RN products User's Guide

Release 4.0

Ranch Networks, Inc
Beacon Hill Plaza, Suite 200
65 Highway 34, Morganville, NJ 07751 USA
Ph: +1-732-817-1900

Table of Contents

1. Secure Zones – A Complete Enterprise Security Solution 11
   1.1 Secure Zones vs. VLANs & Firewall 16
   a. Physical and Virtual Secure Zones 18
2. NAT Concepts 21
   2.1 What is NAT? 21
   2.2 Transparent Address Assignment 21
      2.2.1 Static Assignment 21
      2.2.2 Dynamic Assignment 21
      2.2.3 Transparent Routing 21
      2.2.4 ICMP Error Packet Translation 21
   2.3 Variations of NAT 22
      2.3.1 Traditional NAT 22
      2.3.2 Basic NAT 22
      2.3.3 NAPT 22
      2.3.4 Bi-directional NAT 23
      2.3.5 Twice NAT 23
   2.4 RNxx device NAT Terminology 23
      2.4.1 NAT 23
      2.4.2 One-to-One Full NAT 25
      2.4.3 One-to-One Half NAT 27
      2.4.4 No NAT 28
3. Configuring RNxx device 29
   3.1 Product Activation 31
   3.2 System Configuration 35
   3.3 Maintenance 35
   3.4 Management Port Config 37
      3.4.1 Management Port Config for RN20/40/41 37
      3.4.2 Management Access configuration for RN300 40
   3.5 Image Config 41
      3.5.1 Downloading Image to RN device 41
      3.5.2 Update Configuration 42
      3.5.3 Version Info 44
   3.6 Syslog and alerts configuration 45
      3.6.1 Syslog messaging configuration. 45
      3.6.2 Email messaging configuration 46
      3.6.3 Email messaging notification configuration 47
   3.7 User Admin 48
   3.8 SSL Config 50
   3.9 Diagnostics 51
   3.10 Features Upgrade 55
   3.11 56
   3.12 Reboot 56
   3.13 Securing the access to RNxx device management GUI 57
      3.13.1 Remote access to the RNxx management GUI 57

3.13.2 RNxx management GUI access monitoring 60
4. Network Management 62
4.1 Zone Configuration 63
4.2 Topology Configuration 65
4.2.1 The Physical Zone Configuration 66
4.2.2 The Virtual Zone configuration 67
4.2.3 The Zone additional services configuration 69
4.3 Routing Configuration 70
4.4 Port Configuration 71
4.5 Spanning Tree Protocol (RN5, RN20, RN40, RN41 models): 73
4.6 Topology information 74
5. Firewall Configuration 75
5.1 RNxx firewall components 75
5.2 RNxx firewall concept 77
5.3 Security Profile 79
5.4 Firewall Rules 81
5.4.1 The IP Addresses and Port Settings Configuration 88
5.5 Global Security Settings 94
5.6 NAT Configuration 95
5.7 DHCP Configuration 100
5.7.1 DHCP Relay Configuration 100
5.7.2 DHCP Server Configuration 101
5.8 MAC security configuration (RN 5/20/40/41 models only) 107
5.9 User Authentication 109
6. VPN Configuration 117
6.1 VPN overview 117
6.2 IPSec primer 117
6.3 IKE Overview 120
6.4 NAT Traversal overview 121
6.5 Ranch Networks VPN configuration. 122
6.5.1 VPN Global Configuration. 122
6.5.2 RN VPN Tunnel Set Up. 124
6.6 RN VPN monitoring 132
7. Bandwidth Accounting and Control 134
7.1 Outbound policies configuration: 138
8. Server Groups and Servers 145
8.1 Server Groups Configuration 145
8.2 Servers in Server Group 146
9. Load Balancing 147
9.1 Basic Steps to Implement RNxx Load Balancing 153
9.2 Load Balancing configuration example 154
9.2.1 Step 1 – Server Groups and Servers Configuration 154
9.2.2 Step 2 156
9.2.3 Step 3 157
9.2.4 Step 4 158

9.2.5 Step 5 (Monitoring) 163
9.2.6 Email notification 165
10. Servers Health Monitoring 167
10.1 Server Group Configuration 171
10.2 Steps to configure HTTP & FTP Health Monitoring 175
10.2.1 HTTP HM Configuration 175
10.2.2 FTP HM Configuration 178
10.2.3 Email notification 180
11. Multicast Configuration 182
11.1 Multicast Terms and Concepts 182
11.2 Configuring RNxx device20 Multicasting 184
12. High Availability Configuration 189
12.1 Configuring High Availability 192
13. Port Mirroring Configuration 194
(RN 5/20/40/41 models only) 194
13.1 Steps to configure Port Mirroring on RN20 195
14. Software Update Steps & Changing RN Models 199
14.1 Step 1 – Obtain the latest RN image. 199
14.2 Step 2 – Backup the existing configuration. 199
14.3 Step 3 – Download the software image to RN 199
14.4 Step 4 – Reboot RN with a new image 200
14.5 Step 5 – Enter Activation Key (if required) 200
14.6 Step 6 – Check device is booted with new version 200
14.7 Changing RN Models: 201
15. RN Network Configuration examples. 203
15.1 Example 1 : RN device with three physical zones 203
15.1.1 Step 4 : Bring Up the physical ports assigned to the zones 209
15.2 Example 2 : RN device with virtual zones 216
16. Example 3 : Different NAT configurations examples 223
17. Example 4: RN syslog configuration 229
18. RNxx log messages definitions 232
18.1 The fields of the RNxx log message 232
18.2 Log Message categories 233
18.3 The log messages list and description 234
18.3.1 Login / Logout related 234
18.3.2 Front Panel settings modifications 236
18.3.3 Reboot messages 237
18.3.4 FW service status 237
18.3.5 RNxx Management settings modifications 238
18.3.6 Image file changes 239
18.3.7 Configuration file changes 239
18.3.8 FW user administration 240
18.3.9 Zone configuration 241
18.3.10 Topology configuration 242
18.3.11 Routing configuration 243

18.3.12 Port configuration 244
18.3.13 FW Rule administration 245
18.3.14 Security Profile administration 246
18.3.15 NAT administration 247
18.3.16 DHCP Relay configuration 248
18.3.17 MAC Security administration 249
19. RN Services Configuration routes 250
19.1 Networks Services Configuration route 250
19.2 Firewall Configuration Route 251
19.2.1 Security profiles and Rules Configuration 251
19.2.2 User Authentication Configuration 252
19.3 Bandwidth Accounting and Control Configuration route 253
19.4 Servers Group and Load Balancing Configuration route 254
20. Dictionary 257
20.1 NAT 257
20.2 Interface (zone topology) 257
20.3 Port (zone topology) 257
20.4 Rule 257
20.5 Rule (firewall) 257
20.6 Rule (load balancing) 257
20.7 Secure profile 257
20.8 Secure zone 257
20.9 Secure physical zone 257
20.10 Secure virtual zone 257
20.11 Subnet 257
20.12 VPN 257

Figure 1. Conventional Firewall Security 11
Figure 2 The relation between the secure zone and the network objects 13
Figure 3 Traffic trough the secure zone of RNxx device 14
Figure 4. RNxx device Secure Zones 15
Figure 5. Conventional VLAN Approach 16
Figure 6. Secure Zones Approach 17
Figure 7 Physical Secure Zone Topology 18
Figure 8. Virtual Zones Topology 19
Figure 9. NAT Option 24
Figure 10. One-to-One Full NAT Option 25
Figure 11. One-to-One Half NAT option 27
Figure 12. No NAT Option 28
Figure 13 RNxx device Management Interface main elements 29
Figure 14 RNxx device Management Interface main elements (cont.) 30
Figure 15. RNxx device Product Activation Screen 34
Figure 16. System Configuration -> Maintenance 35
Figure 17. System Configuration -> Mgmt Port Config 38

Figure 18. Management Infrastructure 39
Figure 19 System Configuration->Management Port Configuration (RN300) 40
Figure 20 System Configuration->Image Configuration->Download Image..... 41
Figure 21. System Configuration->Image Config->Update Configuration..... 42
Figure 22 System Configuration->Image Config ->Version Info 44
Figure 23. System Configuration -> Syslog Config 45
Figure 24 System Config-> Syslog->Email Config 46
Figure 25 System Config-> Syslog->Email Notification 47
Figure 26. Map: System Configuration->User Admin->ADD/DELETE USERS 48
Figure 27. System Configuration->Current User..... 49
Figure 28. Map: System Configuration->SSl Config 50
Figure 29. System Configuration->SSL Config 50
Figure 30 System Configuration->Diagnostics->Ping 51
Figure 31 System Configuration->Diagnostics->ARP table 52
Figure 32 Add ARP entry screen..... 52
Figure 33 Add ARP entry screen (cont.) 53
Figure 34 Add ARP entry screen (cont.) 53
Figure 35 System Configuration->Diagnostics->Network Statistics 54
Figure 36. System Configuration->Reboot..... 56
Figure 37 The management and data ports (RN5/20/40/41) 57
Figure 38 System Configuration->Maintenance..... 58
Figure 39 Users Configuration..... 59
Figure 40 Network Management->Zone Configuration..... 63
Figure 41. Physical and Virtual Zones..... 65
Figure 42 Network Management->Topology Config->Physical Zones..... 66
Figure 43 Network Management->Topology Config->Virtual Zone..... 67
Figure 44 Network Management->Zone Configuration..... 69
Figure 45 Network Management->Routing Configuration 70
Figure 46 Network Management->Port Configuration 71
Figure 47 The traditional firewall..... 77
Figure 48 The traditional approach (incoming outgoing connections)..... 79
Figure 49 RNxx firewall approach 80
Figure 50 RNxx firewall rule configuration path 81
Figure 51. Custom Security profile configuration..... 82
Figure 52. Firewall Configuration->Security Profiles..... 83
Figure 53. Firewall Configuration->Security Profiles (cont.) 84
Figure 54. Firewall Configuration->Security Profiles->Basic (rules) configuration..... 85
Figure 55. Firewall Configuration->Security Profiles->Basic Rules->IP settings..... 88
Figure 56. Firewall Configuration->Security Profiles->Basic Rules->IP settings (cont.) 88
Figure 57. Firewall Configuration->Security Profiles->Basic Rules->IP settings (cont.) 89
Figure 58.Firewall Configuration->Security Profiles->Basic Rules->Port settings..... 89
Figure 59. Firewall Configuration->Security Profiles->Basic Rules->Port settings (cont.)
..... 90
Figure 60. Firewall Configuration->Security Profiles->Basic Rules->Port settings (cont.)
..... 90

Figure 61. Firewall Config->Security profiles->Basic (rules) Config->Advanced Configuration 91
Figure 62. Firewall Configuration->Security Profiles->Global Settings..... 94
Figure 63. Firewall Configuration->NAT Configuration 95
Figure 64. Firewall Configuration->NAT Configuration (cont.)..... 96
Figure 65. Firewall Configuration->NAT Configuration->Zones with No NAT Configuration 97
Figure 66. Firewall Configuration->NAT Configuration->One-to-One NAT Configuration 98
Figure 67 Firewall Configuration->NAT Configuration->Static NAT Configuration..... 99
Figure 68. Firewall Configuration -> DHCP Relay Configuration 100
Figure 69. Firewall Configuration->MAC security Configuration..... 107
Figure 70. User Authentication Logic 109
Figure 71 AD and LDAP server DNS config 110
Figure 72 Firewall Configuration->User Authentication-> Authentication Servers 111
Figure 73 Firewall Configuration->User Authentication-> Authentication Servers 112
Figure 74. Firewall Configuration->User Authentication->General Configuration..... 113
Figure 75.Firewall Configuration->User Authentication->User Configuration..... 114
Figure 76. Firewall Configuration->User Authentication->User Administration 115
Figure 77. Firewall Configuration->User Authentication->Session Administration 116
Figure 78 VPN->VPN Global Configuration 122
Figure 79 VPN->VPN Tunnel Set Up->Tunnel Config 124
Figure 80. Bandwidth Management Concepts..... 134
Figure 81. Outbound Traffic Control..... 137
Figure 82. Bandwidth Accounting and Control ->Outbound Traffic Policies 138
Figure 83.Bandwidth Accounting and Control ->Outbound Traffic Policies->BW Class Name 139
Figure 84. Bandwidth Accounting and Control ->Outbound Traffic Policies->Contract Traffic Filter..... 140
Figure 85. Bandwidth Accounting and Control ->Inbound Traffic Policies 142
Figure 86. Server Groups and servers->Server Groups Configuration..... 145
Figure 87. Server Groups and servers->Server in Server Group Configuration..... 146
Figure 88. Load Balancing Concepts..... 148
Figure 89. Server Groups Configuration 154
Figure 90. Servers in Server Group Configuration..... 155
Figure 91. Load Balancing-> Server Configuration ->Server Groups Configuration..... 156
Figure 92. Load Balancing -> Switching Configuration -> Virtual IP Configuration ... 157
Figure 93. Load Balancing ->Switching Configuration-> Switching Rules 158
Figure 94. Load Balancing ->Switching Configuration-> Switching Rules (cont.)..... 159
Figure 95. Load Balancing->Switching Config->Switching Rule->IP Settings 160
Figure 96. Load Balancing-> Switching Config->Switching Rule->IP Settings (cont.) 161
Figure 97. Load Balancing-> Switching Config->Switching Rule->IP Settings (cont.) 161
Figure 98. Load Balancing-> Switching Config->Switching Rule->Port Settings 161
Figure 99. Load Balancing-> Switching Config->Switching Rule->Port Settings (cont.) 162

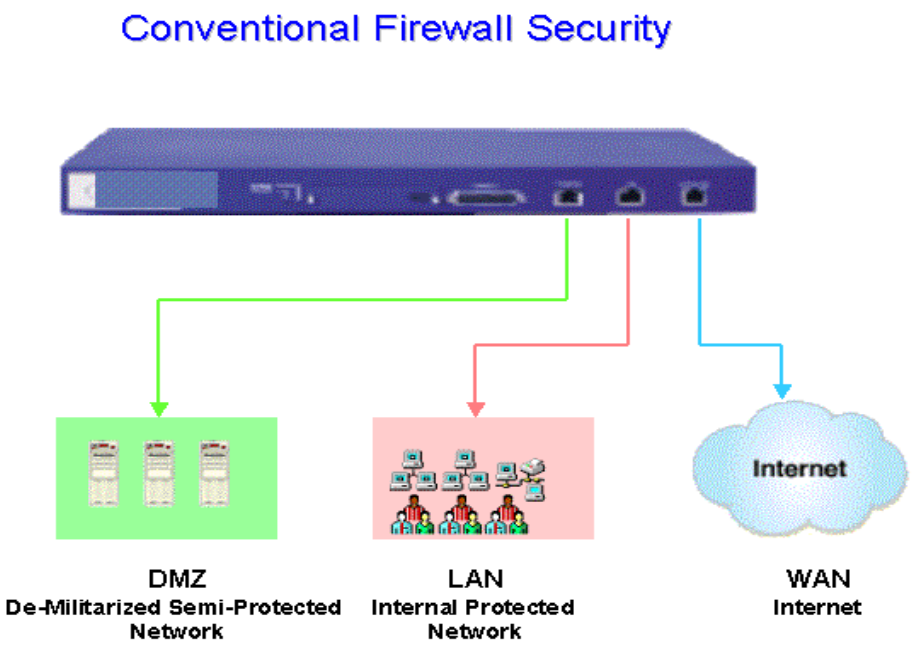
Figure 100. Load Balancing-> Switching Config->Switching Rule->Port Settings (cont.) 162
Figure 101. Load Balancing->Server Configuration->Servers Statistics 163
Figure 102. Load Balancing->Server Configuration->Server Groups Statistics 164
Figure 103. Server Health Monitoring->Server Group HM 171
Figure 104. Server Health Monitoring->Server Group HM (cont.) 171
Figure 105. Server Health Monitoring->Server Group HM (cont.) 174
Figure 106: Health Monitoring -> HTTP HM Configuration 175
Figure 107.Server Group HM -> HTTP monitoring Configuration 176
Figure 108. SHM screen with the server groups configured for HTTP HM 177
Figure 109 Health Monitoring->FTP HM Configuration 178
Figure 110. Health Monitoring -> Server group HM , FTP HM configuration 179
Figure 111. Mutlicast Setup 185
Figure 112. Multicast Settings->IGMP Interface 186
Figure 113. Multicast Settings->IGMP Cache 187
Figure 114. High Availability Configuration 189
Figure 115. High Availability Configuration Screen 192
Figure 116. Port Mirroring Setup 195
Figure 117 . Port Mirroring -> Port Mirrors Configuration 196
Figure 118. Port Mirroring -> Port Mirrors Configuration (cont.) 197
Figure 119. Port Mirroring -> Port Mirrors Configuration (cont.) 198
Figure 120: System Configuration -> Image Config -> Version Info 200
Figure 121. RN examples : Network Assets for the example 203
Figure 122. RN Login screen 204
Figure 123. RN Web interface first screen 205
Figure 124. RN Examples - Zone Configuration 206
Figure 125. RN examples - Topology Configuration (Physical Zone) 207
Figure 126. RN examples - Routing Configuration 208
Figure 127. RN examples - Port Configuration 209
Figure 128. RN examples - Topology Information 210
Figure 129. RN examples - Firewall configuration 211
Figure 130. RN examples - Security Profile Configuration 212
Figure 131. RN examples - Internet Zone rules 213
Figure 132. RM examples - Security profiles 214
Figure 133. RN examples - The configured topology 215
Figure 134. The initial picture for Virtual topology example 216
Figure 135. RN examples - Login screen 217
Figure 136. RN examples - the RN interface first page 218
Figure 137. RN examples - Topology with the virtual zones 219
Figure 138. RN examples - Topology for the "Visitors" Zone 220
Figure 139. RN examples - The final network topology (Virtual zones) 221
Figure 140. Example 3 - Network Topology 223
Figure 141. Example 3 - Zone Configuration 224
Figure 142. Example 3 - Zone Topology Configuration 225
Figure 143. Example 3 - NAT Configuration 226
Figure 144. Example 3 - Security Profiles -> Rules Configuration 227

Figure 145. Example 3 - One-to-One NAT Configuration 228
Figure 146.Example 3 - One-to-One NAT Configuration (cont.) 228
Figure 147.Example 3 - One-to-One NAT Configuration (cont) 229
Figure 148. RN Syslog Configuration 230

1. Secure Zones – A Complete Enterprise Security Solution

Conventional security solutions and products that are deployed in the enterprise networks are based on the premise that the enterprise is a trusted domain and malicious activities and security breaches occur exclusively from external sources, i.e. Internet But as numerous surveys show one of the greatest threats to business computer systems, network and data isn't from hackers or competitors. It is from employees, partners and other trusted insiders with authorized access to company's systems, networks and proprietary information.

Figure 1. Conventional Firewall Security



. A conventional firewall partitions the enterprise into three distinctive domains:

- External (WAN) – resources outside of the enterprise perimeter.
- Internal (LAN) – resources within the perimeter that need protection
- DMZ (De-Militarized Zone) – A set of corporate resources that need certain level of protection but is "directly" accessible from external domain.

The conventional firewall activates security policies and rules for the traffic that traverses the boundary between external and internal domains, treating the latter as completely secure. But as we mentioned earlier, the major threat to the enterprise resources emanates from within that internal domain, and here conventional firewall is helpless. It should be noted that network equipment vendors try to add security capabilities to L2/L3 switches and routers, but these capabilities lack the breadth and depth of the firewalls, and as such cannot be relied on to protect against internal threats.
So, what the enterprises need today is the ability to apply firewall concepts and techniques to internal domain as well, treating it as a source of potentially devastating attacks.

Ranch Networks offers a comprehensive solution that encompasses both an external and internal security with an introduction of **Secure zones**.
RNxx device provides the much needed functionality by enabling network managers to define and enforce security policies not only at the perimeter of the enterprise, but also, and most importantly, within its coveted internal networks.
In addition to its security capabilities, RNxx device offers a set of high-value features, like bandwidth management, VPN, VoIP, load balancing, port aggregation and MAC-based filtering that greatly enhance the efficiency of network operation without major capital investments.

As was stated earlier, the entire operation of RNxx device is based on the concept of a secure zone.

Secure zones enable network managers to implement security policies not just at the perimeter, but also throughout the whole enterprise. With this approach Internet is treated like any other zone with its own set of policies and rules

The Secure zone - is a collection of objects such as: physical ports, subnets, virtual LANs and more .All of the mentioned above objects are regulated by the set of the rules that created for the zone. The following table is a definition of the main objects inside the zone

Table 1 Objects Definition

Name of the Object	**Description**	**Assignment**
Port	The physical port on RN device	Assigned to the zone, multiple ports could be assigned to the same zone
Subnet	The IPv4 subnet that connected to RN device	Assigned to the zone, multiple subnets could be assigned to the same zone
Network interface of the zone	The IPv4 Setting (IP address and network mask)	Assigned to the zone, multiple interfaces could be assigned to the same zone

Security profile	The set of the rules for the Zone	Assigned to the zone (also could be assigned to the user (see User Authentication))
Virtual LAN	VLAN that reside ether on RN device or coming from outside	Assigned to the zone, multiple VLAN tags could be assigned to the same zone

Figure 2 The relation between the secure zone and the network objects

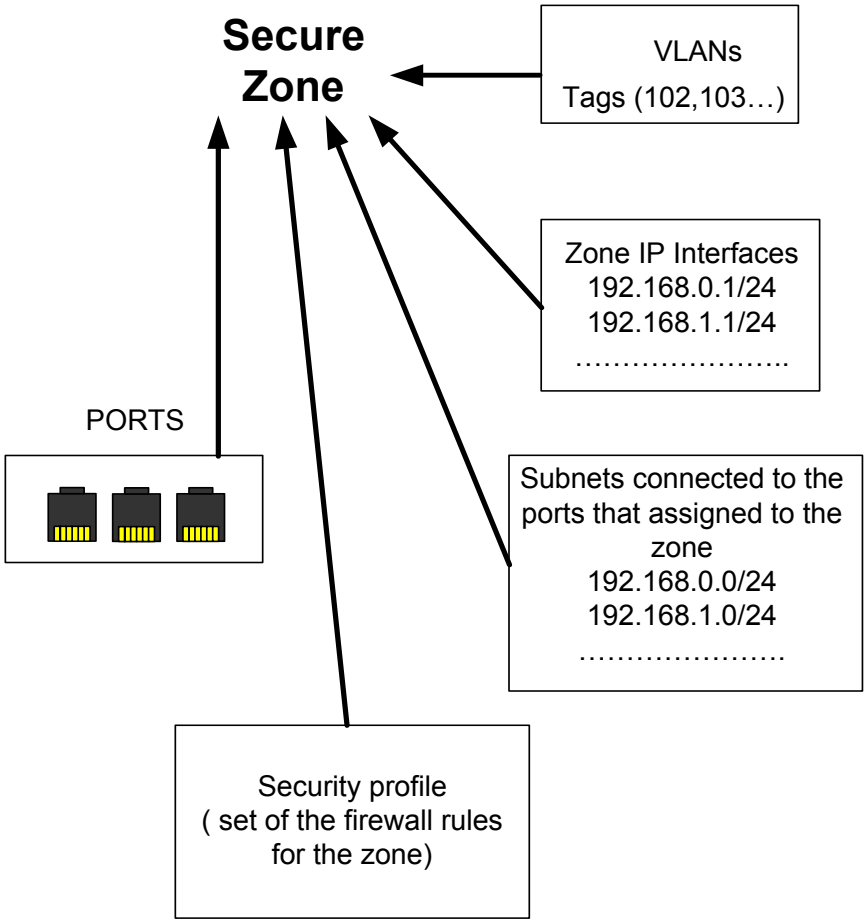
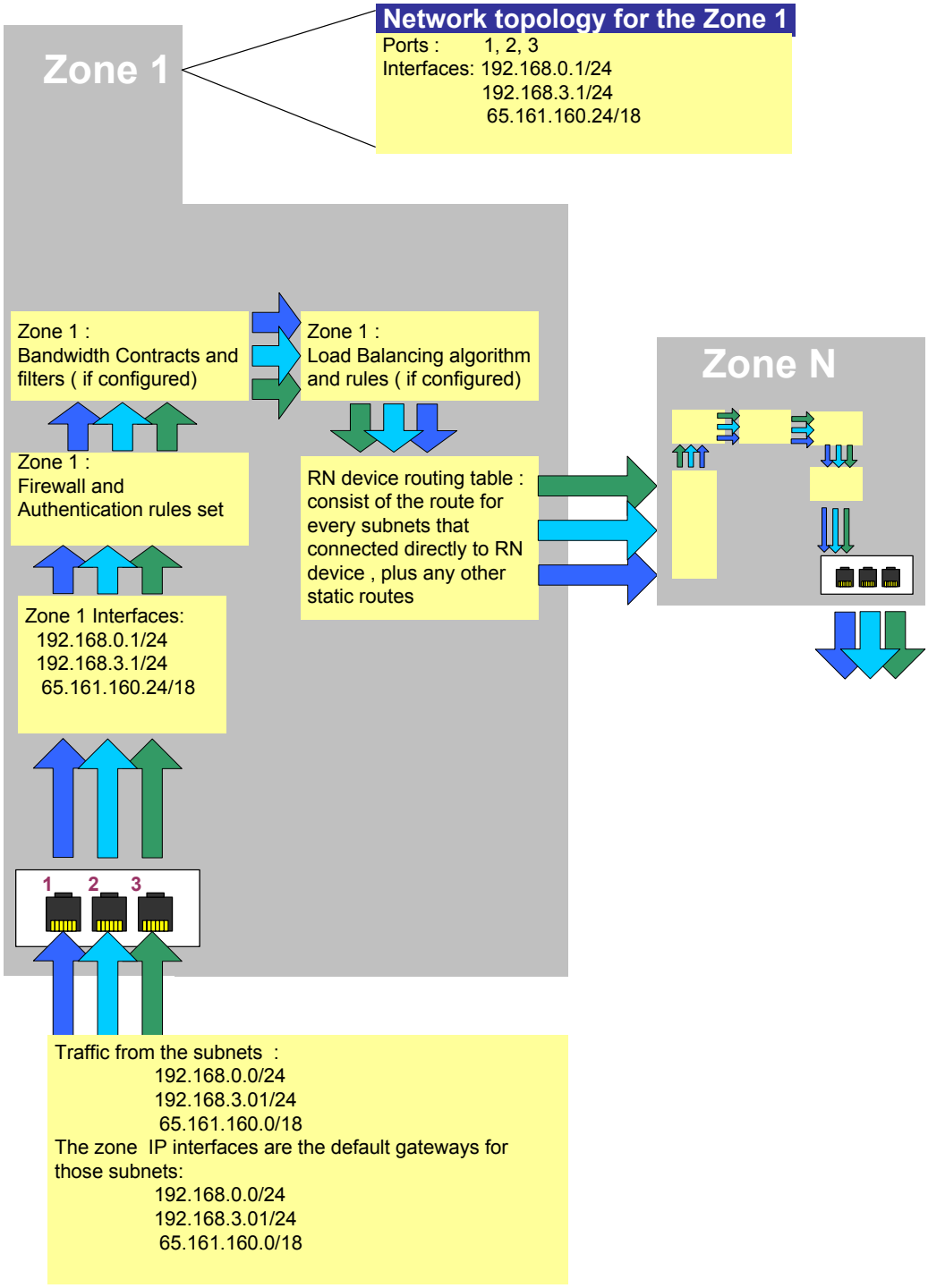
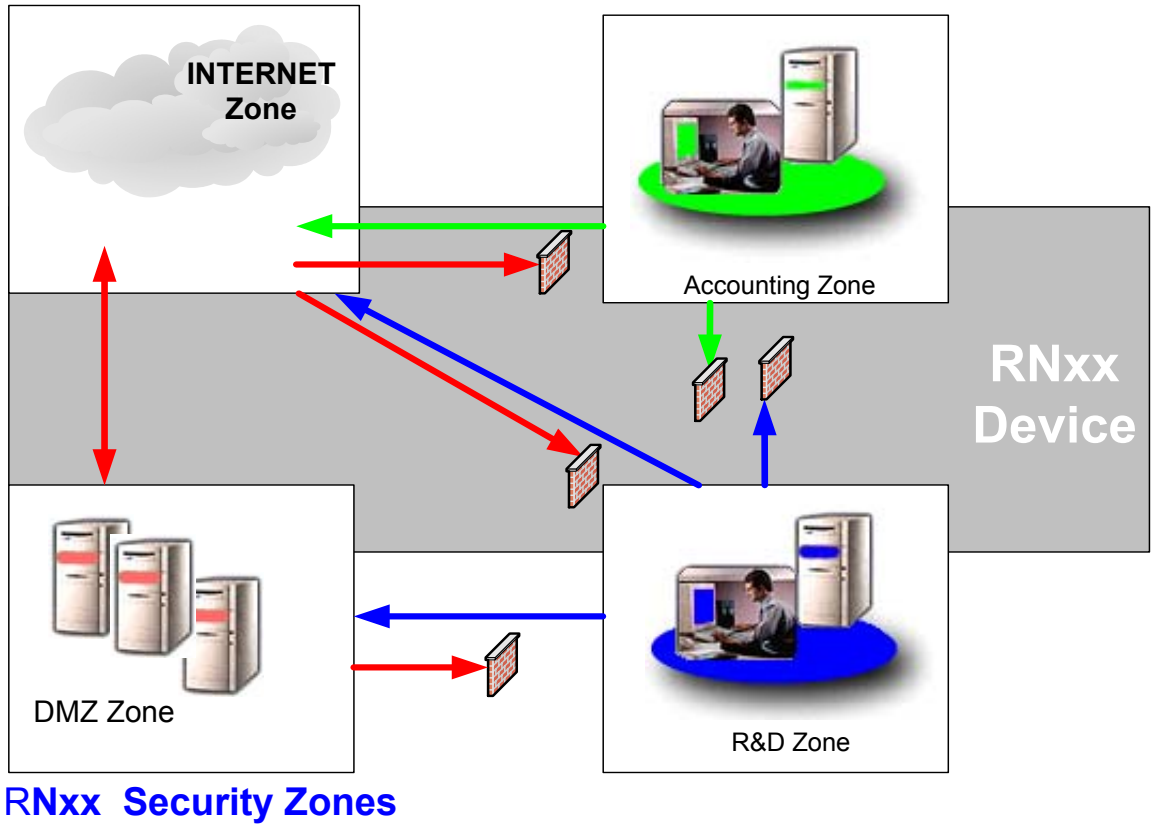


Figure 3 Traffic trough the secure zone of RNxx device



All the network resources in the same zone are considered trustworthy, and the traffic between them, i.e. intra-zone traffic, is switched at layer 2 and is not protected by RN device . Alternately, members of different secure zones are considered untrustworthy, and the traffic between them (inter-zone traffic) traverses the multitude of security-related services within RNxx device .

Figure 4. RNxx device Secure Zones



On **Figure 4** accounting and R&D departments along with Internet and DMZ constitute four distinctive secure zones with individual sets of policies. These policies are applied to the traffic once it crosses the zone boundaries.

1.1 Secure Zones vs. VLANs & Firewall

Figure 5 below represents a typical network topology that is used today to segregate and control traffic from one department to another in a financial institution. For example, all hosts in Investment banking division are on VLAN A, Trading on VLAN B, and Legal on VLAN C.

Figure 5. Conventional VLAN Approach

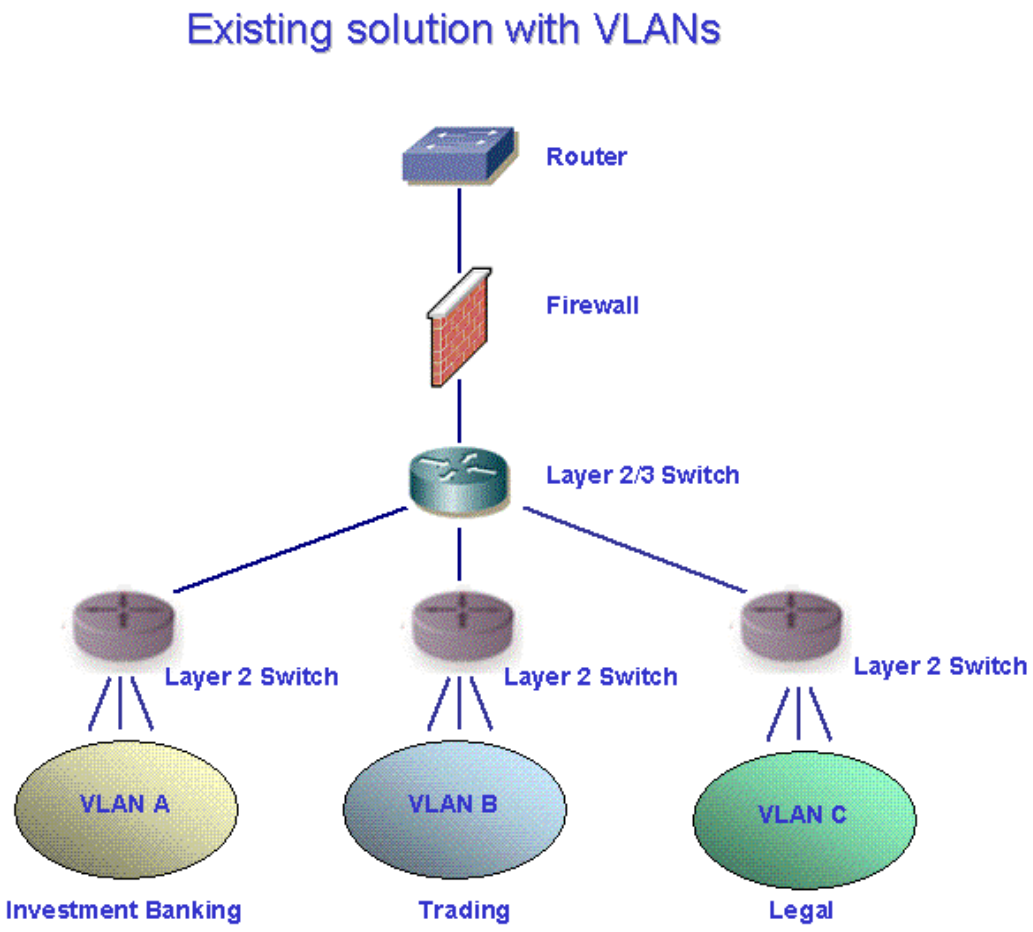


Figure 6 shows a similar topology based on secure zones. As you may notice, in order to achieve the same level of security, a conventional VLAN approach has to include a firewall in each department, which often makes it prohibitively expensive.

Secure zones can even span geographical areas; in these cases network managers can activate RN device bandwidth management and quality of service (QoS) functionality to efficiently utilize low-bandwidth WAN links.

Figure 6. Secure Zones Approach

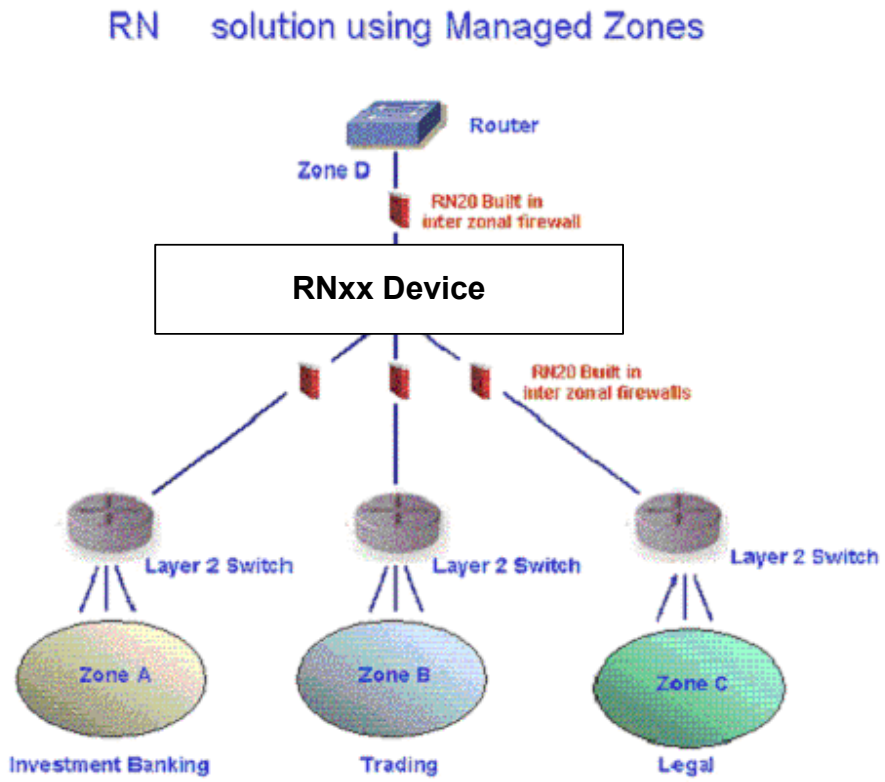


Table 2 summarizes the benefits of deploying secure zones versus conventional VLANs approach.

Table 2. Secure Zones vs. VLANs Benefits

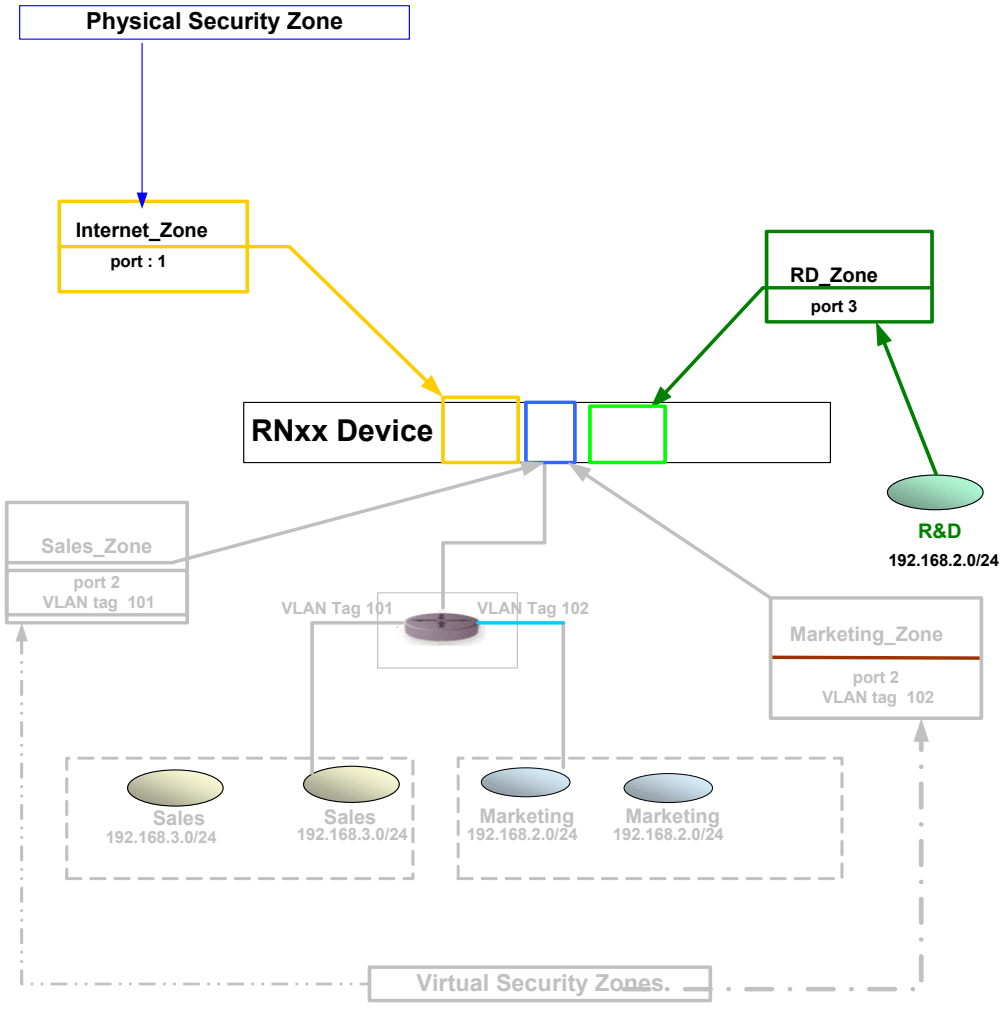
Description	VLANs	Secure Zones
Filtering based on physical port	Yes	Yes
Filtering based on IP header	Yes	Yes
Port based traffic mirroring	Yes	Yes
Filtering based on Layers 4-7	No	Yes
Stateful firewall	No	Yes
DoS prevention	No	Yes
IDS redirection of selective traffic	No	Yes
Load balancing	No	Yes
Bandwidth management	No	Yes
Real-time service monitoring	No	Yes

a. Physical and Virtual Secure Zones

There are two types of Secure Zones that can be configured on RN DEVICE
Physical Zones:

Physical Secure Zones correspond to the physical ports on the front of the box. One or more of these physical ports can be grouped together into a zone to create a Physical Secure Zone. This means that all equipment connected to these ports are in the same Zone. The following picture shows a typical network topology where RN DEVICE is configured with only Physical Secure Zones.

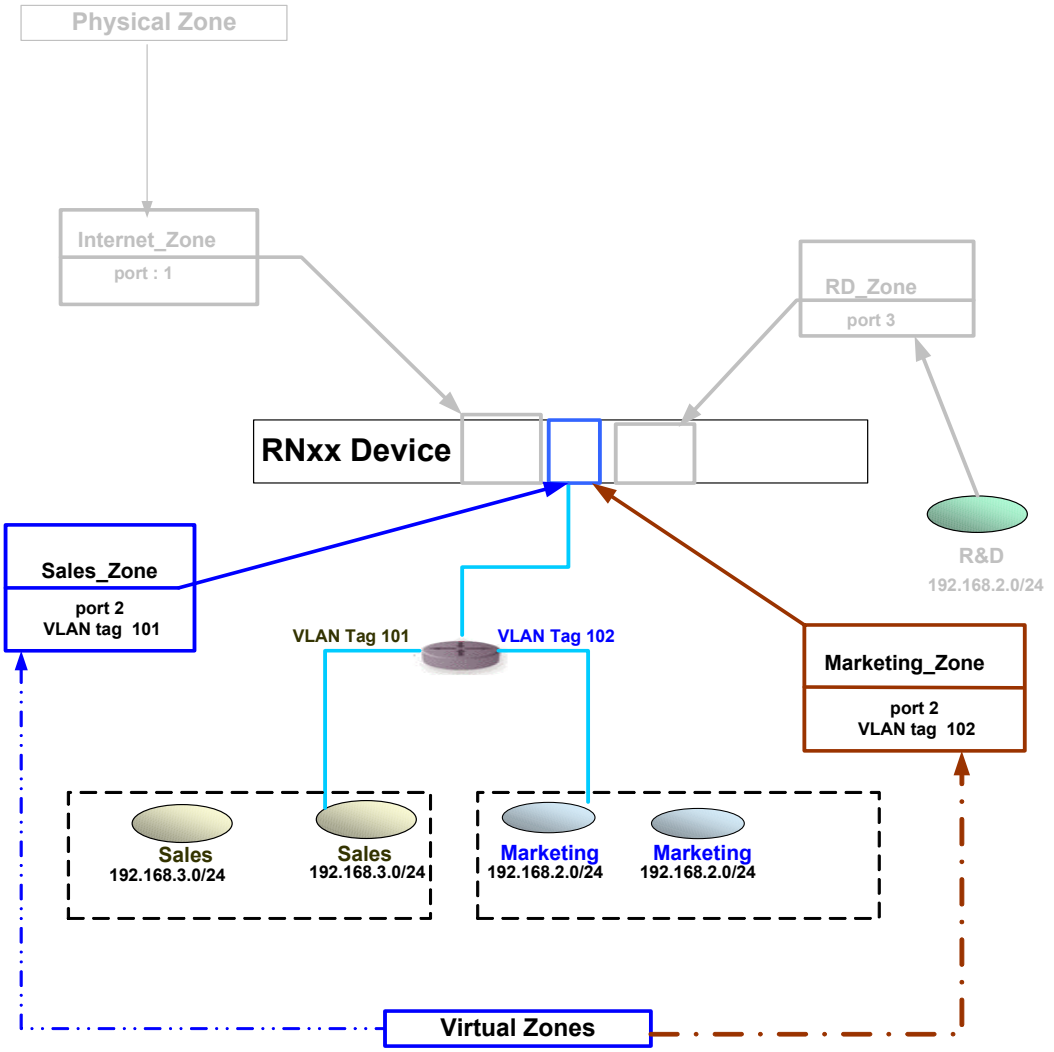
Figure 7 Physical Secure Zone Topology



Caution : Using Physical Zone configuration it is very important for a network administrator to check that there is no connectivity between layer2 switches that belong to a different zones. If there is a connection, then the traffic between zones won't be passing through the RN DEVICE firewall engine, thus no security will be enforced between zones.

Virtual zones:
Virtual Zones are groups of VLANs that are grouped together to be defined as a Virtual Zone. The VLANs can be coming from any of the physical ports. So in this case the Virtual Zone does not directly correspond to any of the physical ports on the front of the box. The picture below shows an example of how to use Virtual Zones to divide up an existing network into zones without having to rewire the network.

Figure 8. Virtual Zones Topology



The Virtual Zone example above shows how to configure multiple existing switches and create multiple Secure Zones where the users are scattered across organization.

2. NAT Concepts

Before we divulge into details of the Network Address Translation (NAT) capabilities supported by RNxx device, we would like to give a short overview of different terms and meanings associated with NAT. For the readers, who would like to enrich their knowledge of the NAT technology, we recommend to refer to RFC2663 "IP Network Address Translator Terminology and Considerations".

2.1 What is NAT?

NAT is a method by which IP addresses are mapped from one address space to another to provide transparent routing to the end hosts. Despite a plethora of variations in mapping techniques, all NAT devices adhere to the following rules:

- Transparent address assignment
- Transparent routing through translation
- ICMP error packet payload translation

2.2 Transparent Address Assignment

NAT assigns addresses in internal/private space to addresses in external/public space and vice versa to provide transparent routing between address domains. Address assignment is done at the start of the session and might be either static or dynamic.

2.2.1 Static Assignment

During static assignment there is a one-to-one mapping between addresses in the private space and public space for the lifetime of the NAT operation. With static assignment there is no address administration within NAT.

2.2.2 Dynamic Assignment

In the case of dynamic assignment, external addresses are assigned to private addresses based on usage requirements and traffic flows determined by NAT. When the last session using dynamic assignment is completed, public addresses are freed and may be re-used by subsequent sessions.

2.2.3 Transparent Routing

NAT device is deployed at the border between address spaces and translates IP addresses in the packet headers so that when the packet leaves one domain and enters another, it can be properly routed. NAT is also careful not to propagate the routing information from one domain to another, where this information is deemed inappropriate.

2.2.4 ICMP Error Packet Translation

All ICMP error messages with the exception of Redirect message type have to be modified to make NAT truly transparent. This modification touches not only the IP header of the error message, but also the original IP packet (or its part) embedded in the ICMP error message.

2.3 Variations of NAT

There are many variations in NAT that find their niche in the enterprise networks. The NAT flavors provided herein capture the essence of address translation, but are by no means exhaustive.

2.3.1 Traditional NAT

Traditional or outbound NAT allows hosts in the private space to transparently access on external network. With traditional NAT the sessions are uni-directional, initiated from the private network. IP addresses of the hosts on external network are unique and valid both on external and internal networks. However, internal addresses are unique only within a private space and may not be valid externally. In other words, NAT would not advertise internal addresses to the external domain, but external addresses may be advertised on the private network. Within traditional NAT, one should differentiate between basic NAT and NAPT (Network Address Port Translation).

2.3.2 Basic NAT

Basic NAT allocates a block of external addresses that are assigned to the hosts on a private network when they originate sessions to the external entities. For the packets outbound from the private domain, the source IP and related fields such as IP, TCP, UDP and ICMP header checksums are translated. For the inbound packets, the destination IP address and the checksums listed above are translated.

2.3.3 NAPT

NAPT extends the concept of address translation by including translation of transport identifiers as well (TCP and UDP port numbers, ICMP query identifiers). This allows a set of internal hosts to share a single external address. It should be noted that NAPT can be combined with basic NAT to allow a pool of external addresses to be used in conjunction with port translation.
For outbound packets, NAPT would translate the source IP, source port and related IP and transport header checksums. For inbound traffic, destination IP address, port and IP and transport header checksums will be translated.

2.3.4 Bi-directional NAT

With bi-directional or two-way NAT sessions can be initiated from external as well as internal domains. Internal and addresses are bound to globally unique addresses, statically or dynamically when connection are established in either direction. The name space between the hosts in internal and external domains is assumed to be end-to-end unique.
In a typical bi-directional NAT application hosts in external address space access private addresses by using DNS for address resolution. A DNS application-level gateway has to be employed in conjunction with bi-directional NAT to facilitate name to address mapping.
The address space requirements for traditional NAT are applicable here.

2.3.5 Twice NAT

Twice NAT is a variation of NAT that translates both source and destination IP addresses when the packet crosses the address boundary. This NAT flavor is necessary when there is a collision between internal and external address spaces. The most common application for the twice NAT is when a site numbers its internal resources using public addresses that were officially assigned to a different enterprise.

2.4 RNxx device NAT Terminology

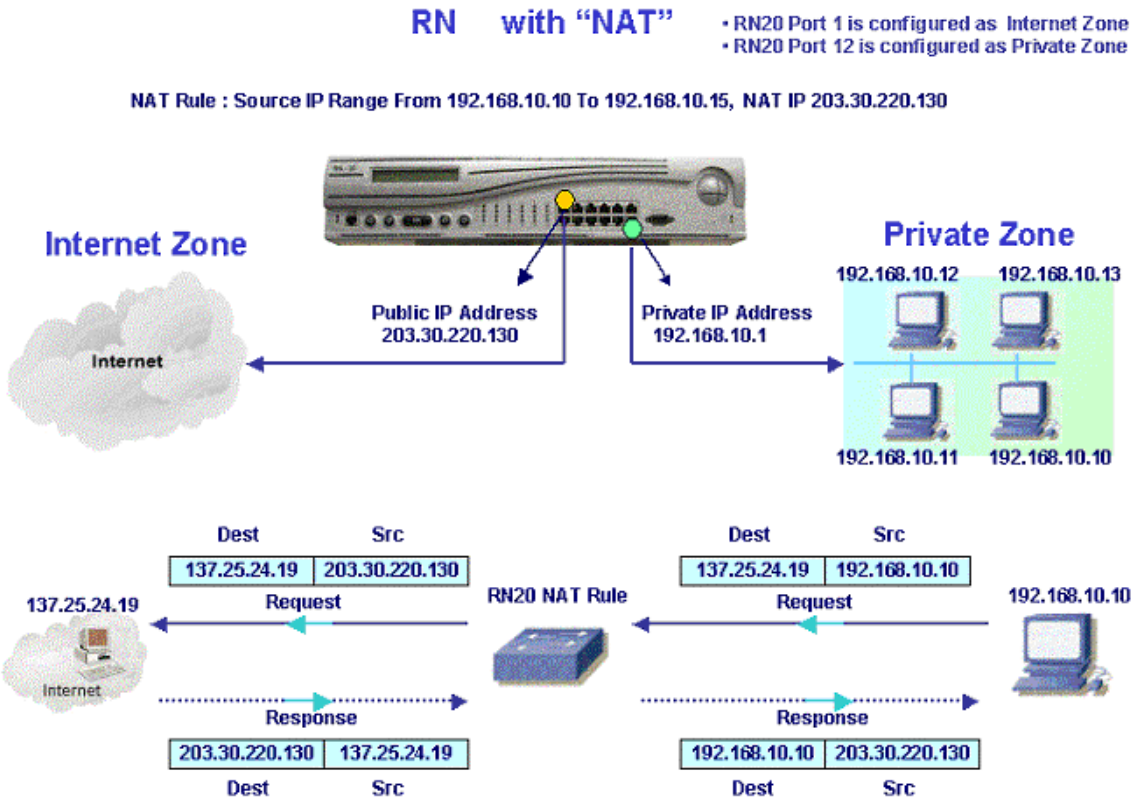
NAT functionality implemented in RNxx device strictly follows the technology guidelines outlined above, but the terminology used in RNxx device NAT configuration options is somewhat different and needs explanation.
RN supports the following NAT:

- NAT
- One-to-One Full NAT
- One-to-One Half NAT
- No NAT

2.4.1 NAT

NAT option is analogous to traditional or outbound NAT described in the previous section. All sessions are initiated only from the private address space to the public space, and not vice versa. This option might utilize either static or dynamic address assignment and also add port translation (NAPT), which in RNxx device parlance is called NAT Overload. The diagram below illustrates a simple NAT scenario.

Figure 9. NAT Option



In this scenario a simple NAT rule is configured on RNxx device for the secure zone that is used as a private (LAN) network. The rule defines a range of source addresses, e.g. 192.168.10.10 – 192.168.10.15, and a single outbound NAT address 203.30.220.130, which happens to be the address of the interface to the secure zone that is used to connect to the ISP(Internet). All request emanated from the hosts in this range will be modified by RNxx device, i.e. their source IP addresses will be substituted by the NAT address, which is a valid routable address in the public domain.

It should be noted that since a single NAT address is used for outbound traffic, port translation has to be invoked to maintain sessions from different hosts to the same destination.

All address and port mappings are stored by RNxx device in the NAT table, which is used to correctly forward the response packets back to the session originator.

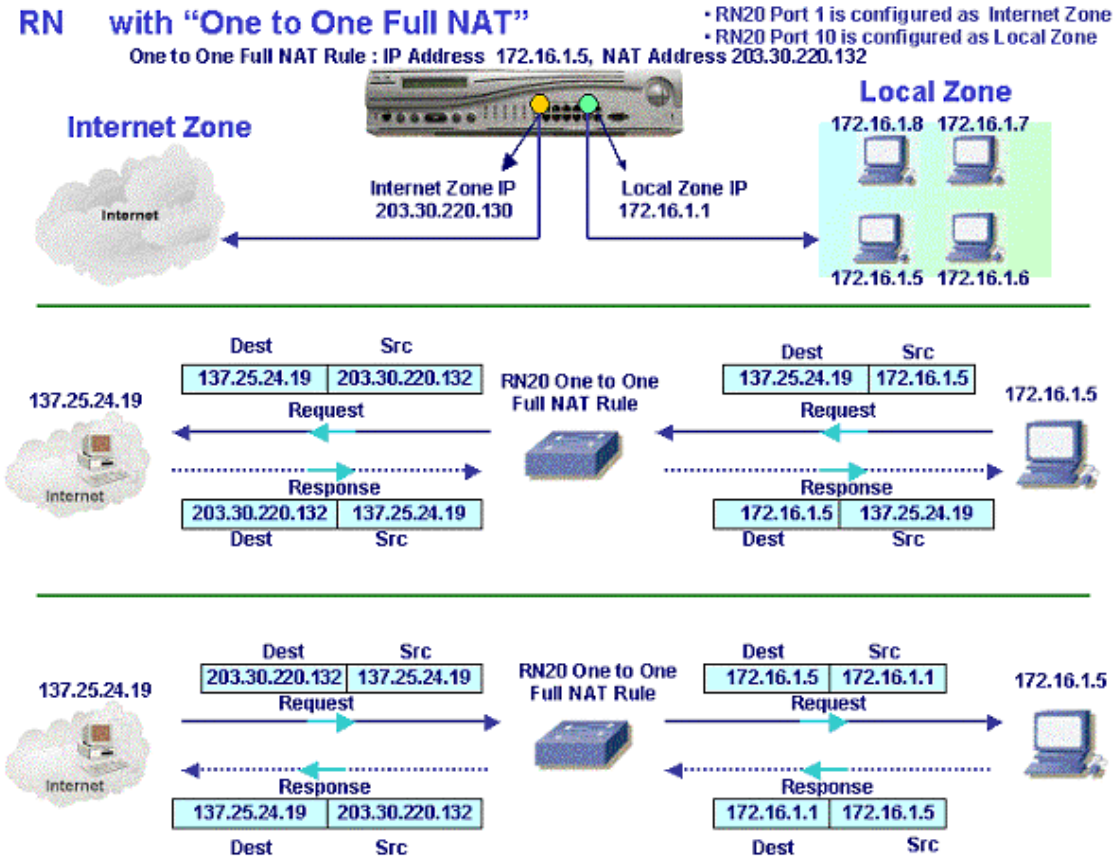
2.4.2 One-to-One Full NAT

One-to-One Full NAT option is essentially a mixture of bi-directional and twice NAT described above. This option enables the hosts in both the private and the public domains to initiate sessions. When the session is initiated from the private host, One-to-One Full NAT behaves exactly as a traditional NAT with one-to-one mapping of private and public addresses. In other words, for each private address there exists a unique public address.

When the session is initiated from the public domain, One-to-One Full NAT is a twice NAT in that both the source and destination IP addresses are translated.

As shown on Figure 10, a host in the secure zone with the name Local is configured with a private address. The Local zone interface IP is 172.16.1.1. Internet connectivity is available through the secure zone **Internet** with its interface IP 203.30.220.130.

Figure 10. One-to-One Full NAT Option

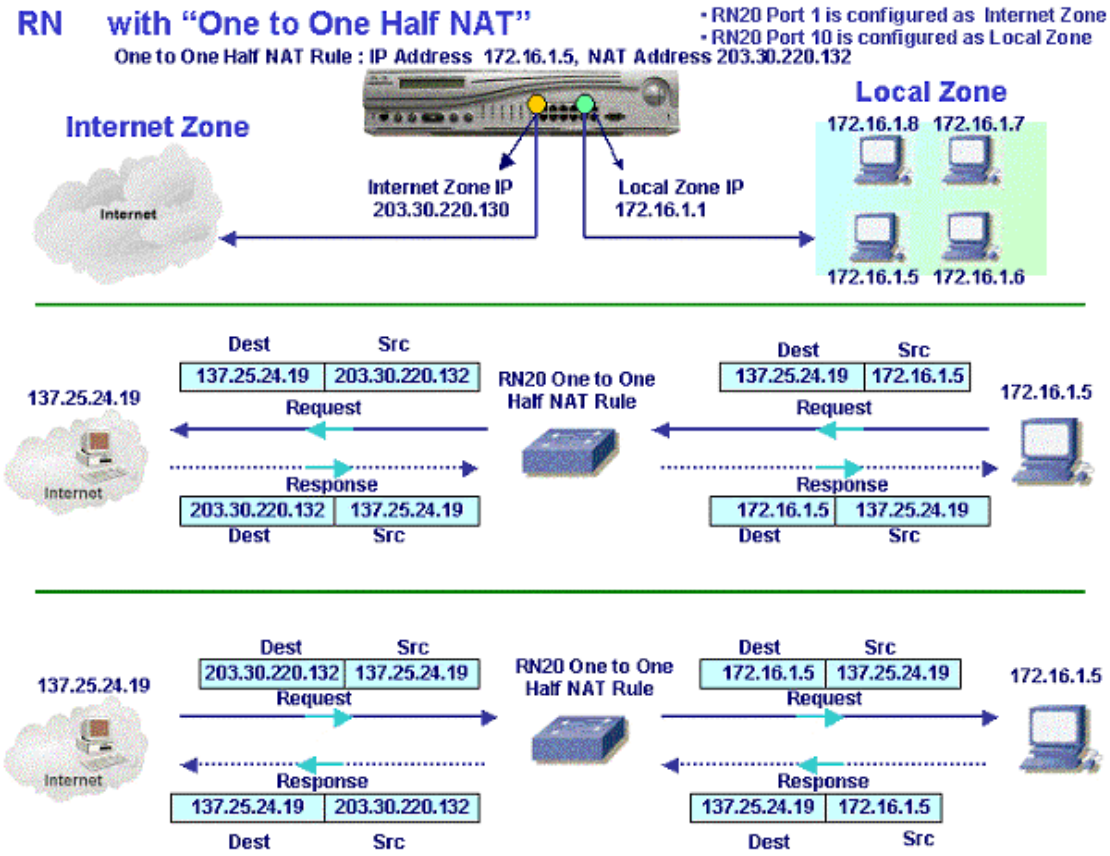


The local host 172.16.1.5 initiates a session with an Internet destination 137.2.24.19. A One-to-One Full NAT rule is created for the secure zone Local, according to which the source address 172.16.1.5 is substituted with 203.30.220.132. When the Internet host 137.25.24.19 receives a request, it responds back to 203.30.220.132, and RNxx device restores the original 172.16.1.5 as the destination address.
When a session is initiated from a public domain, i.e. internet host 137.25.24.19, destined to the local host, the source address in the request packet is resolved (via DNS) to the public address 203.30.220.132 associated with the private address 172.16.1.5. When the packet traverses RNxx device and the One-to-One Full NAT rule is applied, RNxx device substitutes both the source and destination addresses to 172.16.1.1 and 172.16.1.5 respectively, so that the packet looks as if being originated locally. Reply follows the same path, and original addresses are restored.

2.4.3 One-to-One Half NAT

A One-to-One Half NAT option implements the standard bi-directional NAT functionality. It allows sessions to be initiated in both directions and differs from the full NAT option only in handling the traffic from a public space to the private behind RNxx device. As you may see on the diagram below, when the session is originated from the Internet host, its source address is left intact, and only the destination address is translated from the public space to the private address.

Figure 11. One-to-One Half NAT option



Caution : 1) The NAT Address used in either One to One Full or One to One Half NAT should be unique. Any RNxx device interface IP Address can't be used for this.

