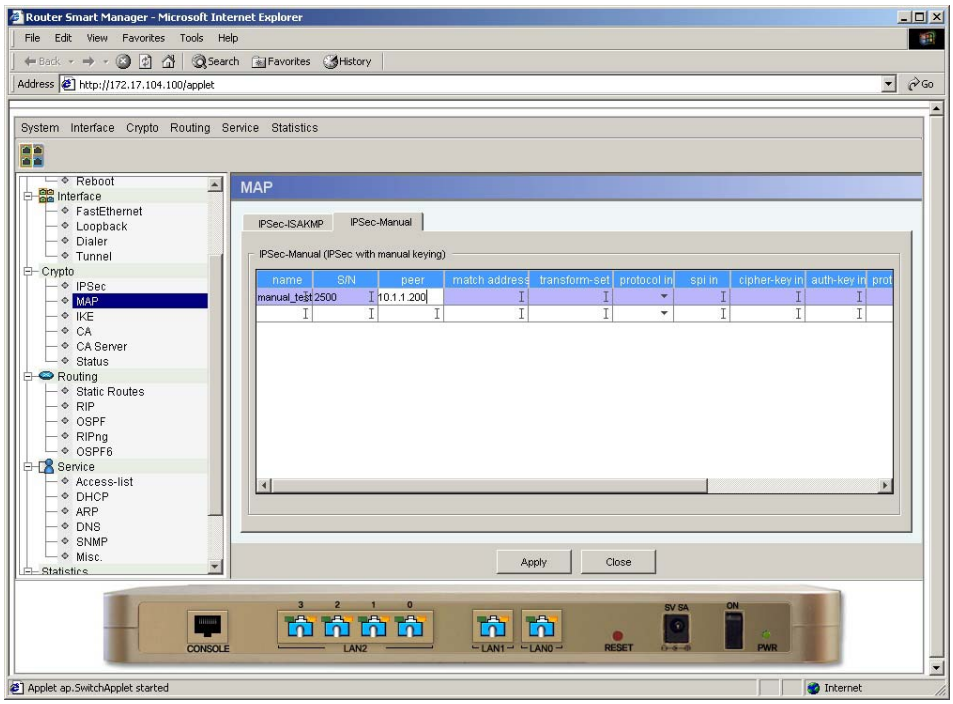
(Figure3-172) Input IPSec-Manual Name

Input “2500” for Sequence Number.



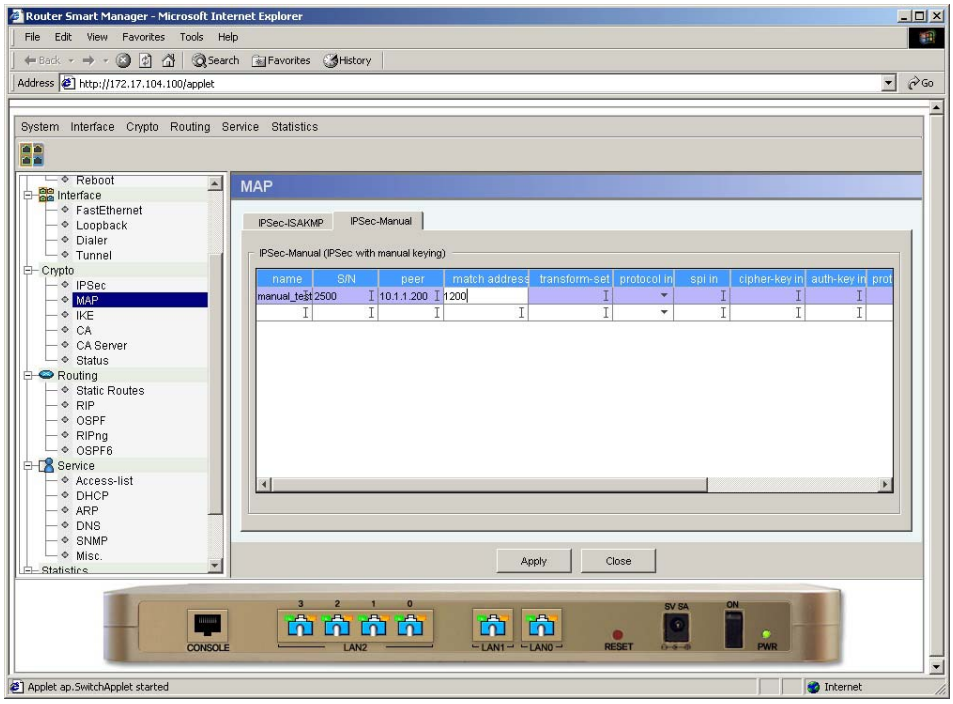
(Figure3-173) Input IPSec-Manual S/N

Input “10.1.1.200” for IP Address of Peer Interface.



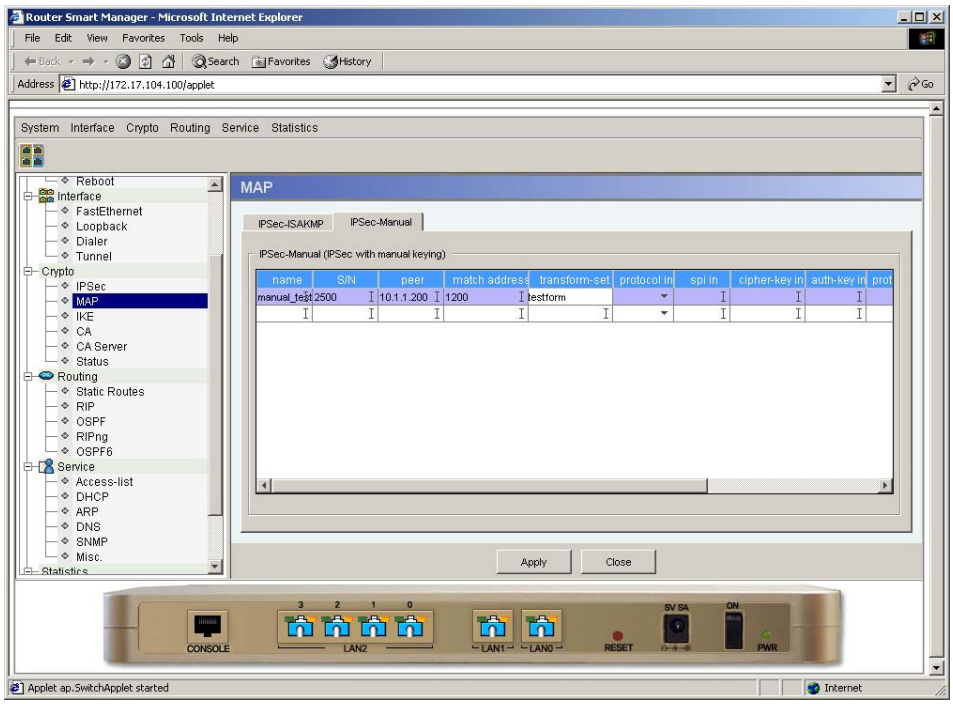
(Figure3-174) Input IPSec-Manual Peer Address

Input “1200” for the tag number of Access-List which has secured Packet info.



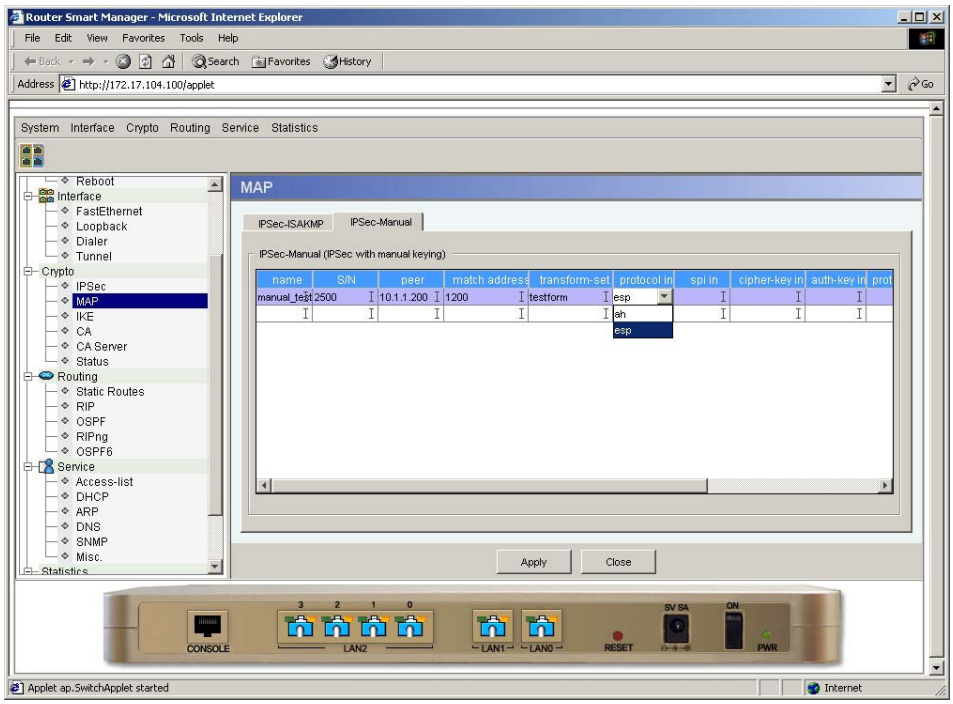
(Figure3-175) Input IPSec-Manual Match Address

Input Transform-set "testform" which is created from IPSec menu.



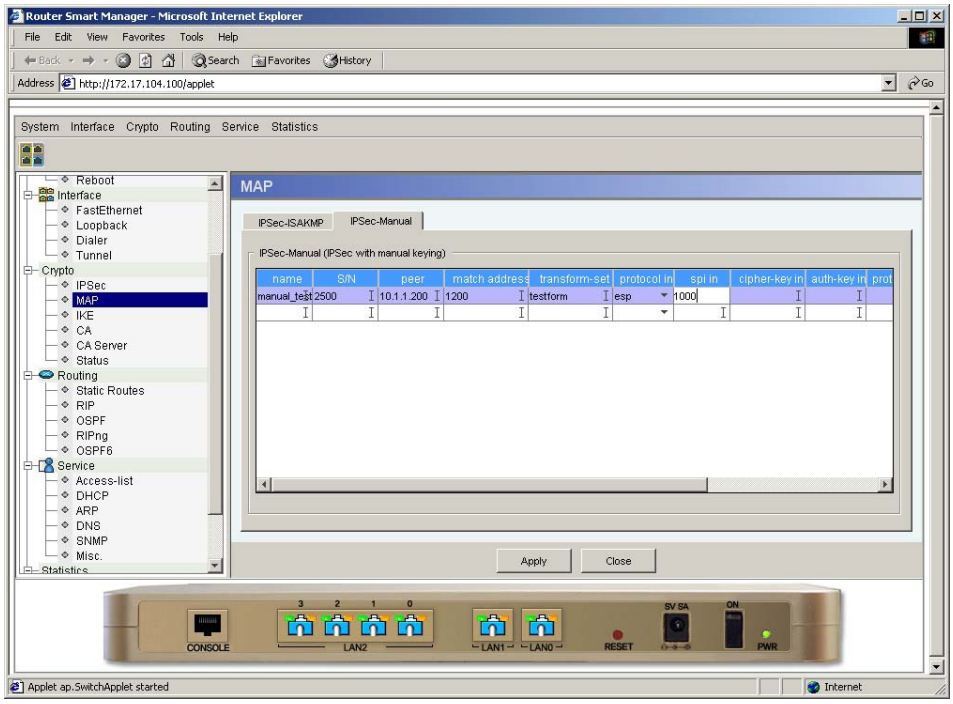
(Figure3-176) Input IPSec-Manual Transform-set

Select protocol "esp" to use for Inbound IPSec session.



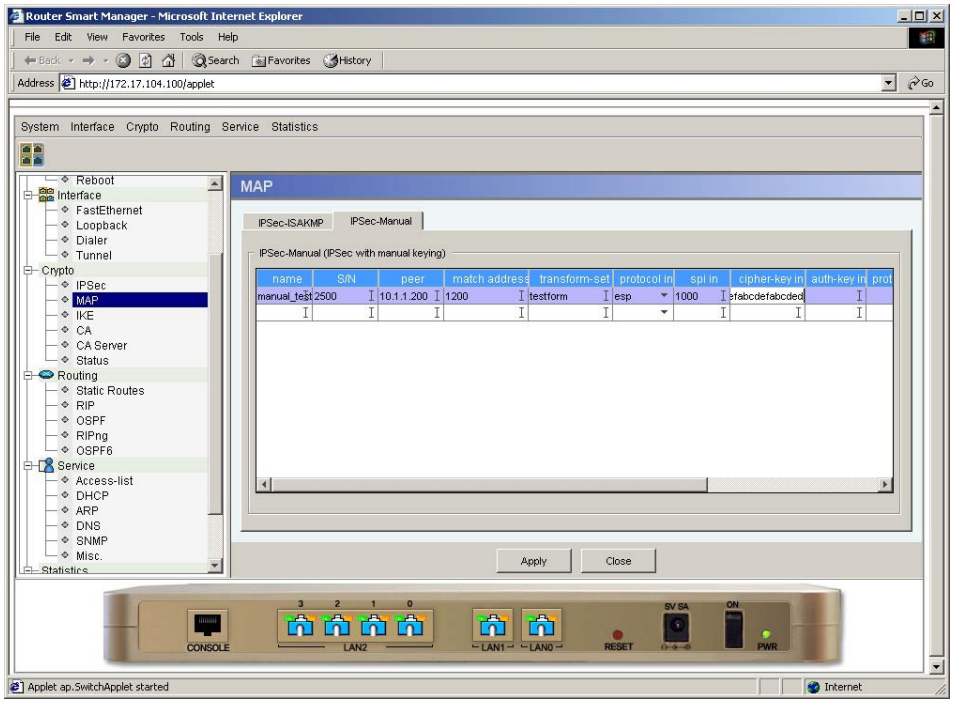
(Figure3-177) Select IPSec-Manual Protocol in

Input SPI in “1000” for Inbound IPSec session. It has to be the same value as the value in SPI out of the Peer.



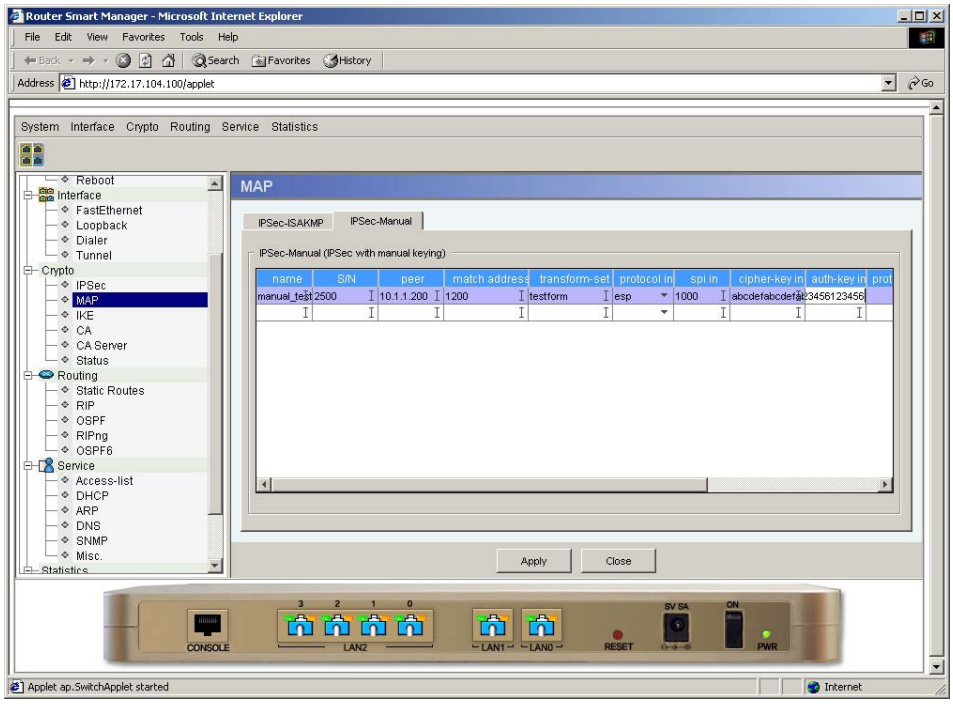
(Figure3-178) Input IPSec-Manual Spi in

Input 24 byte Hex value for Cipher-key to use in Inbound IPSec session. This has to be the same value as the value in Cipher-key out of the Peer.



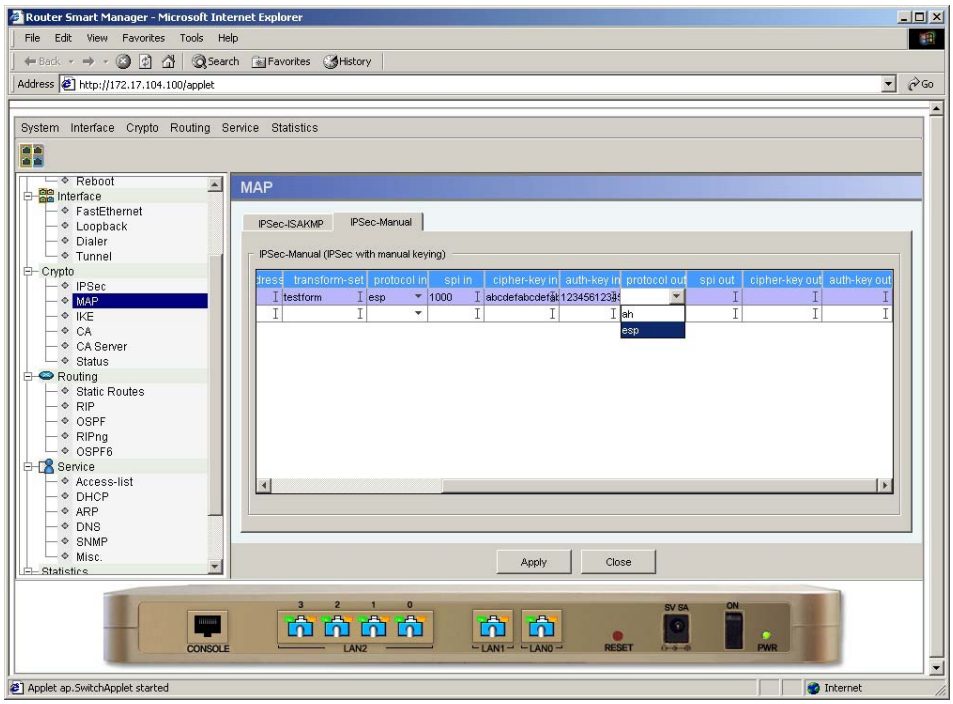
(Figure3-179) Input IPSec-Manual Cipher-key in

Input Inbound Authentication-key for IPSec session. This has to be the same value as the value in Authentication-key out of the Peer.



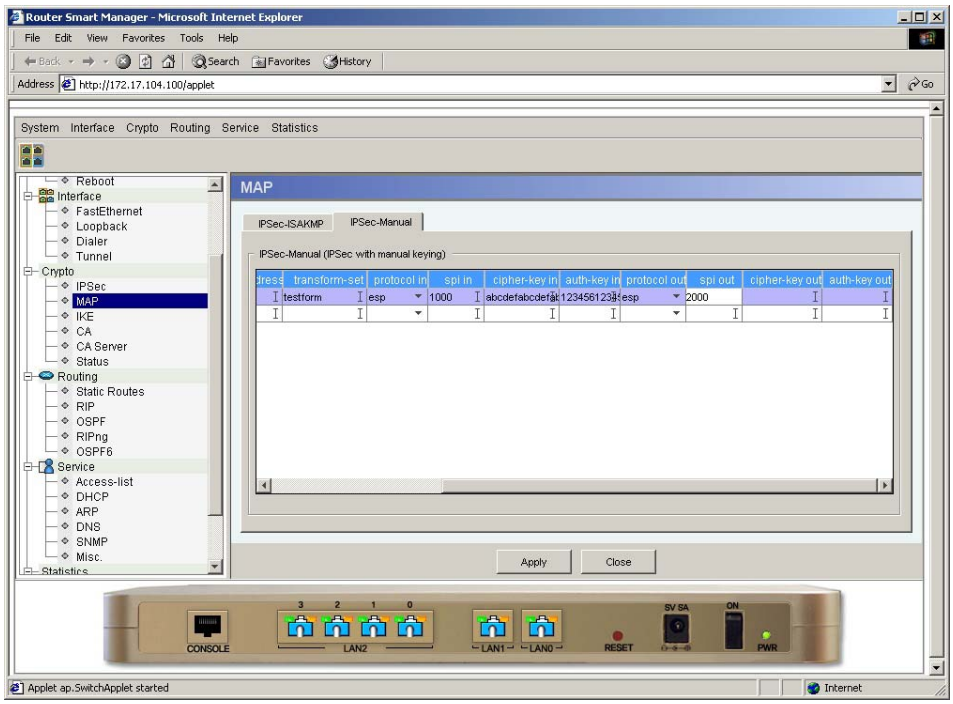
(Figure3-180) Input IPSec-Manual Auth-key in

Select protocol "esp" to use in Outbound IPSec session.



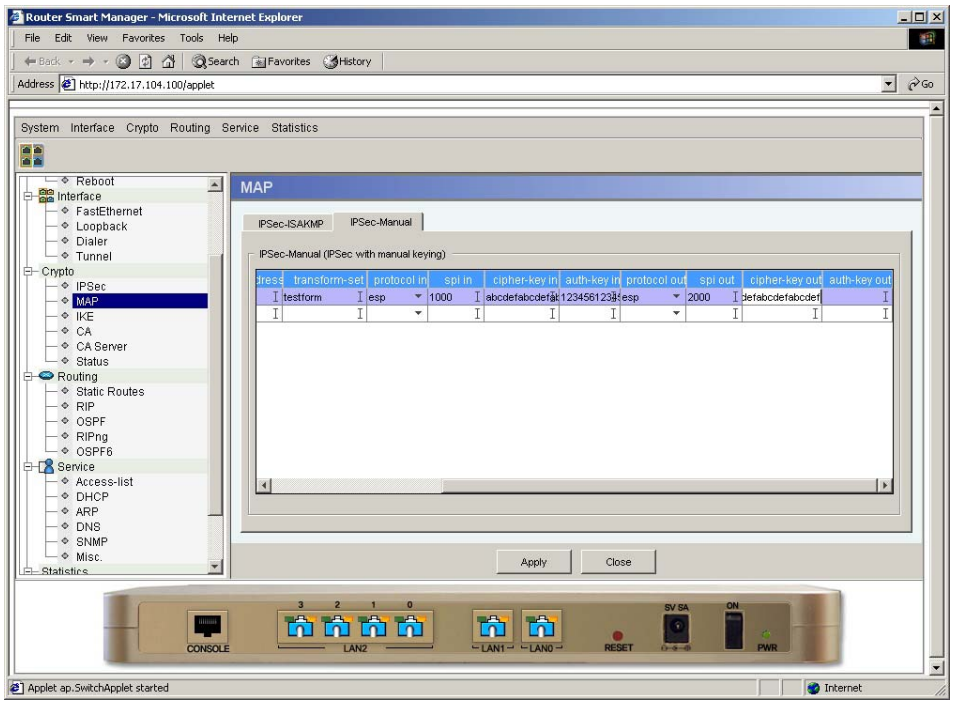
(Figure3-181) Select IPSec-Manual Protocol out

Input SPI out “2000” for outbound IPSec session. It has to be the same value as the value in SPI in of the Peer.



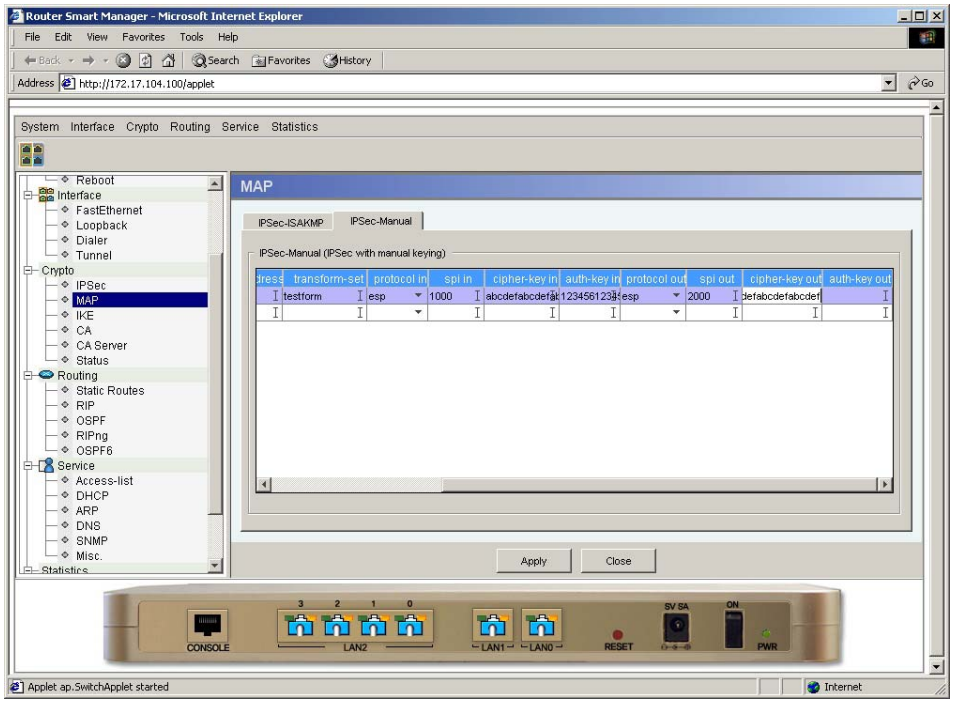
(Figure3-182) Input IPSec-Manual Spi out

Input 24 byte Hex value for Cipher-key to use in outbound IPSec session. This has to be the same value as the value in Cipher-key in of the Peer



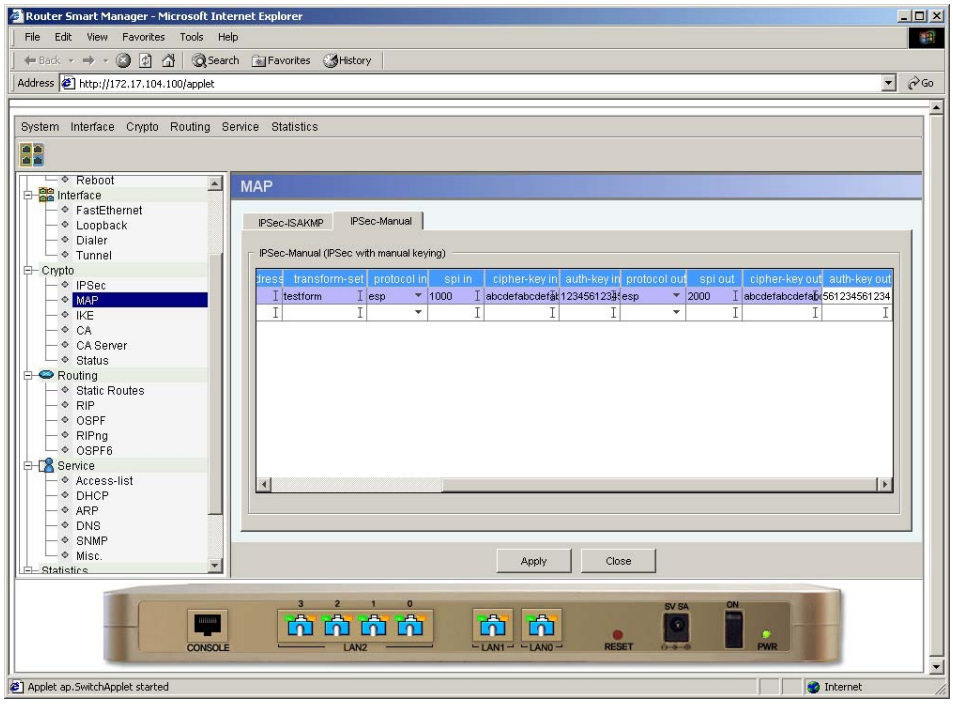
(Figure3-183) Input IPSec-Manual Cipher-key out

Input 24 byte Hex value for Cipher-key to use in outbound IPSec session. This has to be the same value as the value in Cipher-key of the Peer.



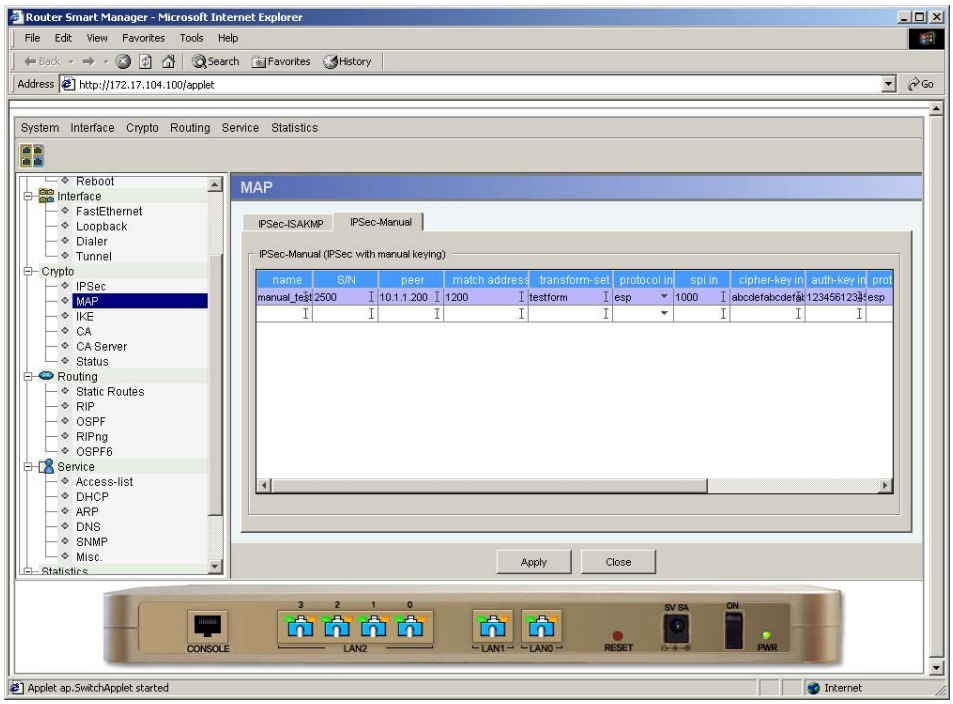
(Figure3-184) Input IPSec-Manual Cipher-key out

Input Authentication-key value to use in outbound IPSec session. This has to be the same value as the value in Authentication-key of the Peer.



(Figure3-185) Input IPSec-Manual Auth-key out

Click “Apply” to verify.

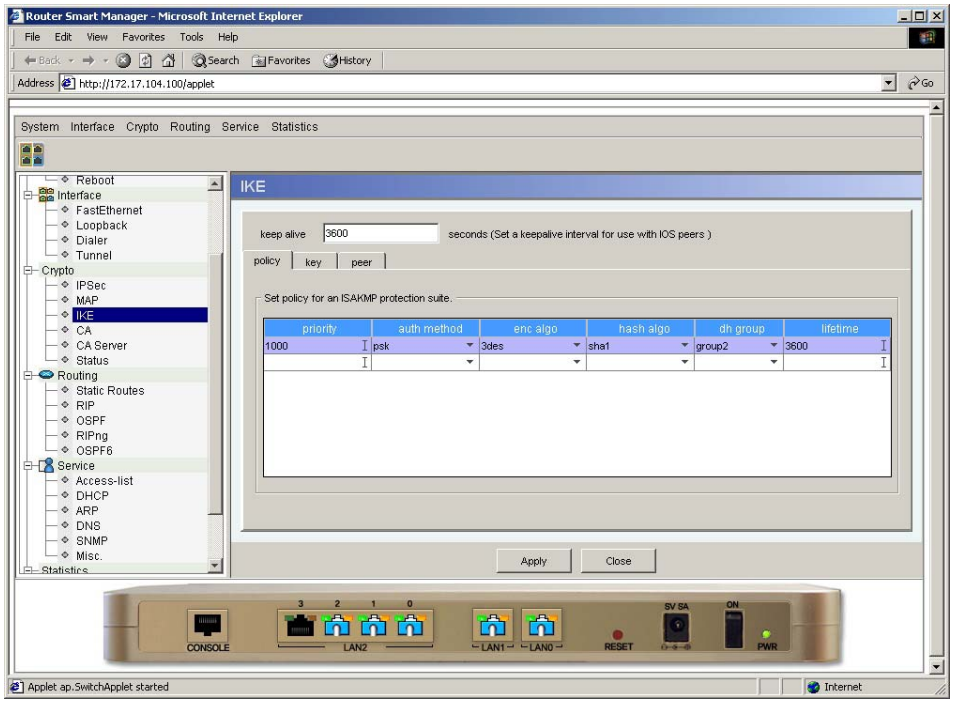


(Figure3-186) Verify IPSec-Manual settings

IKE

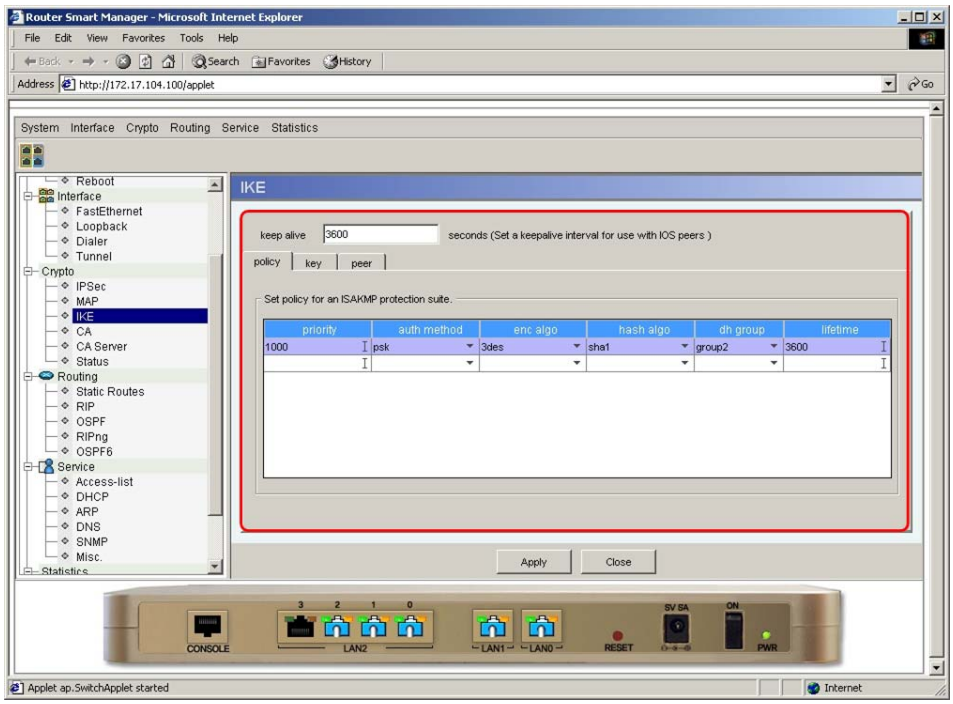
IKE (Internet Key Exchange) is a protocol which provides and negotiates securely authenticated key data in order to have Security Association. IKE is different from ISAKMP. ISAKMP only provides key exchange common frame work which can be used by any key exchange protocols while IKE defines actual key exchange. IKE provides key information so that other factors of IPSec can create encryption and authentication keys.

IKE menu consists of Policy, Key, and Peer.



(Figure3-187) IKE Policy Main page

Table 3-29 describes each element of IKE Policy menu.



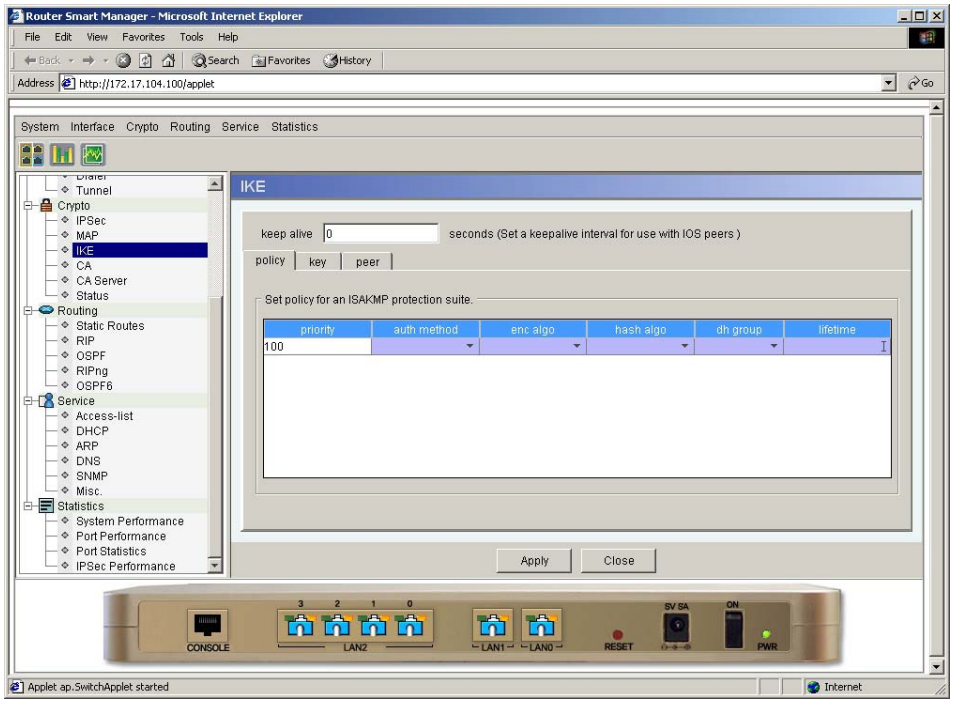
(Figure3-188) IKE Policy Menu

<Table 3-29> IKE Policy menu Discription

Elements	Description
Priority	It sets priority on IKE Policy. Choose from 1 to 10000. Lower number has high priority.
Auth Method	It decides Peer authentication method. There are Psk (Preshared Key) and rsasig (RSA Signature).
Enc Algo	It decides encryption algorithm for message. Select one from 3des, blowfish, aes, cast.
Hash Algo	It selects an algorithm authenticates data integrity. Choose one from md5, sha1.
Dh Group	It decides Diffie-Hellman Group. choose one from Group1, Group2 and Gruop5
Lifetime	It decides lifetime of IKE Policy.

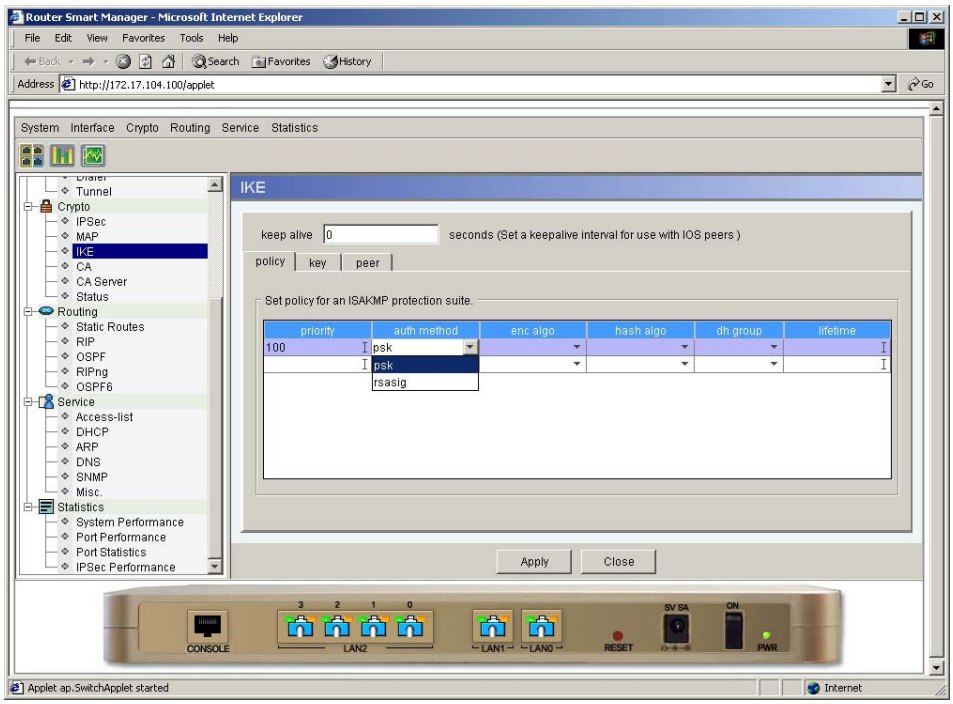
Figure 3-191 shows how to create a Policy.

First, input “100” in Priority field.



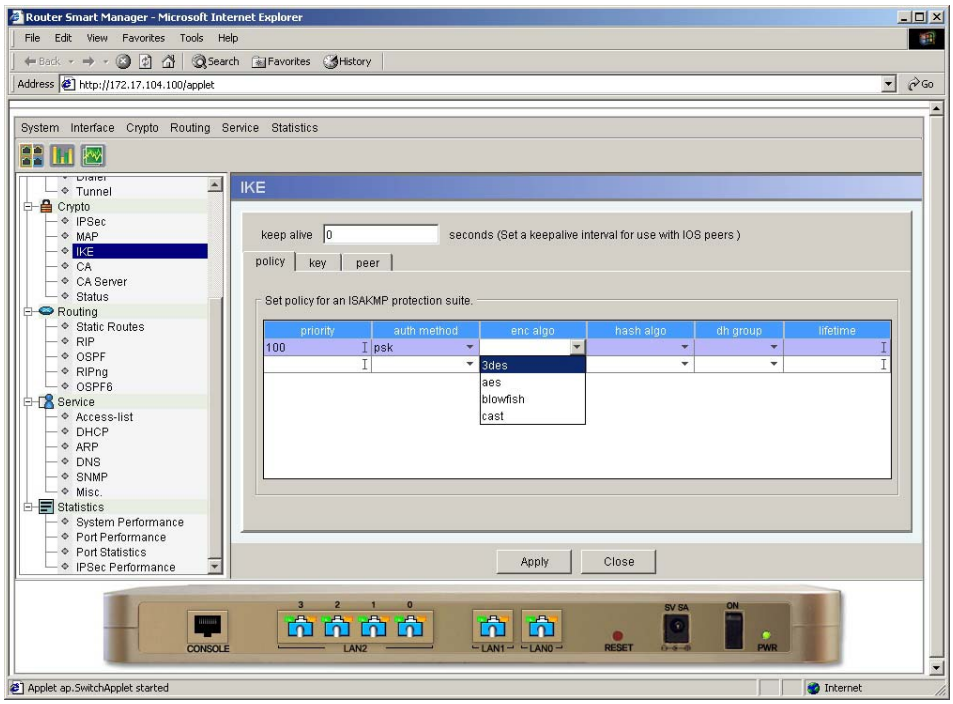
(Figure3-189) Input IKE Policy Priority

Select psk (Preshared Key) for Authentication Method.



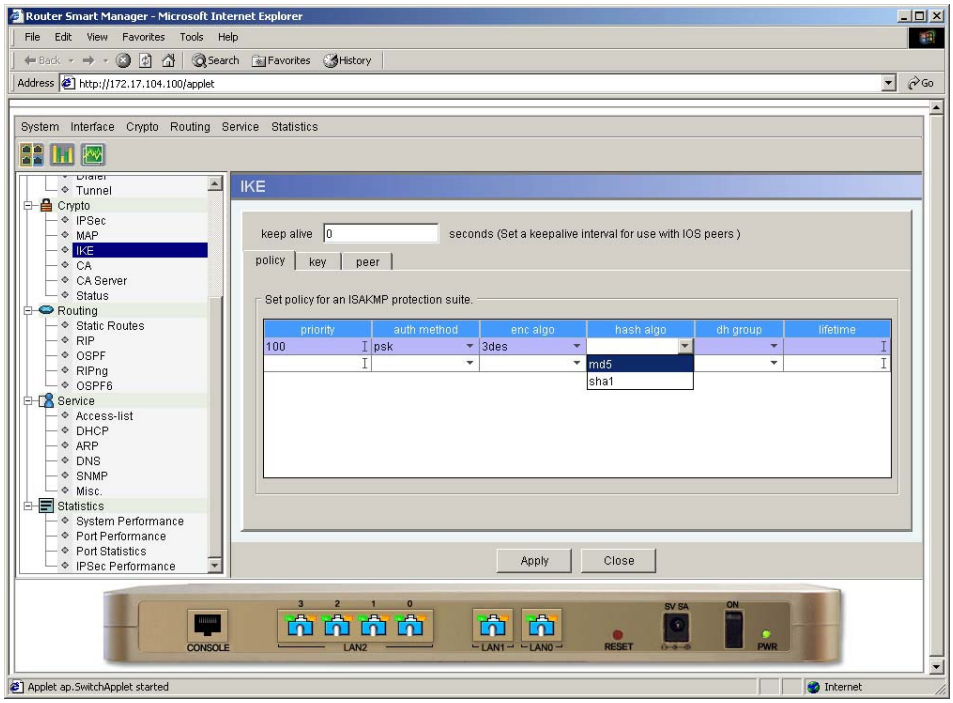
(Figure3-190) Select IKE Policy Authentication Method

Select 3des for Encryption Algorithm.



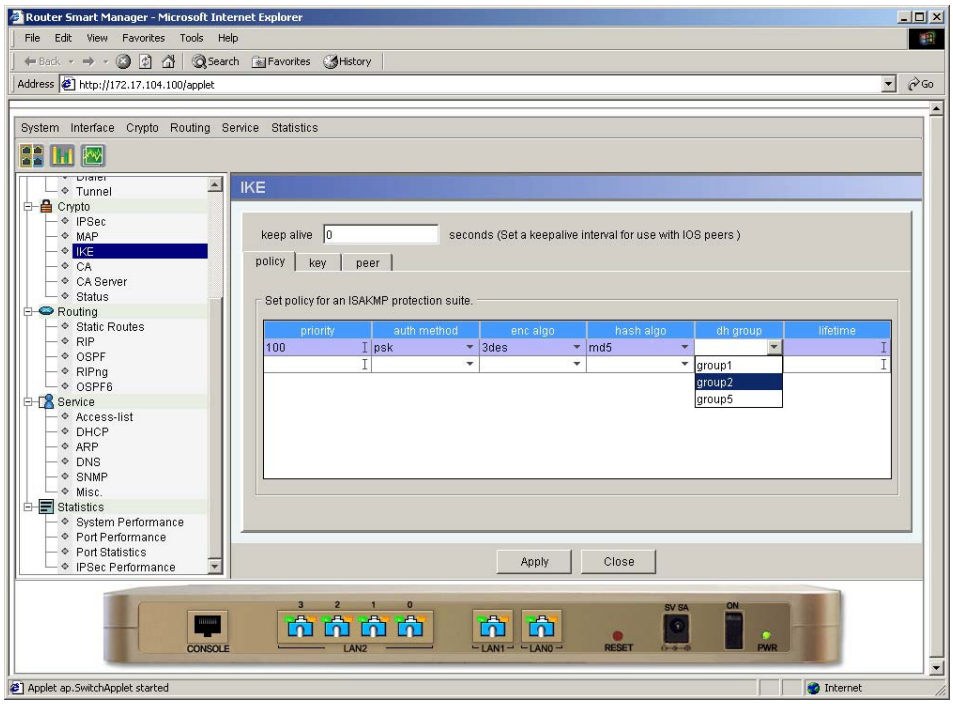
(Figure3-191) Select IKE Policy Encryption Algorithm

Select md5 for Hash Algorithm.



(Figure3-192) Select IKE Policy Hash Algorithm

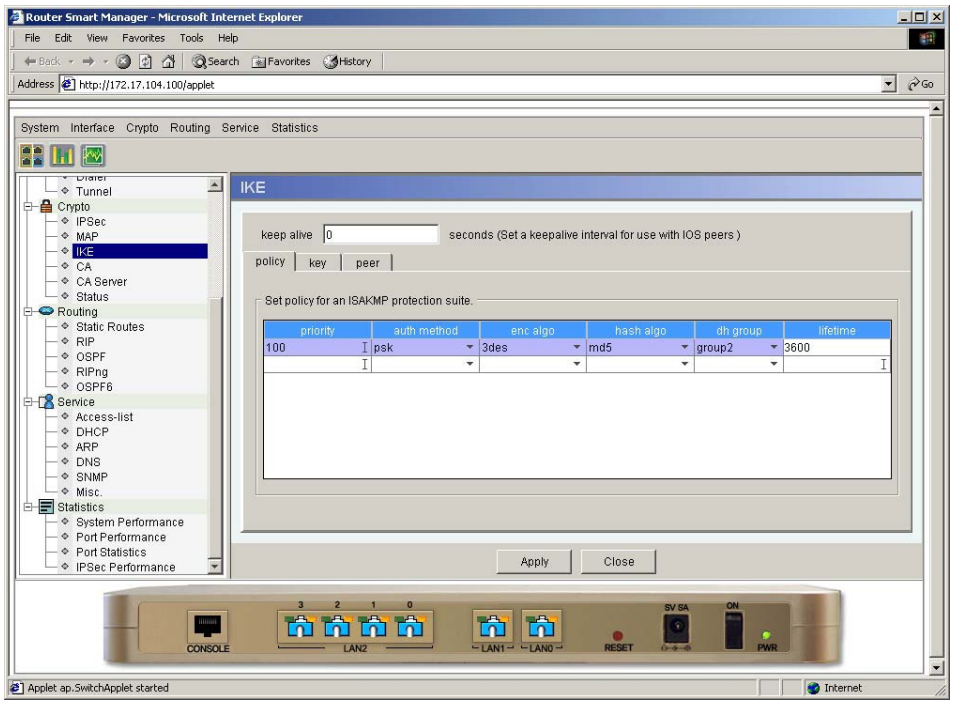
Select Diffie-Hellman Group “2”.



(Figure3-193) Select IKE Policy Diffe-Hellman Group

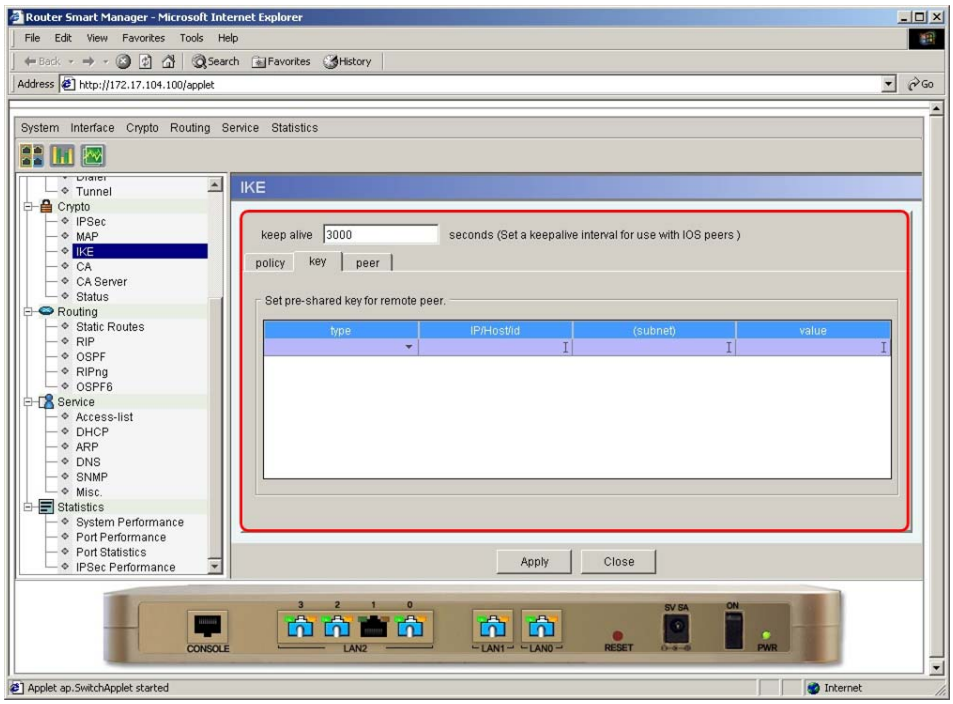
Input “3600” for Policy Lifetime.

Click “Apply” to verify.



(Figure3-194) Input IKE Policy Lifetime

Table 3-30 describes each element of IKE Key menu.



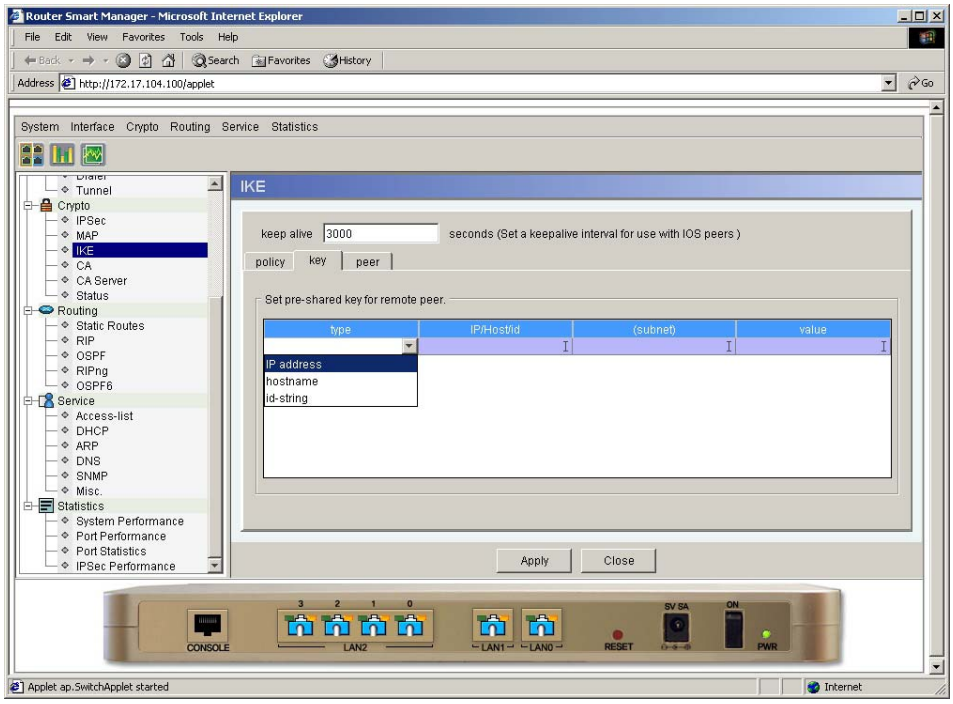
(Figure3-195) IKE Key Menu

<Table 3-30> IKE Key Menu Description

Elements	Description
Type	It decides the type to exchange Preshared Key. Select one from IP Address, Hostname, ID. Use DNS for Hostname, or Domain-List is needed.
IP/Host/id	Input IP Address, Hostname or Peer ID.
Subnet	Input subnet mask when IP Address is selected.
Value	Input Preshared Key value.