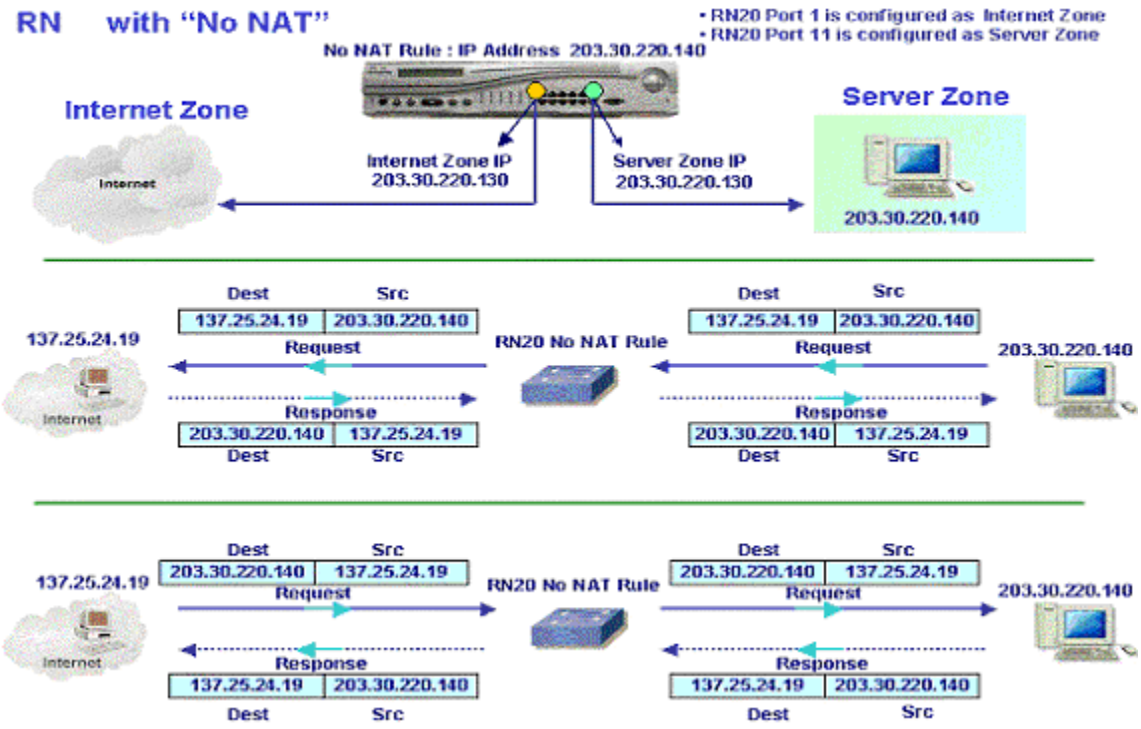
2) In case of One to One Half NAT, the local host behind RNxx device has to be configured with default GW pointing to its RNxx device interface. In the above example, the local host 172.16.1.5 should have default GW configured as it's Local zone interface, 172.16.1.1
In case of One to One Full NAT, configuring local host's default GW to its RNxx device interface is NOT mandatory.

2.4.4 No NAT

The No NAT option, if selected, simply disables NAT functionality. No address translation takes place; both internal and external addresses are unique and exposed to all domains, so network managers have to exhibit extra caution when defining these firewall rules.

Caution : Using a public address for a server behind RNxx device firewall involves security risks, if proper firewall rules are not in place

Figure 12. No NAT Option



Tip: This No NAT option is mostly suitable for VPN Server deployments, which tend to have certain incompatibilities when accessed through NAT. You can deploy VPN Server behind RNxx device firewall with public IP address without any NAT conflicts, again with strict firewall access rules.

3. Configuring RNxx device

One of the benefits of RNxx device is its simple, intuitive, albeit rich browser-based management interface. You can configure the most complex functions with a simple click of a mouse. The following screen shot explain the layout and main elements of RNxx device configuration interface.

Figure 13 RNxx device Management Interface main elements

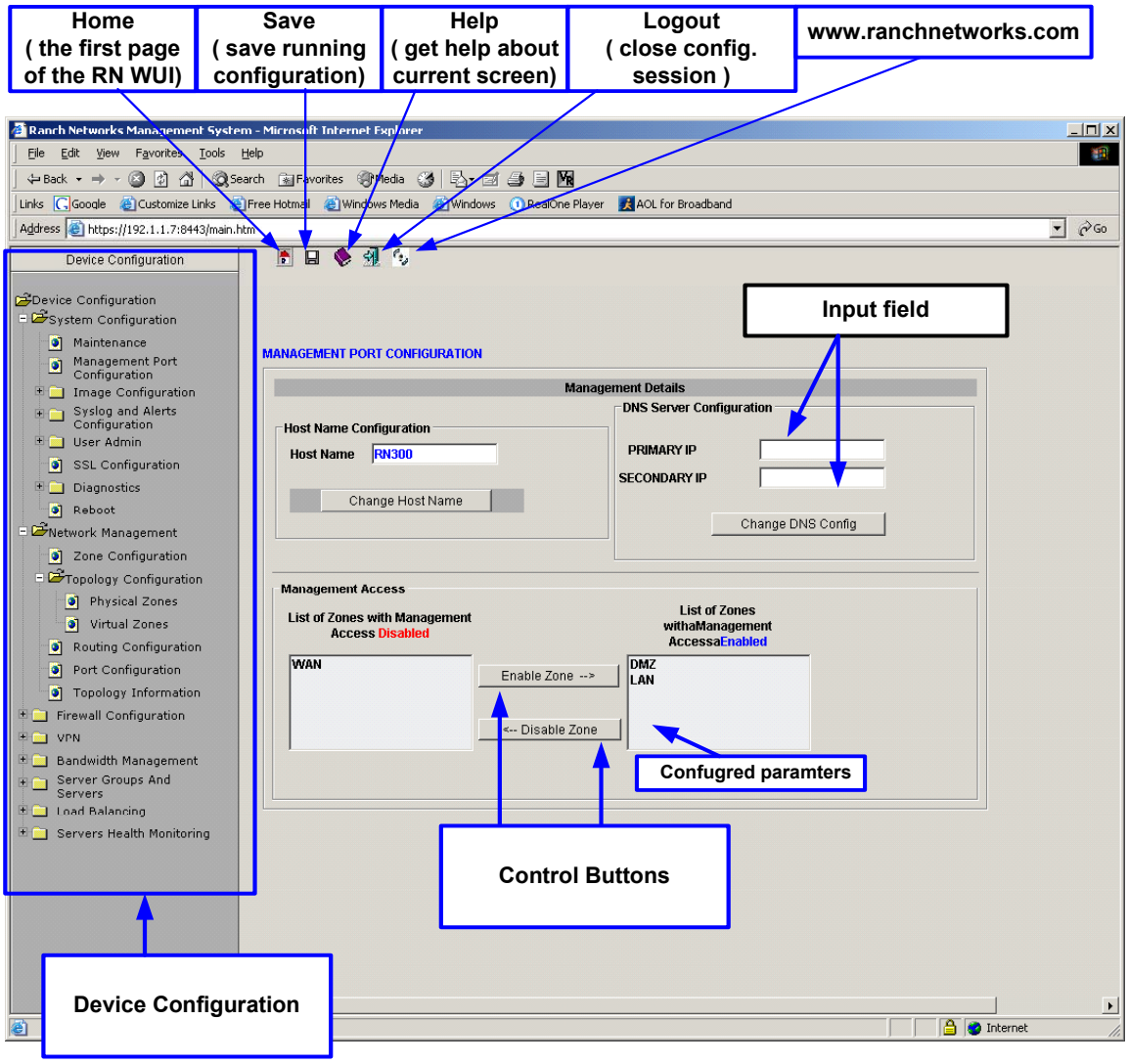
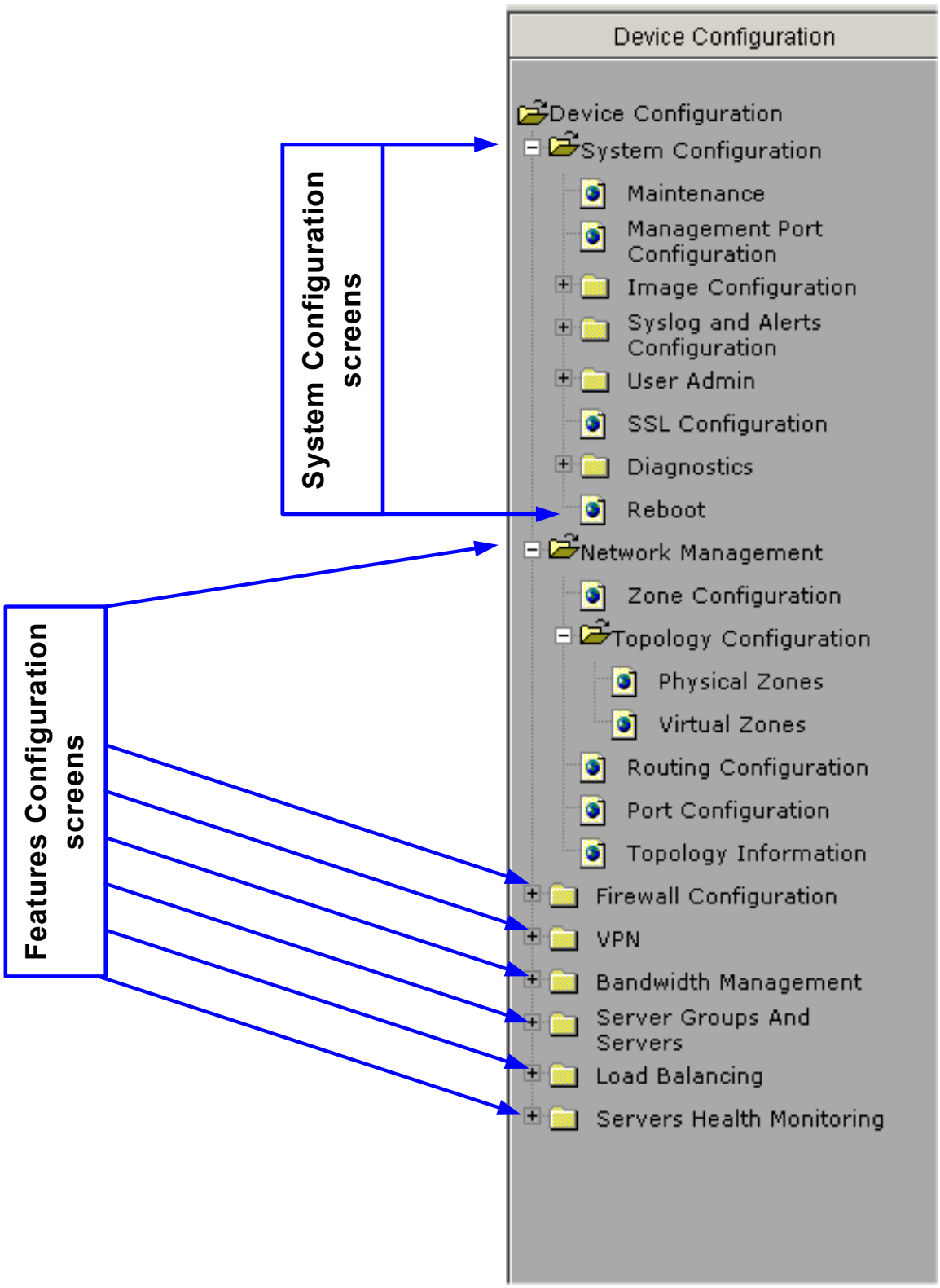


Figure 14 RNxx device Management Interface main elements (cont.)



3.1 Product Activation

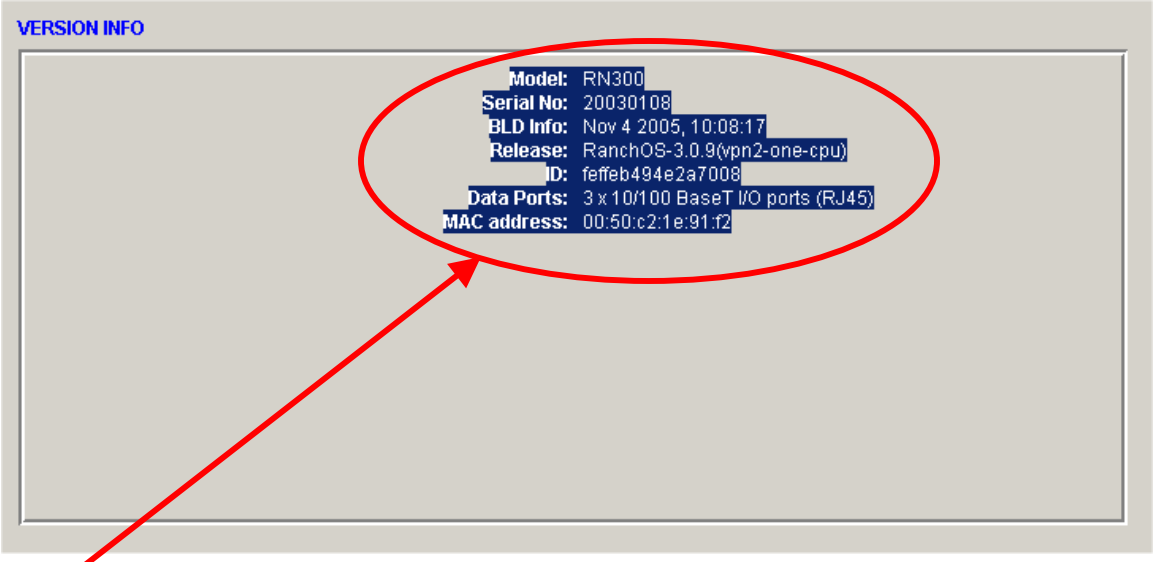
When the customer receives an RNxx device from the Ranch Networks (or the distributor of Ranch Networks), the activation key is already preset and the device is fully functional. ***The user doesn't need to do anything with the activation key in this case***. Also , to restore the initial software image (that came with RNxx device), the Product Activation Key ***is not required*** .

When the user installs ***a new firmware image***, the user has to request a valid activation key from Ranch Networks (or the distributor of Ranch Networks) to activate the product.

To request the product activation key:

Step 1. Gather the information about the device

Go to **System Configuration->Image Configuration->Version Info**



Select the product information , copy and paste it to the email or the text file

Warning !!!

The information screen in the RanchOs 3.0.9 and lower
would not show the **ID** field. In this case the only way to see the **ID** of the
RN device is to load the new software and reboot it. After the reboot the ID
value could be found on the software activation key screen . It is strongly recommended
in this case to contact the technical support team of Ranch Networks first , setup the
time, the support representative will be standing by and will generate the key for You as
soon as the ID field will be supplied over the phone or email.

The reason for this is that the RN device will not bring up any of its services unless the
new software is activated. So in other words the there would not be any traffic through
the RN device at this time.

Recommendations for **RN 5/20/40/41** models :
The software upgrade should be performed first on the backup software image
(A or B)

Step 2 . Send the information to Ranch Networks

The direct request for the Product Activation Key could be sent to :
support@ranchnetworks.com
with the subject - **Image Upgrade** and the following information :

Model number
Serial number
BLD Info
Release
ID
Data Ports
MAC Address
Feature List

Step 3. Getting the new image

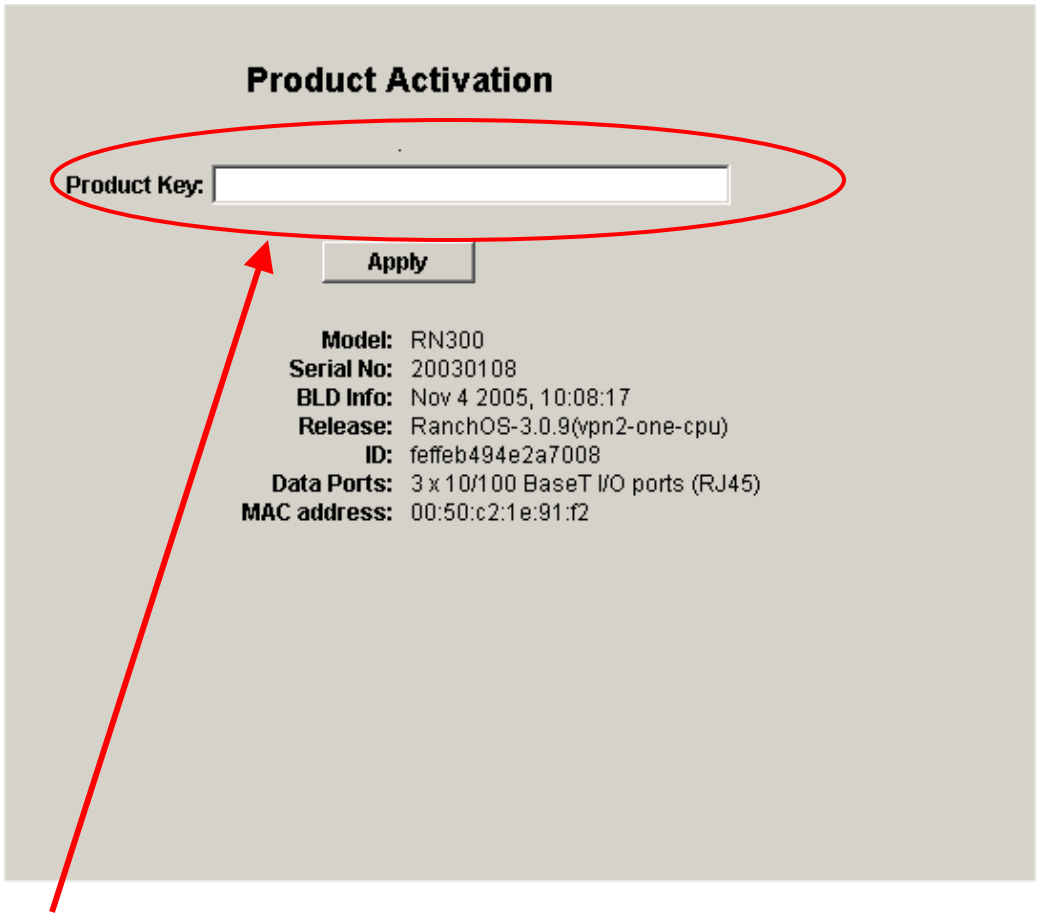
Download the new image using the instruction from the Ranch Networks support team. (You will find the all necessarily information in the email You received as a respond for You request)

Download the new image to the RNxx device (the **Image Config** of this manual for more information about steps and procedures). Reboot the RNxx device.

Step 4

After the first reboot with the new image the user will be prompted with the following screen, where the user has to type in the activation key in order to activate the new firmware and get to the RNxx device configuration GUI.

Figure 15. RNxx device Product Activation Screen



Enter the product activation key .
(You will find the product activation key in the email You received as a respond for You request).
Press the **Apply** button.

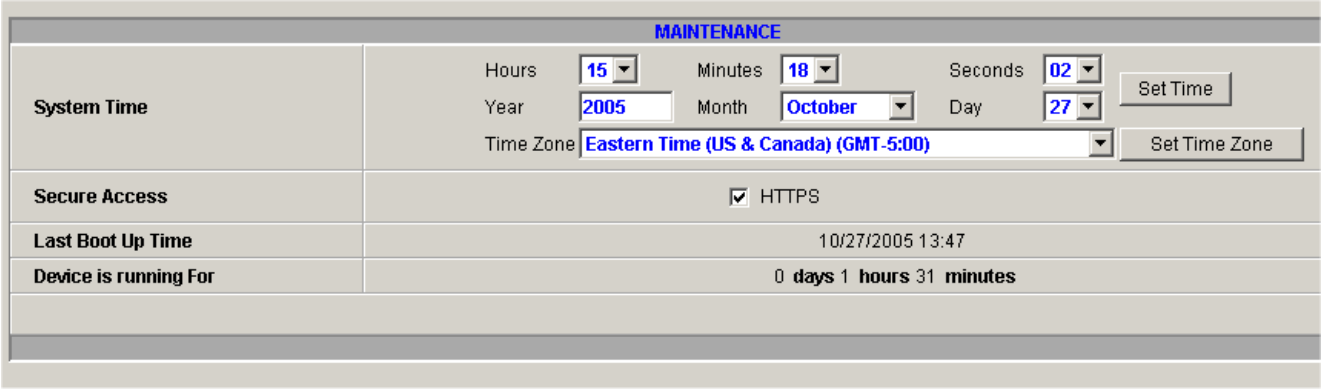
3.2 System Configuration

System configuration screen allows you to set basic properties of the unit, such as systems time, management port, select system image and configuration, define users, SSL certificates, etc. The Systems configuration screen has the following tabs:

Maintenance, Mgmt Port Config, Image Config, Syslog Config, User Admin, SSL Config, Diagnostics , Reboot.

3.3 Maintenance

Figure 16. System Configuration -> Maintenance



The Maintenance tab contains the following configuration parameters:

System Time: Select the appropriate time zone and click 'Set Time Zone' to change the time accordingly and to save the zone. If the time shown is different than your local time, select the appropriate time by dragging down hours , minutes, seconds, month, day and year. Click on 'Set Time' to save.

> **Caution :** If you configure future time/date values of current RN settings, browser will log you out. You will have to re login. This will not affect any services provided by RN

Secure Access : When HTTPS option is checked, only secure management session can be established with the unit (for example, https://192.168.1.1), your browser has to support SSL and contain a valid client and server certificates.

If the HTTPS option is left unchecked, both HTTP and HTTPS sessions will succeed.

Front Panel Access : When checked, all read / modify maintenance options on the front panel LCD are enabled. If unchecked, front panel Keyboard /LCD is in read-only mode. (**only applicable to RN20 device model**)

> **Caution :** Once RN is configured in the network, disabling Front Panel access provides added physical security if it is in remote location

Last Boot Up Time: Gives the date and time of last reboot.

Device is running for: This counter shows days, hours and minutes since the last system boot. This field should be considered as the RNxx device uptime.

3.4 Management Port Config

3.4.1 Management Port Config for RN20/40/41

IP address, subnet mask and default gateway for the management interface can be configured in this mode. Once these parameters are set or modified, click on 'Change Mgmt IP settings' to save.

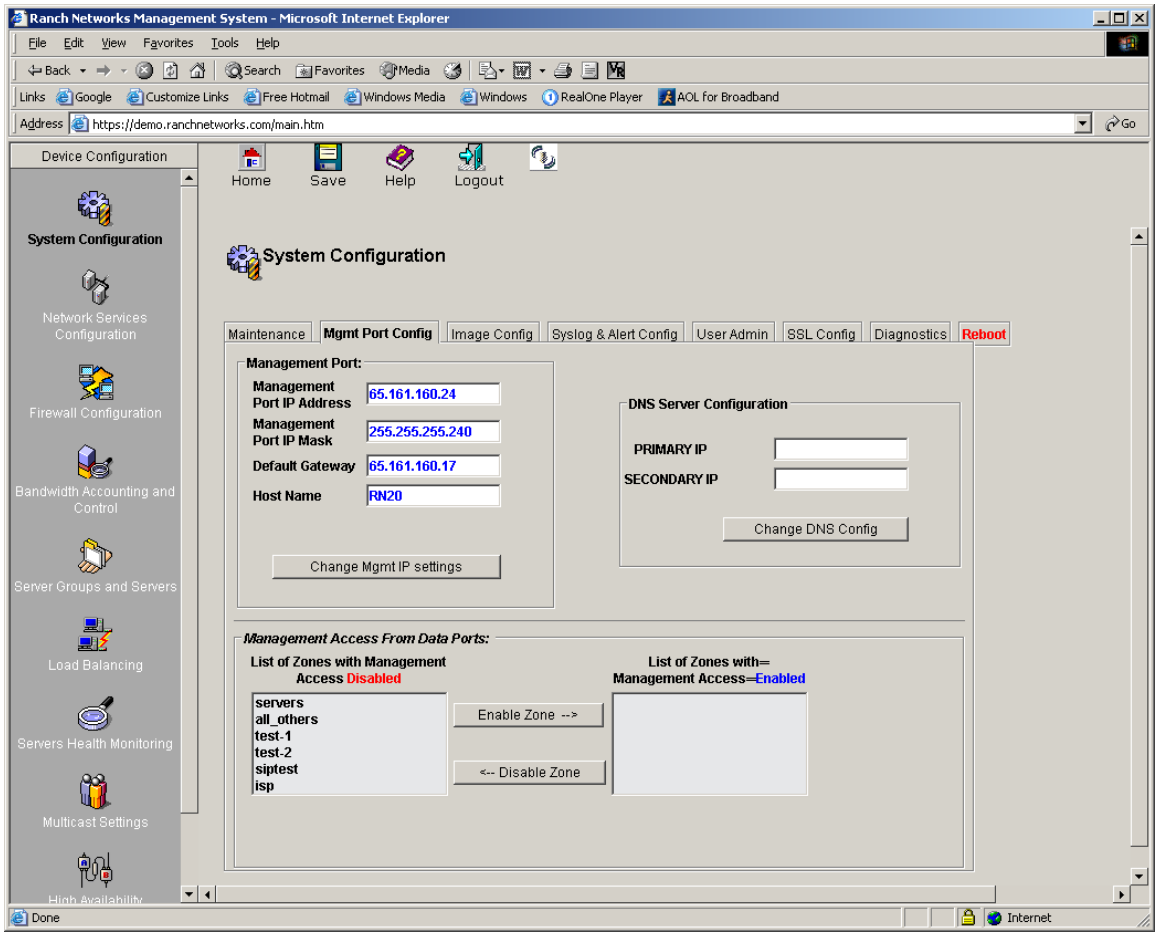
> **Caution :** Changing the IP address of the RN management interface will take effect immediately and will result in loosing the existing connection to the device. To connect again, use the newly assigned IP address.

By default your management workstation and RN management interface have to be connected to the same subnet. If this is not the case, and your workstation is on a different subnet, necessary routes have to be configured to establish connectivity. Refer to "RN Installation Guide" to correctly connect you management station. An example of the management infrastructure for RN is given on Figure 18.
In addition to Management Port, the network administrator can access the RN configuration through one of the data ports. In order to do that the data ports have to be configured and assigned to one of the Secure Zones. There are two steps required to enable access to the configuration GUI:

1. Enable access to the Management GUI by selecting a zone from the list of disabled zone and moving the zone to the list of enabled zones.
2. Set up a firewall rule for the enabled zone to allow access to Zone's IP address and destination ports 8080, 8443.

To access the Management GUI the Zone's IP address has to be used with the port number 8080(HTTP) or 8443 (HTTPS), for example if the zone was configured with IP address 192.168.1.1 then to access the Management GUI the following URL has to be used: **http://192.168.1.1:8080** or **https://192.168.1.1:8443**

Figure 17. System Configuration -> Mgmt Port Config

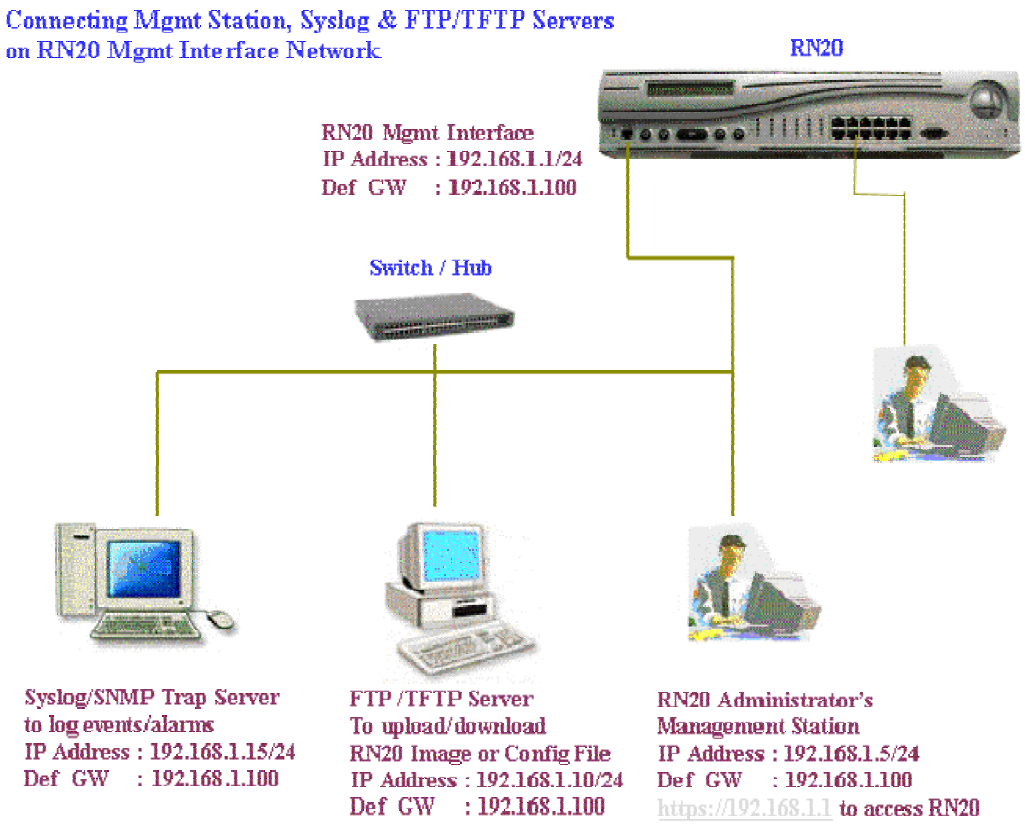


Caution : The management interface of RN is not protected by the firewall and should be used only for the local administration , only data ports should be used for the remote administration of RN. When using the data ports for the remote administration the access should be governed by the appropriate firewall rules .

Management Port
used only for the local administration

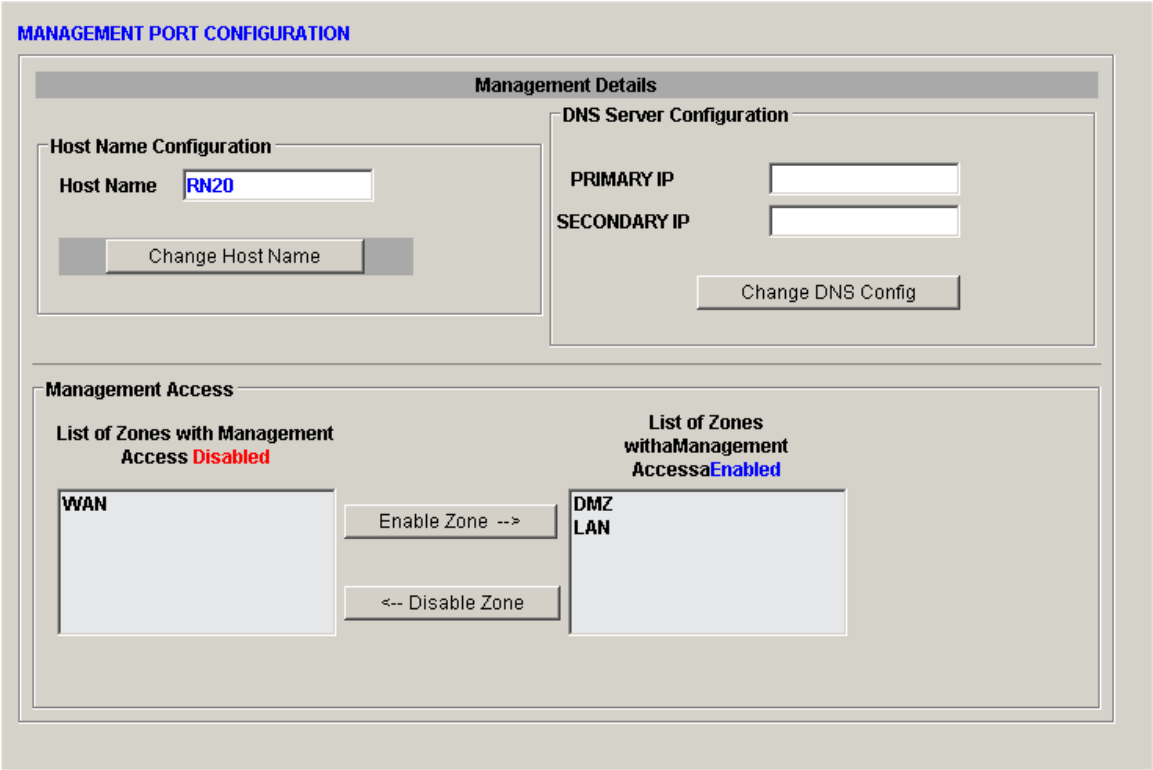
Data Ports
used for the local and remote administration

Figure 18. Management Infrastructure



3.4.2 Management Access configuration for RN300.

Figure 19 System Configuration->Management Port Configuration (RN300)



The network administrator can access the RN (RN300 model) configuration through one of the data ports. In order to do that the data ports have to be configured and assigned to one of the Secure Zones. There are two steps required to enable access to the configuration GUI:

3. Enable access to the Management GUI by selecting a zone from the list of disabled zone and moving the zone to the list of enabled zones.
4. Set up a firewall rule for the enabled zone to allow access to Zone's IP address and destination ports 8080, 8443.

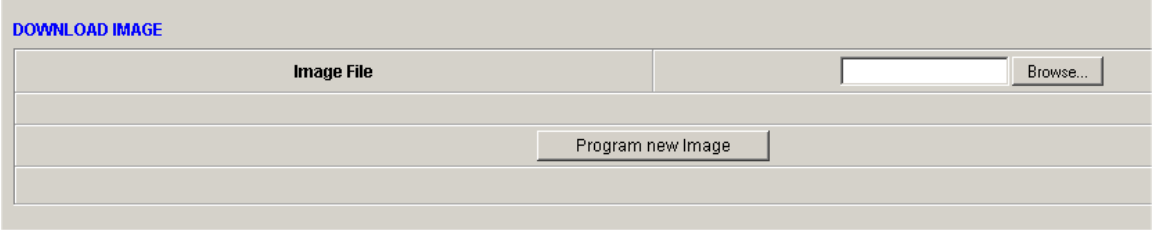
To access the Management GUI the Zone's IP address has to be used with the port number 8080(HTTP) or 8443 (HTTPS), for example if the zone was configured with IP address 192.168.1.1 then to access the Management GUI the following URL has to be used: **http://192.168.1.1:8080** or **https://192.168.1.1:8443**

3.5 Image Config

Image is an operating system kernel, which is the software core of the unit. In case of update or restore procedures the RN image could be downloaded to RN device through HTTP .

3.5.1 Downloading Image to RN device

Figure 20 System Configuration->Image Configuration->Download Image



To load the new software image on RN device:

- Copy the new image on the workstation that is used for the RN management;
- Go to **System Configuration->Image Configuration->Download Image**;
- Press the **Browse** button and navigate to the file that consists of the new image;
- Press the **Program new Image** button.
- Wait until the message that confirms download will appear at bottom of the screen;
- Go to **System Configuration->Reboot** and reboot the RN device

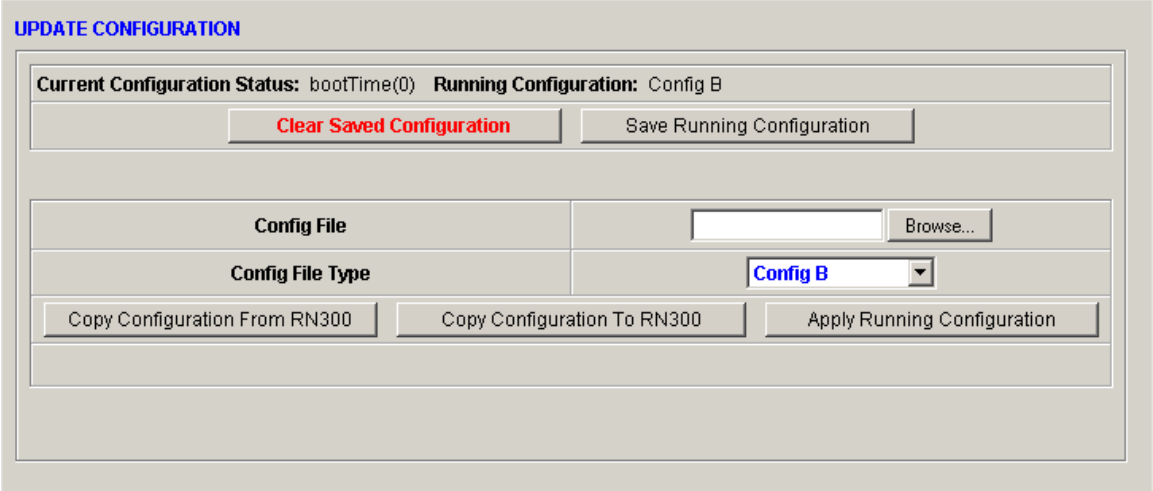
Caution : Any existing image file will be overwritten if you download new image file. RN has to be rebooted with new image to take effect.

3.5.2 Update Configuration

Configuration file contains a set of rules or instructions that define RNxx device functionality. For example, entries for security zones, firewall, and NAT rules are part of the configuration file. RNxx device supports two configuration files ConfigA & ConfigB that are stored on the device at any given time. Any one of the config files can be assigned as default, so RNxx device will continue to come up with the same configuration every time it is rebooted.

Configuration files can be downloaded on to RNxx device or uploaded from RNxx device via FTP, which is activated through you browser.. A newly installed unit has to be configured from scratch in order to create a valid configuration file.

Figure 21. System Configuration->Image Config->Update Configuration



Save Running Configuration :
If the running configuration is modified, e.g. any entries are added, deleted or changed, these modifications take effect immediately, but will be lost if the unit is rebooted. In order to preserve the changes across reboots, you have to save the running configuration by pressing the 'Save Running Configuration' pushbutton.

Clear Saved Configuration:
If it is required to start a unit with a clean slate, mostly in cases of grave misconfiguration, it can be achieved by clicking on the 'Clear Saved Configuration'. After reboot RN will come up clean and has to be configured from scratch.

Copy Configuration from RN:
When the configuration of RN device is settled (all changes are accepted and the running configuration was saved) it is strongly recommended to save the configuration file on the external storage.
Press **Browse** button .
Chose the location and name for the configuration file .
Press **Copy Configuration from RNxx** button.

Copy Configuration to RN:
This procedure is similar to **Copy Configuration from RN** procedure , but in this case the configuration file will be downloaded to RN device . The procedure is intended for the recovery or deployment purposes.
After the configuration file is downloaded , RN should be rebooted with the type of the configuration (that was restored) as a default configuration type.

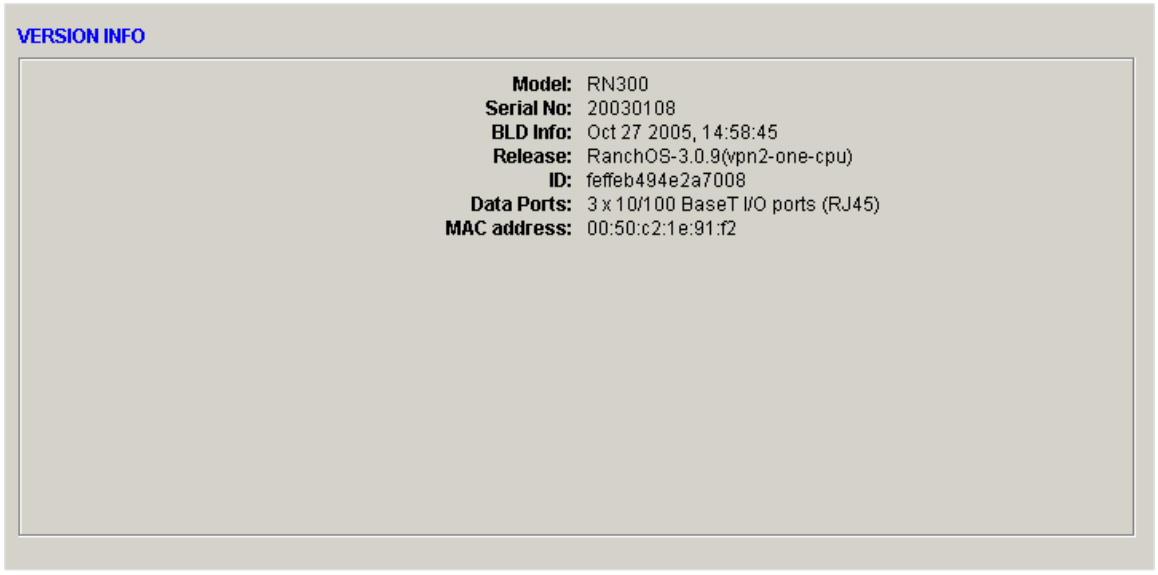
Apply Running Configuration :
By pressing this button the downloaded configuration will be applied on the fly , without reboot.

Caution : Any existing config file will be overwritten if you download new config file of same type. RN have to be rebooted with new config file to take effect.

3.5.3 Version Info

This screen has the pure informational purpose. It shows the model , software and the serial number information.

Figure 22 System Configuration->Image Config ->Version Info

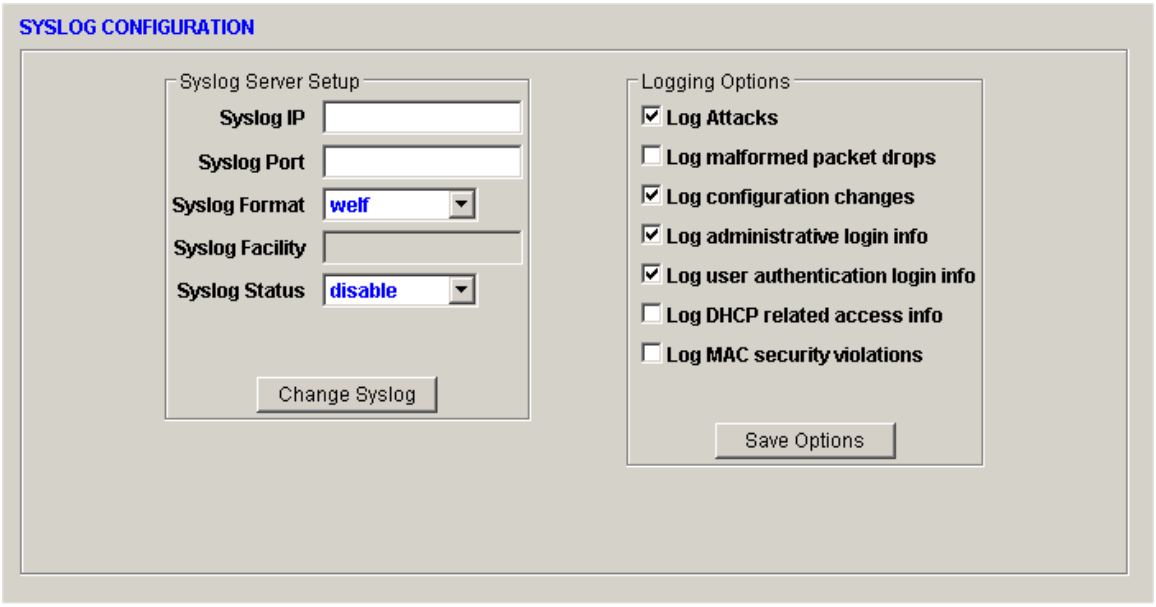


3.6 Syslog and alerts configuration .

Syslog server is part of RNxx device management infrastructure and is used to receive events in the form of log and email messages from the unit(s).

3.6.1 Syslog messaging configuration.

Figure 23. System Configuration -> Syslog Config



RNxx device supports both Unix and WELF style logging. As shown on the screen above, syslog related properties are displayed by selecting a Syslog Config tab.
Parameters such are Syslog IP , Syslog port (default tcp/514), Syslog Format (unix or welf), Syslog Facility(in case of unix format), and Syslog Status (enable/disable) can be configured.
By default the following Log messages will be send to the Syslog server (if Syslog is enabled)

- All RNxx device configuration changes
- All Administrator logins attempts
- All User authentication logins/logouts attempts

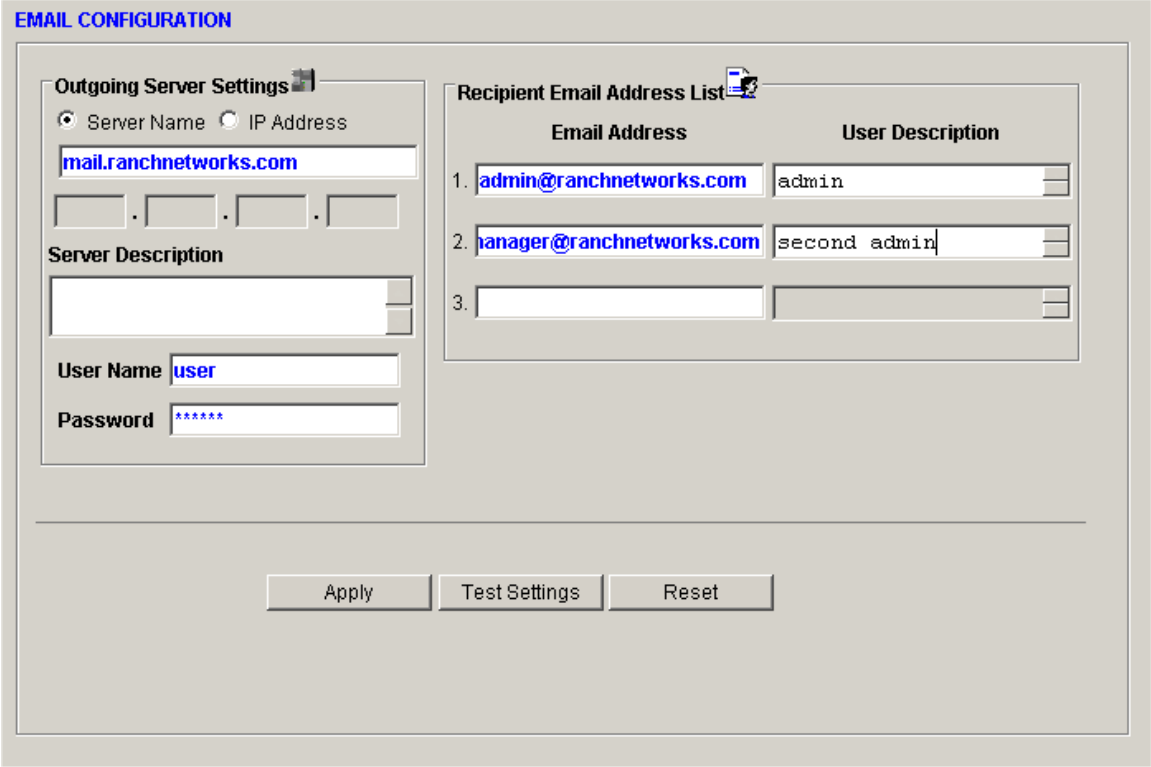
The network administrator can enable the following Log messages that are not enabled by default:

- All malformed Packets
- All DHCP related messages
- All MAC security violations, if MAC security is configured.

To finish Syslog messages configuration click on "Save Options" button.

3.6.2 Email messaging configuration

Figure 24 System Config-> Syslog->Email Config

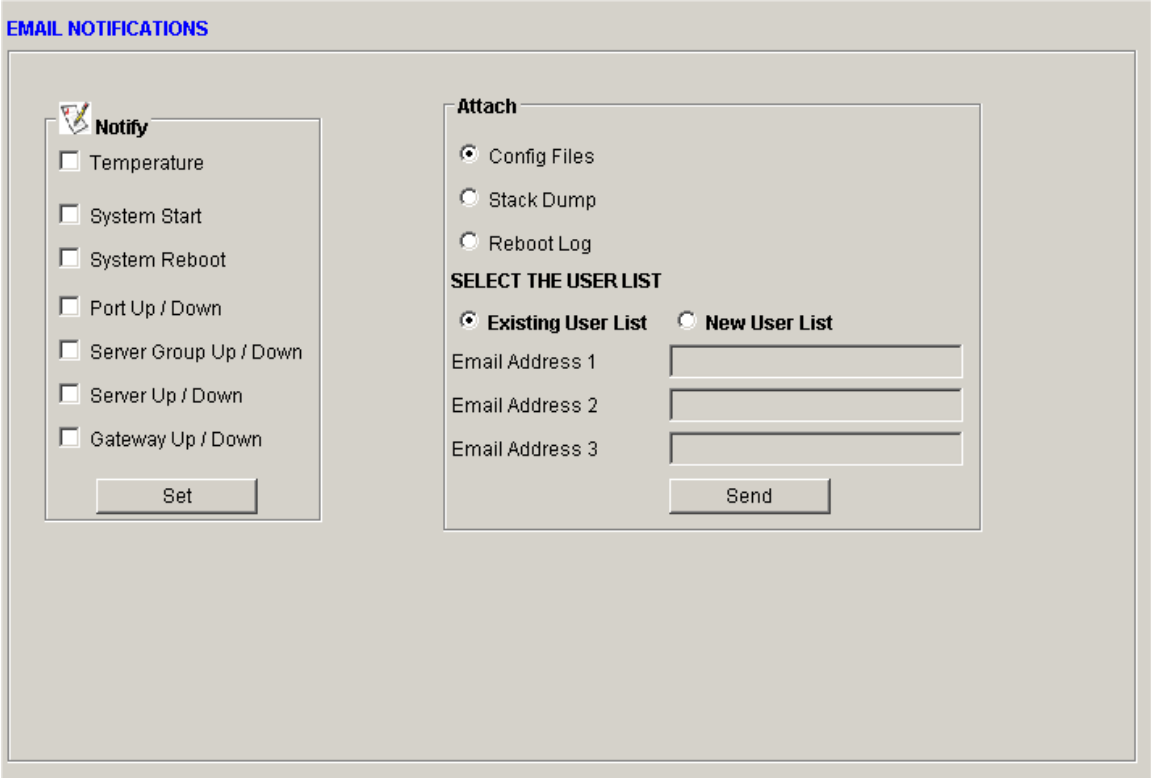


The RNxx device could be configured to send email notification of certain events (see Email Notification). The email configuration consists of the common part such as:
Outgoing Server – could be configured as IP Address or DNS name ;
Server Description - the description of the server;
User Name – the name that will be used to login to SNNMP server (if required);
Password - the password that will be used to login to SNNMP server (if required);
Email Address – the email addresses where the messages will be sent;
User Description – the description of the recipients.

After the configuration is settled by pressing **Apply** button, press **Test Settings** button and the test message will be sent to the list of the recipients.

3.6.3 Email messaging notification configuration

Figure 25 System Config-> Syslog->Email Notification

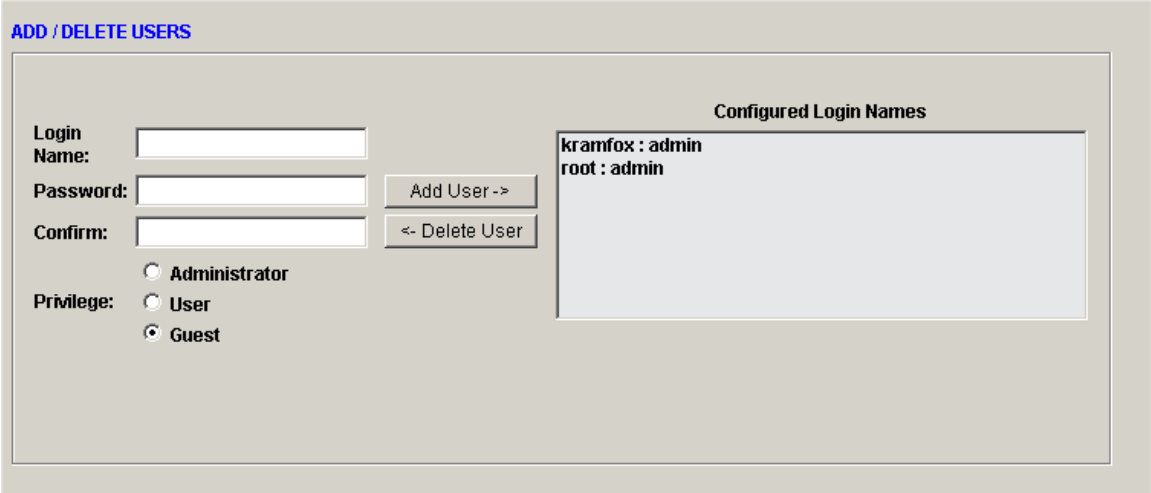


The email notification configuration consists of the list of the events that will trigger the email communication:
Temperature – the internal temperature status of RNxx device
Power Swap - the swap to another power supply
Fan Failure – the malfunction of the fan or fans
System Start – the start of the RNxx device
System Reboot – the reboot of RNxx device
Switch Over – the redundancy switch
Port UP/Down - the change of the data ports status
Server Group UP/Down – the change of the server group status
Gateway UP/Down – the change of the default gateway

Along with the notification the additional info could be attached to the email message : Config Files, Stack Dump or Reboot Log.

3.7 User Admin

Figure 26. Map: System Configuration->User Admin->ADD/DELETE USERS



There are three classes or types of users that can access RNxx device : administrator, user and guest. Administrators have full control over the unit and can perform all administrative tasks. Users can read and modify the running configuration but cannot save it. Guests can only view configuration and not allowed to make any changes.

RNxx device is shipped with a default administrator with a user name 'root' and password 'ranchroot'. It is strongly recommended to create your own administrative user and delete the default one, or at least to change its password. (The password can be changed by deleting the existing user and adding it again.)

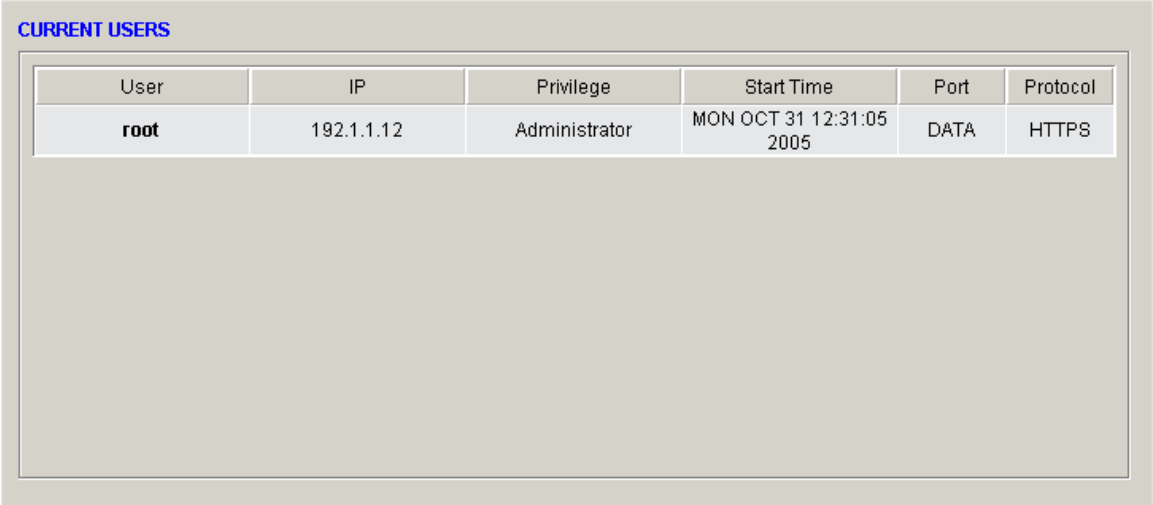
The User Admin screen shown below is used to add new and delete existing users.

User Admin field's description:
Login Name: the user name that is used for this login (the length - from 3 to 40 characters);
Password: the password that is used for this login;
Confirm: the confirmation field for the password;
Privilege: Administrator - the user has a full access to RNxx device (super user)
User - the user can configure everything except the System configuration
Guest – the user has the view-only privilege.
To add user:
Enter the users name and passwords.
Define the correct permission.
Press Add User button.

To delete User:
Select the user from the list.
Press Delete User button.

The next screen **Current Users** shows the current management users .

Figure 27. System Configuration->Current User



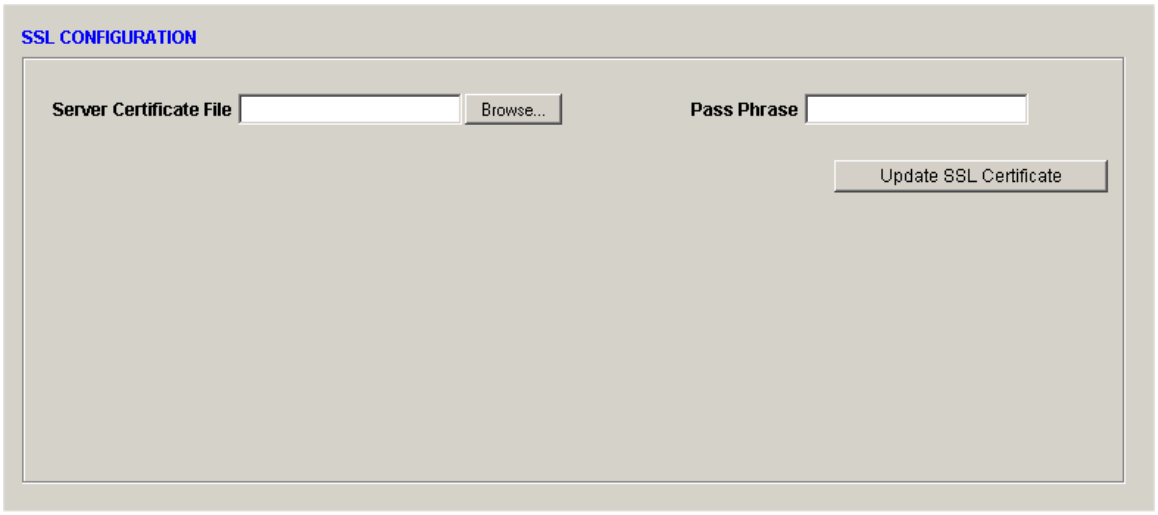
User: the name of the user ;
IP: the IP address of the management station ;
Privilege: the type of the user (administrator, user or guest);
Start time: the time the management session begun ;
Port: the type of the port that used for this session (management or data port);
Protocol: the IP protocol that was used to establish this session.

3.8 SSL Config

Figure 28. Map: System Configuration->SSl Config

You can download your own SSL certificates onto RNxx device .

Figure 29. System Configuration->SSL Config

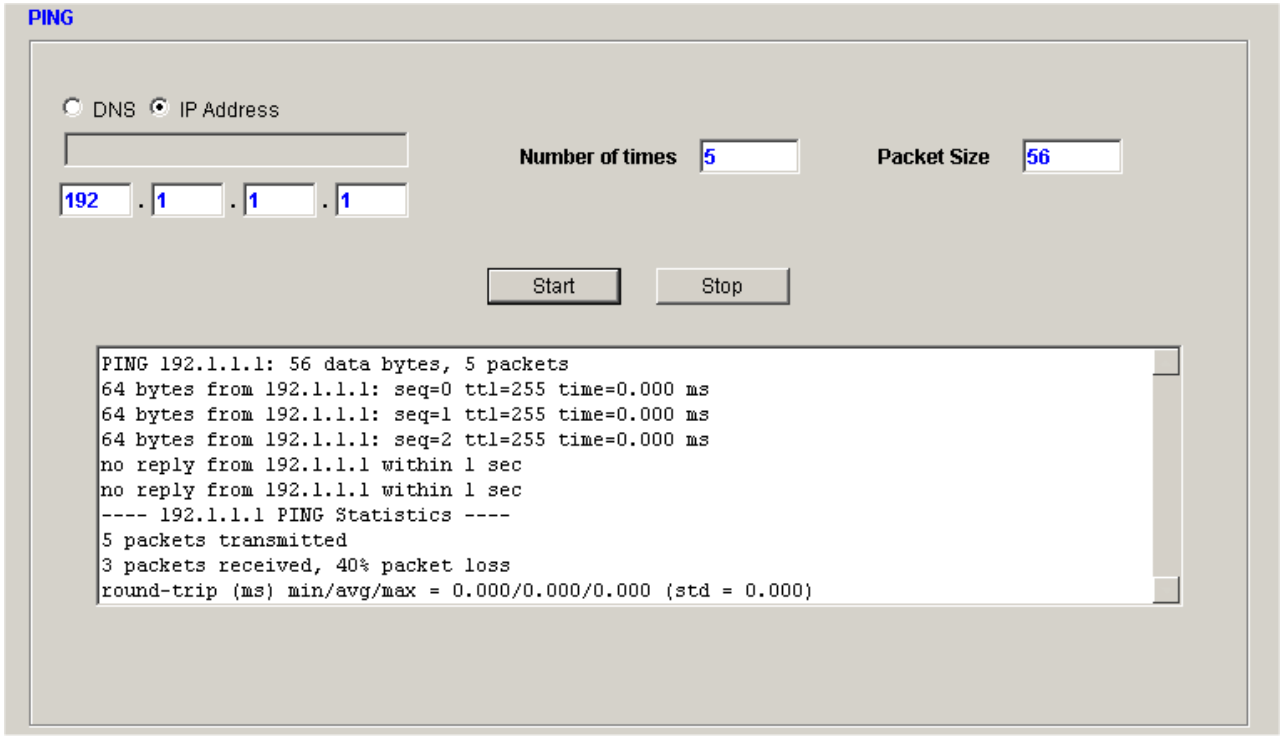


3.9 Diagnostics

The **Diagnostics** mode could be used as a simple network analyzer to perform following tasks:

Ping – to check network connectivity from RNxx device to the remote host;
ARP table – to show a current ARP table of RNxx device;
Network Statistics - to analyze the traffic that is passing trough RNxx device

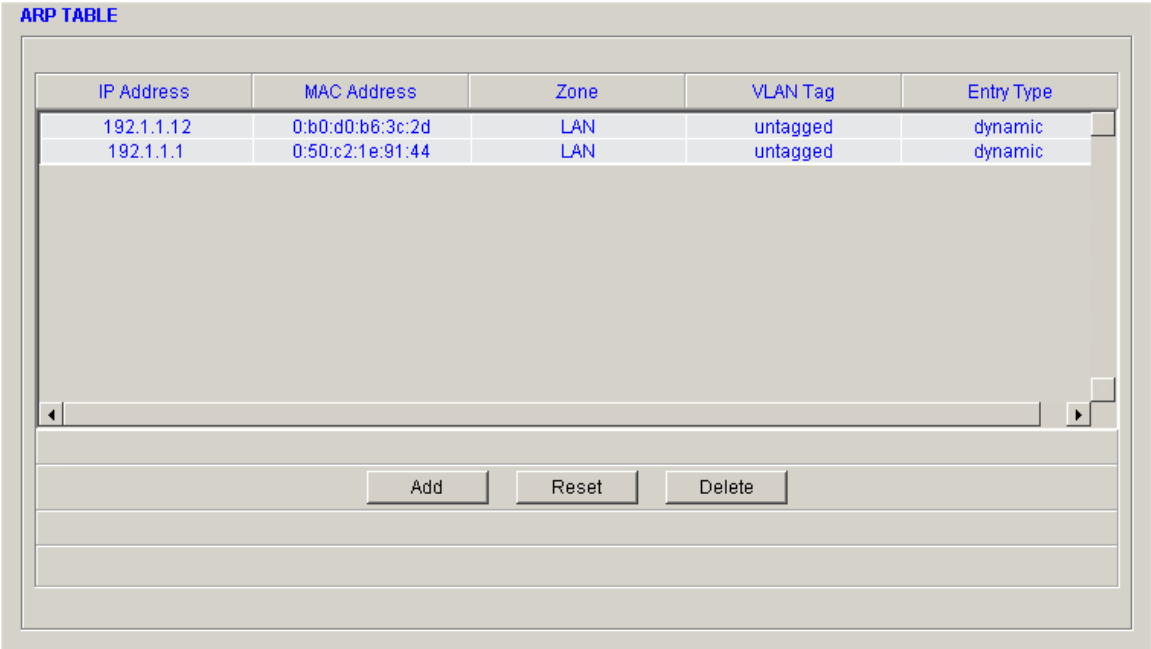
Figure 30 System Configuration->Diagnostics->Ping



To ping the remote host - edit the following fields:
IP Address – IPv4 addressing format (xxx.xxx.xxx.xxx);
Number of times - the amount of ICMP pools to be executed;
Packet Size – the size of ICMP packet.

Press **Start** to begin ping, press **Stop** to quit diagnostic.

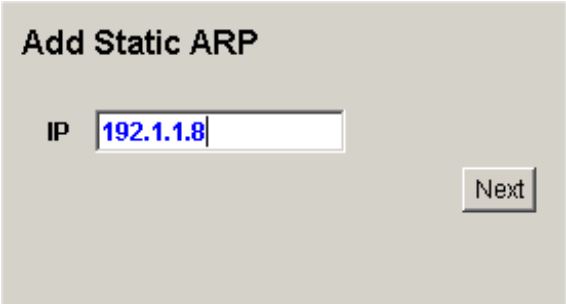
Figure 31 System Configuration->Diagnostics->ARP table



To delete the ARP entry selects the entry from the list and press the **Delete** button.
To refresh the ARP table press the **Reset** button.

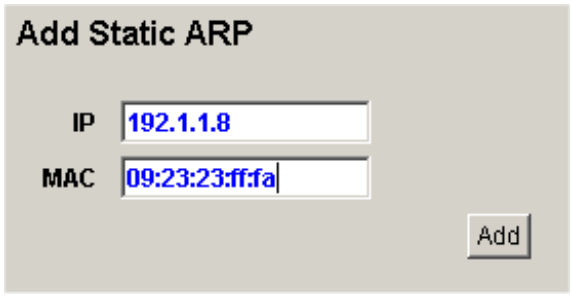
To add the static entry to the ARP table:
Press the **Add** button , the following screen will appear

Figure 32 Add ARP entry screen



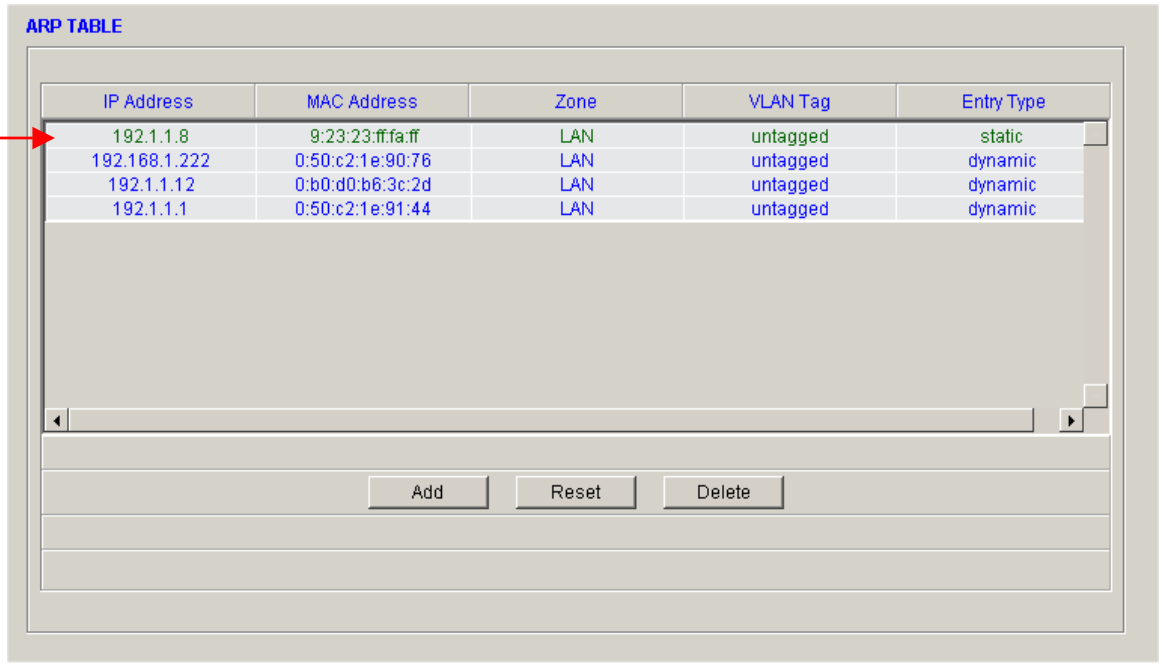
Type in the **IP Address** for the entry, press the **Next** button.

Figure 33 Add ARP entry screen (cont.)



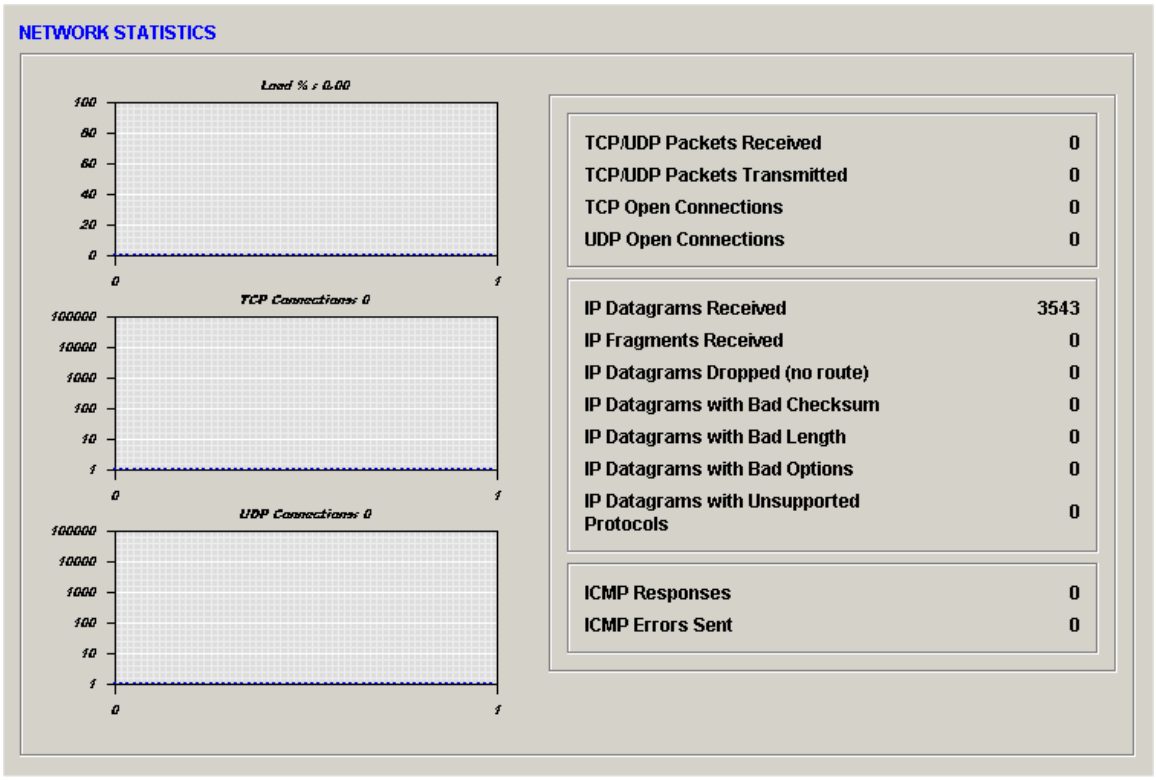
Type in the MAC address for this entry, press the **Add** button.

Figure 34 Add ARP entry screen (cont.)



The added static ARP entry

Figure 35 System Configuration->Diagnostics->Network Statistics

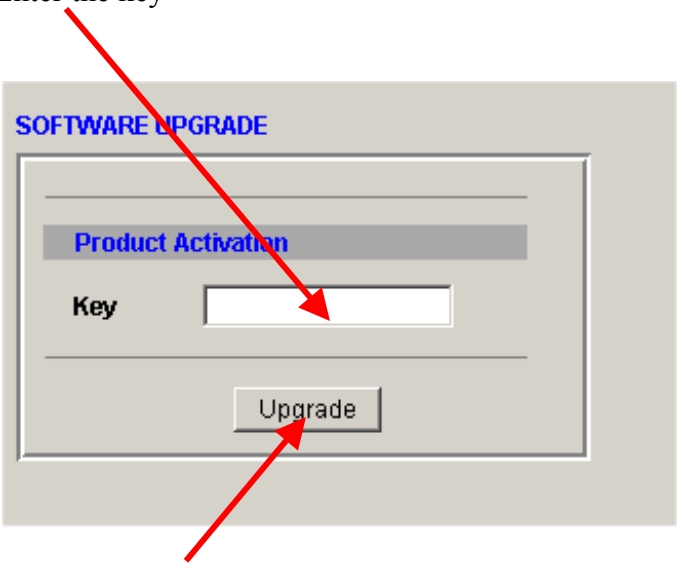


3.10 Features Upgrade

To enable the additional features of the RNxx device , the special feature activation key required . For example : if the RNxx device was bought without the VPN feature then this feature should be purchased from Ranch Networks (or from distributor of Ranch Networks equipment) .
As a result the purchase the customer will get the special feature upgrade key that will enable the VPN feature on the RNxx device.

The licensing information about the product also should be collected and sent along with request for the new feature purchase.
(see the article Product Activation of this manual for more information about the steps and procedures).

After the feature activation key is received it should be entered to the RNxx device.
Go to **System Configuration->Feature Upgrade.**
Enter the key

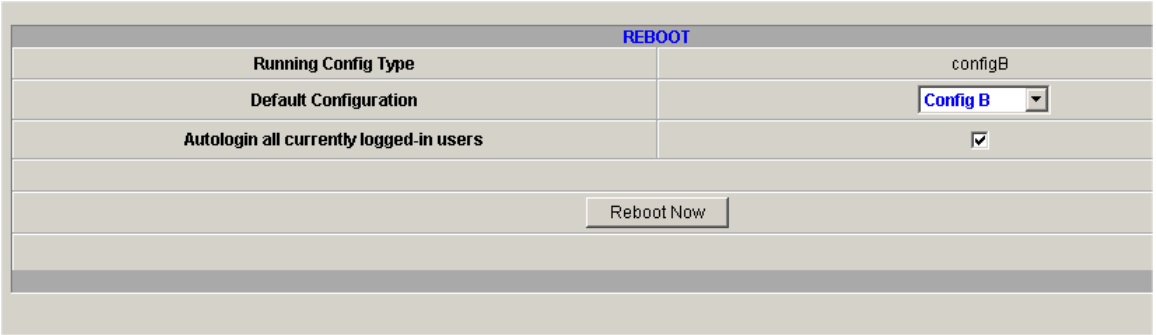


Press the **Upgrade** button.
The new feature will be available for the immediate use.

3.11

3.12 Reboot

Figure 36. System Configuration->Reboot



Reboot screen fields description:

Running Config Type: the present configuration (A or B);
Default Config Type: the configuration that will be loaded at the next reboot;
Autologin all currently logged-in users: If the option is selected - all users session that existed before, will be reestablished after the reboot.

To reboot RN device press the **Reboot Now** button .

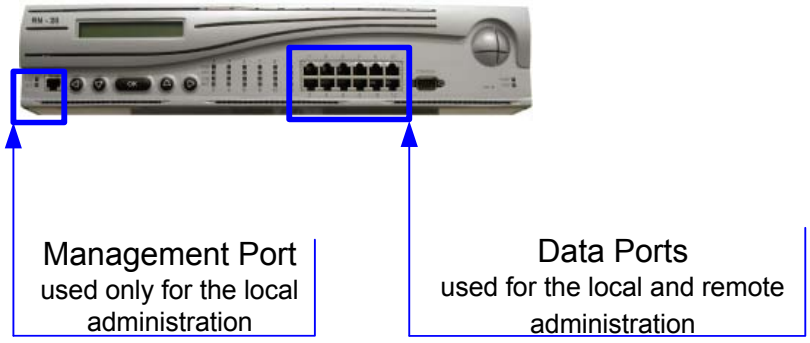
3.13 Securing the access to RNxx device management GUI.

3.13.1 Remote access to the RNxx management GUI

The RNxx management GUI could be accessed trough the management port (RN5, RN20, RN40, RN41), also it could be accessed through the data ports (RN5, RN20, RN40, RN41, RN300).

The management port is the separate RJ45 port located on the right side of the RNxx device front panel (RN5, RN20, RN40, RN41). The next figure shows the location of the management and data ports using RN20 as an example.

Figure 37 The management and data ports (RN5/20/40/41)

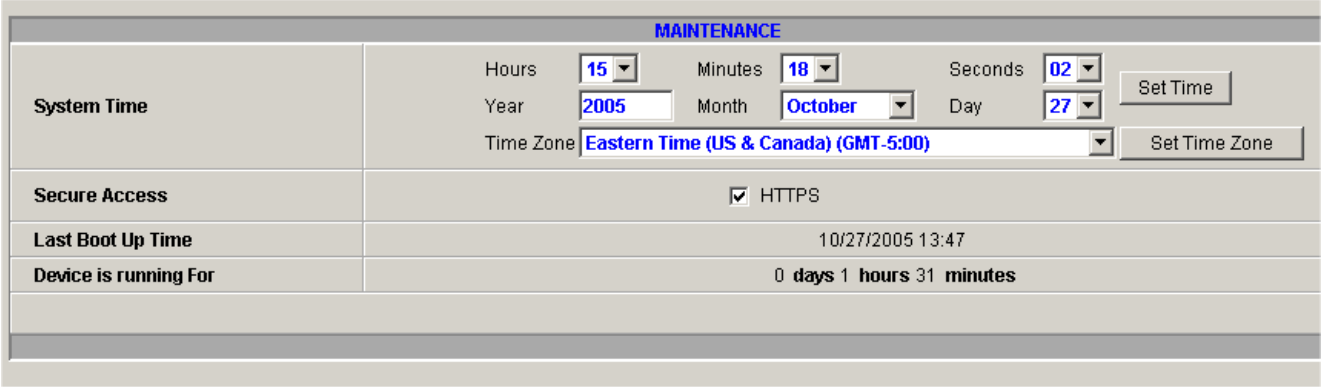


It is strongly recommended that the management port must be used only for the local (access from LAN) administration.

To secure the access to the RNxx management trough the management port:

a) Go to System Configuration->Maintenance

Figure 38 System Configuration->Maintenance



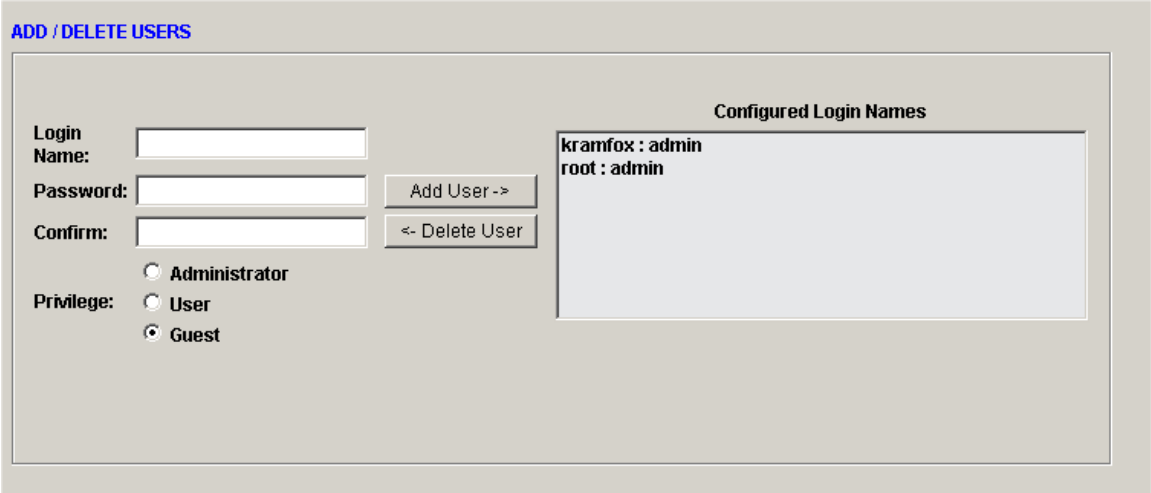
b) Check the Secure Access HTTPS option , it will accept only HTTPS connection to the RNxx management GUI.

> **Caution :** this change will terminate current session and will force the administrator to start a new session.

c) Make sure that all users that are configured to use RNxx management GUI are given the sufficient permissions. For example:
The user that will control the whole system, including the system configuration itself (System Configuration mode) , should have the administrative privilege (administrator). The administrator has the read-write permission for all configurations.
The user that supposed to have access to the services configuration only (everything bellow System Configuration mode) should have the **user privilege.**
The user privilege permits read-only access to the system configuration (System Configuration mode) and the read-write permission to the services configuration

The user that needs only access for the monitoring must have the guest privilege. The guest privilege permits read-only access to the RNxx management GUI.

Figure 39 Users Configuration



The secure access to the RNxx management trough the data ports.

The access to the RNxx management GUI trough the data ports requires more security considerations. Several levels of the security are recommended:

Normal security – the access to the RNxx management GUI is protected by users privilege and mandatory HTTPS connection. (the same as for the management port access). This level of security could be used for the remote access to the RNxx management from the trusted secure zones that used only for the RNxx management.

High security – the access to the RNxx management is protected by:

a) the users privileges and mandatory HTTPS connection (the same as for the management port access);
b) the users authentication that is enabled for the zone. The zone should be enabled for the RNxx management access. (see chapter **7.6 User Authentication** of this manual for more information)
c) the firewall rule that permit the connection for the management only from certain IP Addresses , ports, zones. (see chapter **7.1 Firewall Rules** of this manual for more information)

This level of security must be used when the RNxx management GUI is exposed to the zone that is used for the common purposes (LAN , WAN, DMZ)

3.13.2 RNxx management GUI access monitoring

The monitoring of the RNxx management access is done trough the RNxx syslog functionality. All activities related to RNxx management (users login, configuration changes …) will be logged to the syslog server that is configured for this RNxx device.

For example this is the message about the successful login:

03-29-2004 11:48:41 Local6.Notice 192.1.1.90 id=firewall time="Mar 29 2004 11:47:39" fw=RN20(192.1.1.90) serial=20030032 pri=NOTICE src=192.1.1.105 dst=192.1.1.90 dstport=80 proto=TCP type=local-mgmt user=admin configid=1 msg=" admin successfully logged in "

The next table gives the detail description for the each part of the message above:

Table 3 Syslog message example

Message	Description
03-29-2004 11:48:41	Syslog Server time
Local6.Notice	Syslog facility name
192.1.1.90	The IP Address of the management port
id=firewall	The id of RNxx device
time="Mar 29 2004 11:47:39"	Firewall time
fw=RN20(192.1.1.90)	The model of the RNxx device and the mgt port IP Address
serial=20030032	The serial number of the RNxx device
pri=NOTICE	The priority of the message
src=192.1.1.105	The IP Address of the users workstation (source IP)
dst=192.1.1.90	The destination IP Address (in this case it is IP of the RNxx)
dstport=80	The port that was used for the connection (HTTP in this case)
proto=TCP	The IP protocol that was used for the connection
type=local-mgmt	The connection was done through the Mgt port
user=admin	The name of the user
configid=1	The set of the configuration that is currently used
msg=" admin successfully logged in "	The message's text (payload)

The next message is the example of the unsuccessful login attempt :

03-29-2004 11:59:48 Local6.Notice 192.1.1.90 id=firewall time="Mar 29 2004 11:58:46" fw=RN20(192.1.1.90) serial=20030032 pri=NOTICE src=10.1.4.2 dst=10.1.4.1 dstport=8443 proto=TCP type=remote-mgmt user=admin4556 configid=1 msg=" Unknown user admin4556 "

For more information about syslog messages see the chapter **18 Log Event Definition** and the chapter **19 Example Syslog Events** of this document .

4. Network Management

Network Management consists of the tools that allow users to manage zones, network topology and data port properties. Zones are created to efficiently and securely partition existing network and impose stringent security rules on the traffic flows traversing it.

Zones may be associated with physical ports, IP subnets and VLANs. The spanning tree can also be enabled or disabled for required ports.

Depending of how the network configuration is done the zones also could be:

MANUAL – the network interface for this zone is configured manually (applies to the physical and virtual zones);

DHCP SERVER - the network interface for this zone is configured manually and this zone will have the DHCP server enable in it (applies to the physical and virtual zones);

DHCP CLIENT – the IP settings for this zone will be obtained from the nearest DHCP server (applies to the physical and virtual zones);

The Network Management group has the configuration modes:

- Zone Configuration
- Topology Configuration
- Routing Configuration
- Port Configuration
- Topology Information.

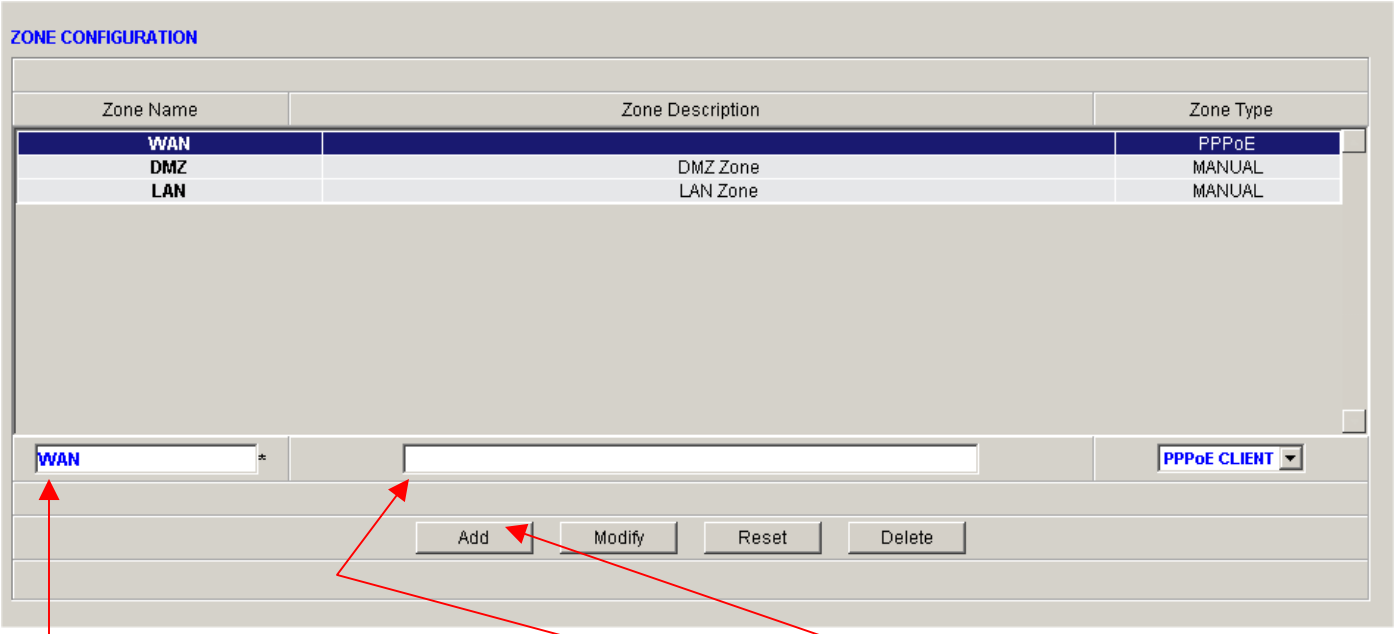
4.1 Zone Configuration

Zones can be created, modified or deleted in the Zone Configuration mode. Each zone entry will have a Zone Name , Zone Description and type of the additional network service such as DHCP Client or DHCP server that is enabled for this zone.

A meaningful zone name, which corresponds to its purpose, should be used while assigning the name, such as 'Internet' or 'DMZ'.

A Zone Configuration screen is shown below.

Figure 40 Network Management->Zone Configuration



To configure the secure zone:
Enter the name for the zone at the **Zone Name** field
Enter the zone description at the **Zone Description** field
Press the Add button .

Caution : a) Zone name cannot be modified once created as this is the index to the zone entry.
b) Any zone entry can be successfully deleted only after deleting its corresponding topology and firewall access rules related to the zone.

Since the zone name is used as an index to the table, it has to be unique, should be no more than 16 characters in length, and should not contain the following characters: **.,(){}**. The zone description is a character string with the maximum length of 64 characters, and should not contain the same characters, prohibited for the zone name.

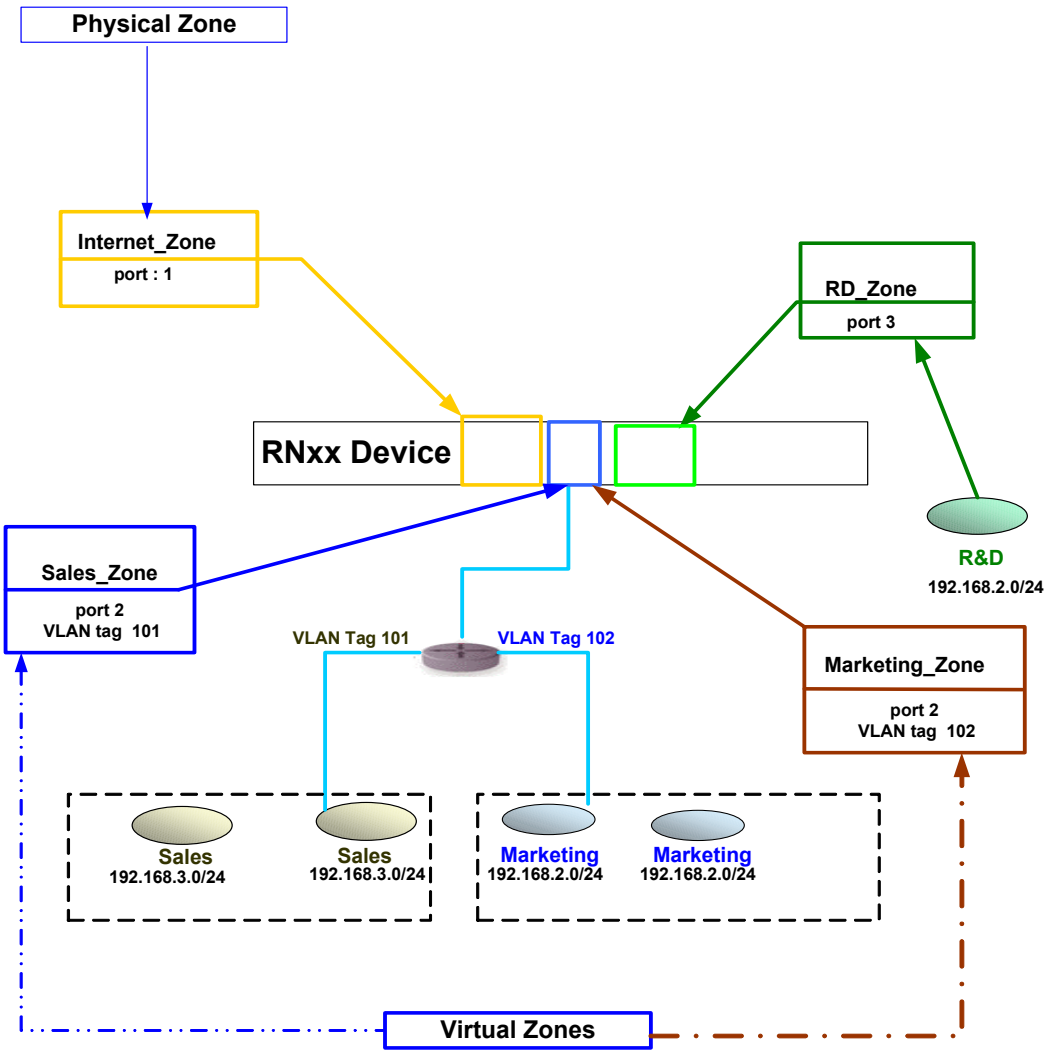
The only following parameters could be modified after the zone was created:
Zone Description and **DHCP** settings

4.2 Topology Configuration

There are two types of zones that can be configured RNxx device. One is a physical zone, the other - a virtual zone. Each physical zone has one or more physical ports that cannot be shared with other zones. In case of virtual zones, the same port can be assigned to different zones. The topology of the zone essentially defines a set of entities, such as ports, interfaces and VLANs that belong to the zone. The zone could be physical or virtual.

Physical Zone - consists of one or more ports and one or more IP interfaces;
Virtual Zone - consists of the ports, VLANs and IP interfaces.

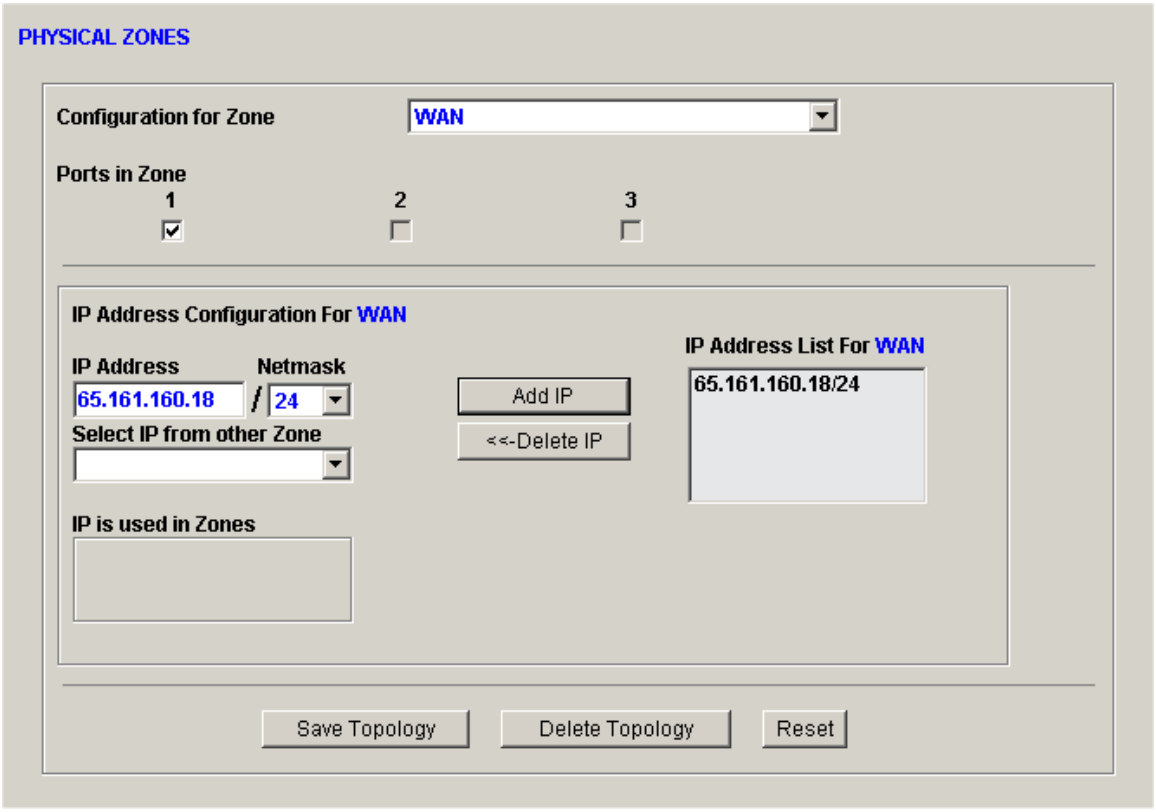
Figure 41. Physical and Virtual Zones



4.2.1 The Physical Zone Configuration

A sample screen for the physical zone configuration is given below.
The zone with a name "**WAN**" is a physical zone that consists of one port (port 1) IP interfaces 65.161.160.18/24

Figure 42 Network Management->Topology Config->Physical Zones



Fields Description:
Configuration for Zone - the name of the zone selected from the list of existing zones.
Ports in Zone - the list of available (unassigned) RN physical ports.
(a port is assigned by checking a checkbox located under the port number)
IP Address Netmask - the IP settings for the zone IP interface
(the parameters should be entered in IPv4 format or selected from **Select IP from other Zone**)

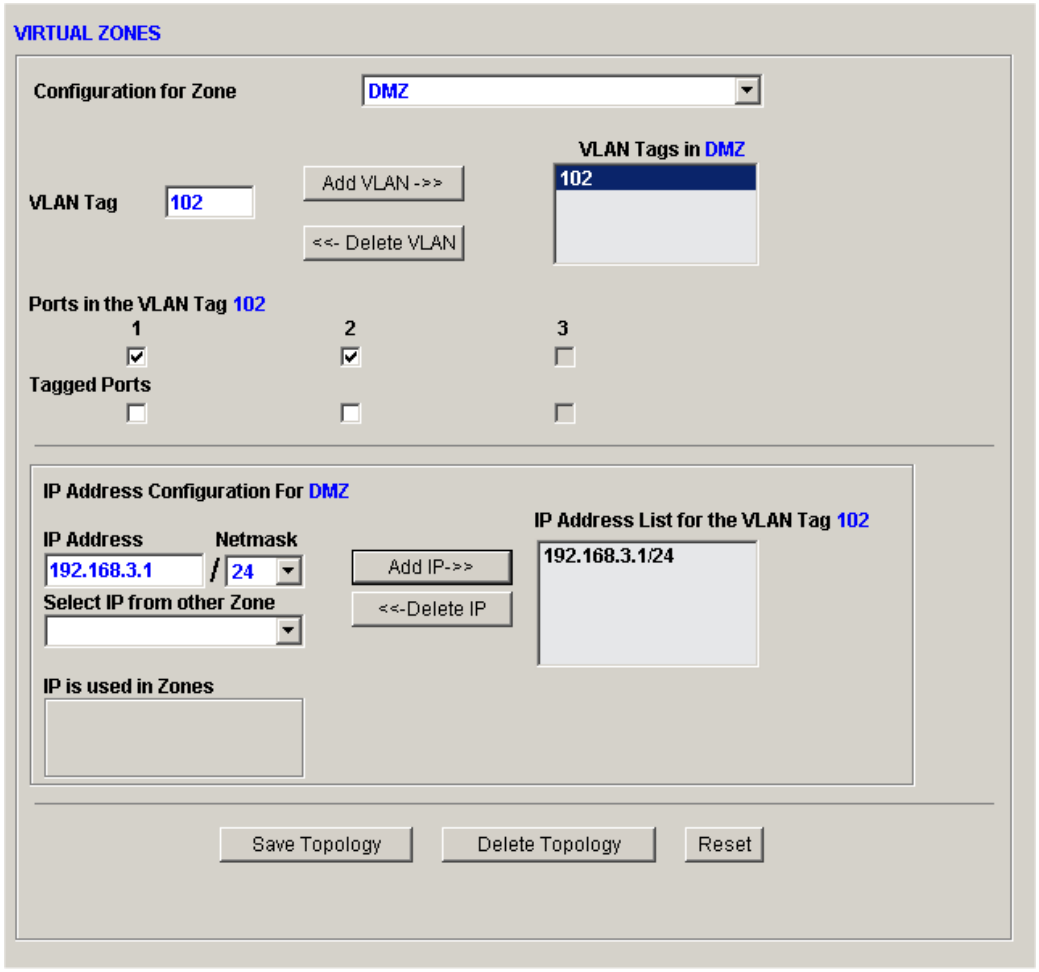
Configuration steps to perform:

- Select the zone from **Configuration for Zone** list.
- Assign ports by marking the checkboxes under the port numbers.
- Enter or select from the list IP Address and Netmask for the zone IP interface.
- Press **Add IP** button.
- Press **Save Topology** button.

4.2.2 The Virtual Zone configuration

The next screen shows the virtual zone configuration.
The zone with a name “DMZ” is defined as a virtual zone that consists of:
Port 2 and port 1 (tagged port)
192.168.3.1/24 interface
VLAN tag 102

Figure 43 Network Management->Topology Config->Virtual Zone



Fields Description:
Configuration for Zone - the name of the zone selected from the list of existing zones.
VLAN Tag - the tag for the VLAN. RNxx device supports multiple VLANs (this parameter should be in the range from 2 to 4000).
Ports in the VLAN Tag - the list of ports that belong to a selected VLAN.
Tagged Ports - the list of tagged ports that belong to a selected VLAN.
IP Address Netmask - the IP settings for the zones IP interface
(this parameters should be entered in IPv4 format or selected from **Select IP from other Zone**)

Configuration steps to perform:

- Select the zone from **Configuration for Zone** list.
- Enter the VLAN tag at **VLAN Tag** field (101 according to the topology used in this example).
- Press **Add VLAN** button
- Assign ports to VLAN by marking the checkboxes under the **Ports in the VLAN Tag** (ports 2 and 4 according to the topology used in this example).
- Define the tagged ports by marking the checkboxes under the **Tagged Ports**
- Enter IP Address and Netmask for the zone IP interface.
- Press **Add IP** button.
- Press **Save Topology** button.

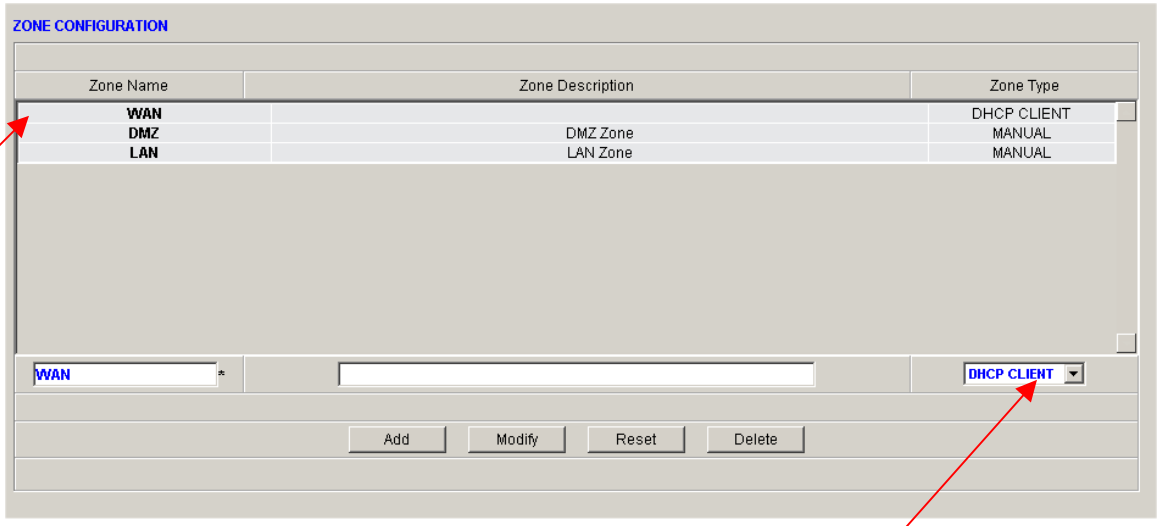
Note: To convert a zone from one type to another the zone topology must be deleted first

4.2.3 The Zone additional services configuration

To configure the additional services such as enabling DHCP Client:

Go to **Network Management->Zone Configuration**

Figure 44 Network Management->Zone Configuration



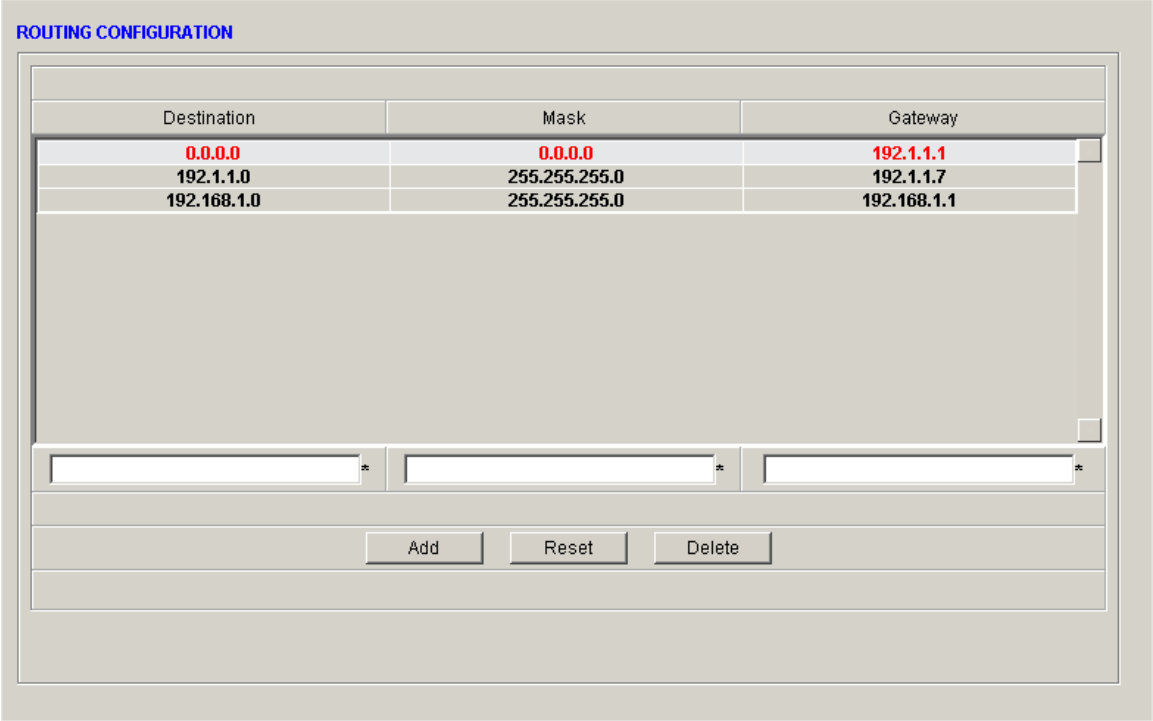
Select the zone (for example **WAN**)
Change the services value from **MANUAL** to **DHCP CLIENT**
Press the **Modify** button

After the zone was configured with additional service **DHCP CLIENT**
the IP Settings for this zone interface will be obtained automatically from the nearest DHCP Server.

4.3 Routing Configuration

When a zone is configured, interface specific routes are automatically created in the routing table. These routes cannot be deleted and exist as long the zone topology they serve. You can manually add static routes by using 'Routing Configuration' tab. Enter the destination network, subnet mask and corresponding gateway IP address, and then click 'Add' to add the route. Click 'Delete' if you wish to delete manually created routes.

Figure 45 Network Management->Routing Configuration

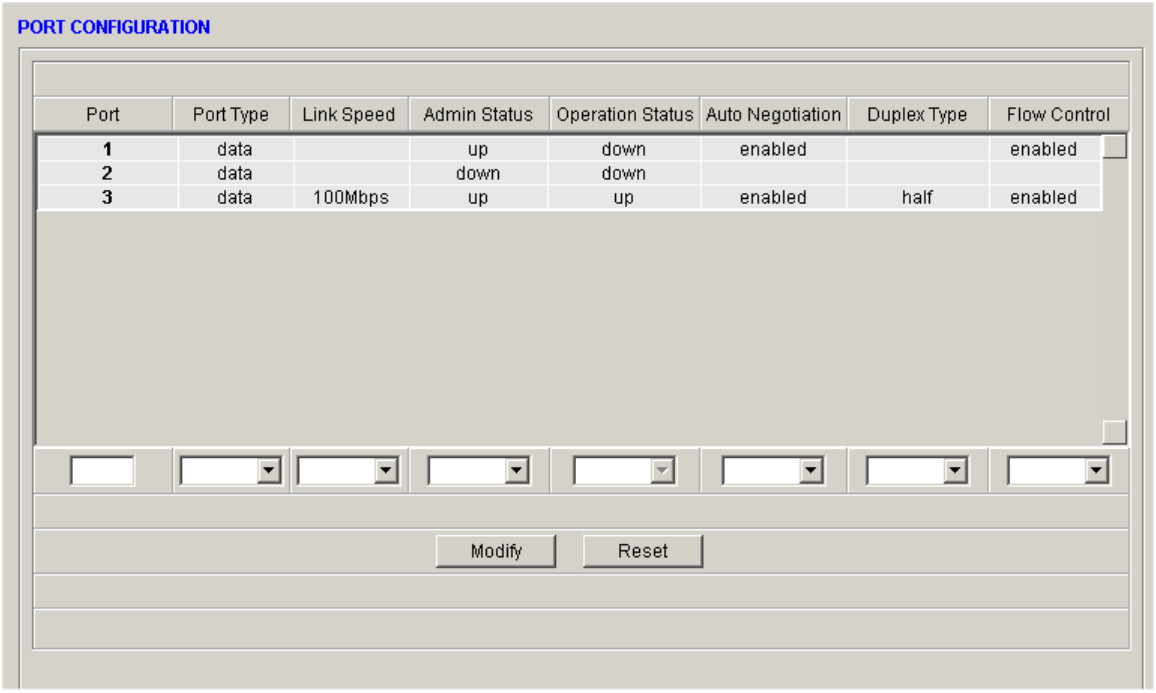


If the unit communicates with other layer 3 devices, you have to configure a next hop default gateway. RNxx device supports up to 8 default gateways, which are constantly monitored If an active default route (colored in red) becomes unavailable, the next gateway in the list will become active.

4.4 Port Configuration

Port properties such as port type, port speed, administrative status, operational status, auto negotiation, duplex/half-duplex and flow control can be monitored and administered from the Port Configuration tab

Figure 46 Network Management->Port Configuration



Port Type: It can be 'data' or 'highAvlb'. By default every port will be in data type mode to offer regular network operation. When it is required to dedicate a port and connect to other RN device for redundancy service, it has to be in 'highAvlb' type.

Link Speed: The ports can operate in 10Mbps or 100Mbps depending on the operating speed of its peer device connected to it.

Admin Status: By default the admin status of every data port on RNxx device is down. Only when a zone topology is created and a port is assigned to a zone, the physical data port can be administratively brought 'up'. This offers added security and flexibility in managing the enterprise network.
The corresponding **LNK** LED for any port on the front panel will be ON when the port is brought administratively 'up'. If the **LNK** LED is OFF for any port, either port is administratively 'down' or physical link or network connection is not available from the peer device to which it is connected. A 'Green' **LNK** LED indicates the port is operating in 100Mbps mode and in 10Mbps mode if it is 'YELLOW' in color.

Operation Status: This will be 'up' only when RNxx device port has established successful physical link to its peer device. On front panel, the corresponding 'ACT' LED will be flashing when there is actual data flow. A 'Green' flashing ACT LED indicates the port is operating in 100Mbps mode and in 10Mbps mode if it is 'YELLOW' flashing in color.

Auto Negotiation: Auto Negotiation feature allows ports to auto-negotiate port speed, duplex mode, and flow control. By default, auto negotiation is enabled for every port.

Duplex Type: Type can be Full or Half. Full duplex mode allows packets to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link.

Flow Control: Flow control is a mechanism that minimizes packet loss during periods of congestion on the network. Flow control is supported on ports operating in half duplex and full duplex modes. It can be enabled on any port. By default it is disabled.

4.5 Spanning Tree Protocol (RN5, RN20, RN40, RN41 models):

STP is a bridge-based protocol that provides protection from network loops. It can be enabled on any port. By default STP is disabled. RNxx device provides SSTP (Single Spanning Tree Protocol)

To enable STP:
Check the Spanning Tree Protocol Enable box.
Check the port (or ports).
Press the Set button.

Once a network loop is detected, STP will disable one or more ports on the RN20 automatically. All such ports are colored in red as shown in the figure below.

To disable STP:
Clear the Spanning Tree Protocol Enable box.
Press the Set button

4.6 Topology information

Topology Information tab displays the relationships between various entities of the existing zones from the following views: Zones, Ports, VLANs, and Subnets.

5. Firewall Configuration

Firewall Configuration menu allows you to set the firewall rules, enable a specific NAT mode, define DHCP relay service, define MAC-based security and user authentication for the zone.
Firewall Configuration has the following tabs:

Firewall Rules, NAT Configuration, DHCP Relay Configuration,
MAC security, User authentication

5.1 RNxx firewall components

The RNxx security system consists of several layers of defense:

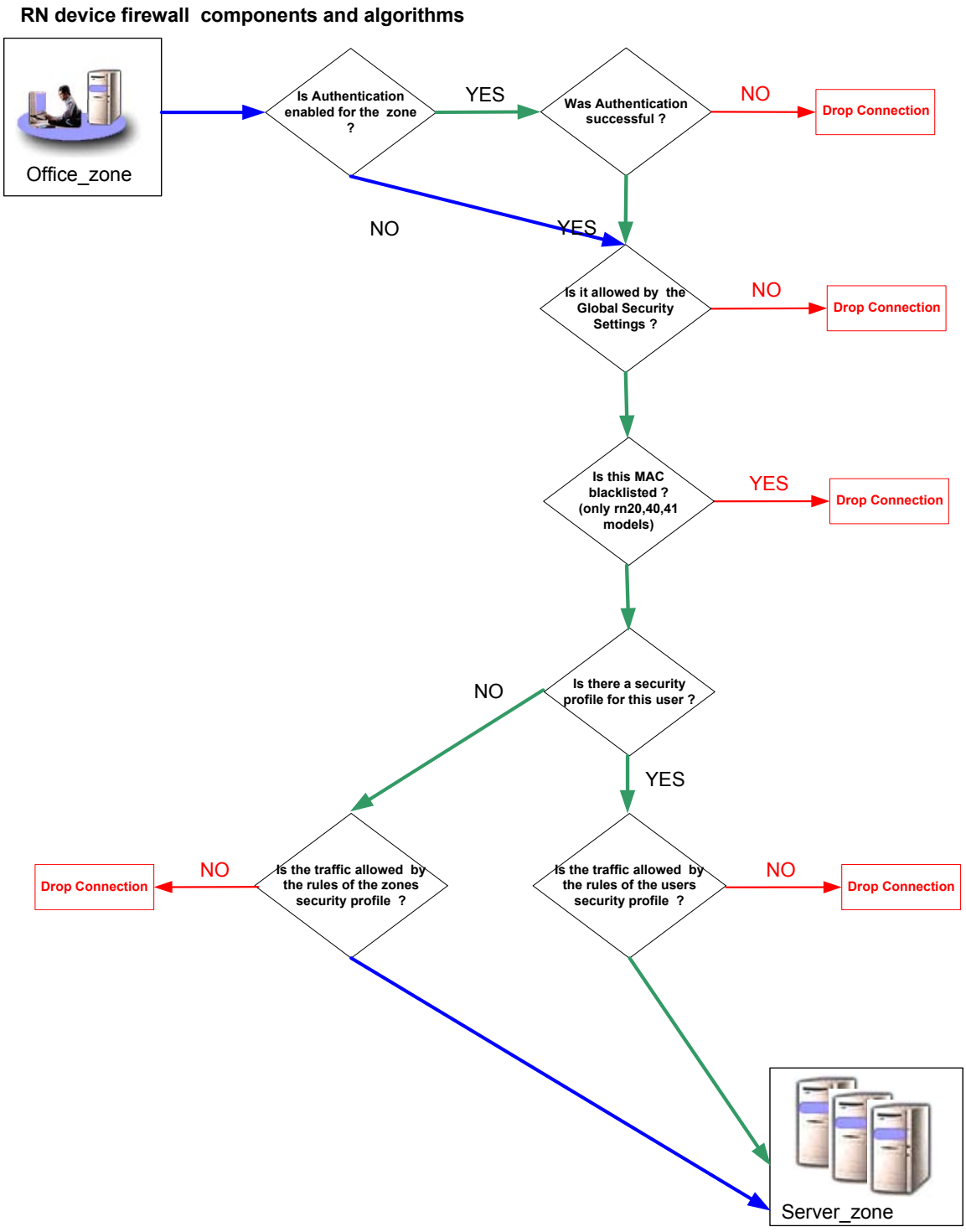
User Authentication - authenticates the users using Active Directory, LDAP, RADIUS or local database

Global firewall settings - defines global security settings for all secure zones and the RNxx device itself

MAC security - controls the network traffic for the secure zone using MAC addresses

Security profile – the set of the rules that controls network traffic for a given zone or user (in the case of user authentication)

The next diagram illustrates the major components of the RNxx security system and the relations between them.



5.2 RNxx firewall concept

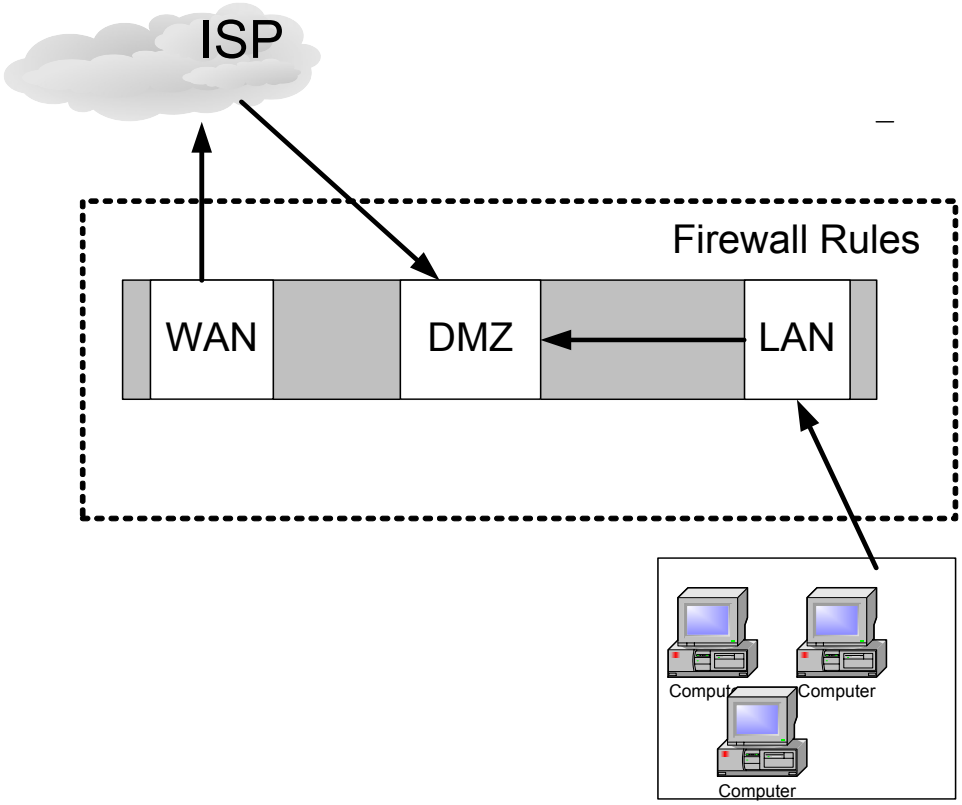
The RNxx firewall concept is based on the secure zone

Security zones enable network managers to implement security policies not just at the perimeter, but also throughout the whole enterprise. With this approach Internet is treated like any other zone with its own set of policies and rules

A conventional firewall partitions the enterprise into three distinctive domains:

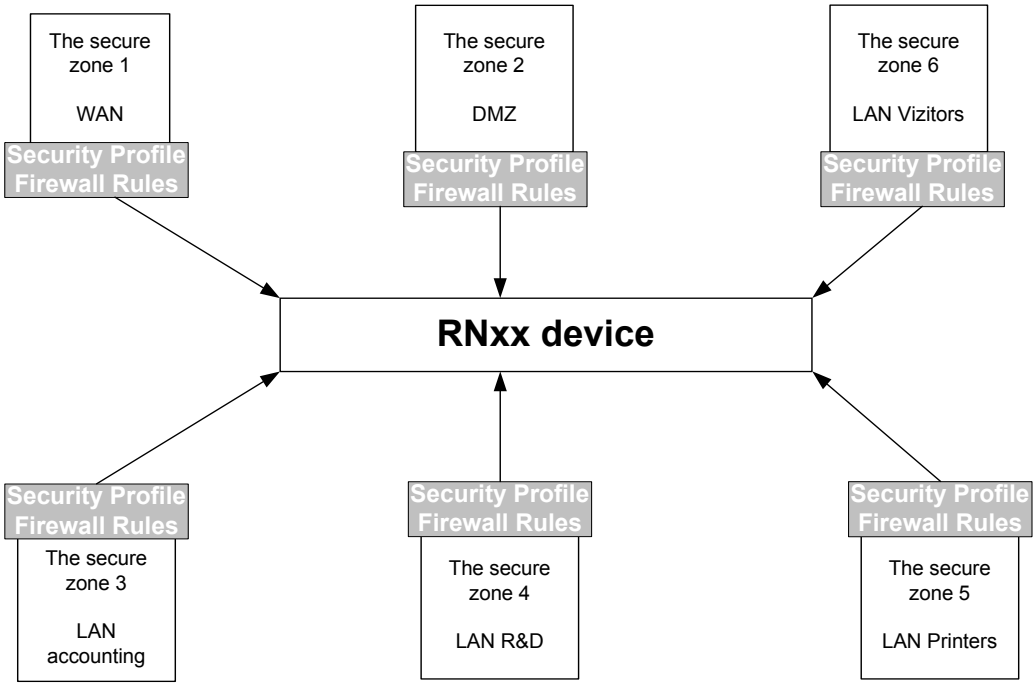
- External (WAN) – resources outside of the enterprise perimeter.
- Internal (LAN) – resources within the perimeter that need protection
- DMZ (De-Militarized Zone) – A set of corporate resources that need certain level of protection but is "directly" accessible from external domain.

Figure 47 The traditional firewall



Unlike the traditional firewall, the RNxx firewall does not assume pre-defined roles for the Network segments that are connected to it. Instead, RNxx firewall is based on the secure zones concept described above. Using the secure zone concept, a network administrator can seamlessly segment existing pre-configured network, and provide external/internal security. A **security profile** consists of an ordered set of firewall rules. Multiple security profiles can be created and applied on a per zone, user or group basis to achieve total control over the traffic.

The following diagram shows a topology with six secure zones. In this case, the internal network (LAN) has been segmented into four secure zones without modifying the existing IP subnet infrastructure.



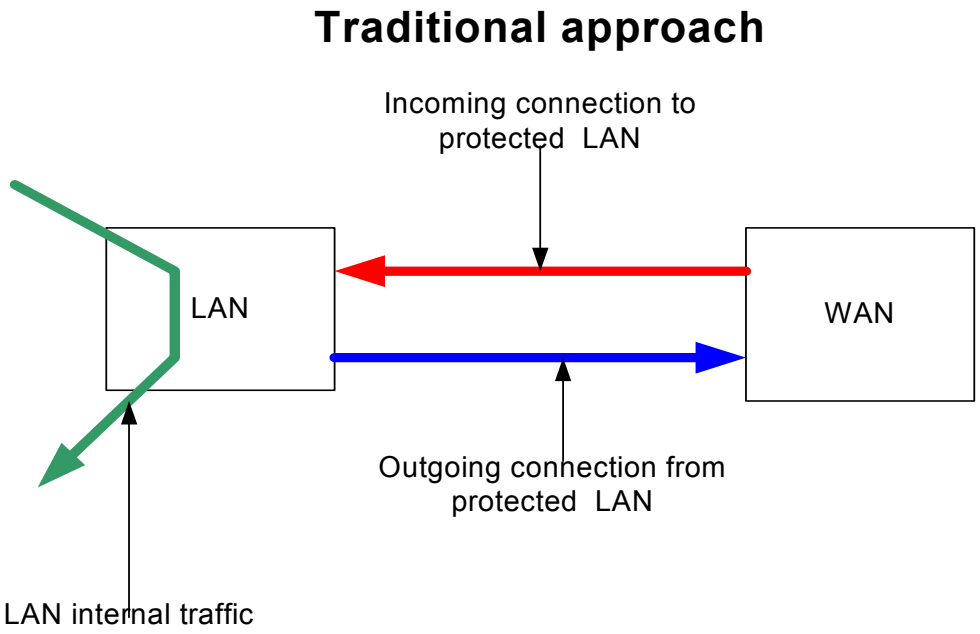
5.3 Security Profile

A **security profile** consists of an ordered set of firewall rules. Multiple security profiles can be created and applied on a per zone, user or group basis to achieve total control over the traffic.

As soon as the secure zone is configured at least one (default) rule is created. The rule default rule number is 65535. The rule 65535 will deny all incoming and outgoing connection for the secure zone.

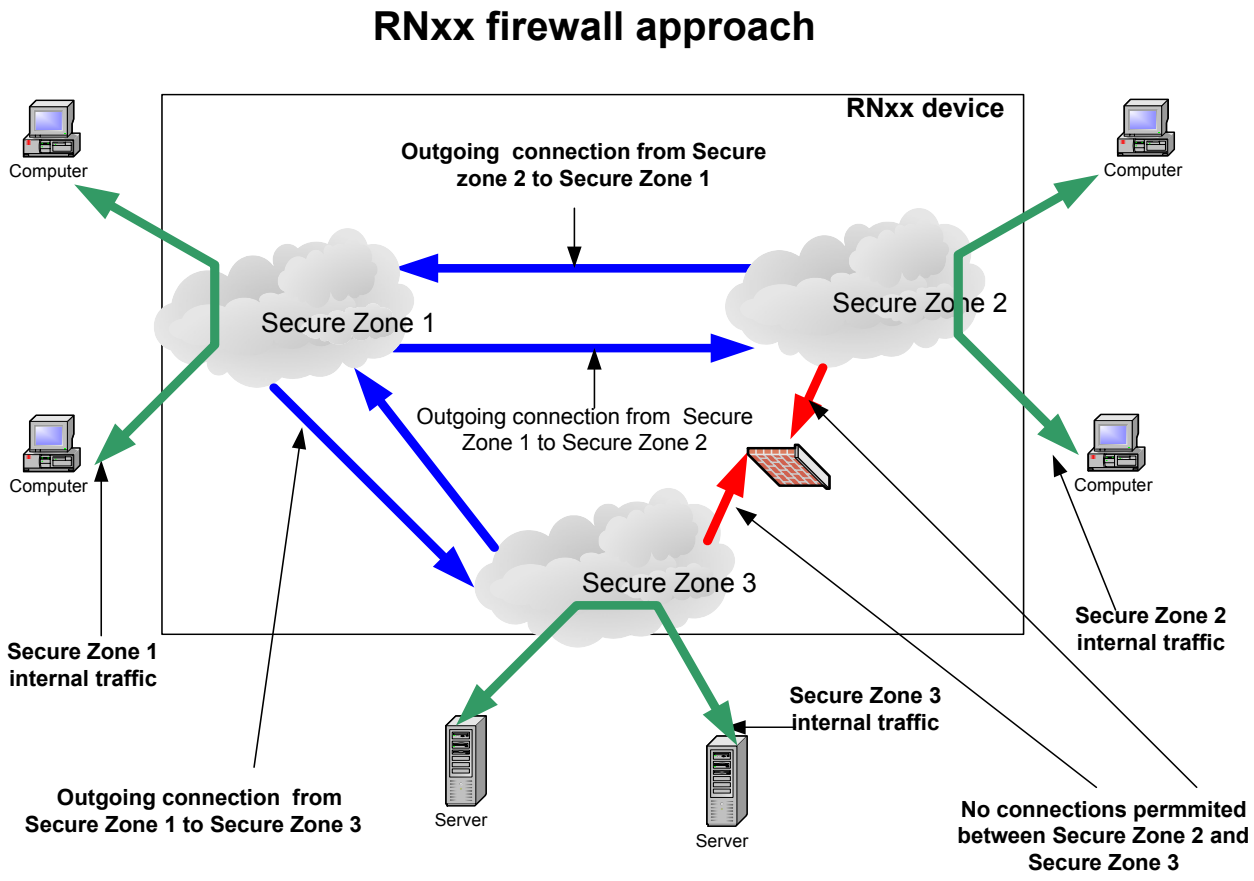
According to the traditional firewall configuration there two type of the connection for the protected network – incoming and outgoing. The next figure shows the traditional approach.