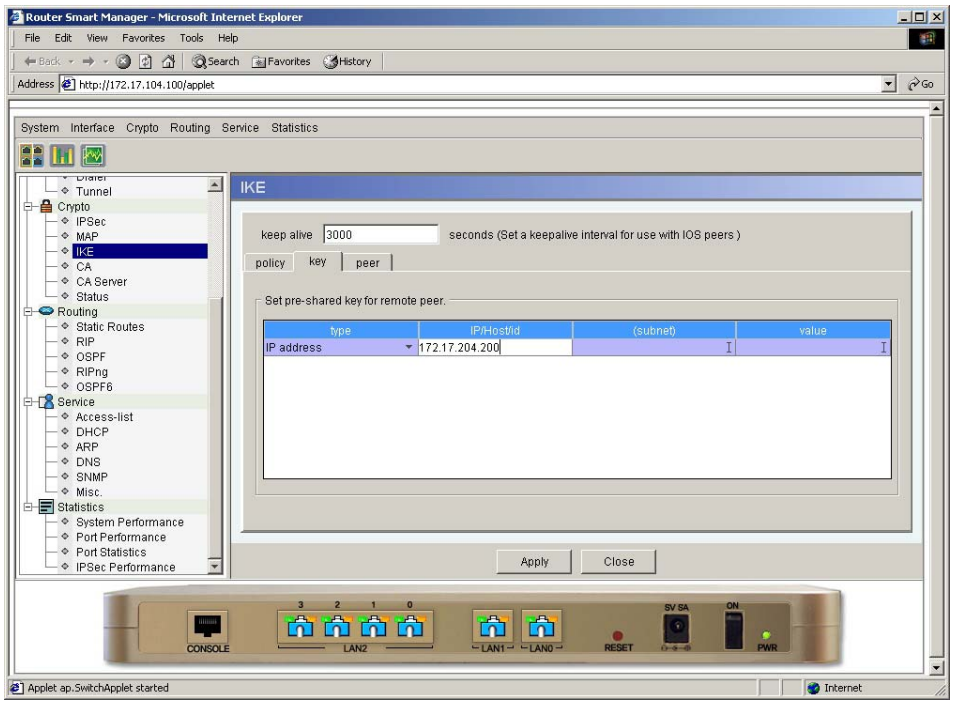
Figure 3-198 shows how to input Preshared Key “addpac_tech”.

First, select “IP Address” as Type.



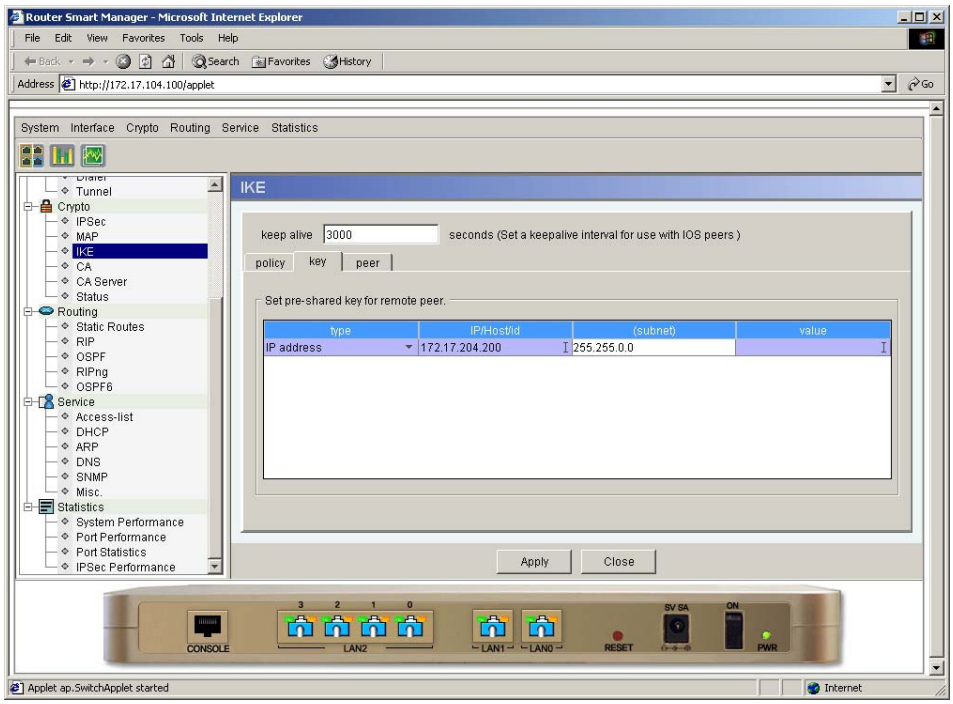
(Figure3-196) Select IKE Key Peer Type

Input IP Address “172.17.204.200” in IP/Host/id field.



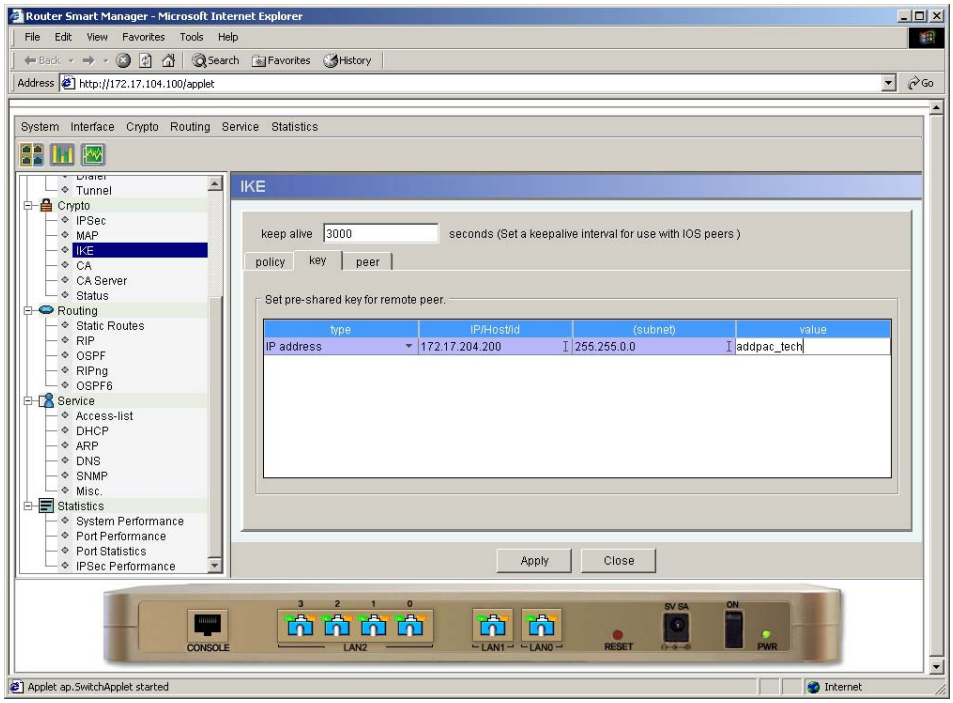
(Figure3-197) Input IKE Key Peer IP Address

Input Subnet mask “255.255.0.0” for IP Address “172.17.204.200”.



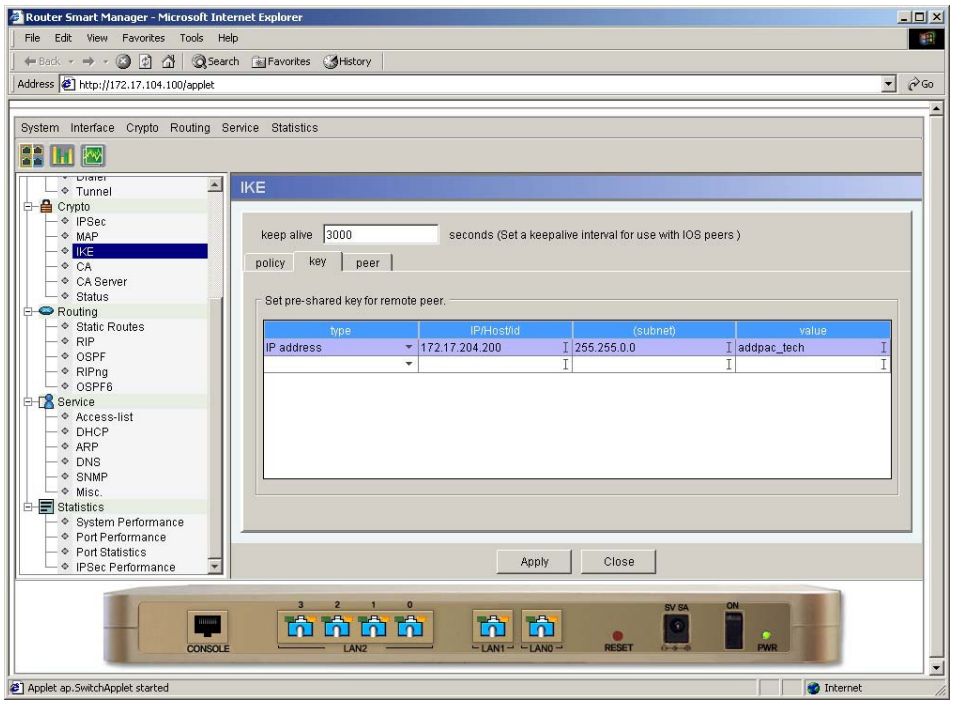
(Figure3-198) Input IKE Key Subnet mask

Input Preshared Key “addpac_tech” in Value field.



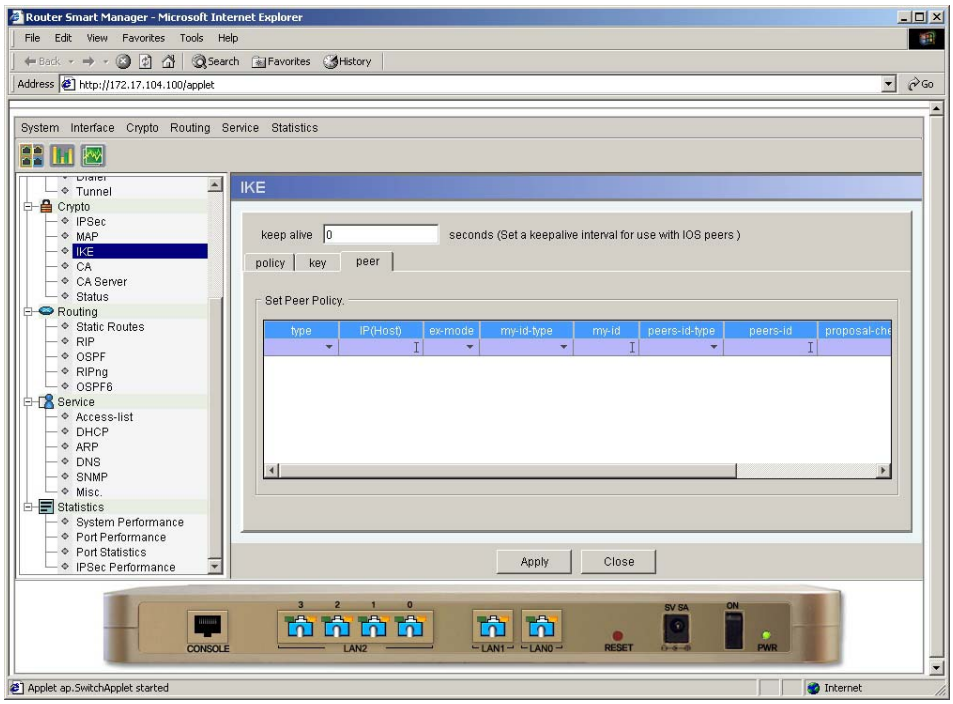
(Figure3-199) IKE Key Menu

Click “Apply” to verify.

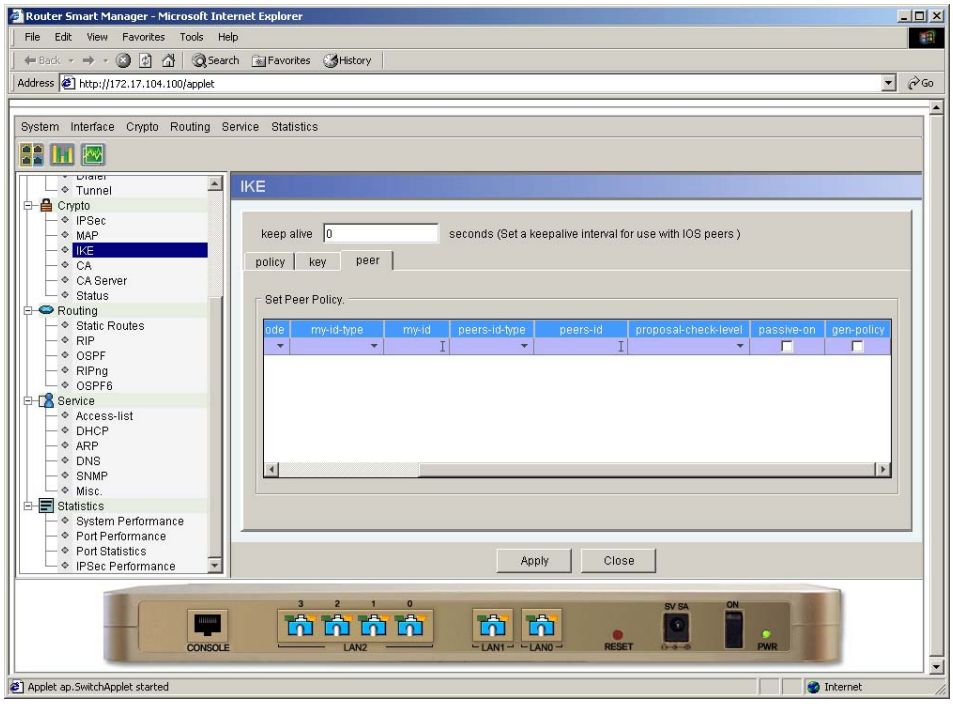


(Figure3-200) IKE Key configuration verify

Figure 3-203, 204 shows IKE Key Peer Menu.



(Figure3-201) IKE Key Peer Menu page I



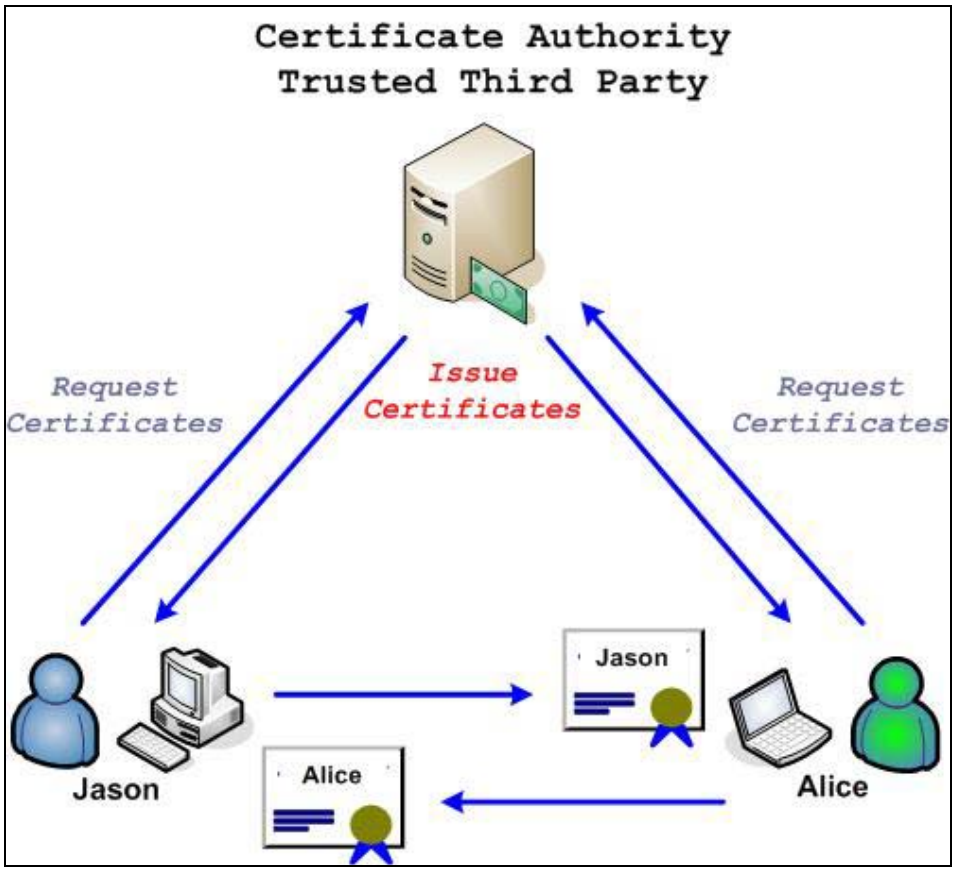
(Figure3-202) IKE Key Peer Menu page II

<Table 3-31> IKE Key Description

Elements	Description
Type	It decides type of Peer. Select one from IP Address, Hostname. Use DNS for Hostname, or Domain-List is needed.
IP(Host)	Input Peer IP Address or Hostname. Use DNS for Hostname or DNS List is needed.
Ex-mode	Choose Exchange-mode. Select one from Base/Aggressive/Main.
My-id-type	Choose My-id-type. Select one from asn1dn/fqdn/ipv4-address/key-id/user-fqdn.
My-id	Input Send Peer ID.
Peers-id-type	Choose Peers-id-type. Select one from asn1dn/fqdn/ipv4-address/key-id/user-fqdn. Select the same one as My-id-type.
Peers-id	Input Receive Peer ID.
Proposal-check-level	It decides acceptance level for SA Request from sender. It is applied on IPSec Lifetime and PFS. (This has to be predefined in Crypto Map of receiver Gateway) select one from exact/obey/strict. “Exact” only enables IPSec SA when the value of sender and receiver is the same, “obey” accepts the value from sender and “strict” enables IPSec SA when Lifetime of sender is the same or less than receiver’s. If Lifetime of sender is more than receiver’s, IPSec SA is disabled. (Based on Lifetime of sender.) In the case of PFS, IPSec SA is enabled in PFS-PFS, PFS-no PFS. If sender is “no PFS” and receiver is “PFS”, IPSec SA is disabled. (Based on sender’s PFS policy).
Passive-on	It starts Negotiation when getting SA Request from Peer. It does not send SA Request actively.
Gen-policy	Check if you want to enable sending SA Request.

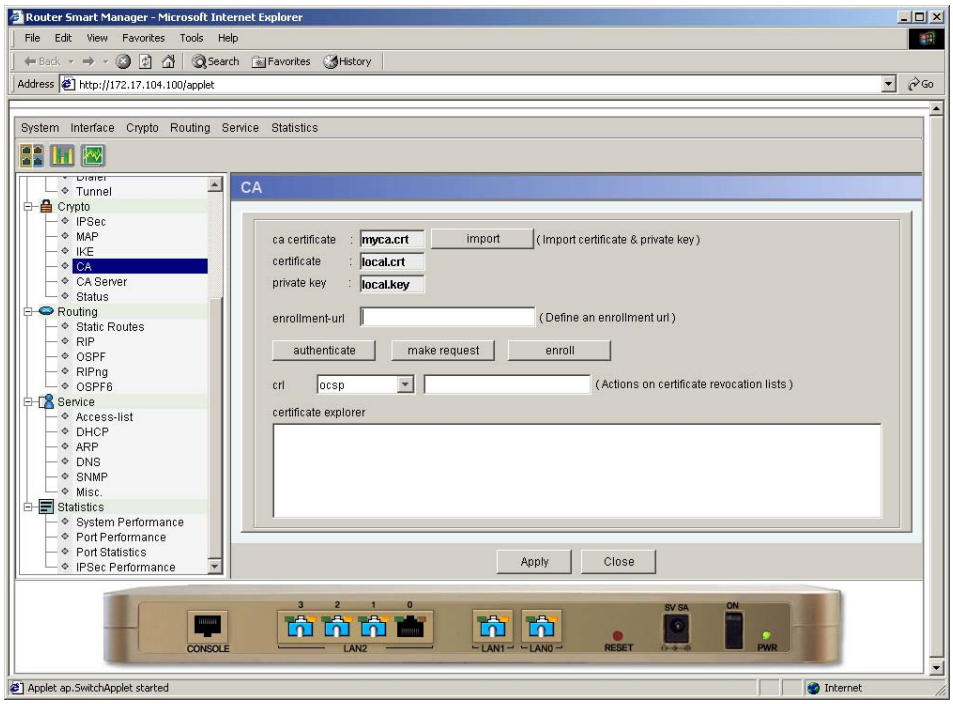
CA

CA (Certification Authority) is for using certification as for VPN gateway configuration. Using certification ensures security for gateways.



(Figure3-203) IPSec using certificate of CA Server

Figure 3-206 shows CA menu.



(Figure3-204) Crypto CA menu

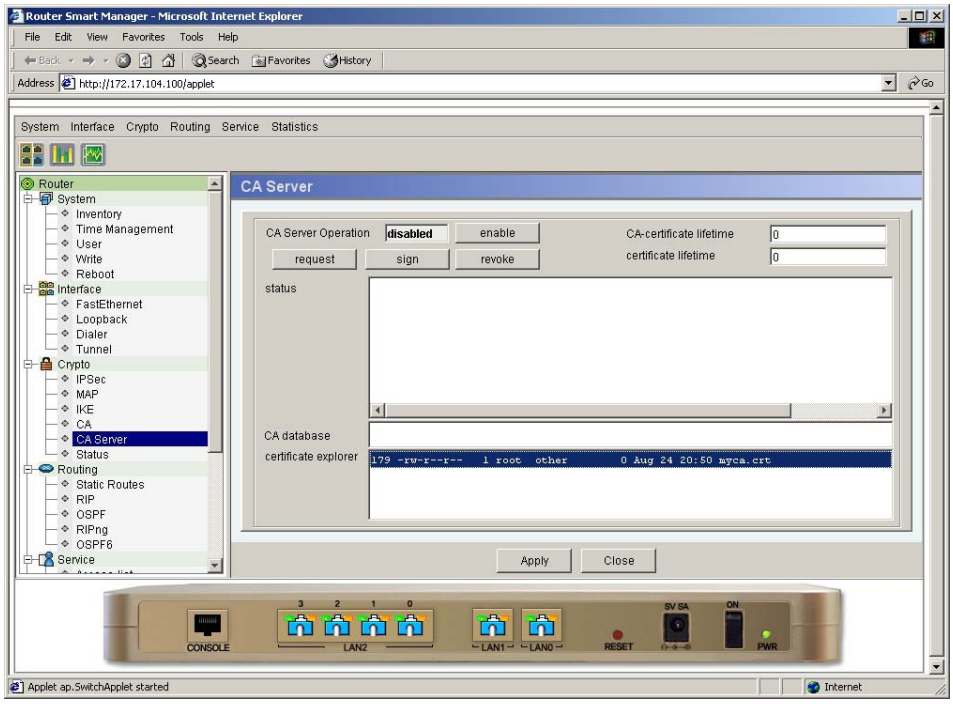
<Table 3-32> Crypto CA Description

Elements	Description
CA Certificate	CA certification file.
Certificate	Certificate file of Gateway.
Private key	Private key file.
Import [Button]	Imports contents of the certificate file.
Enrollment-url	Input URL of CA Server which requests certification.
Authenticate[Button]	Gateway authenticates CA Server.
Make Request [Button]	Create RSA key to check remote Peer.
Enroll[Button]	Request certification from CA Server.
Crl	Input the URL of ocsp/ldap Server to check expiration date of the certification.

CA Server

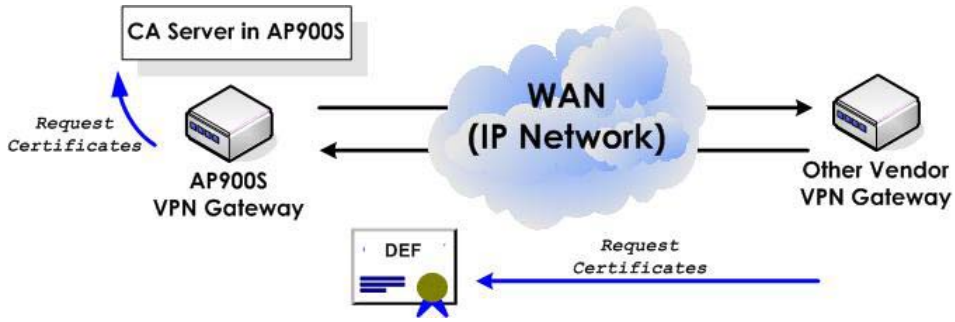
CA (Certification Authority) Server provides a function of issuing certification, IPSec communication by setting AP900S as a CA server.

AP900S enables Gateway to issue certification without a specific CA Server. AP900S does not only play as a CA Server but also plays as a gateway for IPS communication so it realizes easy use of certification.



(Figure3-205) Crypto CA Server main page

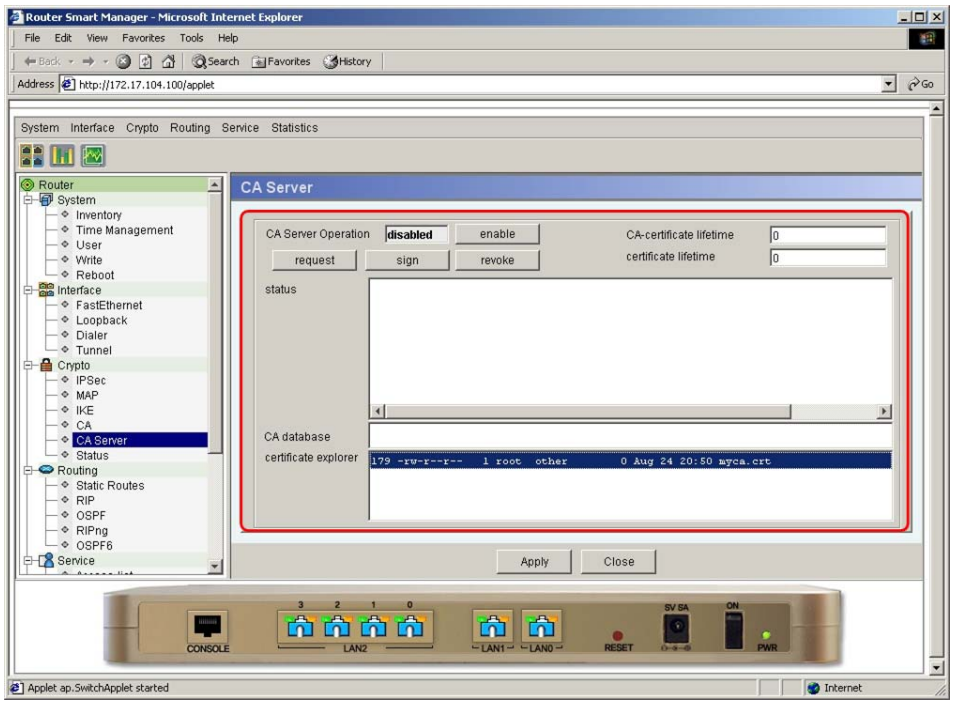
Figure 3-208 shows a network diagram of using AP900S as CA Server.



(Figure3-206) CA Server in AP900S Diagram

AP900S has its own CA Server inside which enables issuing its own certification and also certifications of other VPN Gateways. CA Server of AP900S provides functions of requesting and issuing AP900S certification even for SA Negotiation of AP900S. It also enables to issue certifications for remote VPN Gateways. This function is suitable for the environments which can not operate individual CA Server.

Table 3-33 shows CA Server menu.



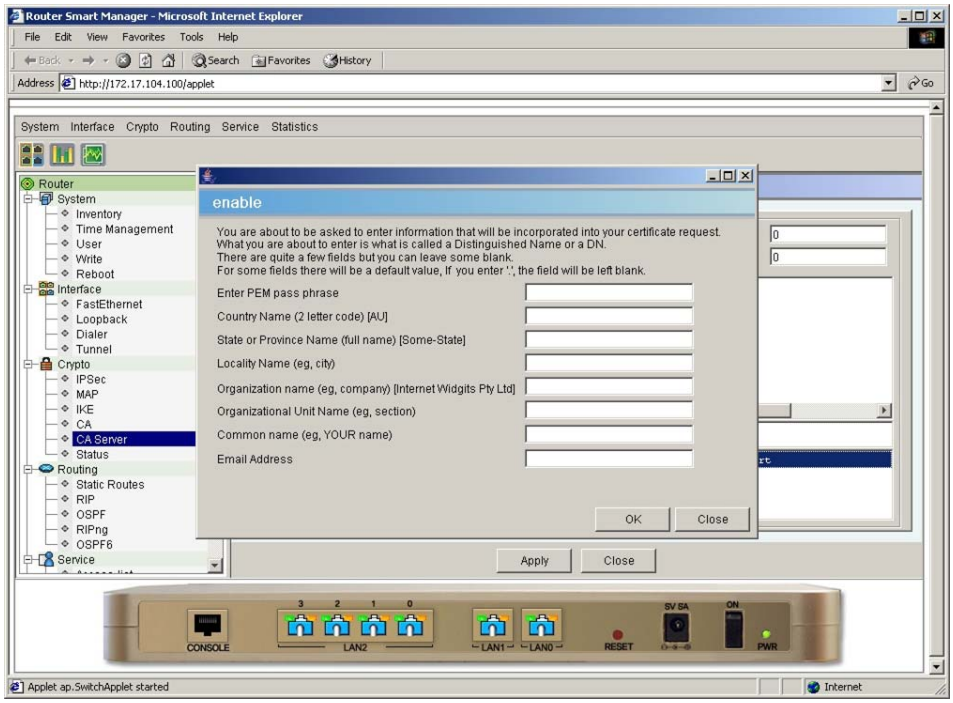
(Figure3-207) Crypto CA Server Menu

<Table 3-33> Crypto CA menu Description

Elements	Description
CA Server Operation	Set CA Server operation to Enable or Disable.
CA-Certificate Lifetime	Input Lifetime as CA Server.
Certificate Lifetime	Input certification Lifetime of CA Server.
Request [button]	Request authentication and 1024bit RSA Key for IPSec communication.
Sign [button]	Sign for requested certification from CA Server using RSA Key and authentication requesting form.
Revoke [button]	Revoke certification by requesting it to CA Server.

Figure 3-210 shows CA Server Enable menu page.

Must Input "." When there is nothing to input in each field.

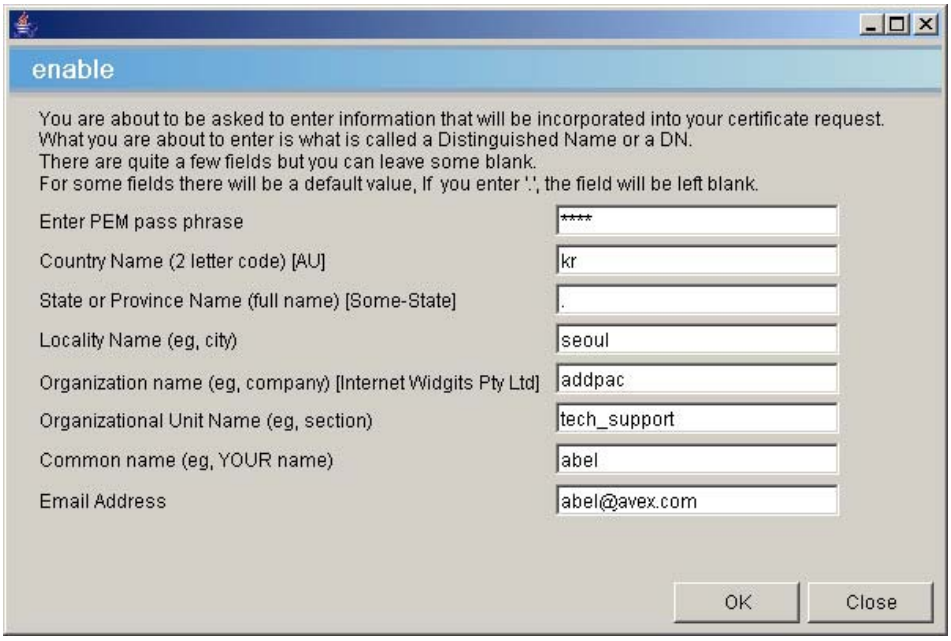


(Figure3-208) Crypto CA Server Enable Menu page

<Table 3-34> Crypto CA Enable menu Description

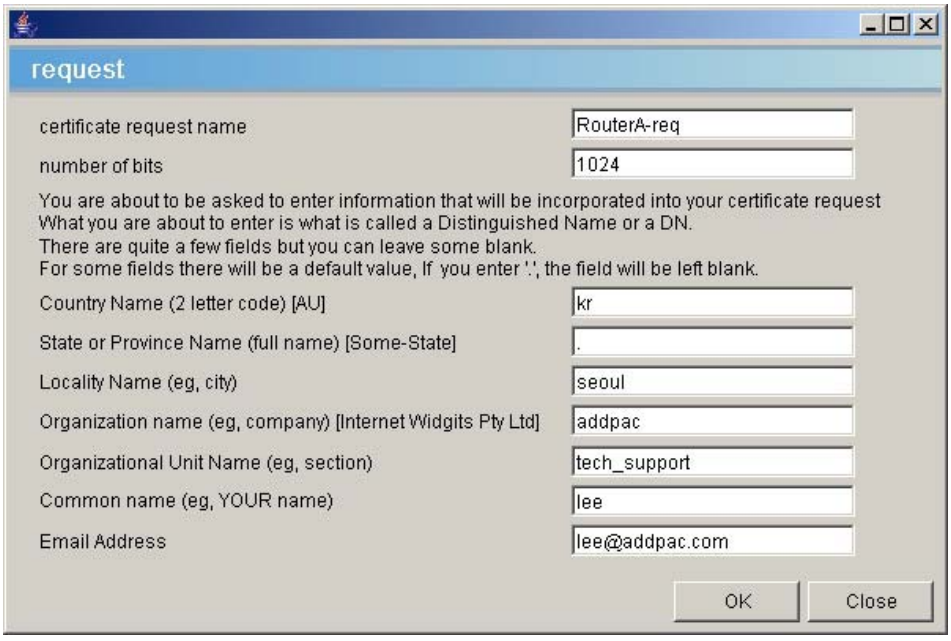
Elements	Description
Enter PEM pass phase	Set Password for the use of creating CA authentication certificate. This password is also used for issuing certification from other gateways.
Country Name	Input country name.
State or Province Name	Input the name of state or province.
Locality Name	Input the name of city.
Organization name	Input the name of organization.
Organization Unit Name	Input the name of department.
Common Name	Input the name of user.
Email Address	Input E-Mail address.

Figure 3-211 shows the parameter setting input example of CA Server Enable.



(Figure3-209) Crypto CA Server Enable input example

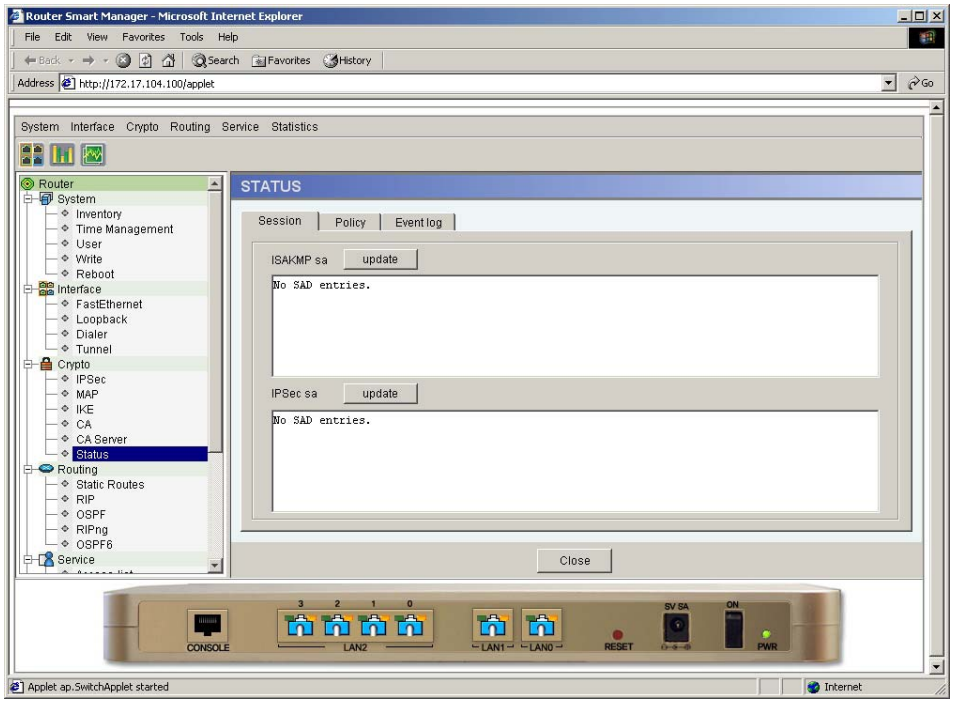
Figure 3-212 shows the parameter setting input example of CA Server Request.



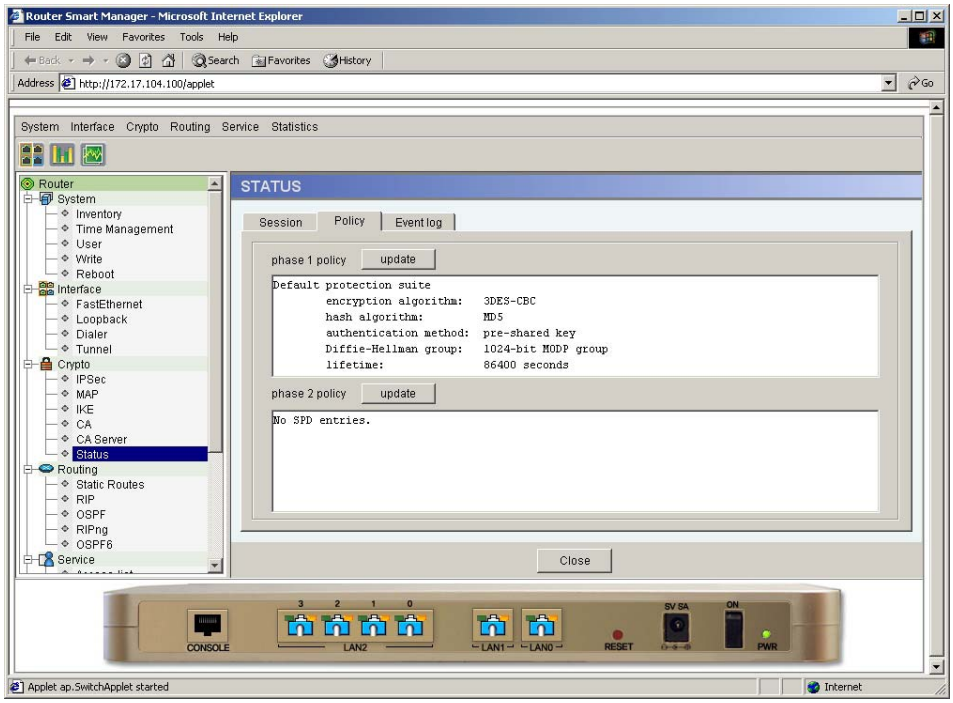
(Figure3-210) Crypto CA Server Request input example

Status

Status menu shows the information on ISAKMP SA Session, IPSec SA Session info, Phase1, Phase2 Policy and Event Log etc. Click “Update” to verify updated status.



(Figure3-211) Crypto Status Session page



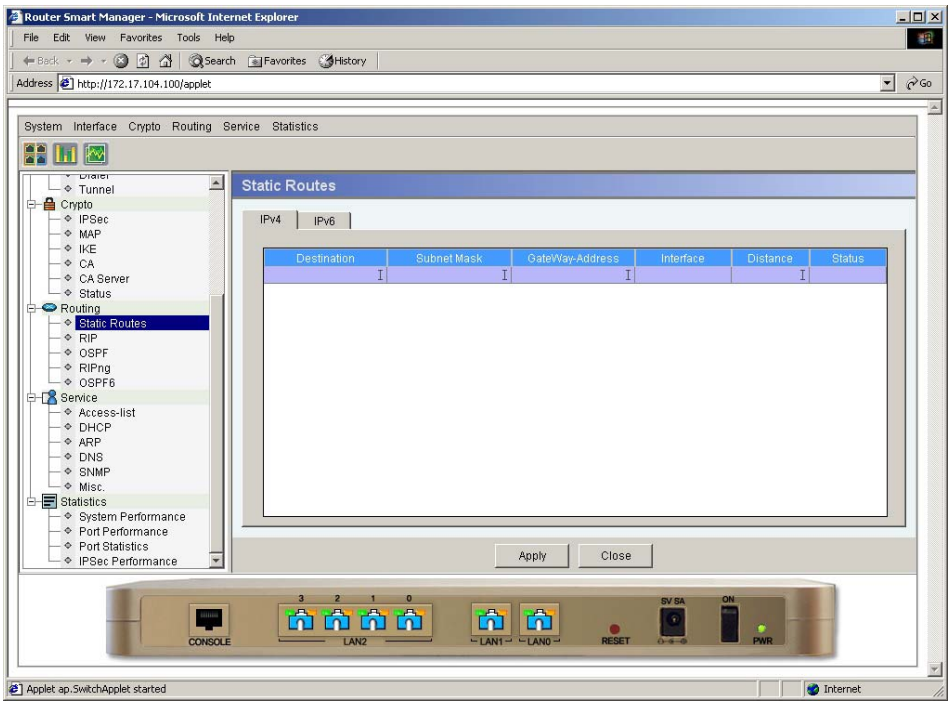
(Figure3-212) Crypto Status Policy page

Routing Menu

Static Routes

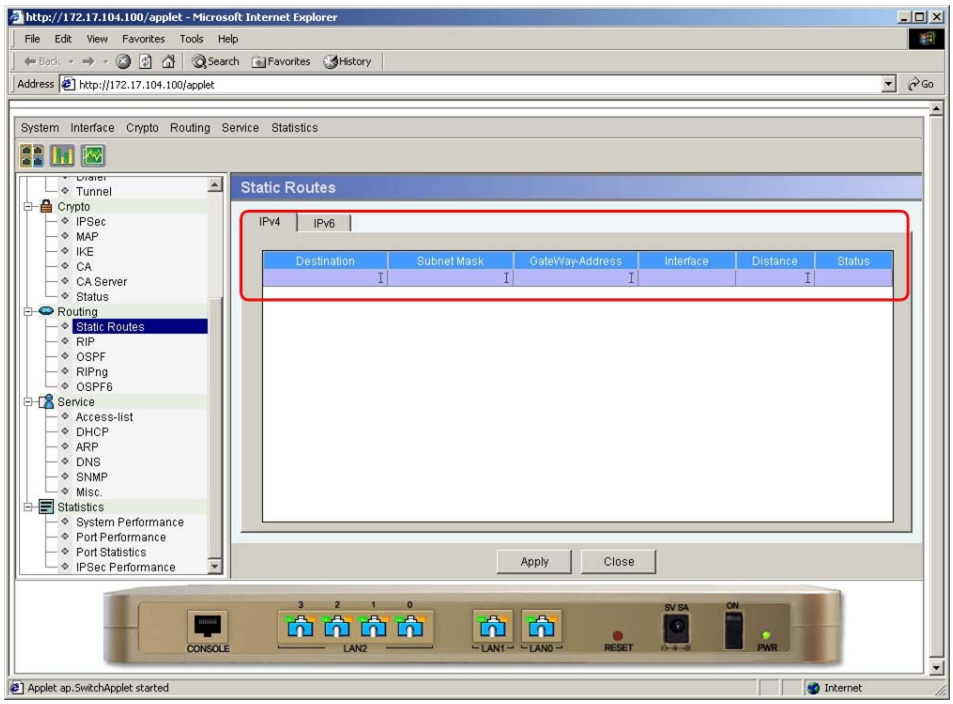
Static Routes enables manual input of Routing Table without using a specific Routing Protocol. Unlike Routing Protocols such as RIP and OSPF, Static Routes do not exchange Routing Table between Routers so it has a benefit of having bandwidth availability. However, it is not commonly used because of its complicated configuration and difficulties of solving network problems.

Static Routes is used when priority over Routing Table which uses Routing Protocols is needed or when Default-Router is needed because Interface uses IP Address.



(Figure3-213) Static Routes Main page

Table 3-35 is a description of IP version 4 Static Routes menu.

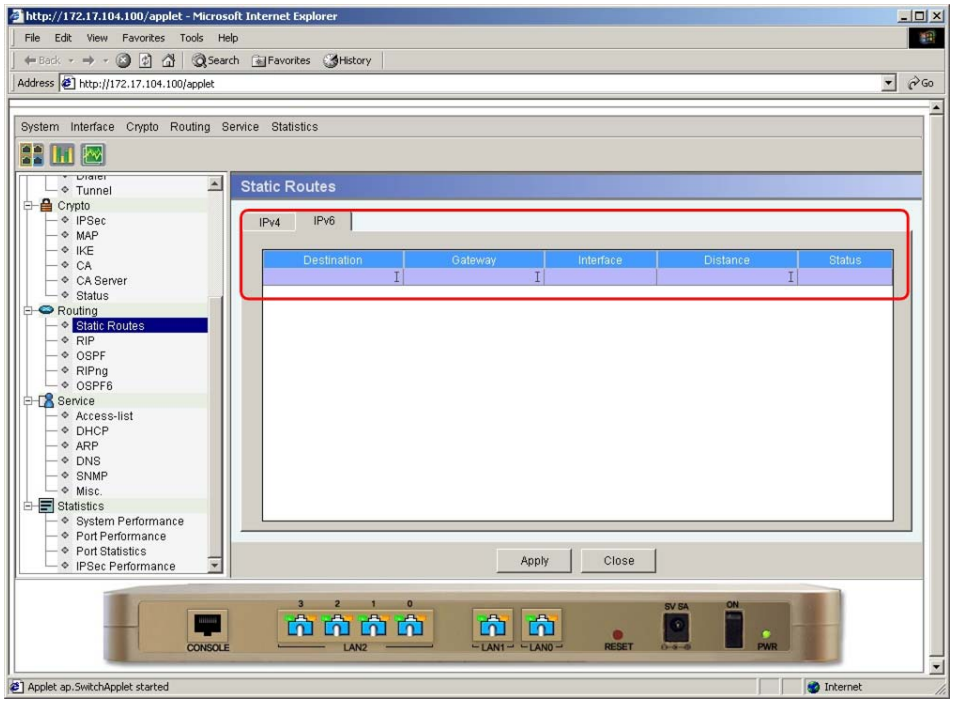


(Figure3-214) IP version 4 Static Routes page

<Table 3-35> IP version 4 Static Routes menu Description

Elements	Description
Destination	Input Destination IP Address. Input “0,0,0,0” for Default Route.
Subnet Mask	Input Destination Subnet mask. Input “0,0,0,0” for Default Route.
Gateway-Address	Input Gateway IP Address.
Interface	Input Local IP Address instead of Gateway IP Address.
Distance	Input priority for Static Route.
Status	Status of current Static Routes.

Table 3-36 is a description of IP version 6 Static Routes menu.



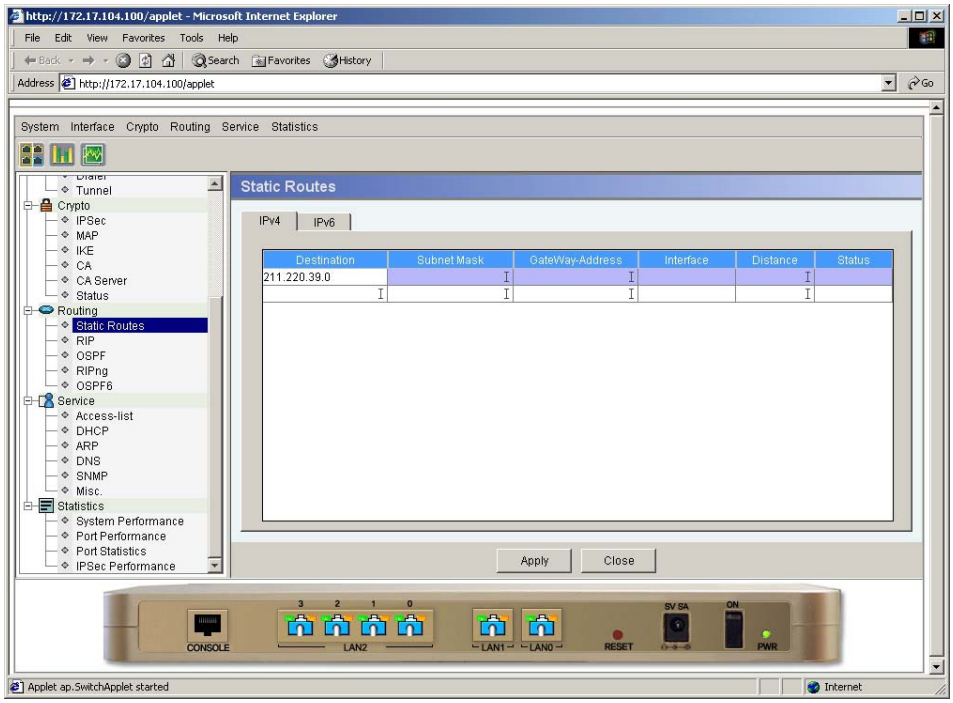
(Figure3-215) IP version 6 Static Routes page

<Table 3-36> IP version 6 Static Routes menu description

Elements	Description
Destination	Input Destination IP Address. Input IP Address and Subnet Mask in IPv6.
Gateway-Address	Input Gateway IP Address.
Interface	Input Local IP Address instead of Gateway IP Address.
Distance	Input priority for Static Route.
Status	Status of current Static Routes.

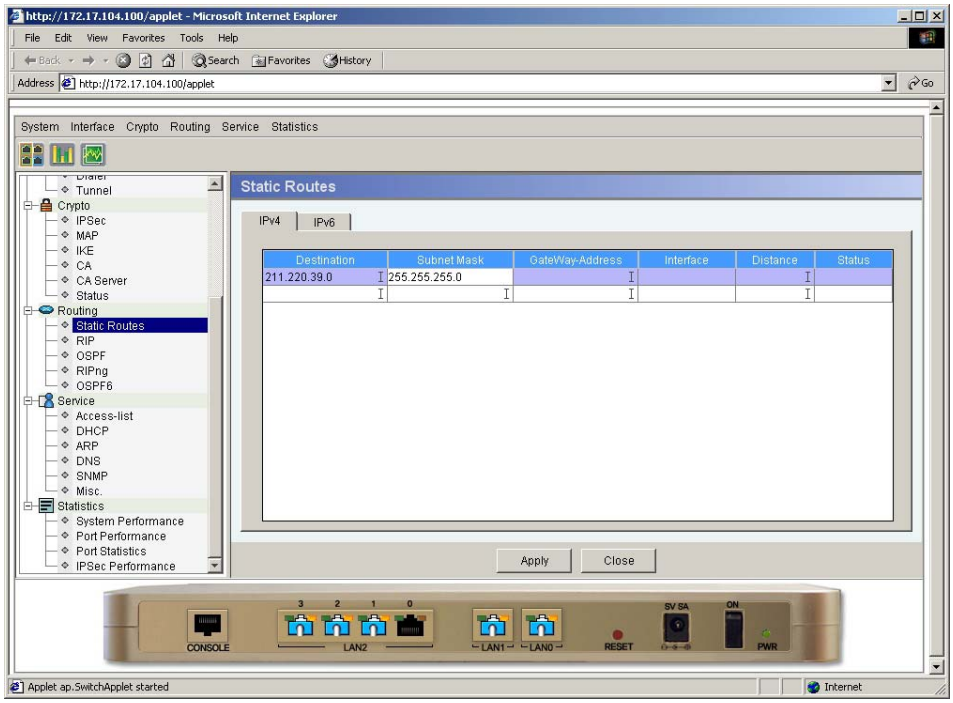
Figure 3-218 shows the example of IP version 4 Static Routes configuration.

Input “211.220.39.0” for Destination IP Address



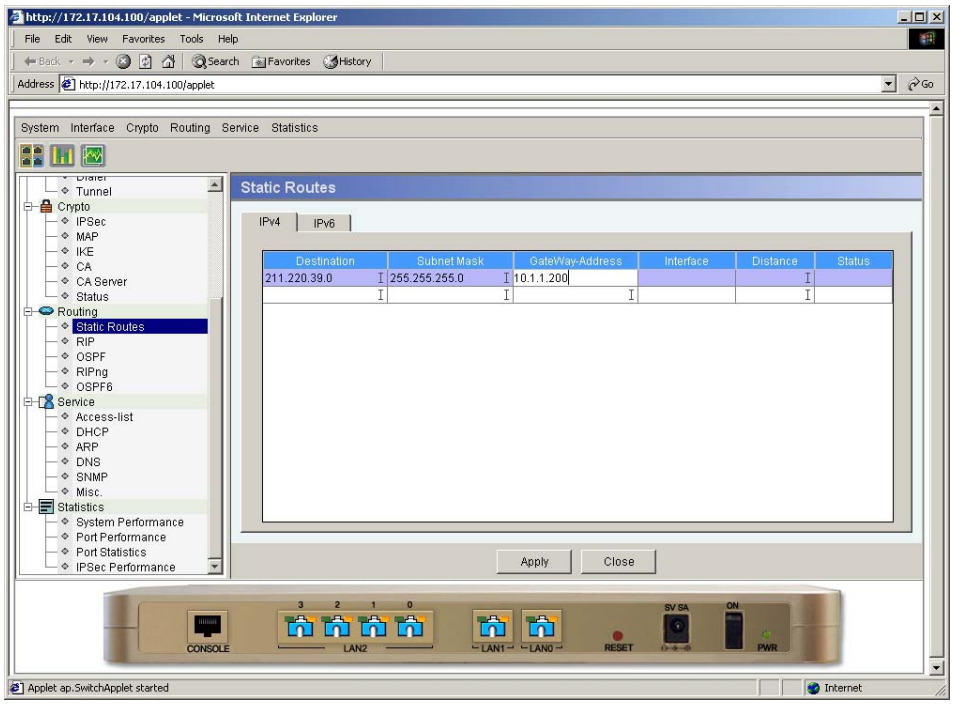
(Figure3-216) Input IP version 4 Static Routes Destination IP Address

Input “255.255.255.0” for Subnet Mask



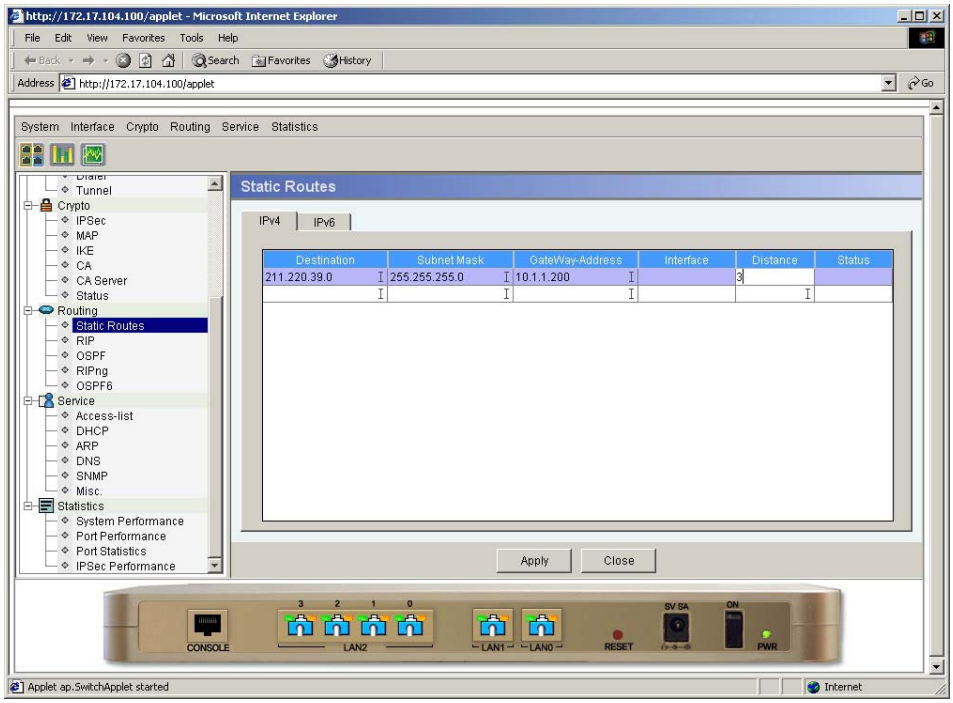
(Figure3-217) Input IP version 4 Static Routes Subnet Mask

Input “10.1.1.200” for Gateway Address



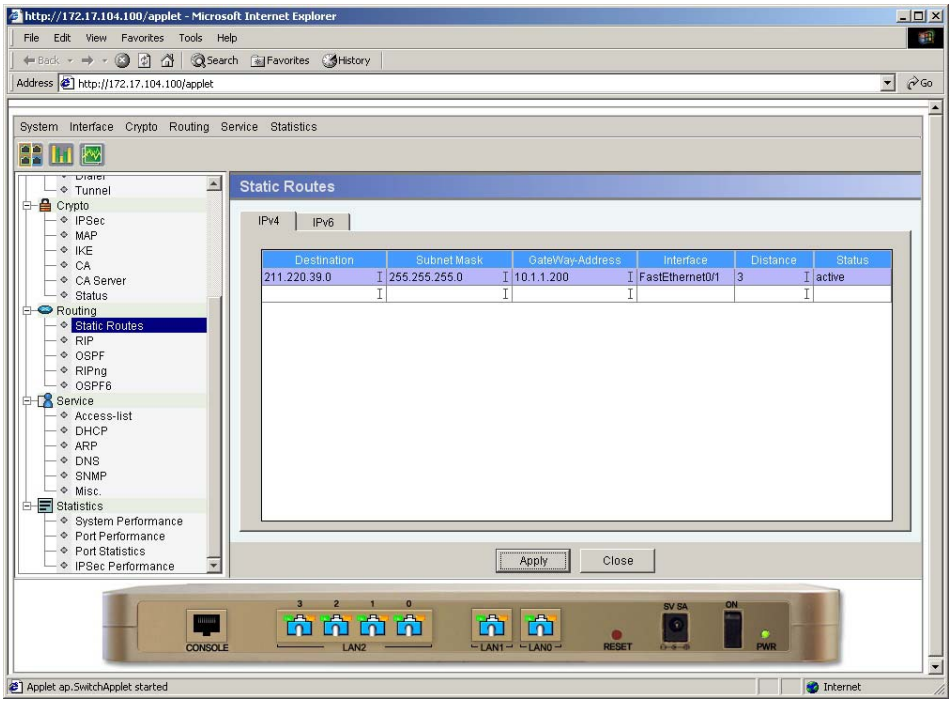
(Figure3-218) Input IP version 4 Static Routes Gateway Address

Input “3” for Distance



(Figure3-219) Input IP version 4 Static Routes Distance

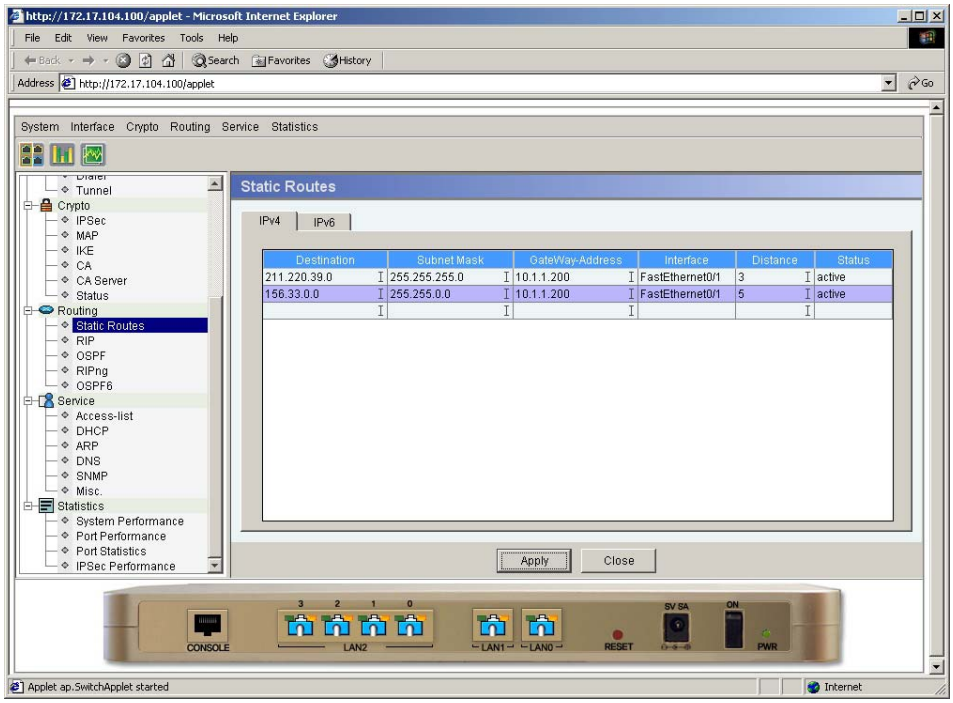
Click “Apply” to verify. It will automatically change the interface value to FastEthernet 0/1 of the same network as Gateway Address and Status field changes to “Active”.



(Figure3-220) Verify IP version 4 Static Routes settings.

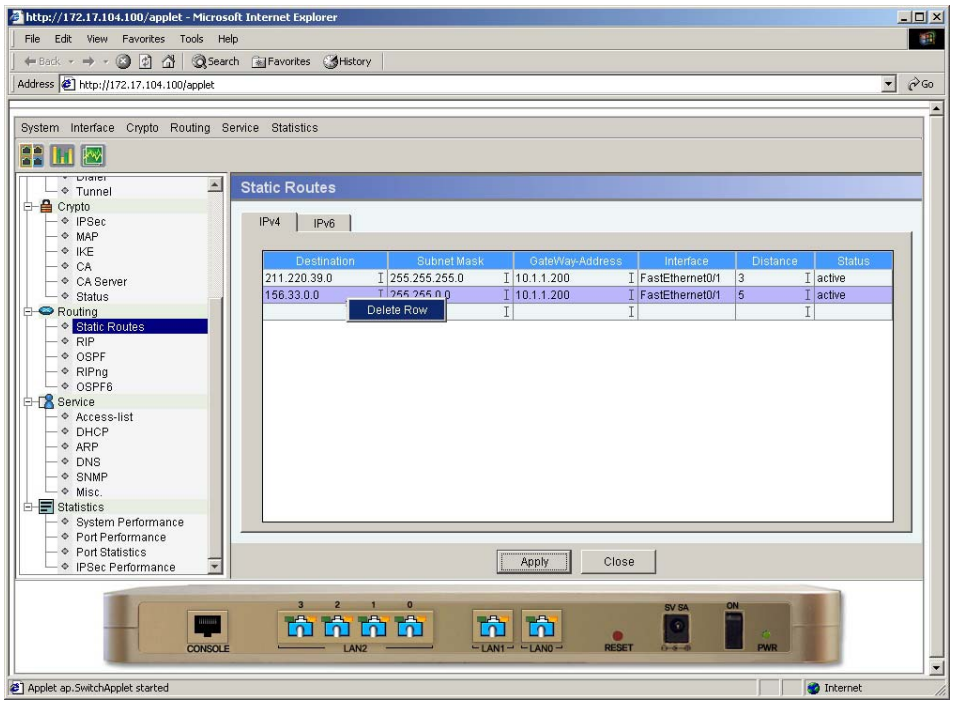
Figure 3-223 shows the example of deleting Static Route of “156.33.0.0/16”

First, select Static Route you want to delete.



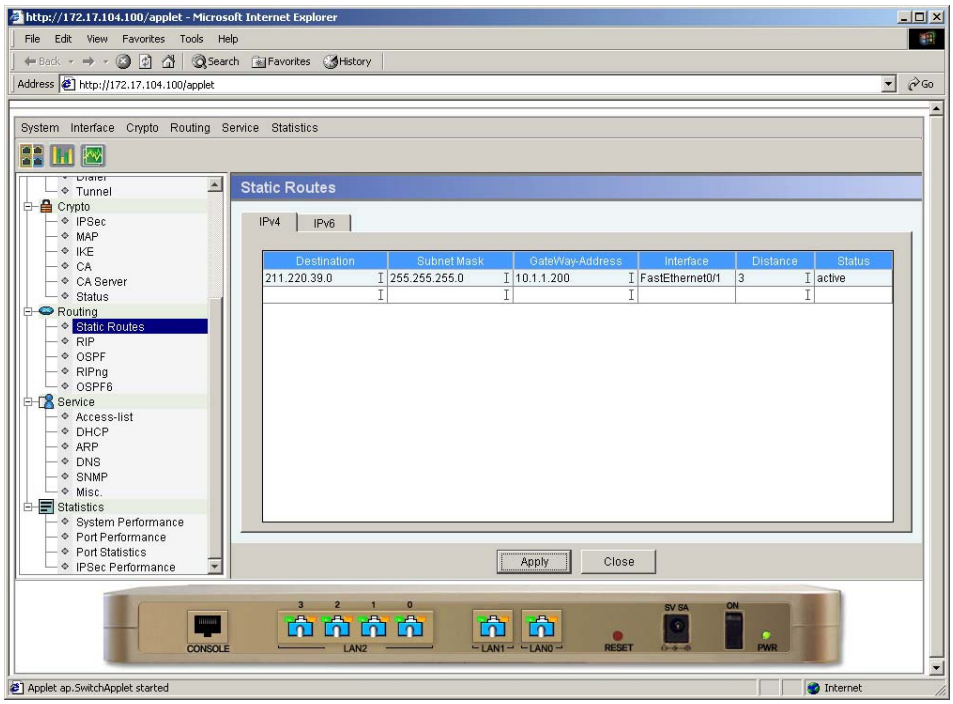
(Figure3-221) Select IP version 4 Static Route you want to delete

Select “Delete Row” by clicking right side of the mouse.



(Figure3-222) Delete IP version 4 Static Route

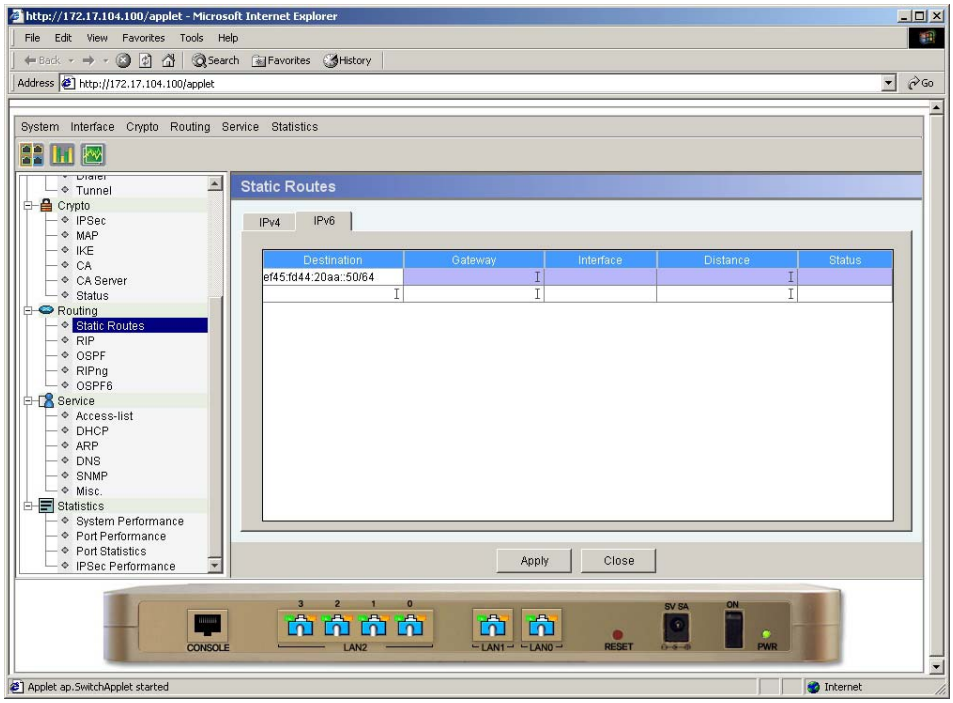
Click “Apply” to verify.



(Figure3-223) Verify IP version 4 Static Routes delete.

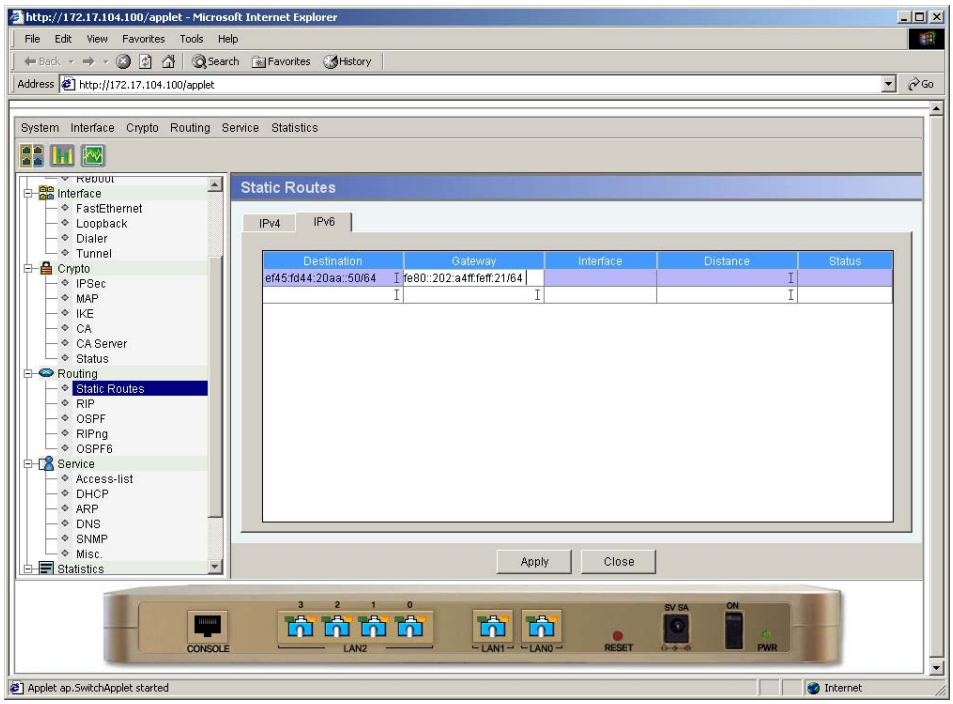
Figure 3-226 shows the example of configuring IP version 6 Static Routes.

Input IPv6 Address and Subnet mask in Destination field.



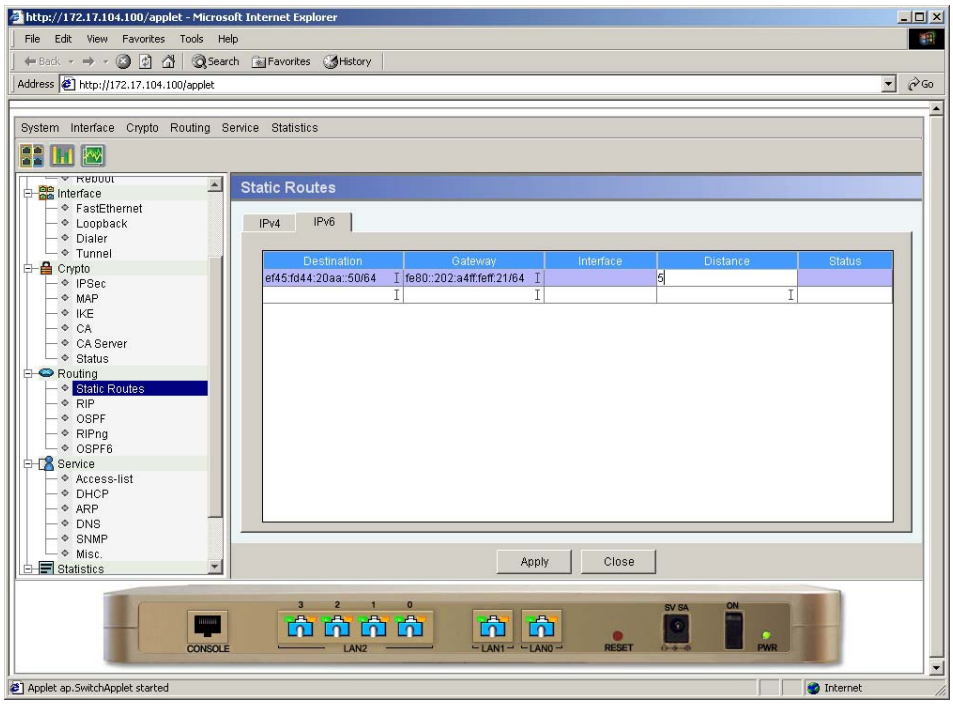
(Figure3-224) Input IP version 6 Static Routes Destination

Input IP Address of the gateway.



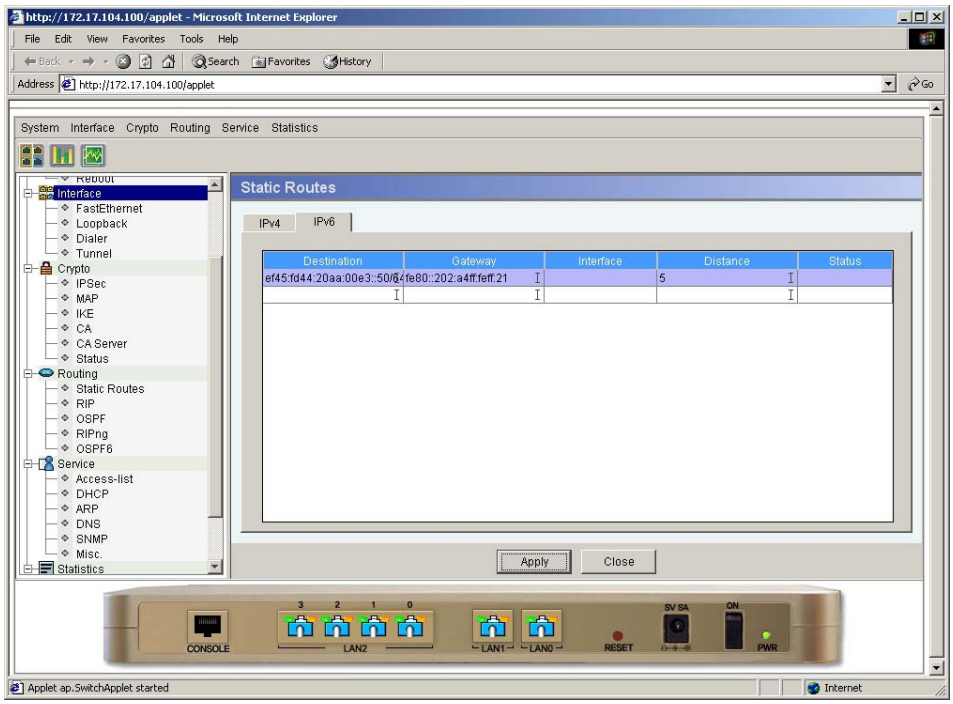
(Figure3-225) Input IP version 6 Static Routes Gateway Address

Input “5” for Distance



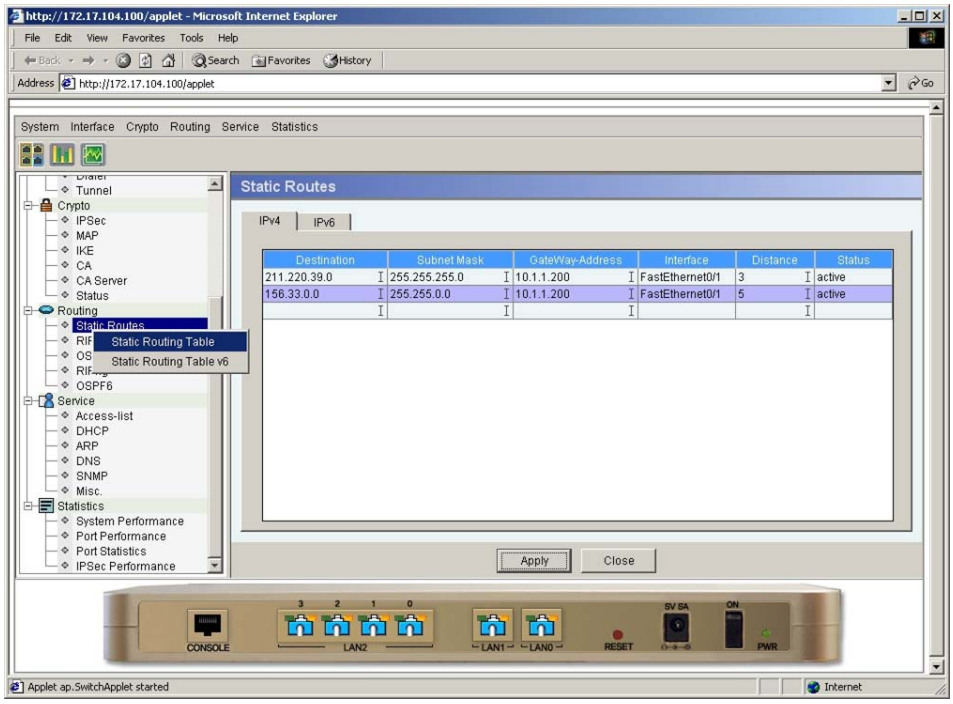
(Figure3-226) Input IP version 6 Static Routes Distance

Click “Apply” to verify.



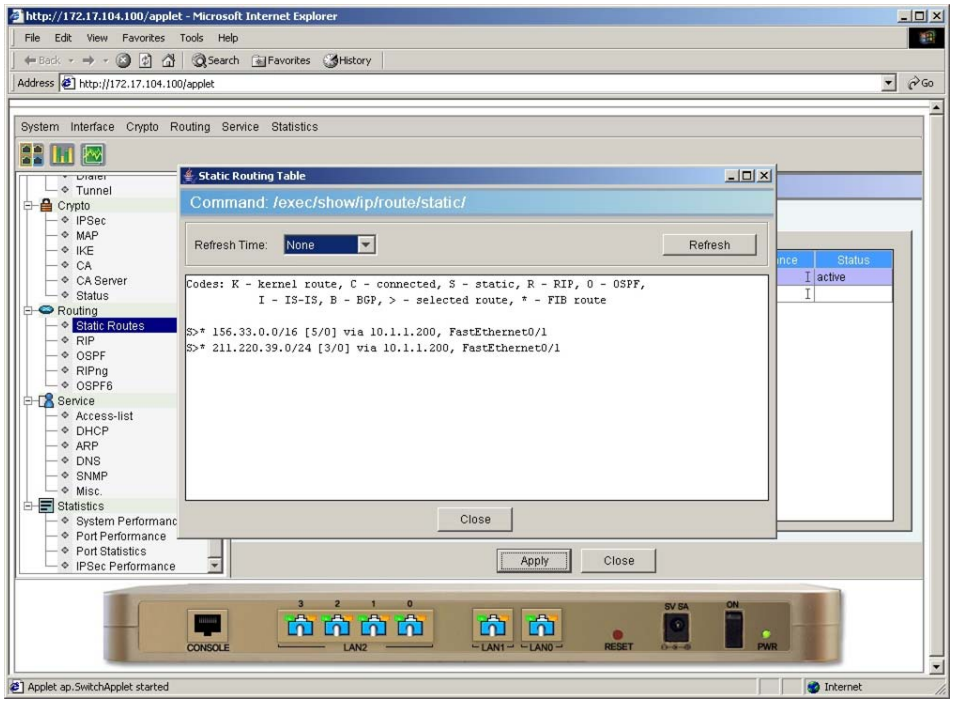
(Figure3-227) IP version 6 Static Routes configuration verify

Click right side of the mouse on Static Routes menu to check created Static Routes. See the Figure 3-230.



(Figure3-228) Select Static Routes Pop menu

Figure 3-231 shows how to check Routing Table by selecting Static Routes Table. Refresh Time can be set from 3~5 second. Click “Refresh” to check.

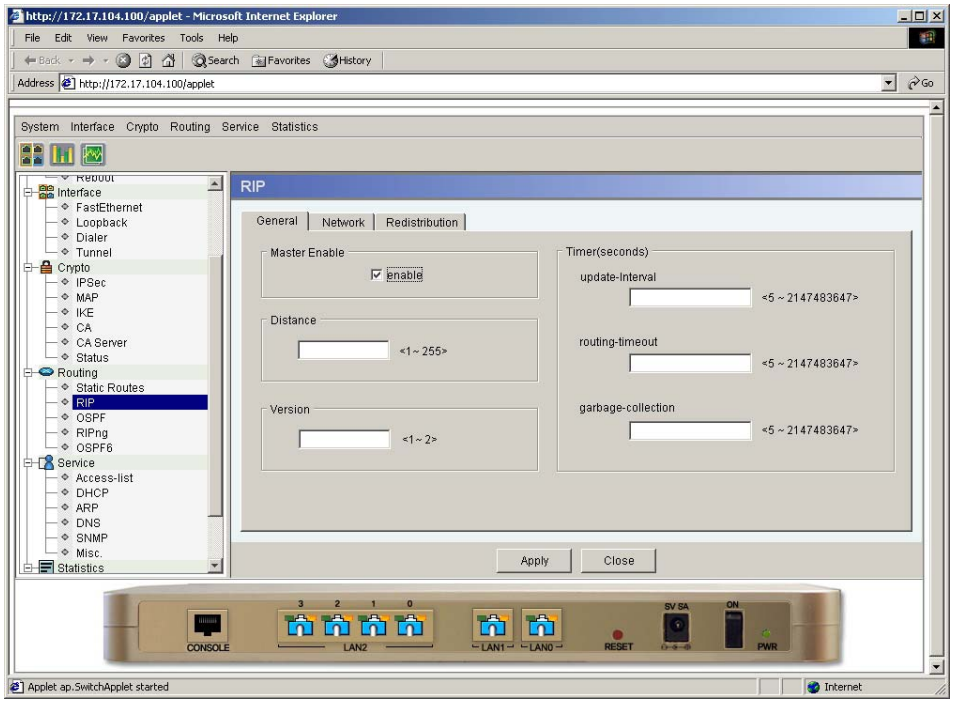


(Figure3-229) IP version 4 Static Routes Routing Table Verify

RIP

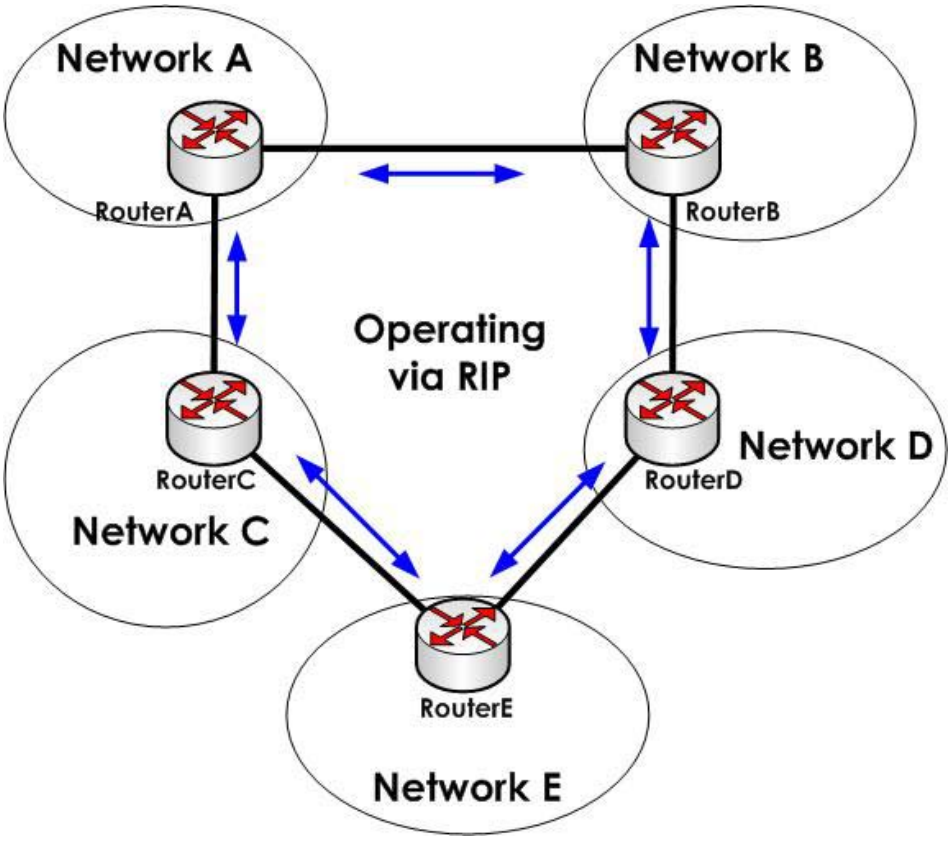
RIP (Routing Information Protocol) is a protocol which is widely used for managing routing information within LAN environments or LAN group networks.

Figure 3-232 shows the main page of selecting RIP.



(Figure3-230) Routing RIP Main page

Figure 3-233 is a Network Diagram using RIP as a Routing Protocol.



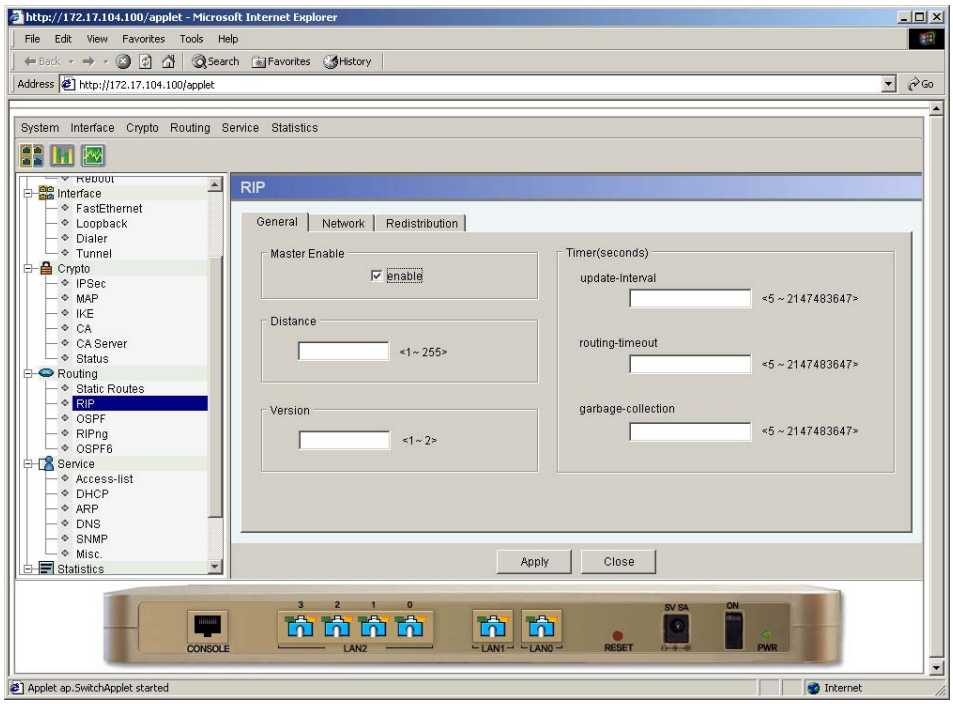
(Figure3-231) RIP Network Diagram

Basically Router A, B, C, D, E knows its own Network information but also each Router knows Network info of A~E through exchanging Routing Table. There are two paths for Network A to Network D. One is "RouterA → RouterC → RouterE" and the other one is "RouterA → RouterB → RouterD → RouterE". RIP choose a path using number of Hops. Less number of Hop is choosed for an optimal path. So "RouterA → RouterC → RouterE" is choosed.

Alternately, RIP will choose the path of "RouterA → RouterB → RouterD → RouterE", when the Link between RouterC and RouterE is down.

After the Link is back on again between RouterC and RouterE, Router A uses the original path for a packet transmits to exchange Routing Table.

Table 3-37 is a description of RIP General menu.



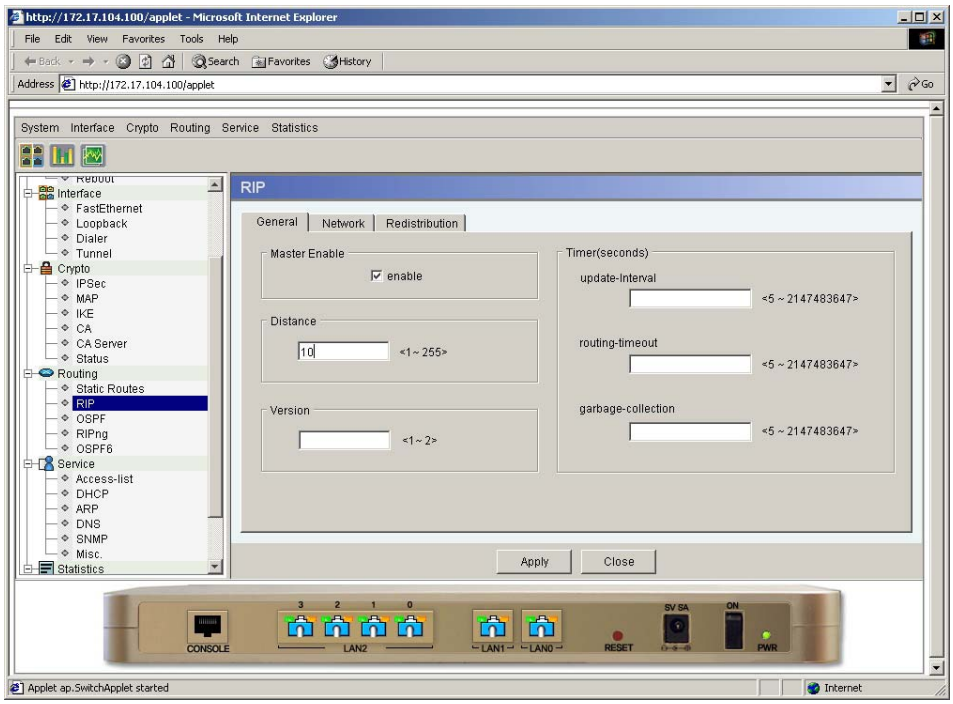
(Figure3-232) RIP General Main page

<Table 3-37> RIP General menu Description

Elements	Description
Master Enable	Select RIP enable or disable
Distance	Choose Distance Value for RIP. You can select from 1~255. Default value is “120”
Version	Choose Version of RIP. Select one from v1, v2. Default is “v2”
Update-Interval	Sets Routing Table update interval. Default value is “30”
Routing-Timeout	Sets waiting time for receiving Routing Table from a specific Interface. Default value is “180” sec.
Garbage-Collection	Sets the time for deleting a Routing Table after Routing-Timeout. Default value is “120” sec.

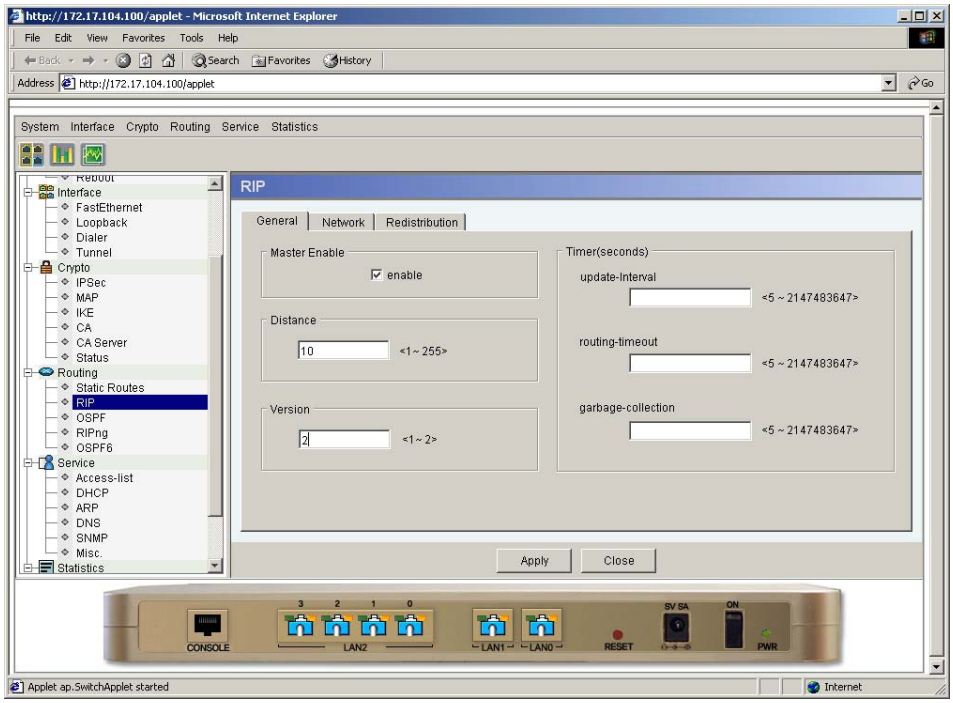
Figure 3-235 shows the example of altering RIP General menu.

Input “10” for Distance



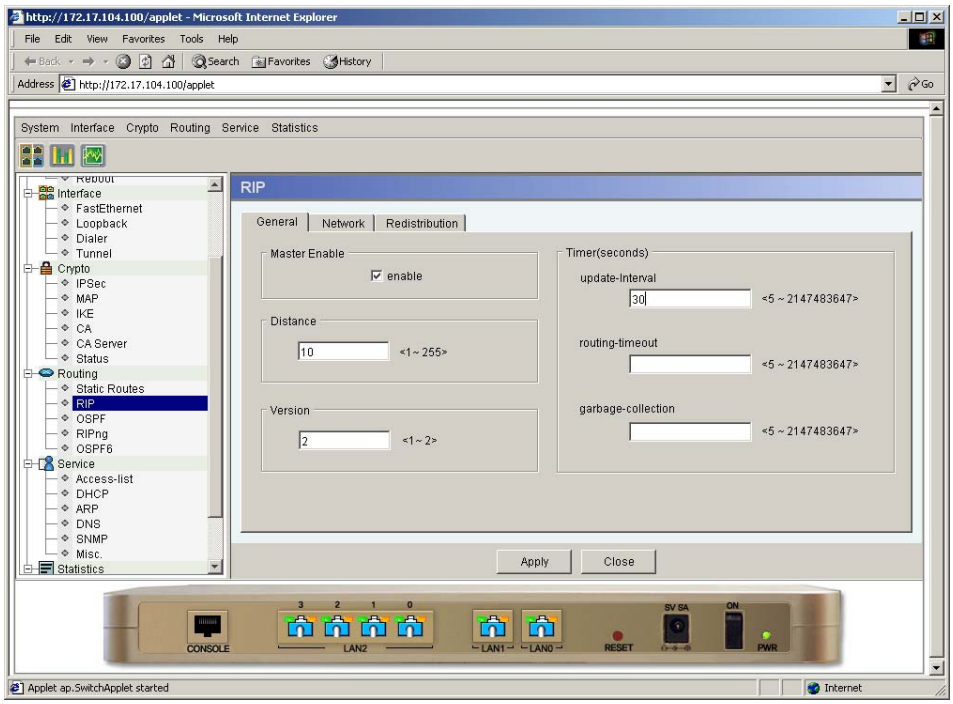
(Figure3-233) Input RIP Distance

Select “2” for Version.



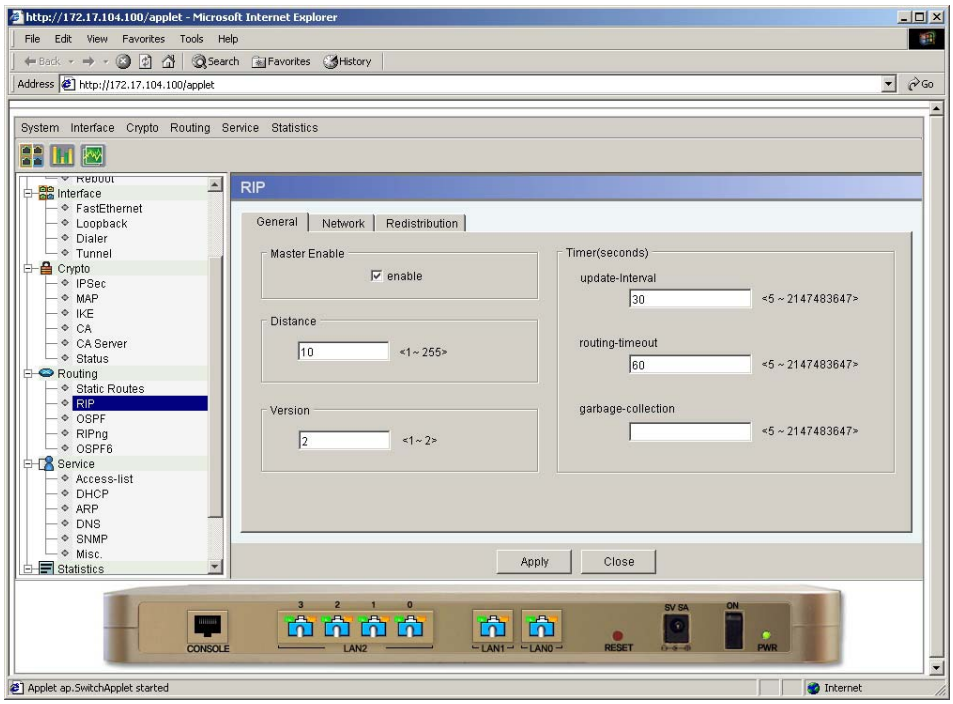
(Figure3-234) Input RIP Version

Input “30” for Update-Interval



(Figure3-235) Input RIP Update-Interval

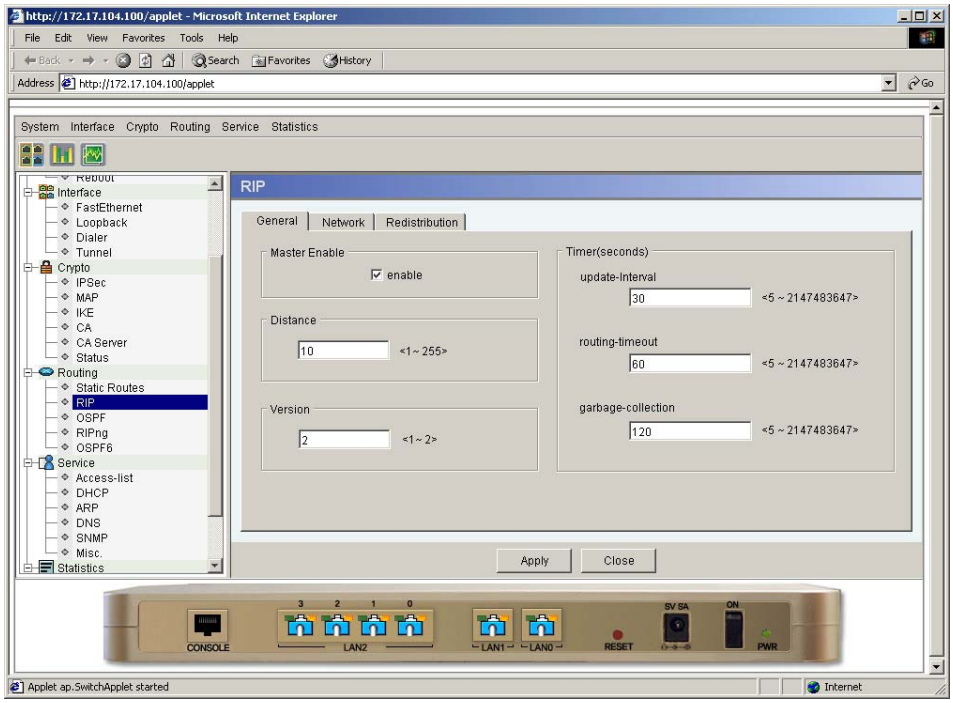
Input “60” for Routing-Timeout



(Figure3-236) Input RIP Routing-Timeout

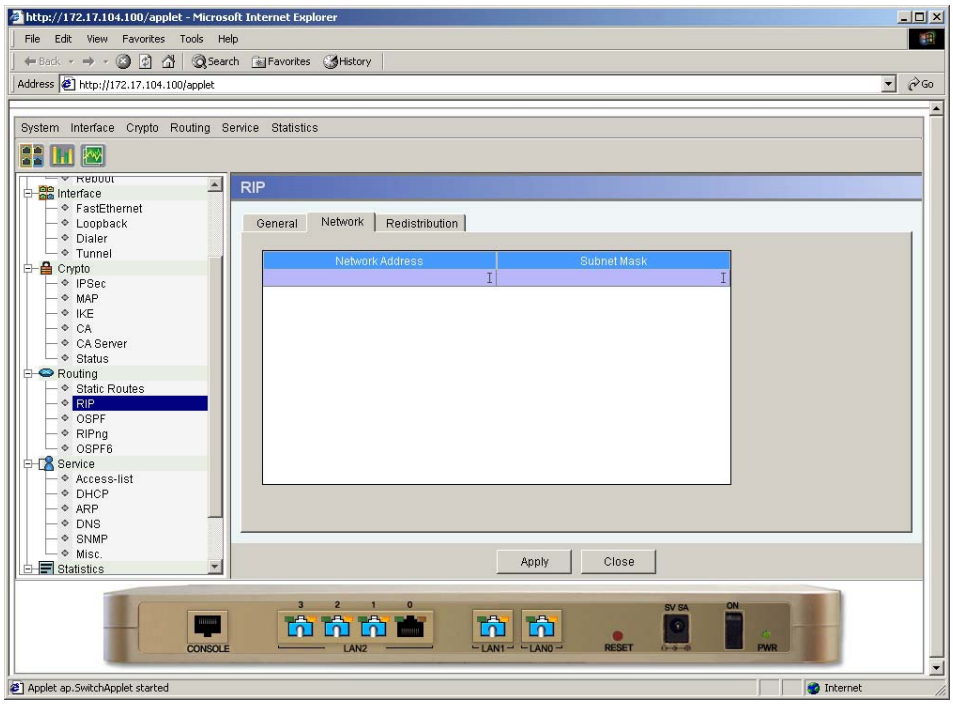
Input “120” for Garbage-Collection

Click “Apply”.



(Figure3-237) Input RIP Garbage-Collection

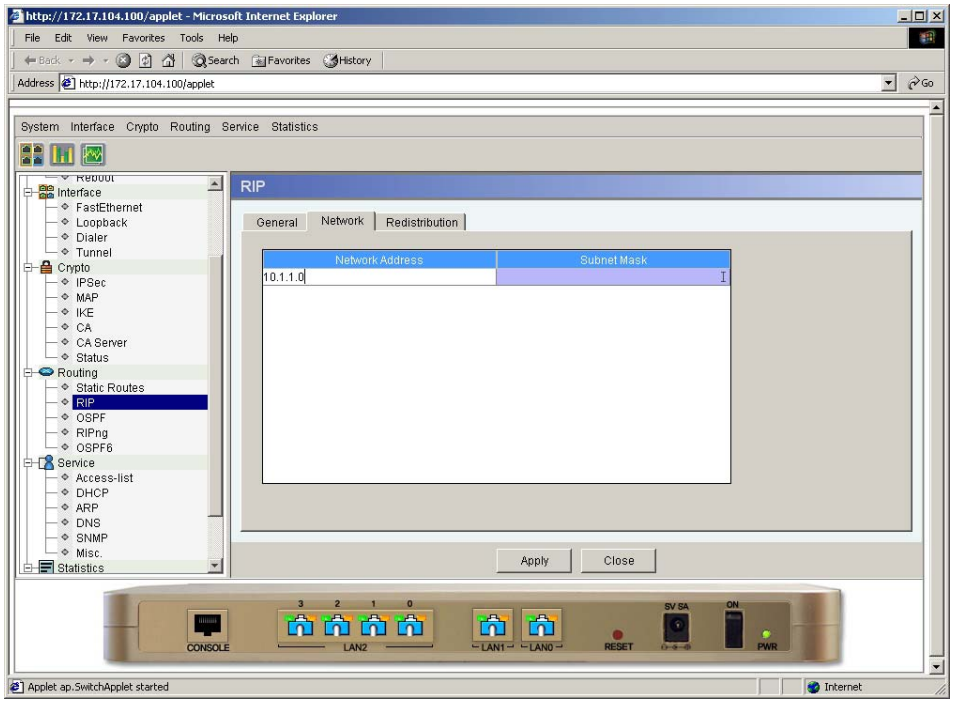
Figure 3-240 shows RIP Network page.



(Figure3-238) RIP Network Main page

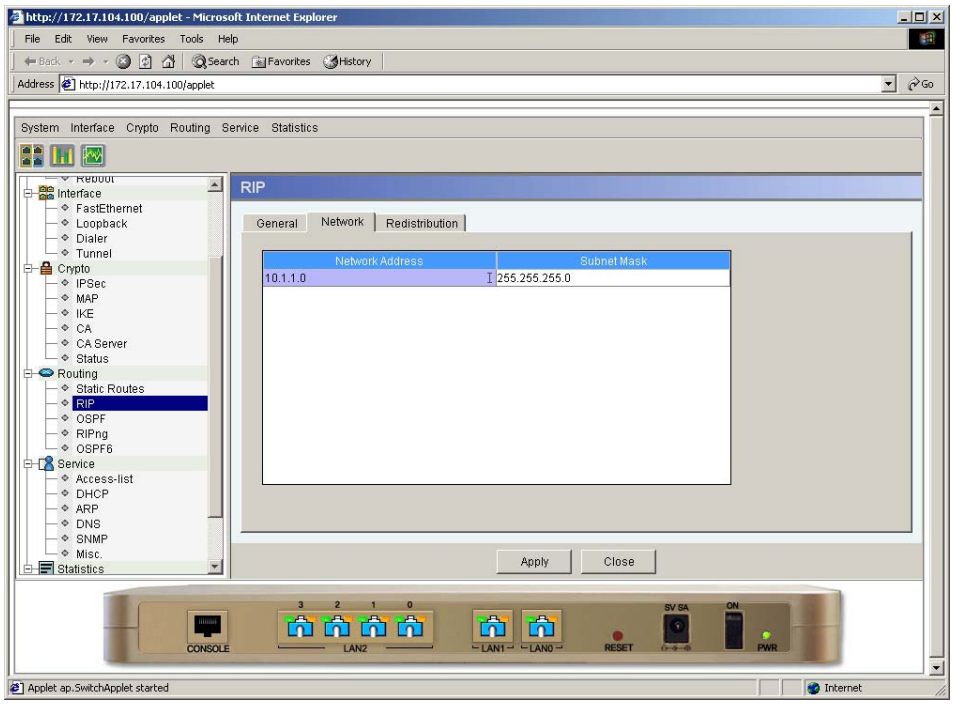
Figure 3-241 shows the example of adding “10.1.1.0/24” to RIP Network.

Input “10.1.1.0” for Network Address



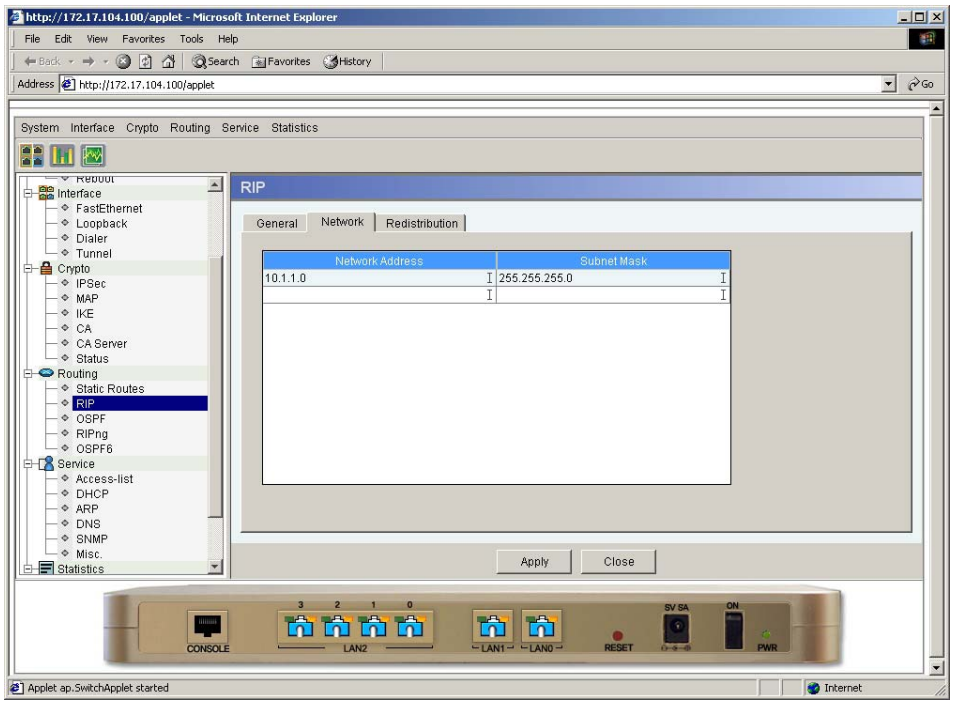
(Figure3-239) Add RIP Network Address

Input “255.255.255.0” for Subnet Mask



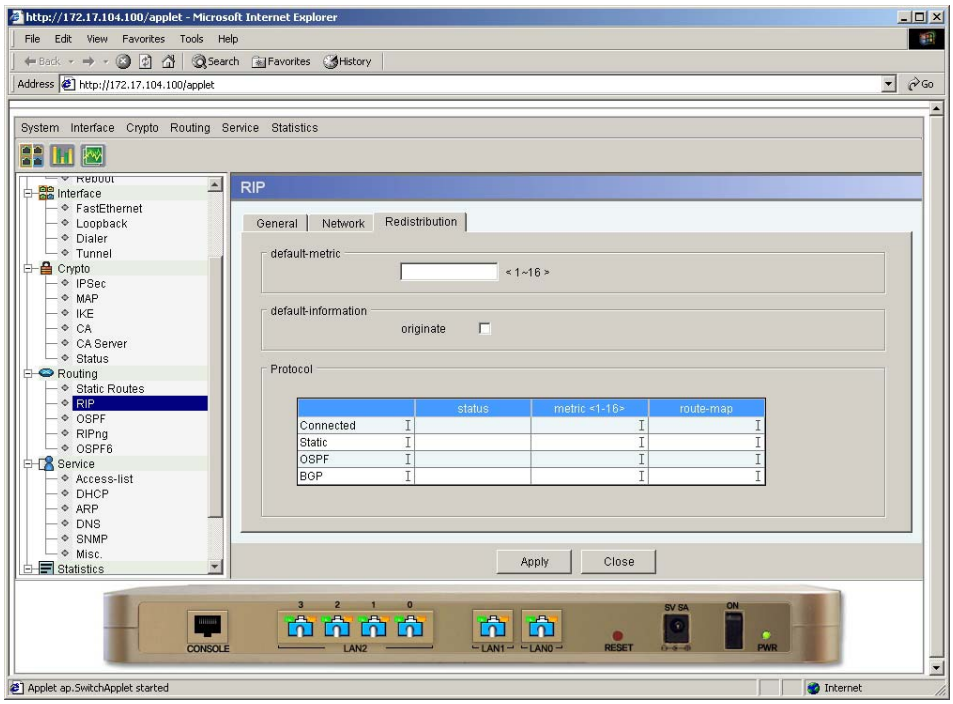
(Figure3-240) Input RIP Network Subnet Mask

Click “Apply” to verify.



(Figure3-241) New RIP Network verify

Figure 3-244 shows RIP Redistribution page.