Figure 48 The traditional approach (incoming outgoing connections)



(Did not understand the description – needs re-working)
The direction of the network traffic through the RNxx device firewall, in general, is similar to the traditional concept. The only difference is : instead of controlling incoming and outgoing traffic to and from protected network RNxx device firewall controls the outgoing traffic from secure zones and the traffic inside the secure zone.

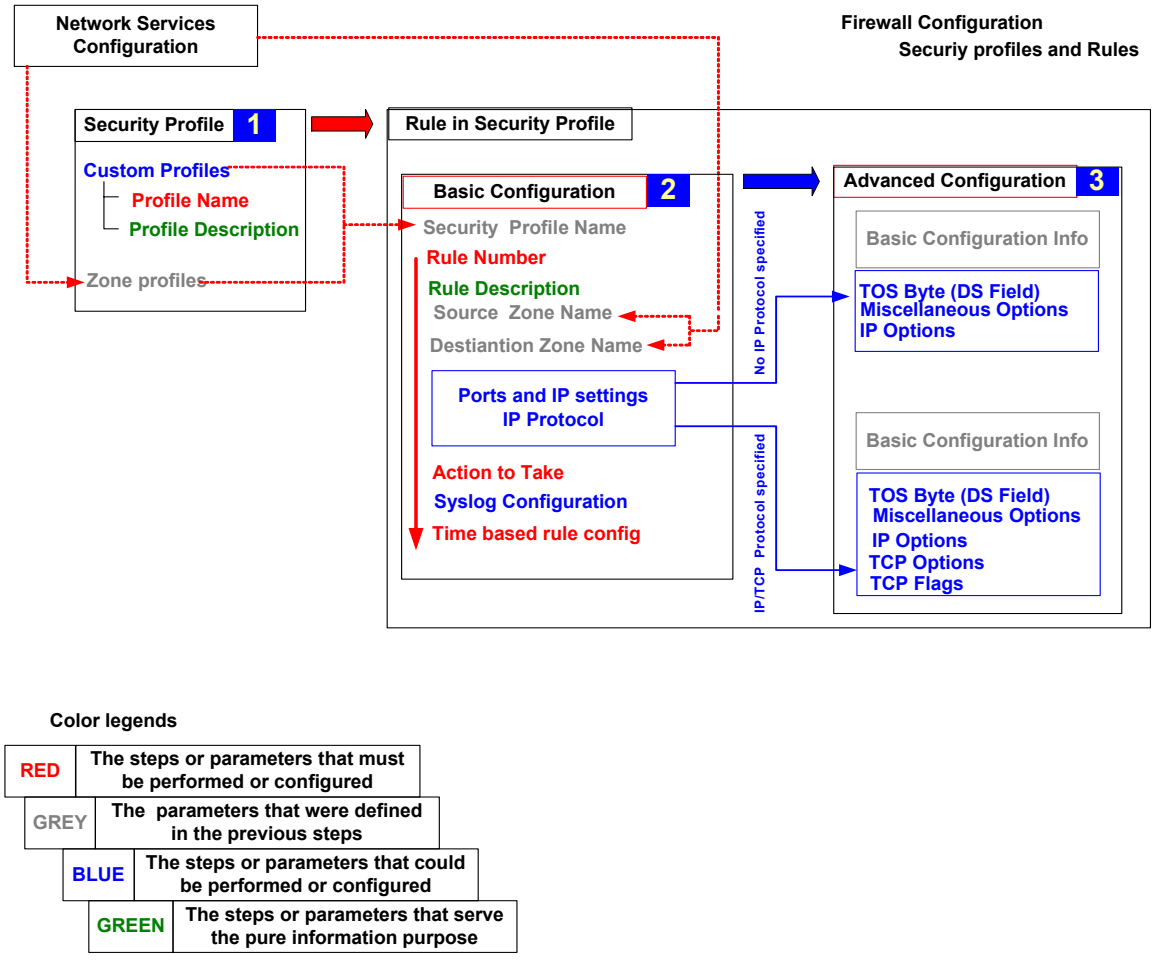
Figure 49 RNxx firewall approach



5.4 Firewall Rules

Firewall access rules control the traffic traversing the security zones. These rules are a set of instructions used by the unit to determine what action has to be performed for the incoming request. The main components of a rule are: zones (source and destination), service ports and IP addresses. The rules have to be configured for each zone. If the request matches one of the rules, RNxx performs one of the following actions such as allow, deny, count, forward or reject the request. The next figure shows the firewall rule configuration path.

Figure 50 RNxx firewall rule configuration path

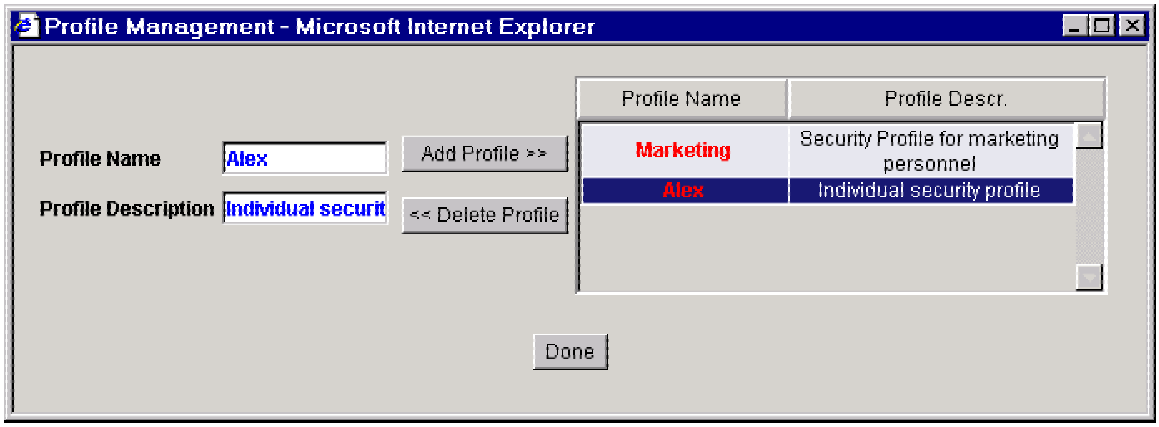


The firewall rules are always applied when the traffic traverses from one zone to another (inter-zone traffic). Conversely, no firewall rules are applied for traffic within the same zone (intra-zone traffic). A set of firewall rules should be configured on each zone. The rules within a particular zone are ordered according to the rule number. The rules are always applied starting from the smallest to the largest rule number. The action (accept, deny, etc.) is taken based on the rule that matches first. Thus, the order of the rules is VERY IMPORTANT, and a more specific rule should always precede a broader rule. An ordered set of firewall rules form a security profile in RNxx device.

By default, RNxx device blocks traffic from coming in and going out of a zone. As soon as a zone is created, a default zone profile with is created automatically. The name of the automatically created zone profile is the same as the zone name. The profile will have one rule to deny all traffic from the zone with the rule number equal to 65535. All user specific rules should be created with the numbers from 1 to 65534.

You can also create your own, custom, security profile by clicking on the hyperlink "Firewall rules for security profile". Clicking on the hyperlink results in a new popup window where a new profile can be configured.

Figure 51. Custom Security profile configuration

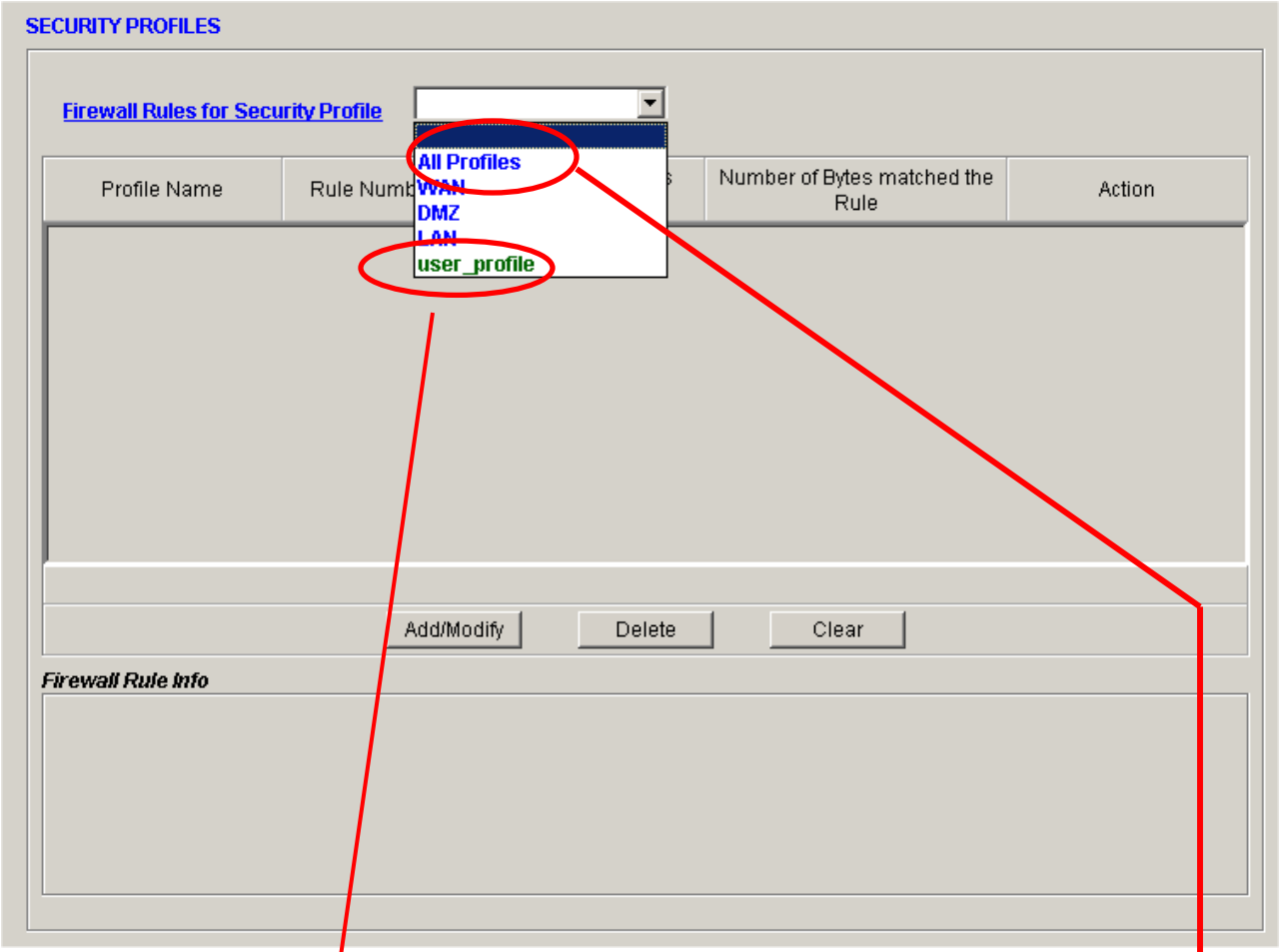


To create a new user defined profile type unique profile name and profile description (optional) and click on "Add Profile" button.
To delete a user defined profile, select the profile and click on "Delete Profile" button.

Caution: User defined profile cannot be deleted if it is associated with at least one of the users configured on the RNxx for User Authentication. To delete that profile first all associations have to be removed by either deleting a user associated with that profile or assigning a different profile for the user.

As soon as a user-defined profile is created, one default rule will be created in that profile. The default rule will have the rule number equal to 65535 with action “deny” all traffic.

Figure 52. Firewall Configuration->Security Profiles



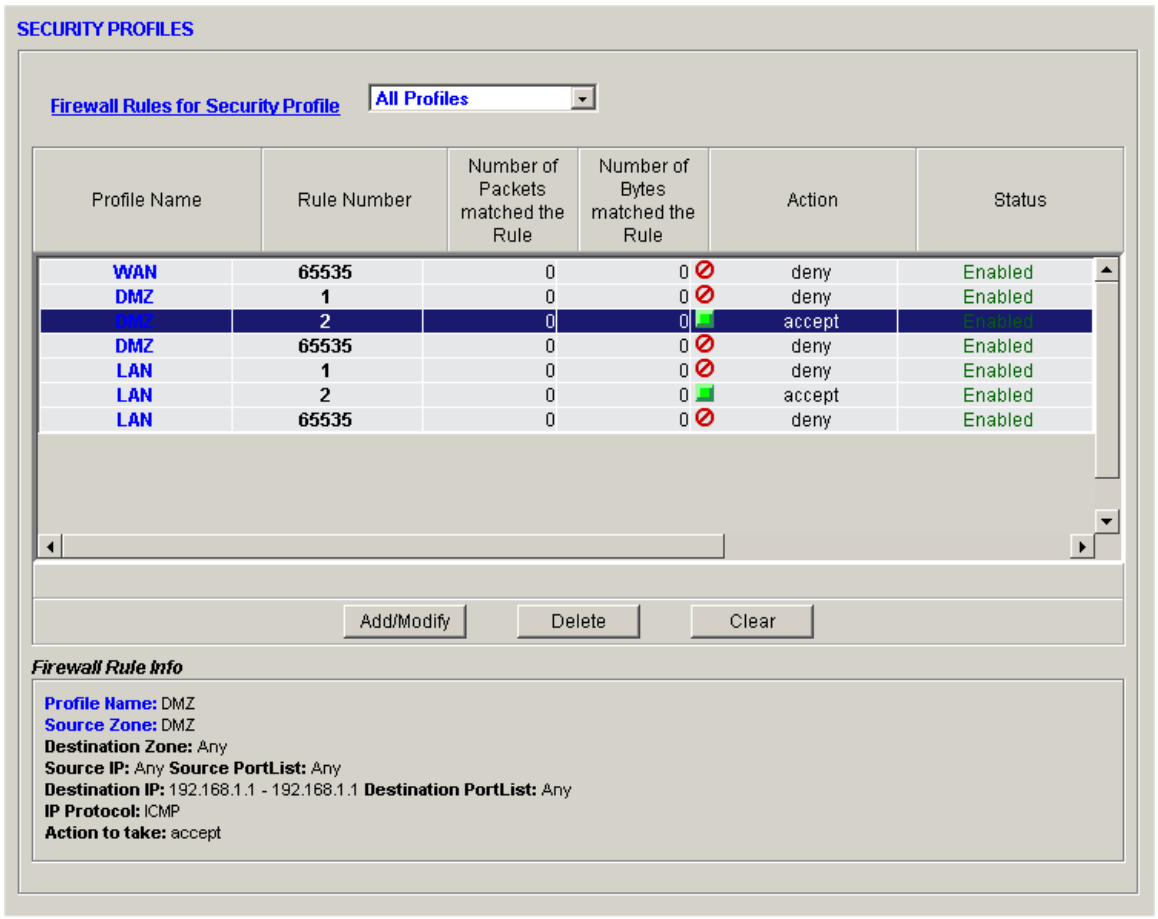
All such **user-defined profiles** can only be used for User Authentication purposes. Refer to the following sections to know more about User Authentication.

A firewall rule consists of packet classification information such as destination zone, rule number, description, source IP address, source port, destination IP address, destination port, and an action to perform.

The only difference in **zone profiles** that are automatically created and the user defines profiles, is in the use of source zone while configuring a firewall rule. For zone profiles, the source zone is fixed and is the same as the zone for which the profile belongs. A user created profile can however, contain firewall rules for any source zone.

The following screen shows the Firewall Rules tab, where the basic rule information can be viewed in a tabular form. Each rule 'hit' statistics, i.e. the number of packets / bytes affected by the rule, can be viewed.

Figure 53. Firewall Configuration->Security Profiles (cont.)



Firewall Rules for Security Profile: You can view all the rules for a particular security profile by selecting the name from the list. If you select All Profiles, all the rules currently defined in RNxx device will be displayed.

Firewall Rule Info: By selecting a particular rule in the table, its summary will be displayed for quick reference.

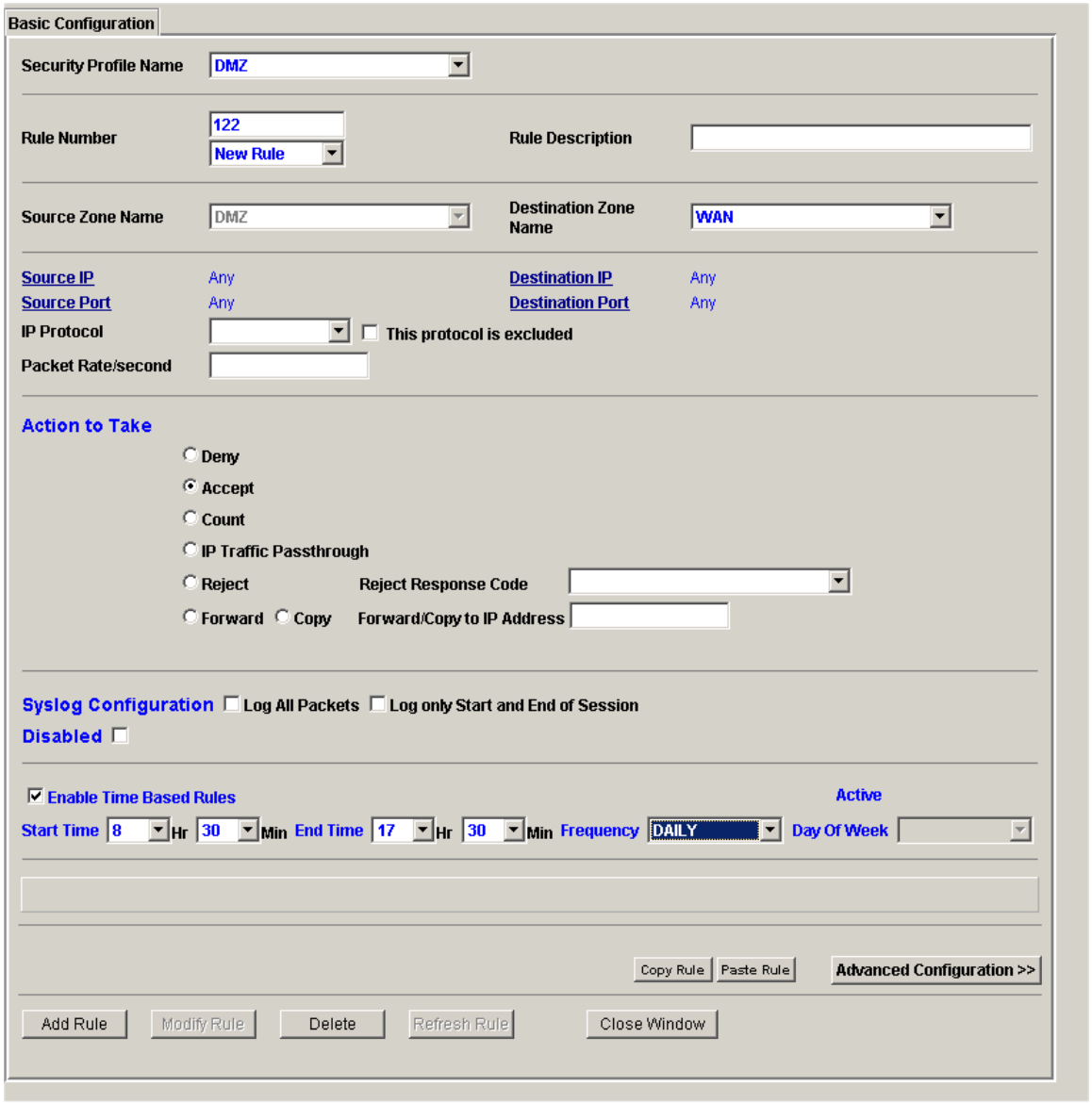
Use 'Add/Modify' button to add a new rule or modify an existing rule. If you wish to delete an existing rule, press 'Delete'. In order to clear the rule statistics, press 'Clear'

When 'Add/Modify' button is pressed, a new window will appear on the screen. The rule-related information is split between the basic and advanced configurations. The basic configuration enables you to define a rule based on source/destination IP addresses, service ports, and packet rate and destination zones. Advanced configuration allows you to define a rule for deep packet analysis using IP and TCP flags/options and ICMP packet

types. For a zone profile, the source zone is fixed and is the zone from which the traffic entered the RNxx device.

Basic Configuration window:

Figure 54. Firewall Configuration->Security Profiles->Basic (rules) configuration



Basic Configuration fields:

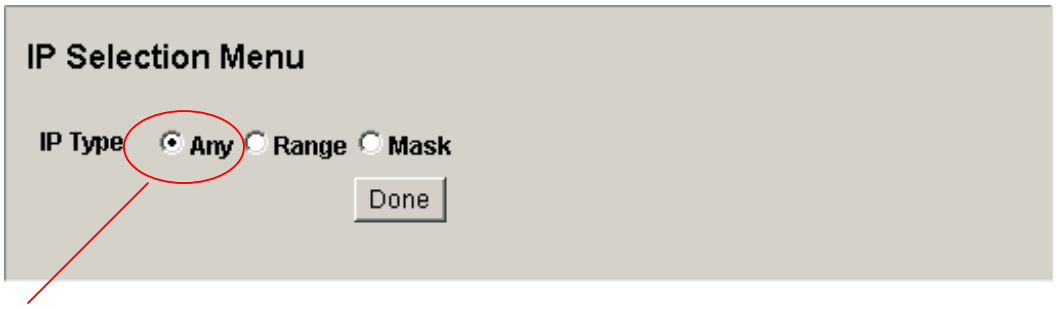
Field Name	Value	Description
Security Profile Name	Selected from the list of existing profiles	This is the profile to be operated upon.
Rule Number	Numeric value 1 – 65534	A unique number for each rule (inside the same profile). Automatically ordered from smallest to largest rule number. To insert a rule in the middle of a rule set, select in between rule number.
Rule Description	String value 0-65 length	A meaningful rule description.
Source Zone Name	Selected from the list of existing zones	This is the source zone for the rule, and rule will be applied to packets that originate from that zone .
Destination Zone Name	All zones or a particular zone from the list.	This is the destination zone for the rule, and the rule will be applied to packets that are destined for that zone.
Source IP	IPv4 format	The originating IP address.
Source Port	Network ports format	The originating service port.
Destination IP	IPV4 format	IP address the traffic is destined for.
Destination Port	Network ports format	Service port the traffic is destined for.
IP Protocol	Selected from list of predefined protocols	A single IP Protocol or All IP Protocols can be selected. All other protocols except the one selected, can be enabled by using 'Except' check box.
This Protocol is excluded	The checkbox	If checked, the selected protocol is excluded from the rule
Packet Rate/Second	Enter numeric value in terms of packets per second (pps)	If the incoming packet rate is greater than the specified rate, the corresponding Action is applied. If not this rule is ignored and the next matching rule is applied.
Action to be taken	Deny, Accept, Count, IP traffic passthrough, Reject, Forward / Copy	**Deny** – will deny according to rule **Accept** – will accept according to rule **Count** – will count packets **IP Traffic Passthrough** – packets will just be routed bypassing all further modules such as stateful firewall, bandwidth limiter, load balancer, NAT, etc. Use very carefully as it may create security holes. Only VPN traffic is recommended for this action. Reject – packets are rejected and selected return

		code is sent. For TCP the only valid code is "TCP: Send reset". All other codes are applicable fro UDP traffic. **Forward/Copy** – will forward or copy packets to a specified IP address. If 'forward', the packet will be diverted to the forwarding IP address instead of its intended destination. If 'copy', a copy of the packet will be sent to the forwarding IP address and the original packet will be sent to its intended destination.
Syslog Configuration	Check or Uncheck	Generates a Syslog message for the rule.
Disabled	Check or Uncheck	Enables or disables the firewall rule
Enable time based rules	Check or Uncheck	Enables the time settings for the firewall rule
Start Time	The time in the military format , for example 17:00(5:00 pm)	The time when the rule will become active.
End Time	The time in the military format , for example 22:00(8:00 pm)	The time when the rule will be deactivated.
Frequency	Daily	The rule will be used everyday (according to the time interval).
	Weekly	The rule will be used once per week on the day defined at the **Day of the Week** field (according to the time interval).
	Weekday	The rule will be used from Monday to Friday every week (according to the time interval).
	Weekend	The rule will be used on to Saturday and Sunday every week (according to the time interval).

5.4.1 The IP Addresses and Port Settings Configuration

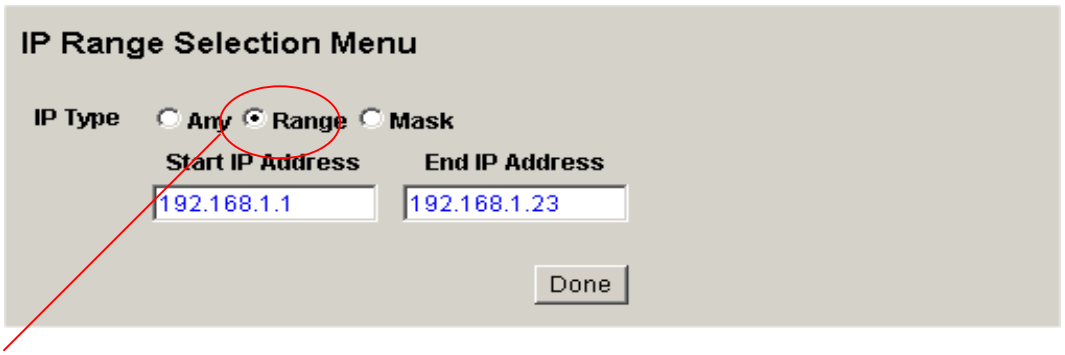
To configure IP Address settings for the rule (Source IP or Destination IP):
Click on **Source IP** or **Destination IP** link in the **Basic Configuration** window.

Figure 55. Firewall Configuration->Security Profiles->Basic Rules->IP settings



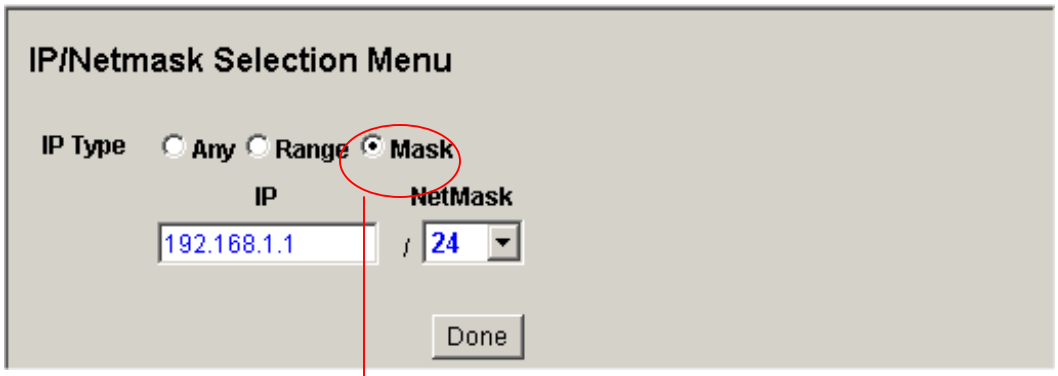
IP Type – Any: all IP Addresses are covered by this rule.

Figure 56. Firewall Configuration->Security Profiles->Basic Rules->IP settings (cont.)



IP Type – Range: this rule will work only for the addresses within the defined range.

Figure 57. Firewall Configuration->Security Profiles->Basic Rules->IP settings (cont.)



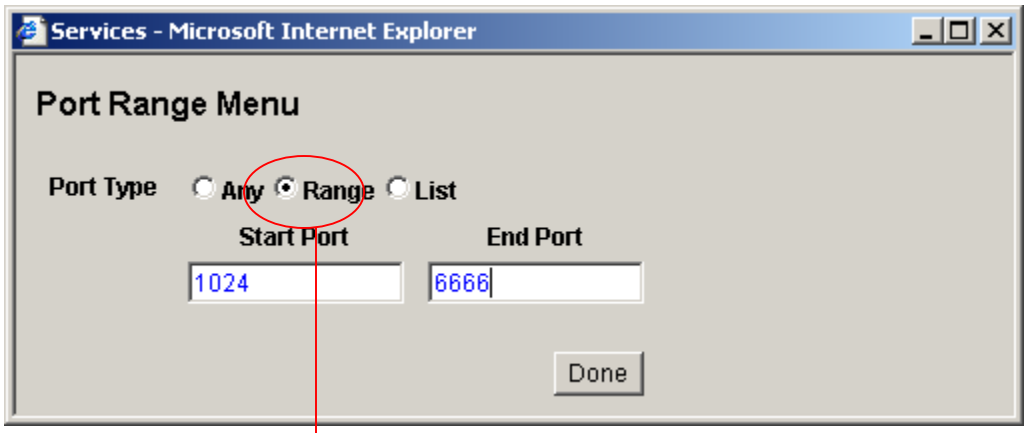
IP Type –Mask: this rule will work only for the IP addresses belonging to a specific subnet.

To configure Network Ports settings for the rule (Source Port or Destination Port): Click on **Source Port** or **Destination Port** link in the **Basic Configuration** window.

Figure 58.Firewall Configuration->Security Profiles->Basic Rules->Port settings

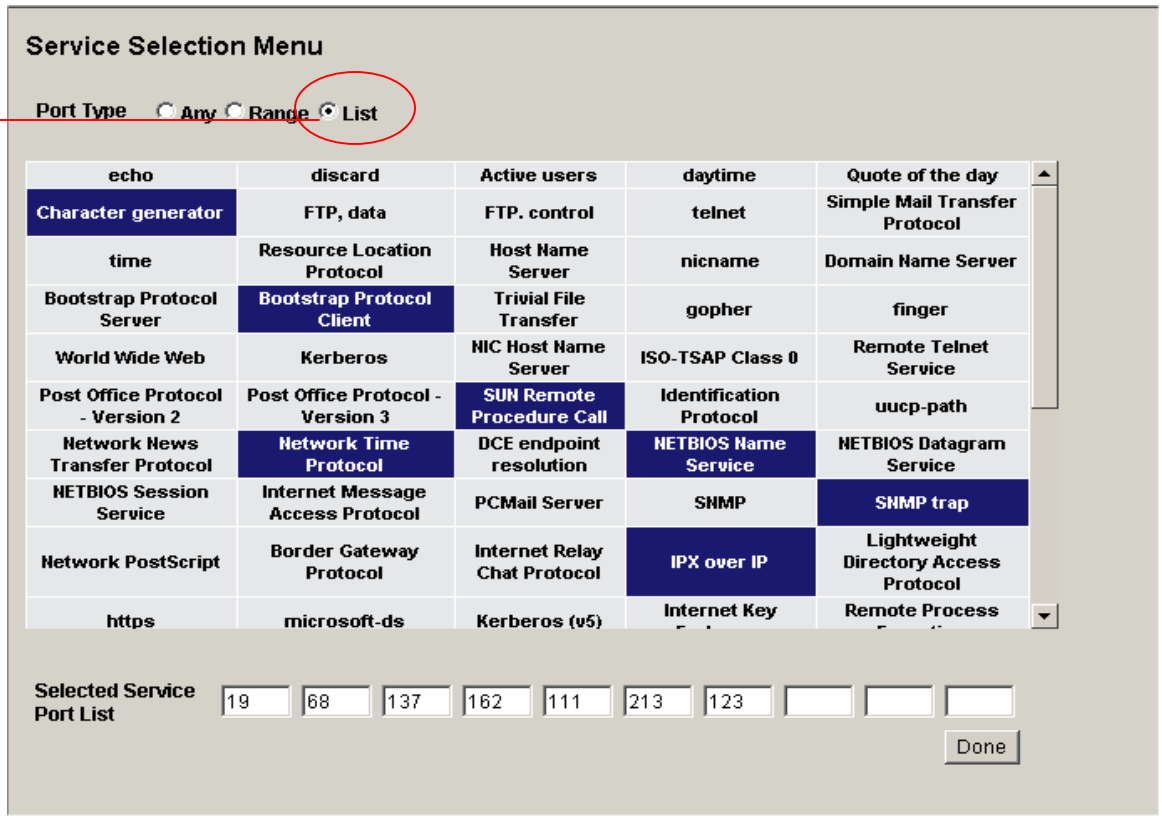
Port Type – Any: all ports are covered by this rule.

Figure 59. Firewall Configuration->Security Profiles->Basic Rules->Port settings (cont.)



Port Type – Range: this rule will work only for the ports within the defined range.

Figure 60. Firewall Configuration->Security Profiles->Basic Rules->Port settings (cont.)



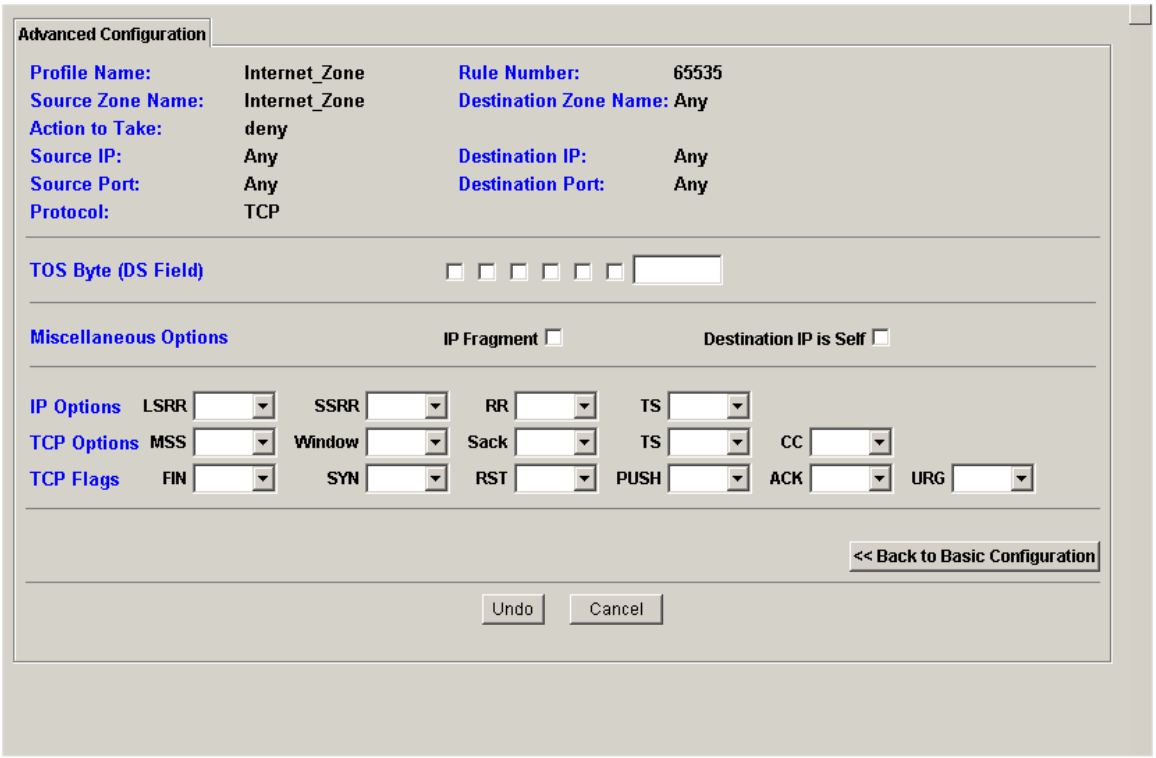
Port Type – List: the list of network ports that will be covered by this rule. The ports can be selected implicitly from the list of services (a well-defined port for the service will be assigned), or configured explicitly. Up to 10 ports are allowed for a single rule.

To save the IP Addresses and Port Settings configuration press Done button.
Control buttons for the Basic Configuration window are located at bottom of the screen.

Add Rule: saves an adds and saves a new rule.
Modify Rule: modifies and saves an existing rule.
Refresh Rule: refreshes the rules screen to show the recent changes.
Copy Rule: copies present rule (usually the rule that is opened for modification).
Paste Rule: creates a new rule with a content that was copied using **Copy Rule** button.
Advanced Configuration: opens a window for Advanced Configuration of the firewall rule.
Close Window: closes the Firewall Rules configuration window.

Advanced Configuration window:

Figure 61. Firewall Config->Security profiles->Basic (rules) Config->Advanced Configuration



Advanced Configuration fields:

Starting from a field **Profile Name** to **Destination Port Type**, the information is just a copy of the previous screen.

TOS bite (DS field) - sets a mask for Type of Service parameter
Miscellaneous Options - sets IP Fragmentation and IP self parameters.

IP Options - sets a packet mask for IP packets (additional to the rule).
TCP Options - sets a packet mask for TCP packets (additional to the rule).
TCP Flags - sets allowed or disallowed TCP communication flags.
ICMP Types Bitmap - creates a bit mask for ICMP packets.

A couple of tips. It is very helpful to start firewall configuration by creating a small table (sketch) for it:

RULE NUMBER

The rule number is a very important part of a firewall rule.

The example of the ***wrong*** placement of the rule:

Rule number 1230- action: Deny everything
Rule number 1240 – action: Allow HTTP

The rule number 1240 will never work because of the wrong order (all traffic was denied before by rule number 1230)

The example of the ***right*** placement of the rule:

Rule number 1230 -- action: Allow HTTP
Rule number 1240 – action: Deny ALL

The rule number 1230 will accept HTTP traffic, and the rule number 1240 will deny everything else.

When creating a rule leave at least 10 numbers interval between the rules for future development.

Source Zone Name Source IP settings Source Ports Do not accept more than You need.		Destination Zone Name Source IP settings Source Ports Do not open more than You need.
Make sure that direction of the rule is right (Source and Destination Zone names)		

IP Protocol settings
Advanced Configuration (if needed)
ACTION (what do you want to do with the network traffic)

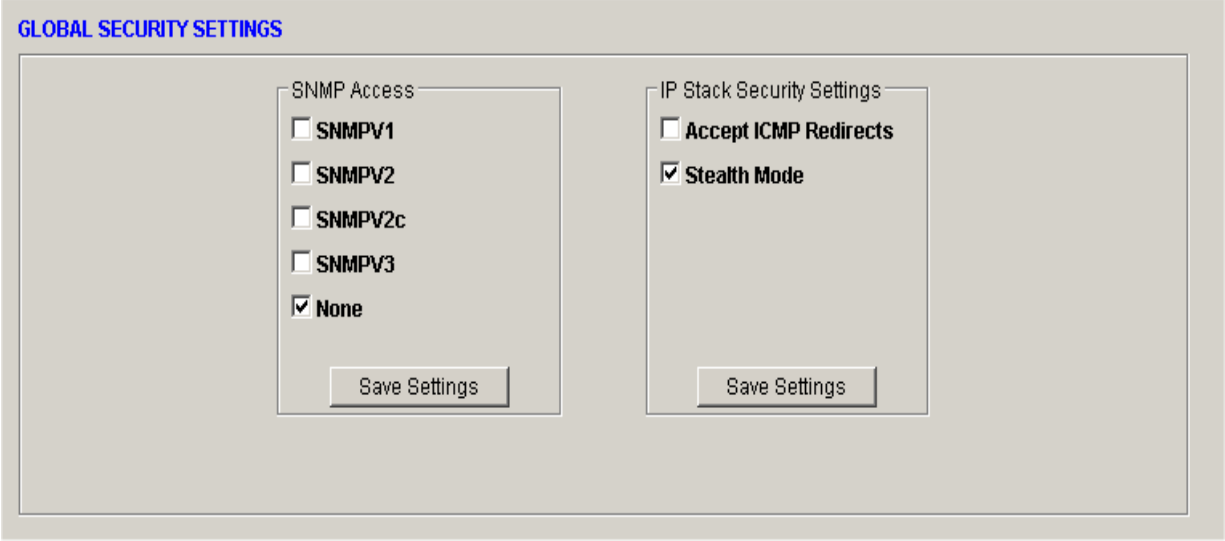
When configuring a new Security Profile, first open everything and test. After that, add the restricting rules as needed (one by one, testing the result after each addition). Adding a meaningful description makes the rules readable and manageable.

5.5 Global Security Settings

The screen bellow allows to enable/disable SNMP access to the RNxx. By default the SNMP access is disabled. To enable SNMP access user has to check one or more options for SNMP access and saved the configuration by clicking on the "Save Setting" button below the check boxes.
The second set of checkboxes on the left side allows configuring ICMP behavior.

- "Enable ICMP Errors" Enable/disable ICMP errors on the RNxx. By default this parameters is set to not to send ICMP errors.
- "Accept ICMP Redirect" Enable/Disable ICMP redirect packets on the RNxx. By default this parameter set to not to accept ICMP redirect packets.

Figure 62. Firewall Configuration->Security Profiles->Global Settings

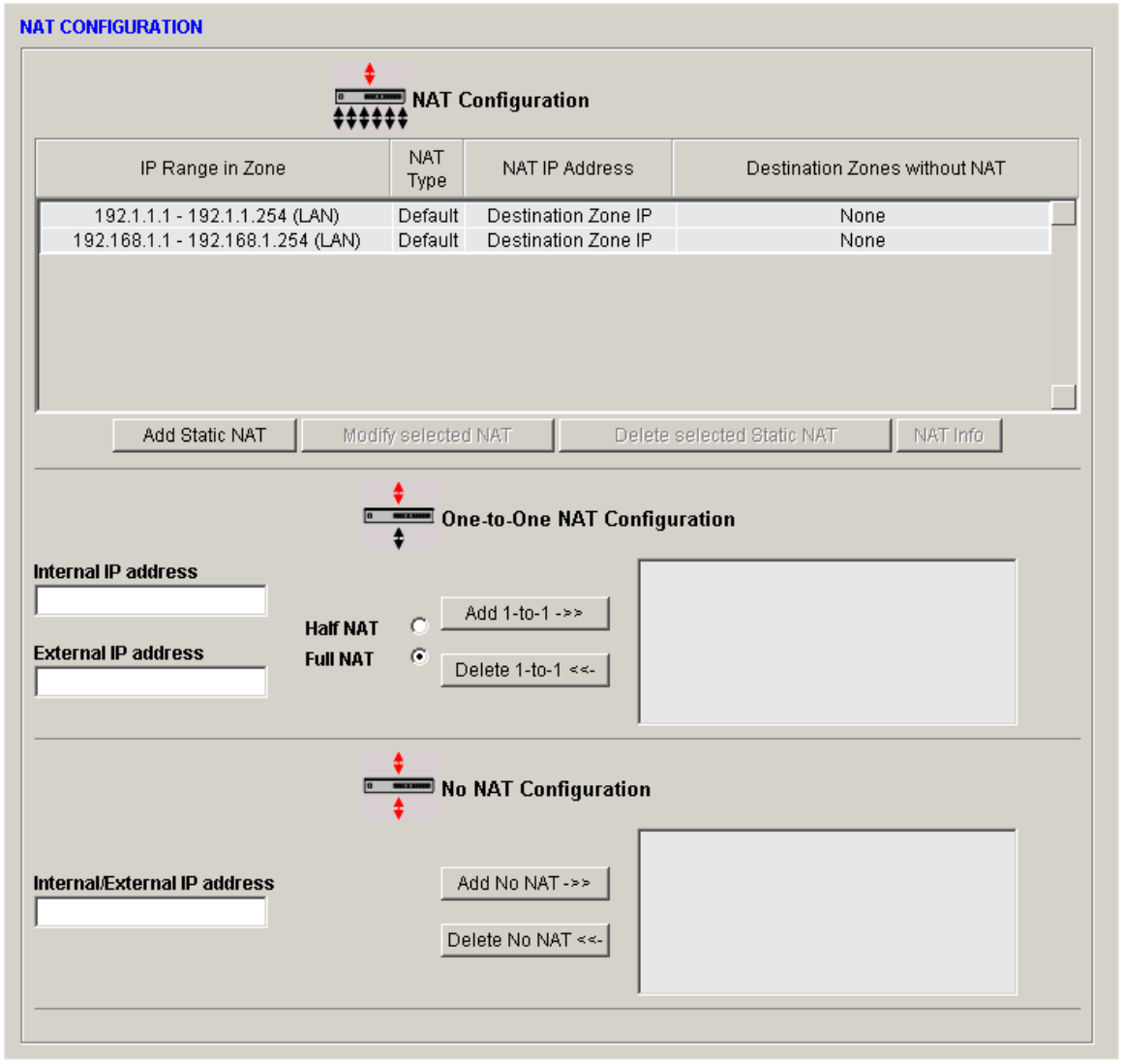


5.6 NAT Configuration

RN supports the following NAT methods:
No NAT, NAT, One-to-One Full NAT, One-to-One Half NAT.

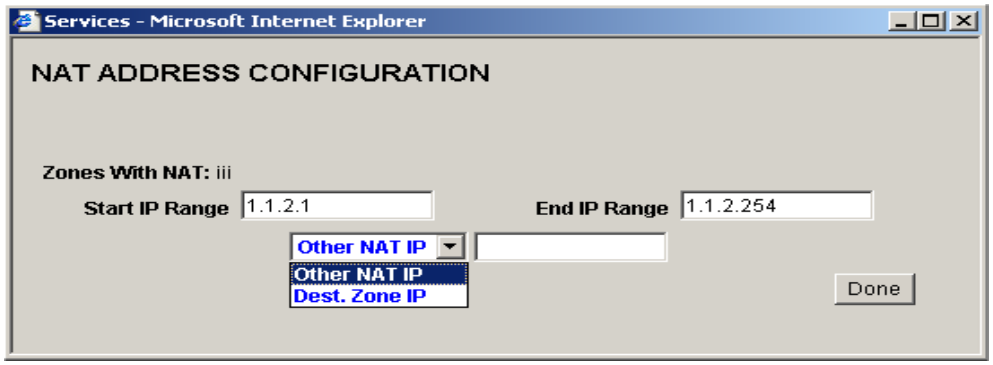
The NAT Configuration tab enables to set and configure the desired NAT mode.

Figure 63. Firewall Configuration->NAT Configuration



NAT configuration steps:
As soon as the IP interface is configured for any zone - the range of IP addresses will appear under **IP Range In Zone**. To configure NAT (many private IP addresses to one public IP address), double click on the IP address range that needs to be NATed. The following popup window will appear:

Figure 64. Firewall Configuration->NAT Configuration (cont.)

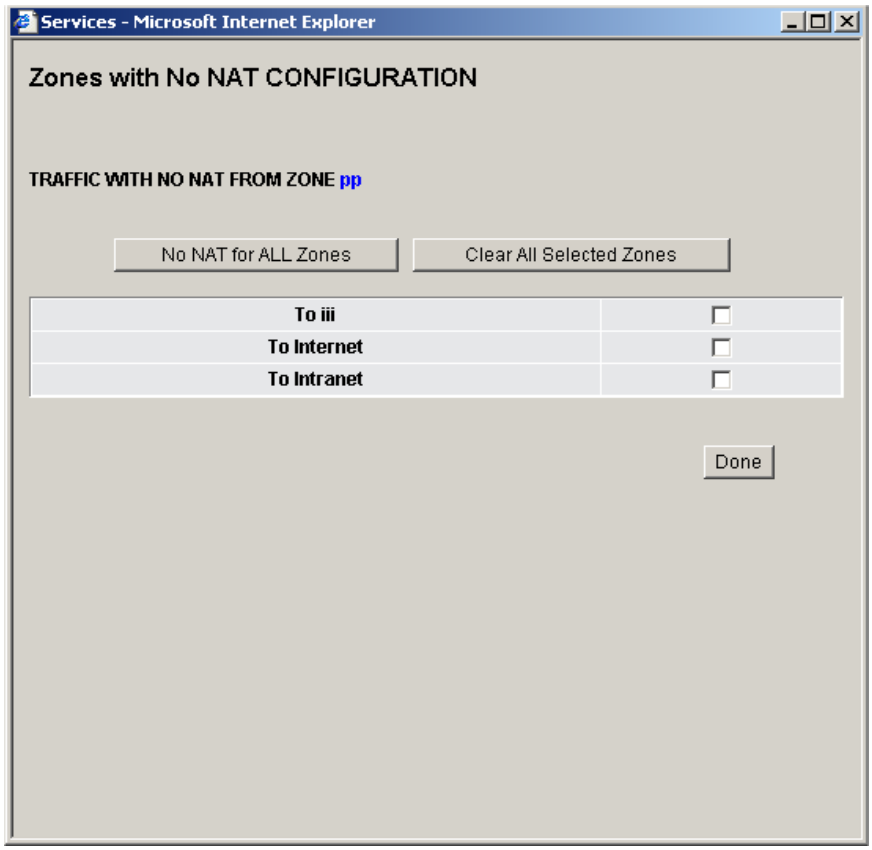


Start IP Range: the first IP address in the range.
End IP Range: the last IP address in the range.

If the option **Dest. Zone IP** is selected - the range will be NATed to the IP Address of the destination zone.
If the option **Other NAT IP** is selected - the range will be NATed to the IP Address that is defined at the field that is located next to the **Other NAT IP** option.
Press **Done** when finished.

To configure No NAT traffic between zones, double click on **Destination Zones without NAT** that corresponds to the selected range. The following window will pop up:

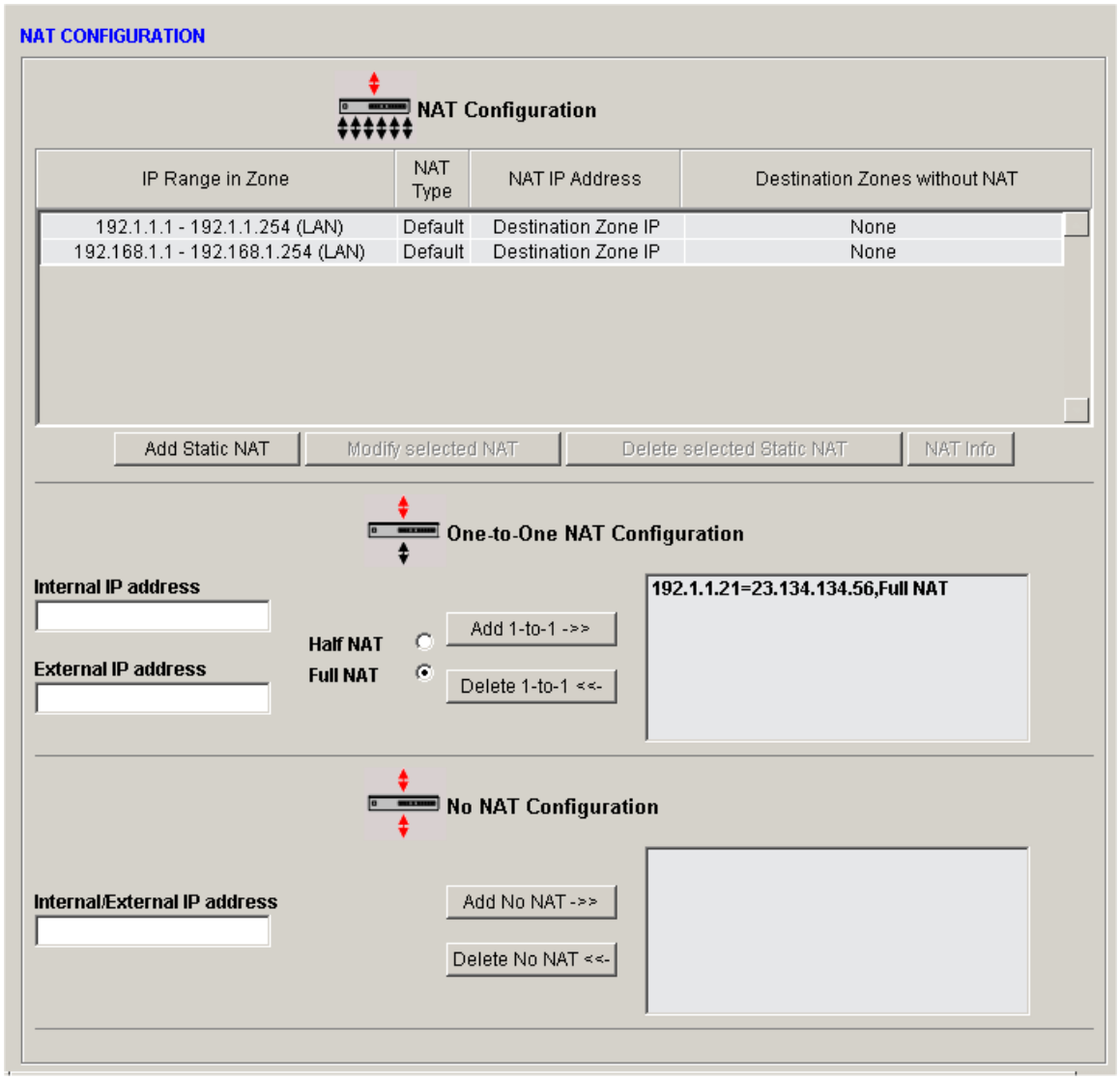
Figure 65. Firewall Configuration->NAT Configuration->Zones with No NAT Configuration



Mark the checkboxes next to the zones where traffic from the selected range will not be NATed. To configure No NAT to all zones press **No Nat To All Zones** button. Press **Done**.

One-to-one NAT configuration steps:

Figure 66. Firewall Configuration->NAT Configuration->One-to-One NAT Configuration



Enter a private IP address in the **Internal IP address** field.
Enter a public IP address in the **External IP Address** field.
Select **Full** or **Half NAT.**
Press **Add 1-to-1**.
The one-to-one configurations settings will appear in a small window next to **Add 1-to-1** button.
To remove one-to-one NAT configuration, select from the entries in this window and press **Delete 1-to-1.**

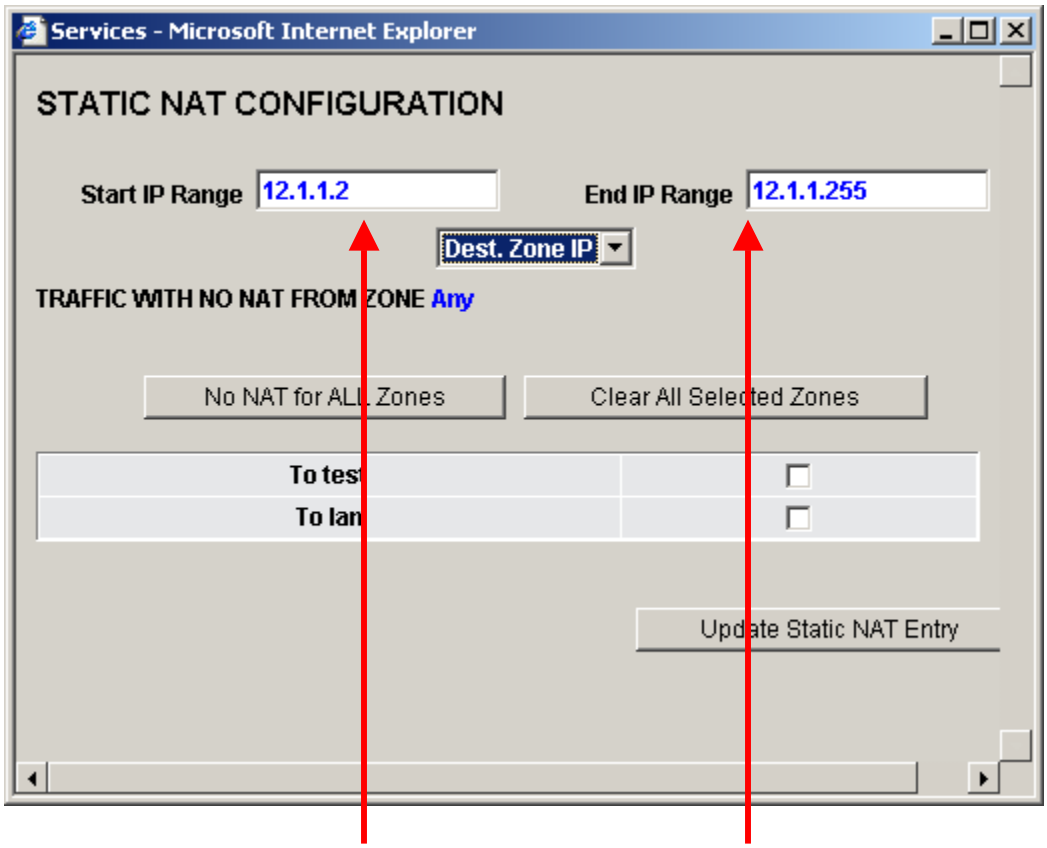
No NAT configuration steps:

Enter External or Internal IP address .
Press **Add No NAT**.
To remove No NAT configuration, select the entry and press **Delete No NAT**.

Static NAT configuration steps:

Press **Add Static NAT** button.
The small window for the Static NAT will open

Figure 67 Firewall Configuration->NAT Configuration->Static NAT Configuration



Enter the value for the Start IP range, then for the End IP Range.
Choose the NAT IP (could be the interface of the destination zone or any other IP Address). The main purpose of the static NAT is to manage the traffic from the subnets that do not belong to any of the existing zones.

5.7 DHCP Configuration

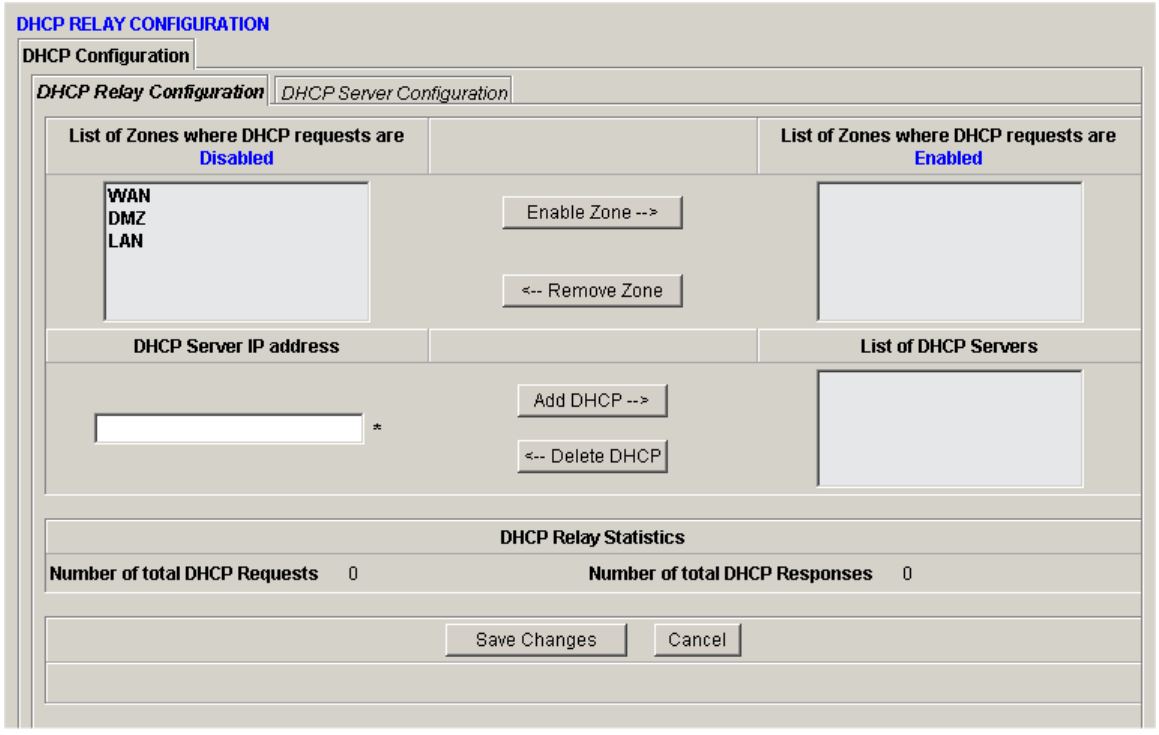
5.7.1 DHCP Relay Configuration

DHCP Relay service will intercept the DHCP Discover broadcasts, send them to the DHCP server, get the DHCP Offer reply, and return it back to the requesting client.
RN is capable of relaying DHCP messages between the clients and DHCP servers in different zones. In this role, the RN functions as the DHCP Relay Agent. Without a DHCP Relay Agent, DHCP server has to be located in every zone

In a large IP network, DHCP servers should be placed in strategic locations serving multiple clients in multiple subnets across different zones. For this configuration to work properly, DHCP messages must be between zones.

The DHCP Relay Configuration tab, allows network manager to properly configure the DHCP Relay service. By default the DHCP Relay agent is disabled for all zones. By selecting a zone and clicking on 'Enable Zone', you will activate the agent for this zone. DHCP servers have to be defined by entering their IP addresses and pressing 'Add DHCP'.

Figure 68. Firewall Configuration -> DHCP Relay Configuration

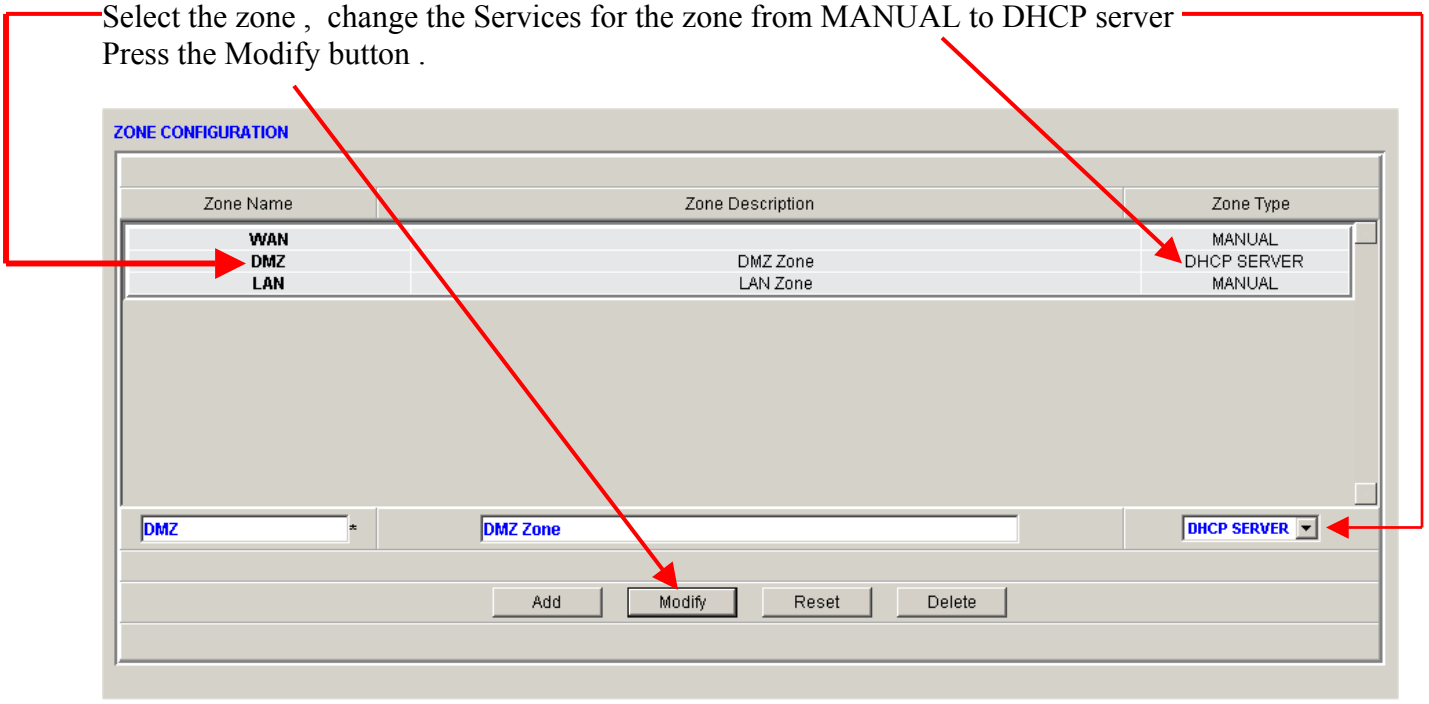


5.7.2 DHCP Server Configuration

The DHCP server is a very convenient way to automate the IP Addresses assigning and housekeeping procedures.