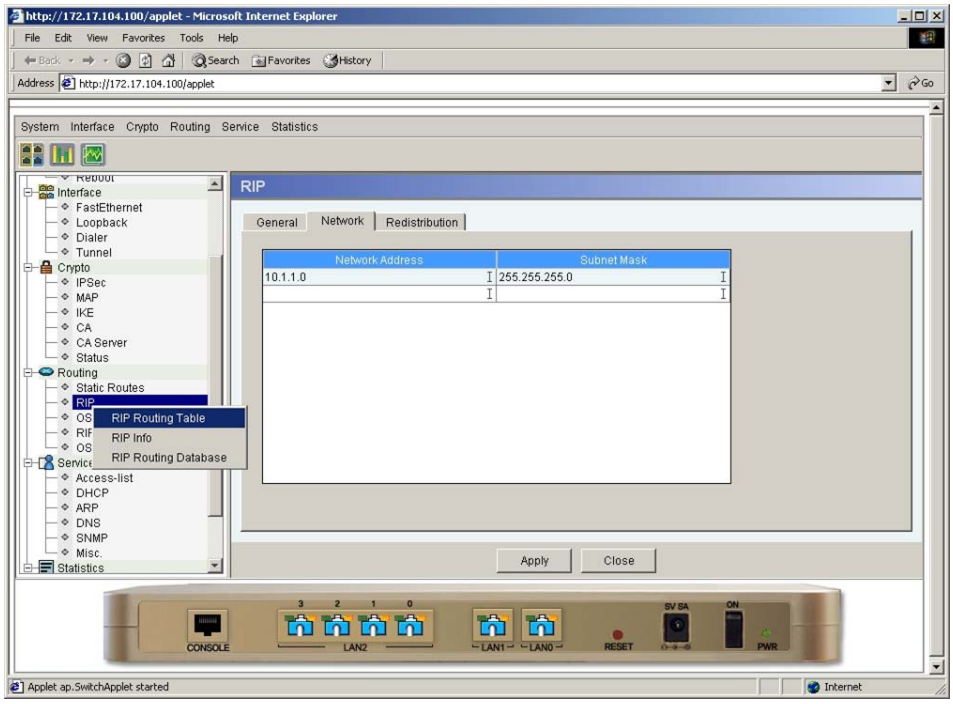


(Figure3-242) RIP Redistribution Main page

<Table 3-38> RIP Redistribution Description

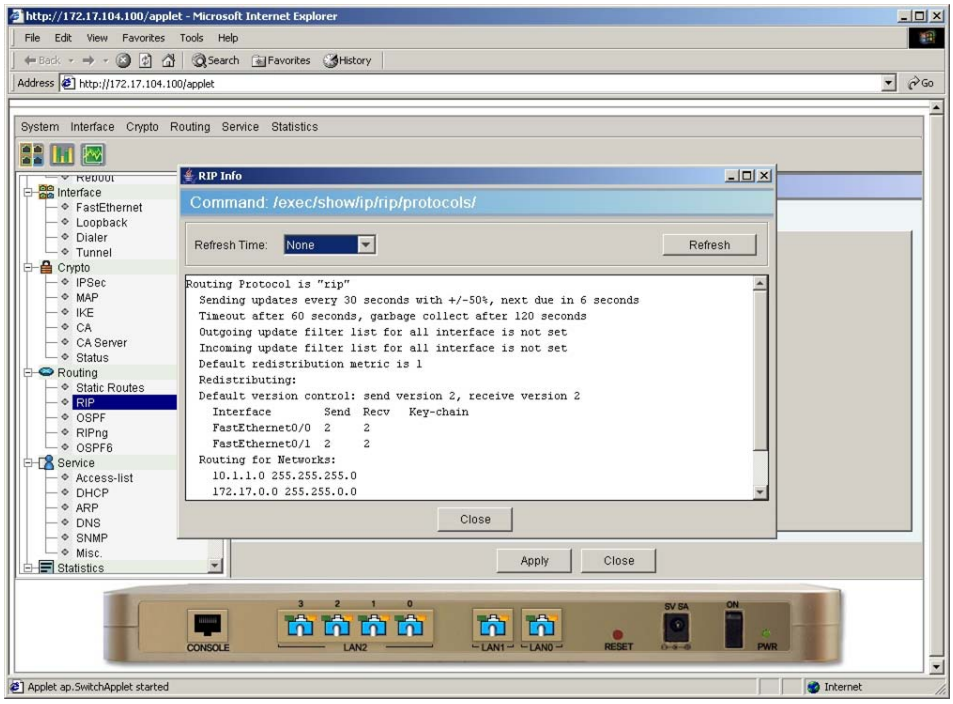
Elements	Description
Default-metric	Sets Offset value for sending RIP Packet. If it is over 16 Metric, RIP considers it as unreachable network. Default value is "1"
Default-Information	It informs Default information when sending RIP Packet.
Protocol Status	It checks protocols for exchanging Routing Protocol and Routing Table.
Protocol Metric	It defines default Metric for exchanging Routing Protocol and Routing Table.
Protocol route-map	It defines Route-map for exchanging Routing Protocol and Routing Table.

Click to see the information on current RIP. Click on right side of mouse. Figure 3-245 will be shown.



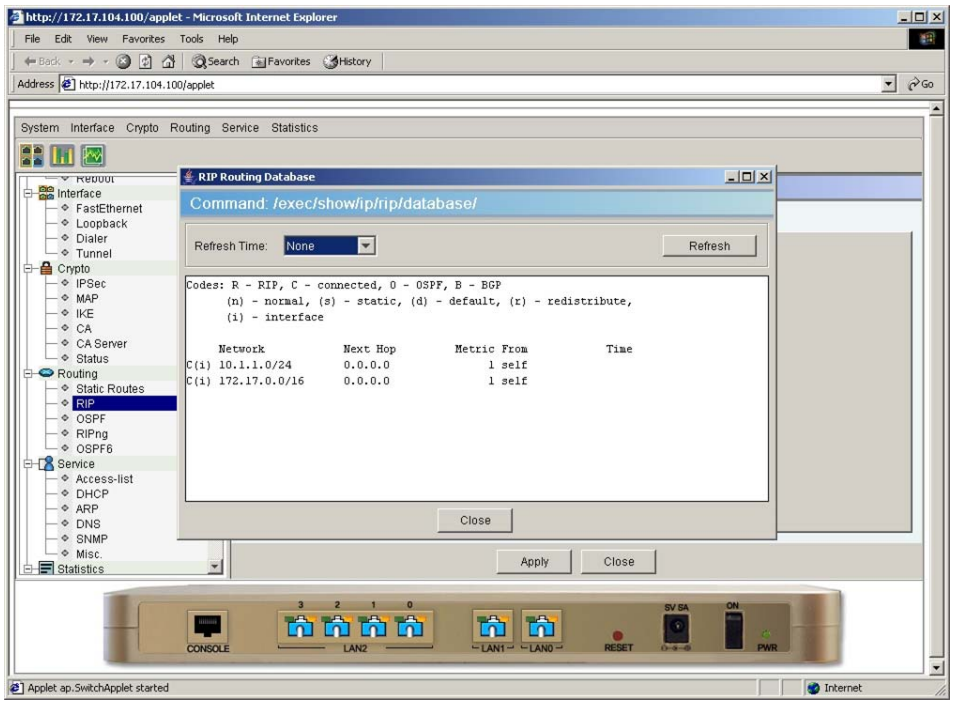
(Figure3-243) RIP Pop menu page

Figure 3-246 shows RIP Info page. Refresh Time can take from 3~5 second. Click “Refresh” to see the page right away.



(Figure3-244) RIP Info Page

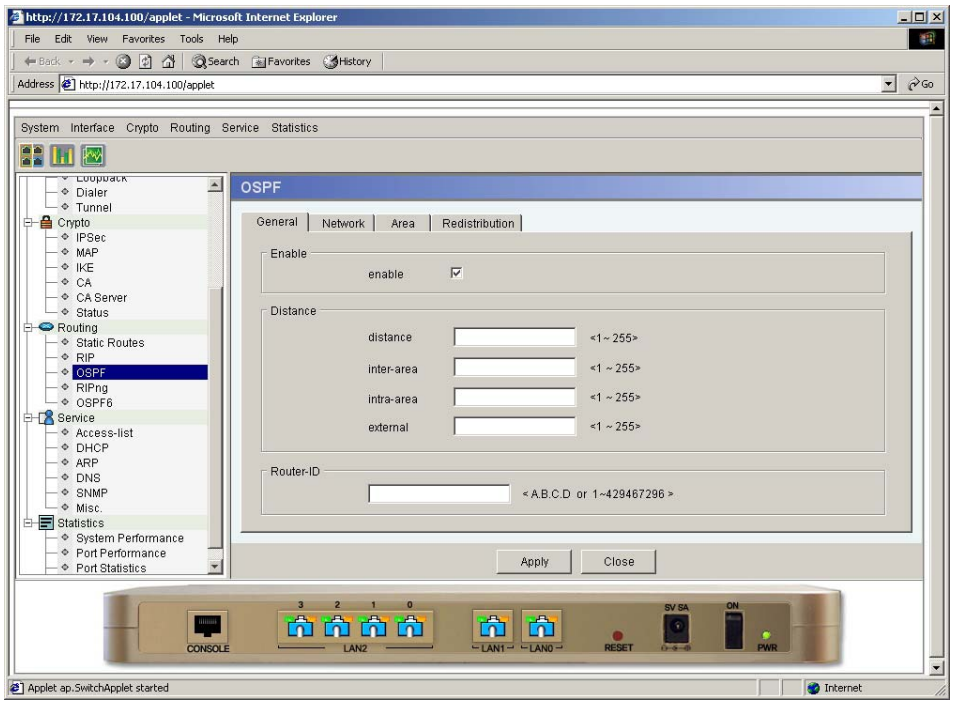
Figure 3-246 shows RIP Database page. Refresh Time can take from 3~5 second. Click “Refresh” to see the page right away.



(Figure3-245) RIP Database Page

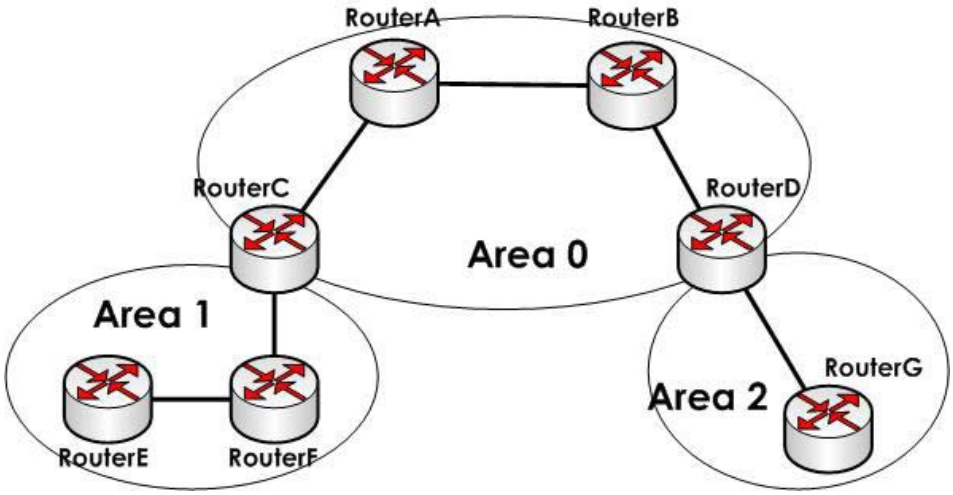
OSPF

OSPF (Open Short Path First) is IGP (Interior Gateway Protocol) which is developed from OSPF Working Group of IETF (Internet Engineering Task Force). OSPF is a Link State Protocol based on Shortest Path First (SPF) algorithm of Dijsktra. OSPF using IP protocol number “89” is a typical routing protocol which runs on Autonomous System. Each OSPF Router sustains database through Autonomous System topology information and creates Routing table to find a shortest path from database.



(Figure3-246) Routing OSPF Main page

Figure 3-249 is an example of OSPF Network Diagram.

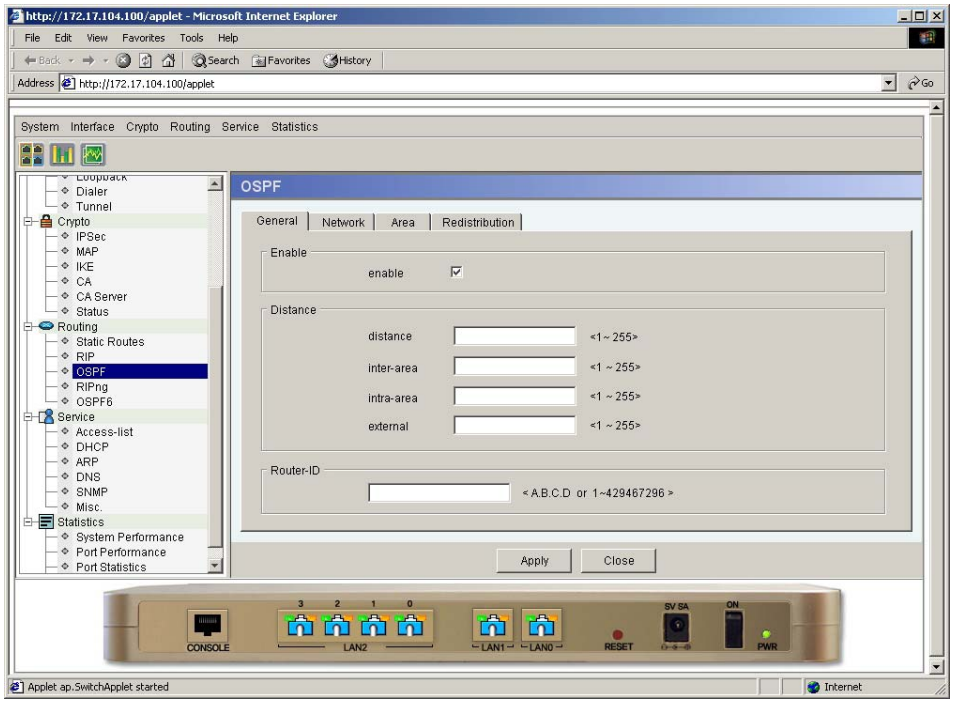


(Figure3-247) OSPF Network Diagram

In this example of Network Diagram, Area 0 is considered as a backbone network for connecting Area 1 and Area 2. RouterA and RouterB play as a backbone router and an inner router, RouterC, RouterD operate as ABR(Area Border Router) also as a backbone router for connecting Area 0, Area 1 and Area 2. Each RouterE, RouterF, RouterG is an inner router for Area 1 and Area 2.

Routing Table of OSPF is exchanged as a Link State Advertisement Packet. This Packet has complex information on Interface status, Bandwidth etc so OSPF is more efficient than RIP which counts number of Hops to find a path.

Figure 3-250 is OSPF General main page.



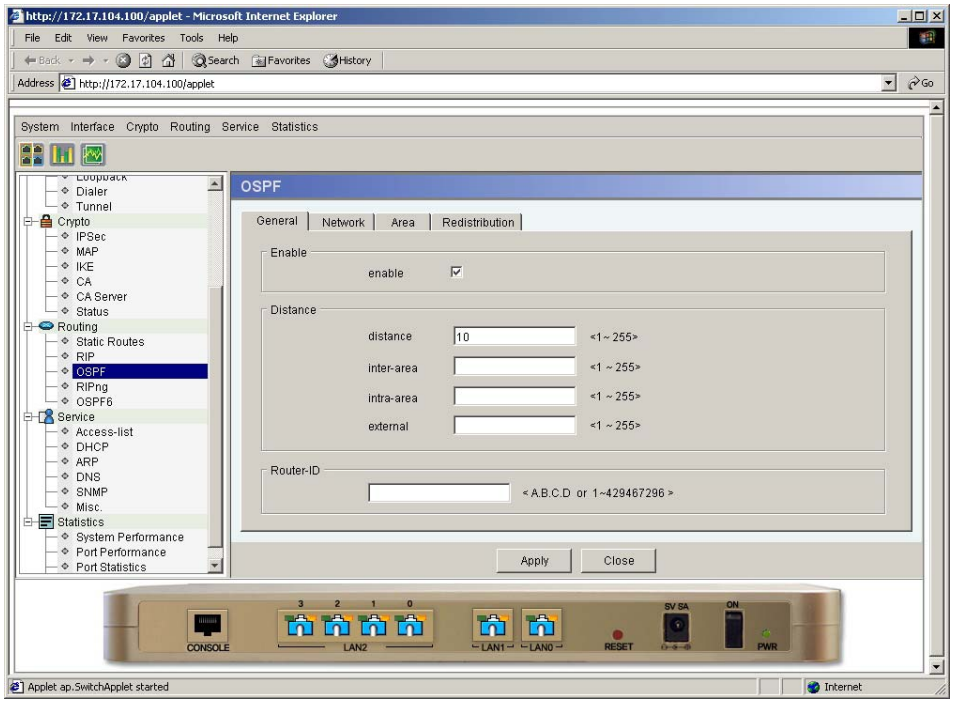
(Figure3-248) OSPF General main page

<Table 3-39> OSPF General Menu Description

Elements	Description
Enable	Enable or Disable of OSPF Protocol.
Distance	Input Distance Value of OSPF Protocol.
Inter-area	Input Distance Value of Inter-area route.
Intra-area	Input Distance Value of Intra-area route.
External	Input Distance Value of External route.
Router-ID	Input Router-ID to identify. Input IP Address or specific number.

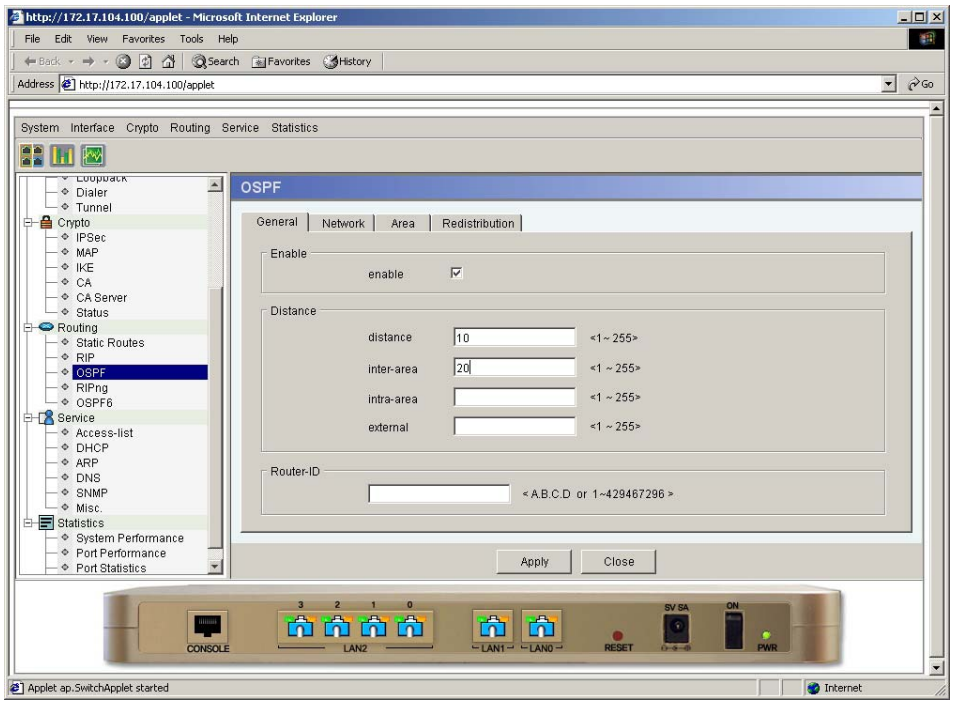
Figure 3-251 shows an example of configuring OSPF General.

First, Check “Enable” box to activate then, input “10” for Distance.



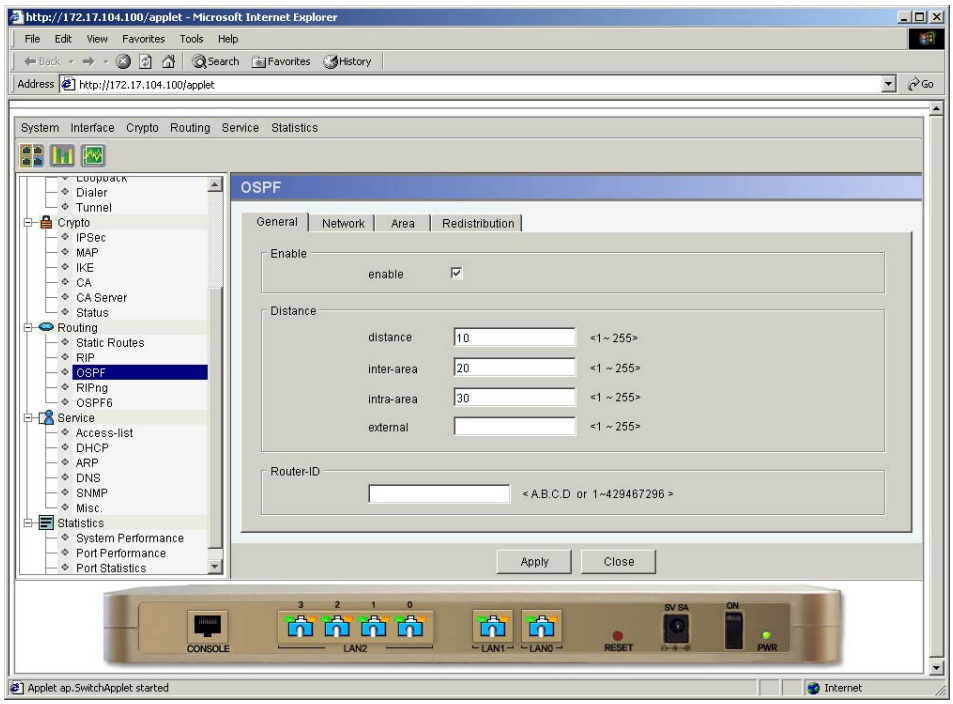
(Figure3-249) Input OSPF General Distance

Input “20” for Inter-area distance.



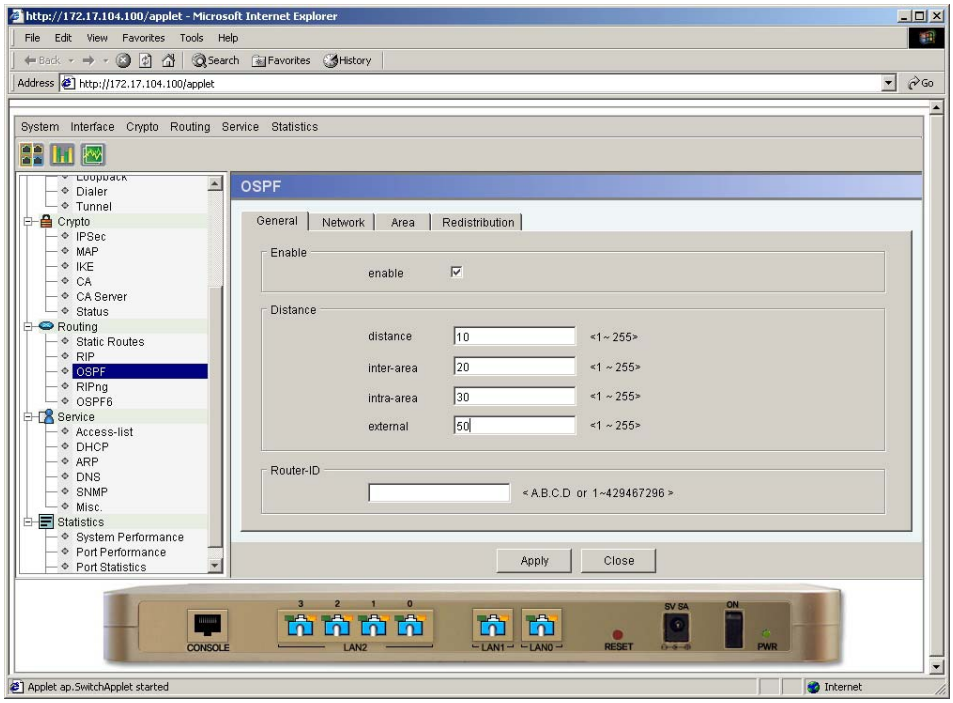
(Figure3-250) Input OSPF General Inter-area Distance

Input “30” for Intra-area distance.



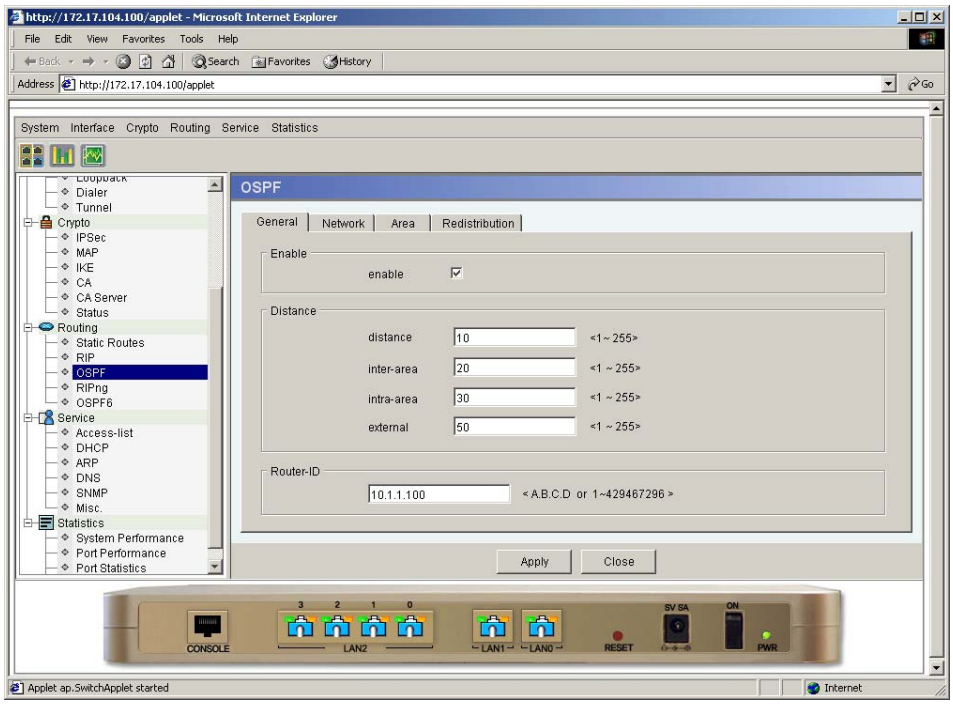
(Figure3-251) Input OSPF General Intra-area Distance

Input “50” for External distance.



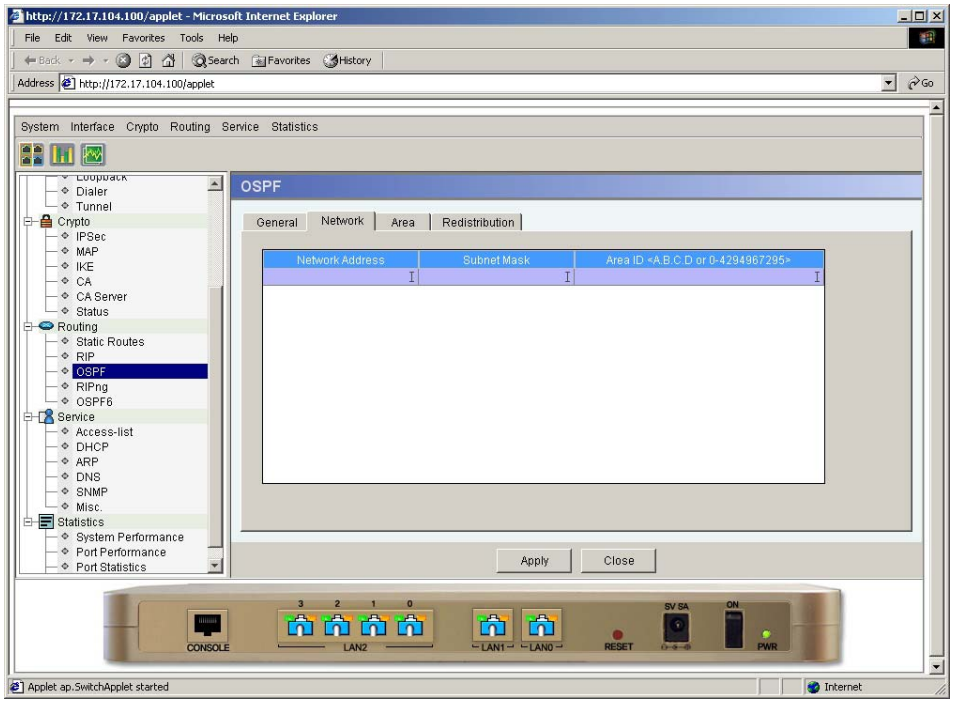
(Figure3-252) Input OSPF General External Distance

Input “10.1.1.100” for Router-ID



(Figure3-253) Input OSPF General Router-ID

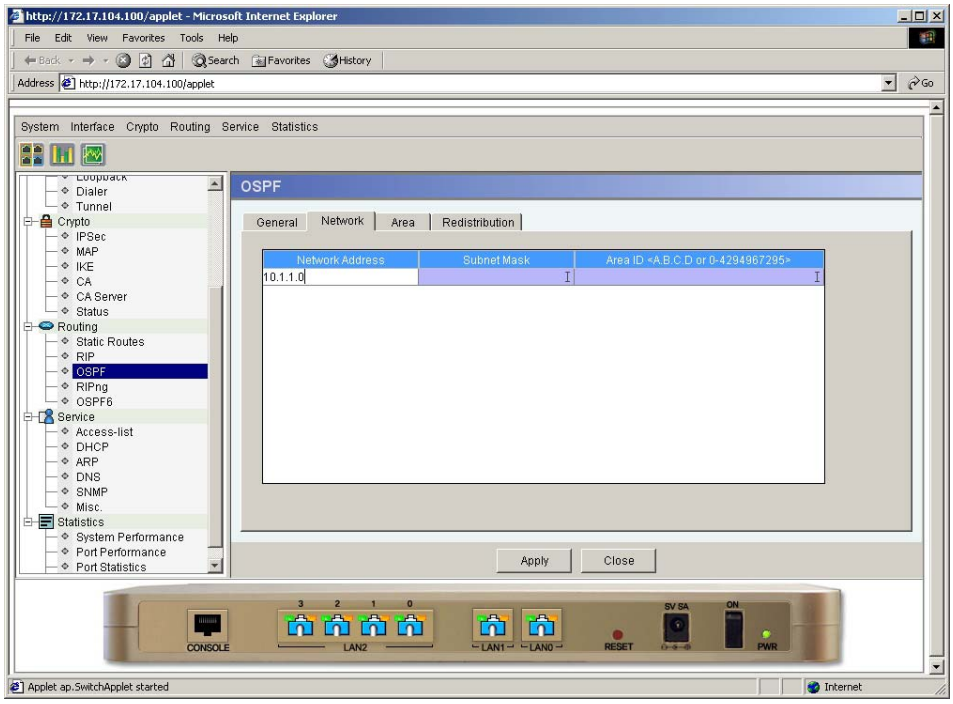
Figure 3-256 shows how to select OSPF Network. User can add or delete OSPF Routing Table in OSPF Network.



(Figure3-254) OSPF Network Page

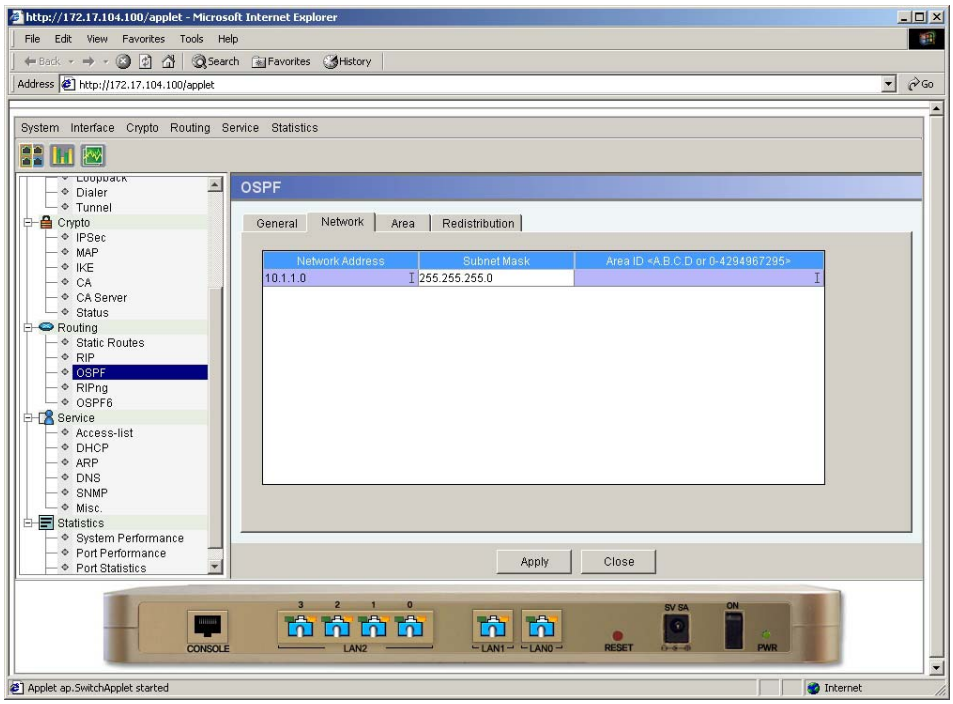
Figure 3-257 shows how to add a new Network “10.1.1.0/24”.

First input Network Address.



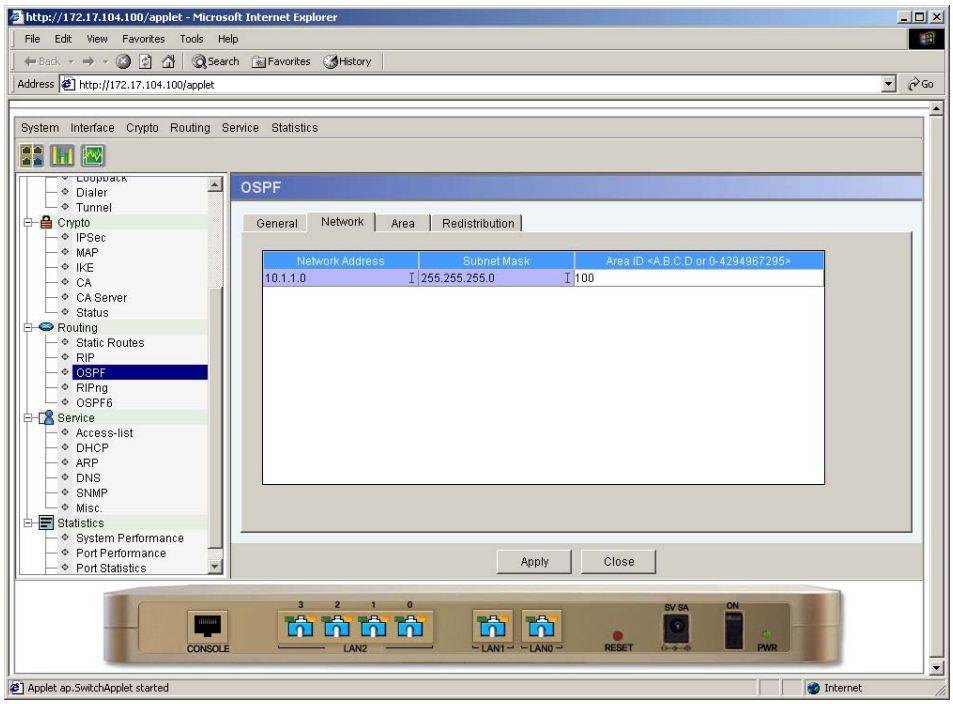
(Figure3-255) Add a new OSPF Network Address

Input Subnet mask “255.255.255.0” for the Network Address.



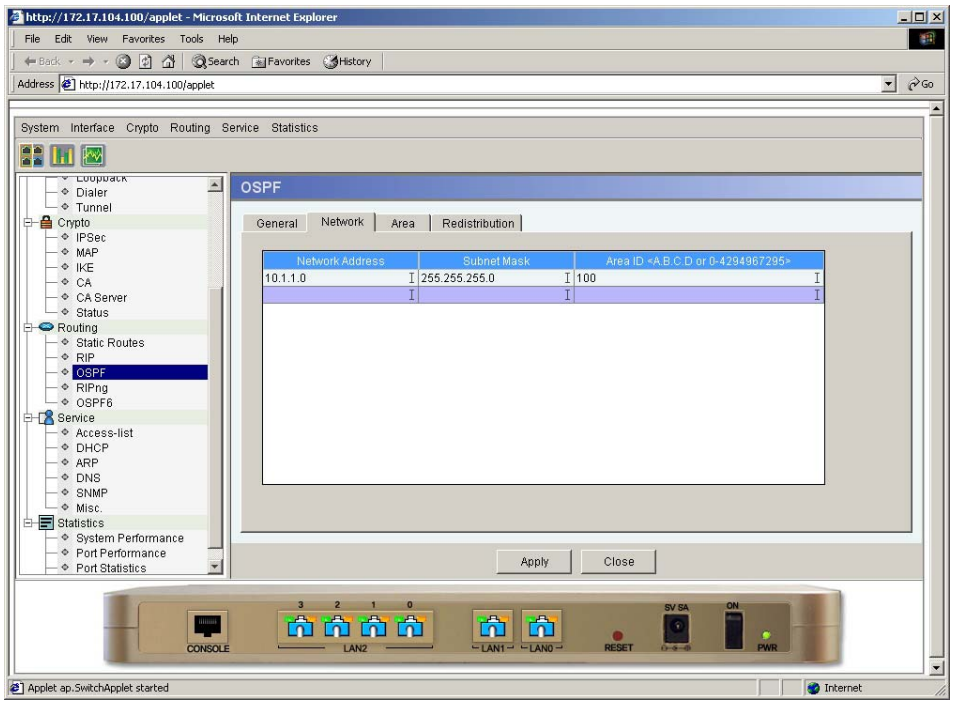
(Figure3-256) Input OSPF Network Subnet mask

Input “100” for Area ID.



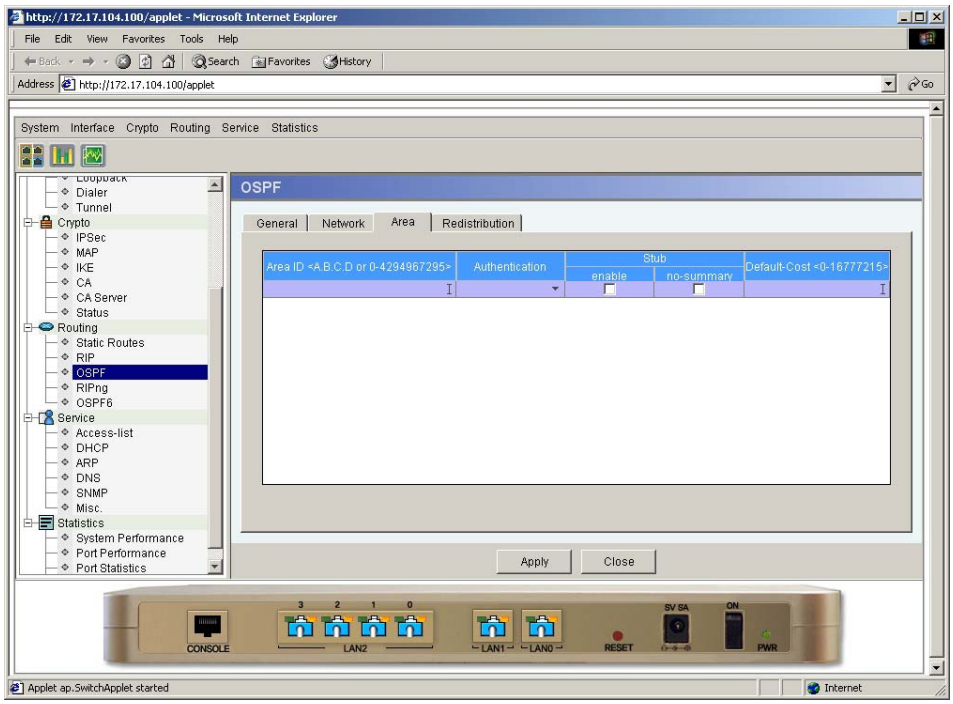
(Figure3-257) Input OSPF Network Area-ID

Click “Apply” to verify.



(Figure3-258) OSPF Network verification page

Area Settings on OSPF Area menu



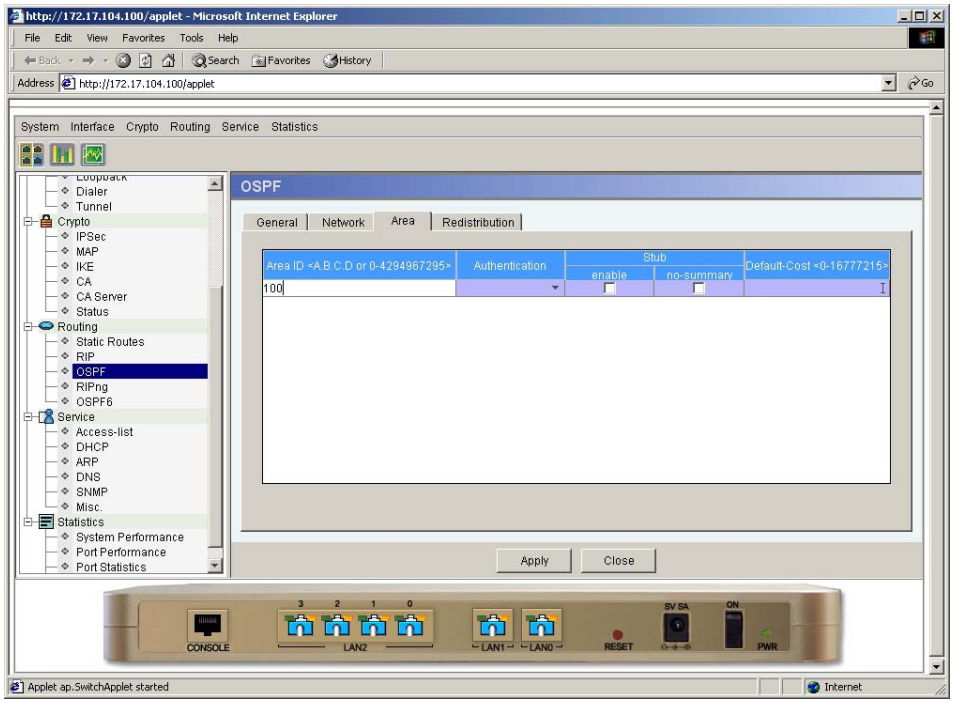
(Figure3-259) OSPF Area page

<Table 3-40> OSPF General Menu Description

Elements	Description
Area ID	Input Area ID.
Authentication	It decides whether to use authentication for exchanging Area info. Select one from None/SimpleText/Message-Digest.
Stub Enable	It decides whether to use Stub Area or not.
Stub no-summary	It is selected when Inter-Area is not included in Stub Area.
Default Cost	Default Cost Value for the Area.

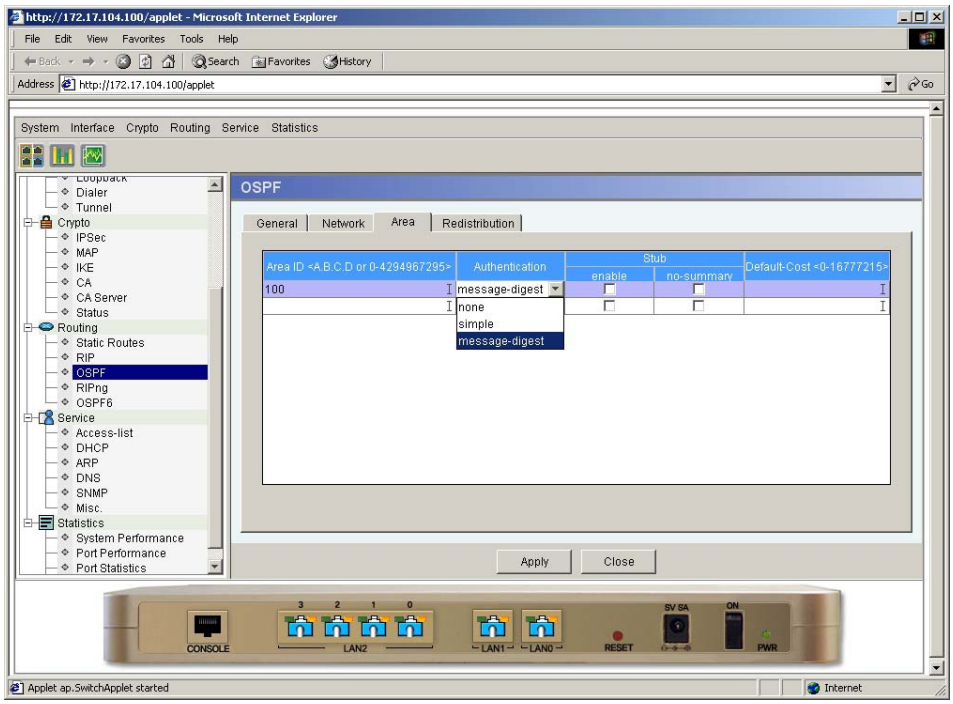
Figure 3-262 shows the example of OSPF Area 100.

Input “100” for Area-ID



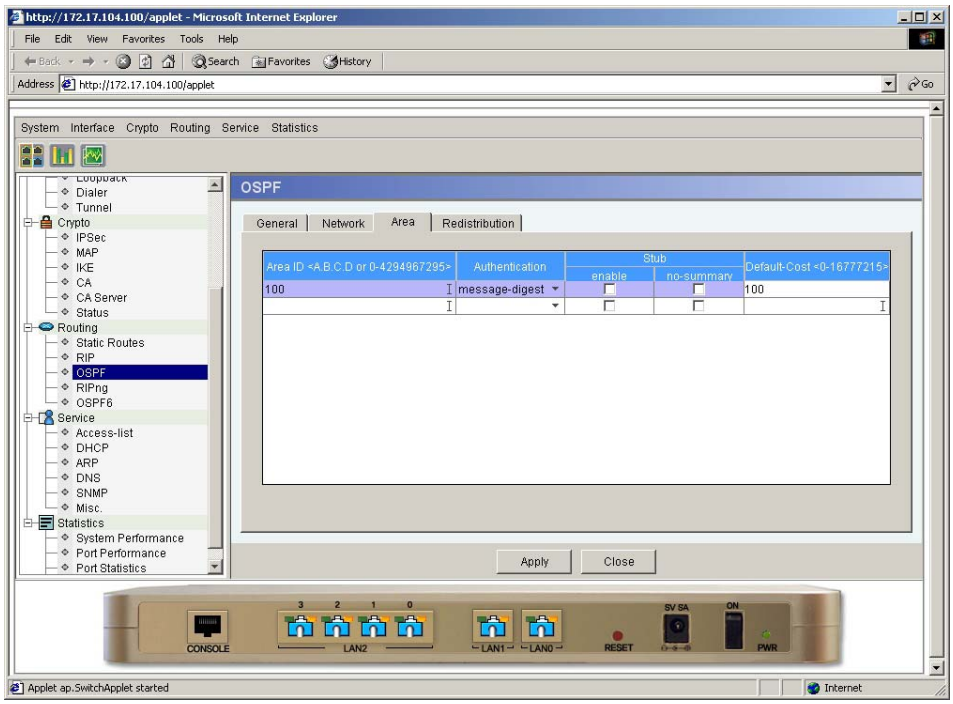
(Figure3-260) Input OSPF Area

Select Message-Digest for Authentication algorithm.



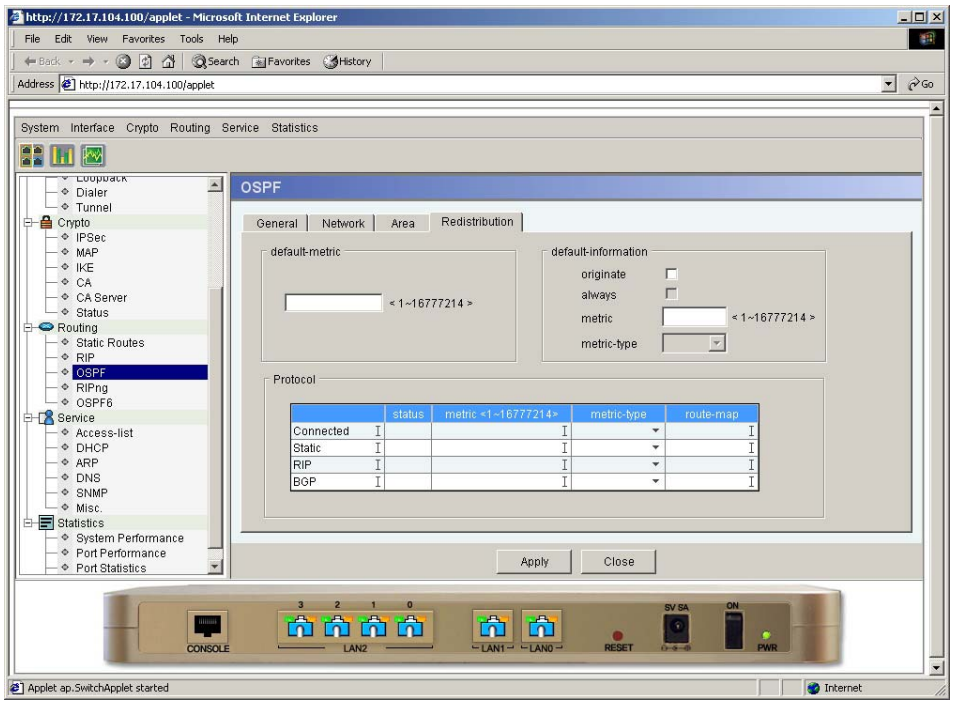
(Figure3-261) Select OSPF Area authentication method

Input “100” for Default Cost Click “Apply” to verify.



(Figure3-262) Input OSPF Area Default Cost

Figure 3-265 shows OSPF Redistribution page.

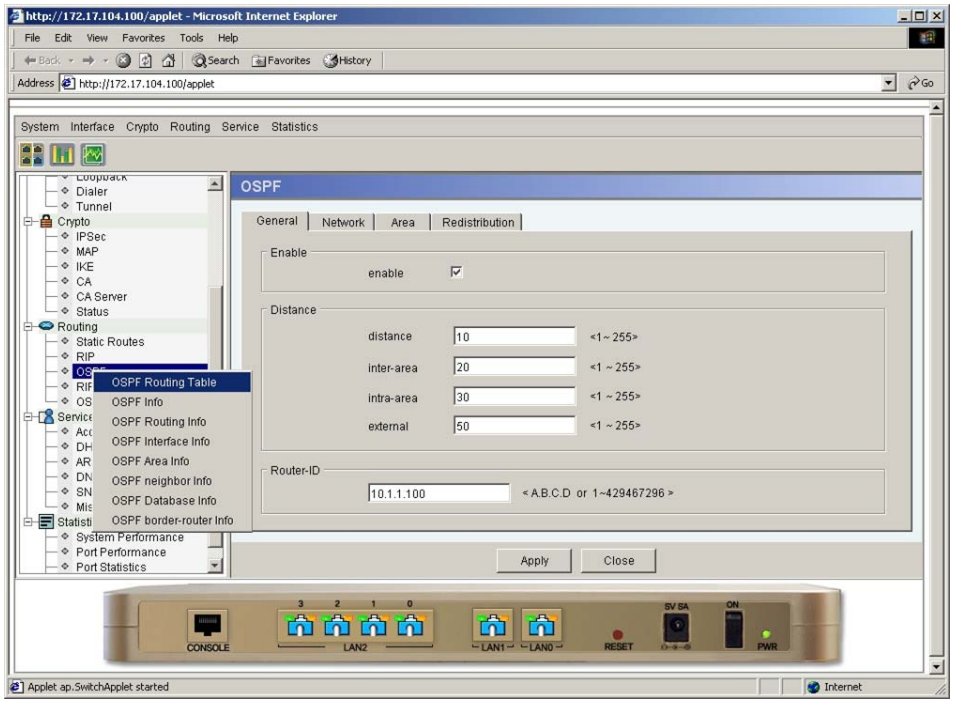


(Figure3-263) OSPF Redistribution page

<Table 3-41> OSPF Redistribution menu Description

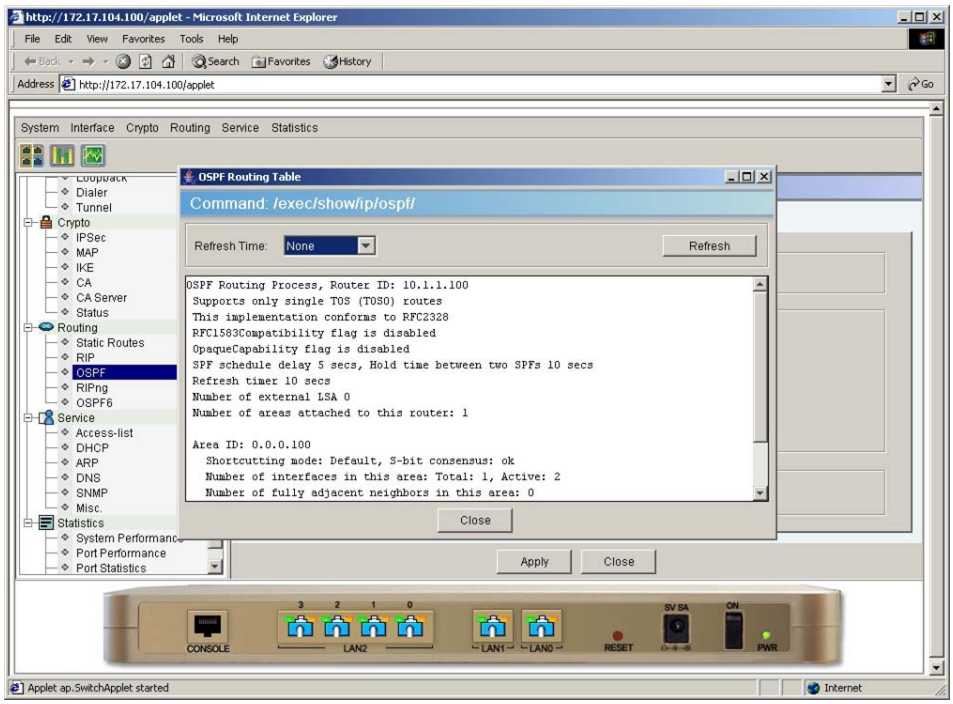
Elements	Description
Default-metric	Set Offset value for sending OSPF Packet.
Default-Information	It informs Default Router when sending OSPF Packet. Originate: Transfer Default-Information. Always: Always transfer Default-route. Metric: Defines metric for Default-route. Metric-type: Defines External Type 1/2 metric for Default-route.
Protocol Status	Check protocol when exchange Routing Protocol and Routing Table besides OSPF.
Protocol Metric	Defines default Metric when exchange Routing Protocol and Routing Table besides OSPF.
Protocol Metric-type	Defines OSPF External Type 1/2 Metric.
Protocol route-map	Defines Route-map for reference when exchange Routing Protocol and Routing Table besides OSPF.

Click right side of the mouse to see the current OSPF information. See the Figure 3-266.



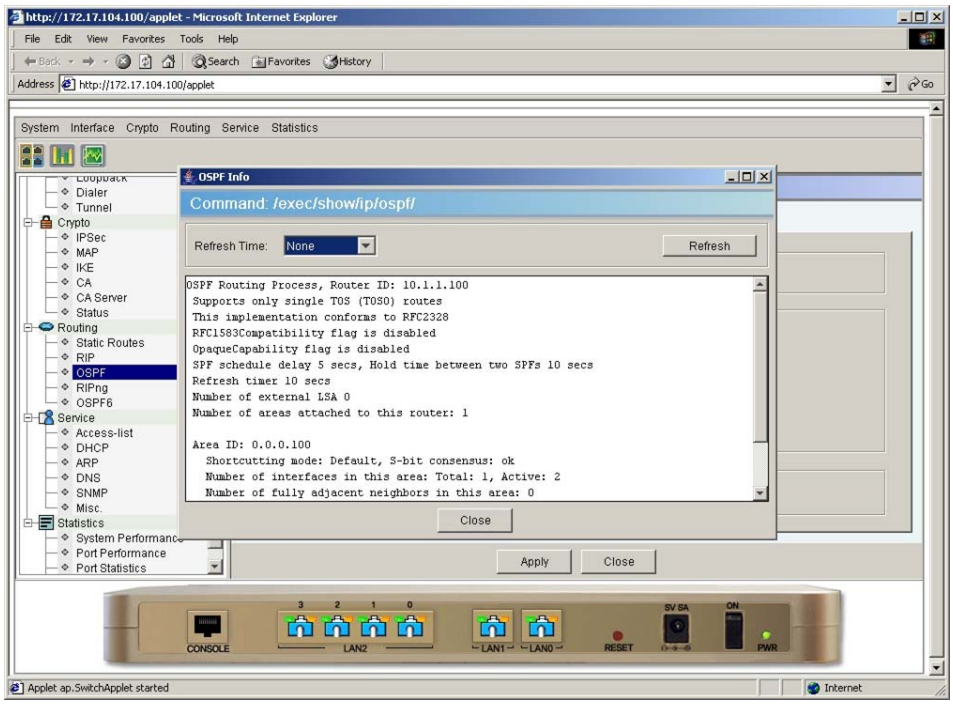
(Figure3-264) OSPF Pop Menu page

This shows OSPF Routing Table page.