To configure DHCP server for the secure zone :

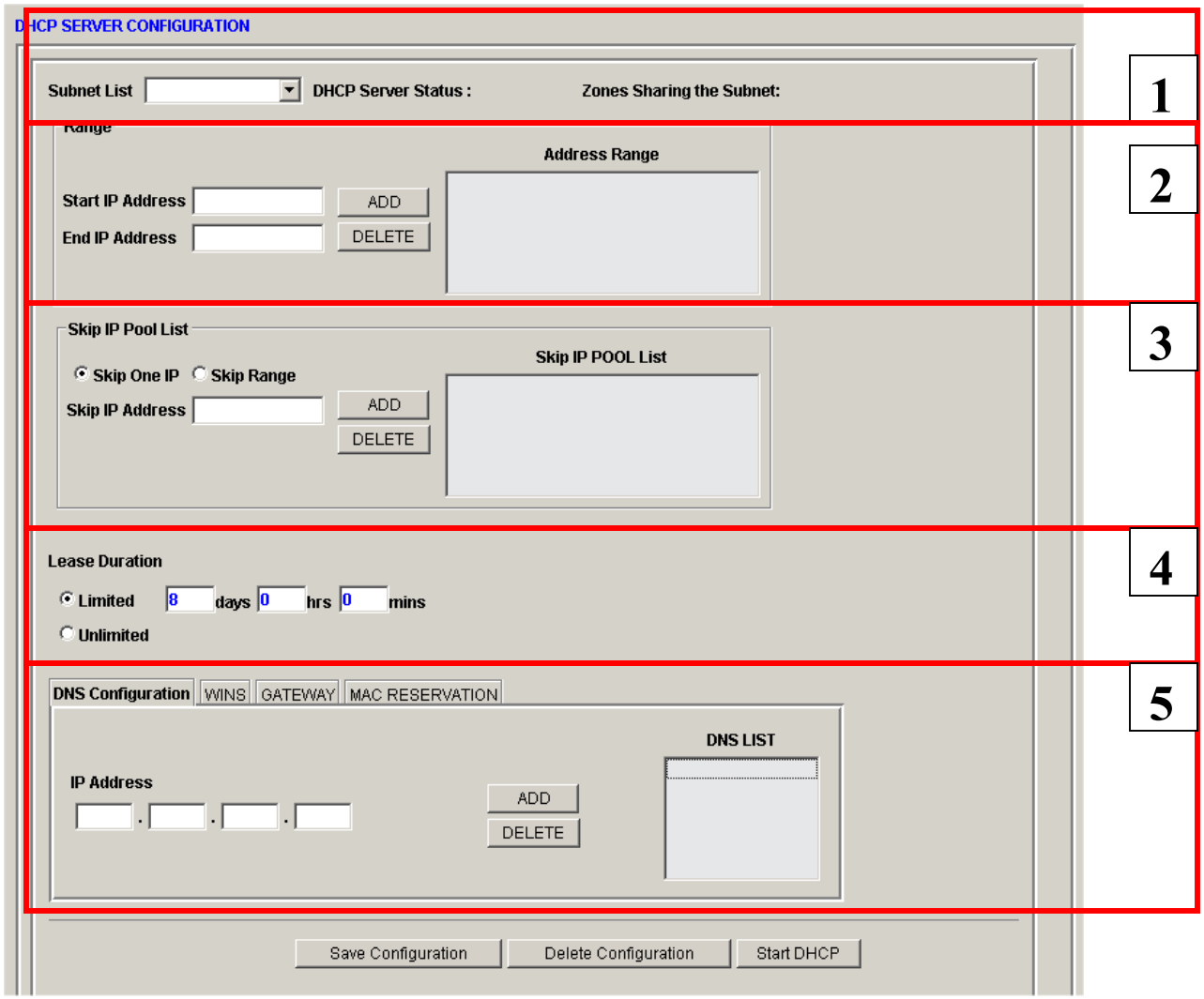
Step 1
Go to : Network Management -> Zone Configuration
Select the zone , change the Services for the zone from MANUAL to DHCP server
Press the Modify button .

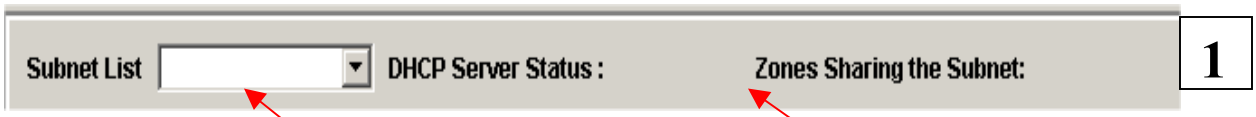


When the DHCP server is enabled for the secure zone the IP Settings for this zone will not be affected by this change.

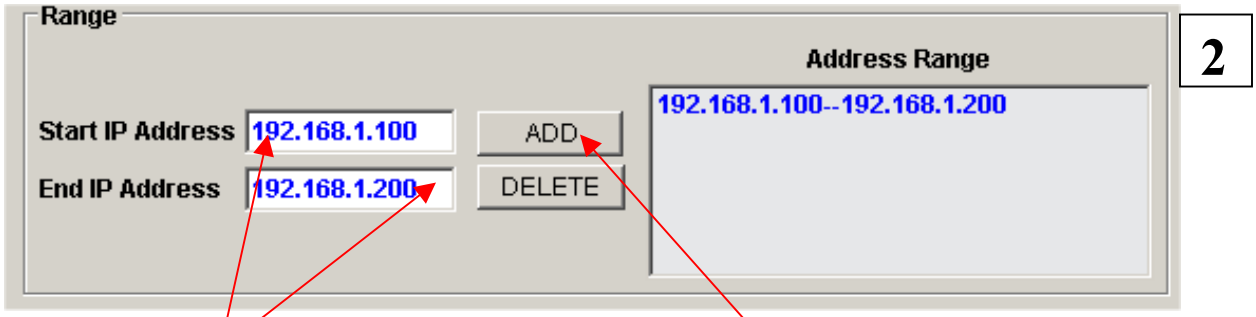
Step 2

Go to : Firewall Configuration->DHCP Configuration-> DHCP Server Configuration

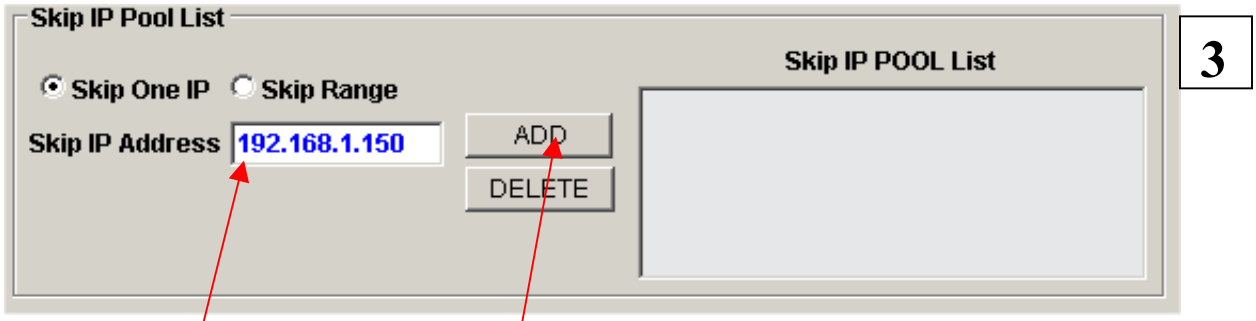




Pick up the subnet for the DHCP Zones to which that subnet belongs



Define the range of the DHCP IP Addresses and press the Add **button.**

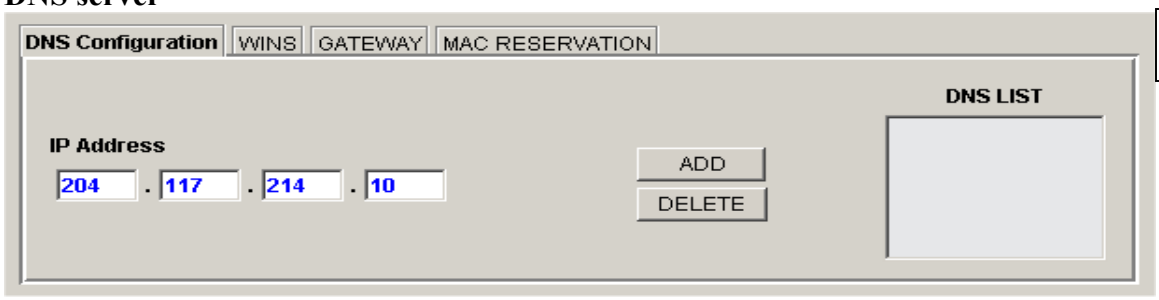


Define the IP Address (or range of the IP Addresses) that should be excluded from DHCP addresses range and press the Add **button.**

Define the Lease Duration for the assigned IP Address .

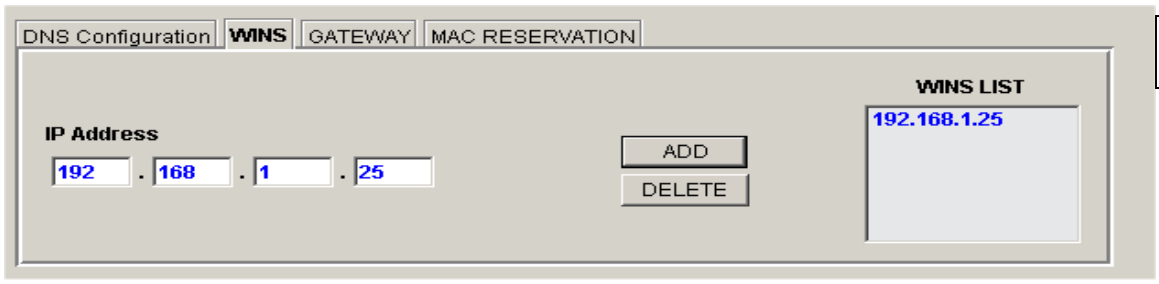
Define the additional parameters that will be sent to the host along with the IP Address :

DNS server



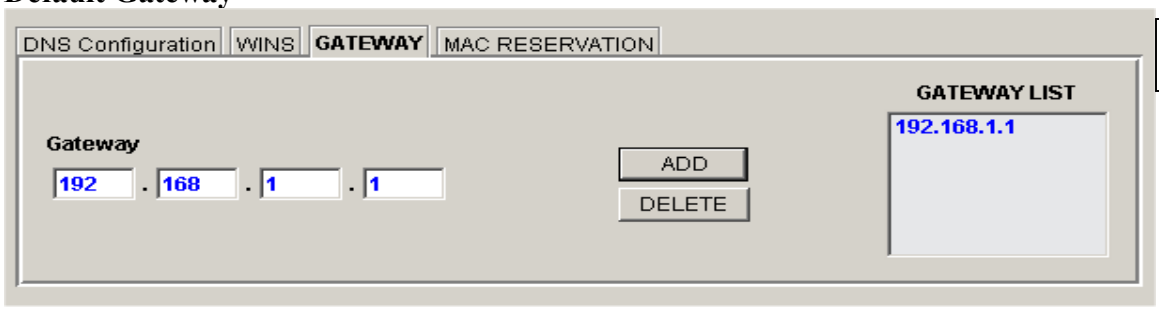
5

WINS Server



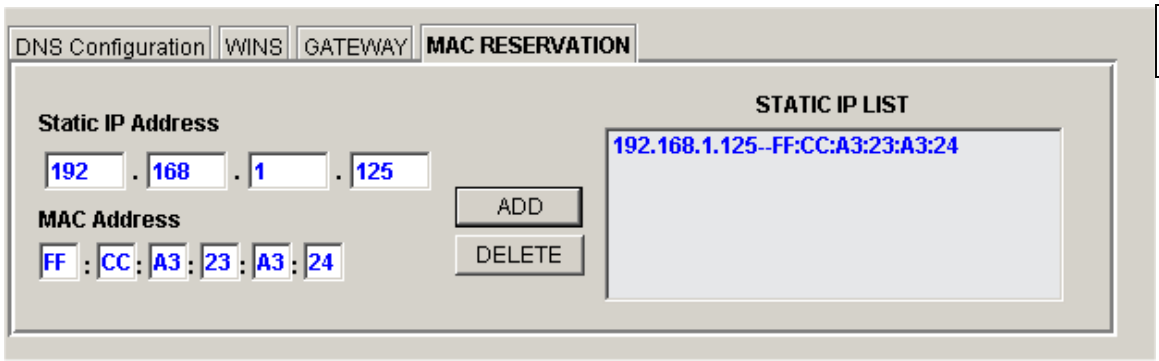
5

Default Gateway



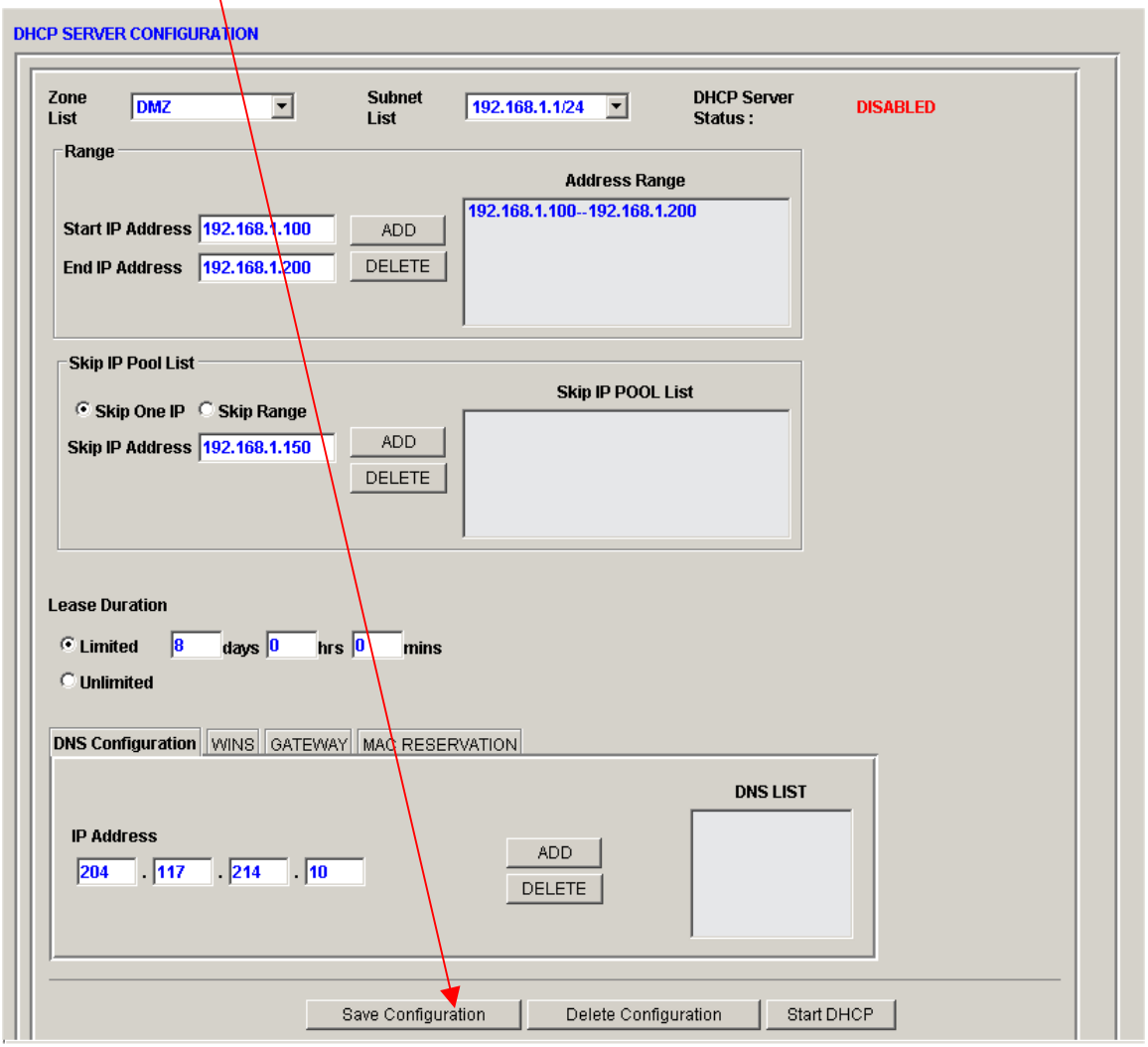
5

MAC preservation (the way to insure that some hosts will be getting the same IP Address every time when the lease will be renewed)



5

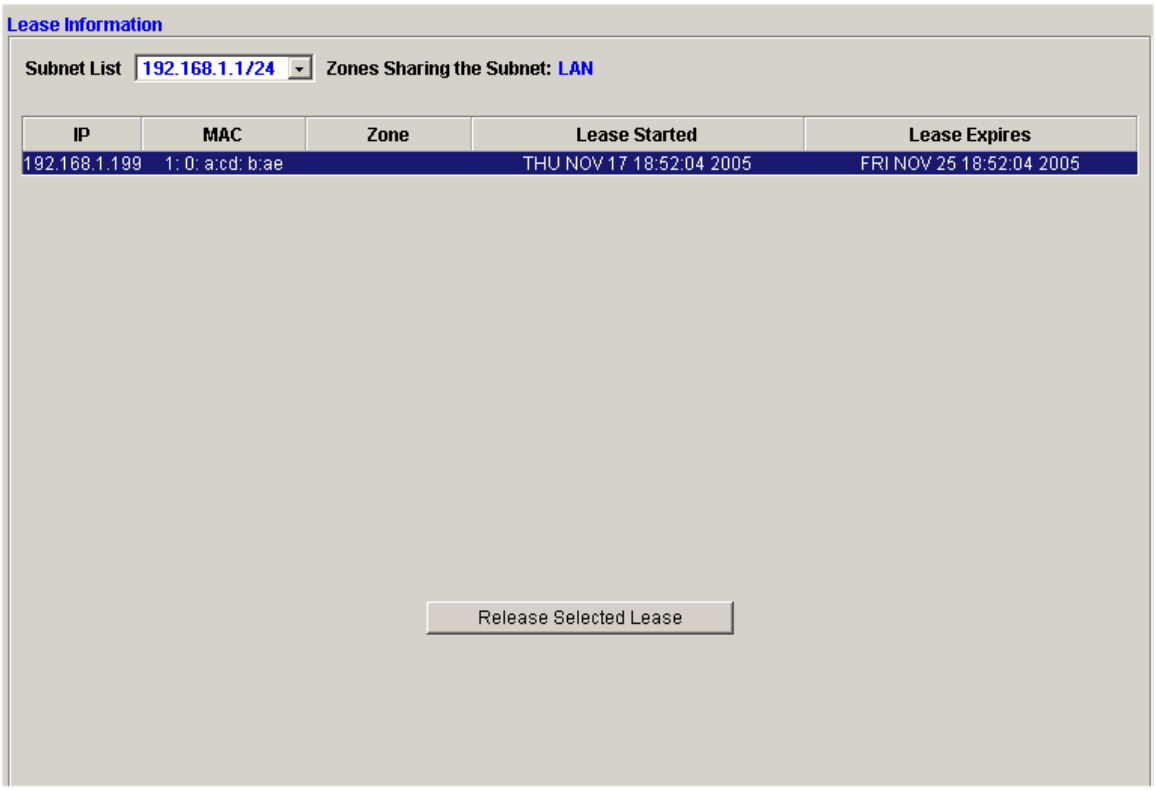
Press the Save Configuration **button**



Step 3

Press the **Start DHCP** button

DHCP Lease Info

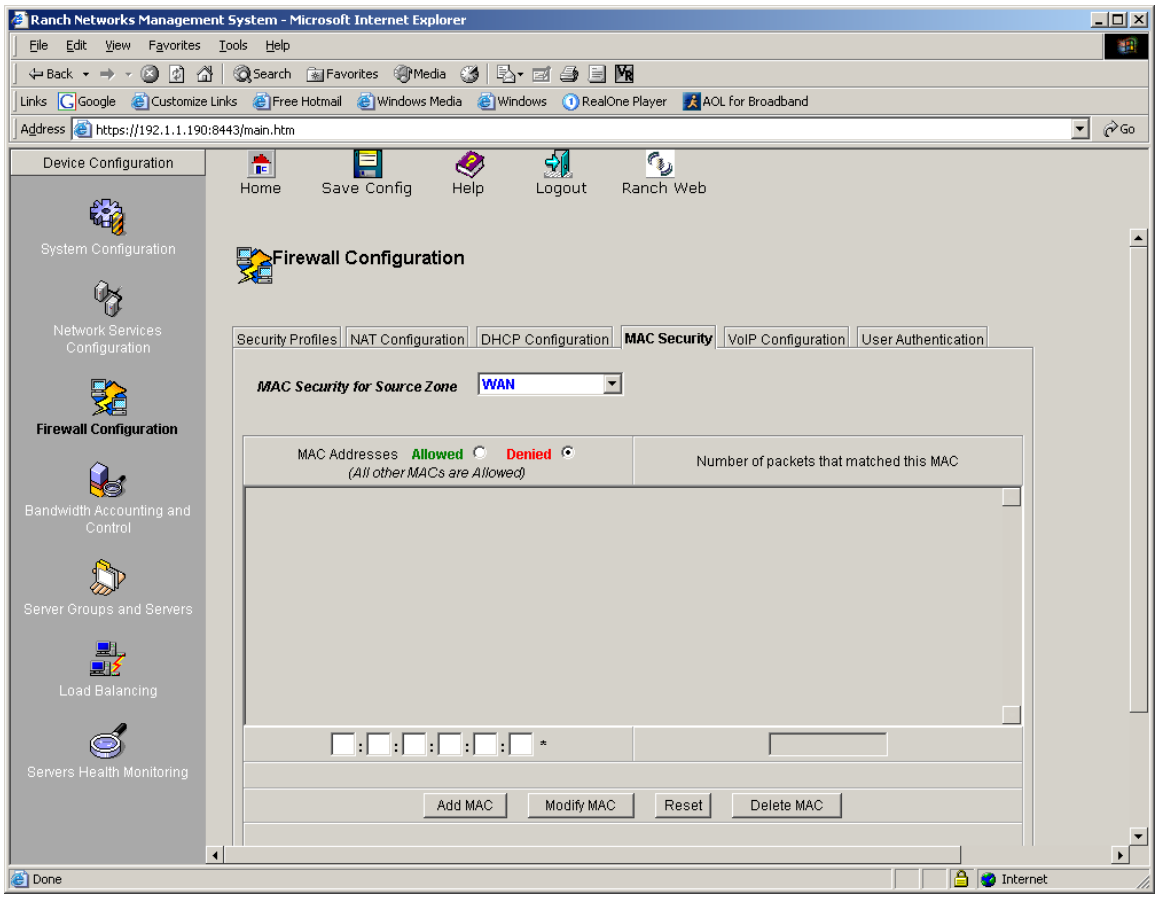


The DHCP Lease info screen shows the information about the current leases.
To terminate the lease :
Highlight the required entry and press the **Release Selected Lease** button

5.8 MAC security configuration (RN 5/20/40/41 models only)

The **MAC Security Configuration** tab is used to create security policies on the MAC level.

Figure 69. Firewall Configuration->MAC security Configuration



MAC Security fields:
Mac Security for Source Zone – the drop-down list of existing security zones.
MAC Addresses Allowed– if selected, will deny the packets with source MAC addresses that are not in the table.
All MAC Addresses Denied - if selected, will deny the packets with source MAC addresses that are listed in the table.

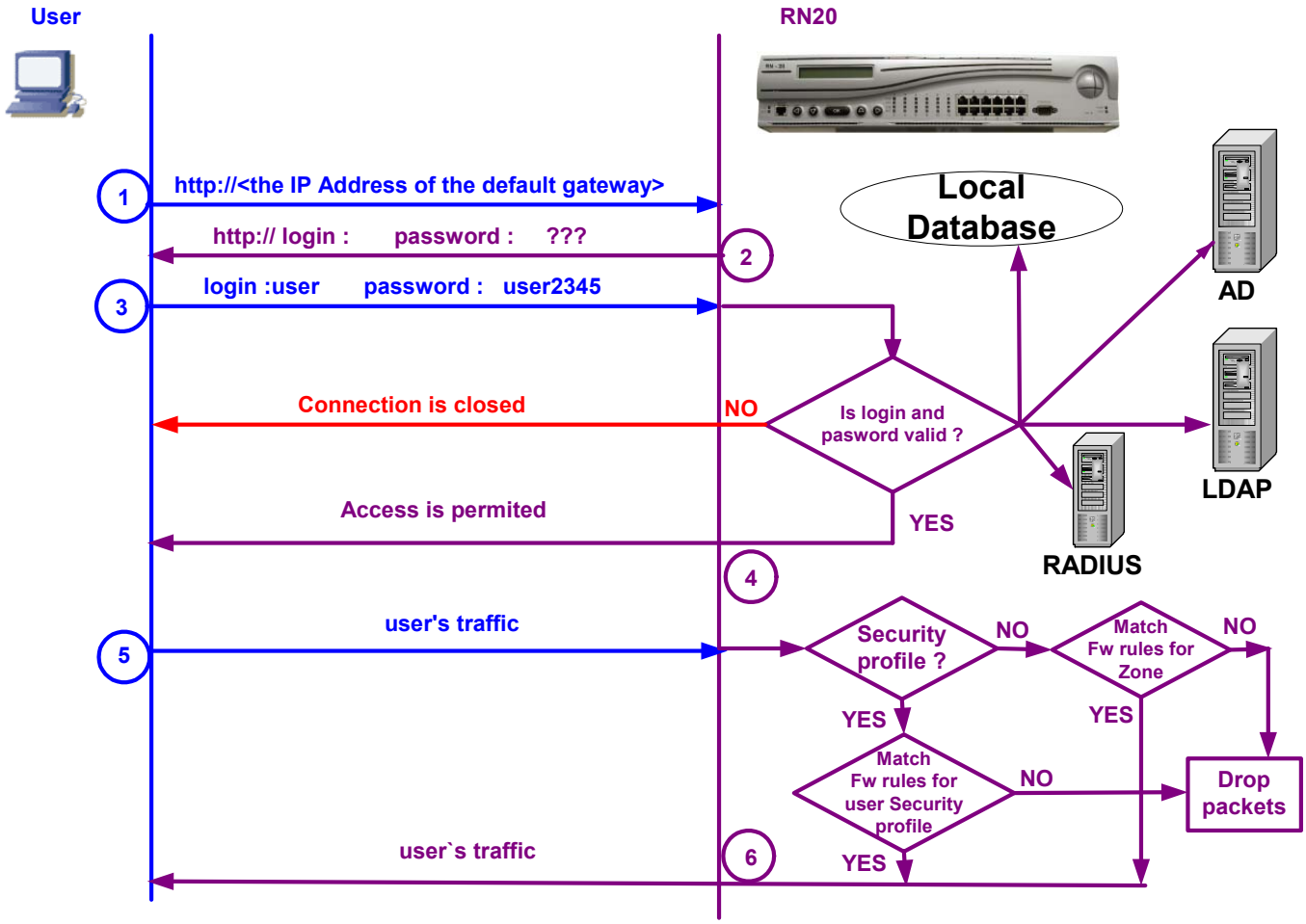
To add a record:
Type in MAC address (in group of 6 fields at the bottom of the screen), then press **Add MAC** button.

T**o modify record:**
Select the row, make changes, press **Modify** button.
To delete record:
Select the row, press **Delete** button.

5.9 User Authentication

User Authentication tab enables you to grant or reject access from specific users and IP addresses, based on their credentials. Before any traffic is allowed to pass through the unit, the user must first be authenticated. RN will use his/her credentials and the security profile to define access rights for that user.

Figure 70. User Authentication Logic



The diagram above shows the logic behind of the User Authentication.

The User Authentication window has the following four tabs:

- General configuration;

Authentication Server;

- User Configuration**;**
- User Administration;

- Session Administration.

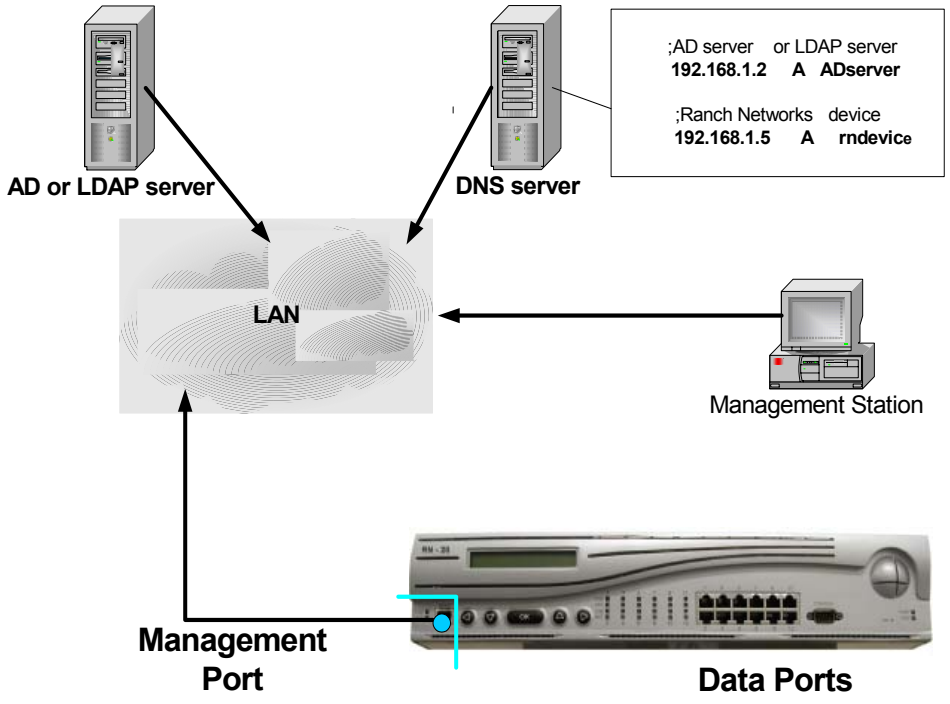
Step 1.

Configuring Authentication Servers.

RN device can authenticate the user by using credentials stored in Local Database or on the external Authentication Servers such as Active Directory, LDAP and RADUIS. So it is recommended to start configure Authentication Servers first. There are certain preparation steps for AD Server and LDAP server:

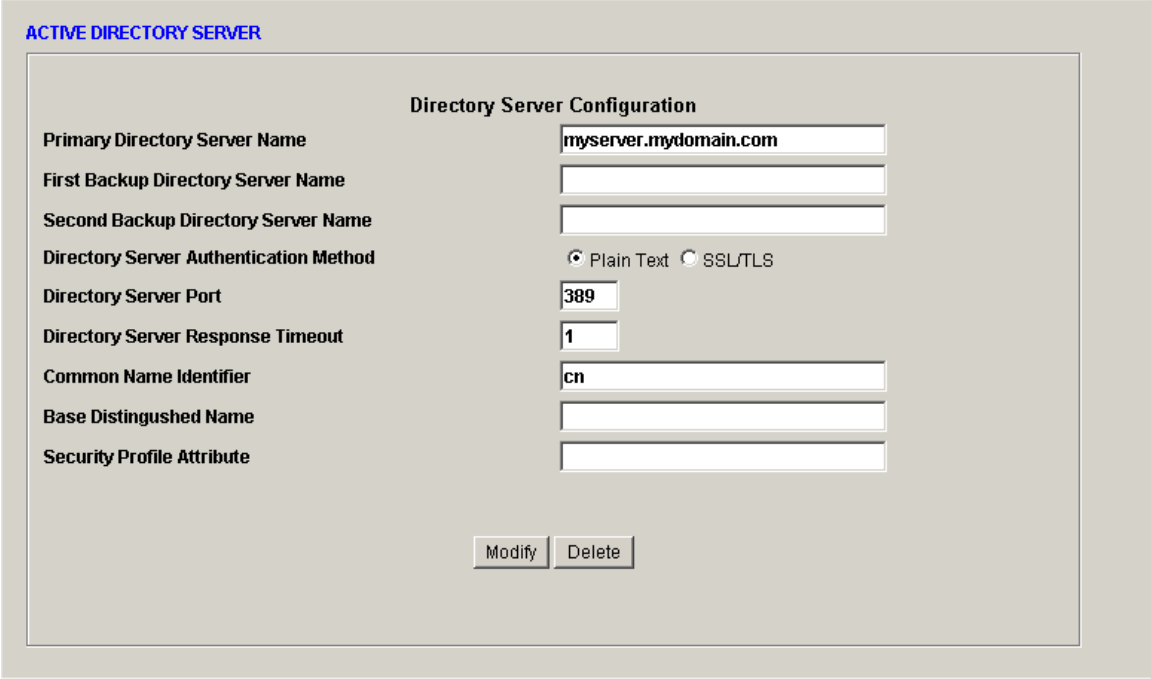
- Configure RN device hostname (see System Configuration->Management Port Configuration for more information)
- Configure the DNS servers for RN device (see System Configuration->Management Port Configuration for more information)
- Make sure AD or LDAP server and RN device is registered at DNS server (nslookup command will return the IP Address corresponding to the Server or RN hostname)

Figure 71 AD and LDAP server DNS config



Active Directory Server configuration:

Figure 72 Firewall Configuration->User Authentication-> Authentication Servers ->Active Directory Server



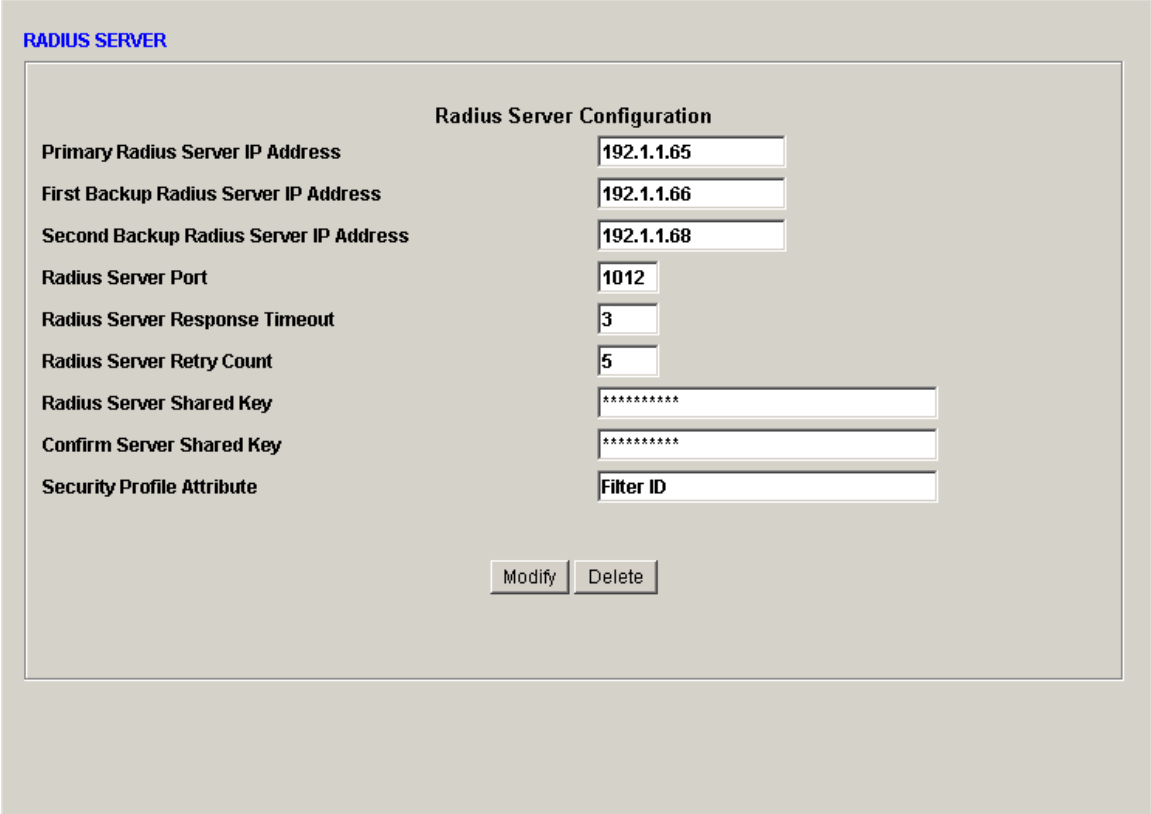
Primary Directory Server Name - Name/IP address of primary AD server
First Backup Directory Server Name - Name/IP address of secondary AD server
Second Backup Directory Server Name - Name/IP address of an additional AD server
Directory Server Authentication Method – the way to communicate with AD Server (Plain Text or SSL/TLS)
Directory Server Port - the TCP port AD Server is listening to
Directory Server Response Timeout - the time in seconds to wait for the answers

Common Name Identifier, Base **Distinguished Name** and Security **Profile Attribute** the parameters that will form the request string for AD server (see MS Windows Active Directory Reference for more information)
For example cn=**marry** - this request is about the user **marry**
cn=**users** - the user belongs to the group **users**
dc=**localdomain.com**
will result in the following request:
cn=**marry,** cn=**users,** dc=**localdomain.com**
Security Profile Attribute - the value at the description field (at AD server) could be configured to provide RN device with the name of the security profile(at RN device) that should be applied for this user.

LDAP directory server configuration
(see Active Directory Server configuration)

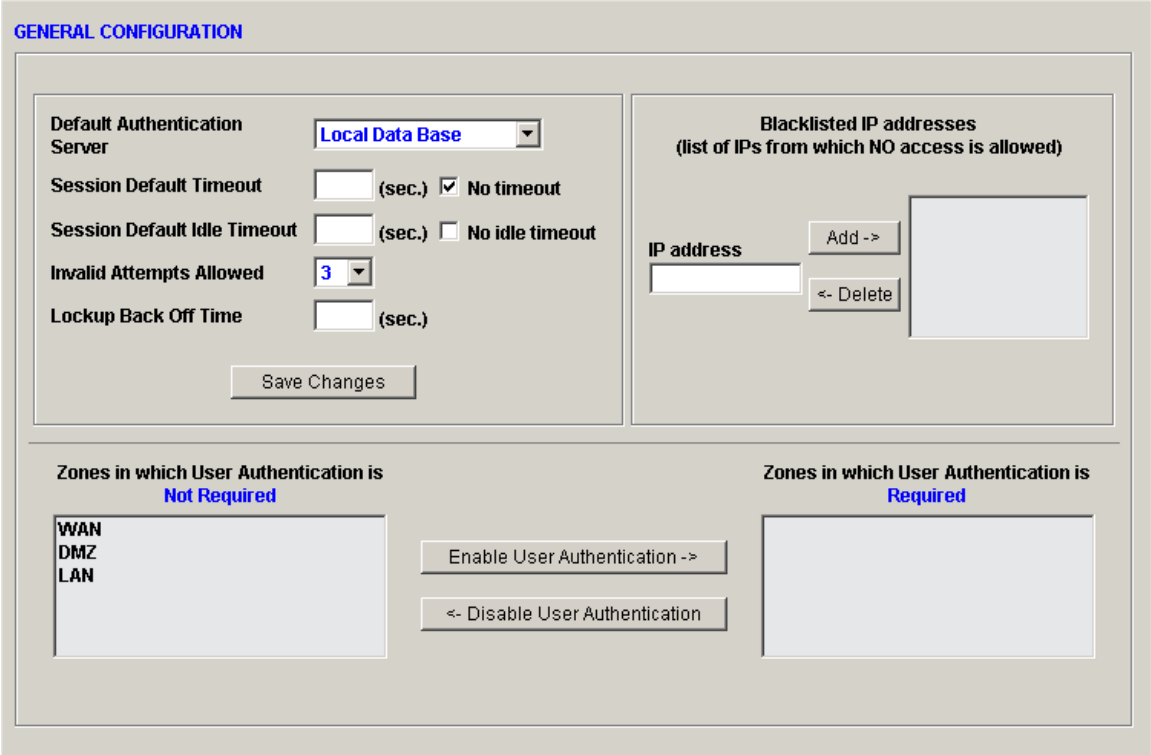
RADIUS Server configuration

Figure 73 Firewall Configuration->User Authentication-> Authentication Servers ->RADIUS server



Primary RADIUS server IP Address – the IP Address of the first RADIUS server to contact
First Backup RADIUS Server IP Address – the IP Address of the second RADIUS server to contact
Second Backup RADIUS Server IP Address – the IP Address of the third RADIUS server to contact
RADIUS Server port - the TCP port RADIUS Server is listening to
RADIUS Server Response Timeout - the time in seconds to wait for the answer
RADIUS Server Retry Count – the amount of attempts to connect to the RADIUS Server
Security Profile Attribute - the value at the Filter-ID field (Radius server) could be configured to provide RN device with the name of the security profile (at RN device) that should be applied for this user.

Figure 74. Firewall Configuration->User Authentication->General Configuration



Step 2.
General Configuration tab sets the system-wide authentication parameters.

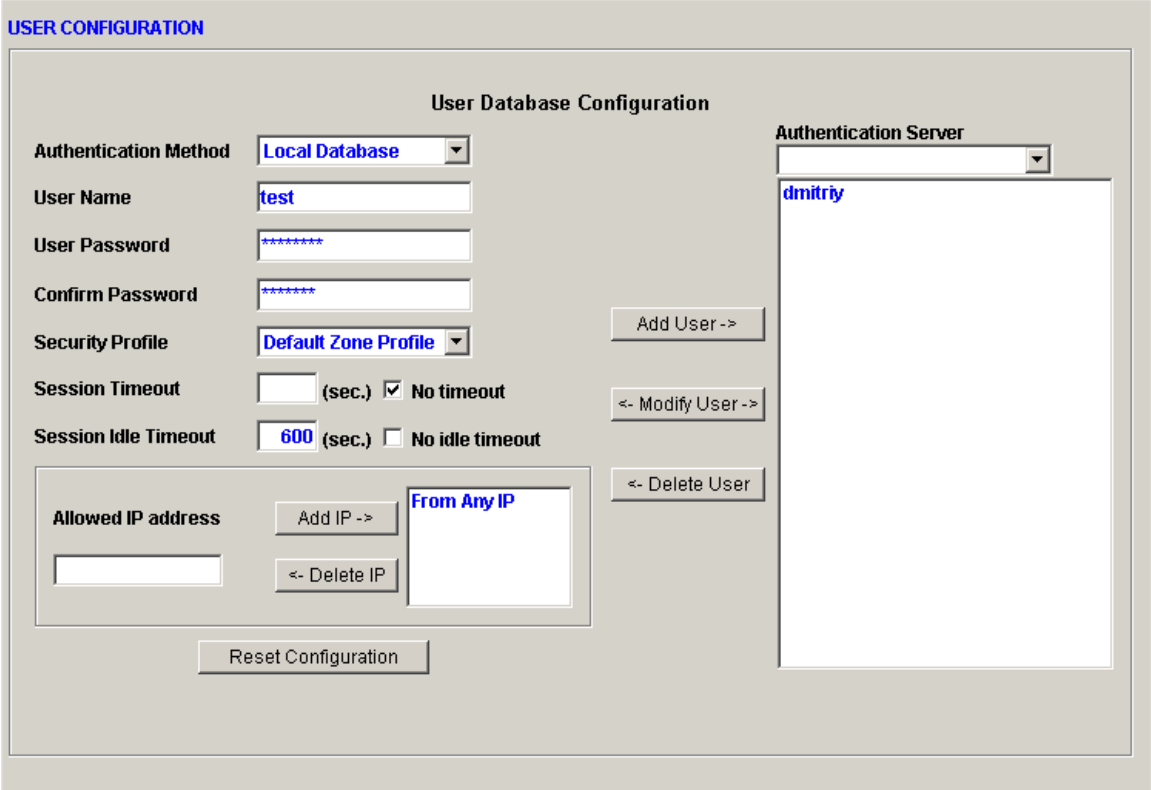
Fields Description:
Default Authentication Server: the server or the local database that performs user authentication.
Session Default Timeout: the user session will be terminated when this timeout expires (in seconds).
Session Default Idle Timeout: the idle user session will be terminated, when this timeout expires (in seconds).
Invalid Attempts Allowed: the number of the unsuccessful login attempts that will cause RN to lock the user account for the time(in seconds) configured in **Lockout Back Off Time.**
Blacklisted IP Addresses: the list of IP addresses that are not allowed to traverse the zones.
To add IP address to the list, type in the address in the input field and press **Add.**
To remove IP Address from the list, select the address and press **Delete.**
Zones in which User Authentication is not required: the list of zones with no user authentication.

Zones in which User Authentication is required: the list of zone with required user authentication.
To enable User Authentication in the zone:
Select the zone from the **Zones in which User Authentication is not required** and press **Enable User Authentication**.
To disable User Authentication in the zone:
Select the zone from the **Zones in which User Authentication is required** and press **Disable User Authentication**.

When all the parameters are set, press **Save Changes** button.

Step 3.
User Configuration tab enables network manager to administer the User Database.

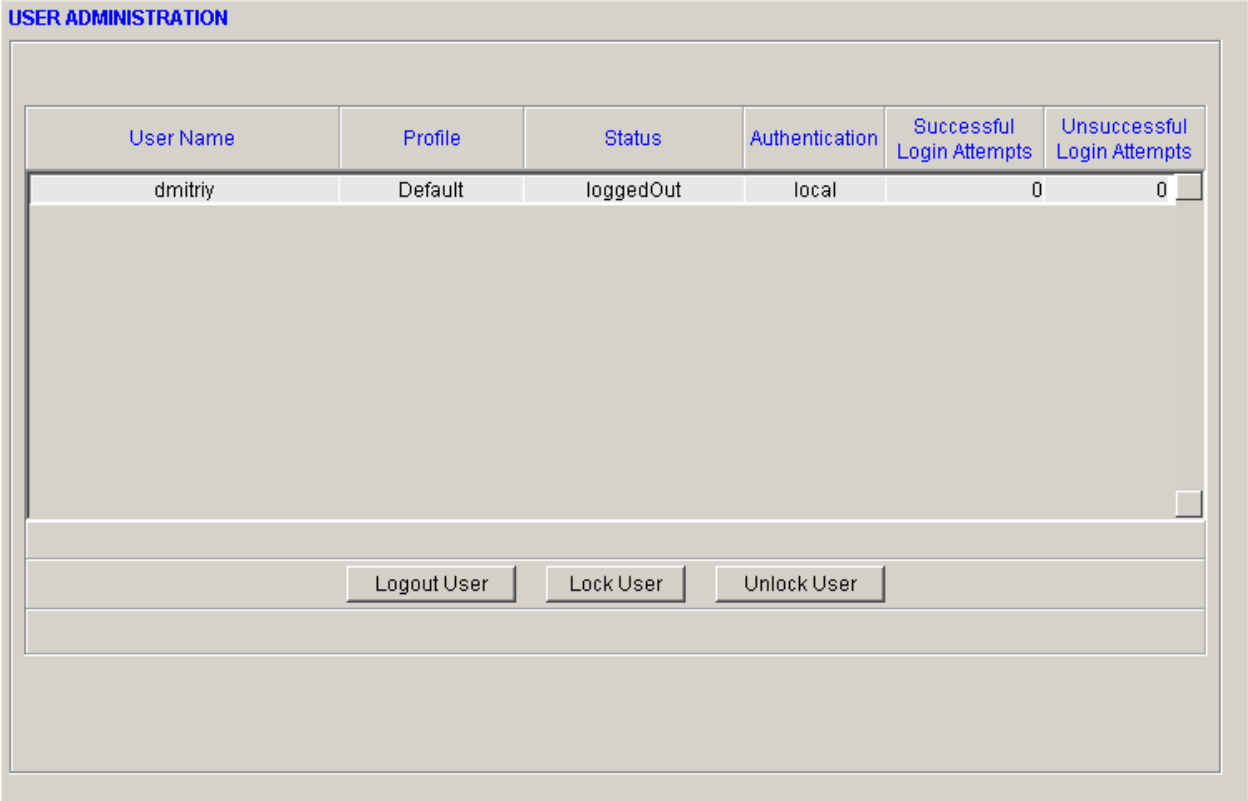
Figure 75.Firewall Configuration->User Authentication->User Configuration



Fields Description:
User Name: the name (login) for the user;
User password: the password for the user;
Security Profile: security profile name, which will be used for the user (the default profile for the zone or a separately created profile could be used)
Session Timeout: the user session will be terminated after this timeout expires (in seconds); this setting will overwrite the **Session Default Timeout** for the zone that this user is coming from.

Session Idle Timeout: the idle user session will be terminated after this timeout expires (in seconds); these settings will overwrite the **Session Default Idle Timeout** for the zone that this user is coming from.
If the checkboxes next to **Session Timeout** or **Session Idle Timeout** are checked, the user will not have time limitation for the active and/or idle sessions.
Allowed IP Addresses: the list of IP addresses that the user must initiate authentication from.
Authentication Server: the server or the local database that contains the user credentials; this setting will overwrite **Default Authentication Server** setting.
To add the user: enter all settings and press **Add User**.
To modify the user settings: select the user, make changes and press **Modify User**.
To delete the user: select the user and press **Delete User**.
The next two screens are the users and sessions statistics and operations tools.
User Administration:

Figure 76. Firewall Configuration->User Authentication->User Administration

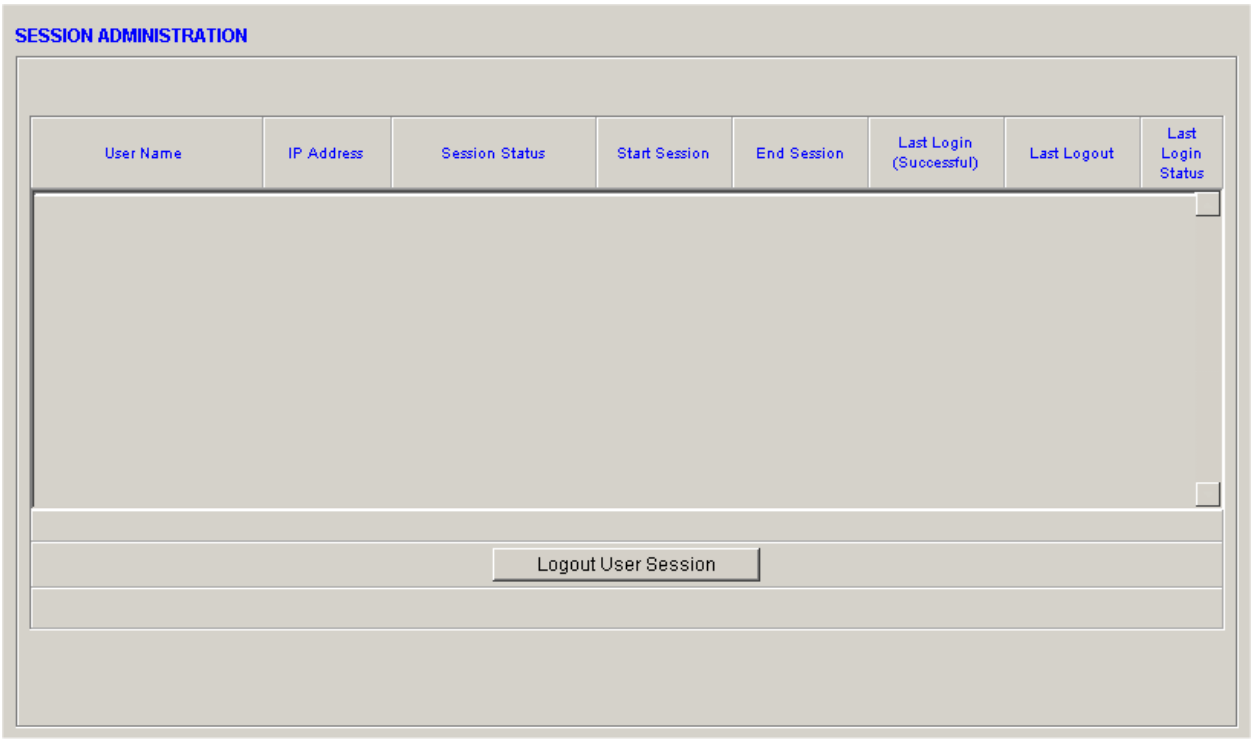


Fields Description:
User Name: the name of the user.
Profile: the security profile that was used for this user.
Status: the real-time status of the session.
Authentication: this field shows whether a remote server or the local database was used.
Successful Login Attempts: the number of successful logins from this user.
Unsuccessful Login Attempts: the number of the failed login attempts from this user.

To logout the user: select the row from the table and press **Logout User**.
To lock (disable) the user: select the row from the table and press **Lock User.**
To unlock (enable) the user: select the row from the table and press **Unlock User.**

Session Administration:

Figure 77. Firewall Configuration->User Authentication->Session Administration



Fields Description:
User Name: the name of the user.
IP Address: the address that was used for this session.
Session Status: the real-time status of the session.
Start Session: the time and the date when the session started.
End Session: the time and the date when the session ended;
Last Login: the time and the date of the last successful login;
Last Login Status: the status of the last login attempt.

6. VPN Configuration

6.1 VPN overview

A VPN is a secure, private communication tunnel between `two or more devices across a public network (like the Internet). These VPN devices can be either a computer running VPN software or a special device like a VPN enabled router.

Even though a VPNs data travels across a public network like the Internet, it is secure because of very strong encryption. If anyone listens to the VPN communications, they will not understand it because all the data is encrypted. In addition, VPNs monitor their traffic in very sophisticated ways that ensure packets never get altered while traveling across the public network.

A Ranch Networks VPN implementation is based on the IPSec suite of the protocols.
IPSec presents two modes and two main protocols:

Transport and tunnel modes
The Authentication Header (AH) protocol

The RN device supports transport and tunnel modes and AH protocol.

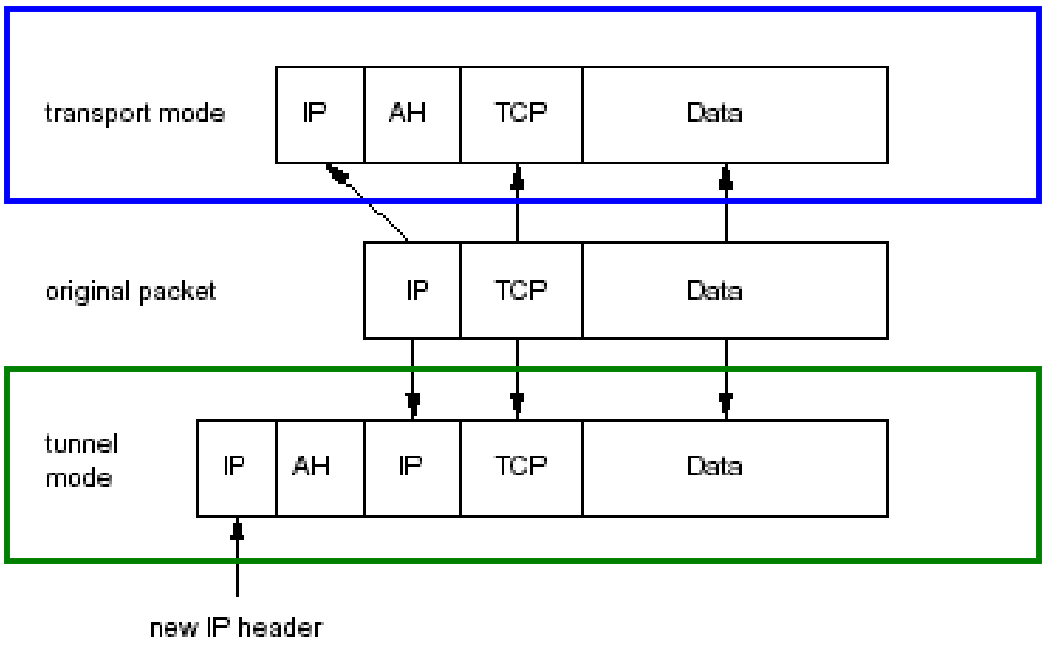
6.2 IPSec primer

IPsec is an extension to the IP protocol which provides security to the IP and the upper-layer protocols. It was first developed for the new IPv6 standard and then turned to IPv4. The IPsec architecture is described in the RFC2401.

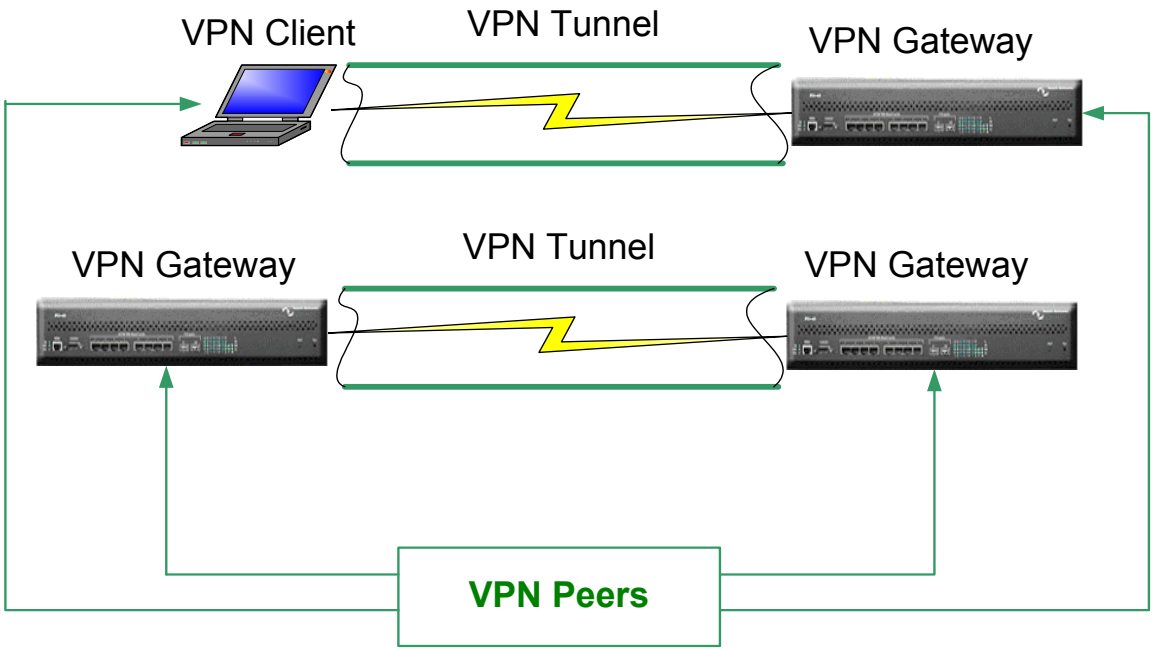
As was mentioned before IPsec uses two different protocols - AH and ESP
It can protect either the entire IP datagram or only the upper-layer protocols. The appropriate modes are called tunnel mode and transport mode.

In tunnel mode the IP datagram is fully encapsulated by a new IP datagram using the IPsec protocol.

In transport mode only the payload of the IP datagram is handled by the IPsec protocol inserting the IPsec header between the IP header and the upper-layer protocol header



For the peers to be able to encapsulate and decapsulate the IPsec packets they need a way to store the secret keys, algorithms and IP addresses involved in the communication. All these parameters needed for the protection of the IP datagrams are stored in a security association (SA). The security associations are in turn stored in a security association database (SAD).



Each security association defines the following parameters:

- Source and destination IP address of the resulting IPsec header. These are the IP addresses of the IPsec peers protecting the packets.
- IPsec protocol (AH or ESP), sometimes compression (IPCOMP) is supported, too.
- The algorithm and secret key used by the IPsec protocol.
- Security Parameter Index (SPI). This is a 32 bit number which identifies the security association.
- Some implementations of the security association database allow further parameters to be stored:
- IPsec mode (tunnel or transport)
- Size of the sliding window to protect against replay attacks.
- Lifetime of the security association.

Since the security association defines the source and destination IP addresses, it can only protect one direction of the traffic in a full duplex IPsec communication. To protect both directions IPsec requires two unidirectional security associations.

The security associations only specify how IPsec is supposed to protect the traffic. Additional information is needed to define which traffic to protect when. This information is stored in the security policy (SP) which in turn is stored in the security policy database (SPD).

A security policy usually specifies the following parameters:

- Source and destination address of the packets to be protected.
- The protocol (and port) to protect.
- The security association to use for the protection of the packets.

The manual setup of the security association is quite error prone and not very secure. The secret keys and encryption algorithms must be shared between all peers in the virtual private network.
Especially the exchange of the keys poses critical problems for the system administrator: How to exchange secret symmetric keys when no encryption is yet in place?

To solve this problem the internet key exchange protocol (IKE) was developed. This protocol authenticates the peers in the first phase. In the second phase the security associations are negotiated and the secret symmetric keys are chosen using a Duffle Hellmann key exchange.

6.3 IKE Overview

The IKE suite of protocols allows a pair of security gateways to:

- Dynamically establish a secure tunnel over which the security gateways can exchange tunnel and key information.
- Set up user-level tunnels or SAs, including tunnel attribute negotiations and key management. These tunnels can also be refreshed and terminated on top of the same secure channel.

Main Mode and Aggressive Mode

IKE phase 1 negotiations are used to negotiate keys. The two IKE peers then use these keys to communicate securely during phase 2 negotiations. IKE uses several modes for phase 1 negotiations: main mode, aggressive mode, and quick mode. You can use main mode or aggressive mode to establish the initial secure tunnels between two security gateways. After that, quick mode can be used to establish and refresh user-level SAs.

The choice of main or aggressive mode is a matter of tradeoffs. Some of the characteristics of the two modes are:

Main mode (recommended)

- Protects the identities of the peers during negotiations and is therefore more secure.
- Allows greater proposal flexibility than aggressive mode.
- Is more time consuming than aggressive mode because more messages are exchanged between peers.

Aggressive mode

- Is faster than main mode.

Exposes identities of the peers to eavesdropping, making it less secure than main mode.

6.4 NAT Traversal overview

Traditionally, IPSec is incompatible with NAT. By using NAT Traversal protocol IPSec traffic can pass through a NAT device.

A new technology known as IPsec NAT Traversal (NAT-T) has been standardized by the **IP Security Protocol Working Group** of the **Internet Engineering Task Force** (IETF) and is defined in **Requests for Comments (RFCs) 3947** and **3948**.

IPsec NAT-T defines both changes in the negotiation process and different methods of sending IPsec-protected data.

To create a VPN from behind a NAT device, the IPSec gateway behind the NAT device, and the gateway in the non-NAT environment must support NAT-T. NAT-T IPSec peers first detect if there is a NAT device between them. This is done in the key negotiation process, and it requires additional messages to be sent.

After two IPSec peers agree that NAT-T is needed, one new and two extra headers will encapsulate IPSec packets between them .

IPsec packet

Original outer IP header	ESP header	Original inner IP header	IP data	ESP trailer	ESP auth

NAT-T IPsec packet

New IP header	UDP header	NAT-T header	ESP header	Original inner IP header	IP data	ESP trailer	ESP auth

The new IP header is the same as the original IPSec outer header except the protocol is changed from AH/ESP to UDP. The UDP header has source port 500, destination port equals to the public IKE port of the peer. This makes the peer think this is an IKE packet. NAT-T works only if the NAT devices along the route between the two IPSec gateways maintain the same address mapping since the last IKE negotiation. The “keepalive” is sent to keep the NAT devices from removing the mapping entries.

6.5 Ranch Networks VPN configuration.

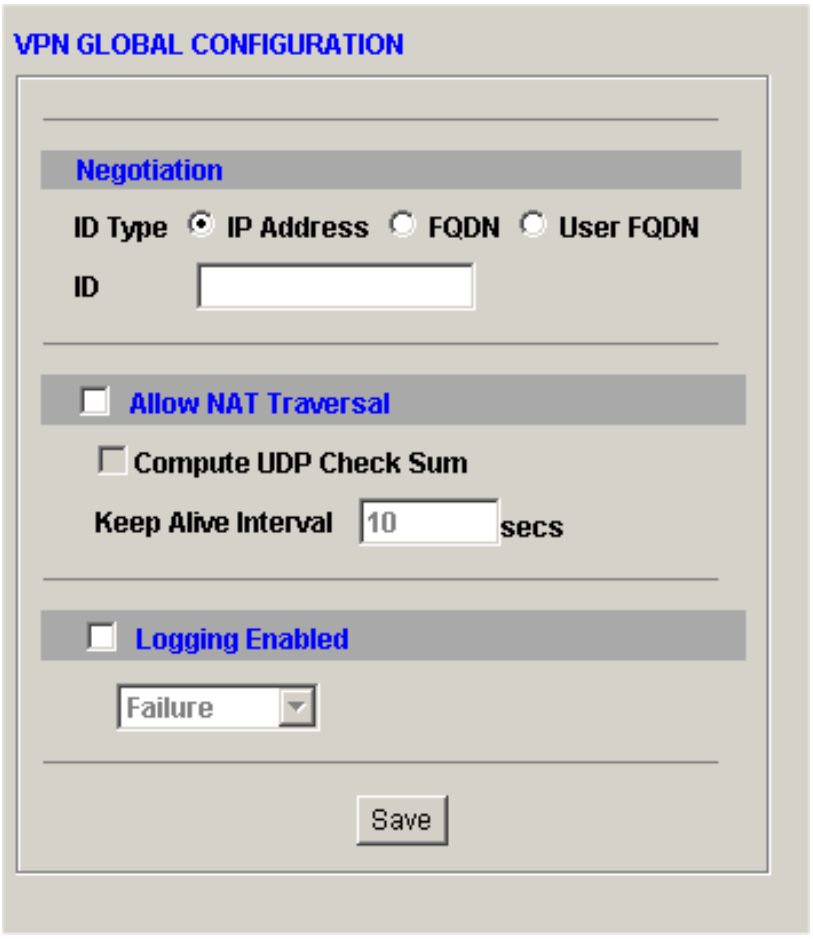
RN VPN configuration consists of:

VPN Global Configuration - The default settings that will be applied to the every configured VPN tunnel.

VPN Tunnel Set Up - The settings for the specific VPN tunnel .

6.5.1 VPN Global Configuration.

Figure 78 VPN->VPN Global Configuration



The VPN Global Configuration defines the following parameters:

Negotiation ID
The unique ID that will represents RN device in the IKE negotiation.
The negotiation ID could be:
IP Address - the IP Address of the RN Device
FQDN - A *fully qualified domain name* of the RN device that consists of a host and domain name, including top-level domain.

User FQDN - A *fully qualified domain name* of the user that consists of a host and domain name, including top-level domain.

Allow NAT Traversal
If checked, RN device will use the NAT Traversal for the all configured tunnels.

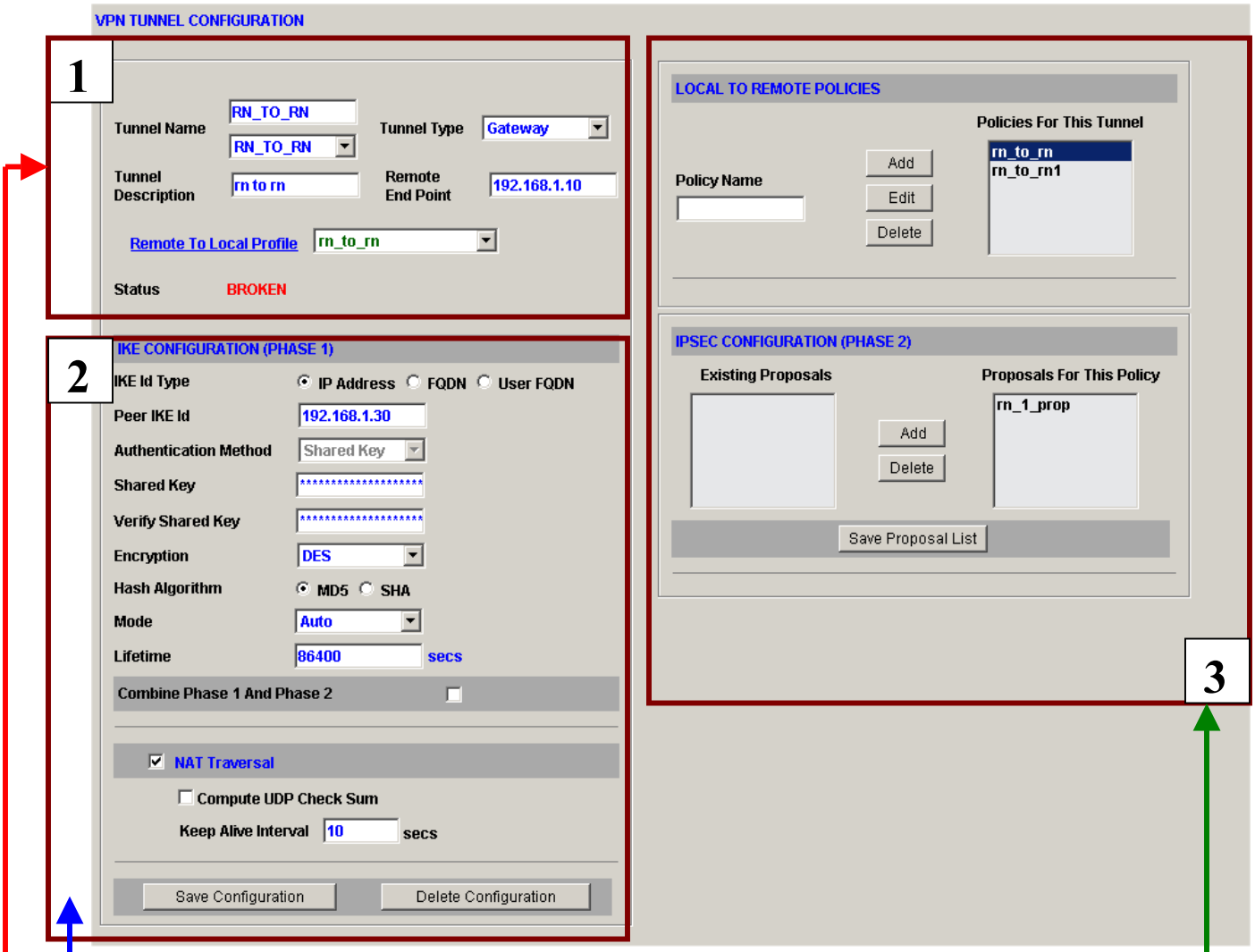
Compute UDP check sum
In case of the UDP protocol will add the value of the UDP checksum, so the UDP packets would not be dropped by the next firewall (this is needed when the other end of the VPN tunnel requesting the NAT traversal)

Keep Alive interval (*n* seconds)
UDP is a connectionless protocol, so, in order to keep the tunnel up the RN device will send the UDP packet to the other VPN peer (every *n* seconds).

Logging Enabled
If enabled - the RN VPN will send the messages to the syslog server.

6.5.2 RN VPN Tunnel Set Up.

Figure 79 VPN->VPN Tunnel Set Up->Tunnel Config



The VPN tunnel setup procedure involves several main steps:

The VPN tunnel name and type setup. The VPN tunnel should be bind to the security zone or to the user security profile (see **User Authentication**)

The VPN tunnel phase 1 parameters configuration

The VPN tunnel phase 2 parameters configuration

Go to **Device Configuration -> VPN -> Tunnel Set Up ->Tunnel Config** .

Step 1 : **VPN Tunnel parameters configuration**

At this step the VPN tunnel is defined by the name, the type and is bind to the certain security zone or the user profile . The following is the description of the fields that are involved in this step(see the aria number 1 on **Figure 2**):

Tunnel Name
The name for the VPN tunnel.

Tunnel Type
Could be **:**
Remote Access **-** the VPN clients will be connecting to this RN device. Configure this type of tunnel for laptop home users or road warriors who connect to office network
Gateway **-** This RN device will be a part of the point-to-point tunnel. Use this type of tunnel to create secure IPSec VPN tunnel between two remote branch offices. This may called as gateway-to-gateway or site-to-site tunnel.

Remote End Point
The hostname or the IP Address of the remote VPN gateway.
This option is configurable only if the Gateway options is chosen
as a VPN **Tunnel Type**(see above)**.**

Tunnel Description
The meaningful description for this tunnel (e.g. **NY branch**)

Remote To Local profile
The security profile that will be used for this tunnel. The security profile fir the VPN tunnel consists of the firewall rules that will be applied to this tunnel. The firewall rules are configured in **Firewall Configuration** mode

Step 2: The VPN tunnel IKE phase 1 parameters configuration

At this step the phase 1 parameters (IKE) are defined for the VPN tunnel . The following is the description of the fields that are involved in this step (see the aria number 2 on **Figure 2**):

Negotiation ID
The unique ID that will represents RN device in the IKE negotiation.
The negotiation ID could be:
IP Address - the IP Address of the RN Device
FQDN - A *fully qualified domain name* of the RN device that consists of a host and domain name, including top-level domain.

User FQDN - A *fully qualified domain name* of the user that consists of a host and domain name, including top-level domain.

Authentication Method
Shared Key - The password that will identify a connecting party during the KE negotiation (phase 1). The Shared Key should be distributed to the VPN clients or gateways that are allowed to established the VPN connection to this RN device

Shared Key
The value of the shared key.

Verify Shared Key
The shared key verification field

Encryption
The security mechanism that will be used to encrypt the messages during the phase 1 (IKE). The RN device supports the following encryption methods :
DES, IDEA, BLOWFISH, RC5, 3DES, CAST

Hash Algorithm
The hash algorithm is used by IPSec to ensure that a message has not been altered. The RN device supports **MD**5 and **SHA** algorithms

Mode
The mode could be : **Auto, Main or Aggressive**

Lifetime
The period of time in seconds. The RN device will renegotiate the phase 1 (IKE) every ***n*** seconds (the **Lifetime** value). Then shorter the **Lifetime** then more secure the VPN tunnel.

Combine Phase 1 and Phase 2
If checked (enabled) will perform the phase 2 negotiation right after the phase 1 (without waiting for the actual data transfer)

NAT Traversal
If checked, RN device will use the NAT Traversal for the all configured tunnels. (will overwrite the global settings)

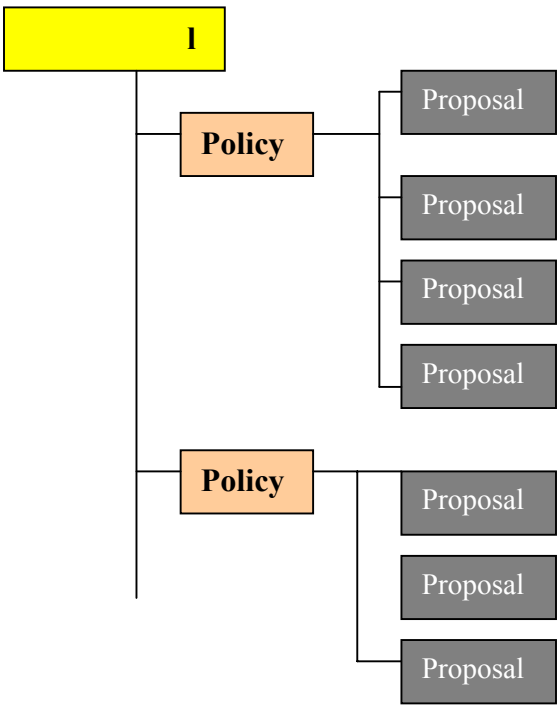
Compute UDP check sum
In case of the UDP protocol will add the value of the UDP checksum, so the UDP packets would not be dropped by the next firewall - this is needed when the other end of the VPN tunnel requesting the NAT traversal (will overwrite the global settings).

Keep Alive interval (*n* seconds)
UDP is a connectionless protocol, so, in order to keep the tunnel up the RN device will send the UDP packet to the other VPN peer every *n* seconds. (will overwrite the global settings)

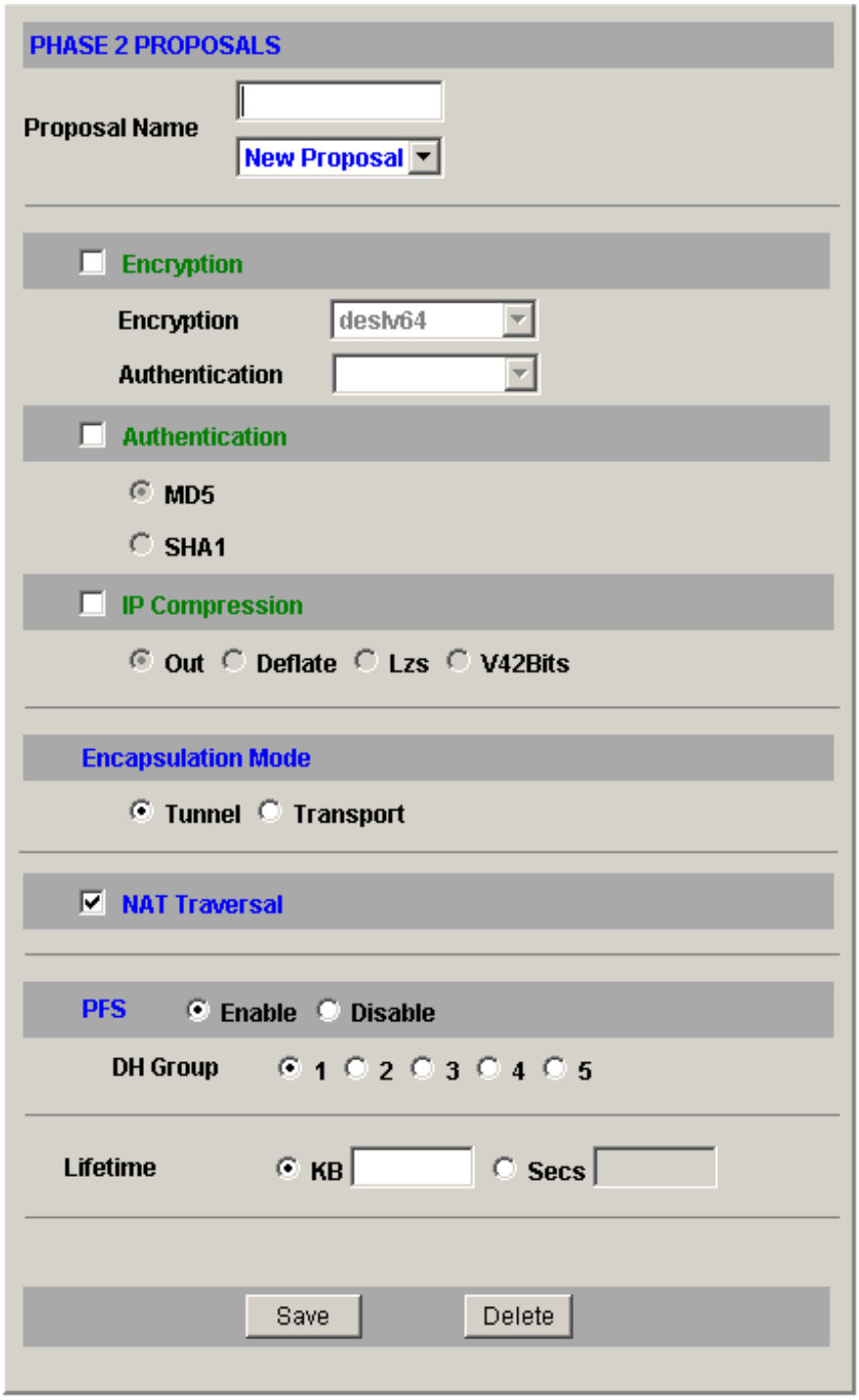
Press **Save Configuration** to save the configured VPN tunnel

Step 3: The VPN tunnel phase 2 parameters configuration

The phase 2 configuration based on the policies and proposals .
The next picture illustrates the relation between the tunnel, policies and proposals



The proposals should be created first
Go to : **Device Configuration -> VPN -> Tunnel Set Up ->Phase 2 Proposals**



Encryption - The RN device supports the following encryption methods :
DES, IDEA, BLOWFISH, RC5, 3DES, CAST, AES, NULL, THREEIDEA, RC4, DESIV32, DESIV64

The RN device supports the following authentication methods :
HMACMD5, HMACSHA, DESMAC, KPDK

Authentication - The RN device supports the following messages authentication methods : **MD5, SHA1**

IP Compression - The IP Compression allows the compression of IP datagram by supporting different compression algorithms. The RN device provides several compression algorithms:
Out, Deflate, Lzs, V42Bits.

Encapsulation Mode – The way that the IP datagram will be encapsulated in the IPSec packet, could be **Tunnel** or **Transport**.

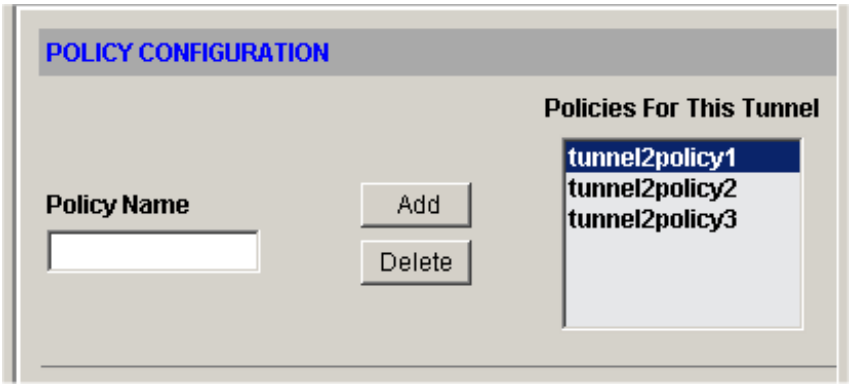
NAT Traversal - If checked, RN device will use the NAT Traversal for the all configured tunnels. (will overwrite the global settings)

PFS - Perfect Forward Secrecy (PFS) allows to add an additional security parameter to tunnel sessions. PFS means that every time encryption and/or authentication key are computed, a new Diffie-Hellman Key Exchange is included. RN device supports the DH Groups from **1** to **5**

Lifetime - This parameter could be defined in Kb or in Secs :
If the lifetime defined as certain amount of the Kb then the security will be renegotiated every ***n Kb*** **.**
If the lifetime defined as certain amount of the seconds then the security will be renegotiated every ***n seconds*** **.**
Then shorter is the life time then more secure is the tunnel.

To save the proposal press **Save** button.

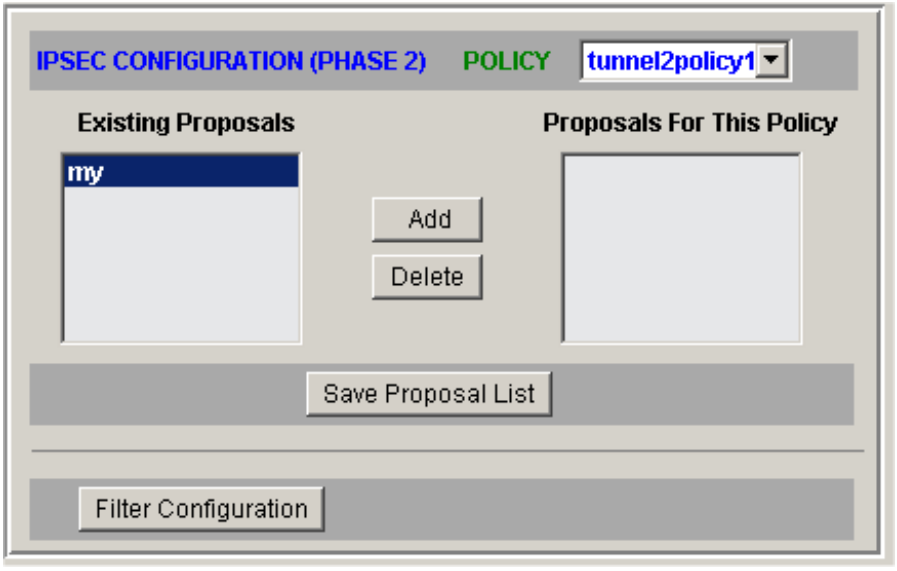
After the proposal is created it could be assigned to the policy and policy could be assigned to the VPN tunnel
Go to : **Device Configuration -> VPN -> Tunnel Set Up ->Tunnel Config**



To create the policy **:**

Go to the **POLICY CONFIGURATION** part of the screen
Enter the policy name at the **Policy Name** field
Press **Add** button
At this point this policy is attached to the VPN tunnel
(multiple policies could be attached to the same VPN Tunnel)

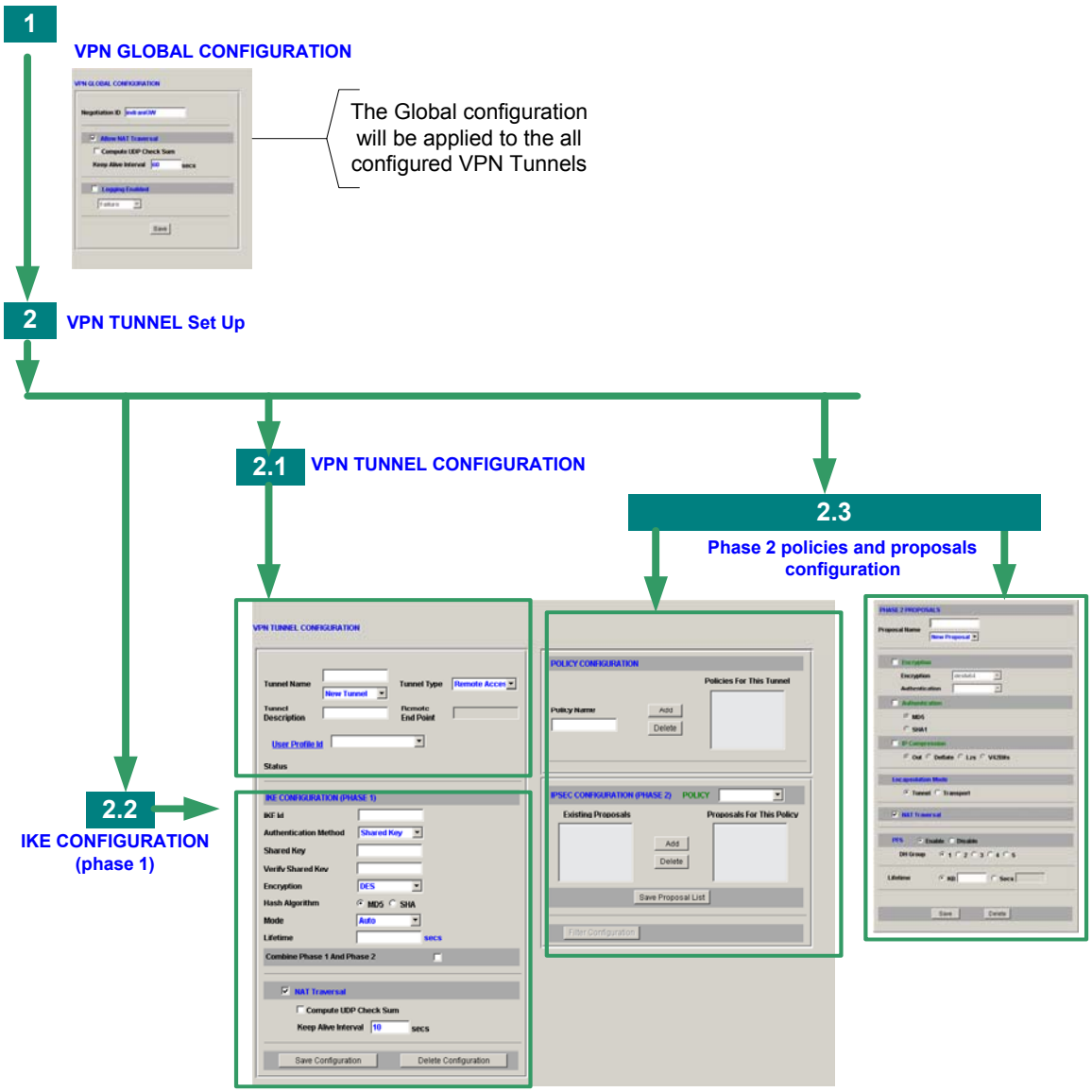
To assign the proposals to the policy:
Go to **IPSEC CONFGURATION (PHASE 2**) part of the screen



Choose the policy from the drop-down menu.
Choose the proposal from the **Existing Proposals** list.
Press **Add** button .
Press **Save Proposal** List

At this point the policy has the list of the proposals and is attached to the VPN tunnel and the RN device is ready for the VPN connections.

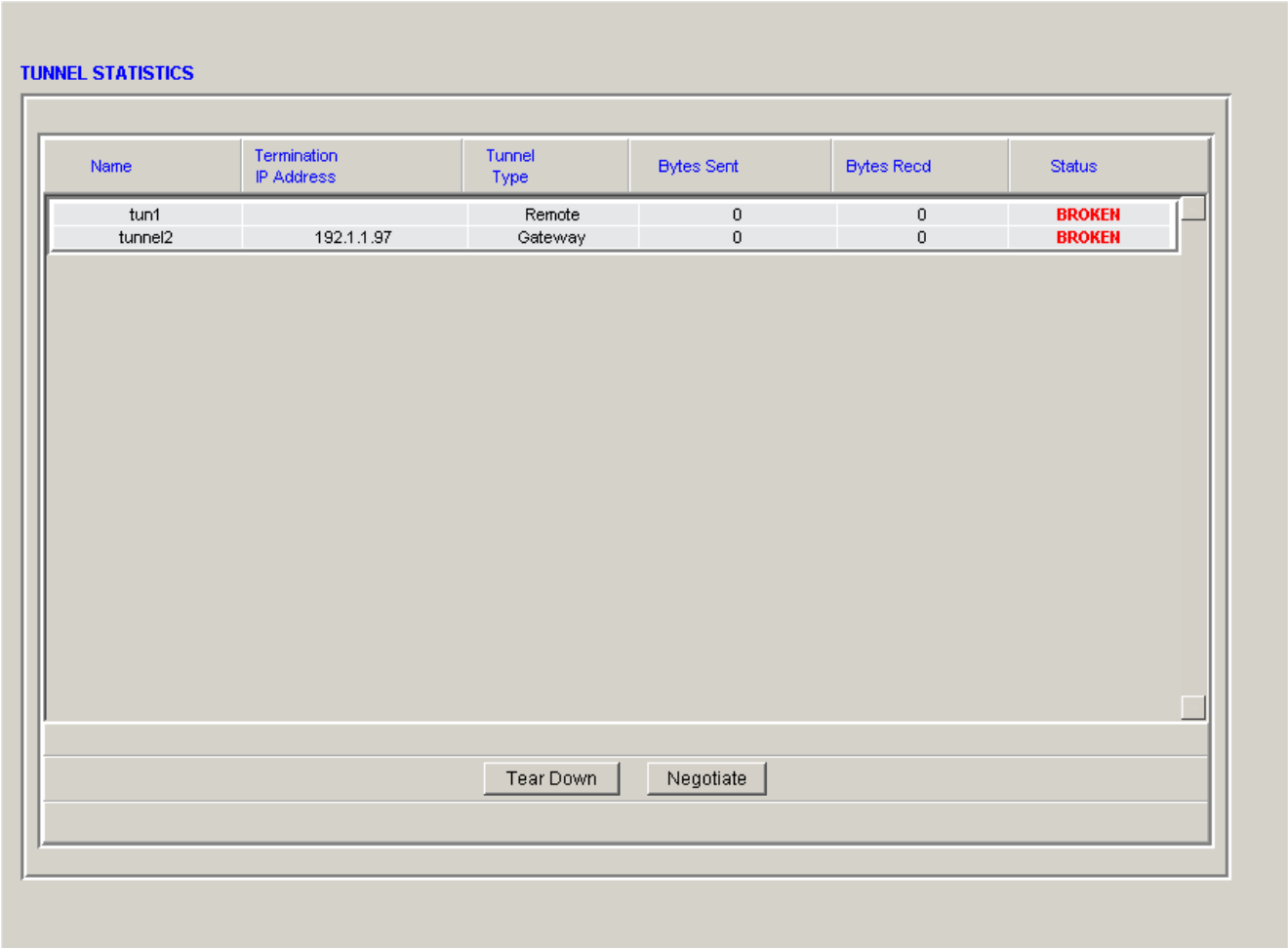
The next picture shows the VPN tunnel configuration route.



6.6 RN VPN monitoring

To see the statistics for the configured VPN tunnels :

Go to **Device Configuration->VPN-.> Tunnel Stats**



Where :

Name
The name of the configured VPN tunnel.

Termination IP Address
The IP Address of the other end of the VPN tunnel.
(in case of gateway to gateway tunnel)

Tunnel Type
The type of the configured VPN tunnel
(remote access or gateway)

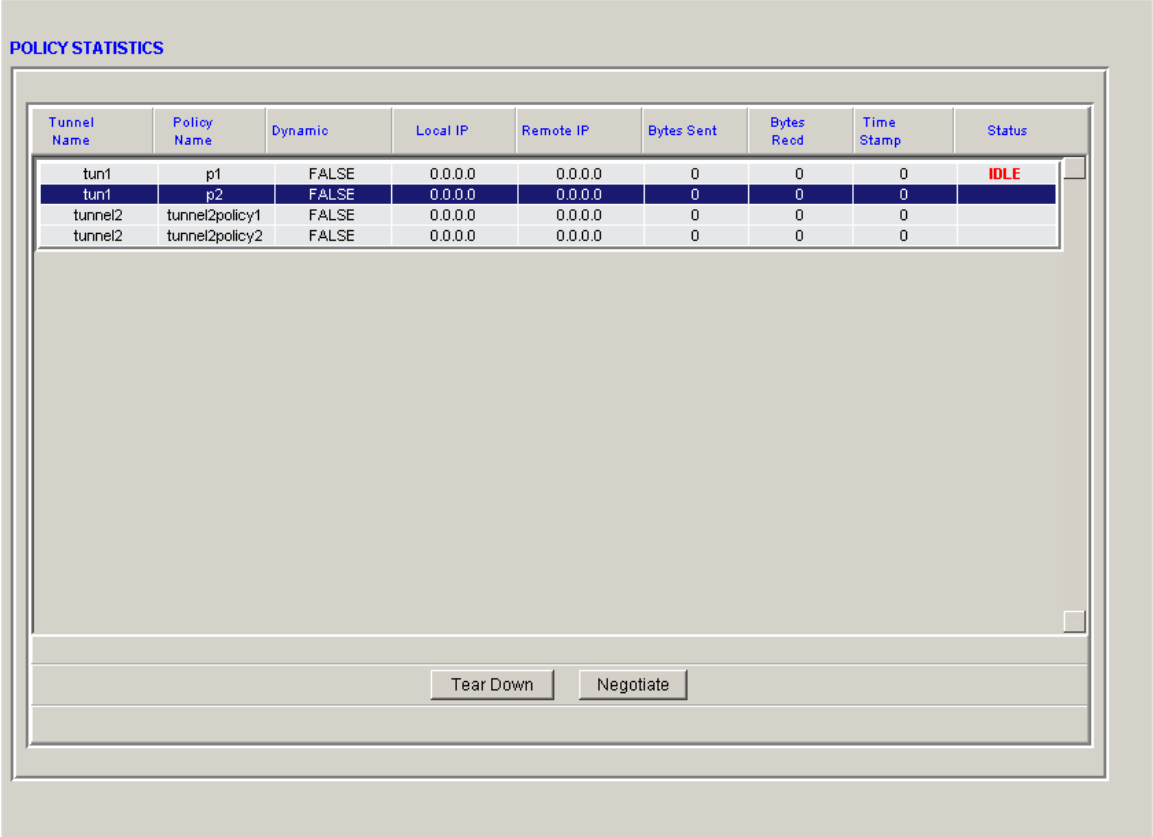
Bytes Send and **Byte Recd**

Bytes statistics for the VPN tunnel

Status
The real time status for the VPN tunnel .

To see the statistics for the configured VPN policies :

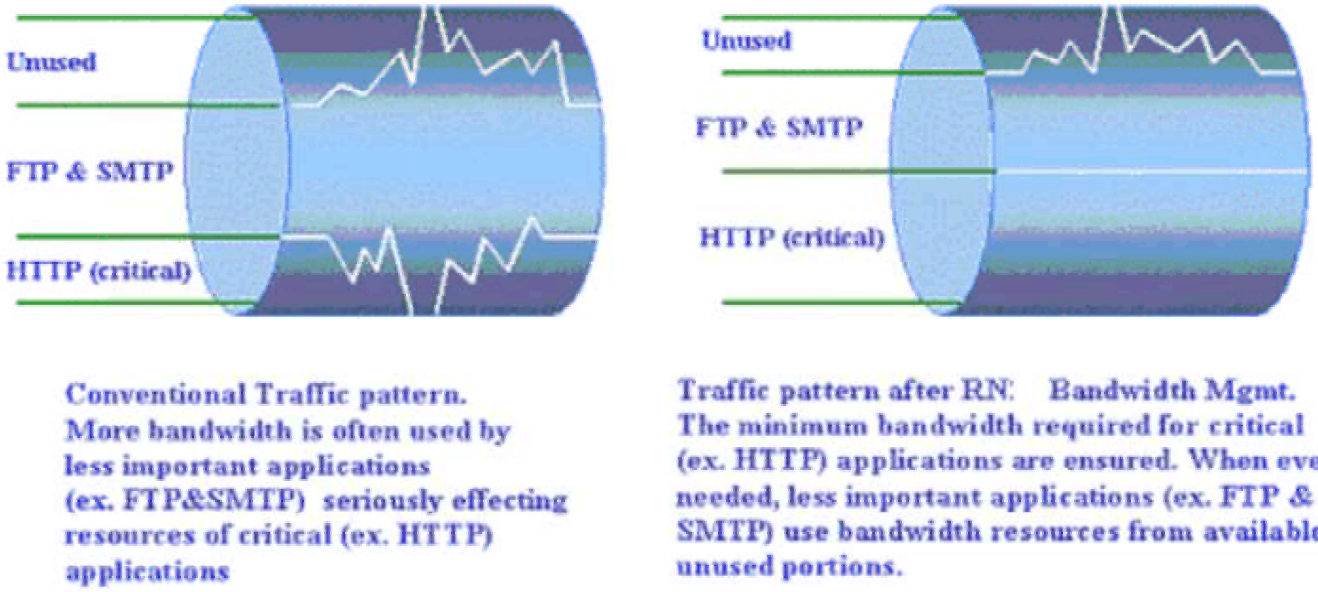
Go to **Device Configuration->VPN-.> Policy Stats**



7. Bandwidth Accounting and Control

All RNxx devices have bandwidth management capability, which can be used to mitigate WAN and Internet performance problems. The traffic shaping technique controls network utilization and actively prevents network congestion. Any RNxx device ensures a required quality of service (QoS) for mission critical applications.

Figure 80. Bandwidth Management Concepts



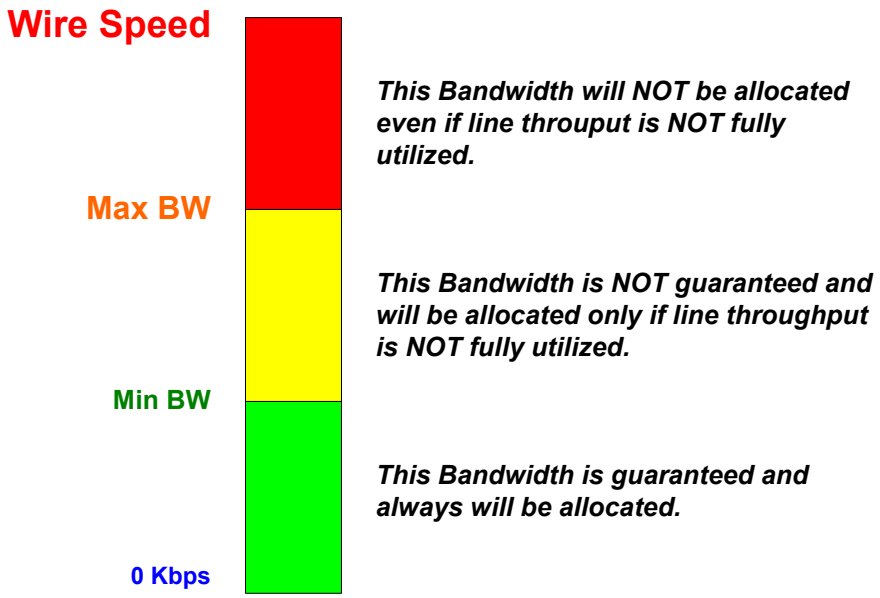
Features:

- Enables bandwidth allocation for critical applications by ensuring that the necessary resources are available.
- Improves network performance by avoiding network bottlenecks.
- Guarantees allocated bandwidth for critical applications.
- Activates bandwidth policies that define maximum, minimum and burst limits per application service, per source or destination IP addresses.
- Reports the total number bytes / packets that were processed with the bandwidth contract along with the number bytes / packets dropped.

Conceptually, any controlled and available bandwidth is divided among “Bandwidth Contracts” (Contracts). Each Contract is unidirectional, applying to inbound traffic or

outbound traffic, but not both. A Contract contains two sets of parameters: *bandwidth* allocated, and what kind of traffic it is applied to (*Flow identification filters*).

The bandwidth parameters are "minimum" and "maximum" bandwidth. The term "minimum bandwidth" means that this bandwidth is always available and guaranteed by RNxx device for the Contract. The term "maximum bandwidth" means that bandwidth for the Contract will never be allowed to exceed this value. Any bandwidth between the minimum and maximum values is available for the Contract, but is not guaranteed by RNxx device. See the figure below, showing the bandwidth allocation for one Contract.



The sum of the Minimum Bandwidth of all Contracts for a particular physical port cannot exceed the total bandwidth available on the port. That is, for a 10Mbps port, the total guaranteed bandwidth cannot exceed 10Mbps. A Contract is assigned to a Zone. As discussed earlier, a Zone may be assigned to one physical port, or across several physical ports; or multiple Zones may be assigned to a single physical port. In all cases, the sum of the minimum bandwidth of all Contracts on a particular physical port cannot exceed the bandwidth of the physical port.

In order to simplify the User interface, any RNxx device allows the user to create "Bandwidth Classes". A Bandwidth Class is *named* pair of Min-Max bandwidth parameters. For example, if Network will be used for large file transfers, then the user might create the following Bandwidth (BW) Class:

BW Class Name – My_FTP
Min bandwidth – 200Kbps
Max bandwidth – 500Kbps

Once created, this BW class might be used one or more times, in any Contracts and any Zones.

The Contract's filtering parameters are: Source IP, Destination IP, Source Port, Destination Port and UDP/TCP Protocols. Using these parameters, RNxx identifies the flows and controls their bandwidth. If the flow will not be identified by any Contracts, then Bandwidth Management System will NOT control such traffic flow. That traffic will be passed through RNxx device "AS IS".
Very important to note, that there are no connections between Firewall rules and Contract's filtering parameters.
There are two types of Bandwidth Management Polices that can be configured on the unit. These policy types differ in a way RNxx device enforces them.

Outbound Traffic Policies: This policy type is generally used in such environments, where there is low bandwidth link that needs to be effectively utilized. For example, a company has a T1 line and wants to prioritize outgoing FTP, HTTP and VoIP traffic. Administrator can assign separate Bandwidth Contracts to FTP, HTTP and VoIP, and RNxx device will enforce these contracts on the link. If one of the contracts is underutilizing the requested bandwidth, its unused portion can be shared among other contracts.

Figure 81. Outbound Traffic Control

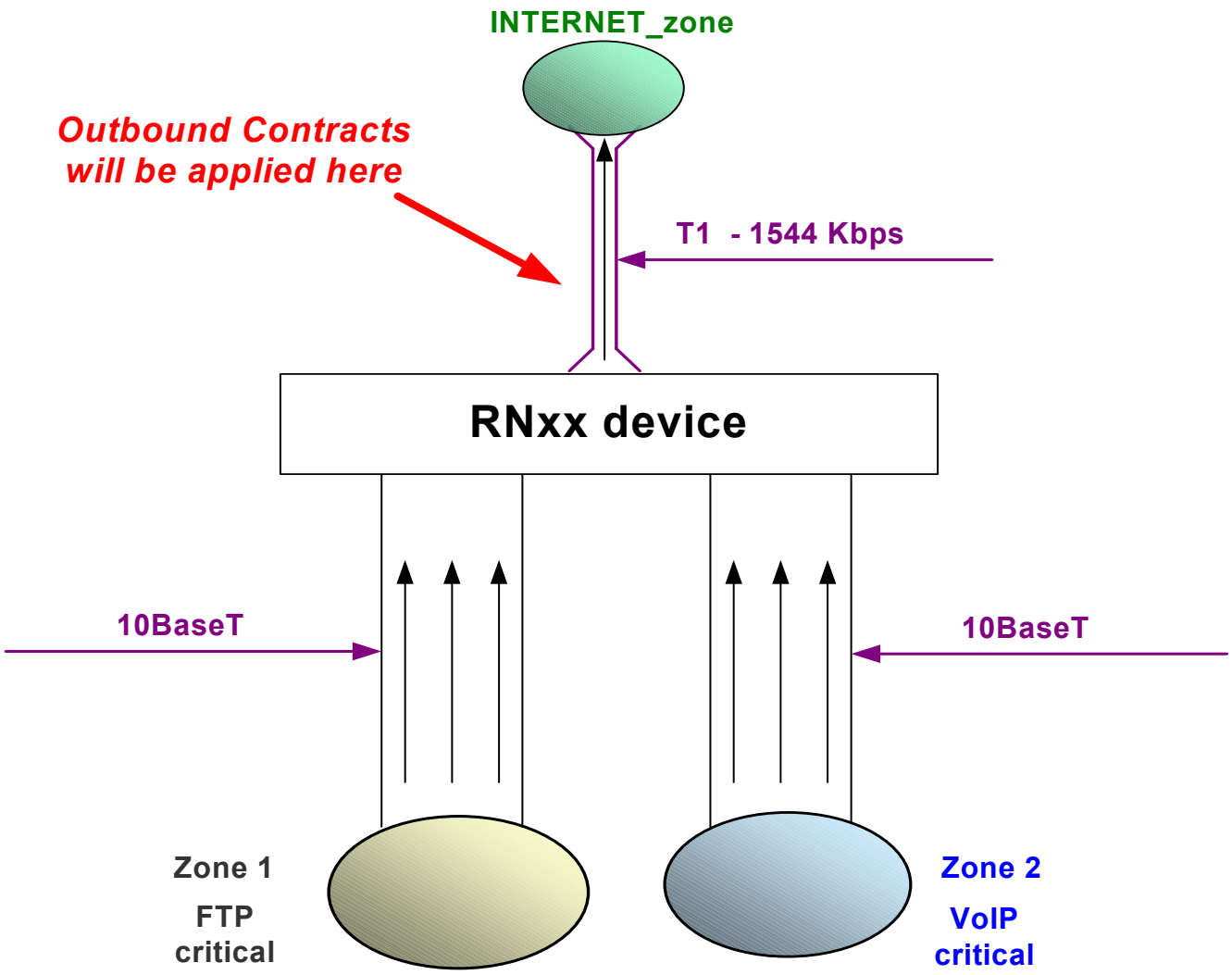
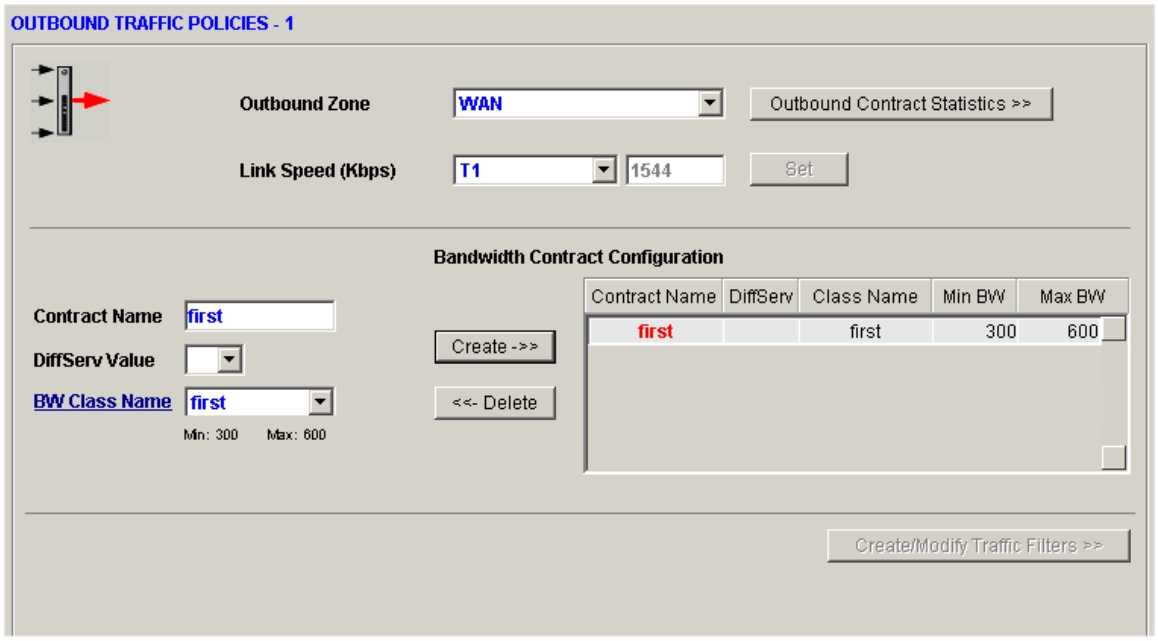


Figure 81 shows the network that is in need of outbound bandwidth management. For each zone there is a critical traffic type.

7.1 Outbound policies configuration:

Figure 82. Bandwidth Accounting and Control ->Outbound Traffic Policies



Fields Description:

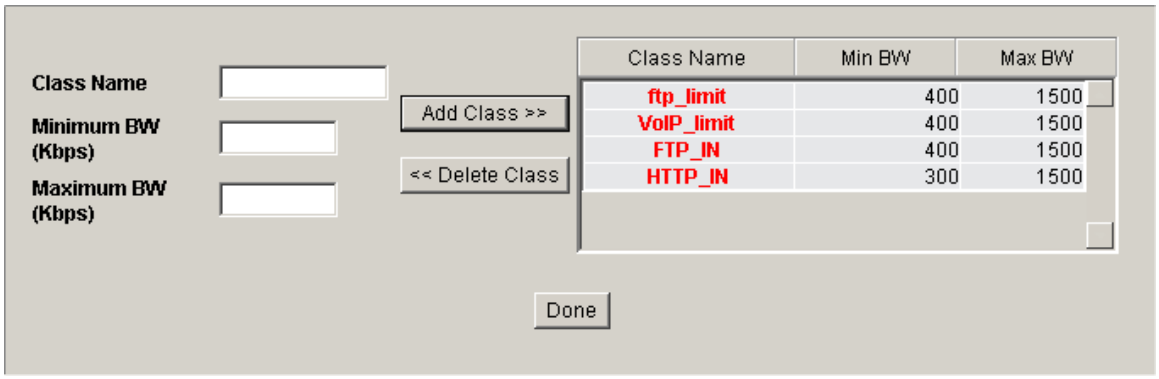
Outbound Zone	Drop-down menu with all configured zones in the system. If a zone has been configured for bandwidth management, selecting it will set previously configured link speed for this zone. When the last contract is deleted from the zone, the zone removes the link speed associated with it.
Link Speed	Outbound link speed for the selected zone. To set **Link Speed,** select one of the standard connections or provide a non-standard link speed and then click on **Set** button.
Contract name	Unique Contract Name, maximum 16 characters.
DiffServ Value	When the administrator sets this field, all packets associated with this contract will have the DiffServ byte set to this value.
BW Class Name	Bandwidth Class that will be used for this Contract. To create BW Class click on the **BW Class Name** link and configure Minimum and Maximum Bandwidth Parameters.
Create ->>	After providing Contract Name, DiffServ and BW Class click on this button to finish Contract creation.
<<- Delete	The administrator can delete a BW contract by selecting it from the Contracts List. All Traffic filters associated with this Contract have to be deleted first.
Outbound Contract Statistics	To see the statistics for this Outbound Zone click on this button to go to Bandwidth Contract Statistics Screen.

Configuration steps to perform:
1. Select **Outbound Zone** from a drop-down menu, where the traffic has to be managed.

2. Set Outbound connection **Link Speed**. Select one of the standard link speeds or configure **User defined** speed and click on **Set** button.

3. To create a bandwidth contract, first a bandwidth class has to be created. It can be done from **BW Class Name** configuration screen. Click on **BW Class Name** link to bring up the configuration screen. Provide a class name and Minimum and Maximum speed and click on **Add Class >>** button. After finishing BW Class configuration click on **Done** button.

Figure 83.Bandwidth Accounting and Control ->Outbound Traffic Policies->BW Class Name



4. To continue Bandwidth Contract configurations provide a contract name.

5. Set **DiffServ Value** if needed. This value will be set for all outgoing packets for this contract.

6. Select **BW Class Name** from dropdown menu.

7. Click on **Create >>** button to finish BW contract configuration.

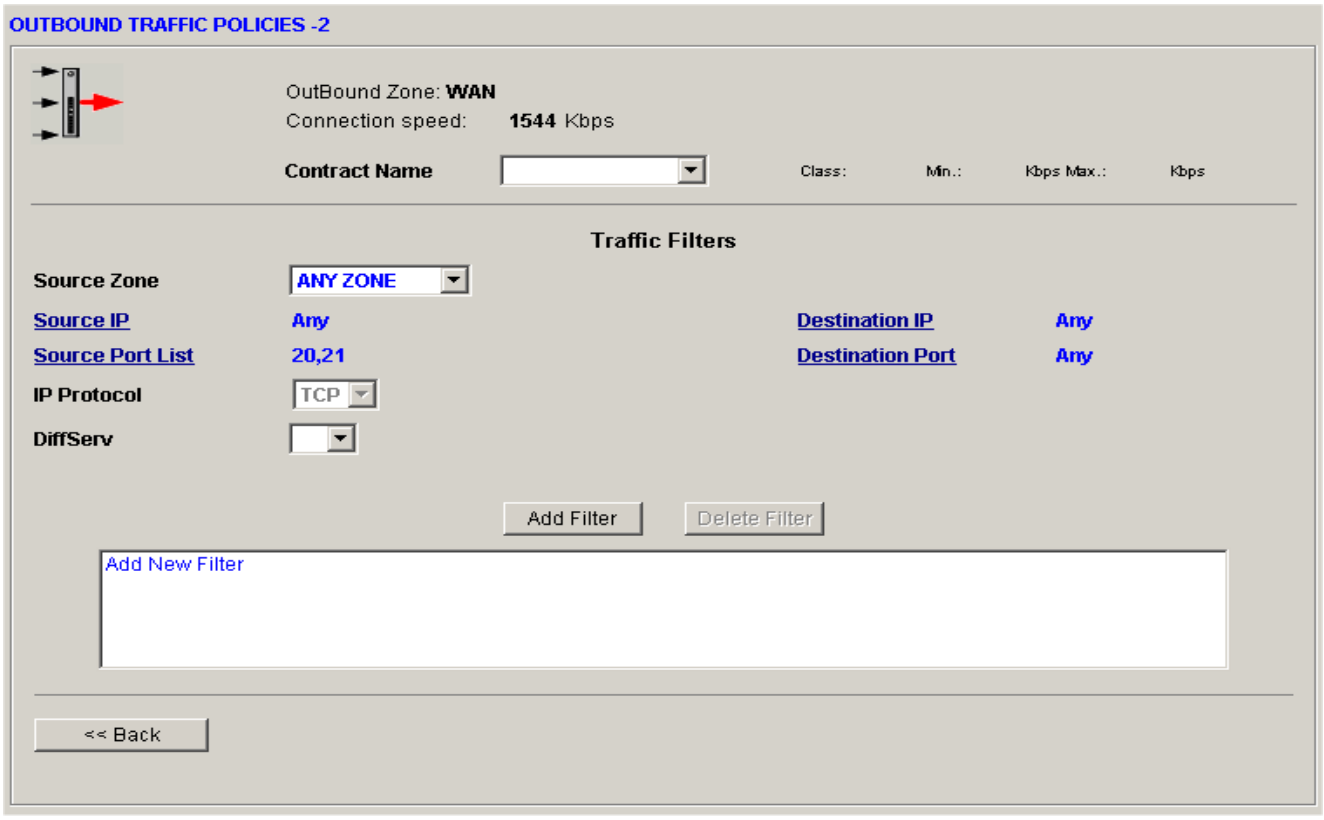
8. Repeat steps 3 to 7 to create more BW Contracts for the Outbound Zone.

9. When all BW contracts configuration is done, the next step is to configure traffic filters and assigned them to Bandwidth Contracts.

10. Click on **Create/Modify Traffic Filters >>** to go to Traffic Filters configuration screen.

Below is a sample filter for the FTP traffic.

Figure 84. Bandwidth Accounting and Control ->Outbound Traffic Policies->Contract Traffic Filter



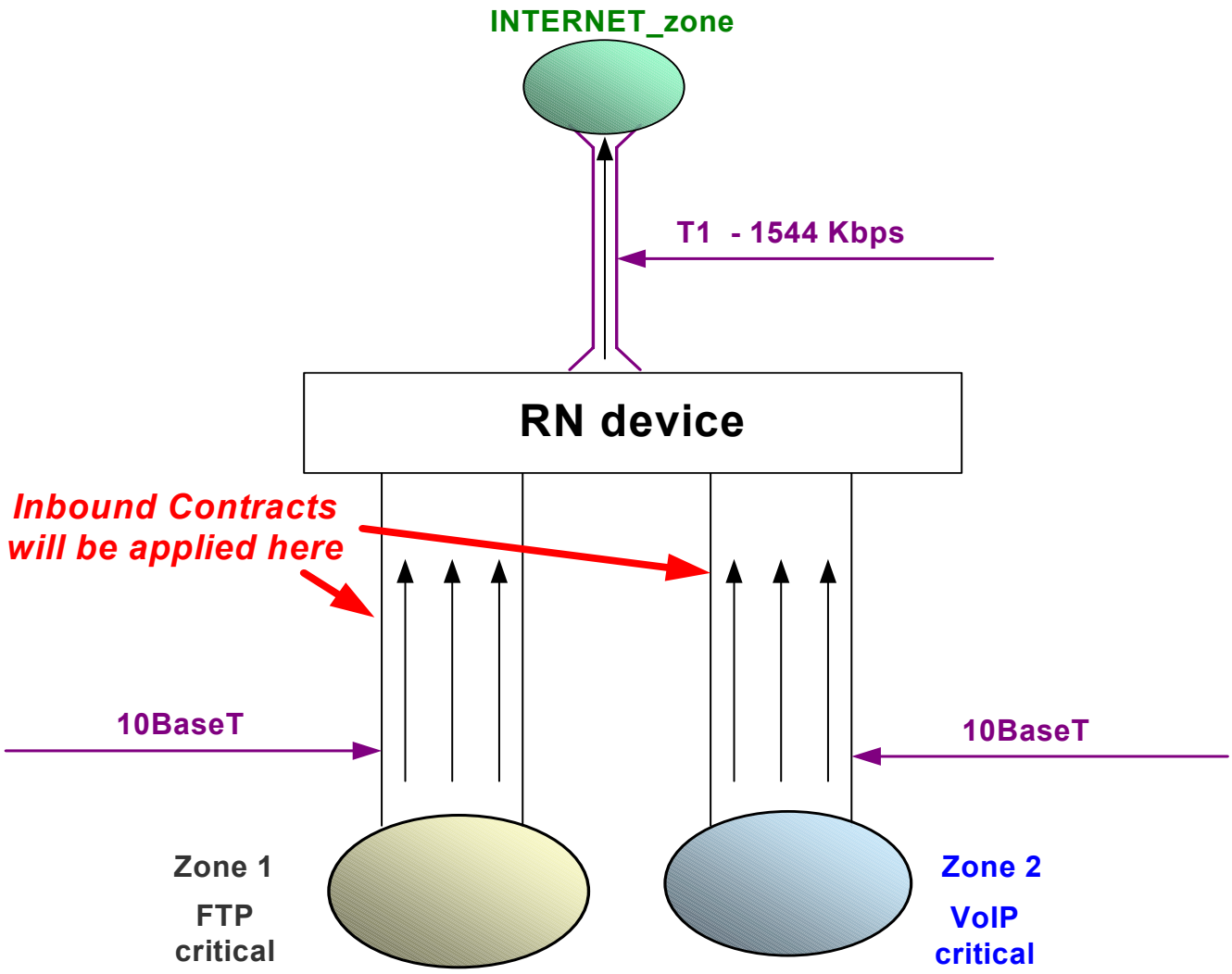
11. On **Traffic Filters Configuration** screen select **Contract Name** from drop-down menu.

12. Configure Traffic filter by setting **Source Zone** (could be ANY), **Source/Destination IP addresses**, **Protocol**, and **Source/Destination Ports**. Traffic also can be classified by **DiffServ** value.

13. Click on **Add Filter** to add it to the list of filters that have been configured for the selected BW Contract.

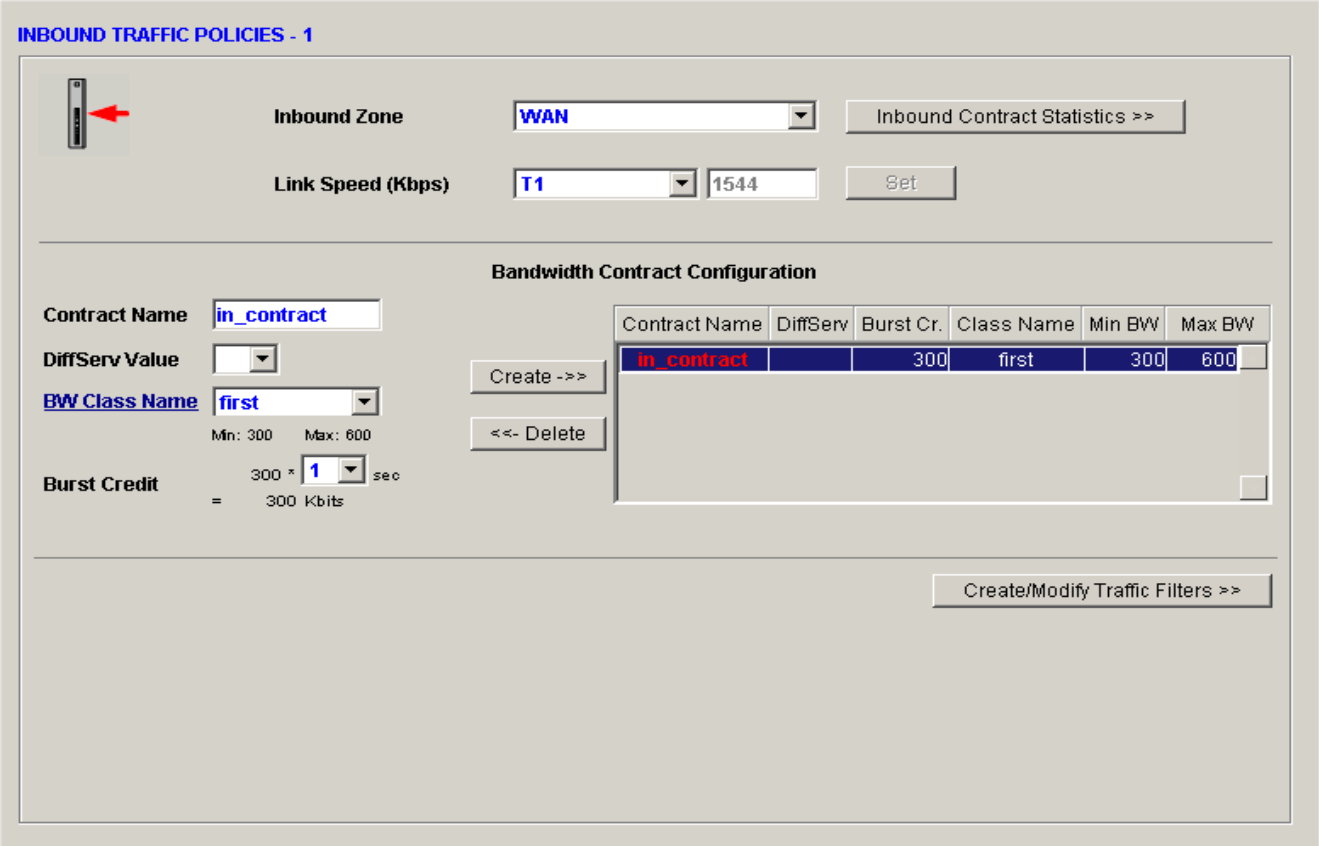
14. To **delete** Traffic Filter, select it from the list and click on **Delete Filter** button.

Inbound Traffic Policies: This policy type is used primarily in data centers, where each customer buys a chunk of bandwidth and cannot exceed it.



The figure shows the network that is in need of inbound bandwidth management. For each zone there is a critical traffic type.