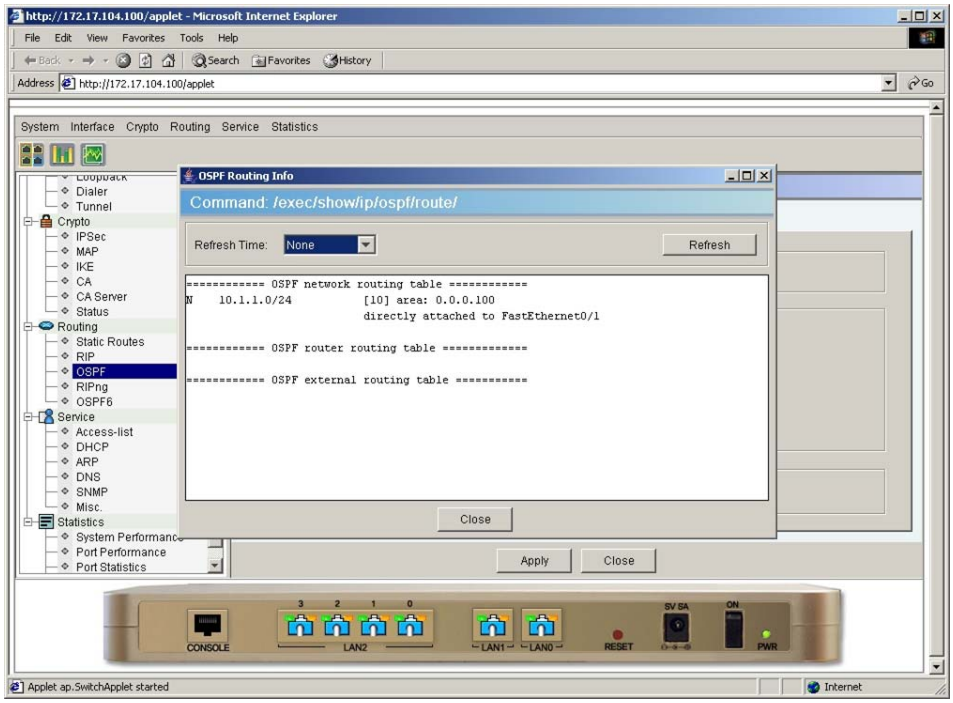
(Figure3-265) OSPF Routing Table page

This shows OSPF Info page.



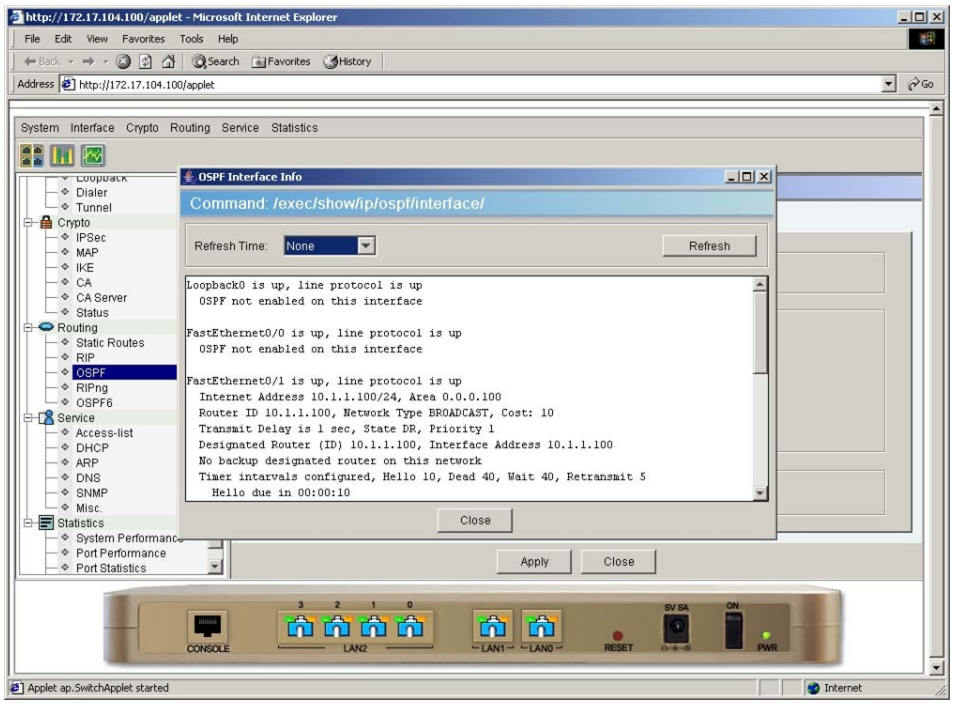
(Figure3-266) OSPF Info page

This shows OSPF Routing Info page.



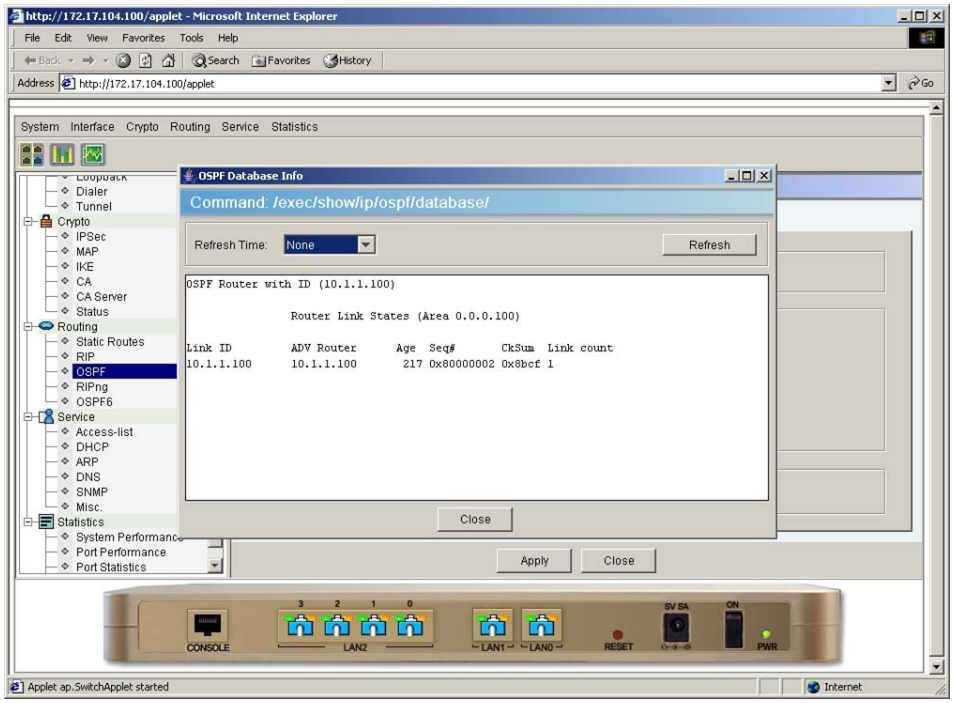
(Figure3-267) OSPF Routing Info page

This shows OSPF Interface Info.



(Figure3-268) OSPF Interface Info page

This shows OSPF Database Info.

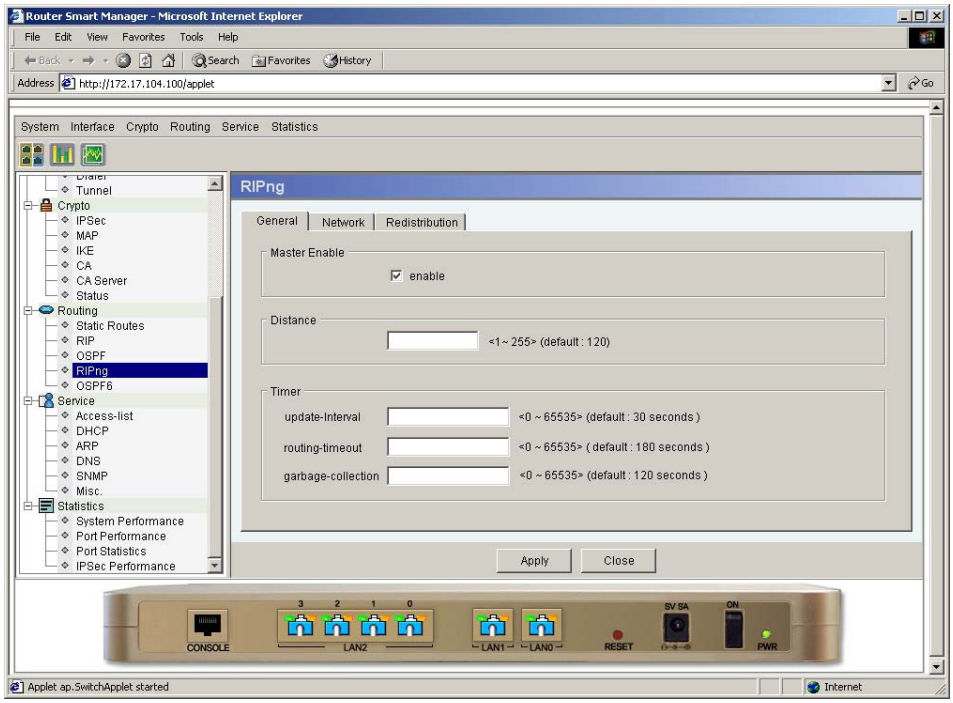


(Figure3-269) OSPF Database Info page

RIPng

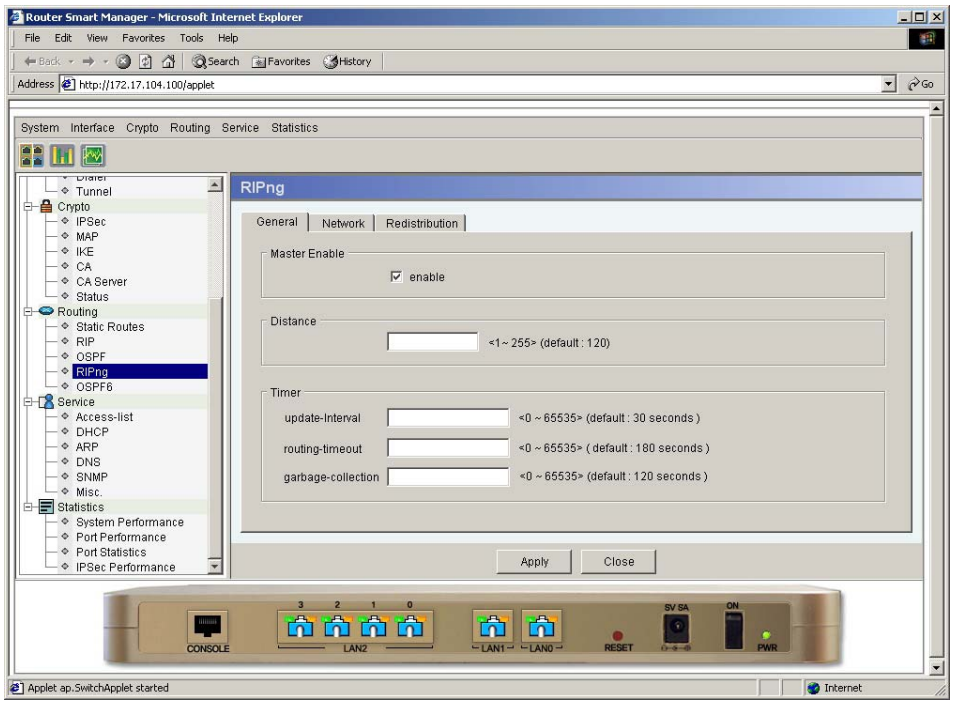
RIP (Routing Information Protocol) is widely used to manage Routing information in LAN or LAN group network environment.

RIPng (Routing Information Protocol next generation) is a IPv6 Routing protocol. It is based on IPv4 RIP.



(Figure3-270) Routing RIPng Main page

Figure 3-273 shows RIPng General Menu.



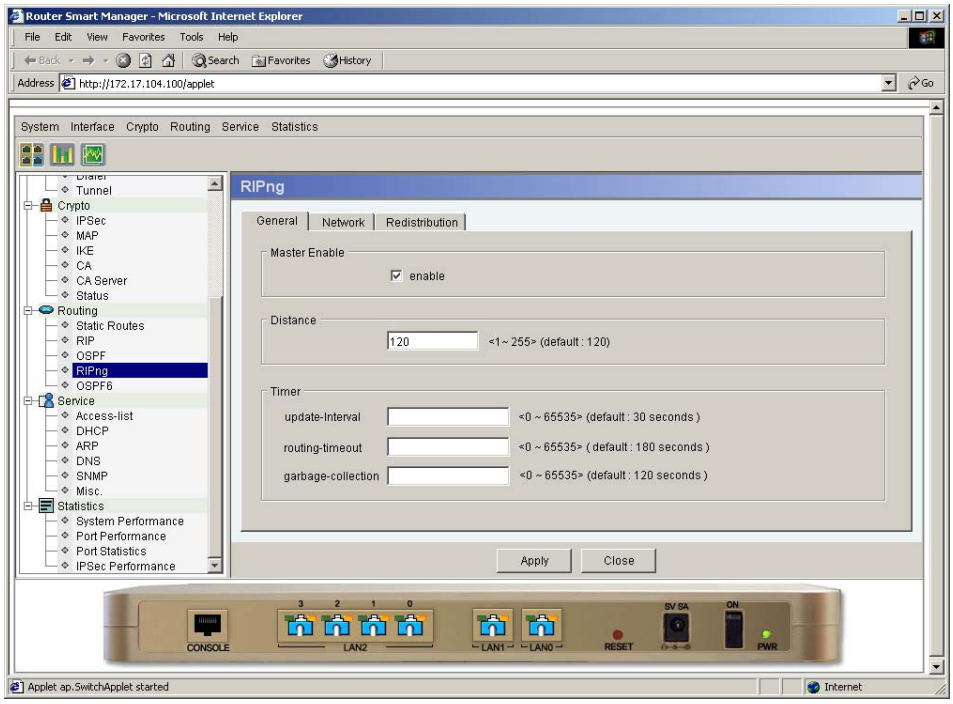
(Figure3-271) RIPng General Menu page

<Table 3-42> RIPng General Menu Description

Elements	Description
Master Enable	Select Enable or Disable for RIPng
Distance	Input Distance Value for RIPng. It can be selected from 1to 255. Default value is “120”
Update-Interval	Input update interval for Routing Table. Default value is “30” seconds.
Routing-Timeout	Sets waiting time for receiving Routing Table from a specific Interface. Default value is “180” sec.
Garbage-Collection	Sets the time for deleting a Routing Table after Routing-Timeout. Default value is “120” sec.

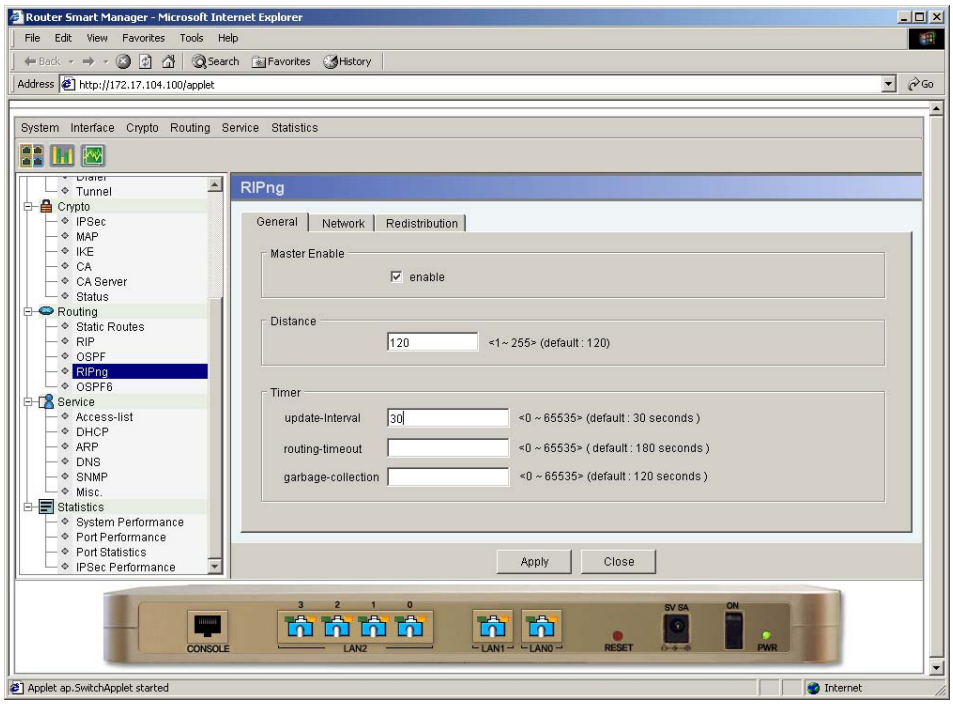
Figure 3-274 shows RIPng General Configuration page.

Input “120” for Distance



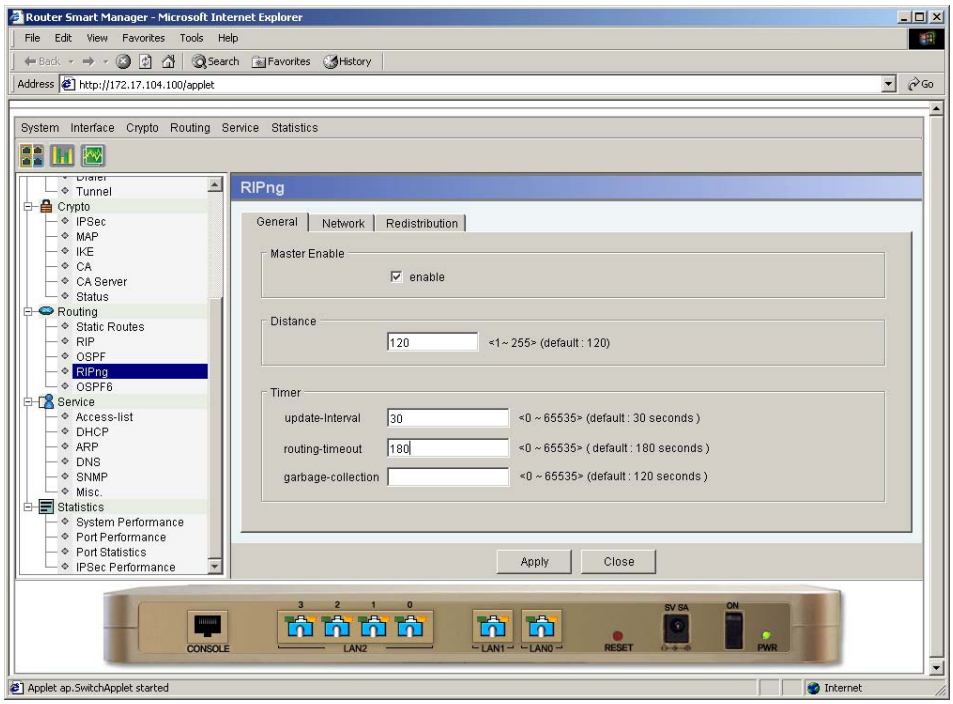
(Figure3-272) Input RIPng General Distance

Input “30” second for Update-Interval.



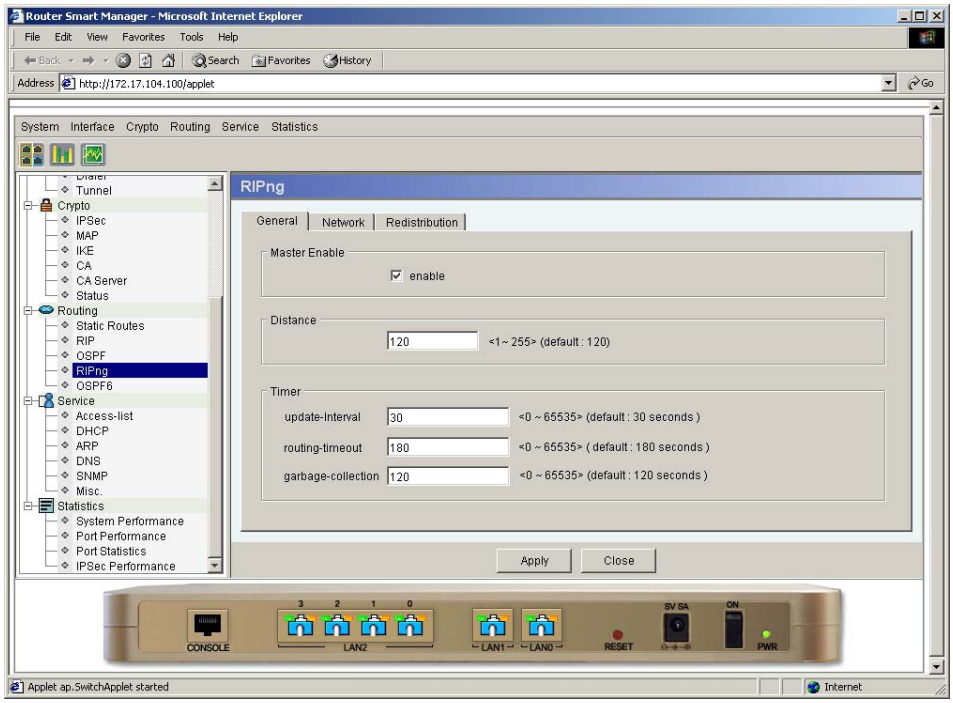
(Figure3-273) Input RIPng General Update-Interval

Input “180” for Routing-Timeout



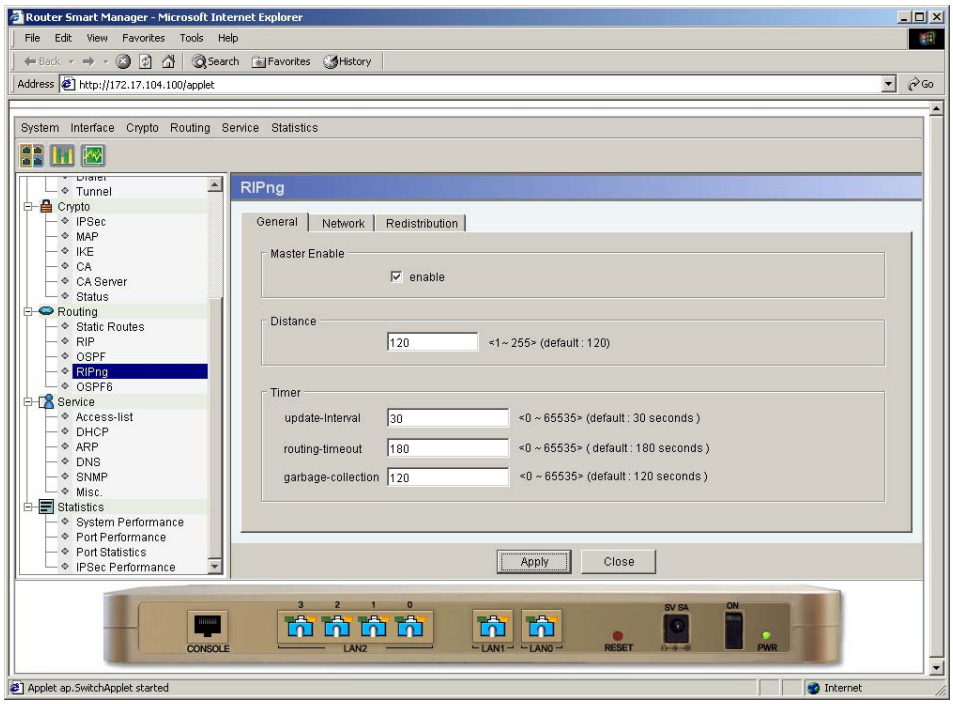
(Figure3-274) Input RIPng General Routing-Timeout

Input “120” for Garage-Collection



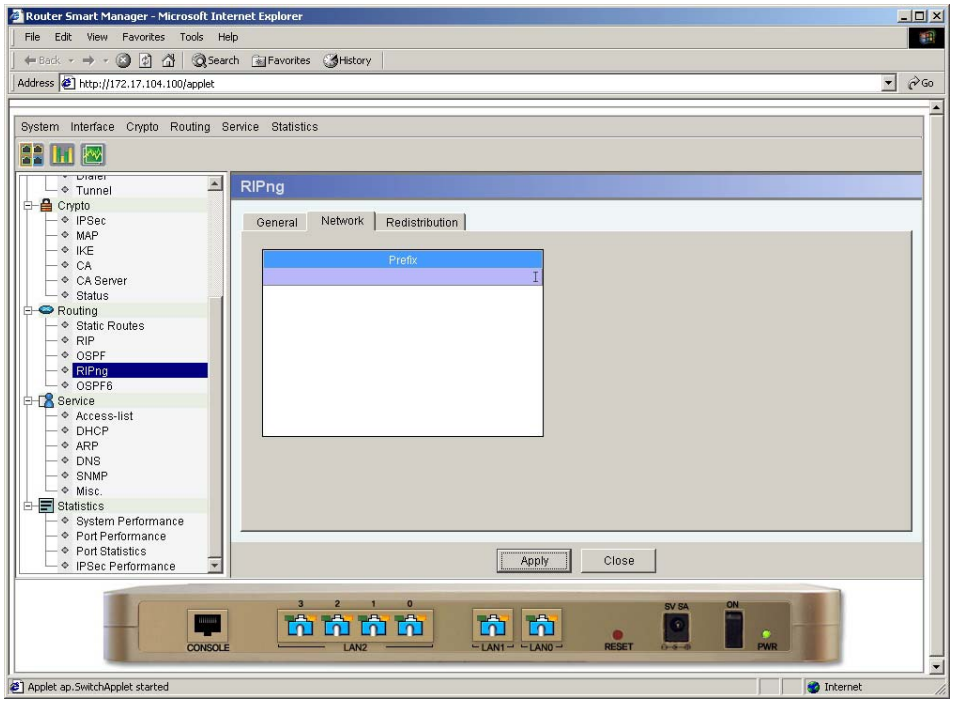
(Figure3-275) Input RIPng General Garage-Collection

Click “Apply” to verify.



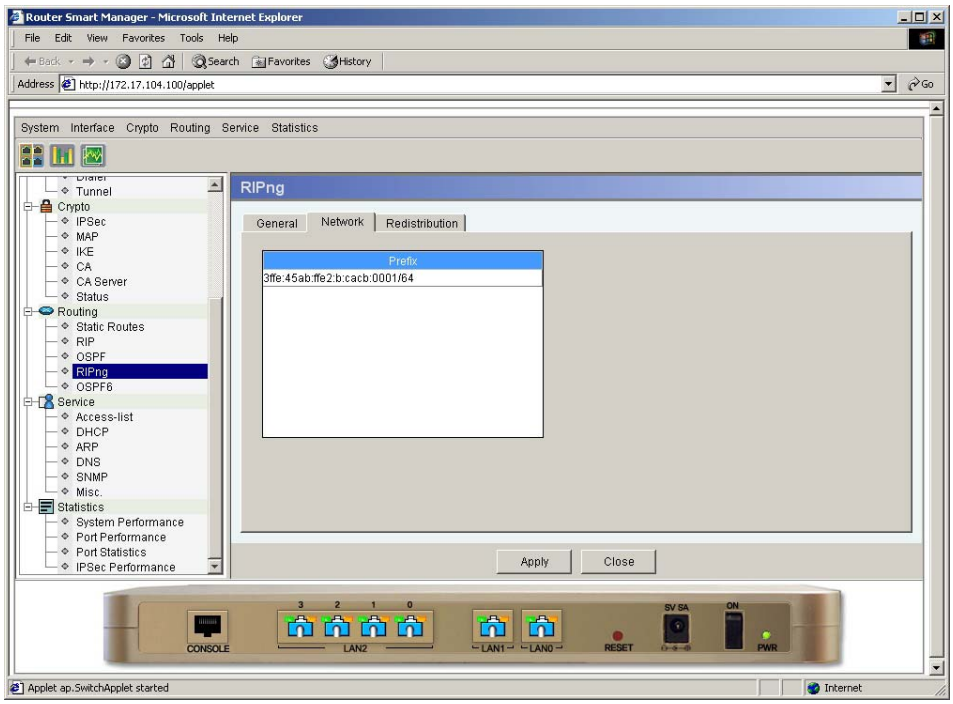
(Figure3-276) RIPng General Configuration verify

Figure 3-279 shows RIPng Prefix menu. Prefix menu plays the same role as RIP for IPv4 Network. So the user needs to input IPv6 network in Prefix field.



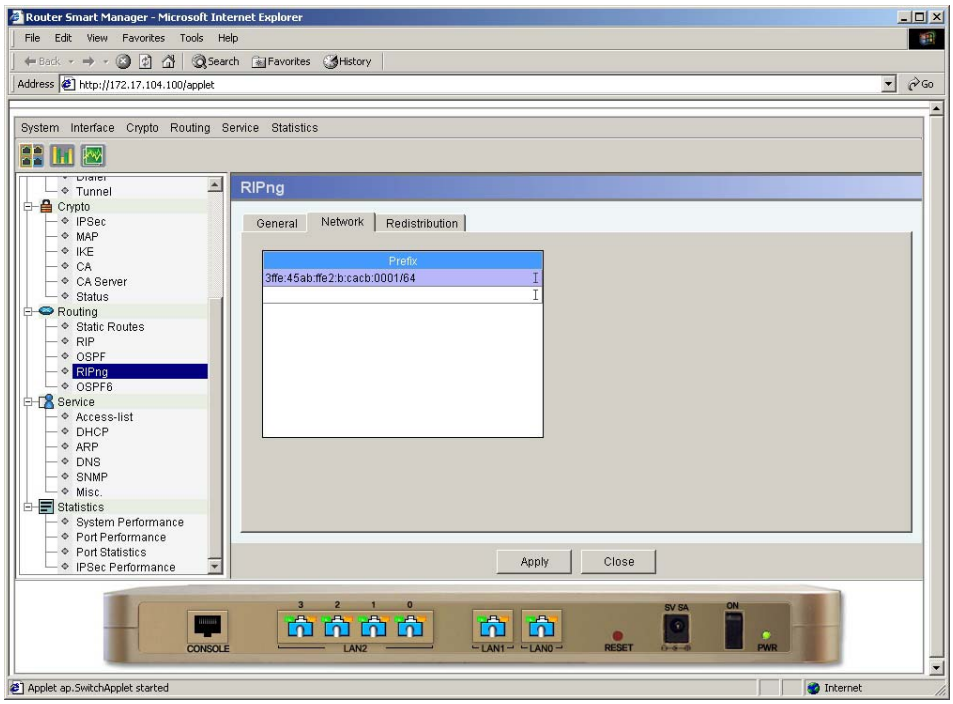
(Figure3-277) RIPng Prefix menu page

Figure 3-280 shows how to input Prefix. Input IPv6 network.



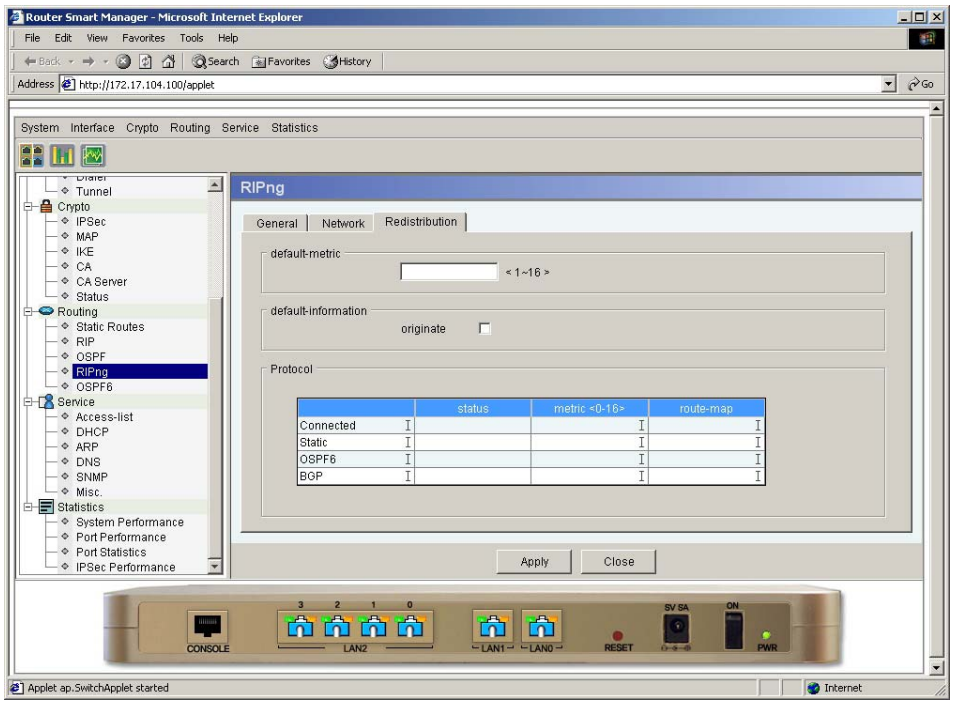
(Figure3-278) Input RIPng Prefix IPv6

IPv6 “3ffe:45ab:ffe2:b:cacb:0001/64” is added.



(Figure3-279) Verify RIPng Prefix IPv6

Figure 3-282 is RIPng Redistribution menu.



(Figure3-280) RIPng Redistribution menu page

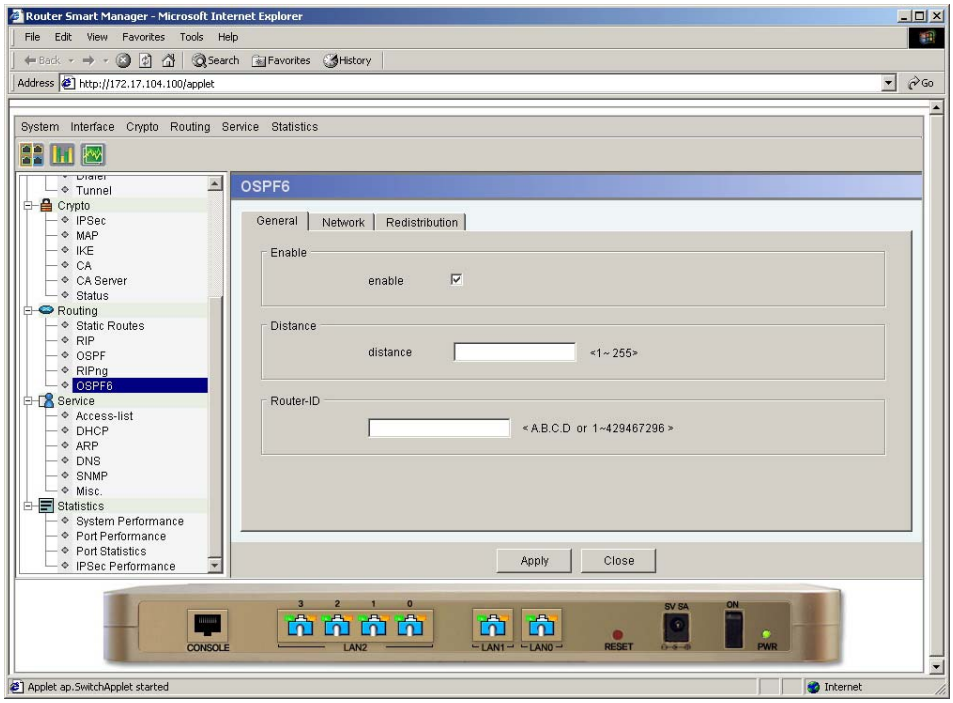
<Table 3-43> RIPng Redistribution menu Description

Elements	Description
Default-metric	Sets Offset value for sending RIPng Packet. If it is over 16 Metric, RIPng considers it as unreachable network. Default value is “1”
Default-Information	It informs Default information when sending RIPng Packet.
Protocol Status	It checks protocols for exchanging Routing Protocol and Routing Table.
Protocol Metric	It defines default Metric for exchanging Routing Protocol and Routing Table.
Protocol route-map	It defines Route-map for exchanging Routing Protocol and Routing Table.

OSPF6

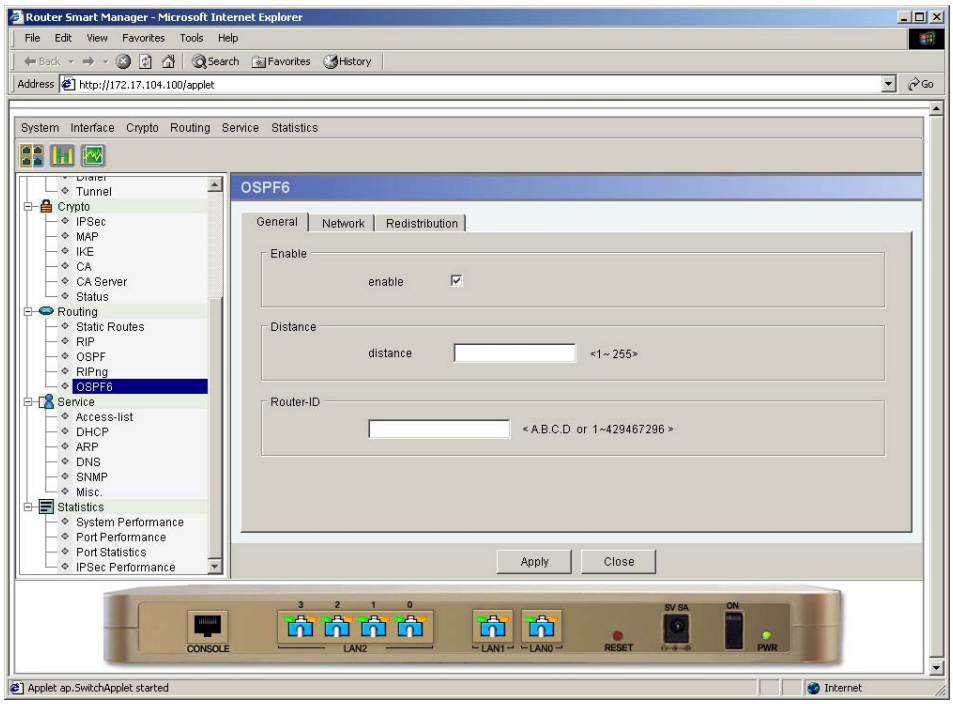
OSPF (Open Short Path First) is IGP (Interior Gateway Protocol) which is developed from OSPF Working Group of IETF (Internet Engineering Task Force). It uses Link State algorithm. OSPF is designed to support IP network so it supports Tagging for Routing info which goes in and out with IP Subnet. Also OSPF supports Packet Authentication to neighboring switches and it uses IP Multicast when exchanging Packet info.

Like OSPF for IPv4, OSPF6 is designed to support IPv6. Therefore basic operation algorithm is the same as OSPF for IPv4.



(Figure3-281) Routing OSPF6 Main page

Figure 3-284 shows OSPF General Menu.

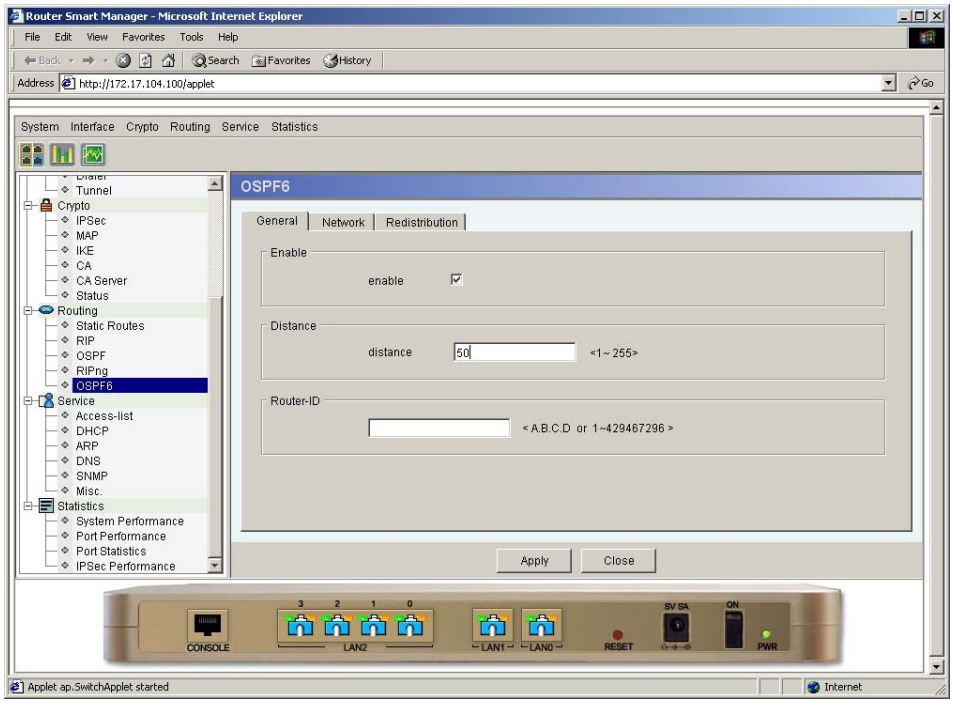


(Figure3-282) OSPF6 General Menu page

<Table 3-44> OSPF6 General Menu Description

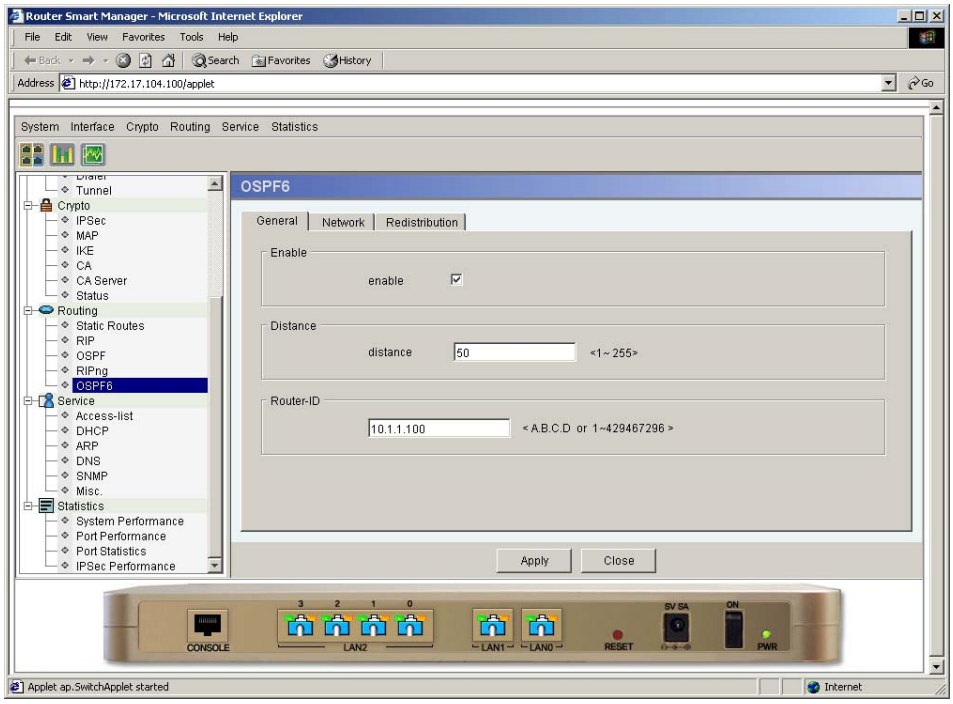
Elements	Description
Enable	Sets Enable or Disable of OSPF Protocol.
Distance	Input Distance Value of OSPF Protocol.
Router-ID	Input Router-ID to identify when exchanging Routing Table. Input IP Address or a specific number.

Figure 3-285 shows the example of OSPF6 General Configuration. First, check “Enable” box to activate then input “50” for Distance.



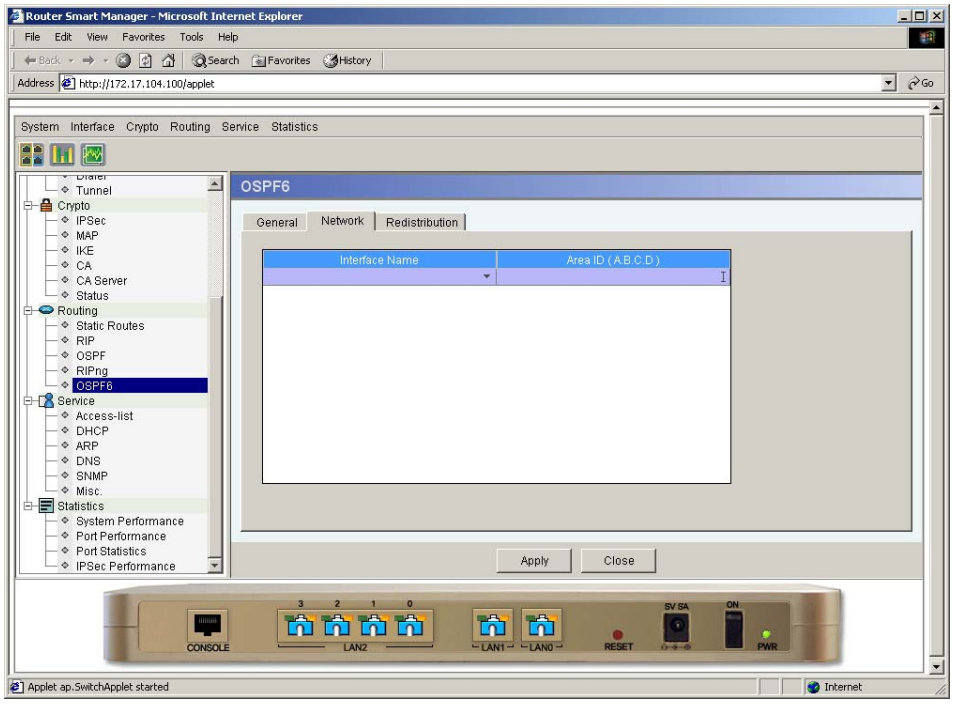
(Figure3-283) Input OSPF6 General Distance

Input “10.1.1.100” for Router-ID



(Figure3-284) Input OSPF6 General Router-ID

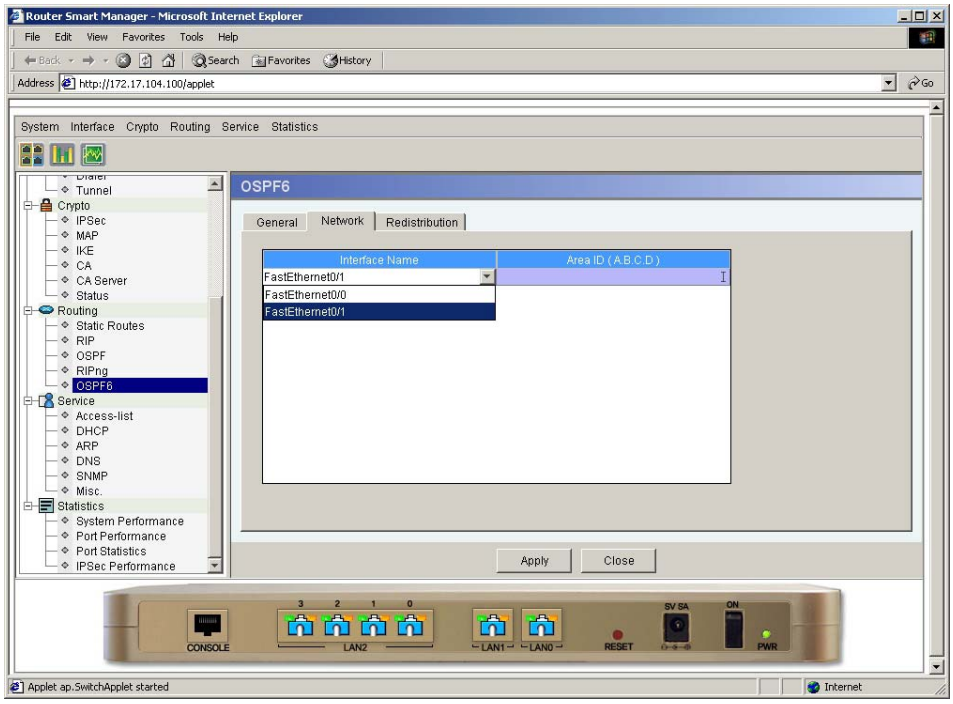
Figure 3-287 shows how to select OSPF6 Network. The user can add or delete OSPF6 Area in OSPF6 Network.



(Figure3-285) Select OSPF6 Network

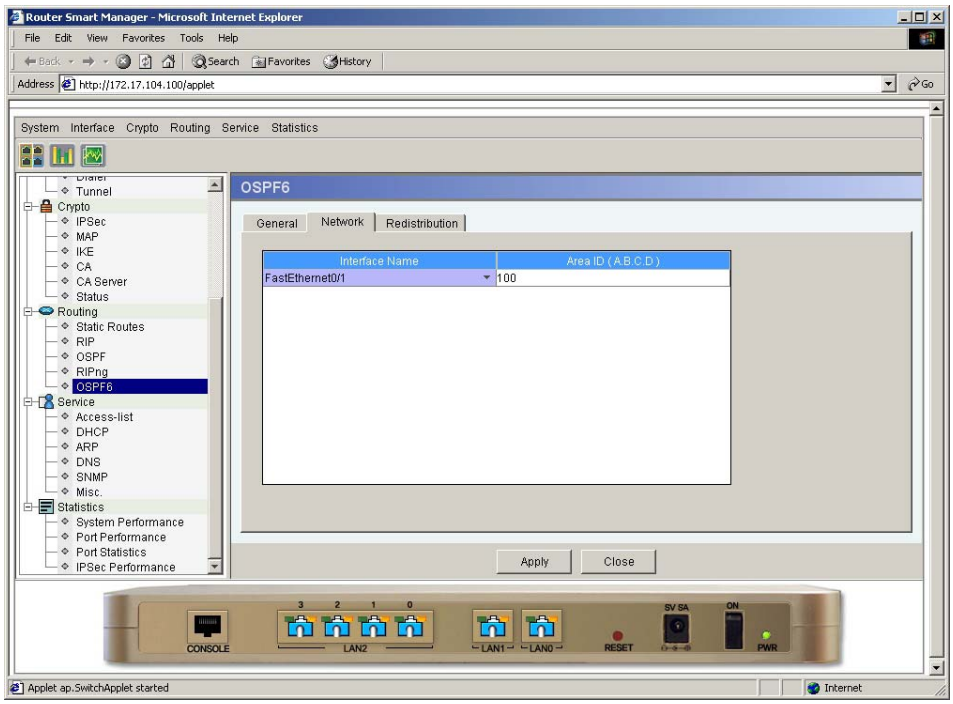
Figure 3-288 shows how to add a new Area.

First, select Interface Fast Ethernet 0/1.



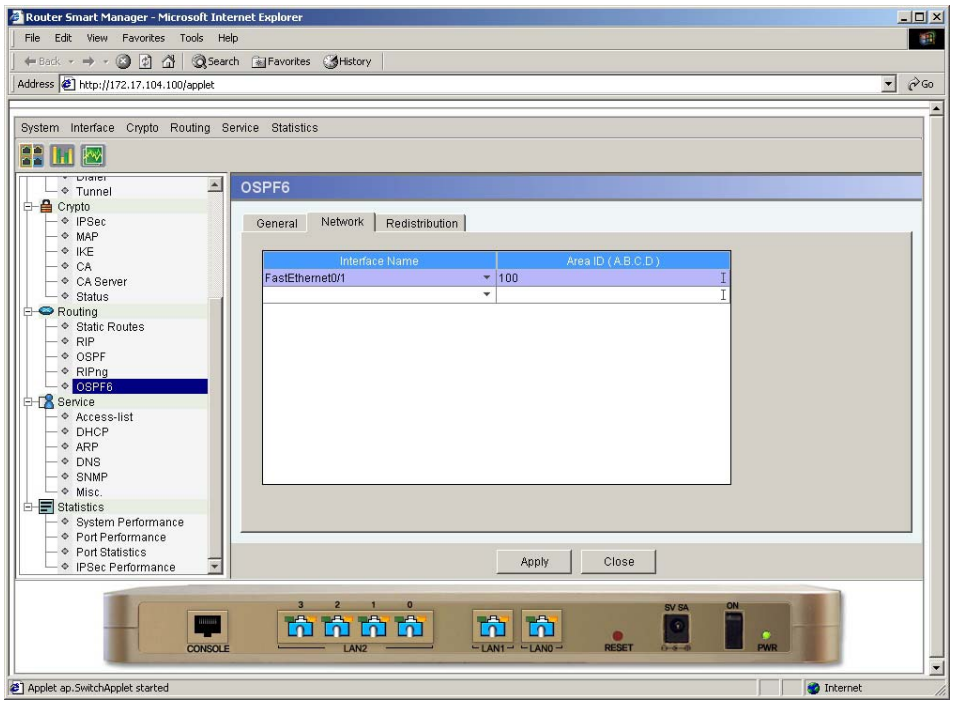
(Figure3-286) Input OSPF6 Network Interface

Input “100” for Area ID



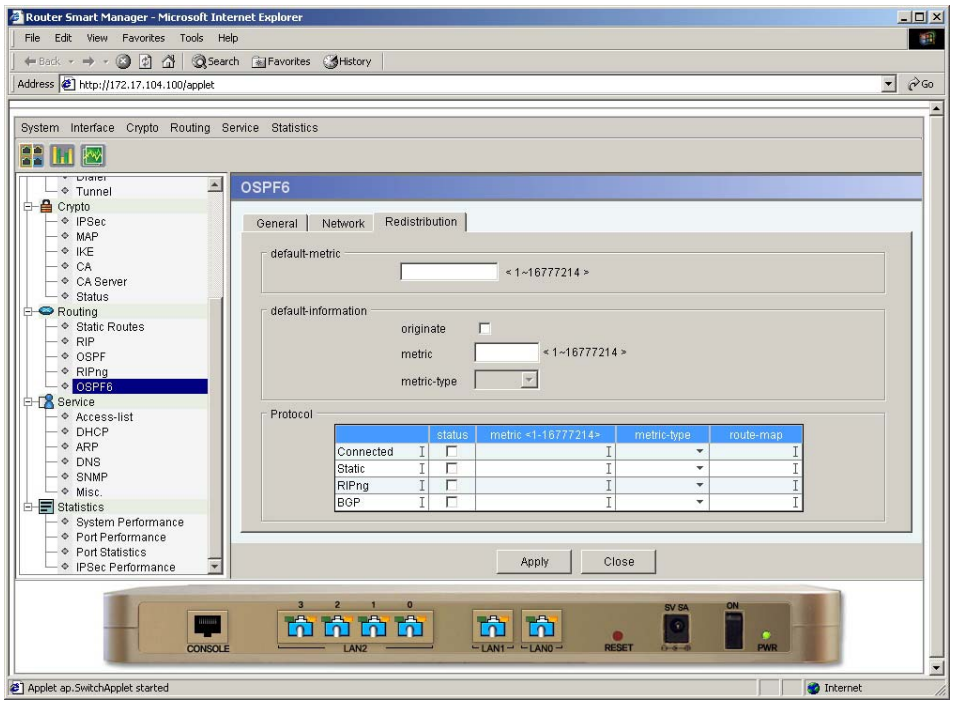
(Figure3-287) Input OSPF6 Network Area ID

Click “Apply” to verify.



(Figure3-288) OSPF6 Network configuration verify

Figure 3-291 shows how to select OSPF6 Redistribution.