Figure 85. Bandwidth Accounting and Control ->Inbound Traffic Policies



Fields Description:

Inbound Zone	Drop-down menu with all configured zones in the system. If a zone has been configured for bandwidth management, selecting this zone will set previously configured link speed for the zone. When the last contract is deleted from the zone, the zone removes the link speed associated with it.
Link Speed	Outbound link speed for the selected zone. To set **Link Speed** select one of the standard connections or provide non-standard link speed and then click on **Set** button.
Contract name	Unique Contract Name, maximum 16 characters.
DiffServ Value	When the administrator sets this field, all packets associated with this contract will have the DiffServ byte set to this value.
BW Class Name	Bandwidth Class that will be used for this Contract. To create BW Class click on the **BW Class Name** link and configure Minimum and Maximum Bandwidth Parameters.
Burst Credit	The administrator can set a priority for the contract by configuring **Burst Credit**. The more Kbits the contract can accumulate the higher the priority of this contract is going to be. This parameter is important when a traffic that belongs to this contract exceeds Minimum bandwidth but less than Maximum

	Bandwidth specified in Bandwidth Class.
Create ->>	After providing Contract Name, DiffServ and BW Class click on this button to finish Contract creation.
<<- Delete	The administrator can delete a BW contract by selecting it from the Contracts List. All Traffic filters associated with this Contract have to be deleted first.
Inbound Contract Statistics	To see the statistics for this Outbound Zone click on this button to go to Bandwidth Contract Statistics Screen.

Configuration steps to perform:

1. Select **Inbound Zone** from drop-down menu, where traffic has to be managed.

2. Set Inbound connection **Link Speed**. Select one of the standard link speeds or configure **User defined** speed and click on **Set** button.

3. To create a bandwidth contract, first a bandwidth class has to be created. It can be done from **BW Class Name** configuration screen. Click on **BW Class Name** link to bring up the configuration screen. Provide a class name and Minimum and Maximum speed and click on **Add Class >>** button. After finishing BW Class configuration click on **Done** button.

4. To continue Bandwidth Contract configuration the user has to provide a contract name.

5. Set **DiffServ Value** if needed. This value will be set for all outgoing packets for this contract.

6. Select **BW Class Name** from drop-down menu.

7. For each contact the administrator can specify a priority. This priority is measured in terms of Kbits that this contract can accumulate then use when requesting bandwidth higher than Minimum and lower that Maximum Bandwidth specified in the Bandwidth Class.

8. Click on **Create >>** button to finish BW contract configuration.

9. Repeat steps 3 to 8 to create more BW Contracts for the Inbound Zone.
10. When all BW contracts configuration is done, the next step is to configure traffic filters and assigned them to Bandwidth Contracts.

11. Click on **Create/Modify Traffic Filters >>** to go to Traffic Filters configuration screen.

12. On **Traffic Filters Configuration** screen select **Contract Name** from dropdown menu. 12. Configure Traffic filter by setting **Source Zone** (could be ANY),

Source/Destination IP addresses, **Protocol**, and **Source/Destination Ports**. Traffic also can be classified by **DiffServ** value.

13. Click on **Add Filter** to add it to the list of filters that have been configured for the selected BW Contract.

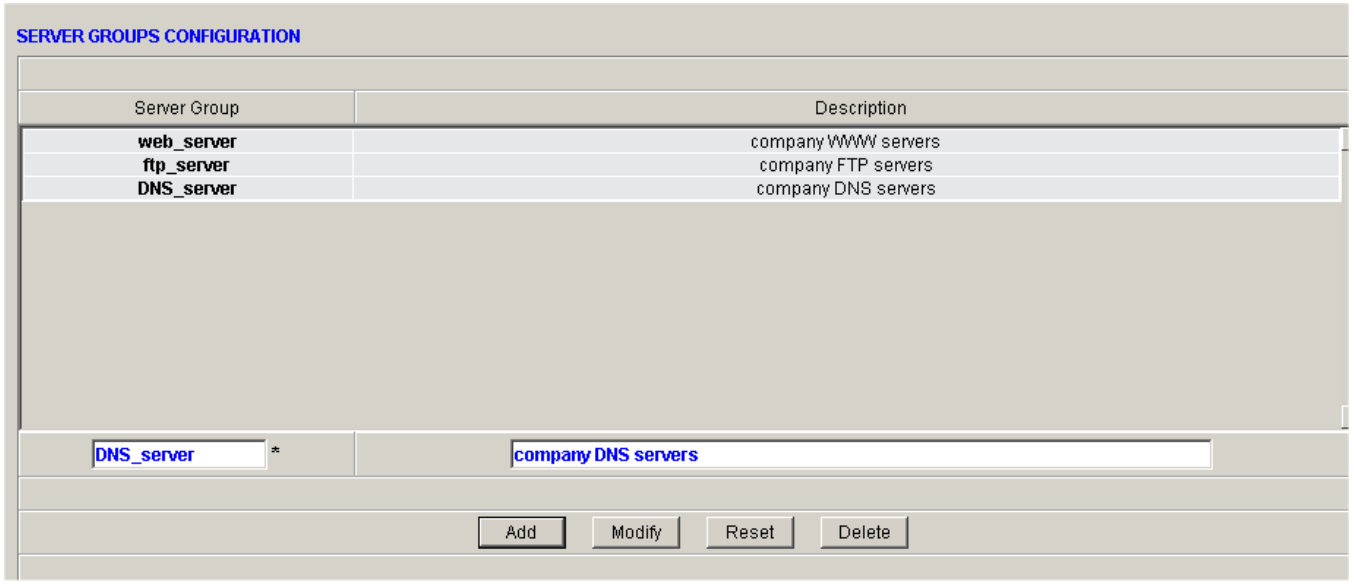
14. To **delete** Traffic Filter, select it from the list and click on **Delete Filter** button

8. Server Groups and Servers

With RNxx device you can combine servers into logical groups and apply load-balancing health monitoring to a group as a whole. Servers can be easily added to and removed from these groups. The following screens explain the Server Groups and Servers menu item.

8.1 Server Groups Configuration

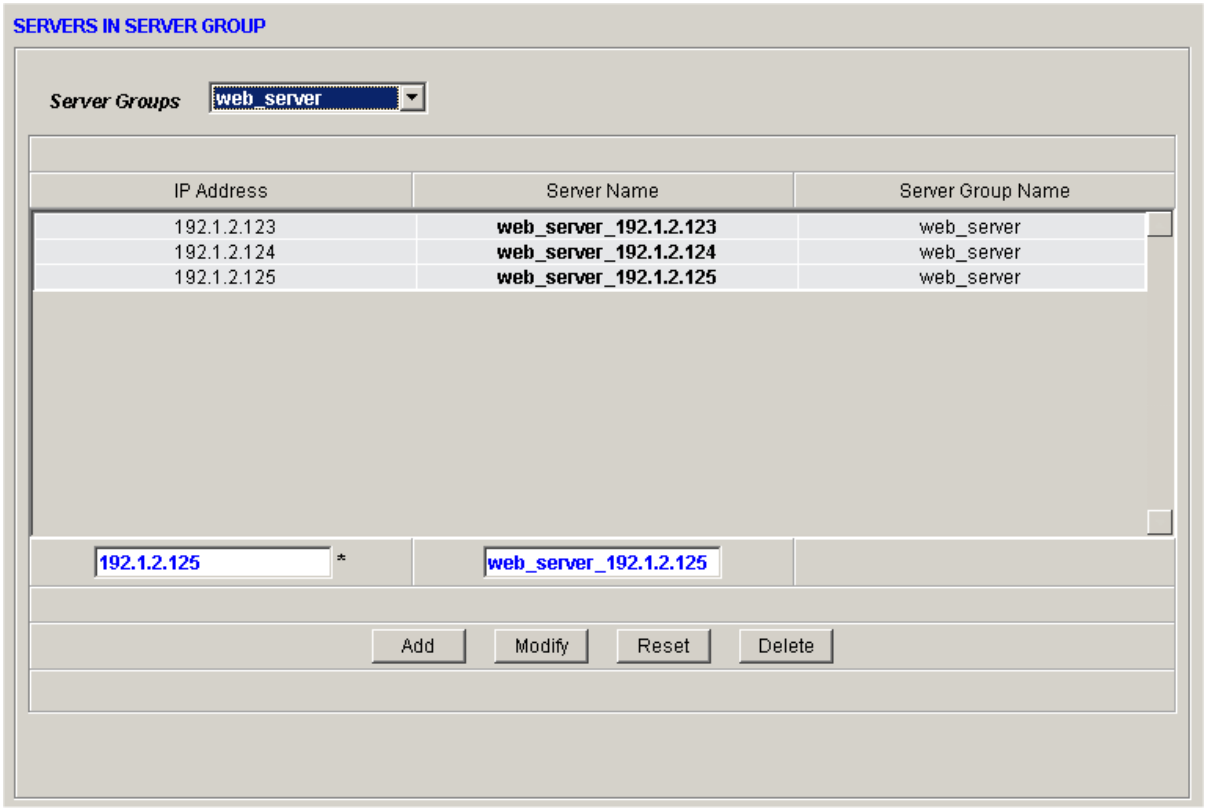
Figure 86. Server Groups and servers->Server Groups Configuration



The Server Groups Configuration tab allows you to create and delete the groups. Enter the Server Group name and its description and click on **Add** button to create a new server group. You can select an existing group and modify its description by clicking on **Modify** or delete it by pressing **Delete**. **Reset** button is used to clear input fields.

8.2 Servers in Server Group

Figure 87. Server Groups and servers->Server in Server Group Configuration



Once the Server Group is created you can add the servers to that group. All you have to do is enter the server name and its IP address and click **Add**. If you need to modify the server name or its IP address, or completely delete the server from the group, press **Modify** or **Delete** respectively.

9. Load Balancing

Server load balancing feature allows administrator spread the user traffic among several servers that provide identical/similar services. Load balancing addresses vital networks concerns:

1. A single server is unable to meet the demand for the application running on it.
2. The network connection from LAN to the server can saturate the server.

3. Servers with mission critical applications might fail and become inaccessible.

4. Software-only load balancing products do not provide adequate quality and performance.

Benefits:

1. **Increased efficiency for server utilization and network bandwidth**. With load balancing, RNxx device is aware of the shared services provided by the group of servers and can balance traffic among them. Traffic gets through more easily, reducing the user competition for connections on over-utilized servers. For even greater control, traffic is distributed according to a variety of user-selectable rules.

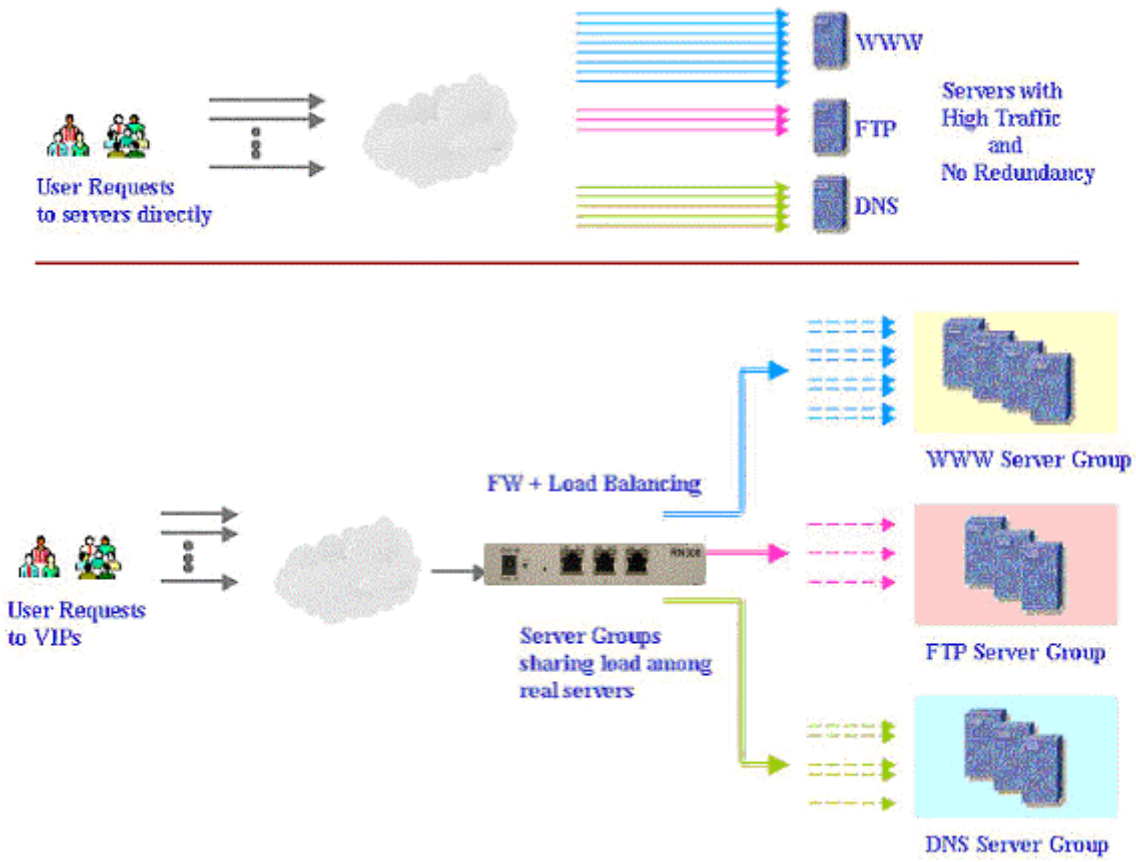
2. **Increased reliability of services**. If any server in a group fails, the remaining servers continue to provide access to vital applications and data. The failed server can be brought back up without interrupting the service.

3. **Increased scalability of services**. As users and applications are added and the server group's capabilities are saturated, new servers can be added to the group transparently.

Load balancing is based on associations between real servers, virtual IP address (VIP) and the switching rule. The real servers are your application servers, such as Web, SMTP or DNS servers. VIP is configured on all RNxx usually a public IP address. You associate a real server (or server group) with VIP by defining a switching rule which has parameters such as service type (http, ftp, dns, etc.), and the destination port. One can also fine-tune a rule by including traffic classification values such as source zone, source IP and source port.

The clients are unaware of the real servers (or server group) behind the VIP, but does experience enhanced performance and availability for TCP/UDP services.

Figure 88. Load Balancing Concepts



In a typical network that employs multiple servers without load balancing, each server usually provides a specific service, such as WWW, FTP, DNS etc. If one of these servers provides access to applications or data that is in high demand, it becomes over-utilized. Placing this kind of high traffic load on a server can decrease the performance of the entire network, as users' requests are rejected by the server and have to be retransmitted multiple times. Ironically, the over-utilization of key servers often happens in the networks where other servers are actually available.

The solution to avoid such situations is Server Load Balancing (SLB). A number of real servers to offer unique service are grouped together. For example, all real servers that offer web services are joined in 'WWW Server Group'. With the SLB enabled, RNxx device is aware of services provided by each group. Any RNxx device can direct user traffic to an appropriate server group, based on a variety of load-balancing algorithms.

RNxx with SLB configuration acts as a front-end to the server groups, interpreting user requests and distributing them among the available members of the group. SLB in RNxx has the following main characteristics.

Virtual IP Address: This is a traditional concept in load balancing. RNxx is configured to act as a virtual server and is configured with a virtual IP address for each collection of services it will load-balance. HTTP, FTP, DNS, SMTP, etc., are examples of some of the services that can be used for load balancing. Each VIP is assigned to a server group which has a number of real servers as members offering similar service. When the user stations request connections to a service, they will communicate with VIP on RNxx40. Based on the request received, RNxx device selects the corresponding group and binds the session to the IP address of the best candidate within this group, It also substitutes the VIP with an actual address of the server in all data packets. More effective address translations can be obtained by using 'Full NAT' or 'Half NAT' mechanisms.

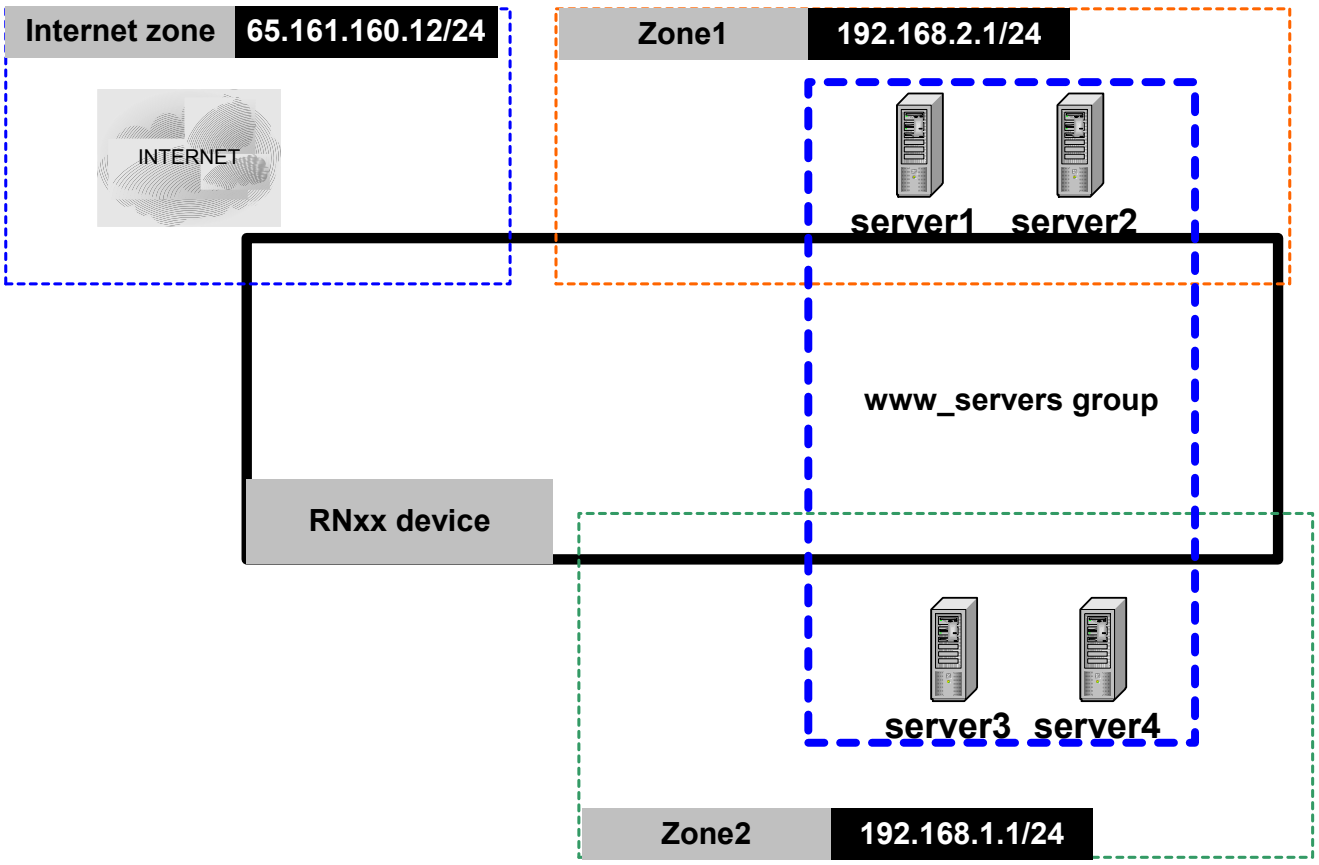
Traffic Classification: More filters can be added to a switching rule to control the types of traffic permitted through RNxx device during load balancing. Filters such as service type, destination port, source zone (the only zone from which user requests are allowed for VIP), source IP (single IP or range of addresses), source port (range or list).

Connection Persistency: RNxx devicexx supports SSL and cookie-based connection persistency. These are few examples of content-based load balancing.

General steps to configure load balancing

Step 1.

Create a server group (for example: www_servers) and populate it with servers (in this example 4 servers). Note, that the servers could be taken from any of configured zones.



Step 2

Configuring the virtual port and IP Address for the server group, choosing the switching algorithm . The Virtual IP Address and the virtual port - the parameters that will represent the server group to the outside world as the one single server.

The Virtual IP Address should belong to one of the secure zones (usually it is a public internet access).

The Algorithm will control the way that traffic will be distributed among the servers in the servers group. It could be selected from the following list:

Round-Robin

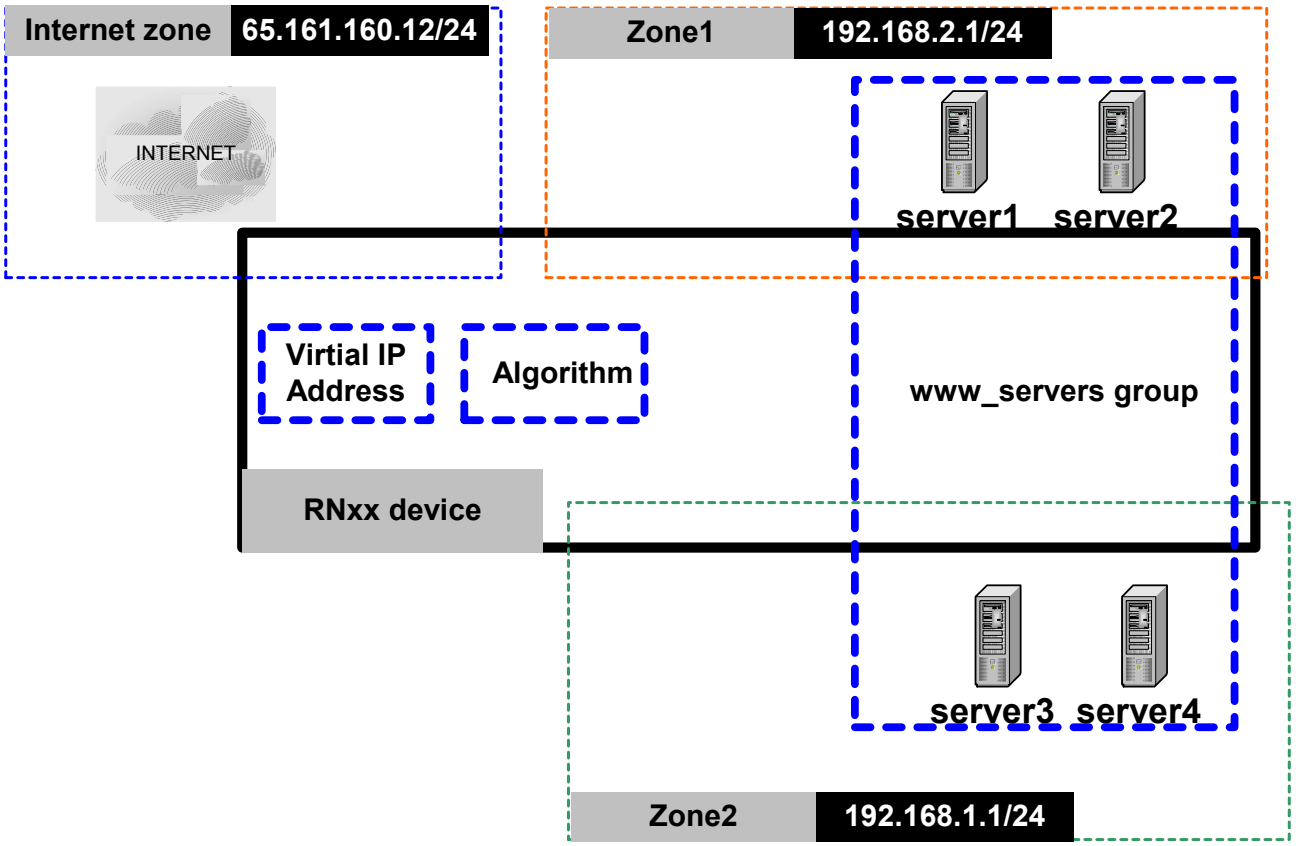
In a round-robin algorithm, the balances assigns the requests to a list of the servers on a rotating basis. The first request is allocated to a server picked randomly from the group, so that if more than one balancer is involved, not all the first requests go to the same server. For the subsequent requests, the balancer follows the circular order to redirect the request. Once a server is assigned a request, the server is moved to the end of the list. This keeps the servers equally assigned.

Weighted Round-Robin

Weighted Round-Robin is an advanced version of the round-robin that eliminates the deficiencies of the plain round robin algorithm. In case of a weighted round-robin, one can assign a weight to each server in the group so that if one server is capable of handling twice as much load as the other, the powerful server gets a weight of 2. In such cases, the IP sprayer will assign two requests to the powerful server for each request assigned to the weaker one.

Least Connections

In this algorithm the balancer will be redirecting the traffic to the least loaded server



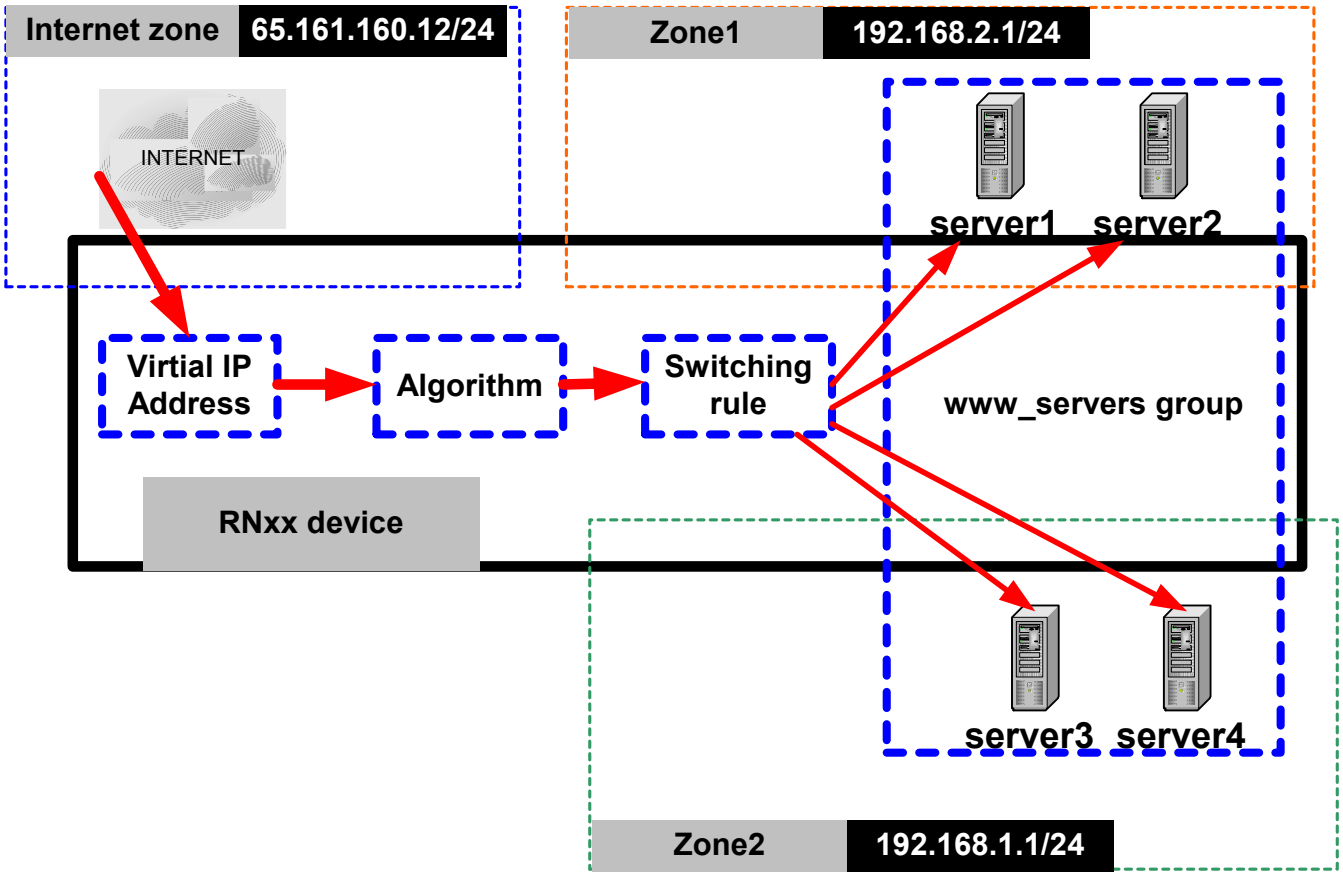
Step 3

The switching rule configuration.

Lets assume that this group of the servers is representing the online shop where the customers purchase something using the credit cards. The session is based on the SSL ID and should finished on the same physical server where it was started.

To achieve that the corresponding switching rule should be configured. The switching rules are very similar to the firewall rules and will be applied in the order according to their numbers.

In our case as soon as the balancer will detect the new SSL ID the traffic for this the session will be "glued" to the same server.



9.1 Basic Steps to Implement RNxx Load Balancing

To configure Load Balancing the following steps are required:

1. On the **Server Group Configuration** tab select a server group from **Server Group** drop down menu.
2. Select load balancing algorithm from **Algorithm** from dropdown menu
3. Set a **port number** in **Port** input field. This port number has to be the real protocol port number the real servers will be listening on in the selected server group
4. Select NAT type from **NAT type** dropdown.
5. If selected algorithm is **Weighted Round Robin**, user has to configure weights on **Servers in Server Group** tab in **Weight** input field.
6. Each server group has to be associated with Virtual IP address. To create Virtual IP address the **Virtual IP Configuration** tab under **Switching Configuration** is used.
7. The last step in configuring Load balancing for the Server Group has to be assigning Virtual IP address to the server group, defining the rules for connection persistency and traffic classification. That can be done on the **Switching Rules** tab and Switching rule configuration popup screen. These are the steps to finish Load Balancing Configuration:

7.1 Select destination Virtual IP from **Destination VIP** dropdown menu.
7.2 Click on Add button to bring up Switching Rule Configuration popup screen.
7.3 On the popup screen type in unique name for the switching rule.
7.4 Select destination Virtual IP from **Destination VIP** dropdown menu.
7.5 Select Server Group from Server Group Name dropdown menu. That will assign Virtual IP to the Server Group
7.6 Select type of service from **Service Type** dropdown menu. That will configure connection persistency for the traffic.
7.7 Configure Virtual port number the Virtual IP address will be listening. This field allows you to configure port mapping for Load balancing. For example: The real servers (configured on **Server Group Configuration** tab) are listening on port 8080 for http traffic, but for Virtual IP can be configured to be listening on port 80. The Load Balancing engine will accept the traffic on the Virtual IP on port 80 and will redirect the traffic to real server using 8080 port.
7.8 Using traffic classification parameters, user can classify the incoming traffic based on source Zone, IP address and ports..
7.9 Click on add rule to finish the switching rule configuration.

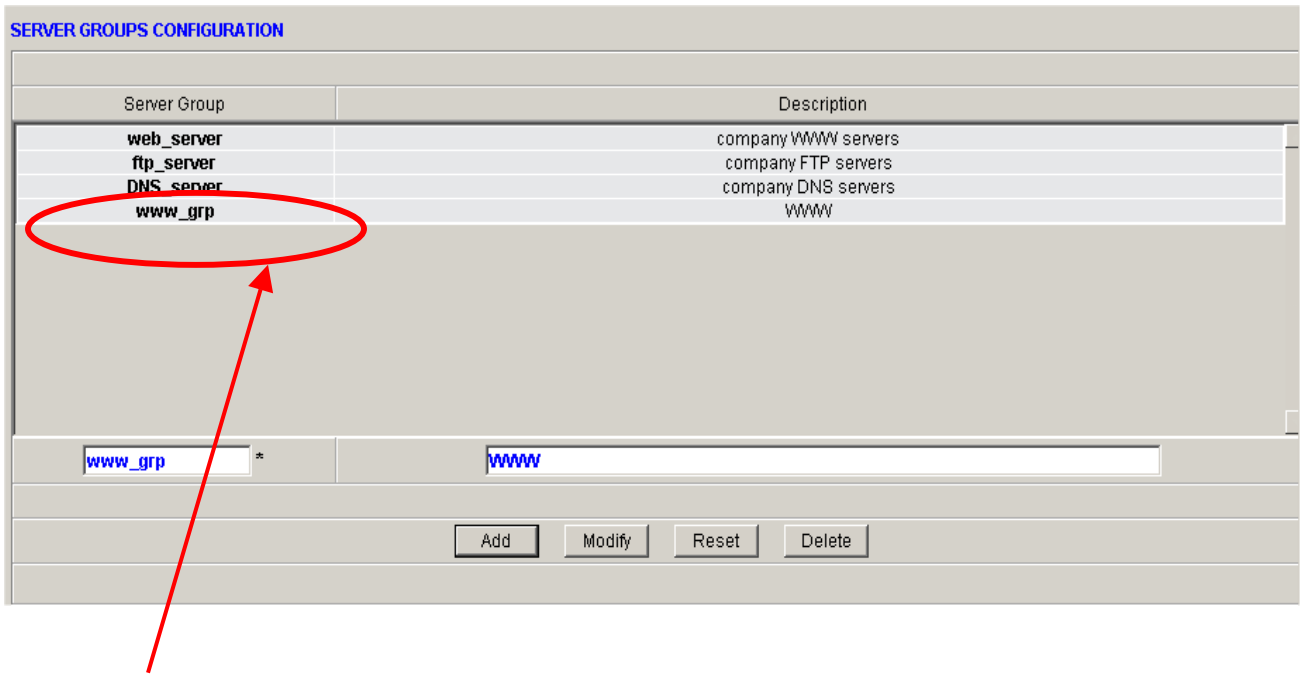
9.2 Load Balancing configuration example

Consider a situation in which a company's high available Web site (HTTP Server) has to be load-balanced with 'round robin' policy among 4 real Web servers for optimum performance. The VIP is 203.30.220.141, which is a public IP address accessible to external users. The internal IP addresses of real Web servers are 172.16.1.1 through 172.16.1.4. Below are the steps to configure such SLB scheme with the screen examples.

9.2.1 Step 1 – Server Groups and Servers Configuration

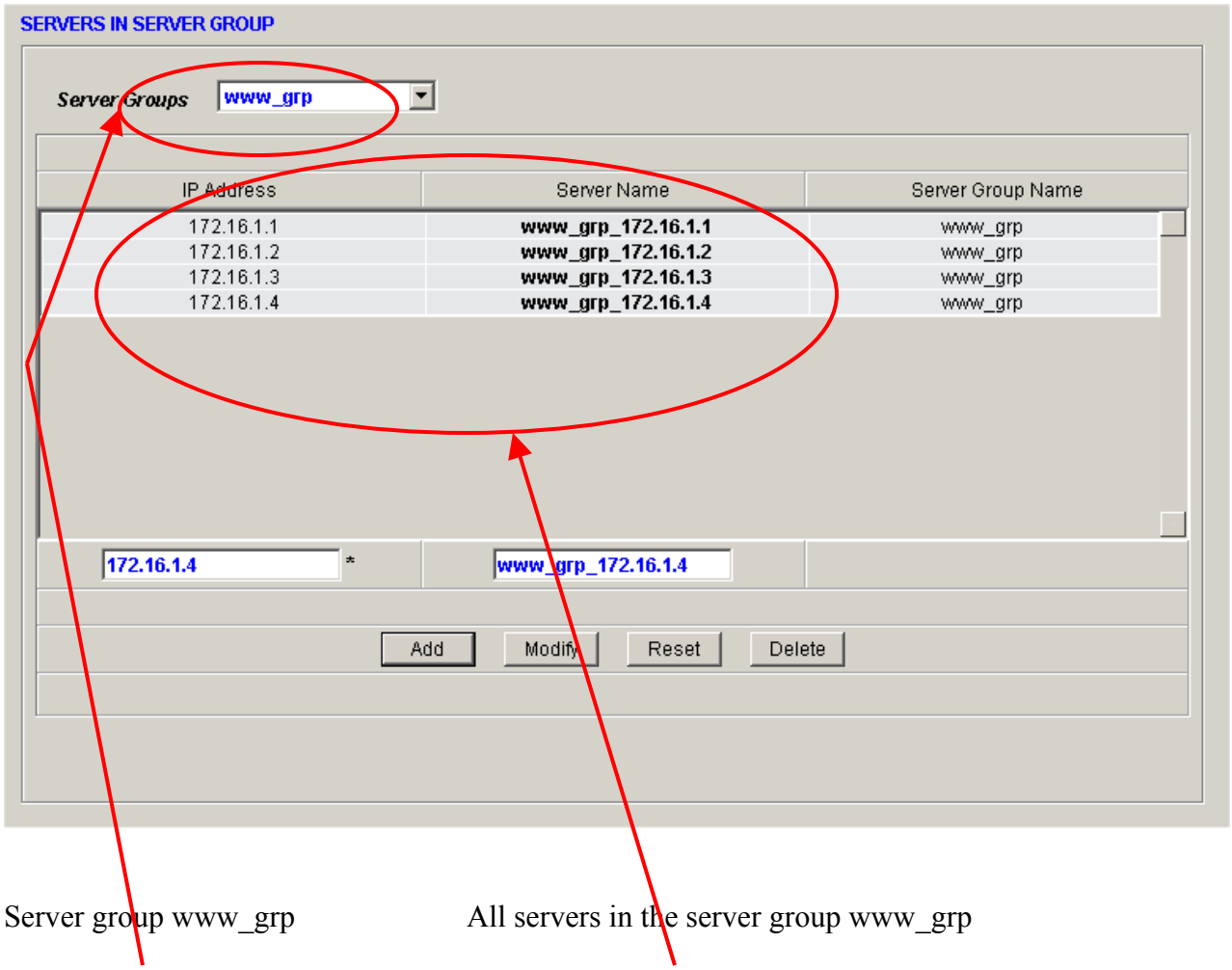
Go to 'Server Groups and Servers' menu item and create a server group called 'www-grp'. Add IP addresses (172.16.1.1 through 172.16.1.4) associated with the members of the group. From now on, this cluster of real servers is referred to as a server group 'www-grp'. See examples bellow.

Figure 89. Server Groups Configuration



Server group www_grp

Figure 90. Servers in Server Group Configuration



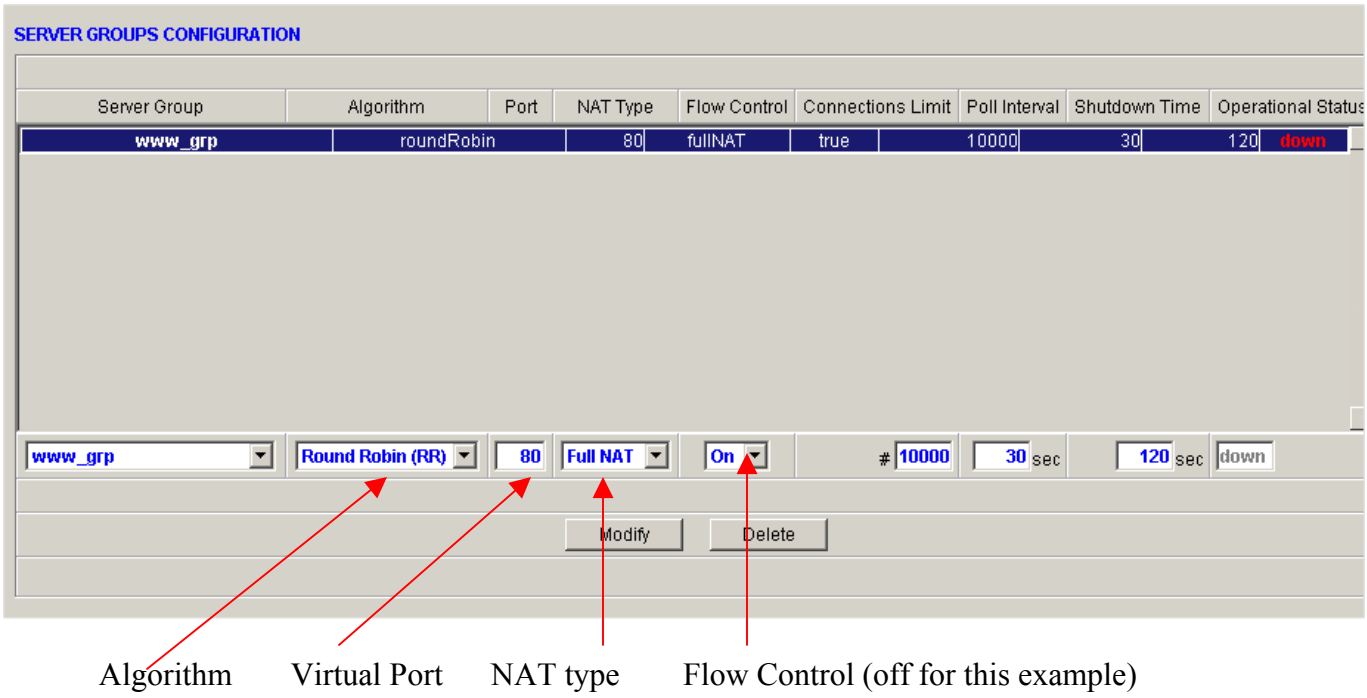
Server group www_grp

All servers in the server group www_grp

9.2.2 Step 2

Go to 'Load Balancing' → Server Configuration → Server Groups Configuration section and configure 'www-grp' with 'Weighted RR', port 80, Full NAT. Select default Flow Control, Connections limit, Poll Interval , and Shutdown Time values.

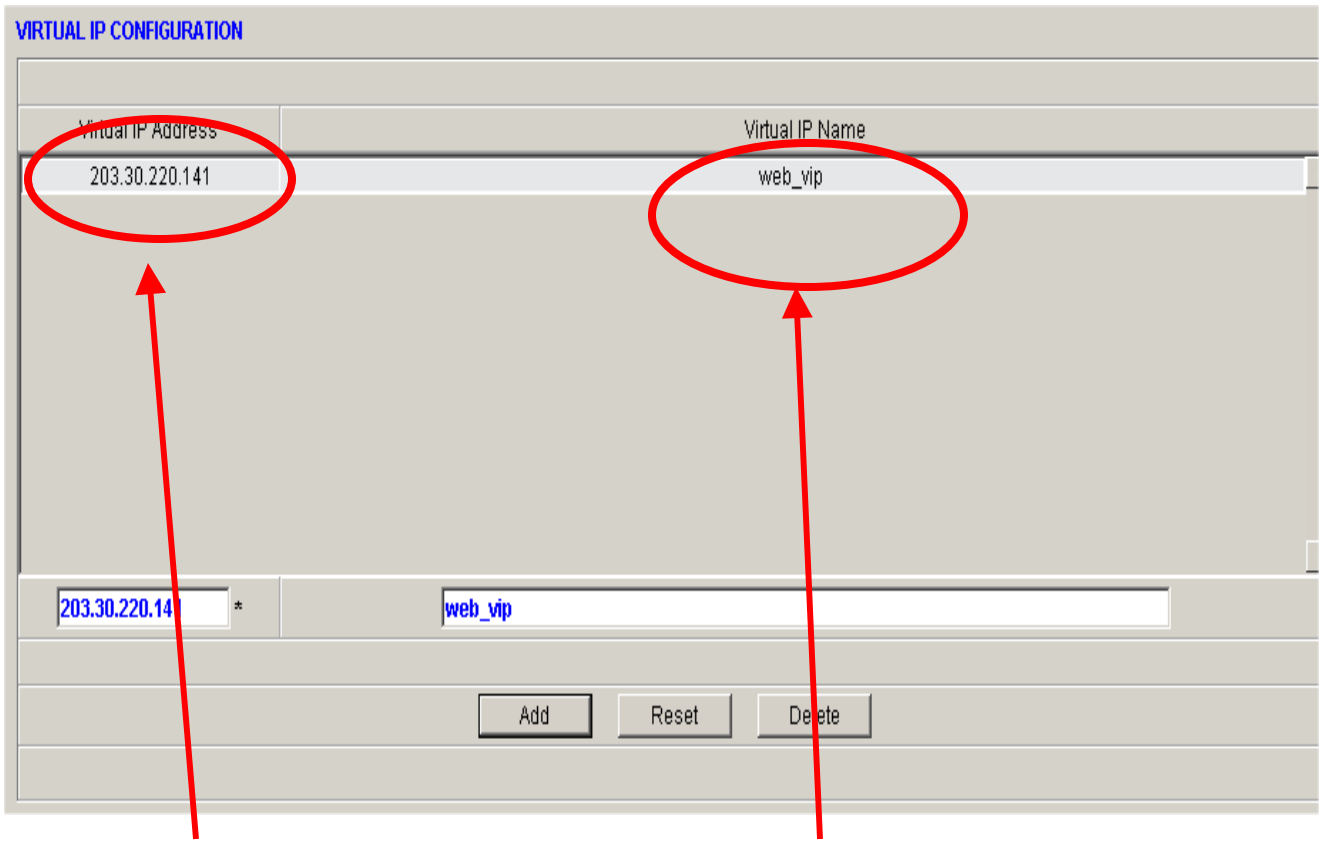
Figure 91. Load Balancing-> Server Configuration ->Server Groups Configuration



Algorithm Virtual Port NAT type Flow Control (off for this example)

9.2.3 Step 3

Figure 92. Load Balancing -> Switching Configuration -> Virtual IP Configuration



At this point the Virtual IP Address will be connected to the Servers group

9.2.4 Step 4

Go to Load Balancing → Switching Configuration → Switching Rules and create a switching rule. In the Switching Rule menu, select 'Destination VIP' as 'web-vip' and click on 'Add'. A new 'Switching Rule Table' template will pop up. Enter rule name, description, destination VIP 'web-vip', server group name 'www-grp', service type 'tcp', destination port '80', inactivity time 10 sec (default) and click on 'Add Rule'. Advanced traffic classification filters can also be configured to allow particular source zone, IP, port types.

Figure 93. Load Balancing ->Switching Configuration-> Switching Rules

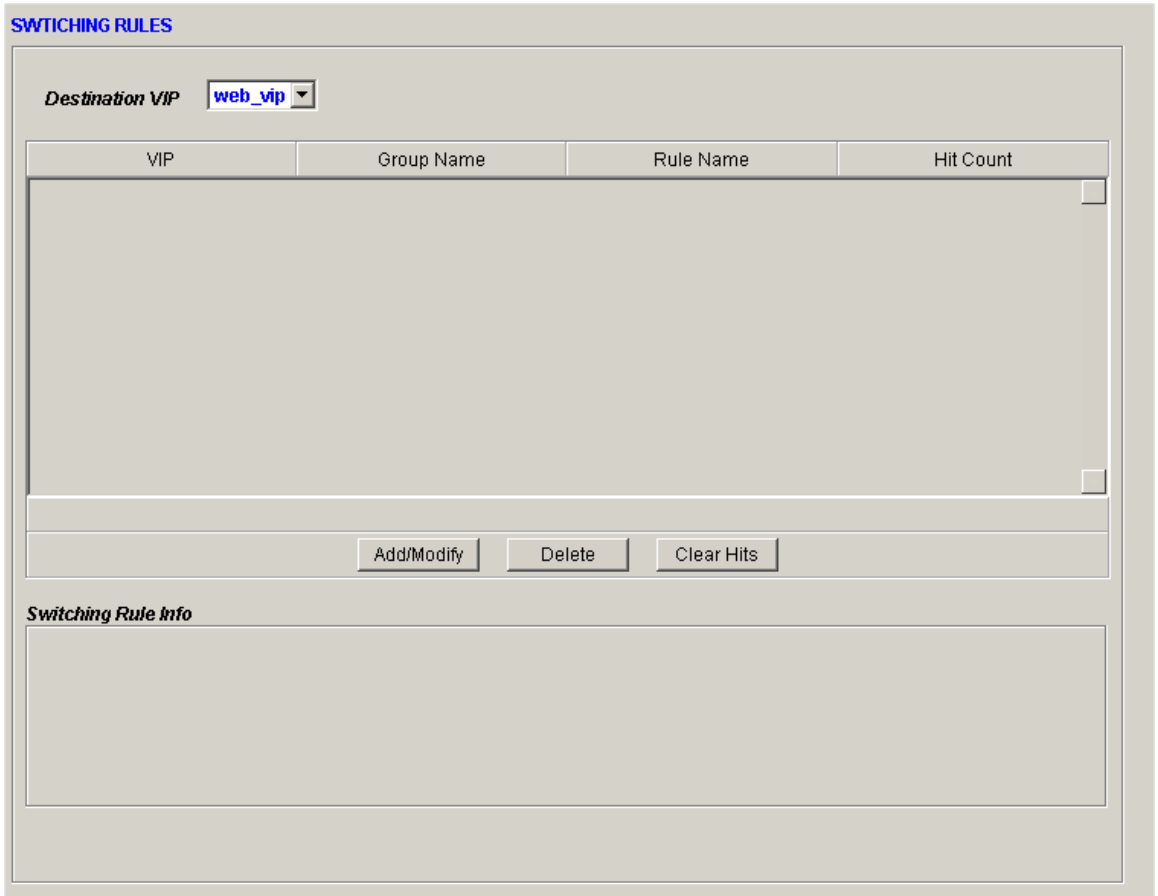
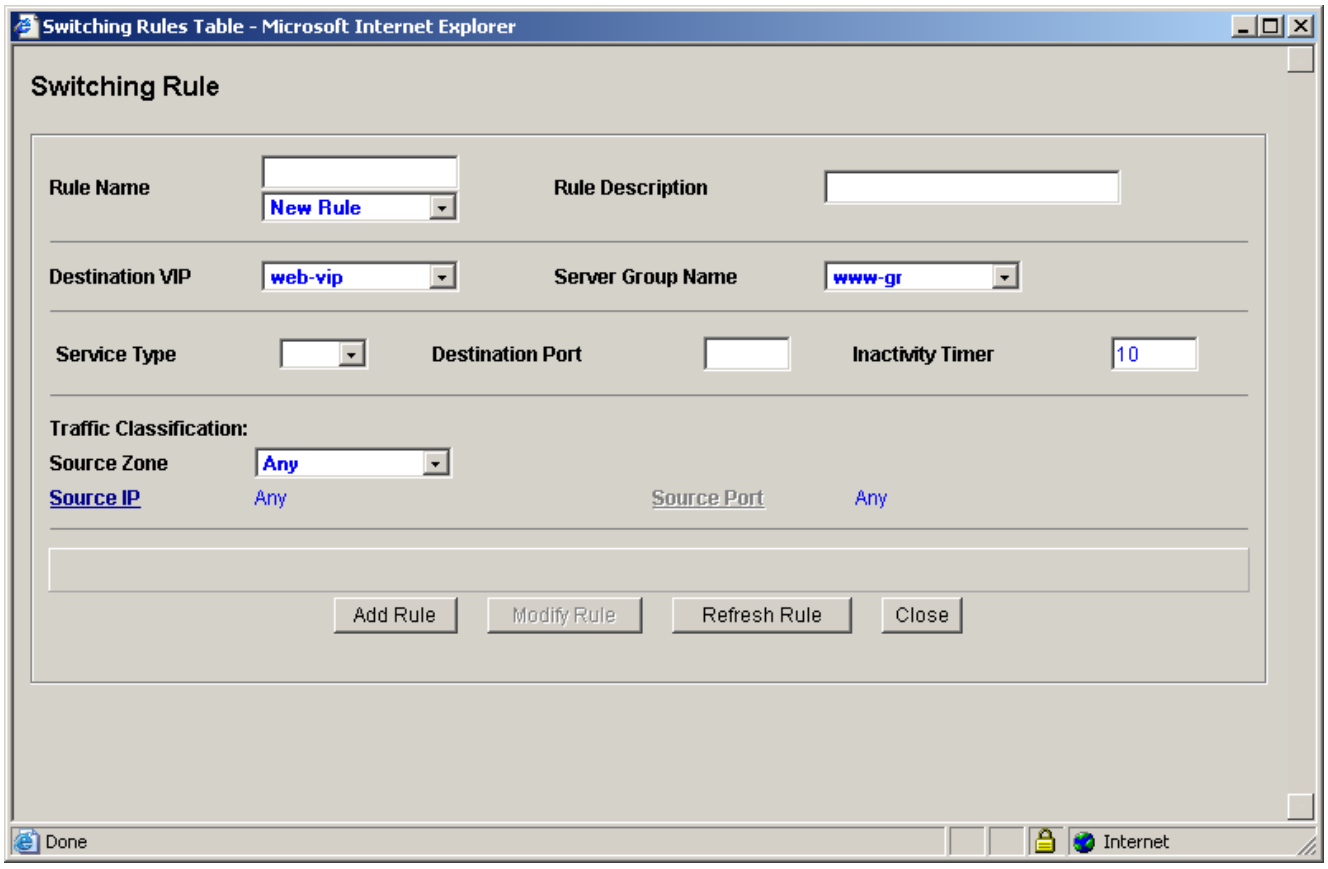


Figure 94. Load Balancing ->Switching Configuration-> Switching Rules (cont.)



Switching Rules Fields Description:
Rule Number: the number for the switching rule;
Rule Description: the logical description for the rule;
Destination VIP - the virtual IP that this rules applies to, the value is defined in **Virtual IP Configuration** table;
Server Group Name – the server group that will be represented by this virtual IP, the value is defined in **Server Groups Configuration** table;
Service Type - the service type value defines the load balancer's behavior at sessions level:

- **TCP** - the session will be attached to the same physical server from the beginning to the end;
- **HTTP** – the session will be routed according to the cookies :
    - Cookie is expired - the next server (according to the selected load balancing algorithm) will be selected;

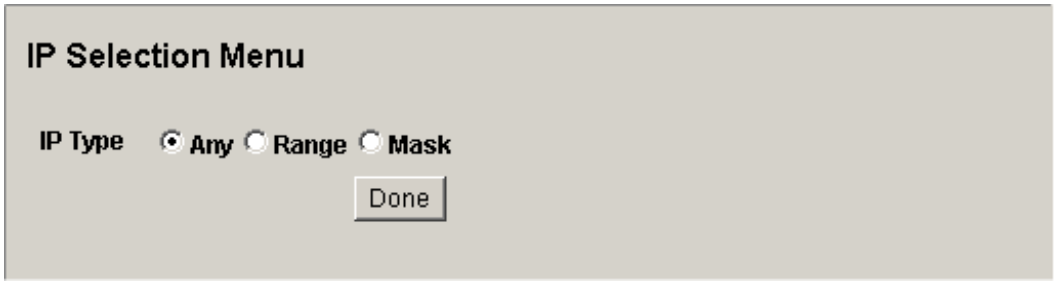
    - Cookie is valid - the session will be continued at the same server (where it was started);
    - There is no cookies - the next server (according to the selected load balancing algorithm) will be selected;
- **FTP** - the session will be attached to the same physical server from the beginning to the end (both ports control and data port are considered as a bundle);
- **HTTPS –** the session will be routed according to SSL ID :
    - NEW SSL session – the packets will routed to the next server (according to the selected load balancing algorithm);
    - SSL ID not expired - the packets will routed to the server where SSL session was started;
    - SSL ID expired – see NEW SSL session ;
- **UDP** – the session will not be attached to same physical server**,** and could be routed according to the selected load balancing algorithm;
- **TCP and UDP** - this service value allows to Administrator define two different behaviors (see **TCP**, **UDP** description) using one rule;
- **TFTP** – see **FTP** description;

Destination Port - the logical port for this service;
Inactivity Timer – the time (in seconds) when the connection between the virtual IP and the real server
Source Zone: the zone from where the traffic is going to be balanced;

The Source IP Addresses and Source Port Settings Configuration

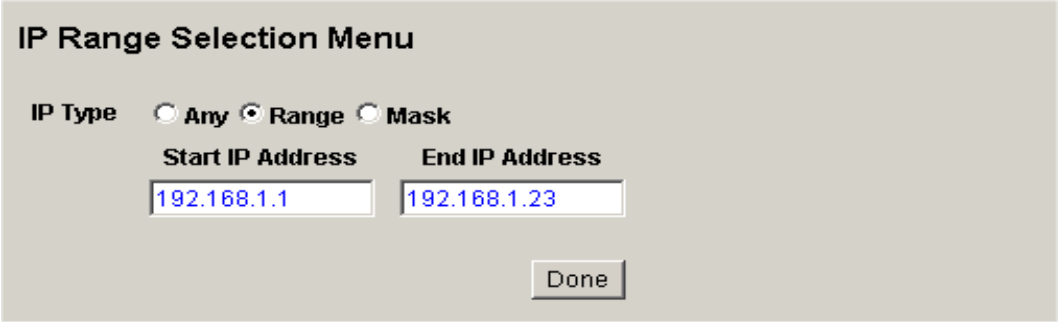
To configure IP Address settings for the rule:
Click on **Source IP** or **Destination IP** link in the **Basic Configuration** window.

Figure 95. Load Balancing->Switching Config->Switching Rule->IP Settings



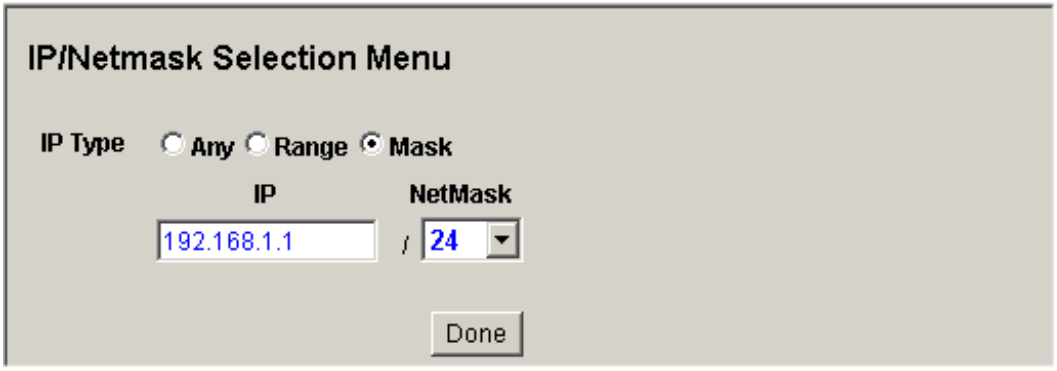
IP Type – Any: all IP Addresses are covered by this rule.

Figure 96. Load Balancing-> Switching Config->Switching Rule->IP Settings (cont.)



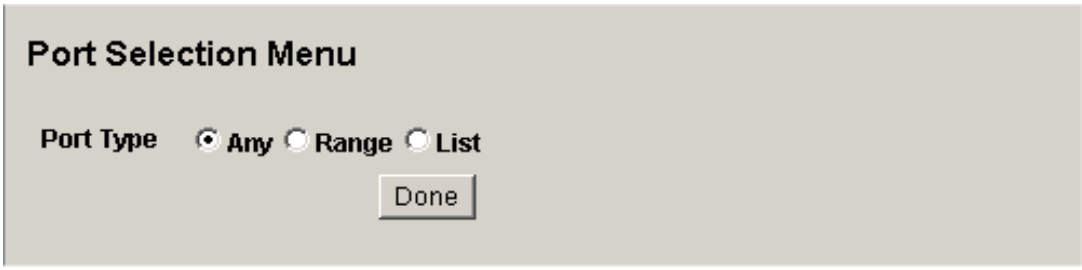
IP Type – Range: this rule will work only for the addresses within the defined range.

Figure 97. Load Balancing-> Switching Config->Switching Rule->IP Settings (cont.)



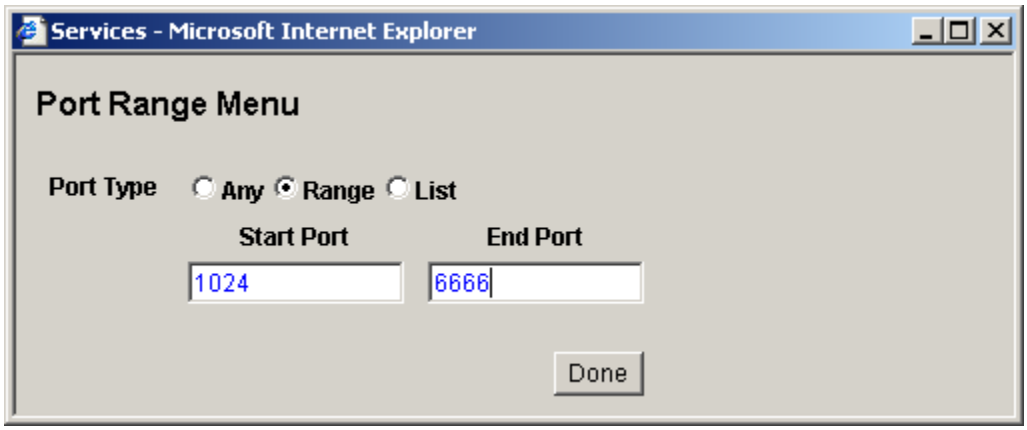
IP Type –Mask: this rule will work only for the IP addresses belonging to a specific subnet.
To configure Network Ports settings for the rule:
Click on **Source Port** or **Destination Port** link in the **Basic Configuration** window.

Figure 98. Load Balancing-> Switching Config->Switching Rule->Port Settings



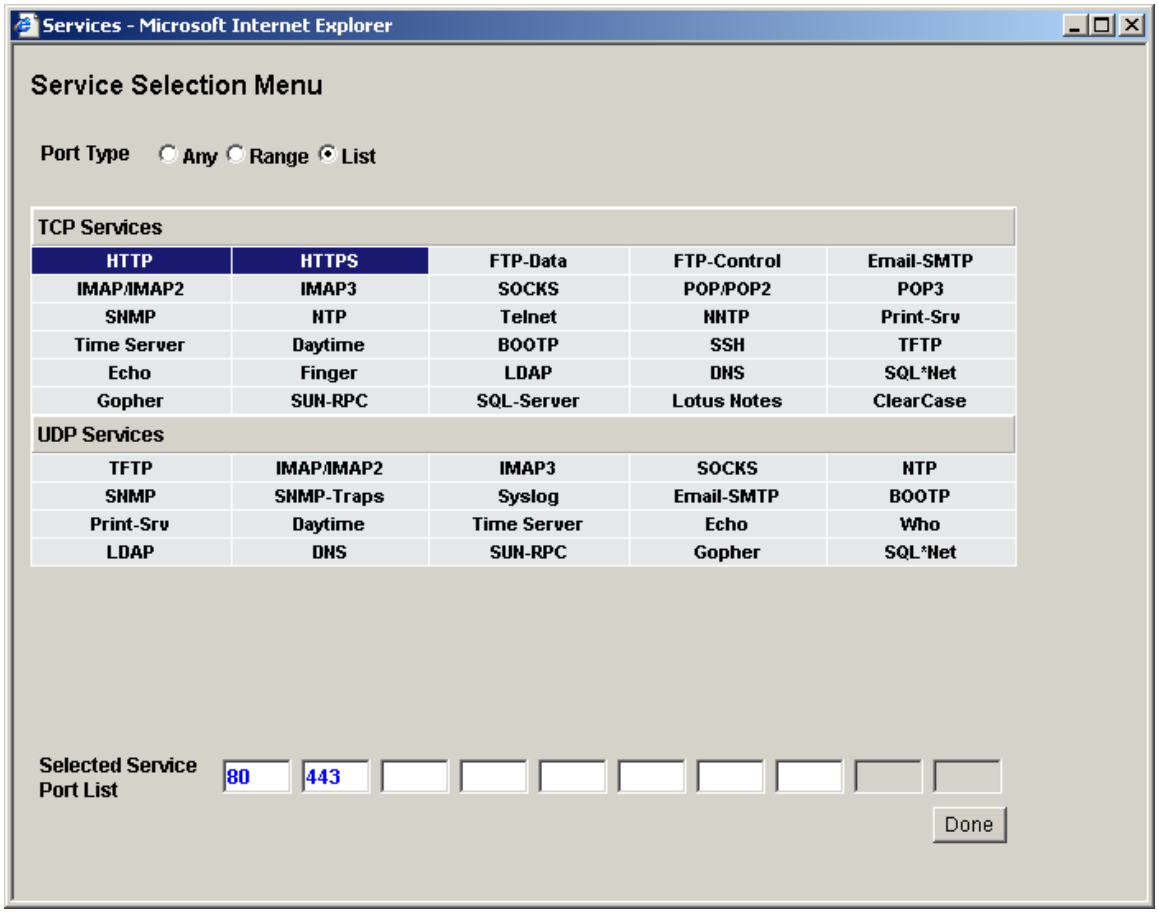
Port Type – Any: all ports are covered by this rule.