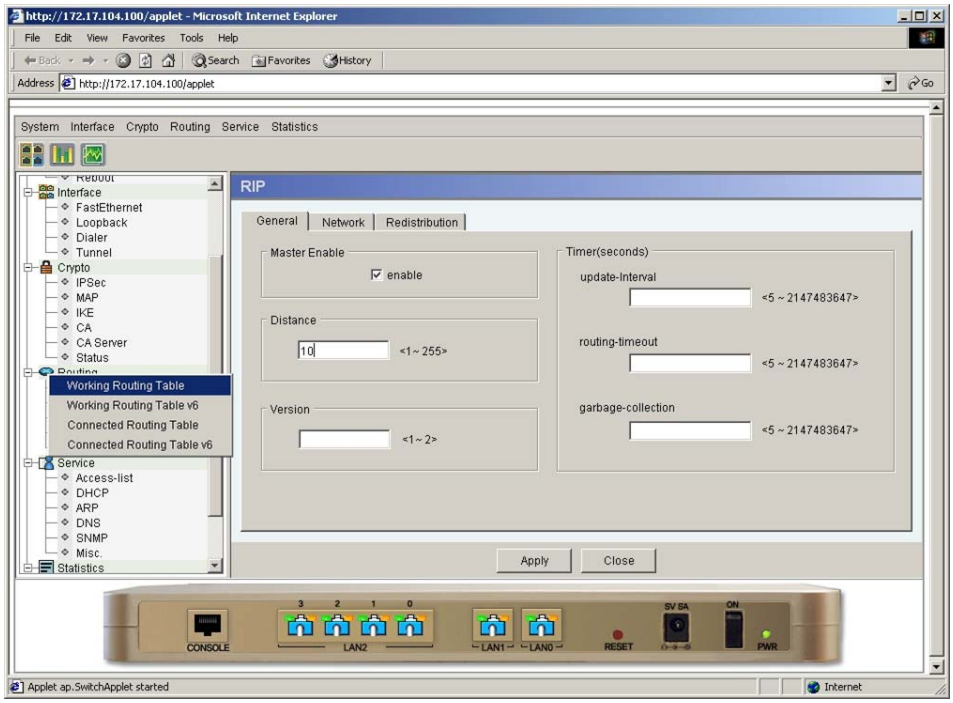


(Figure3-289) OSPF6 Redistribution page

<Table 3-45> OSPF6 Redistribution menu Description

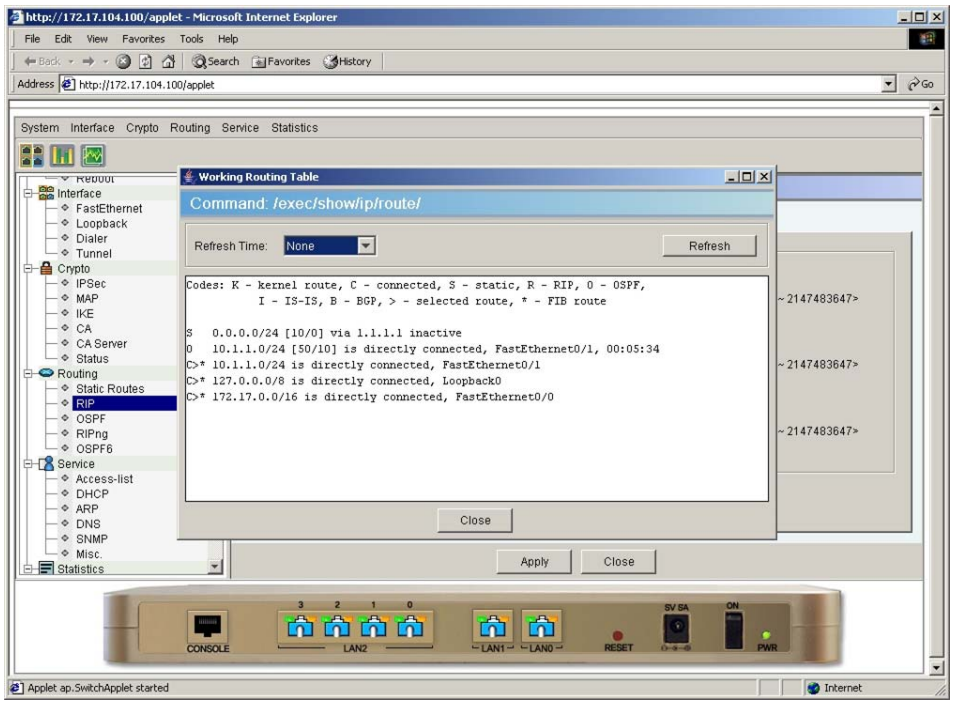
Elements	Description
Default-metric	Defines Offset value for sending OSPF Packet.
Default-Information	It informs Default Router when sending OSPF Packet Originate : Transfer Default-Information Metric: defines Metric for Default-route. Metric-type: defines External Type 1/2 metric for Default-route.
Protocol Status	Check protocol when exchanging Routing Protocol and Routing Table besides OSPF.
Protocol Metric	Defines default Metric when exchanging Routing Protocol and Routing Table besides OSPF.
Protocol Metric-type	Defines OSPF External Type 1/2 Metric.
Protocol route-map	Defines Route-map for reference when exchanging Routing Protocol and Routing Table besides OSPF.

Click right side of the mouse to see the information on current Routing Table. Click “Routing” menu.



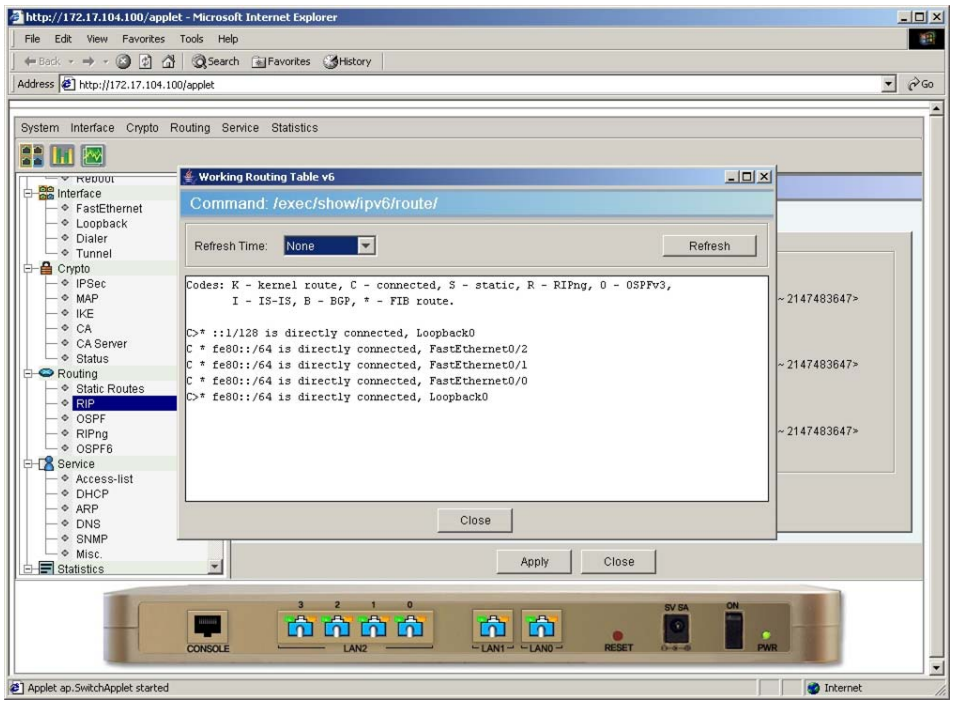
(Figure3-290) Routing Pop menu page

Figure 3-293 shows Working Routing Table page.



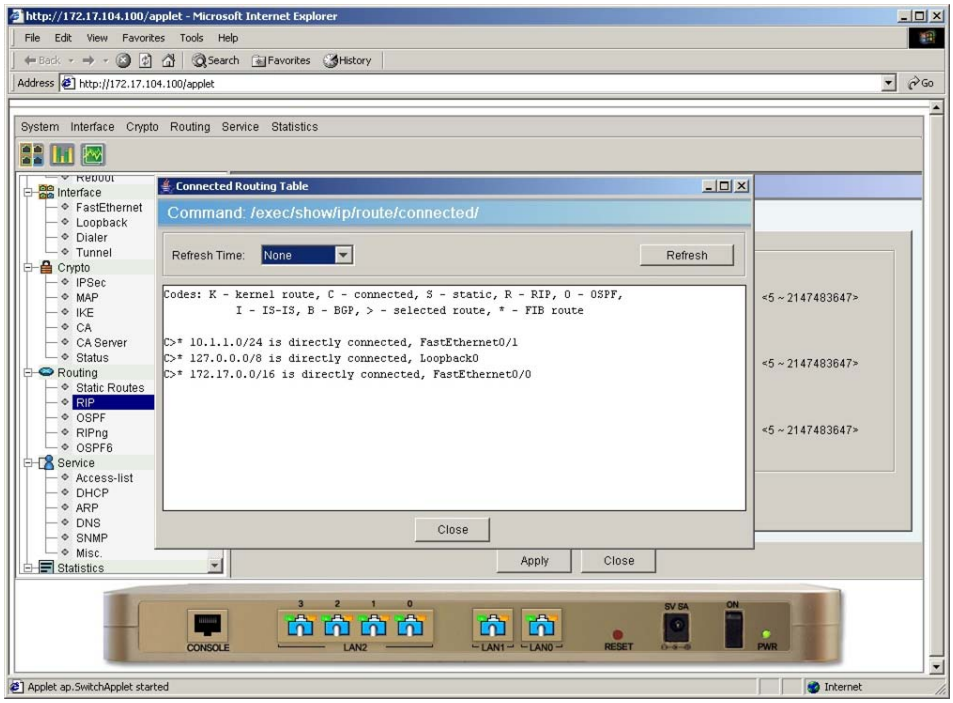
(Figure3-291) Working Routing Table page

Figure 3-294 shows Working Routing Table for IPv6 page.



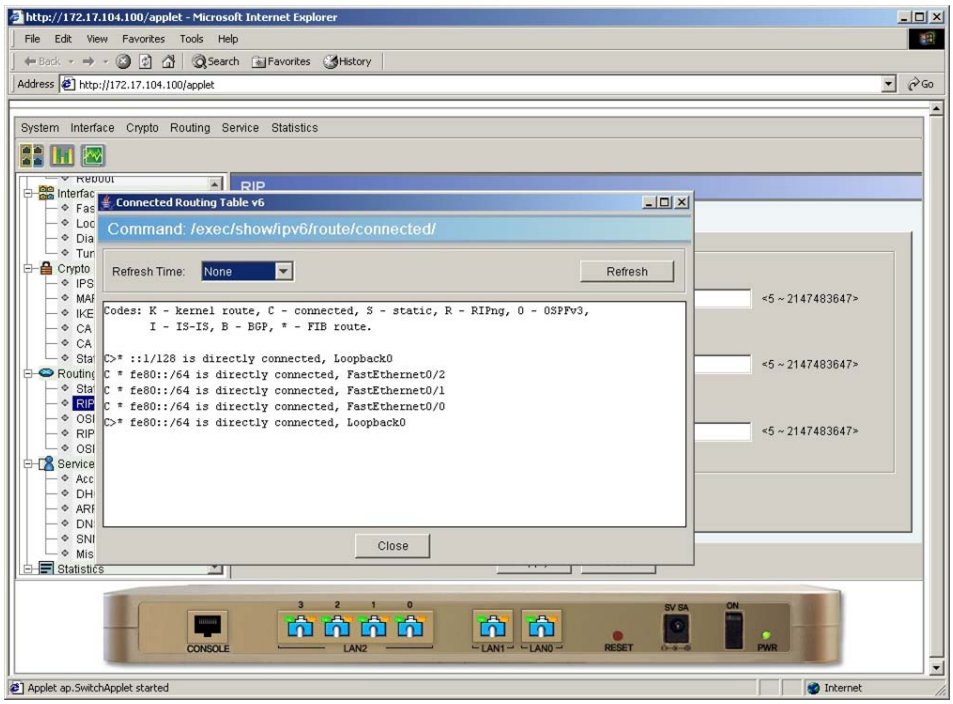
(Figure3-292) Working Routing Table for IPv6 page

Figure 3-295 shows Connected Routing Table page.



(Figure3-293) Connected Routing Table page

Figure 3-296 shows Connected Routing Table for IPv6 page.



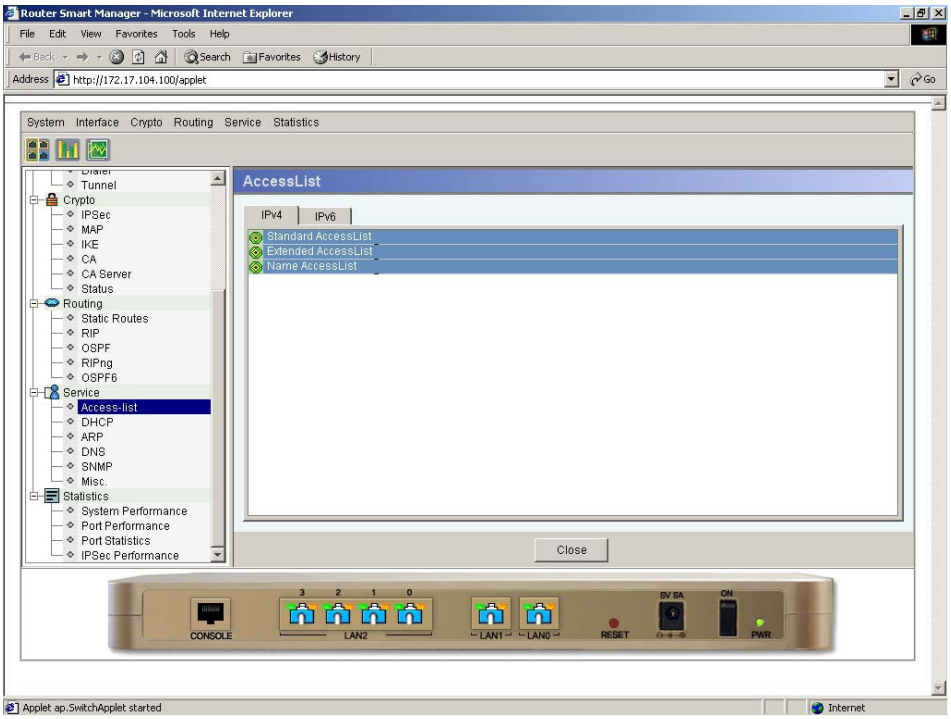
(Figure3-294) Connected Routing Table for IPv6 page

Service menu

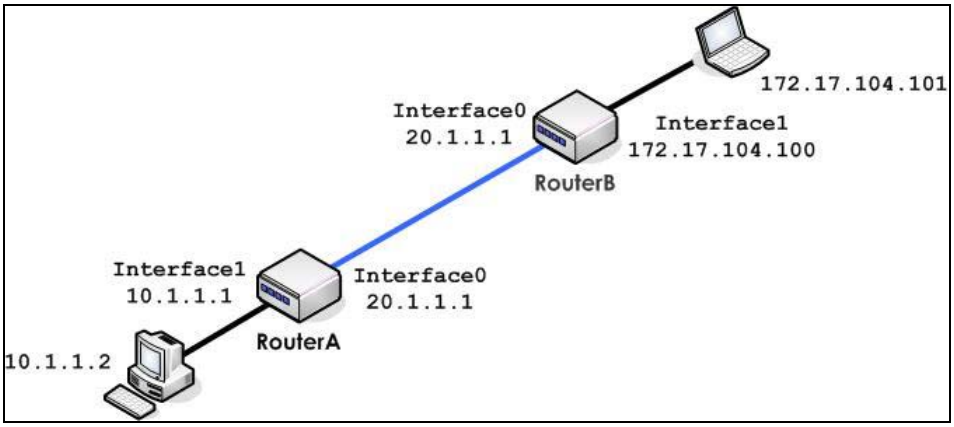
Access-List

Access-List of AP900S can create IPv6 with IPv4 Standard/Extended/Name. Also it has a Copy/Paste function which enables Access-List creation, edition, delete using Smart Manager.

(Caution!) Access-List must have at least one line of Permit sentence.



(Figure3-295) Access-List Main page



(Figure3-296) Access-List Network Diagram

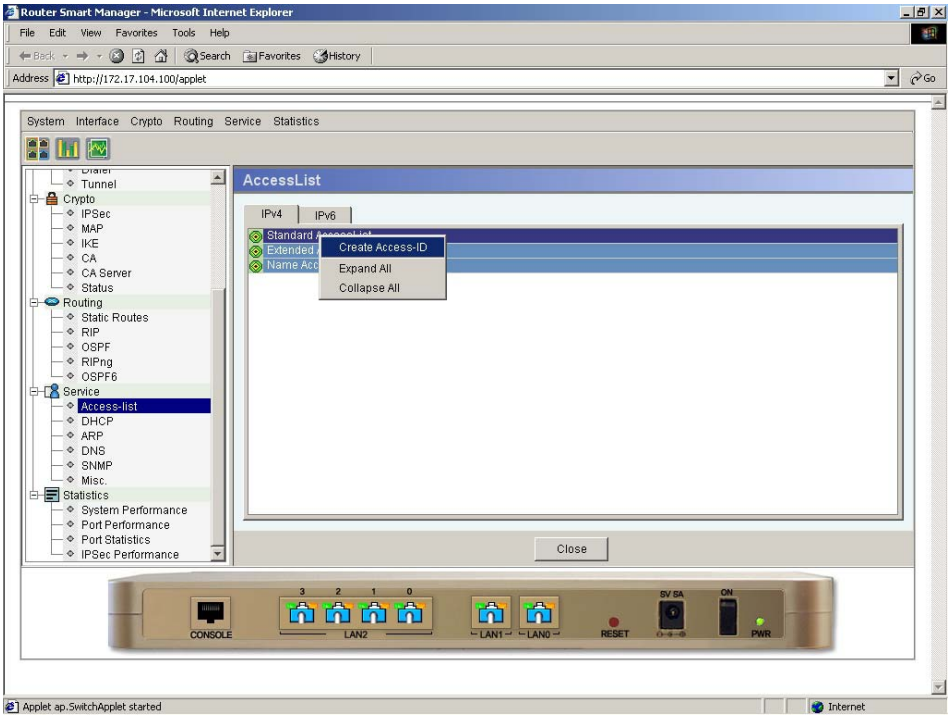
In this example of Network Diagram, host 10.1.1.2 and host 172.17.104.101 can send/receive Packet properly using Routing Protocol such as Static Routing or RIP etc. however, when Access-List which restricts ICMP packet (Source IP Address "10.1.1.2", Destination IP Address "172.17.104.101") is applied to Interface0 of RouterA then host 10.1.1.2 and host172.17.104.101 can not have ICMP communication.

Access-List is applied on interface. Access-List is not only restricts Packet transmit but also it can be applied on Crypto Map. In this Crypto Map, Data is protected by encapsulating Packets which is on Access-List.

Moreover, Access-List is used for filtering received Routing Table when exchanging Routing Table between Routers. And also Access-List is used to create IP-Policy for QoS.

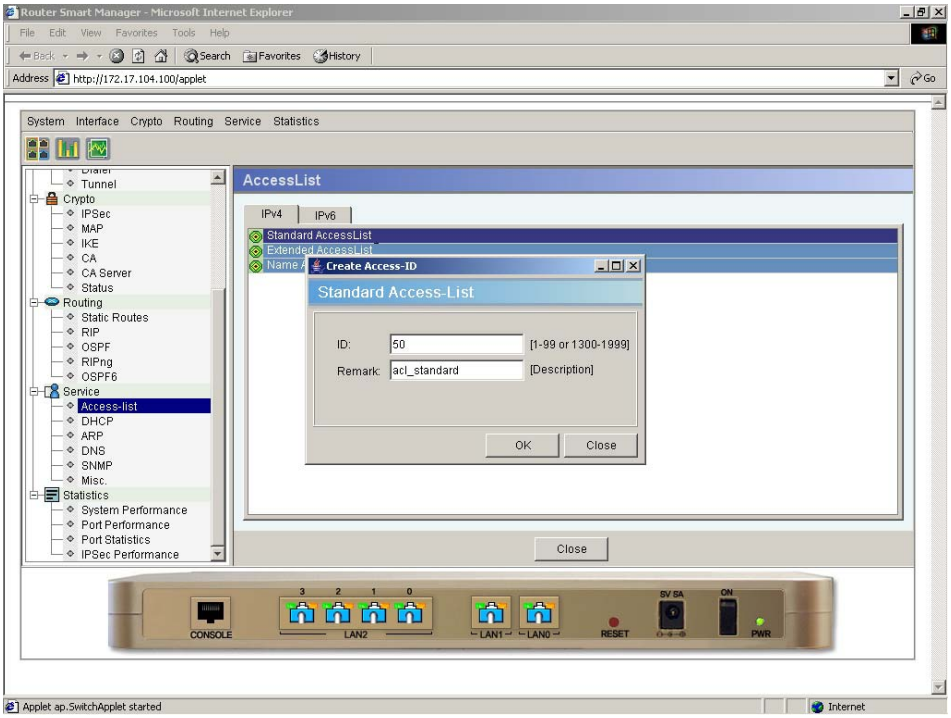
Figure 3-299 shows how to create IPv4 Standard Access-List.

Click "Create Access-ID" by clicking right side of the mouse on Standard Access-List.



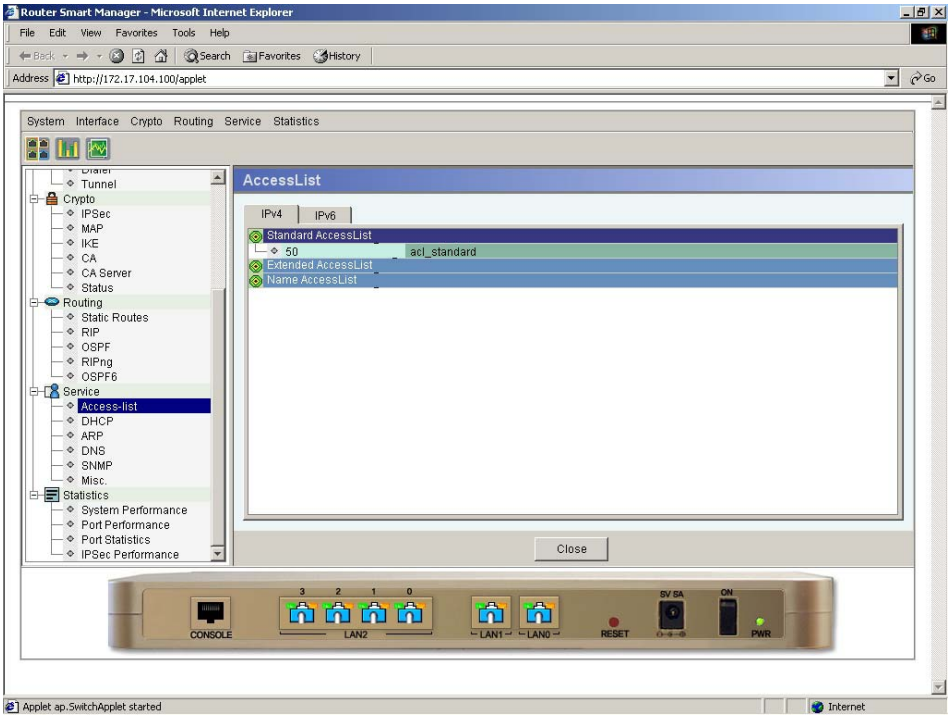
(Figure3-297) Create Standard Access-List

Input "50" for Access-ID, "acl_standard" for Remark. Spaces are allowed for Remark.



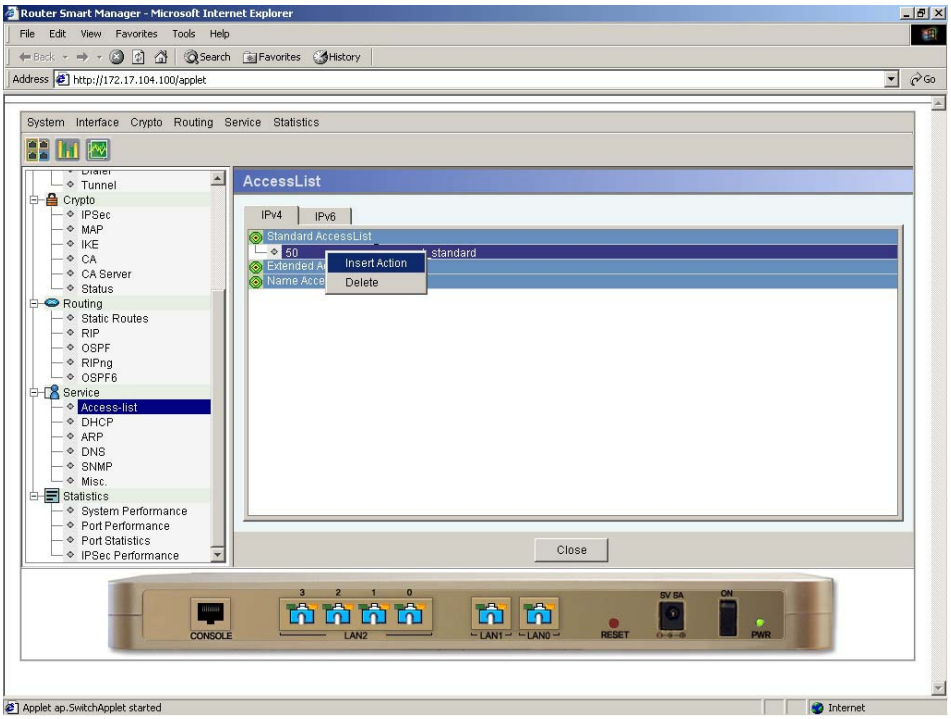
(Figure3-298) Input Access-ID, Remark

Click “OK” to verify. Figure3-301 shows the Access-ID.



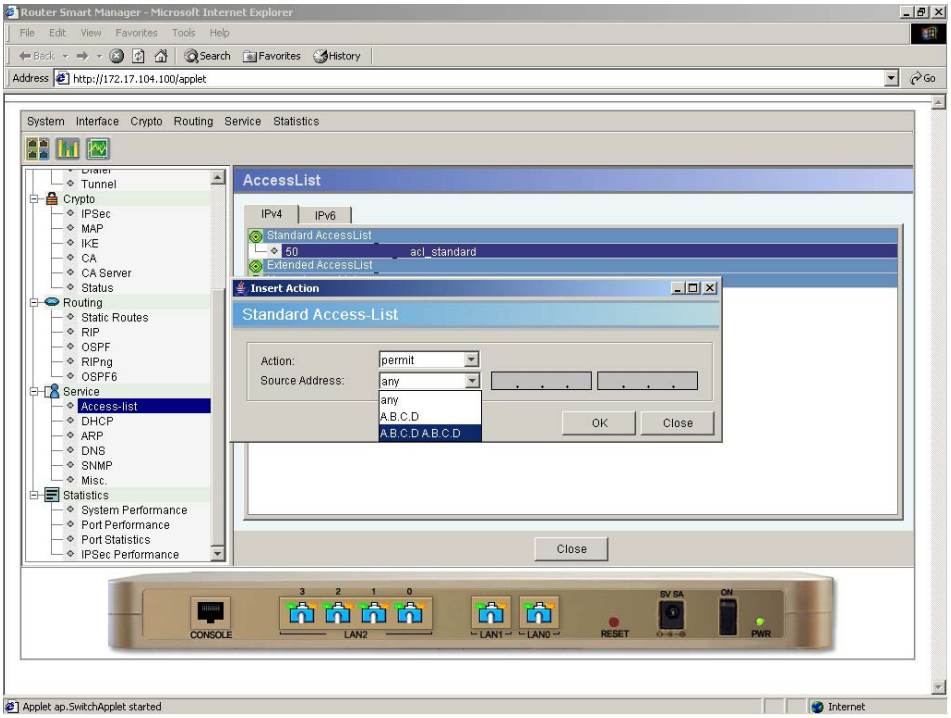
(Figure3-299) Access-ID creation verify.

Select “Insert Action” by clicking right side of mouse on created Access-ID.



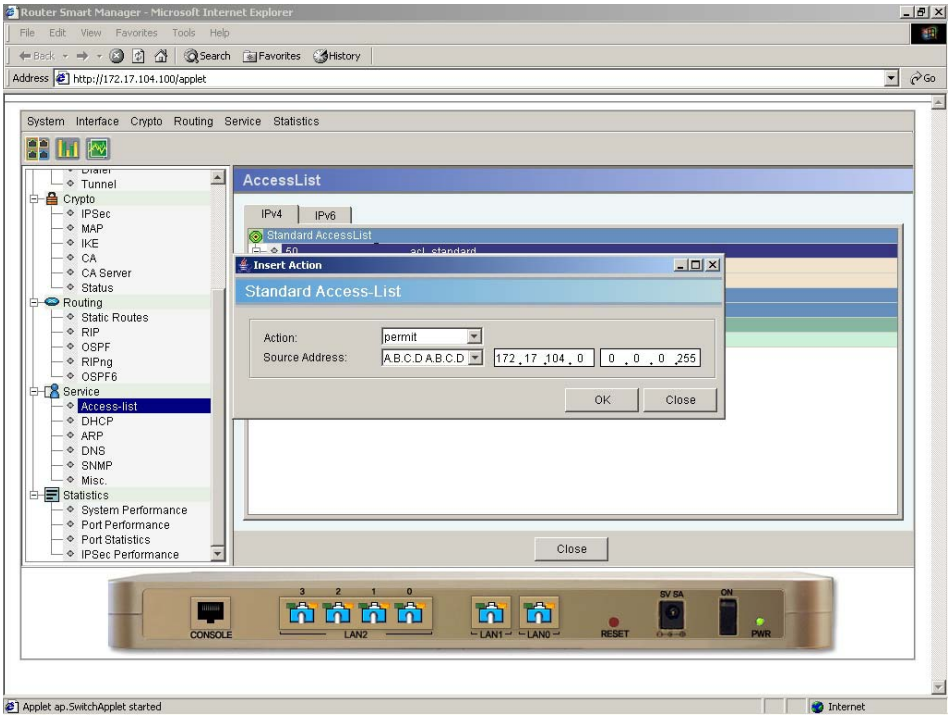
(Figure3-300) Select Insert Action

Select “Permit” for Action, “A.B.C.D, A.B.C.D” for Source Address.



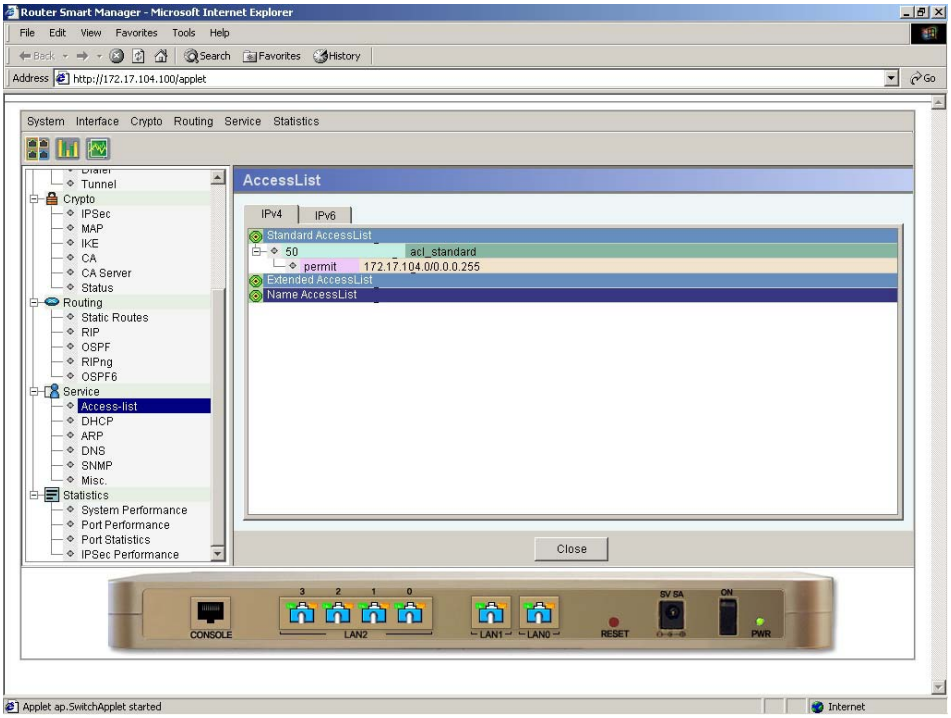
(Figure3-301) Select Action, Source Address Type

Enter “172.17.104.0” for IP Address , “0.0.0.255” for Wildcard bits.



(Figure3-302) Input Source Address Range

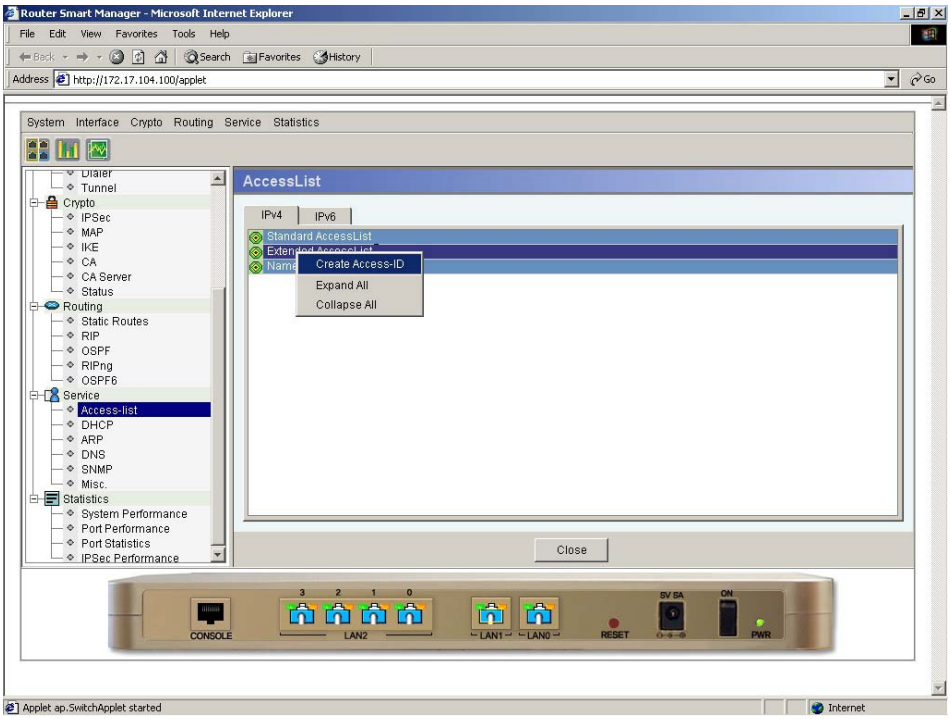
Click "OK" to verify. Permit sentence is created.



(Figure3-303) Access-List creation verify

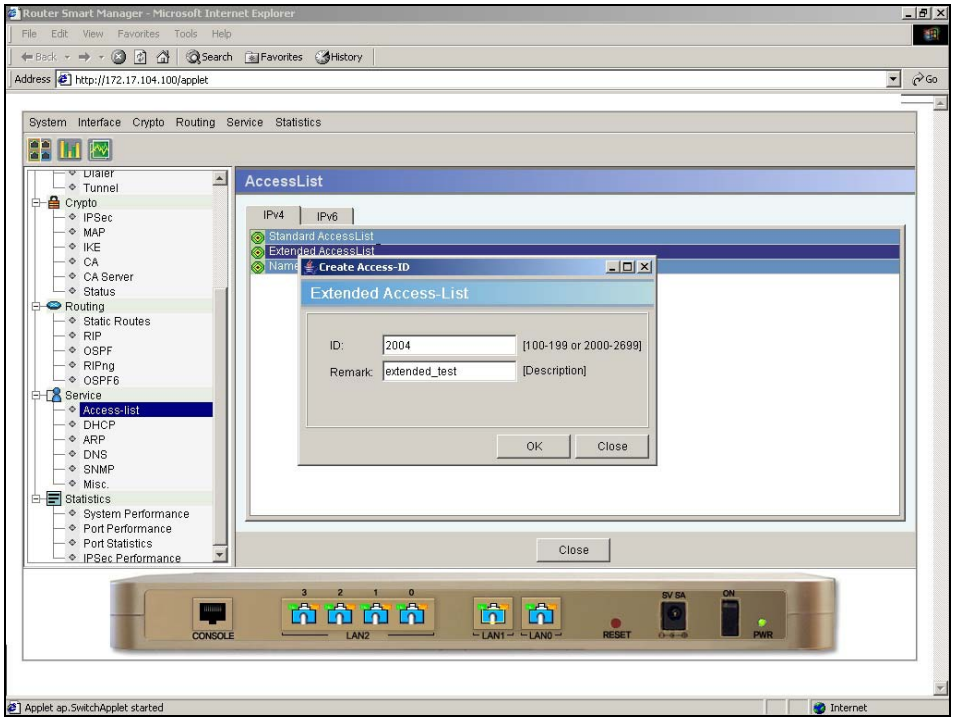
Figure 3-306 shows how to create Extended Access-List.

Select Create Access-ID by clicking right side of the mouse on Extended Access-List.



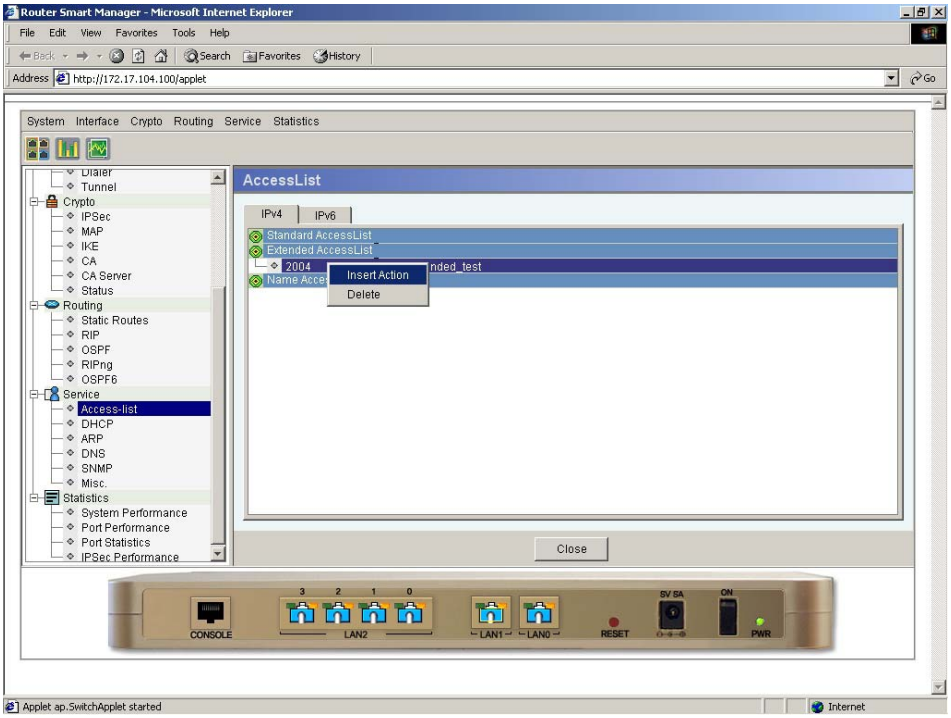
(Figure3-304) Select Extended Access-List Create Access-ID

Enter Access-ID (“2004”), Remark (“extended_test”).



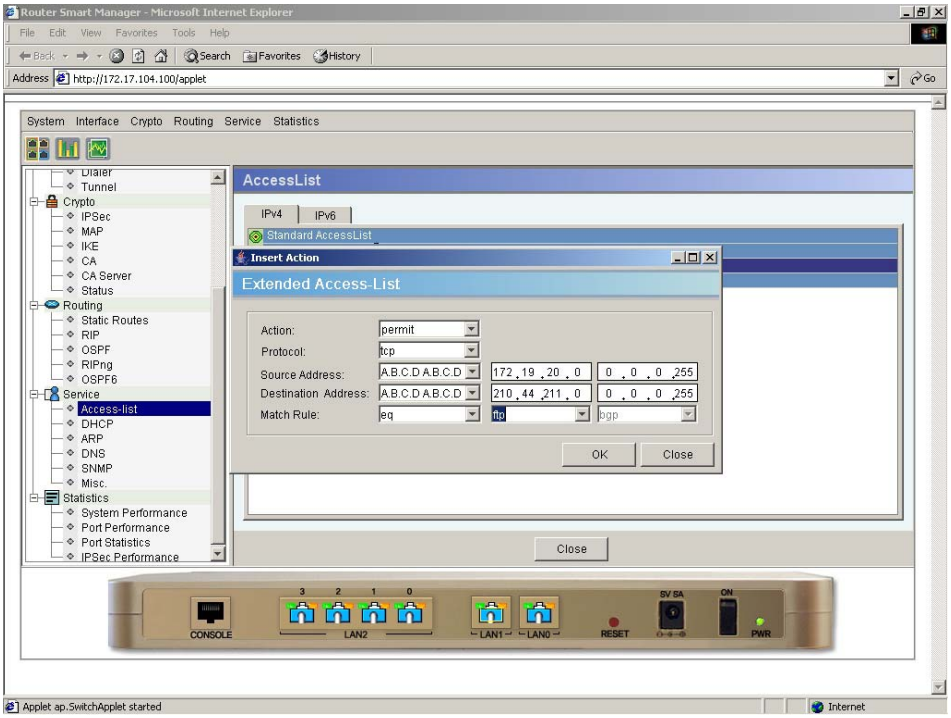
(Figure3-305) Input Extended Access-List Access-ID, Remark

Select Insert Action by clicking right side of the mouse on Access-ID.



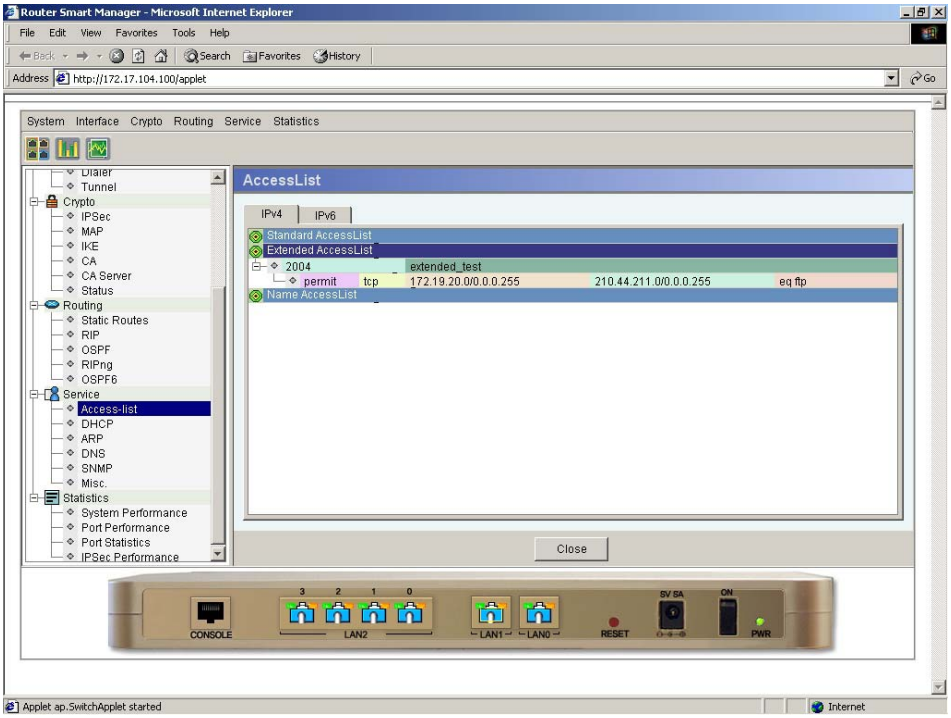
(Figure3-306) Select Extended Access-List Insert Action

Enter the range of Source IP Address, Destination IP Address, input or select Protocol and Permit etc.



(Figure3-307) Extended Access-List

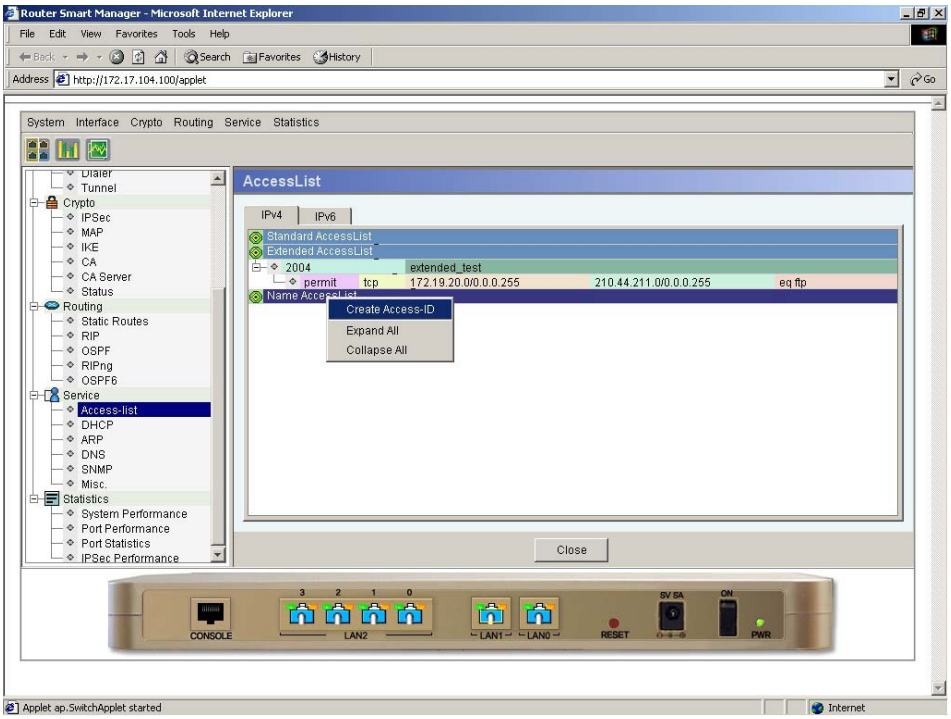
Click “OK” to verify.



(Figure3-308) Extended Access-List creation verify

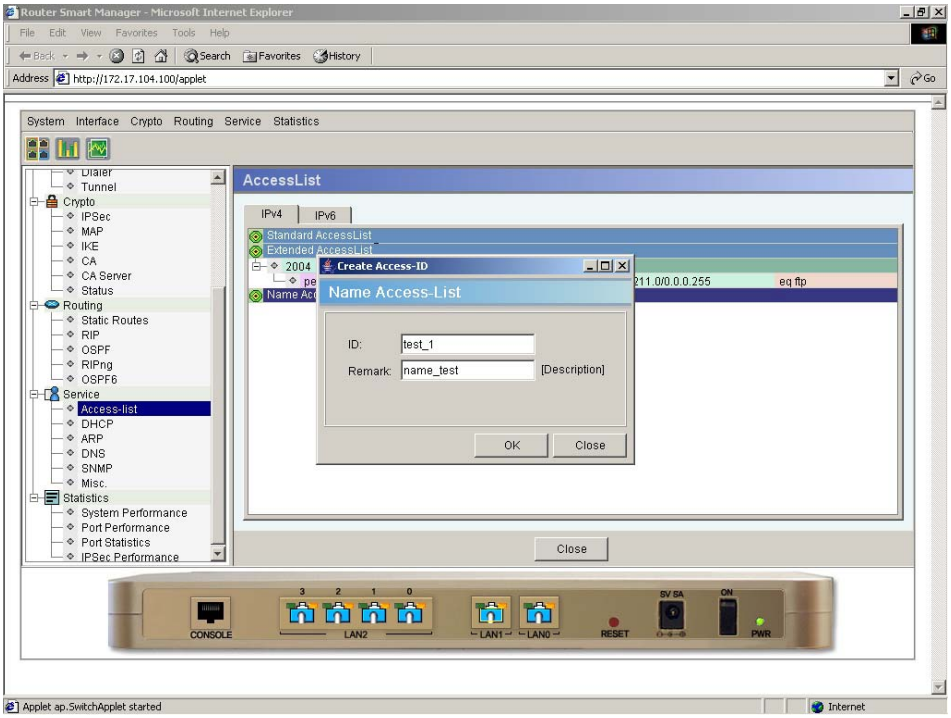
Figure 3-311 shows how to configure Name Access-List.

Select Create Access-ID by clicking right side of the mouse on Name Access-List.



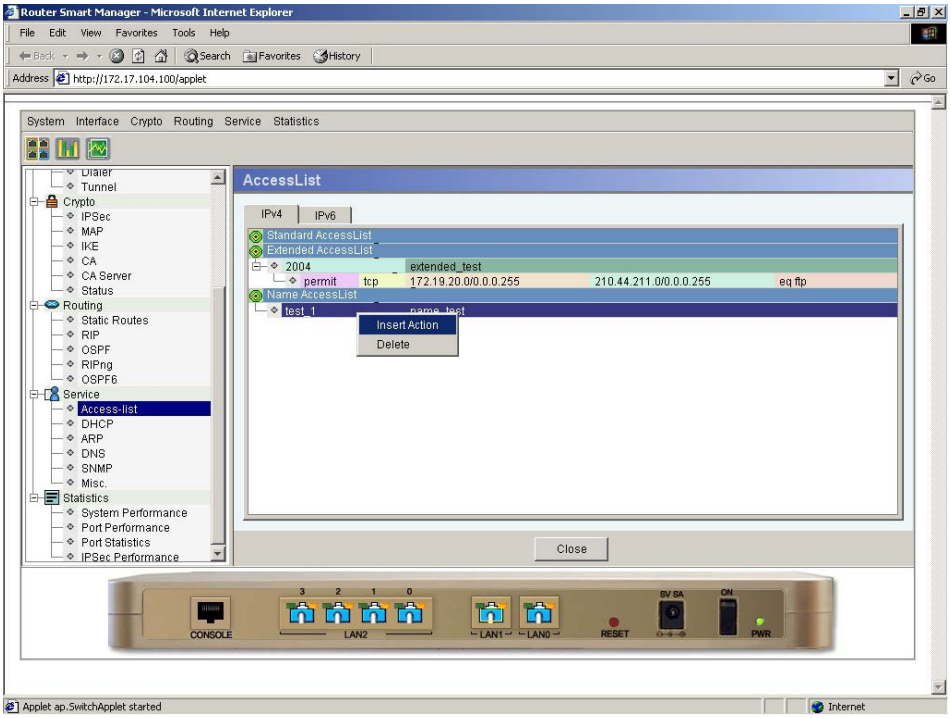
(Figure3-309) Select Name Access-List Create Access-ID

Enter “test_1” for Access-ID, “name_test” for Remark.



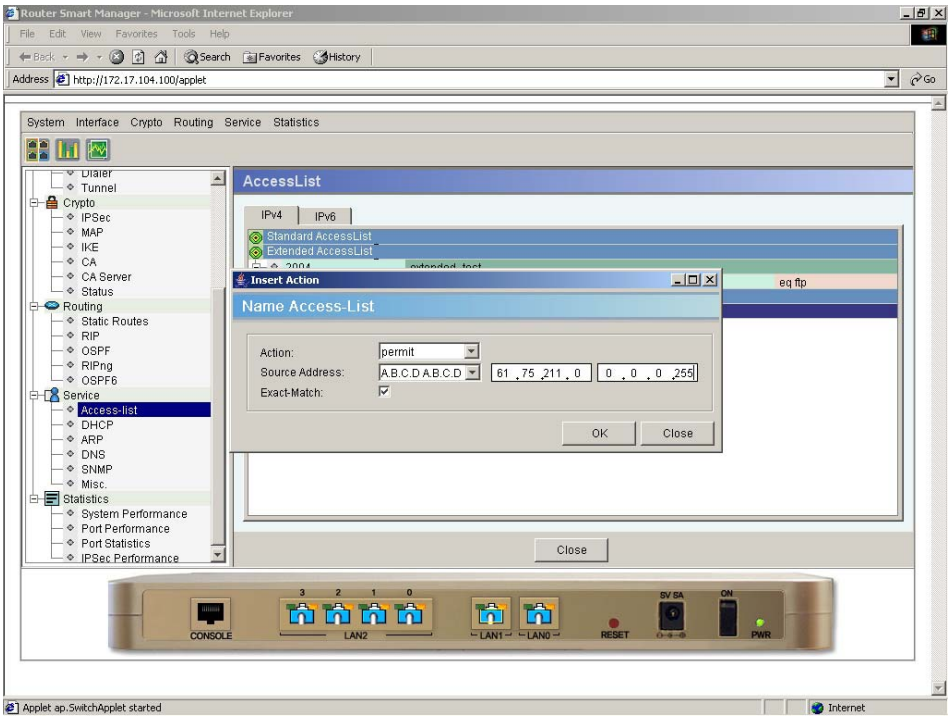
(Figure3-310) Input Name Access-List Access-ID, Remark

Select Insert Action by clicking right side of mouse on the new Access-ID.

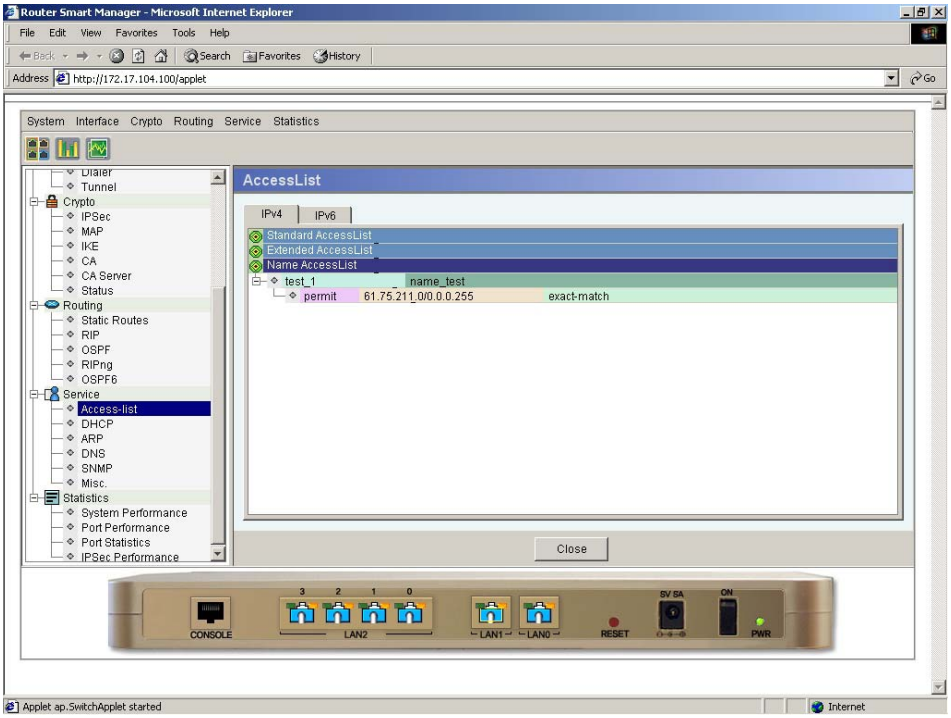


(Figure3-311) Select Name Access-List Insert Action

Input or Select the ranges of Source IP Address and Permit.



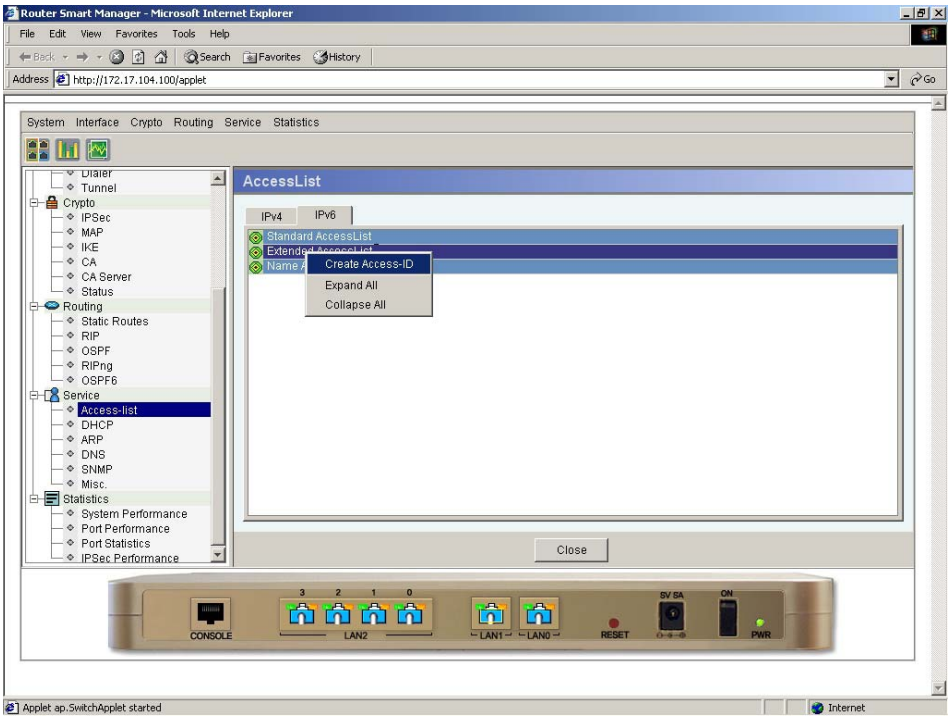
Verify the new Name Access-List.



(Figure3-312) Name Access-List Verify

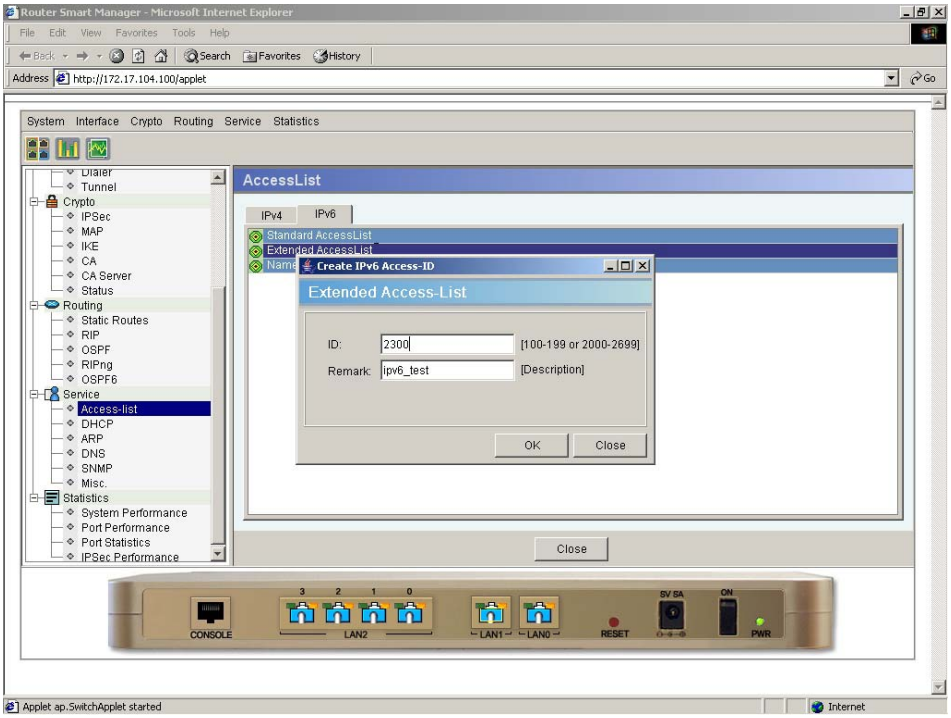
Figure 3-316 shows how to write IPv6 Extended Access-List.

Select Create Access-ID by clicking right side of the mouse on Extended Access-List.



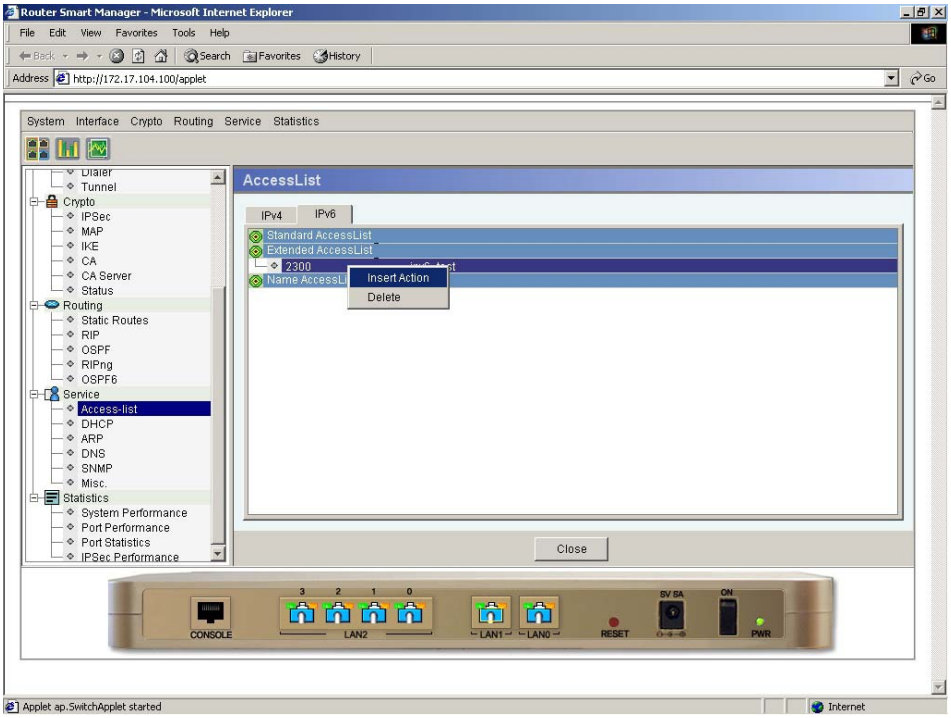
(Figure3-313) Select IPv6 Extended Access-List Create Access-ID

Input “2300” for Access-ID, “ipv6_test” for Remark.



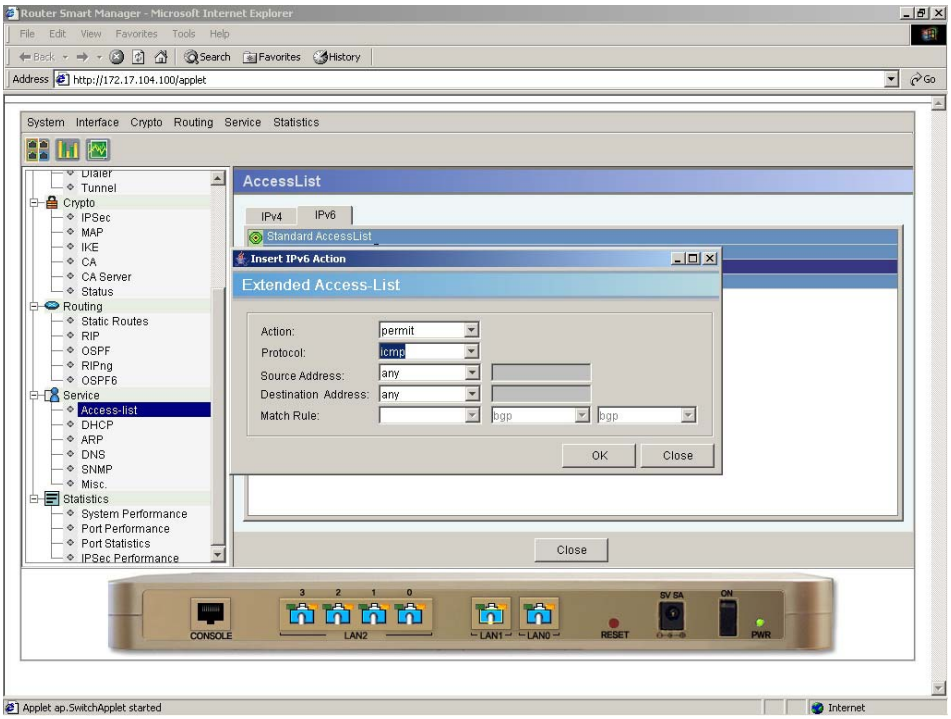
(Figure3-314) Input IPv6 Extended Access-List Access-ID, Remark

Select Insert Action by clicking right side of the mouse on created ID.



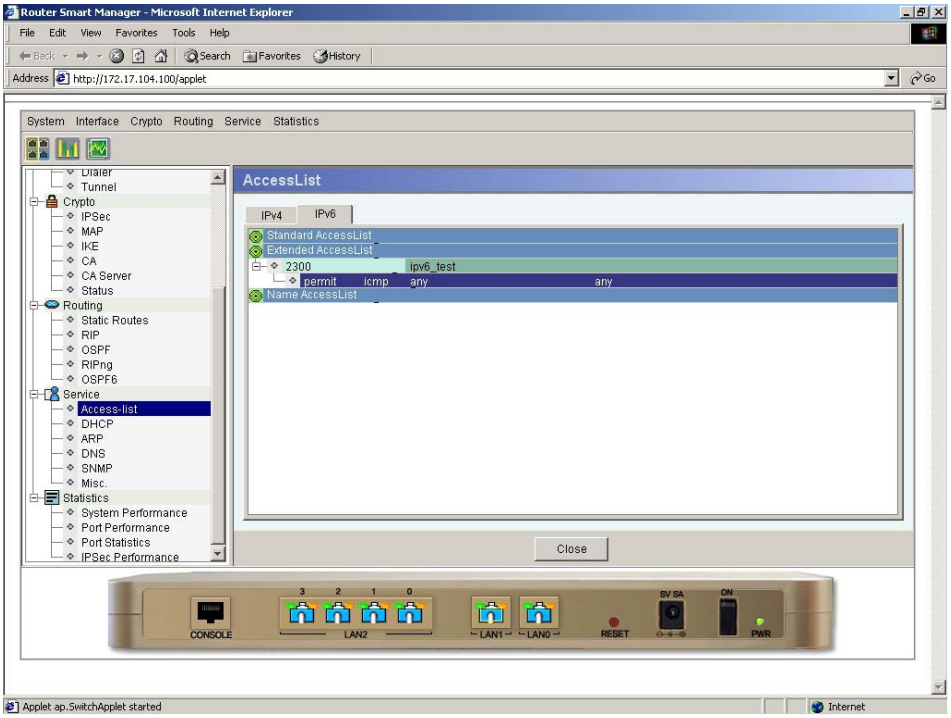
(Figure3-315) IPv6 Select Extended Access-List Insert Action

Select Source IP Address, Destination IP Address, Protocol etc.



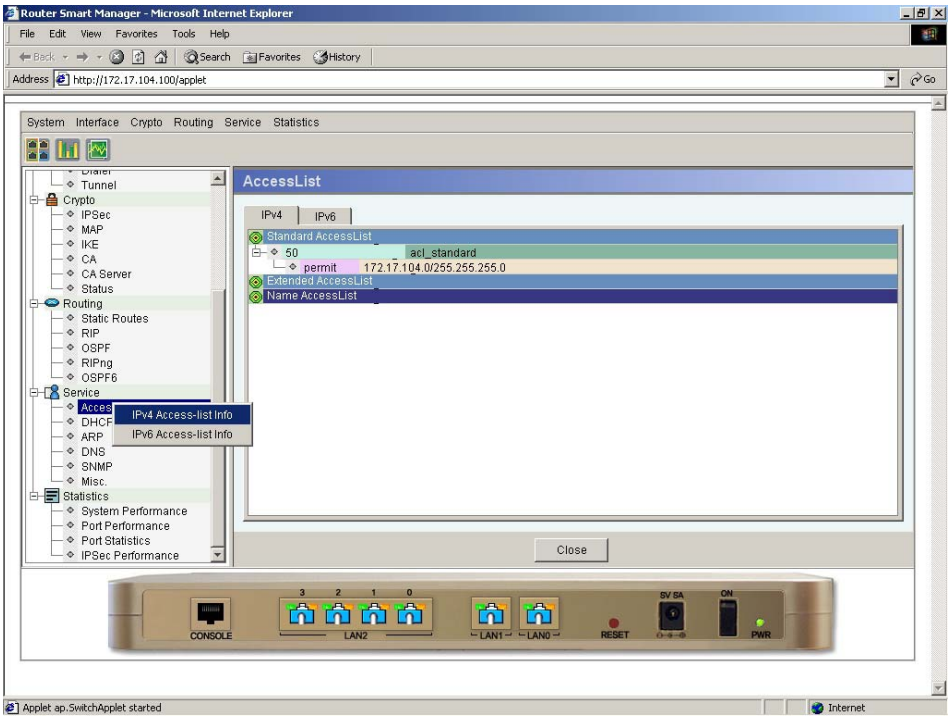
(Figure3-316) Writing IPv6 Extended Access-List

Click “OK” to verify.



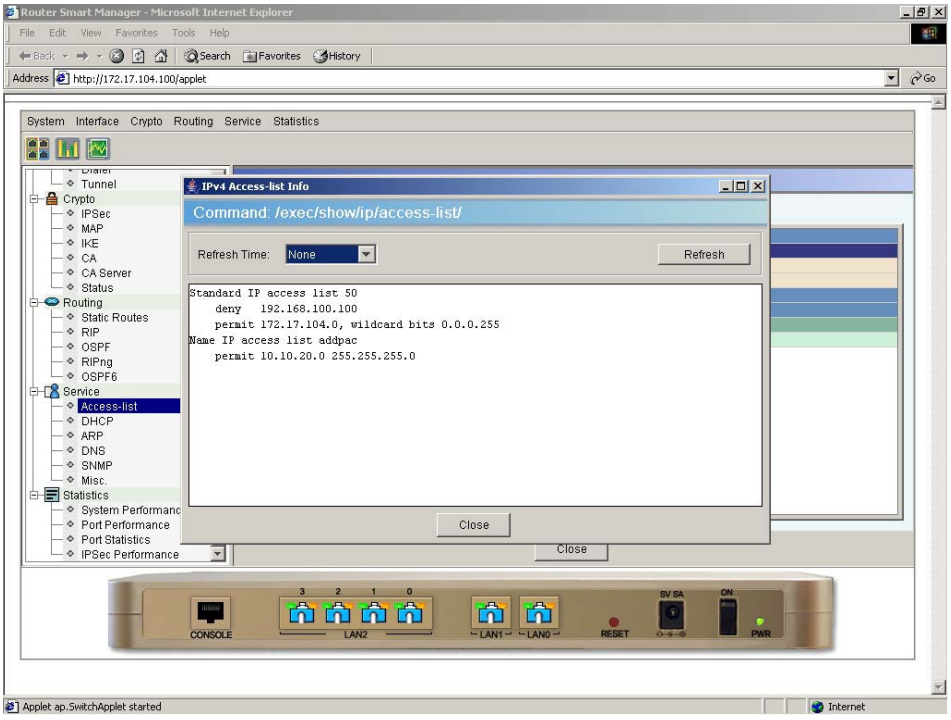
(Figure3-317) IPv6 Extended Access-List creation

Click on right side of the mouse on Access-List to check Access-List. See the Figure 3-321.



(Figure3-318) Access-List Pop Menu

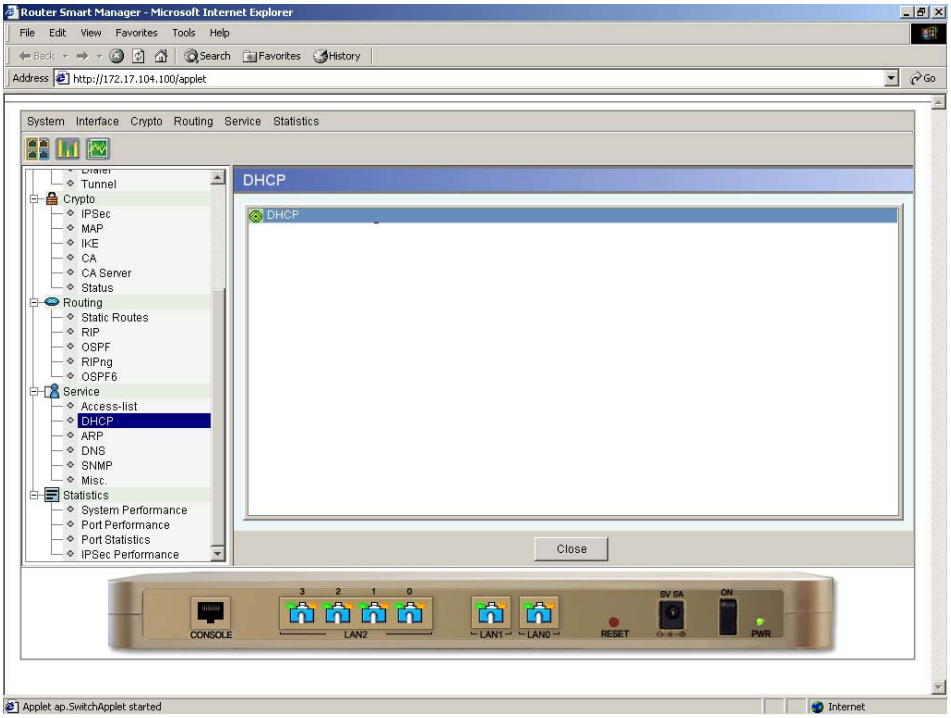
Figure 3-322 shows IPv4 Access-List page.



(Figure3-319) IPv4 Access-List page

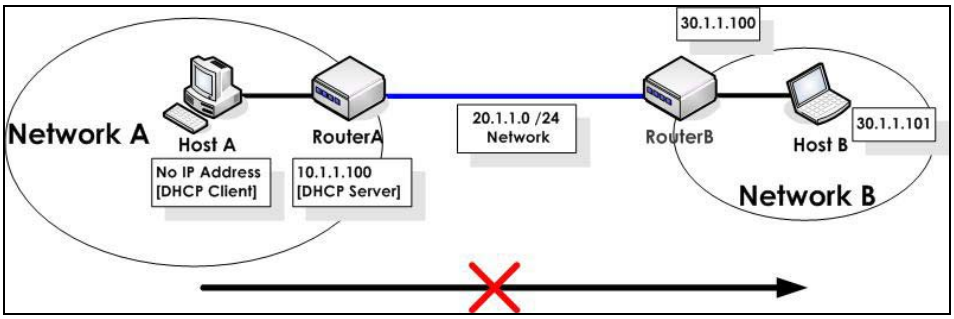
DHCP

DHCP Pool which is created from DHCP (Dynamic Host Configuration Protocol) menu must be applied on appropriate Interface to work properly. More than one of DHCP Pool can be written.



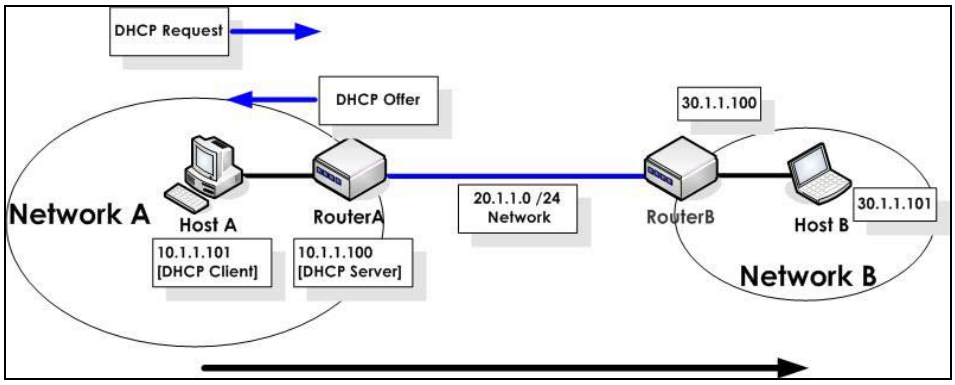
(Figure3-320) DHCP Main page

Figure 3-324 shows the example network diagram of DHCP.



(Figure3-321) DHCP Diagram 1

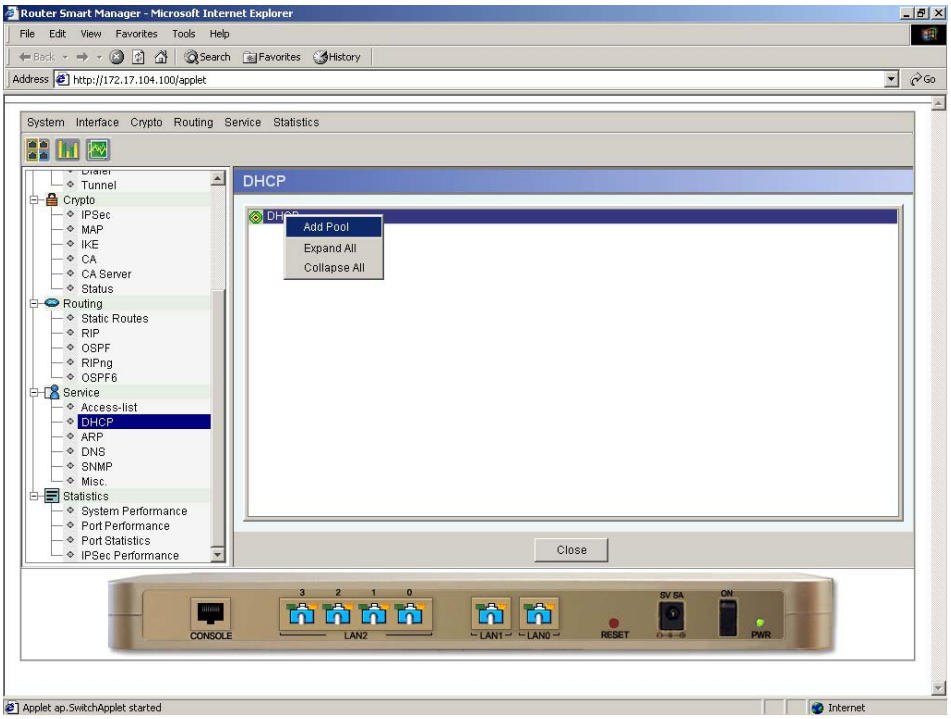
Currently Host A is not able to communicate with Host B because it does not have IP Address. However, DHCP Server is enabled on Router A so if Host A sends DHCP Request to Router A then Host A can assign IP Address from Router A. See the Figure 3-325.



(Figure3-322) DHCP Diagram 2

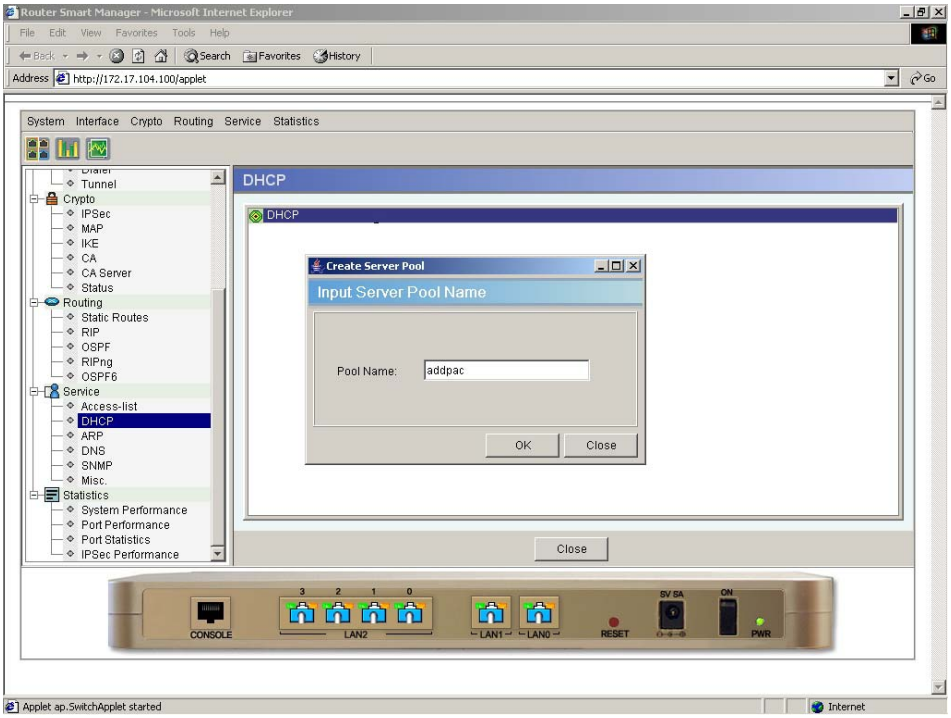
Figure 3-326 shows how to create DHCP Pool.

Select Add Pool by clicking right side of the mouse on DHCP.



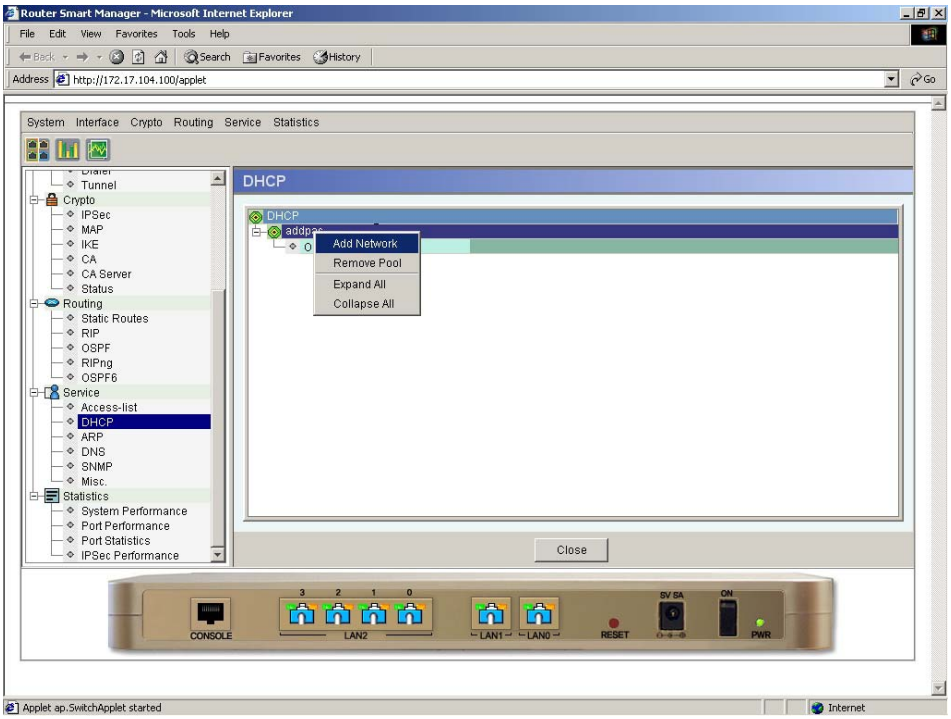
(Figure3-323) Select DHCP Add Pool

Input "addpac" for Pool Name.



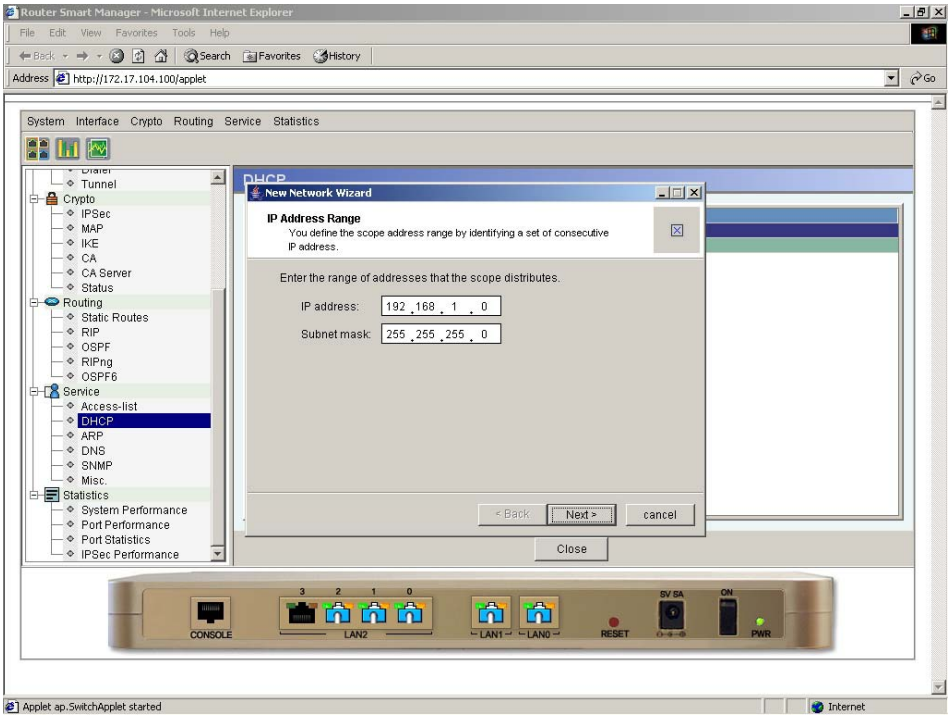
(Figure3-324) Input DHCP Pool Name

Select Add Network by clicking right side of the mouse on created DHCP Pool "addpac".



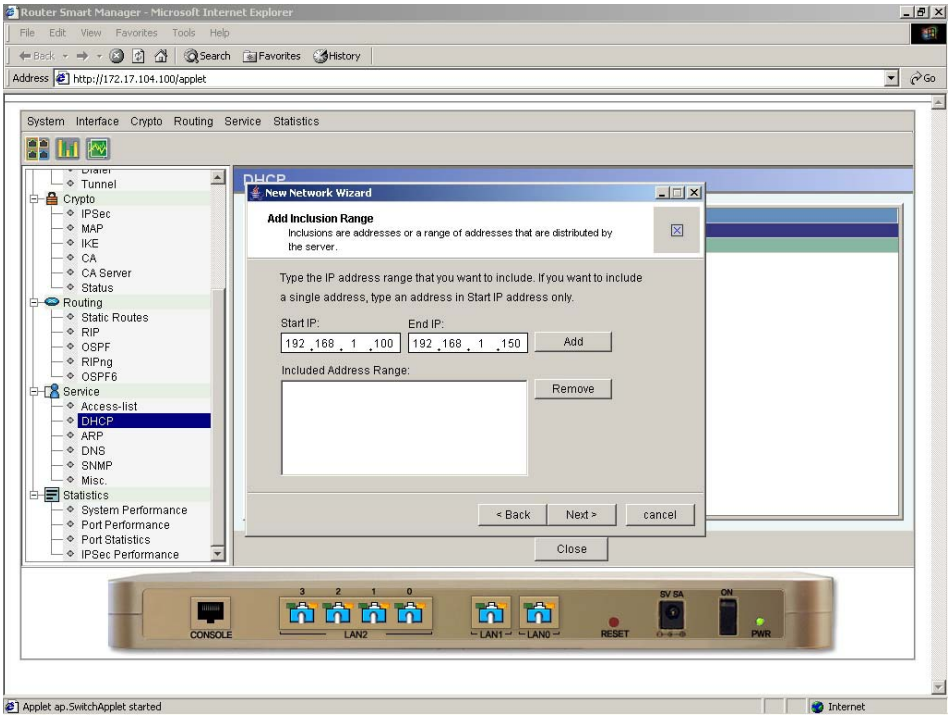
(Figure3-325) Select DHCP Add Network

New Network Wizard is executed Input IP Address Range.



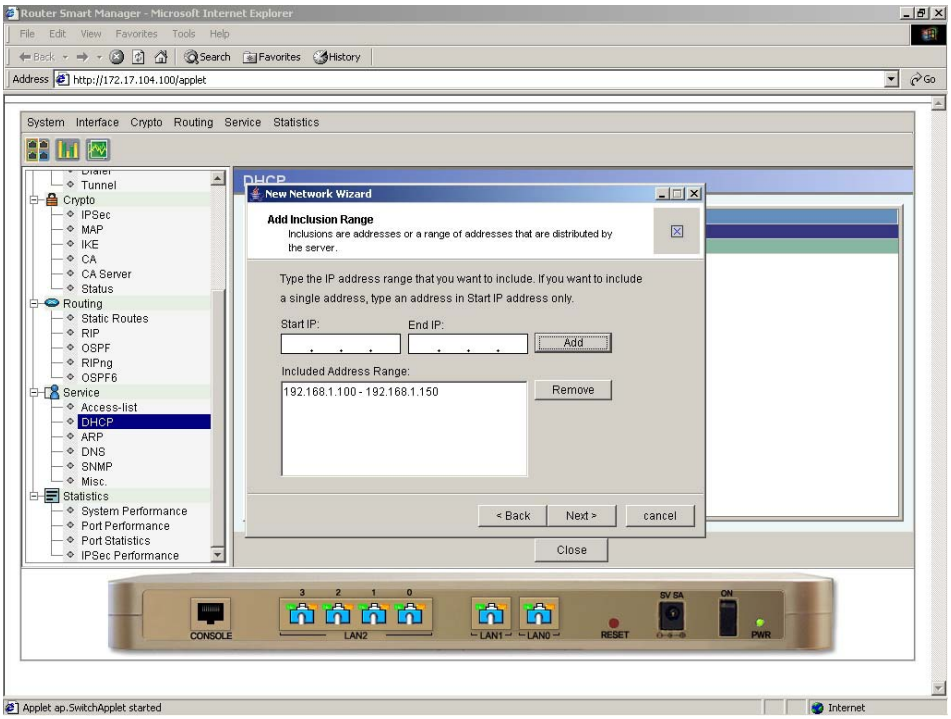
(Figure3-326) Input DHCP IP Address Range

Input the ranges of IP Address which will be providing to DHCP Client.



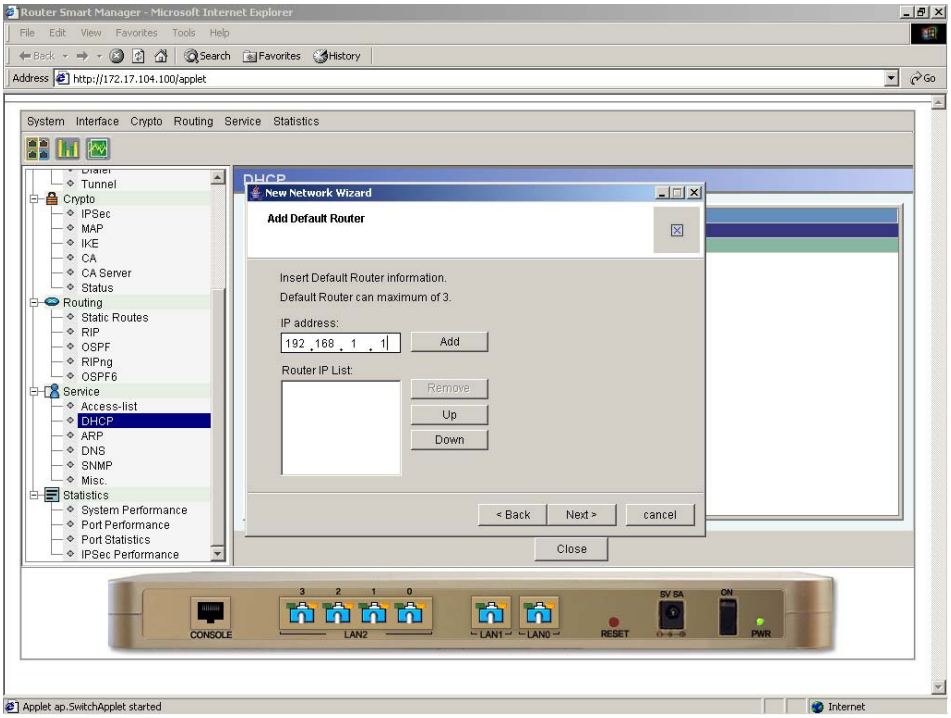
(Figure3-327) Input IP Address Range for DHCP Client

Click "Add" to move to Address Range box.



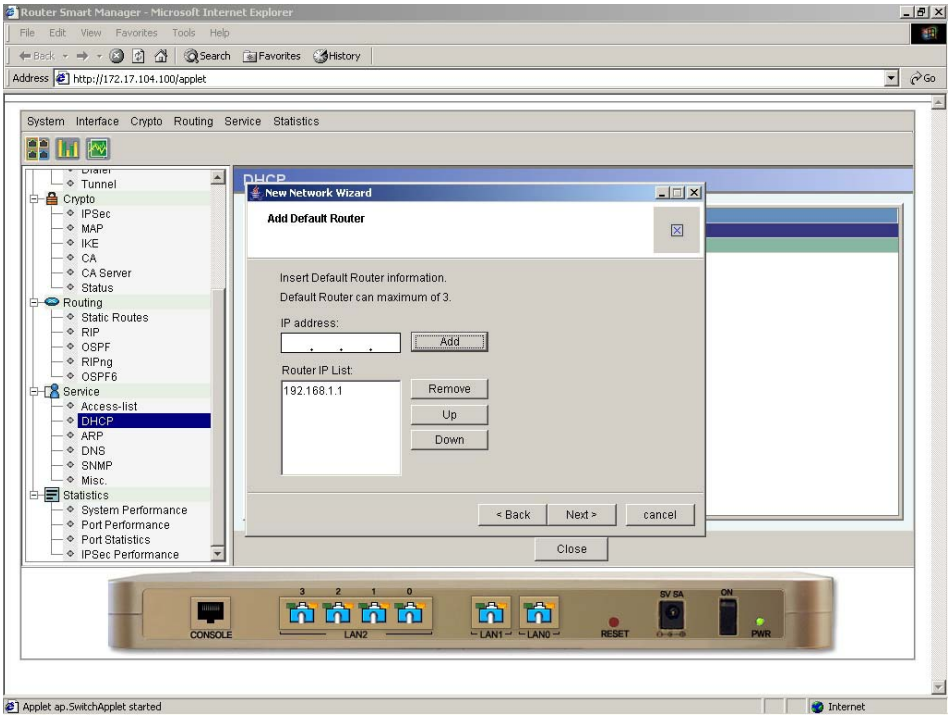
(Figure3-328) Move to DHCP Address Range box.

Input Default Router IP Address. Input Maximum 3 addresses.



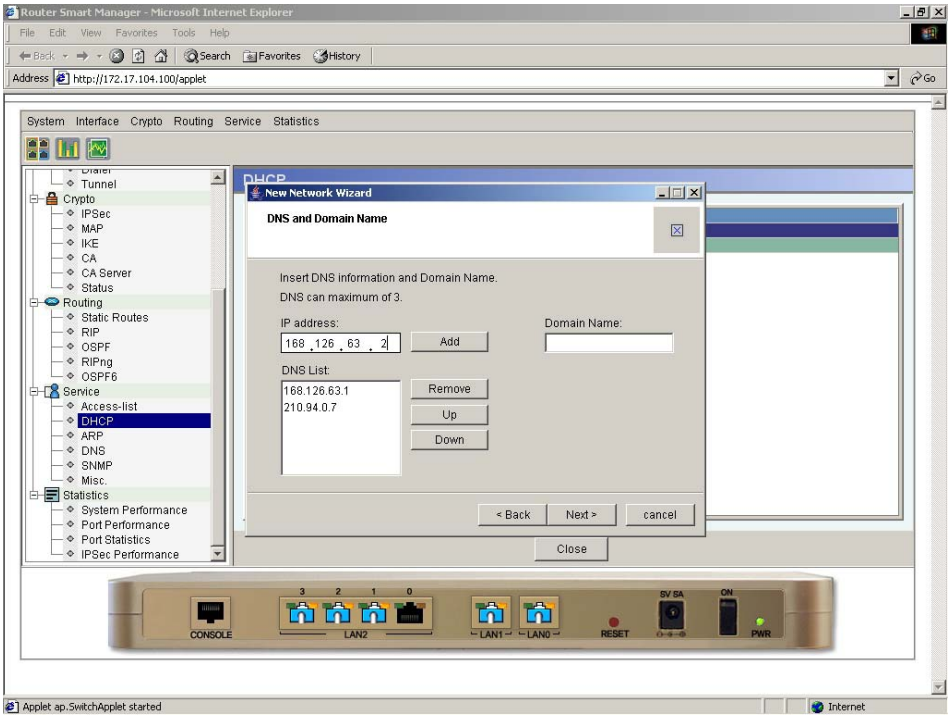
(Figure3-329) Input DHCP Default Router IP Address

Click "Add" to move to Router IP List page.



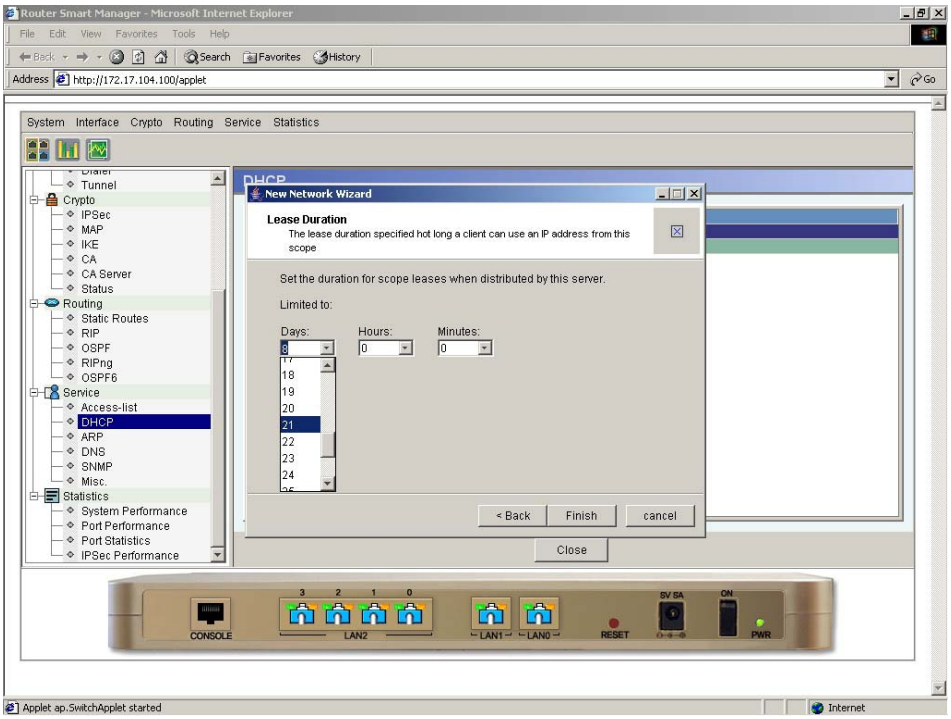
(Figure3-330) DHCP Router IP List page

Input DNS IP Address. Input Maximum 3 addresses.



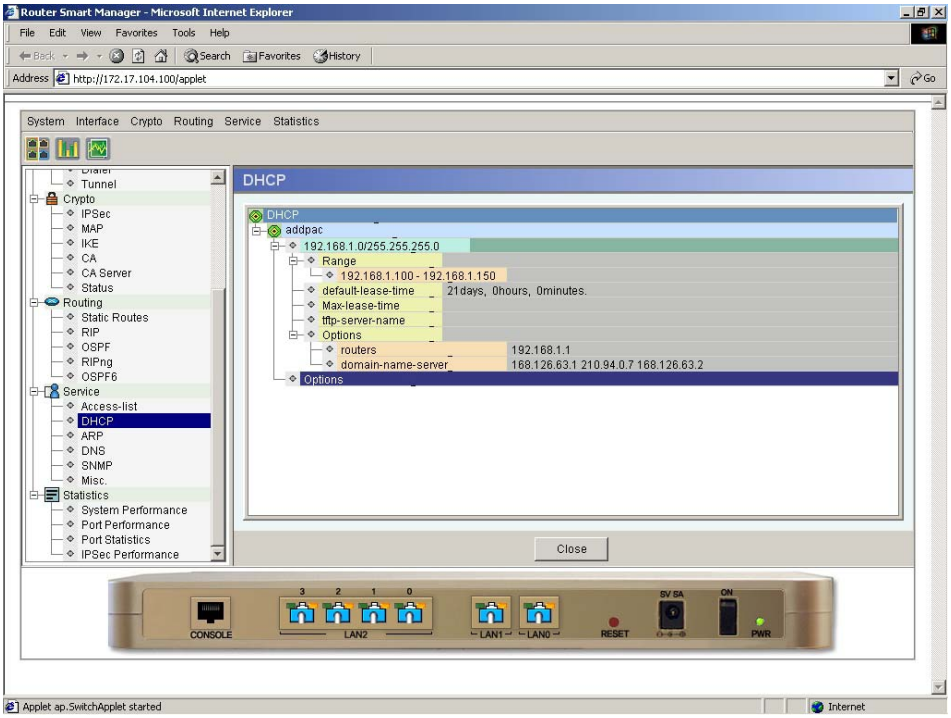
(Figure3-331) Input DHCP DNS IP Address

Select Lease Duration of assigned IP Address.



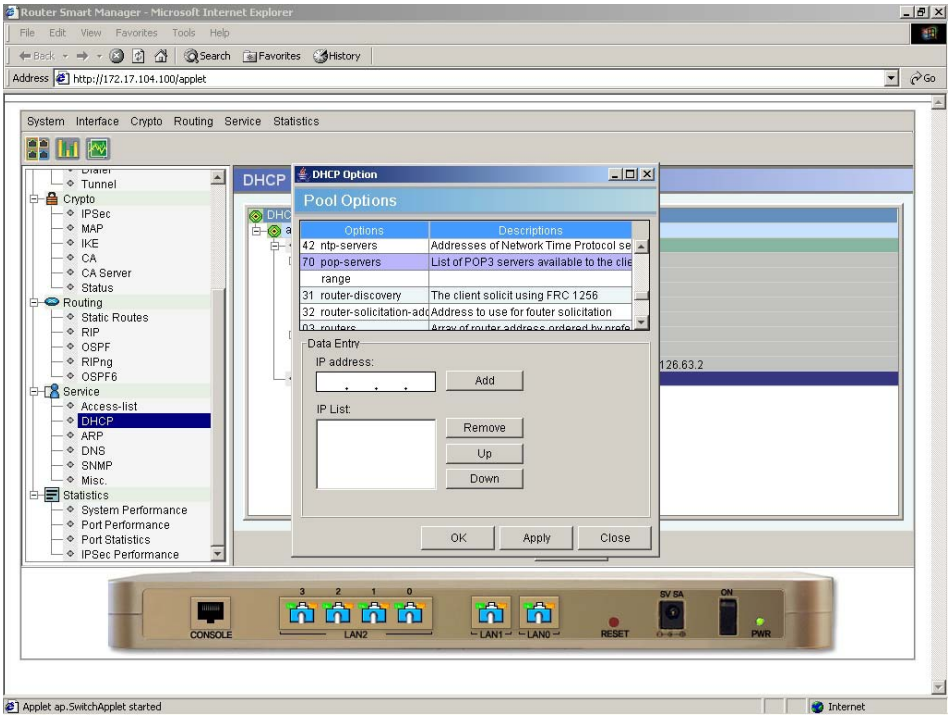
(Figure3-332) Select DHCP Lease Duration

Click "OK" to verify.



(Figure3-333) addpac DHCP Pool configuration

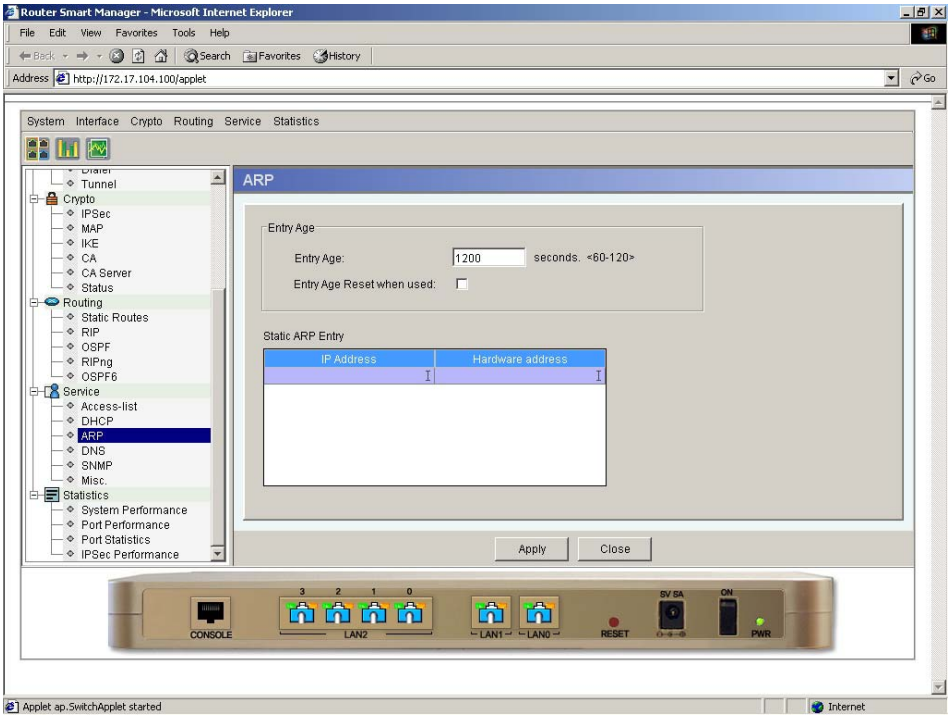
Select "Configuration" to input the value by clicking right side of the mouse on Option to use options such as POP-Server, NTP-Server.



(Figure3-334) DHCP Pool Option page

ARP

ARP (Address Resolution Protocol) is used for matching IP Address on IP Network with Physical Network Address. Physical Network Address indicates Ethernet 48bits MAC Address.



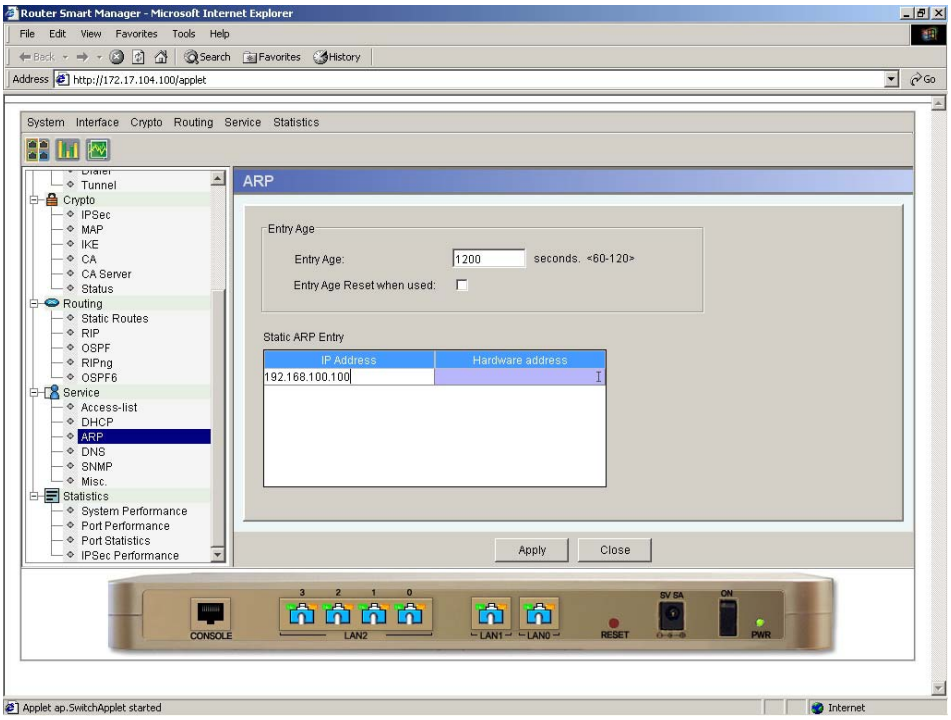
(Figure3-335) ARP Main page

<Table 3-46> ARP Menu Description

Elements	Description
Entry Age	Input the lifetime for MAC Address info on ARP Table. Default value is “1200” seconds.
Entry Age Reset when used	ARP Reset is executed even if the session is on.
Static ARP Entry	It is used when the user wants to register static IP Address and MAC Address of the Host on ARP Table.

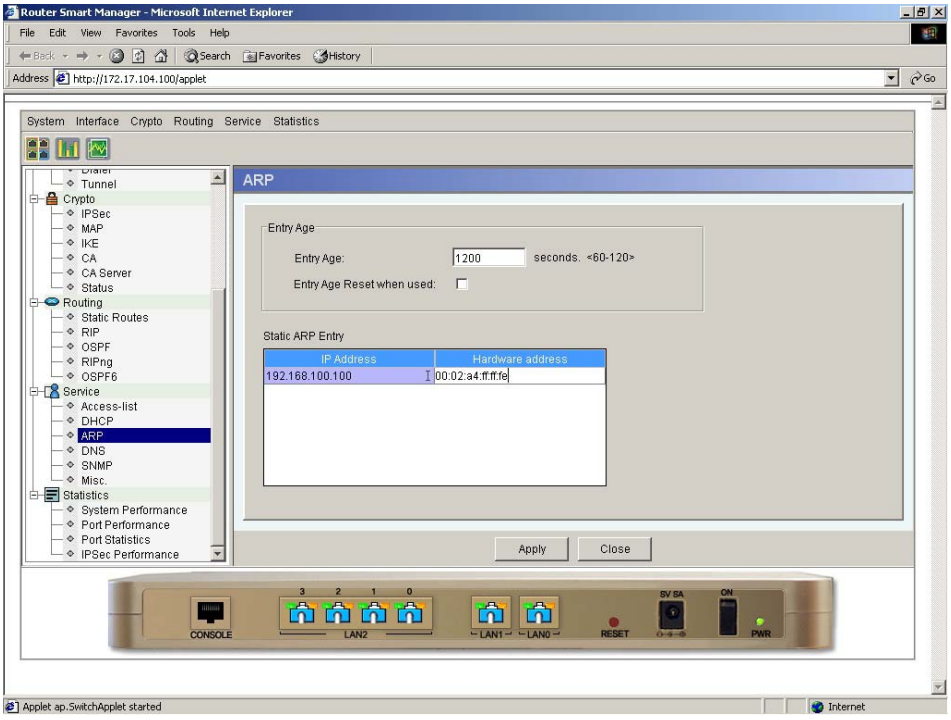
Figure 3-339 shows the example of using Static ARP Entry.

Input “192.168.100.100” for IP address.



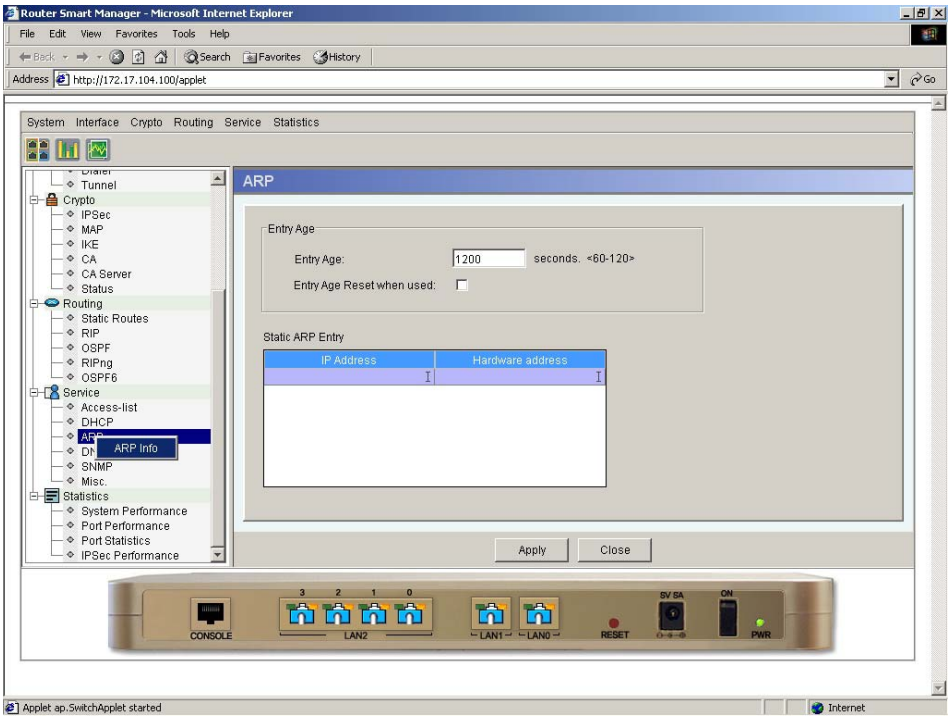
(Figure3-336) Input Static ARP Entry IP Address

Input “00:02:a4:ff:ff:fe” for MAC Address.



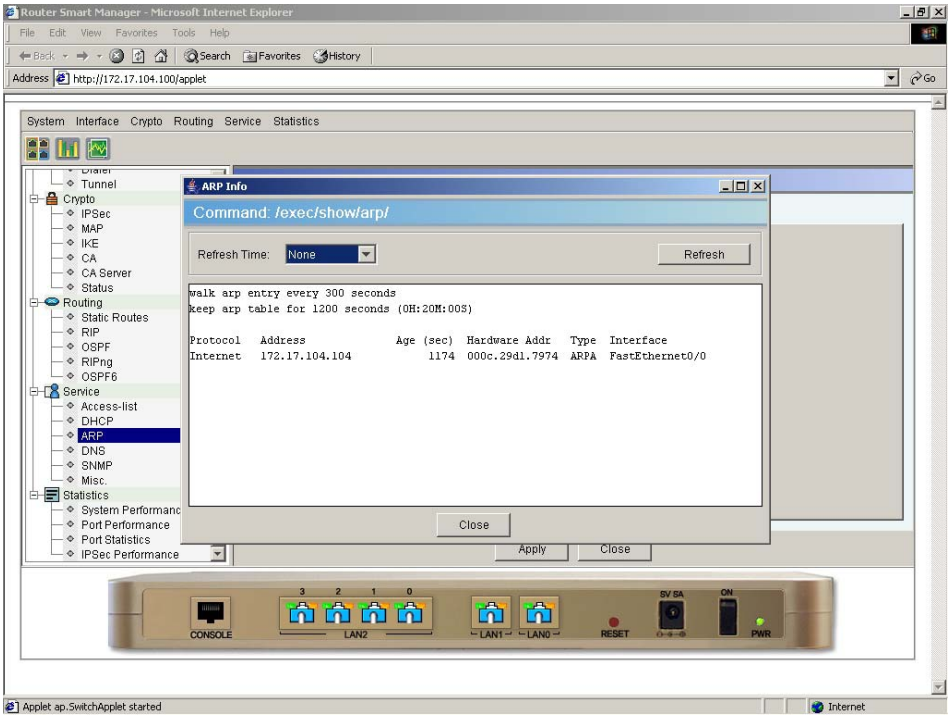
(Figure3-337) Input Static ARP Entry MAC Address

Select "ARP Info" by clicking right side of the mouse on ARP to see the contents of ARP Table.



(Figure3-338) Select ARP Pop Menu ARP Info

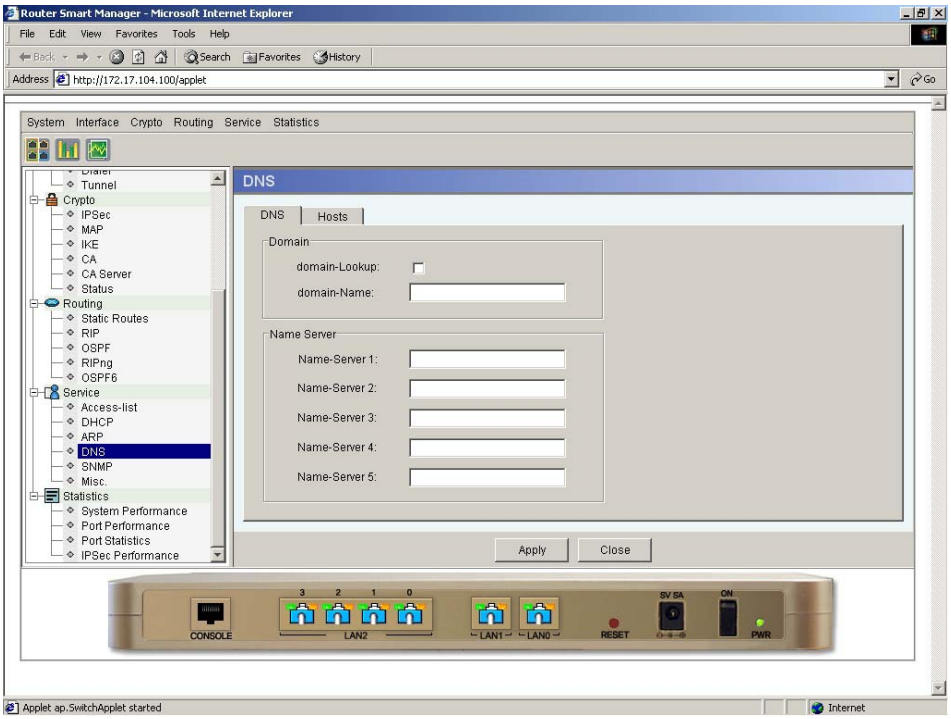
ARP Table content will be shown.



(Figure3-339) ARP Info page

DNS

DNS (Domain Name System) is used to look up the IP Address for internet domain name.

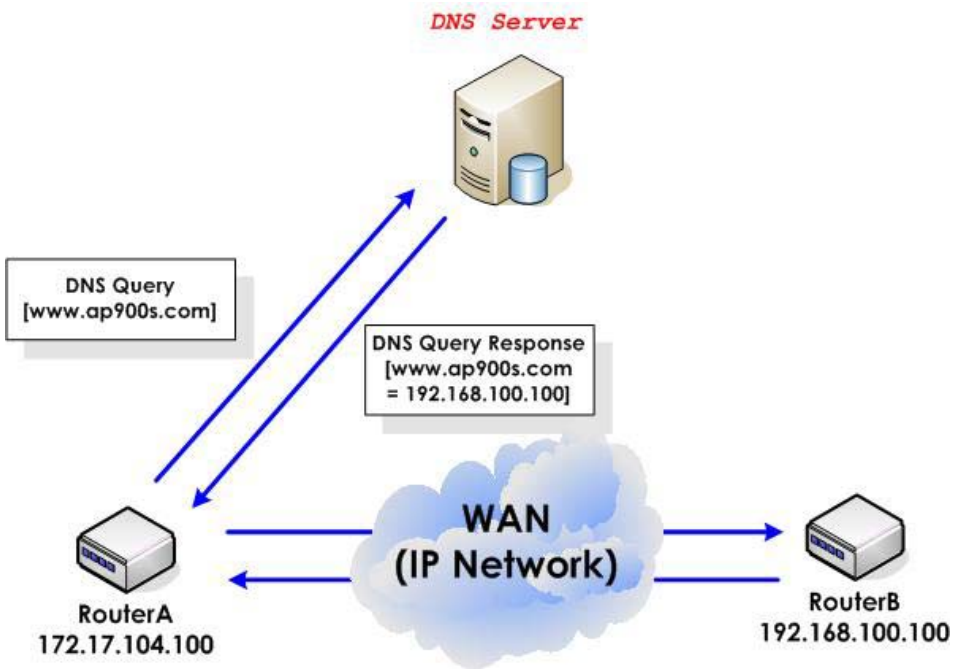


(Figure3-340) DNS Main page

<Table 3-47> DNS menu Description

Elements	Description
Domain-Lookup	It is for Domain-Lookup Service.
Domain-Name	Input Domain Name of AP900S.
Name Server1~5	Input Name Server IP Address. Maximum 5 addresses

Figure 3-344 shows Diagram example of DNS Service

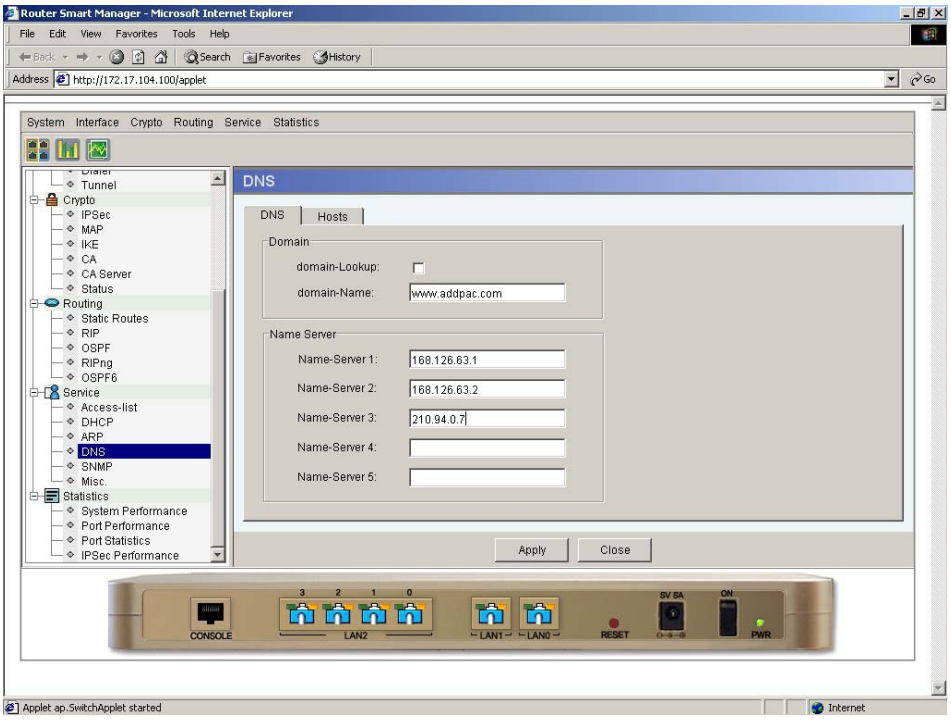


(Figure3-341) DNS Service Diagram example

RouterA only have a domain address of RouterB, "www.ap900s.com" but does not have IP Address of RouterB, then, RouterA can not access to RouterB without DNS Service. So RouterA sends DNS Query for "www.ap900s.com" to DNS Server, DNS Server notify IP Address, "192.168.100.100" as for "www.ap900s.com" to RouterA.

Then RouterA can access to RouterB using IP Address "192.168.100.100" received from DNS Query.

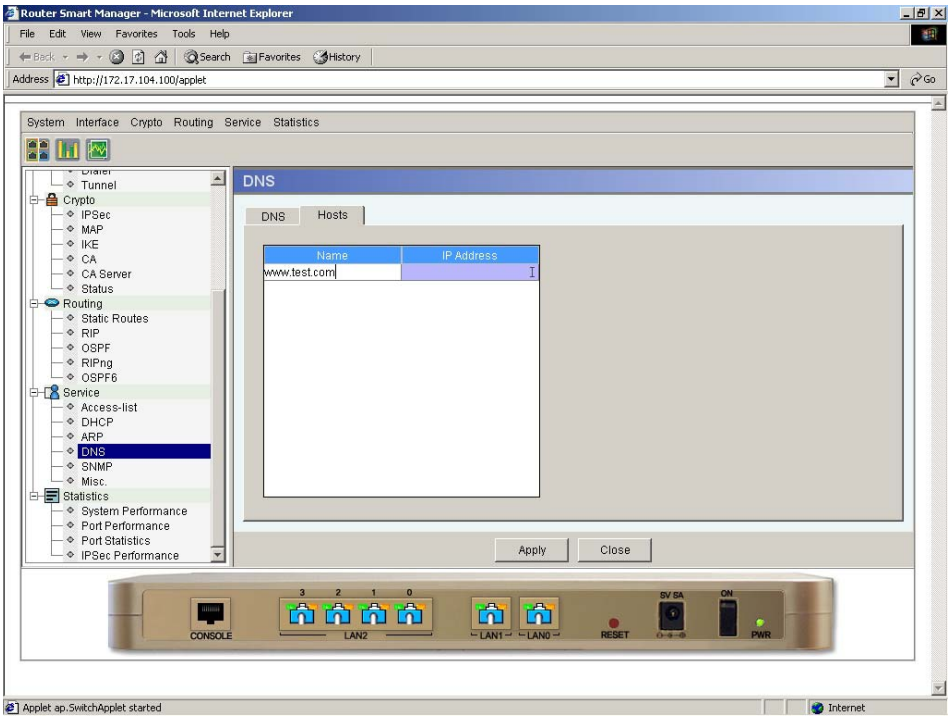
Figure 3-345 shows the example of inputting Domain-Name of AP900S and 3 of DNS Server IP Address.



(Figure3-342) DNS input example

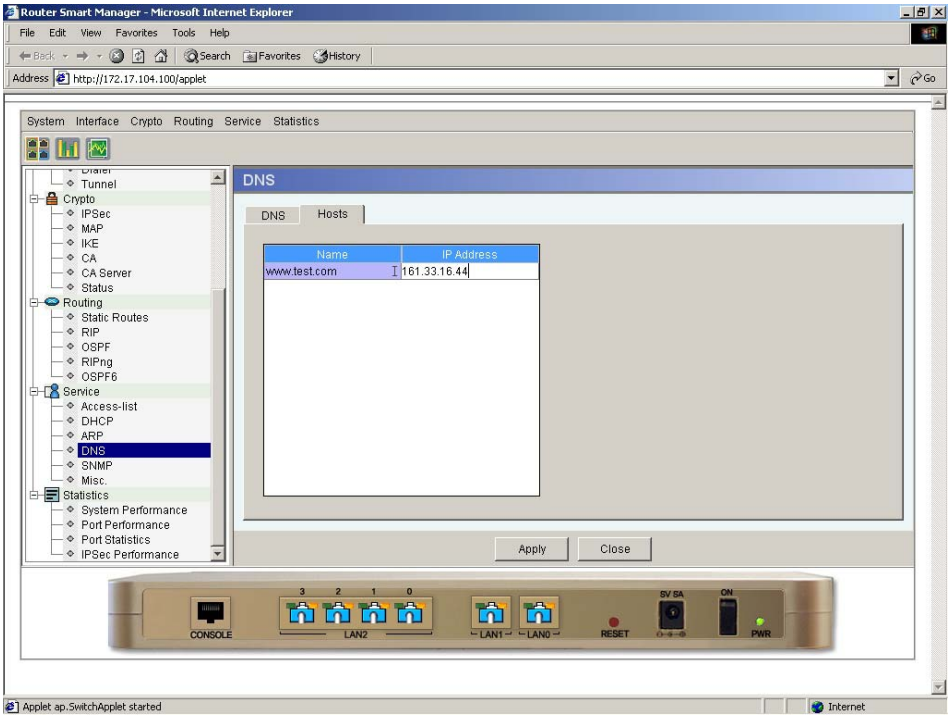
Hosts Menu is used to input Domain IP Address to AP900S without using DNS Server.

Figure 3-346 shows the example of inputting www.test.com in Name filed.



(Figure3-343) Input Host Name

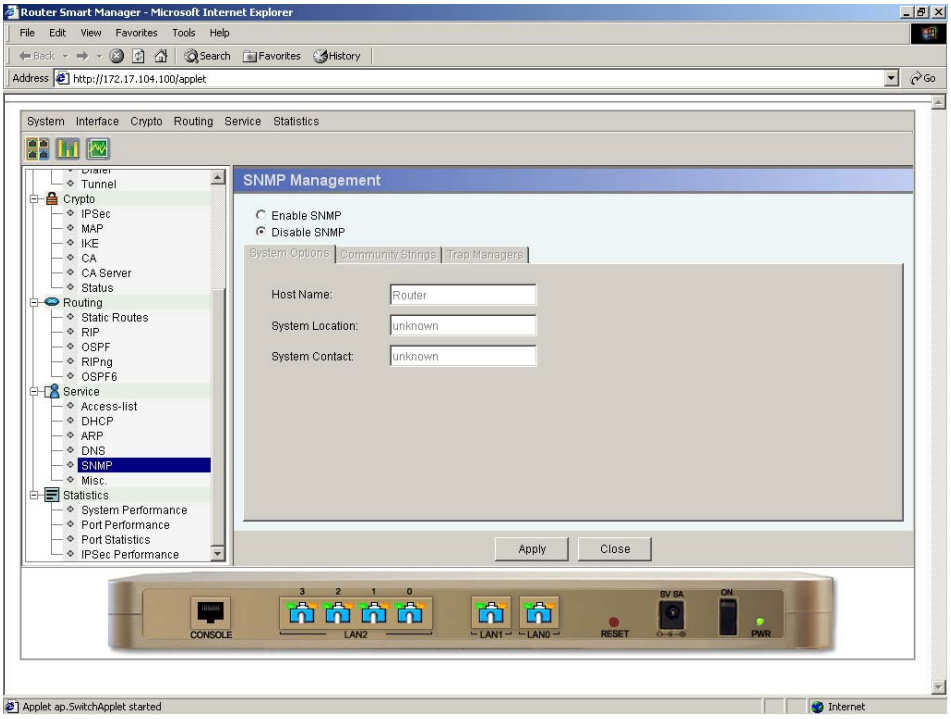
Input IP Address “161.33.16.44” for www.test.com.



(Figure3-344) Input Host IP Address

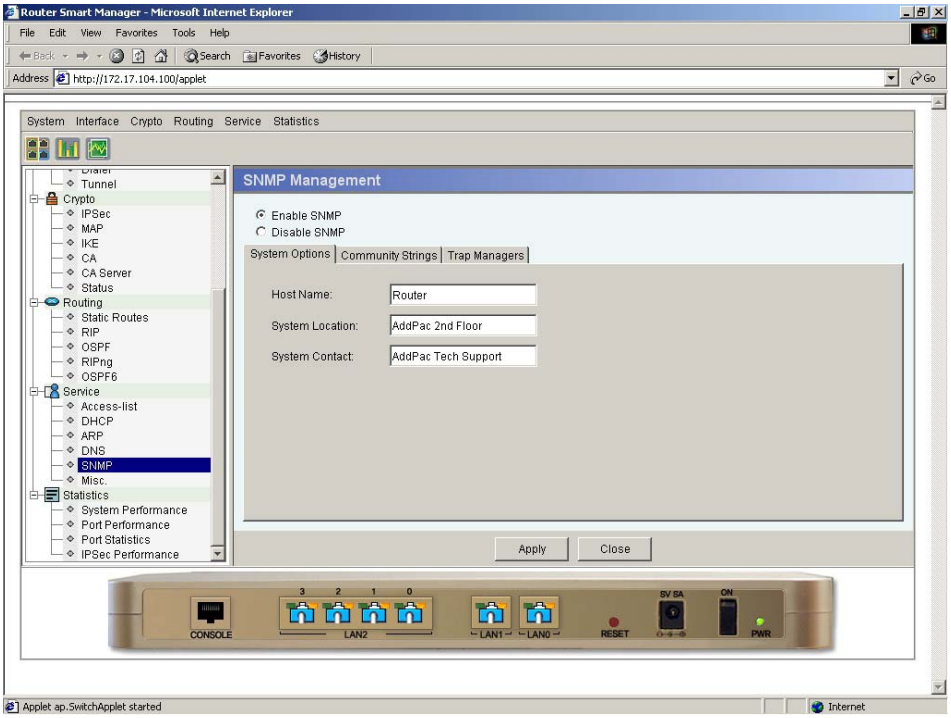
SNMP

It sets SNMP Agent of AP900S so the user can manage AP900S remotely using SNMP Server. Enable SNMP to use. Default is Disable.



(Figure3-345) SNMP Main page

Figure 3-348 shows input example of SNMP System Option.

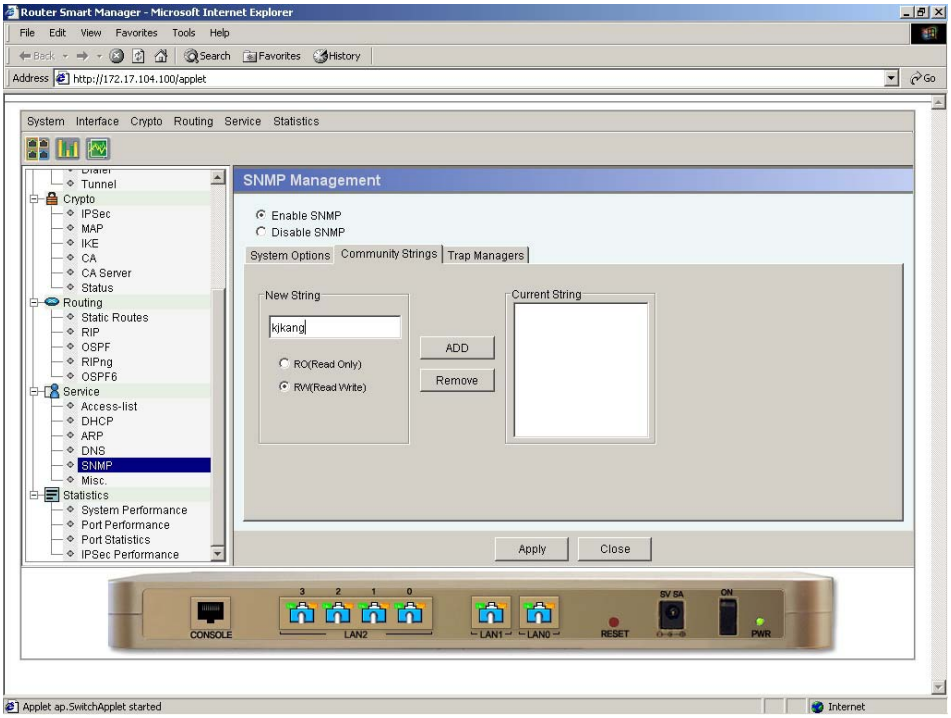


(Figure3-346) SNMP System Option Input example

<Table 3-48> SNMP System Option Description

Elements	Description
Host Name	It sets Host Name of AP900S. You can check the value from "Inventory" Only English characters and numbers can be used for values.
System Location	Input the physical location of AP900S.
System Contact	Input Contact info for any problems on AP900S.

Figure 3-350 shows the example of SNMP Community String.

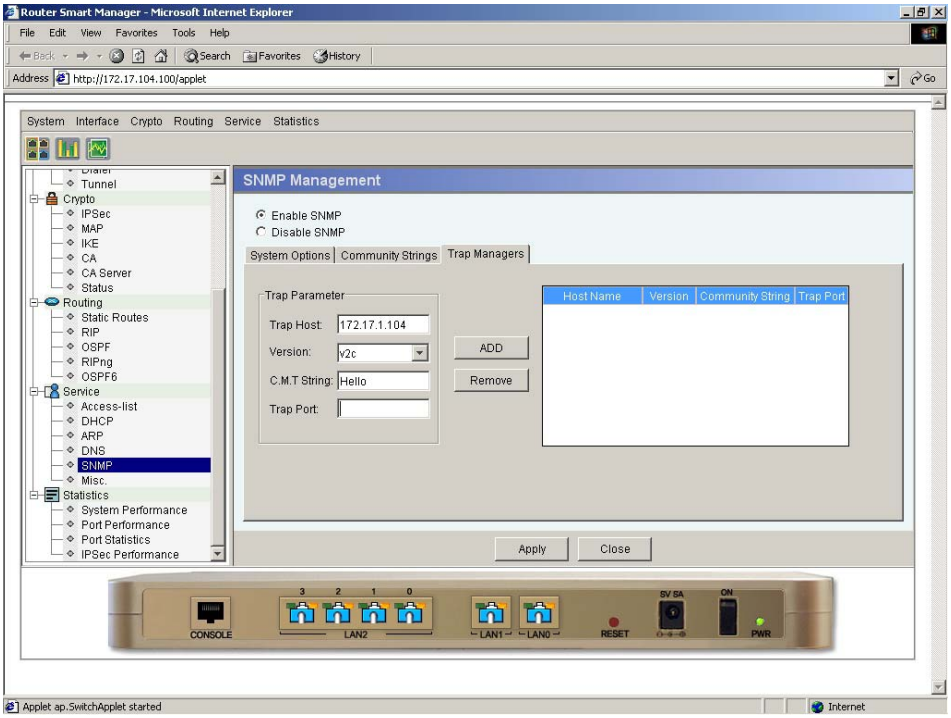


(Figure3-347) SNMP Community String example

<Table 3-49> SNMP Community String Description

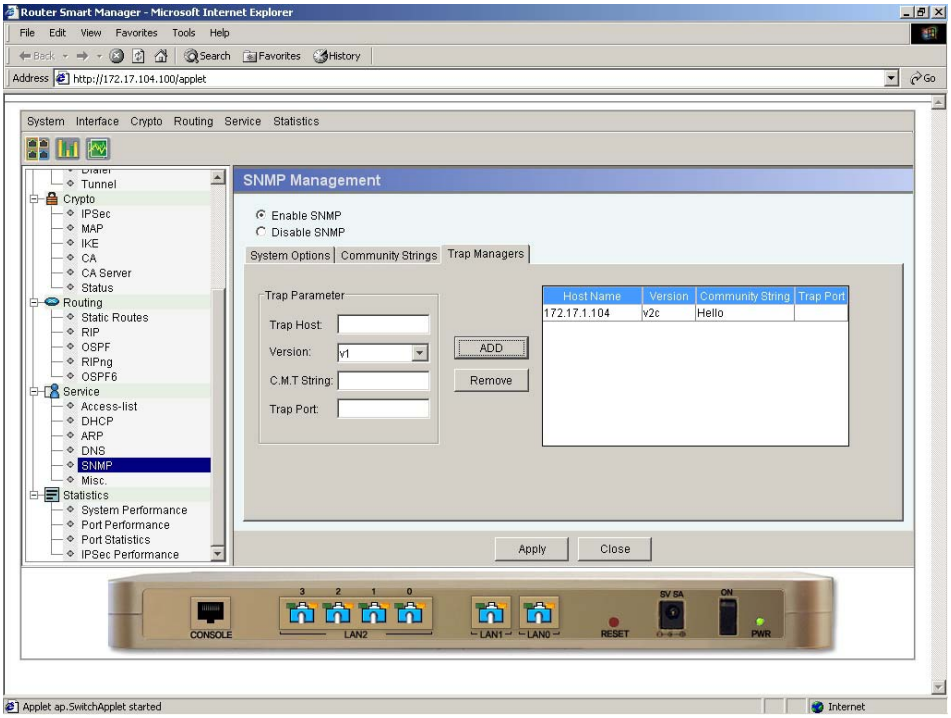
Elements	Description
New String	SNMP Community String. Input a new value then Click “ADD” after selecting RO (Read Only), RW (Read Write) to add.
Current String	It is current Community value. Select Community String value you want to delete then Click “Remove” to delete.

Figure 3-351 shows the example of SNMP Trap Manager.



(Figure3-348) SNMP Trap Managers example

Figure 3-352 shows the example of SNMP Trap Manager.



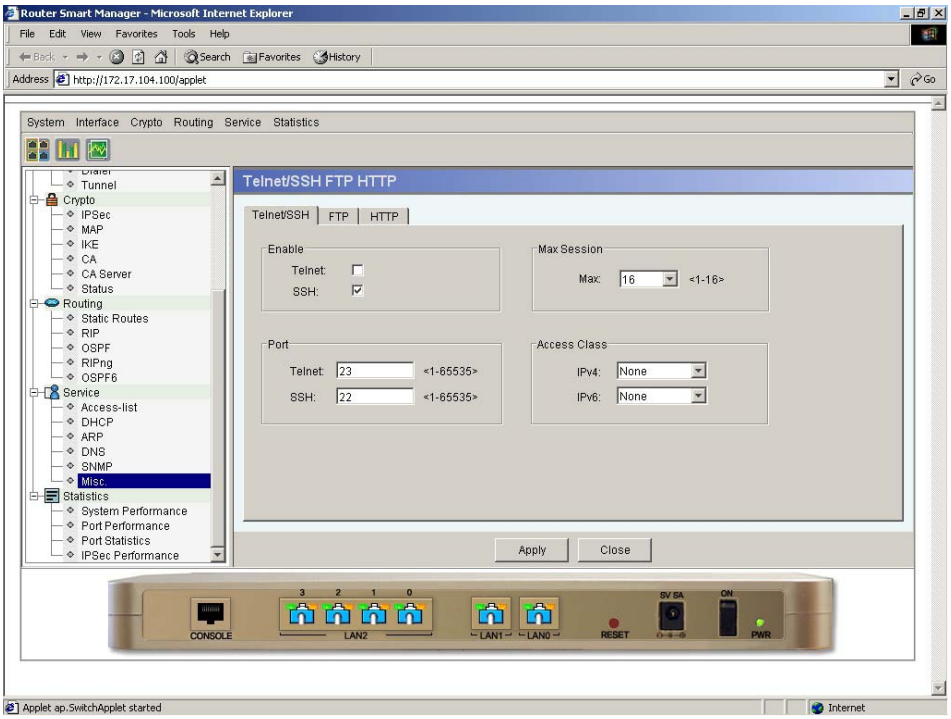
(Figure3-349) SNMP Trap Managers page

<Table 3-50> SNMP Trap Parameter Description

Elements	Description
Trap Host	Input Trap Message to IP Address of host which will be transferred.
Version	Select SNMP Trap Version. It has to be the same as the version of Trap Host.
C.M.T String	Input SNMP Trap Community String.
Trap Port	Input Trap port of SNMP Trap Message.

Misc.

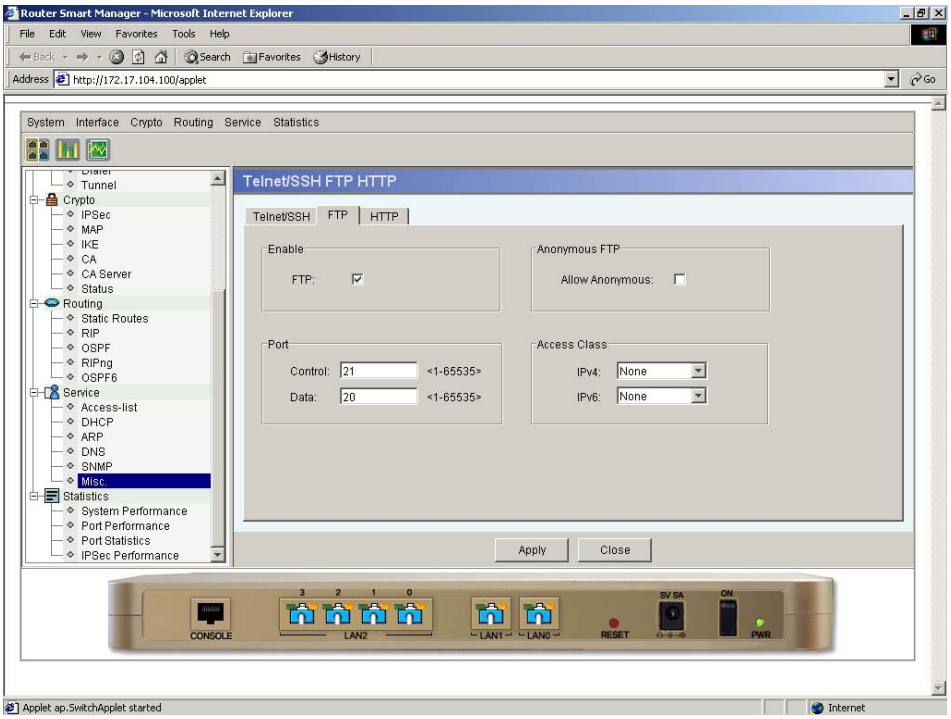
Misc. menu controls Telnet/SSH, FTP, HTTP of AP900S.



(Figure3-350) Telnet/SSH Menu page

<Table 3-51> Telnet/SSH Description

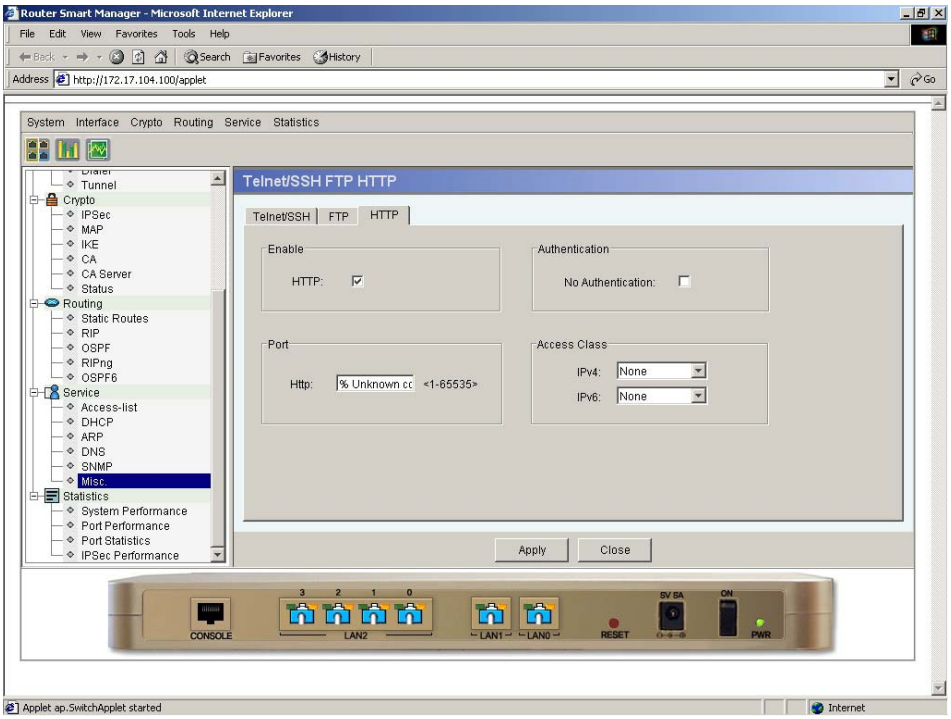
Elements	Description
Enable [Telnet, SSH]	Enable or Disable services such as Telnet, SSH.
Max Session	Limits Remote Access (Telnet/SSH) users.
Port [Telnet, SSH]	Defines TCP Port for Telnet, SSH. Default is 23 for Telnet, default is 22 for SSH.
Access Class	Remote Access Filtering using Access-List of IPv4, IPv6.



(Figure3-351) FTP menu page

<Table 3-52> FTP Description

Elements	Description
Enable [FTP]	Enable / Disable FTP Service.
Allow Anonymous	Allow anonymous FTP access.
Port [Control, Data]	It is used to alter FTP Control Port and Data Port. Default value is 21 for Control Port. Default value is 20 for Data Port.
Access Class	Filtering Remote Access using Access-List of IPv4, IPv6.



(Figure3-352) HTTP Menu page

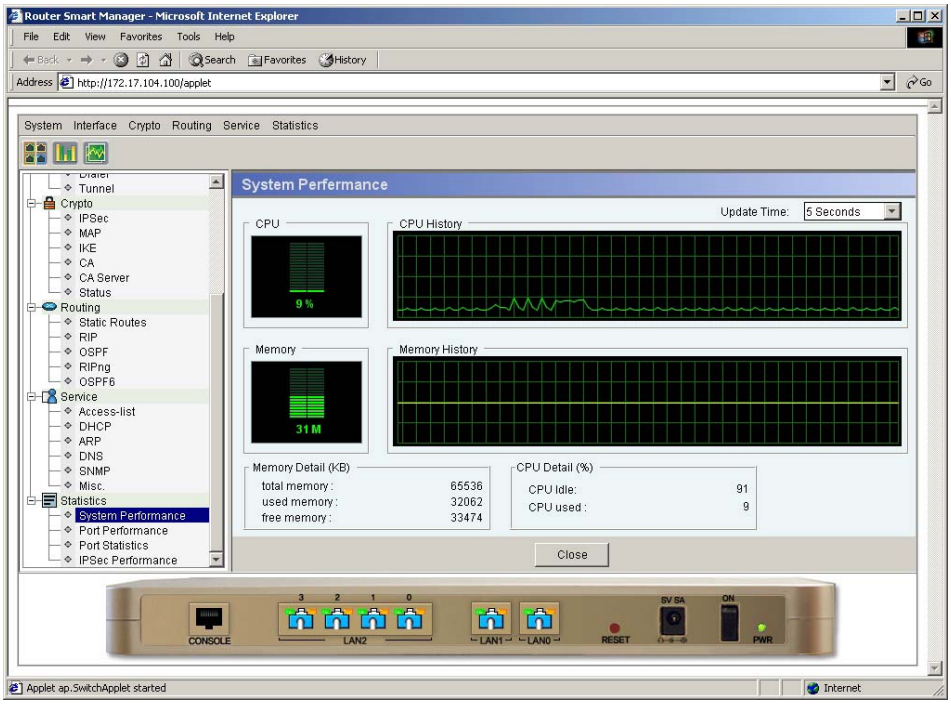
<Table 3-53> HTTP elements Description

Elements	Description
Enable [HTTP]	Enable or Disable HTTP Service.
No Authentication	No authentication for HTTP access.
Port [HTTP]	It is used to change HTTP access Port. Default value of HTTP Port is “80”
Access Class	Filtering Remote Access using Access-List of IPv4, IPv6.

Statistics Menu

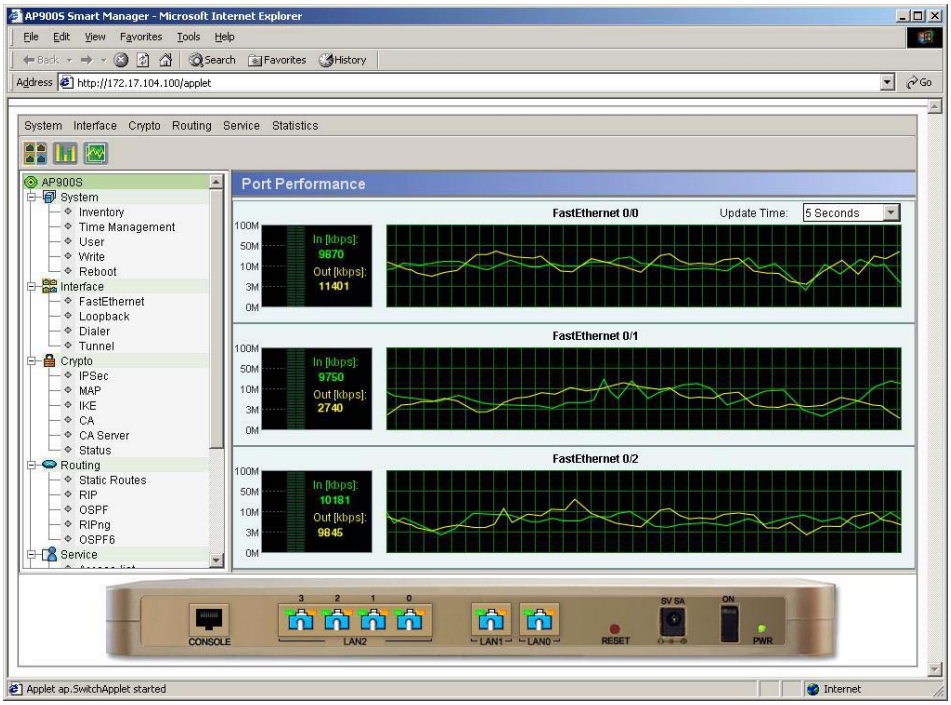
System Performance

System Performance Menu monitors CPU and memory usage of AP900S using graphs. The user can change Update Interval.



Port Performance

Port Performance monitors every Ethernet Port of AP900S. It shows almost real-time data traffic rate about each LAN ports using analog style graphs and digital value. The user can change Update Interval.



(Figure3-353) Port Performance page

Select “show detail” to see a specific Port by clicking right side of the mouse on Port.



(Figure3-354) Port Statistics page

Port Statistics

Port Statistics Menu shows data traffic rate per time for Fast Ethernet 0/0, 0/1, 0/2 of AP900S. It uses analog style graphs and digital numbers. The user can check a specific port time and data traffic rate from the graph using a mouse.



(Figure3-355) System Performance page



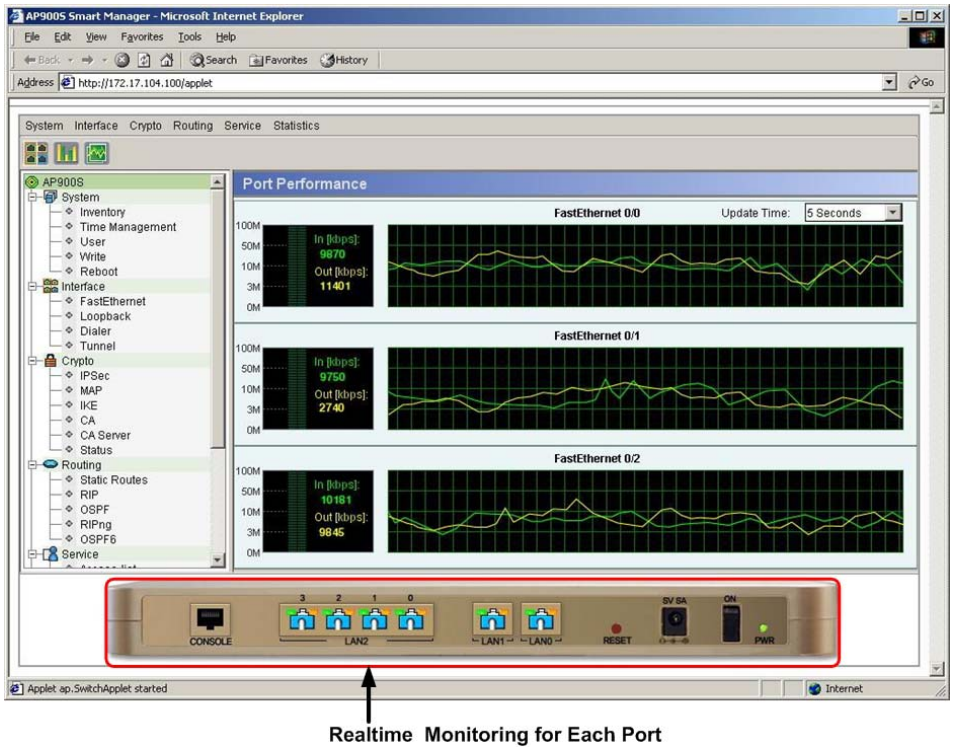
<Table 3-54> Port Statistics Description

Number	Description
①	It shows data traffic rate. The unit is Mbps.
②	It is a mouse Point. Data rate and time of that Point appears as numbers in number 4 and 5.
③	It shows Tx/Rx graph
④	It shows Tx/Rx data rate which the pink stick indicates.
⑤	It shows the time which the pink stick indicates.

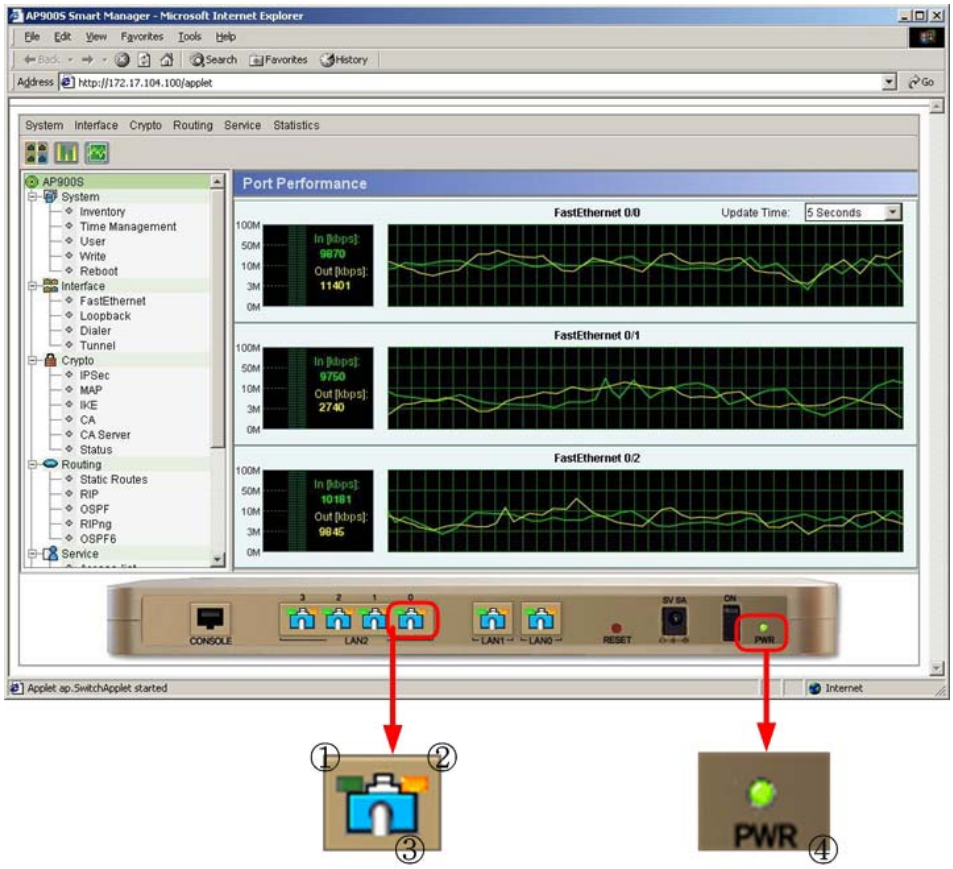
AP900S control method on the front panel

Introducing the front ports of AP900s

The front of AP900S Smart Manager shows real-time operation state of AP900S and Link State of each Port. Also the user can move to Port Configuration, Port Status menu by clicking right side of the mouse on Port.



(Figure3-356) AP900S

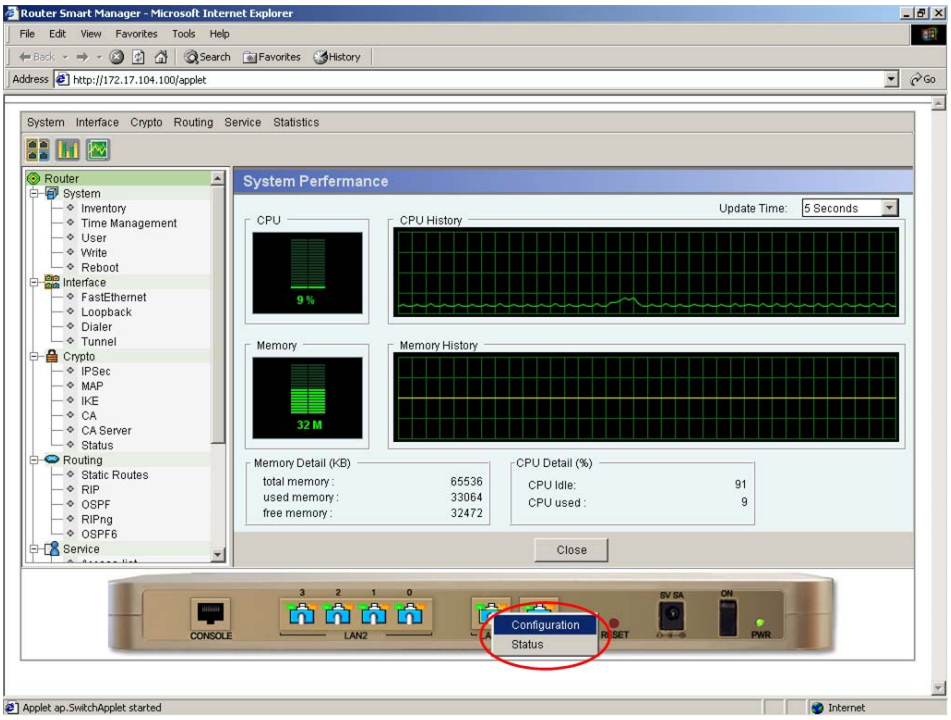


(Figure3-357) AP900S Front

<Table 3-55> AP900S front Description

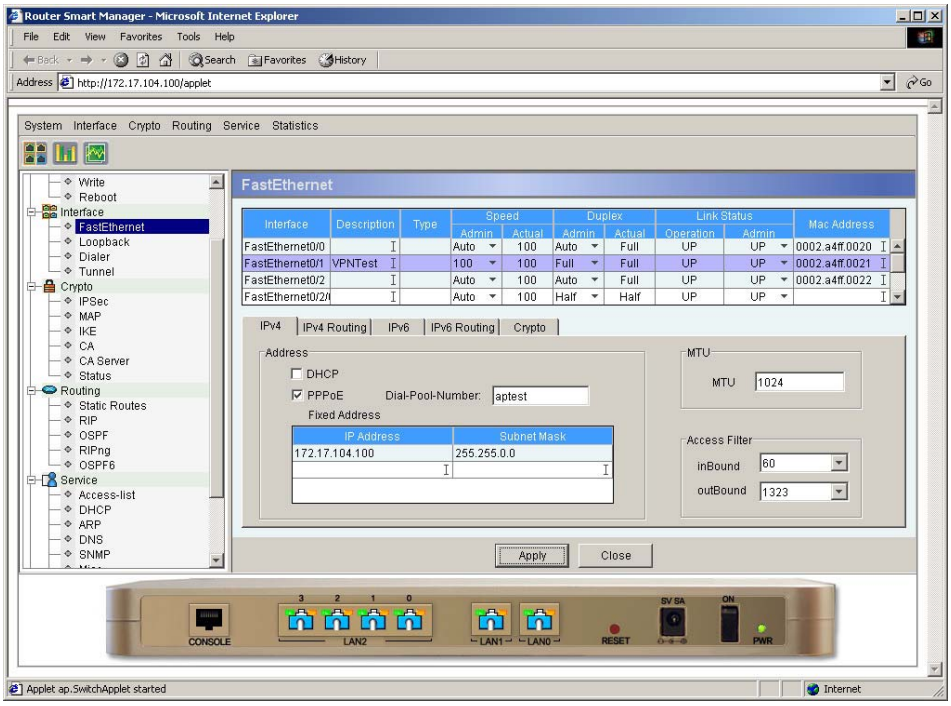
Number	Description
① Link LED	The link state of the port. It is turned off when the link is down, and it blinks in green when the link is up.
② 100Mbps Link LED	It shows 100Mbps Link State of the port. When 100Mbps Link is on, the yellow light is turned on.
③ Connect	If the Port is “Link Up” state, it shows as if UTP cable is on. If the Port is “Link Down” state, it shows Blank.
④ Power LED	Power the AP900S on, the green light is turned on.

The user can execute Port Configuration, Port Status commends by clicking right side of the mouse on a specific Port using Smart Manager.



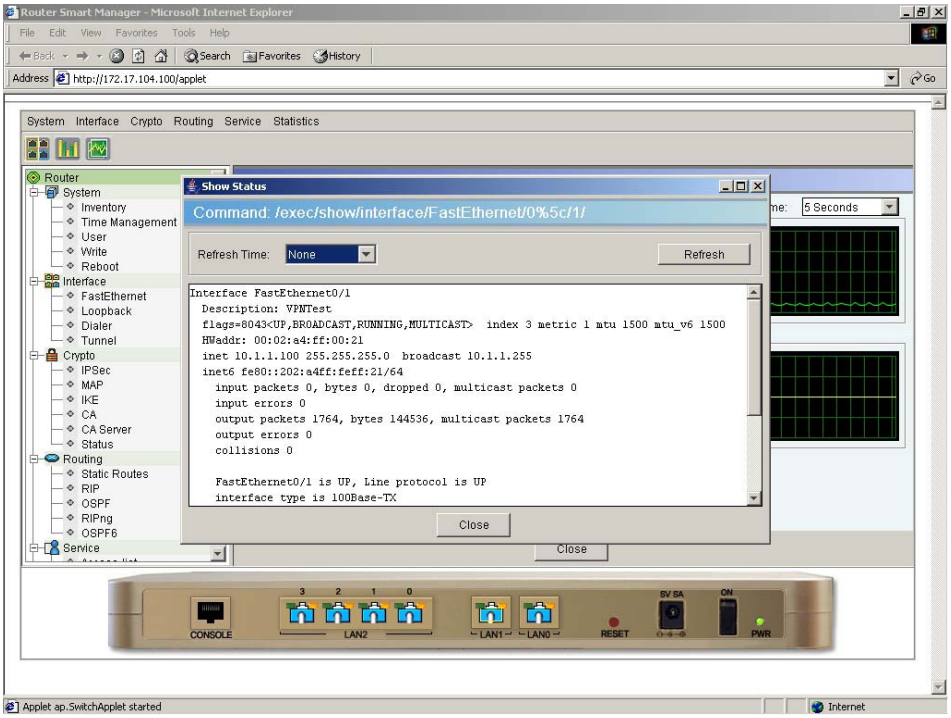
(Figure3-358) Execute AP900S Front Port Configuration

This below Figure 3-363 shows Port Configuration page.



(Figure3-359) Execute AP900S Front Port Configuration

This below shows Port Status page



(Figure3-360) Execute AP900S Front Port Status

Checking list for Smart Manager connection failure

Smart Manager is Java Based Manager of TCP/IP Connection. So the user has to access Web Management System before accessing the Smart Manager. If the TCP/IP Connection is not working properly, check the points below.

1. Make sure if the IP Address of PC is the same as the IP Address of AP900S.
2. Try "Ping" Test to check if it receives Reply Packet properly.

3. Check if HTTP Server is enabled through the Console Terminal.

```
Router# show running-config
hostname Router
------------------------skip-------------------------
http server
```

(Figure3-361) HTTP Server from CLI

4. If the HTTP Server is disabled, try to follow the procedure in Figure3-366. Default login ID is "root/router" in this example.

```
Router#
Router# config terminal
Router(config)# http server
Router(config)# end
Router#
```

(Figure3-362) Enable HTTP Server from CLI

IPSec related technical term

<Table 3-56> IPSec related technical terms

Term	Description
DES	DES is for Encryption and Decryption of Packet Data. It provides high performance Encryption using 56 bit key. Decryption algorithm is used from Remote and it recovers Cipher Text to Clear Text. Shared Secret Keys execute Encryption and Decryption.
3DES	This is a Triple DES algorithm which is transformed from 56 bit DES. 3DES provides much powerful and efficient encryption algorithm by applying 56 bit DES three times.
Diffie-Hellman (D-H)	Diffie-Hellman is Public-key Cryptography protocol. It creates Shared Secret Key for encryption Algorithm (DES or MD5) in unsecured network. Diffie-Hellman is used to create Session Key in IKE. AP900S supports 768, 1024, 153 bit Diffie-Hellman Group.
MD5	It is Message Digest 5. Message Digest 5 is Hash algorithm for Packet Data authentication. AP900S supports HMAC-MD5. Hash is one-way encryption algorithm which uses MD5 for IKE, AH, ESP authentication.
SHA-1	It is Secure Hash Algorithm-1. SHA-1 is a Hash algorithm for authentication of Packet Data. AP900S supports HMAC-SHA-1. IKE, AH, ESP use SHA-1 algorithm for authentication.
RSA Signature	Rivest, Shamir, Adelman Signature is a Public-key encryption system for authentication. IKE use D-H exchange in order to decide Secret Key of IPSec Peer D-H. RSA Signature or Preshared Key is used for authentication.
IKE	Internet Key Exchange. IKE is Hybrid protocol which provides Utility Services such as authentication of IPSec Peer, Negotiation of IKE, IPSec Security Association and key creation for authentication algorithm used by IPSec. IKE and ISAKMP (Internet Security Association Key Management Protocol) is used in the same way.

CA	Certificate Authority. When two IPSec Peer try to communicate, exchanging Digital Certificates is necessary to identify each other. This is CA.
Transport Mode	Transport Mode is used for terminal to terminal security. This mode provides security priority in Transport Layer for Transport Header through packet transforming.
Tunnel Mode	Tunnel Mode is usually used when the destination of packet and secure tunnel terminal is different. So you always have to use Tunnel Mode when tunnel terminal is secure gateway. However Tunnel Mode IPSec can be configured with two hosts. Tunnel Mode encapsulates entire IP datagram after adding a new IP head in order to recognize the start and end point of Tunnel. In this case, Inner header is configured on host, outer header is configured on tunnel terminal.
AH	Authentication Header. AH ensures data authentication, data integrity and security by including information to authenticate IP datagram. AH provides data integrity, data authentication and reply prevents etc.
ESP	Encapsulation Security Payload. It provides data integrity, reply prevents, security function etc. it also provides authentication function depends on types and modes of encryption algorithm.