Figure 99. Load Balancing-> Switching Config->Switching Rule->Port Settings (cont.)



Port Type – Range: this rule will work only for the ports within the defined range.

Figure 100. Load Balancing-> Switching Config->Switching Rule->Port Settings (cont.)

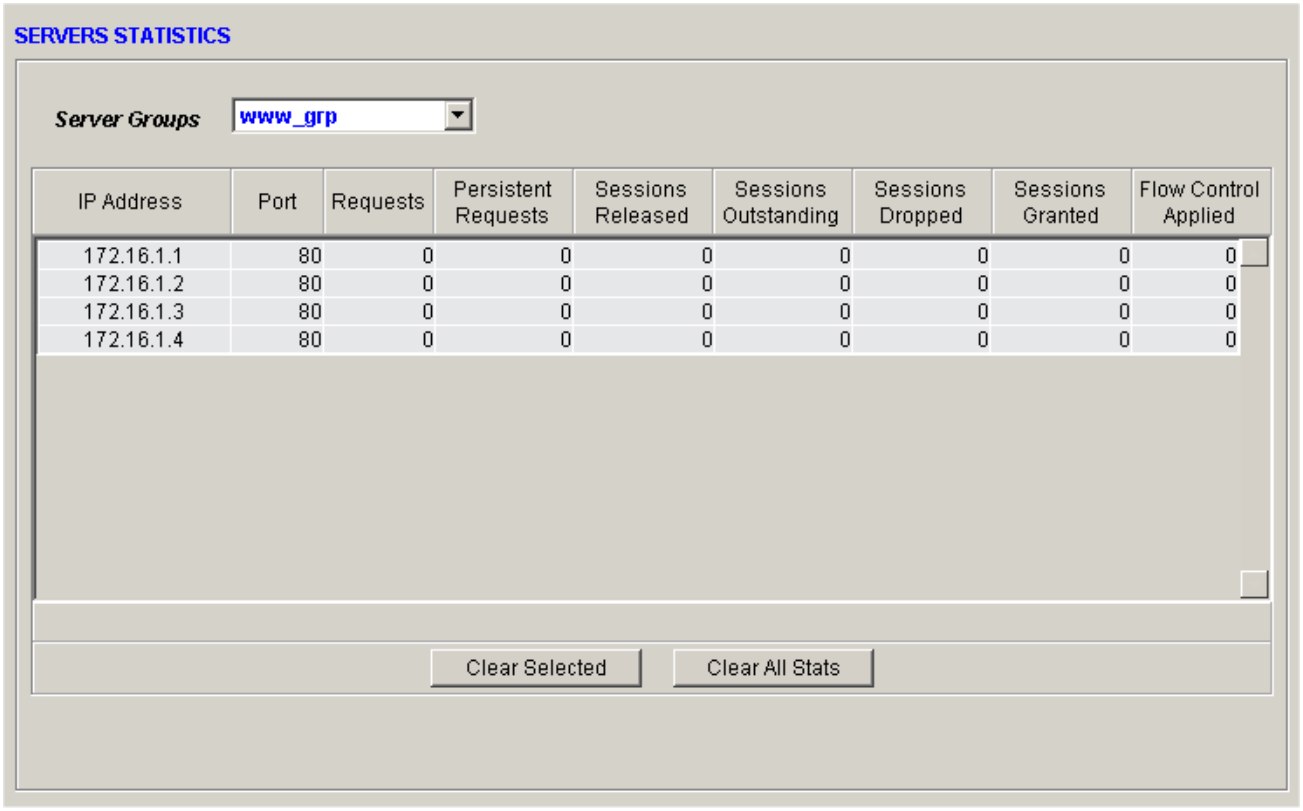


Port Type – List: the list of network ports that will be covered by this rule. Up to 10 ports are allowed for a single rule.
To save the IP Addresses **and** Port Settings **configuration press** Done **button.**

9.2.5 Step 5 (Monitoring)

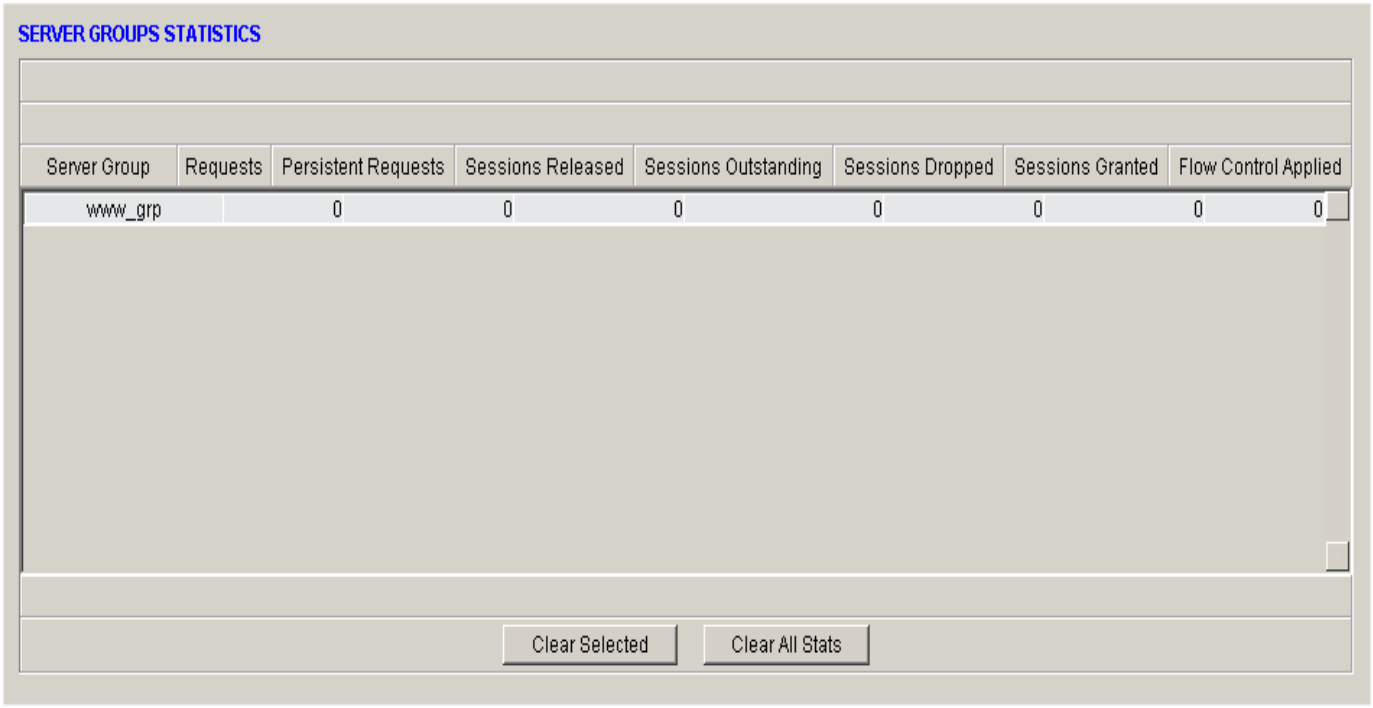
The monitoring tabs such as 'Servers in Server Group', 'Server Groups Statistics', 'Servers Statistics' under Load Balance → Server Configuration menu can be used to monitor operational status of real servers in every server group. Also the number of requests, persistent requests, sessions released, sessions outstanding, sessions dropped, sessions applied for each server group or member real server can be monitored.

Figure 101. Load Balancing->Server Configuration->Servers Statistics



Any user web requests to 203.30.220.141 are processed by RNxx device and equally distributed among members of the server group 'www-grp' in a weighted round robin fashion.

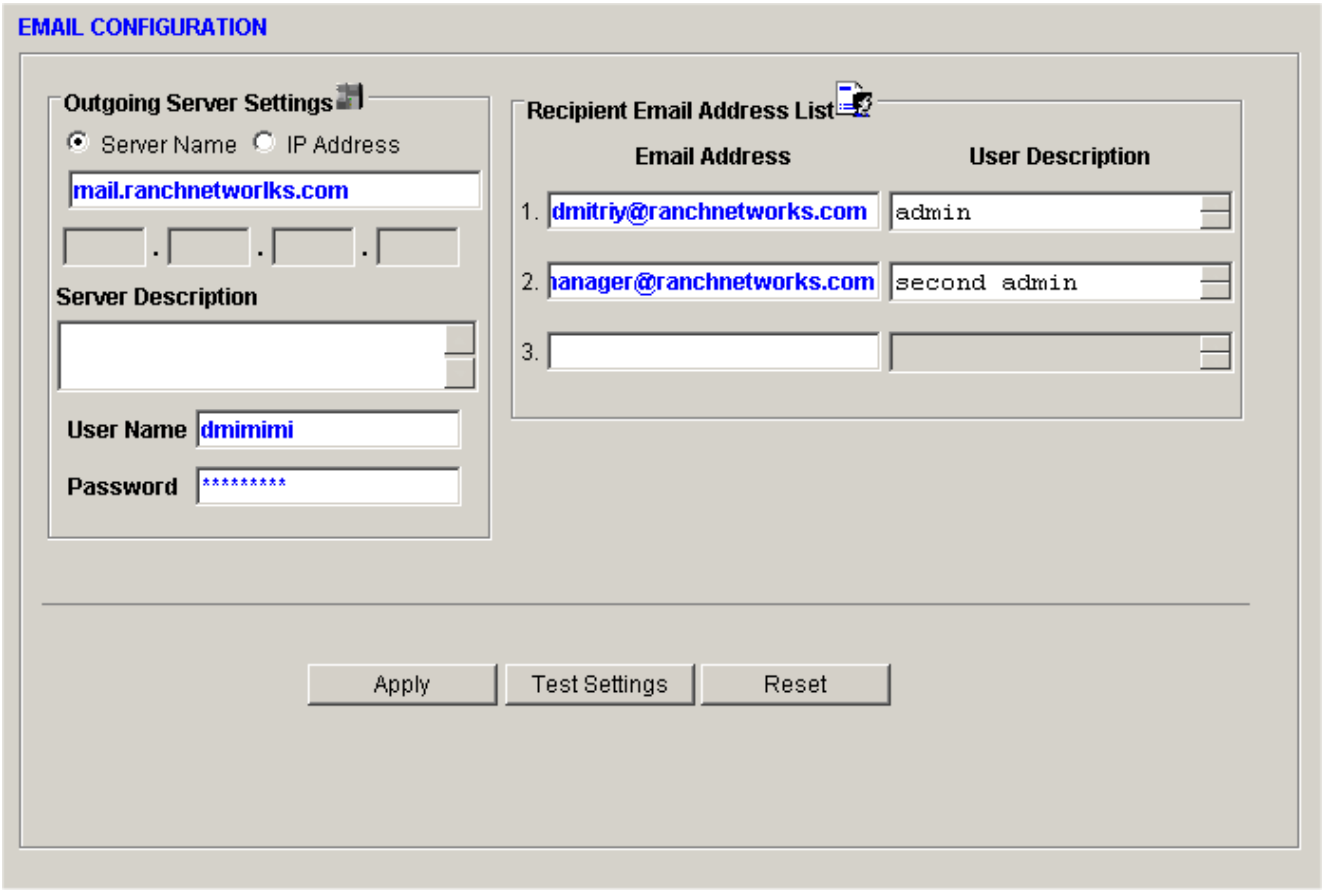
Figure 102. Load Balancing->Server Configuration->Server Groups Statistics



9.2.6 Email notification

One of the most important part of any monitoring process is to get the bad news as soon as possible. Any RNxx device will send the email notification in case of the server or servers group will change their status (DOWN or UP)
The email notification config :

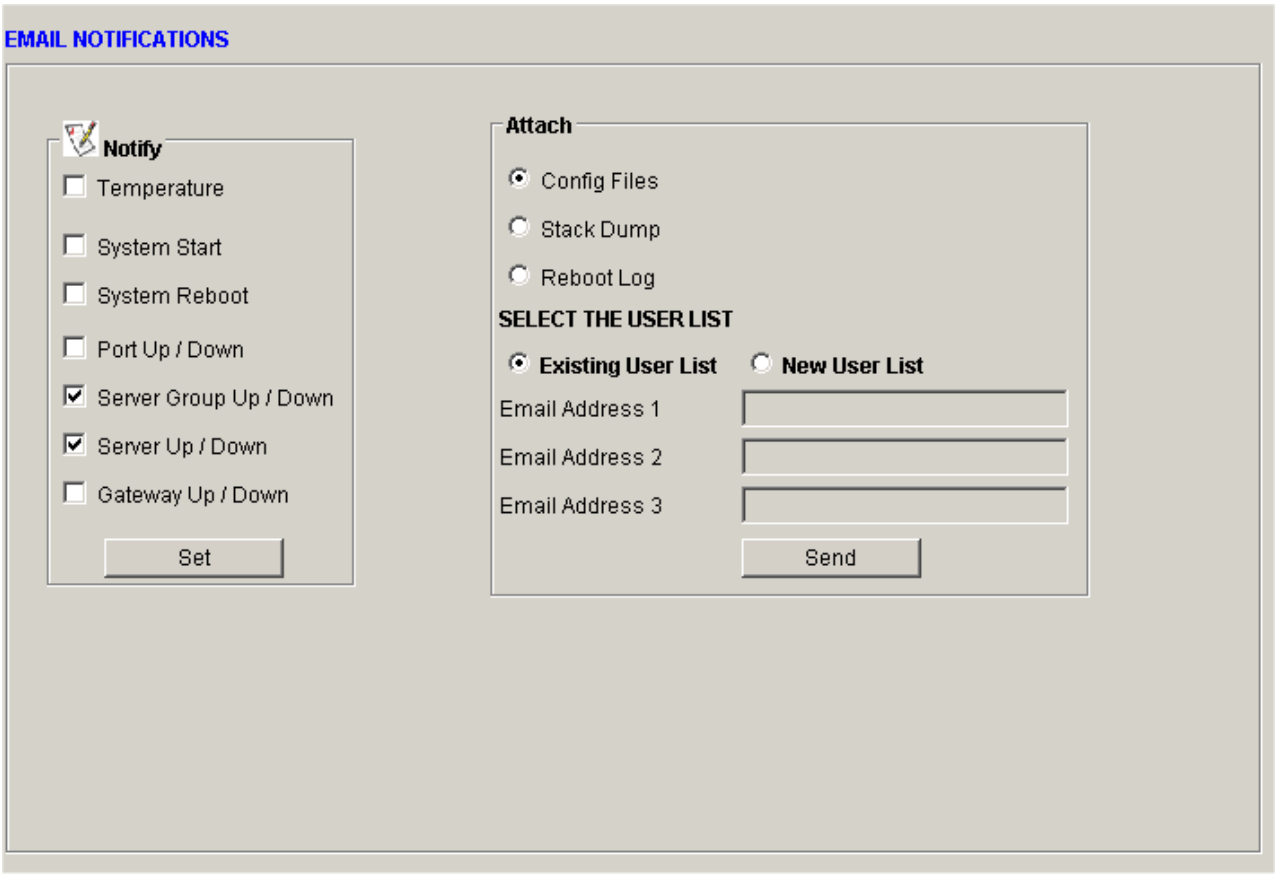
Go to System Configuration->Syslog & Alert Config->Email Configuration



This screen consists of the basic email configuration that will allow RNxx device to send the email notification

Outgoing Server – the email server that is used as to send the email (SMTP server)
Server Description - the description info for the SMTP server
User Name – the user name for the SMTP server (if the login required)
Password – the password for the SMTP server (if the login required)
Recipient Email Addresses List - the list of the recipients that should be notified .

Go to System Configuration->Syslog & Alert Config->Email Configuration->Email Notification



Check the options for the **Server Group UP/DOWN** and **Server UP/DOWN**

10. Servers Health Monitoring

Server Health Monitoring (SHM) is a feature that tracks the operational status of a server when it needs close attention from the network manager. It detects whether your server is operating normally or failed. It is designed to monitor virtually and type of servers including: Web, FTP, Mail, application servers and database servers. Once configured, the monitoring goes on all the time, 24 X 7 coverage. Server Health Monitoring is a high-value feature and a top goal of the production support team.

It should be noted that NO changes to the server are needed to participate in the monitoring process. You don't have to install or upgrade any software modules, there is absolutely no intrusion into the operating environment of the server.

Server Health Monitoring provides the trending information

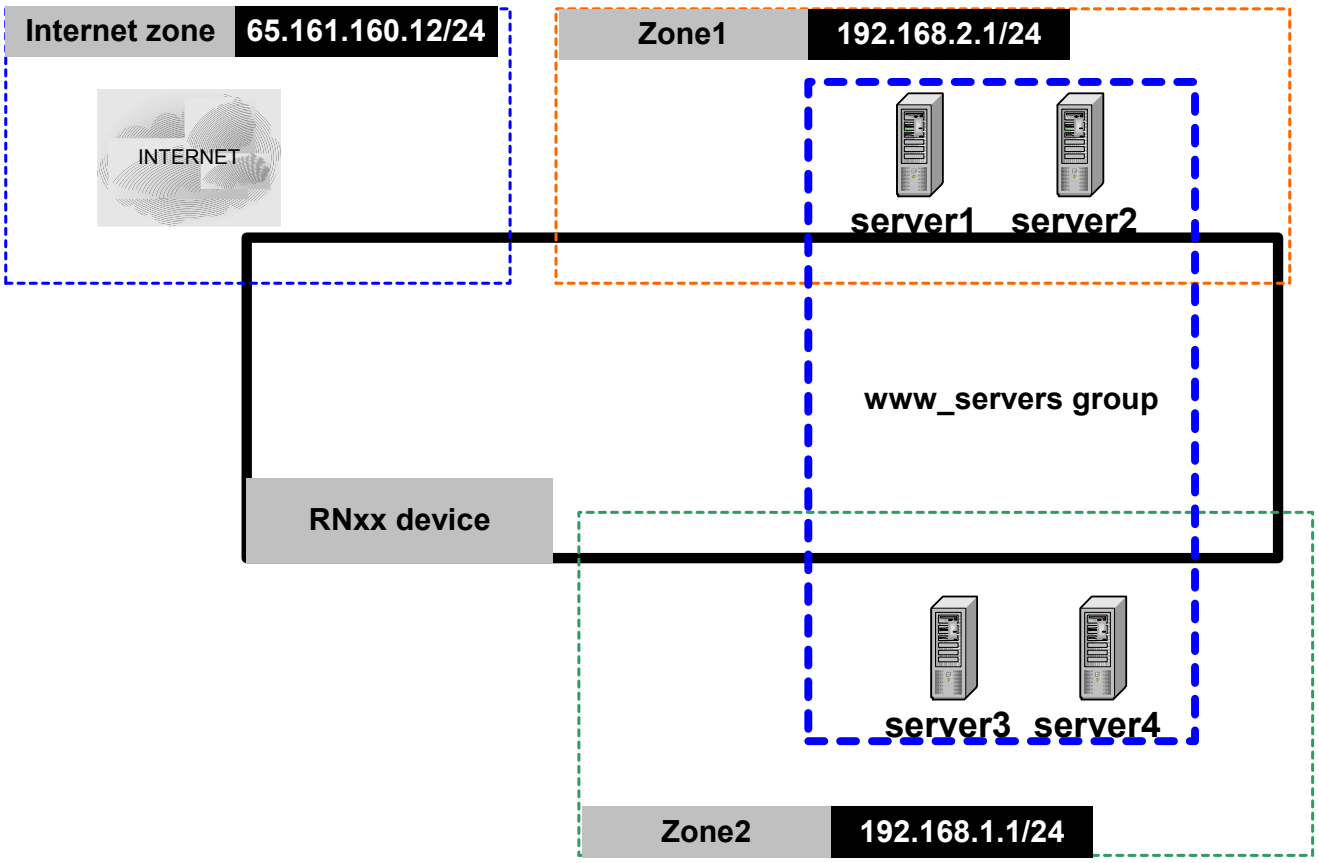
- For executives, who want to make sure their online operations are performing.
- For administrators, who require detailed server-wise reporting.
- For technical managers, who want to right-size their online operations and only purchase equipment when necessary.
- For marketing departments, who want to compare system performance with a Web site traffic volume.

Features:

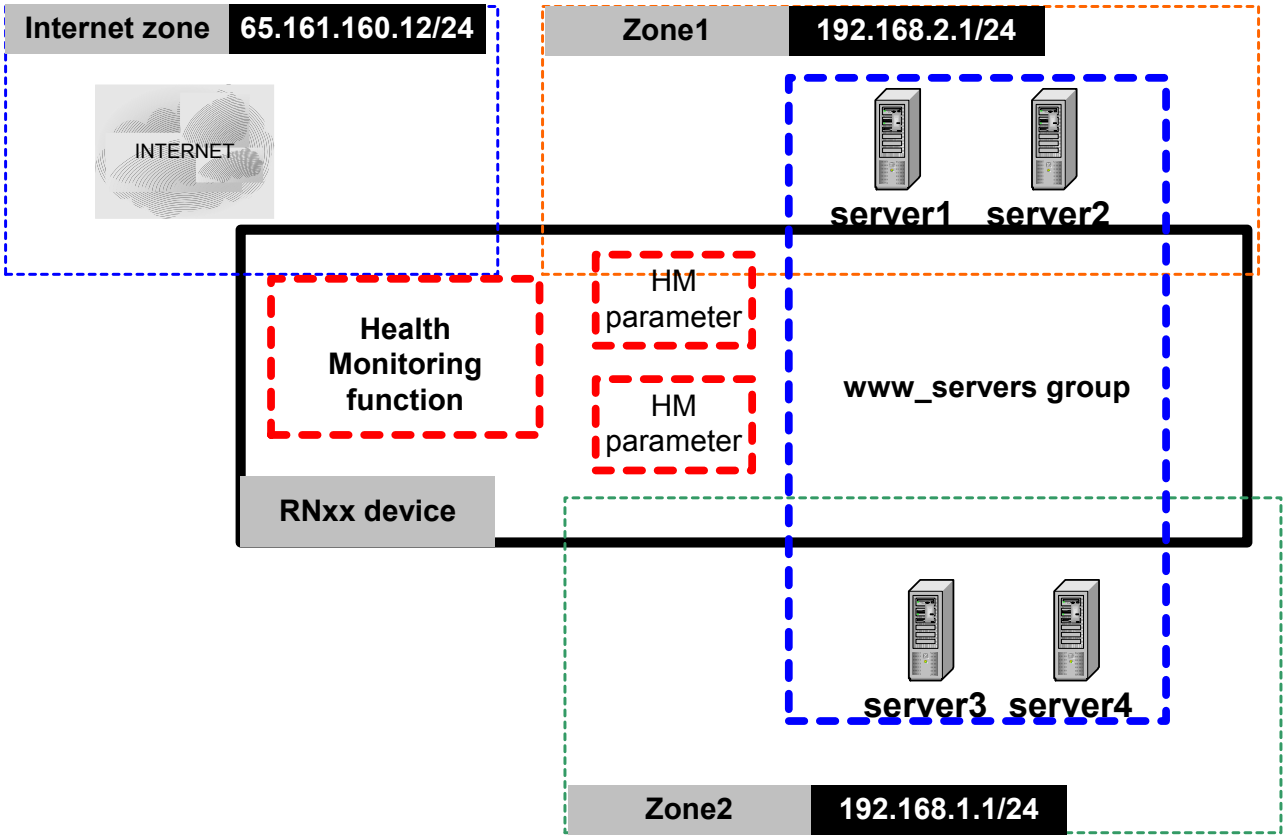
- No server side changes are required.
- 24/7/365 monitoring.
- Monitoring can be enabled at TCP/UDP service levels, regardless of the server's operating system (Windows or Unix).
- End user and administrator perspective.
- Configurable server polling intervals.
- Any TCP/UDP service with port number and ICMP service can be configured for health monitoring. It can be done using several techniques at different layers of the network stack:
    1. At the network (IP) layer using ping (ICMP)
    2. At the transport layer using TCP/ UDP probes on specific ports
    3. At the application layer (Layer 5+) using application specific requests. The supported applications are HTTP and FTP.
- Server-wise reports with detailed parameters such as total number of request, responses, number of missed responses, current operational status, etc.
- Options to configure HTTP (health monitoring URL, and GET/PUT methods), and FTP parameters (IP address, user name, password, file name to GET) per server group.

General steps to configure Server Health Monitoring

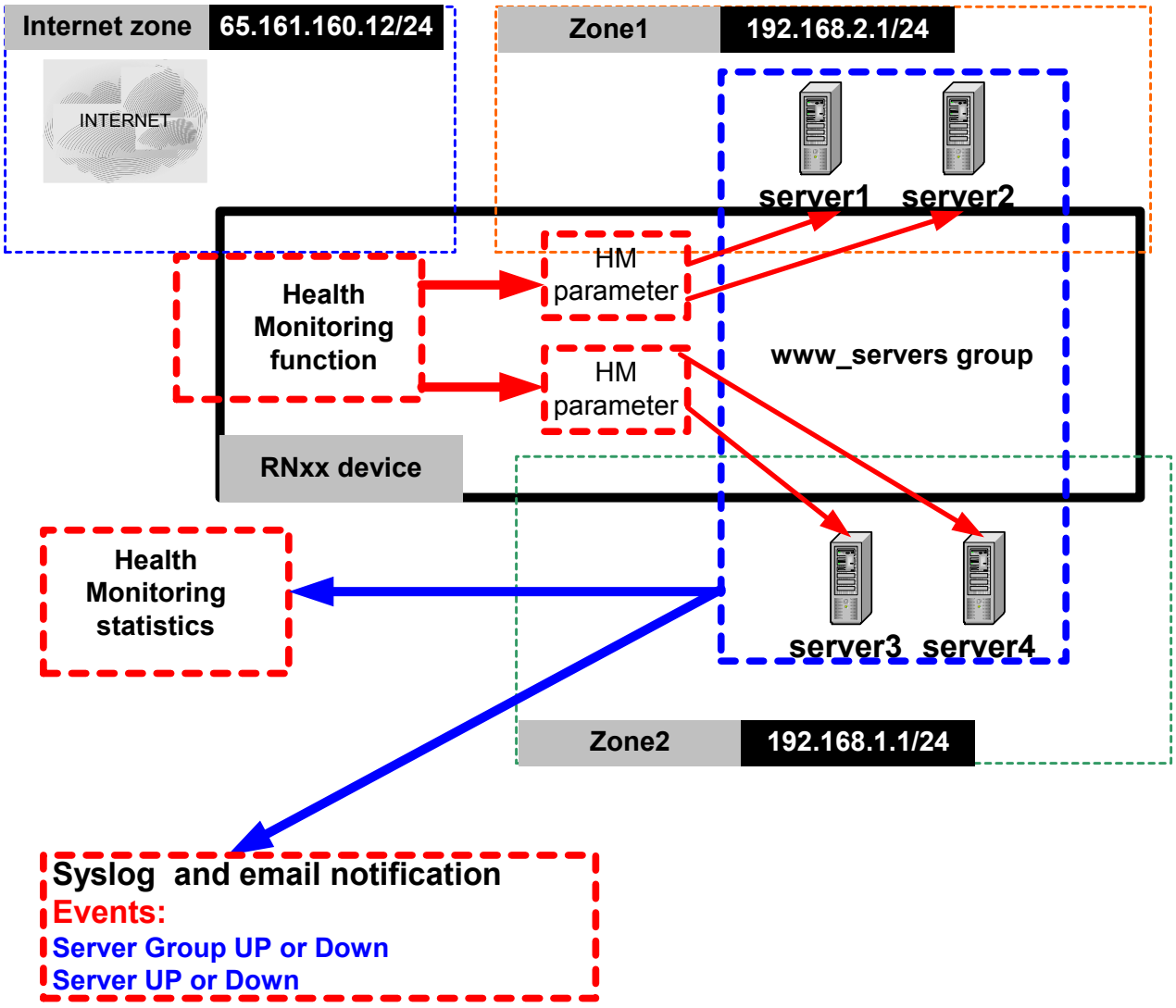
Step 1.
Lets create a server group (for example www_servers) and populate it with 4 servers (the servers could be taken from any of configured zones).



Step 2.
Add the server group to the health monitoring (if the server group was created as a part of the load balancing configuration then it will be added to the health monitoring automatically), configure the parameters for the health monitoring (HTTP,HTTPS,TCP/UDP,ICMP). Assign the health monitoring parameters and pooling frequency to the server group.


Internet zone
65.161.160.12/24
INTERNET
Zone1
192.168.2.1/24
server1
server2
HM
parameter
Health
Monitoring
function
HM
parameter
www_servers group
RNxx device
server3
server4
Zone2
192.168.1.1/24

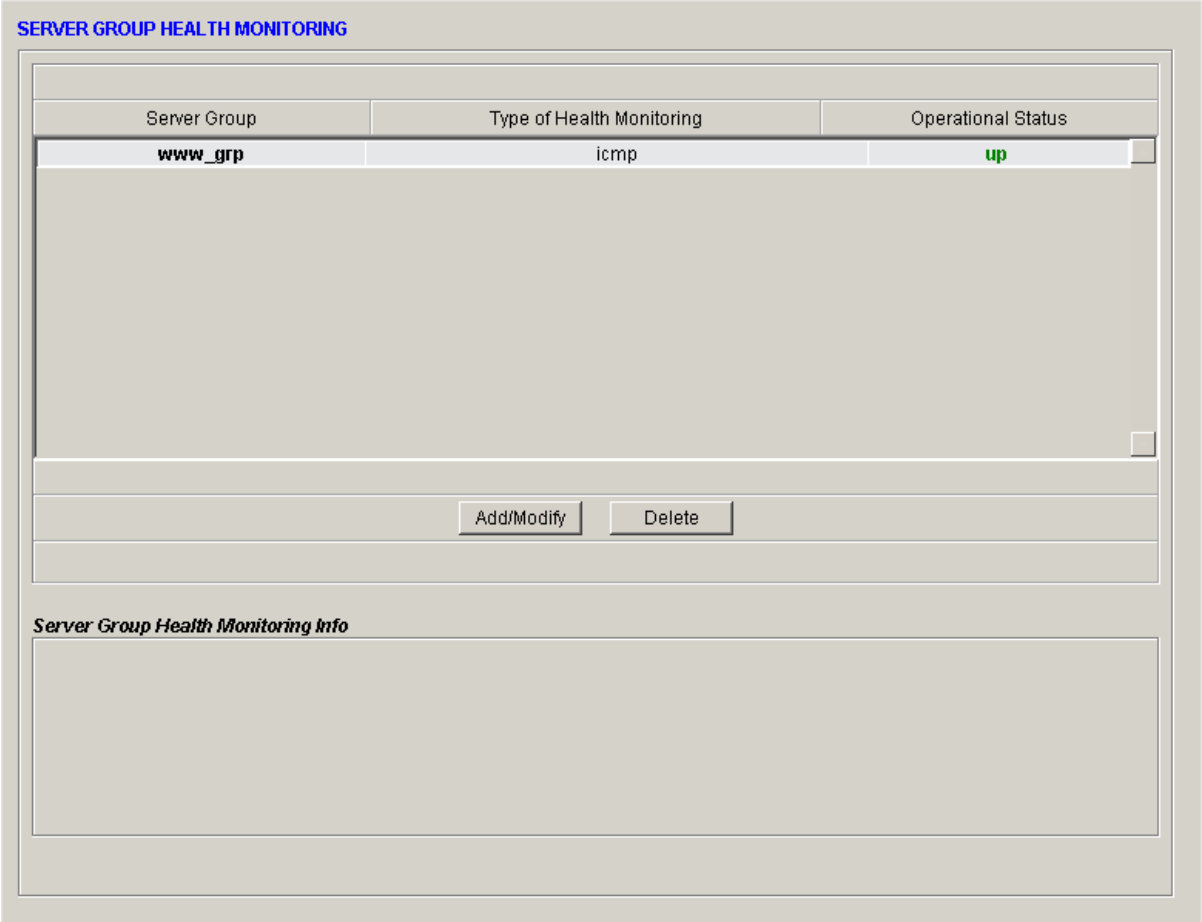
The picture bellow illustrates the health monitoring process



10.1 Server Group Configuration

Go to Servers Health Monitoring → Server Group HM to start SHM configuration for any server group and its members.

Figure 103. Server Health Monitoring->Server Group HM

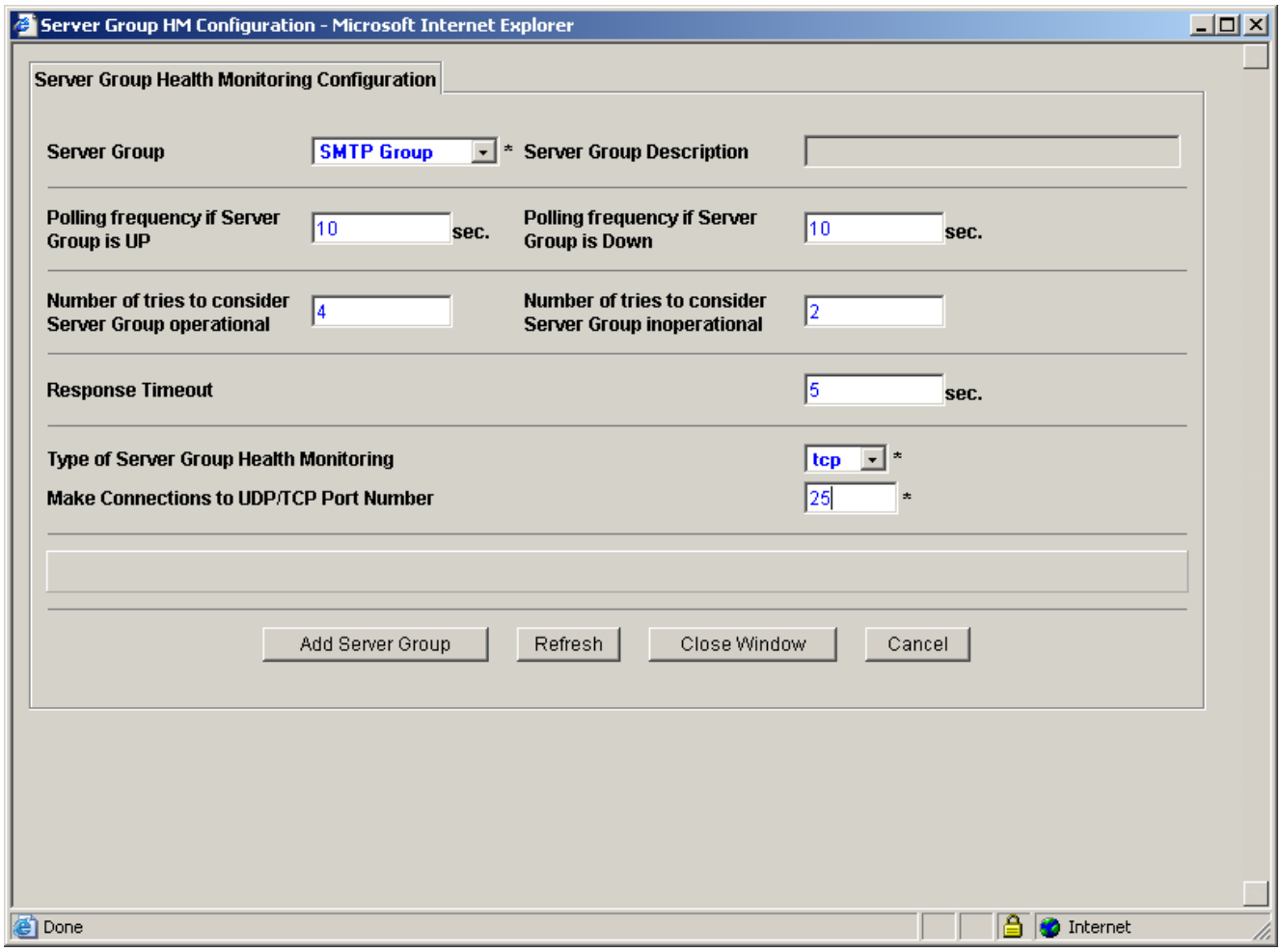


Server Group HM Fields:

Server Group Name: The name of the server group to be monitored.
Type of Health Monitoring: The method that is used for monitoring process (e.g., tcp, udp, http, ftp, icmp, etc.).
Operational Status: The current operational status of the group. It could be either '**up**' or '**down**', the value being a result of the monitoring process.

Click on 'Add / Modify' button to add a new configuration (or to modify existing configuration entry). A new 'Server Group HM Configuration' popup window appears. Select the desired Server Group from 'Server Group' drag down list, for instance, SMTP Server Group. Select 'Type of Server Group Health Monitoring' as 'tcp', enter TCP/UDP port number as '25' and click on 'Add Server Group'. This example uses default polling frequency, number of retries to declare a result, and response time.

Figure 104. Server Health Monitoring->Server Group HM (cont.)



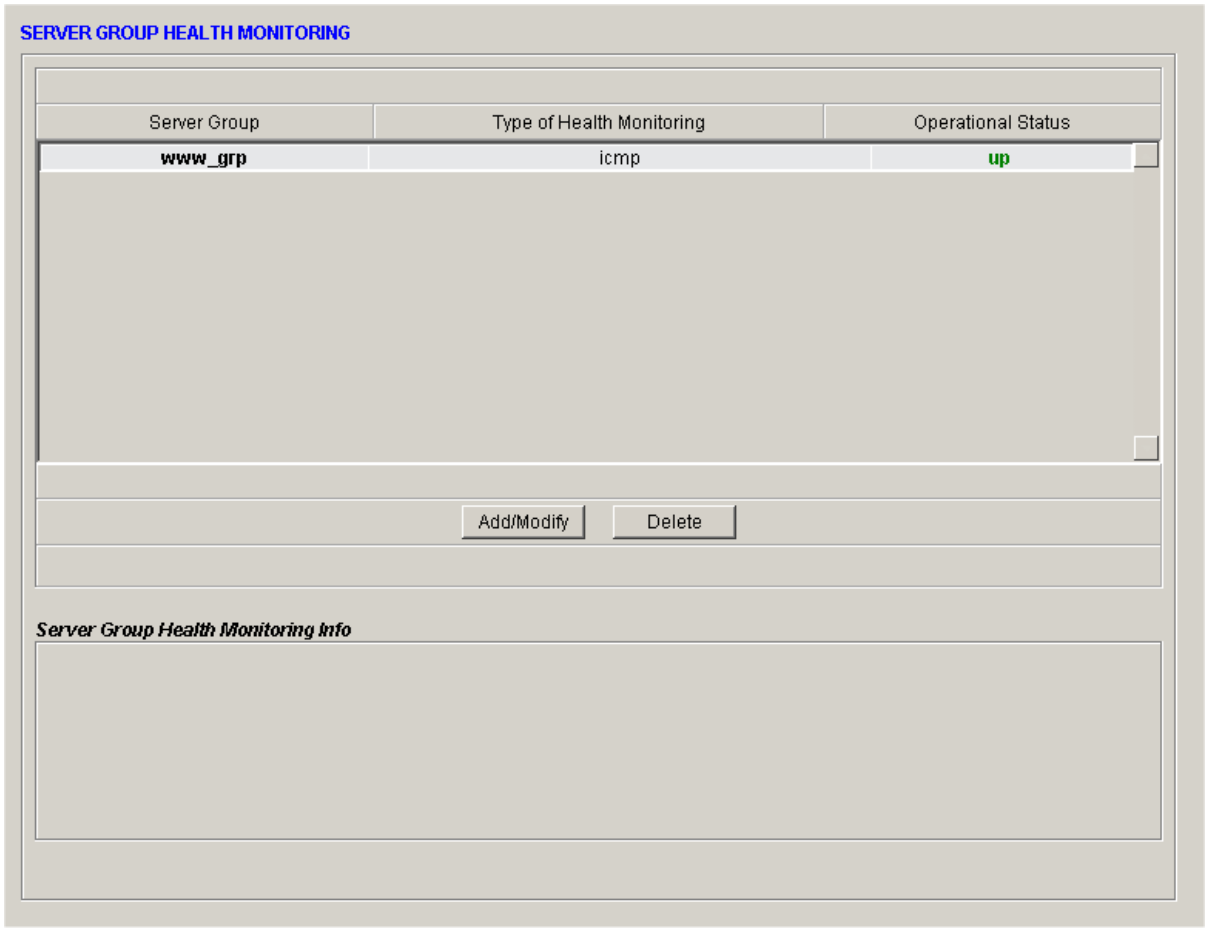
Server Group Health Monitoring Configuration fields:

Server Group: The server group to be monitored. The value is selected from a drop-down menu and should be configured in **Server Groups and Servers**.
Server Group Description: The logical description of the server group. The value is optional and should be defined in **Server Groups and Servers**.
Type of Server Group Health Monitoring: The protocol that will be used for the health monitoring (for ex, tcp, udp, icmp, http, ftp, etc.).
Make Connection to UDP/TCP Port: The service port number that will be used for the connection; should only be a numeric value.
Polling frequency if Server Group is UP: The time between the consequent polls if the server group in operational; should be a numeric value only.
Number of tries to consider Server Group operational: The number of the successful attempts (polls) to the server group that will promote this group to the operational status; should be a numeric value only.

Polling frequency if Server Group is Down: The time between the polls if the server group was considered non-operational; should be a numeric value only.
Number of tries to consider Server Group non-operational: The number of the unsuccessful attempts (polls) to the server group that will demote this group to the non-operational status; should be a numeric value only
Response Timeout: The interval (in seconds), after which the poll will be considered as unsuccessful; should be a numeric value only.
FTP parameters configuration: The name of the FTP parameter. It can be selected from a drop-down menu (all FTP parameters such as login, password has to be configured in **FTP HM configuration** table), and set only if FTP method is selected for health monitoring.
HTTP parameters configuration: The name of the HTTP parameter. It can be selected from a drop-down menu (HTTP parameters has to be configured in **HTTP HM configuration** table), and set only if HTTP or HTTPS method is selected for the health monitoring, up to 5 different HTTP parameters could be selected.

Click on 'Close Window'.
This server group entry is listed in the main **Server Group HM** table.

Figure 105. Server Health Monitoring->Server Group HM (cont.)



Any TCP/UDP service and ICMP service can be enabled for monitoring against any existing server group.

Server HM Stats fields:

All the values on this screen are the result of the health monitoring process.

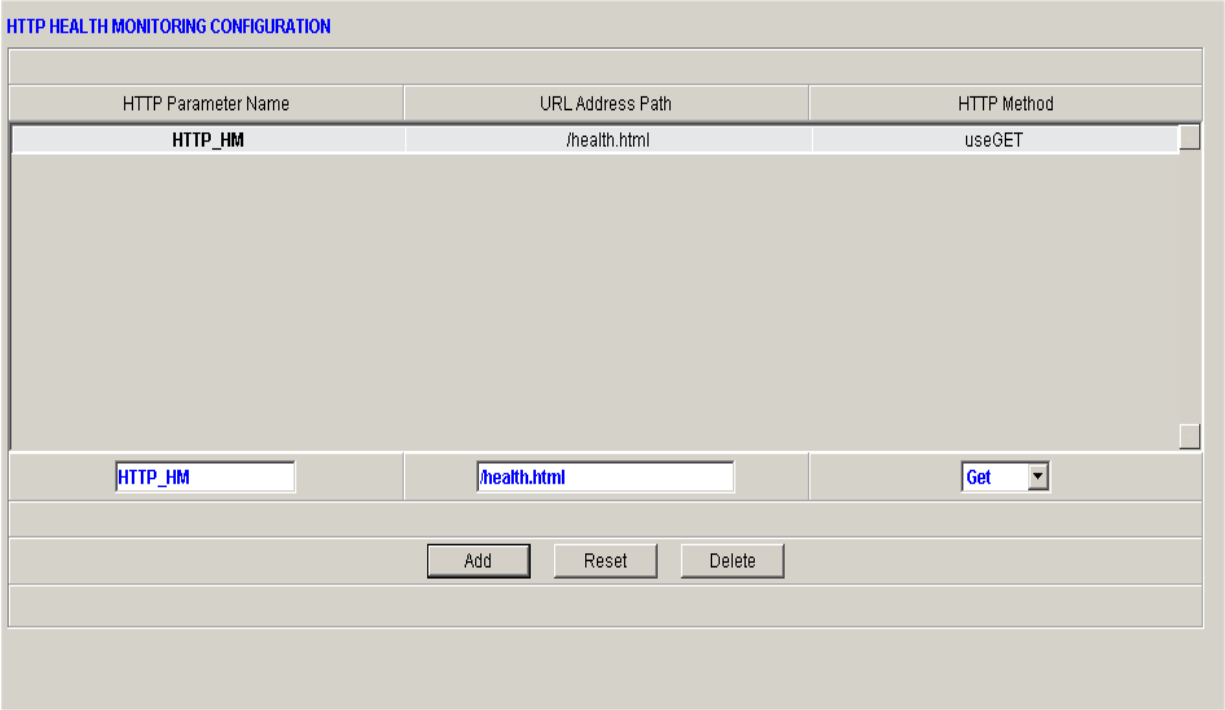
Server IP: IP address of the server (read-only value, inherited from the Server table).
Operational Status: The operational status of the server '**up**' of '**down**' read only value
Requests/Responses: The number of requests/responses since the monitoring started.
Responds Missed: The number of unsuccessful polls.
Operational/Unavailable Min: The amount of time the server status was up/down since the monitoring started.
Average / Minimum / Maximum Response Time milliseconds: The minimum, average and maximum response time since the stats collection started started.
Clear Selected: To clear(restart) the statistics for the server, select the row from the table and press **Clear Selected.**

10.2 Steps to configure HTTP & FTP Health Monitoring

RN40 provides advanced features to configure HTTP/HTTPS and FTP health monitoring (HM) at application level by enabling network manager to define individual HTTP & FTP HM configuration parameters.
First you need to complete HTTP and/or FTP HM configuration before adding HTTP or FTP server group for health monitoring.

10.2.1 HTTP HM Configuration

Figure 106: Health Monitoring -> HTTP HM Configuration



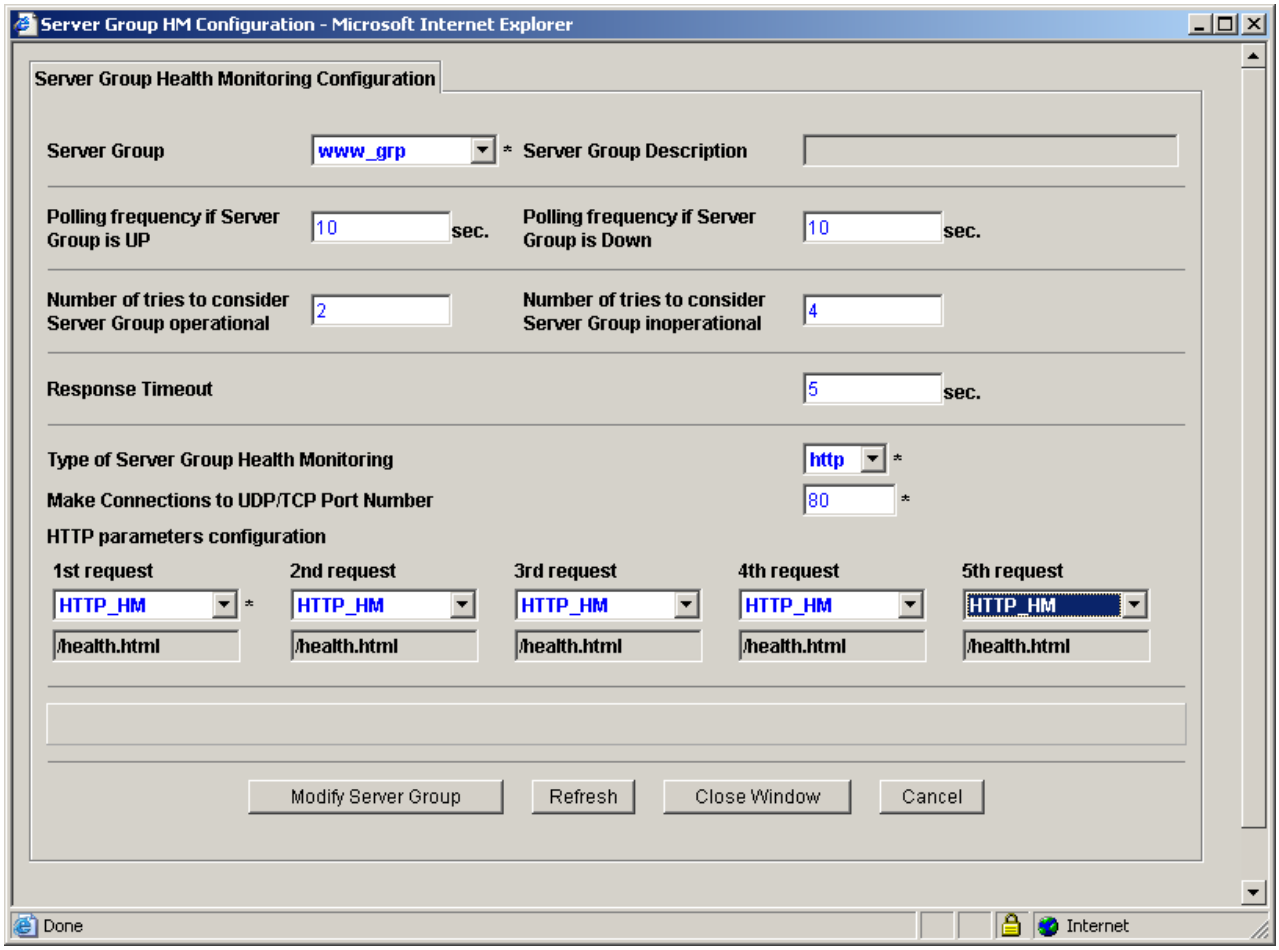
HTTP HM Configuration fields:

HTTP Parameter Name: Enter a unique name (a string characters).
URL Address: URL to be used for HTTP HM.
HTTP Method: HTTP method to be used for HM (GET/PUT/POST).

Go to Server Health monitoring → HTTP HM Configuration menu
Add URL, file names and HTTP method along with parameter names and clicking on 'Add' button. Use full directory path relative to the main HTTP server directory and ensure that the files used for monitoring are physically present and have the 'read' privileges.

Once HTTP HM Configuration is completed, go to 'Servers Health Monitoring' → 'Server Group HM' menu to actually configure HTTP server group for health monitoring.
Click on 'Add/Modify' to add HTTP server group and new window will pop up.

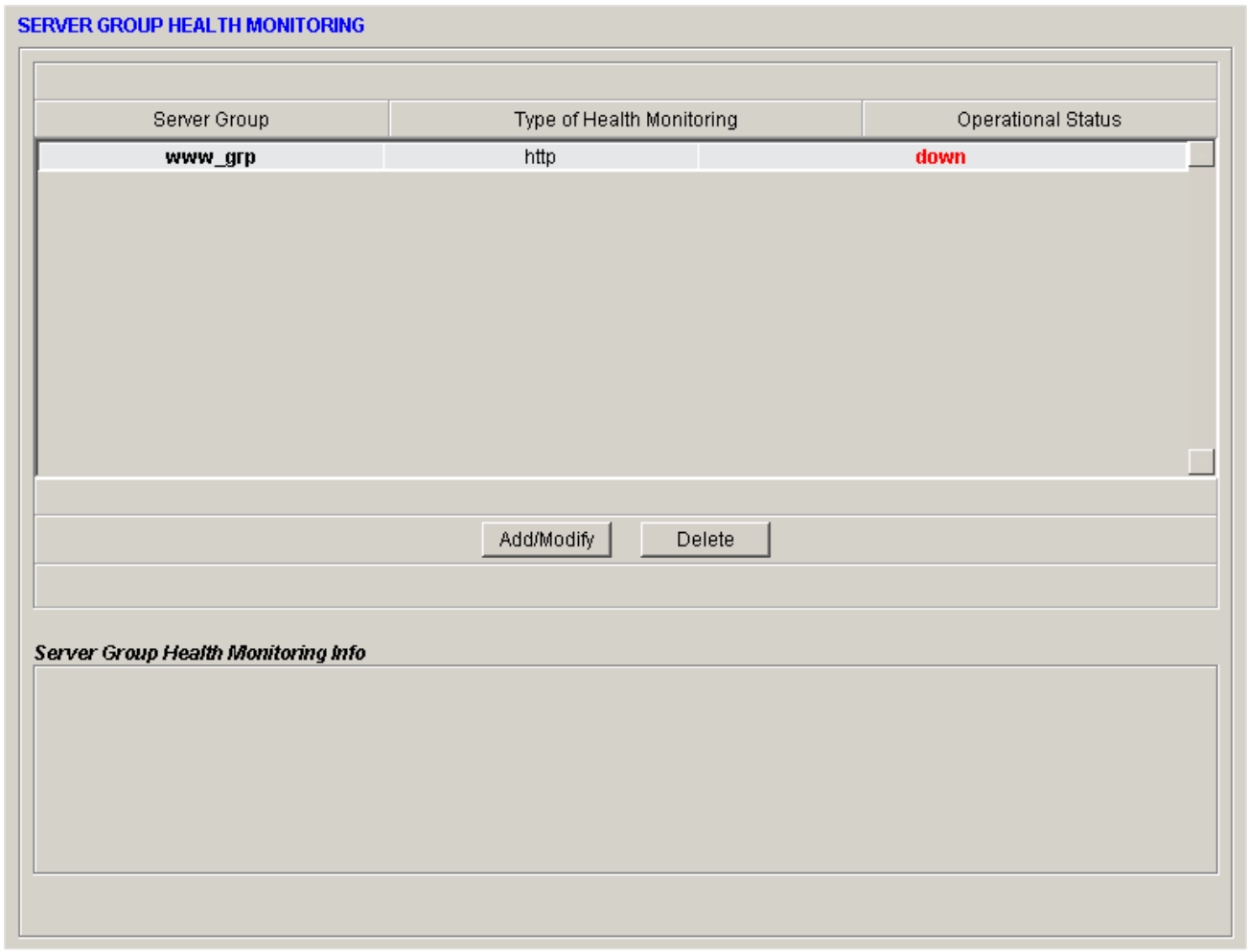
Figure 107.Server Group HM -> HTTP monitoring Configuration



Select Server Group 'Web Group', Type of Server Group Health Monitoring 'http', tcp number '80' and under HTTP parameters configuration select the pre- configured HTTP parameters for the 1st request, 2nd request and so forth.. Click on 'Add Server Group' to add this 'Web Group' for monitoring.

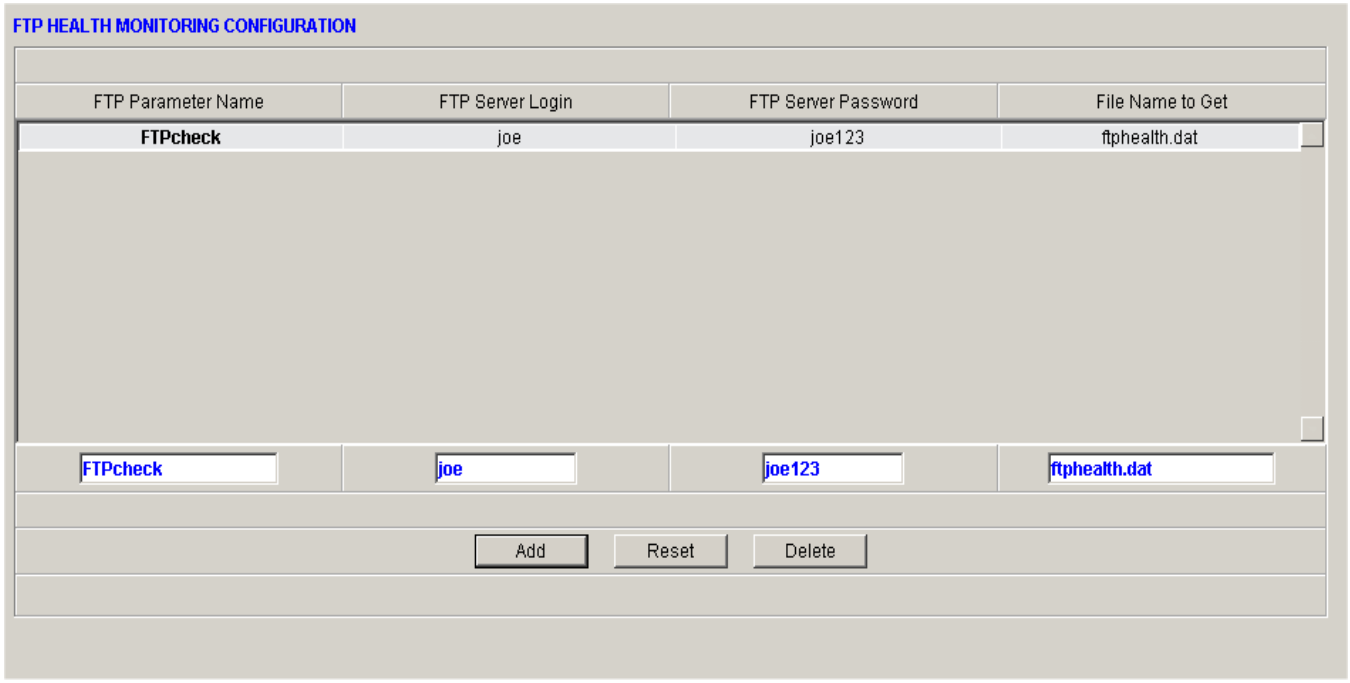
Click on 'Close Window' when finished.

Figure 108. SHM screen with the server groups configured for HTTP HM



10.2.2 FTP HM Configuration

Figure 109 Health Monitoring->FTP HM Configuration



FTP HM Configuration fields:

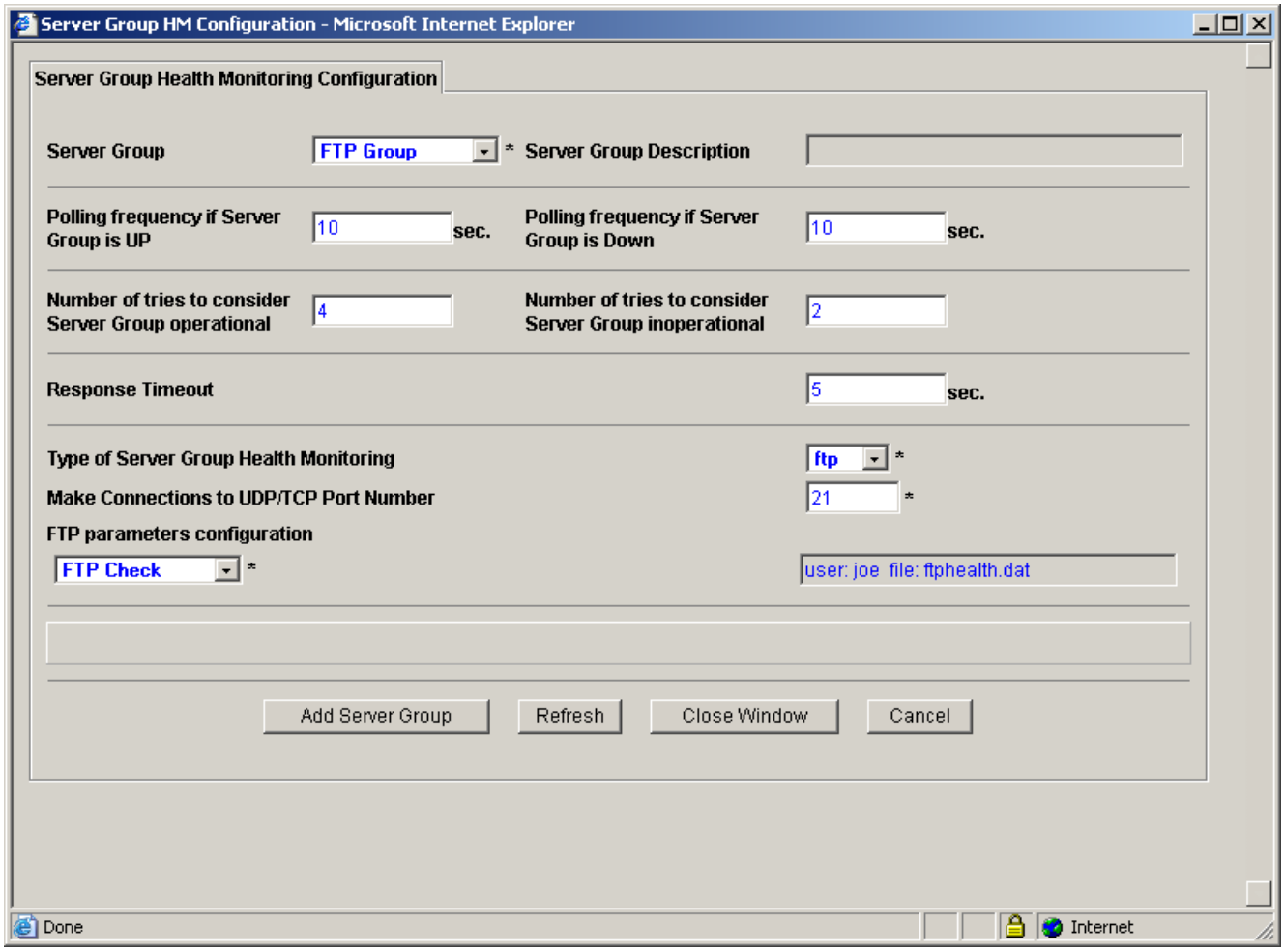
FTP Parameter Name: Enter a unique name (a character string).
FTP Server Login: The login id on the FTP server that needs to be monitored.
FTP Server Password: The password for the above id on the FTP server.
File Name to Get: The name of the file to be retrieved.

Go to Server Health monitoring → FTP HM Configuration menu.
Enter the FTP user name (for example, joe), password (joe123) and FTP health file (for example, ftphealth.dat) along with FTP reference parameter name (for instance, FTP Check). Please verify that the ftphealth.dat file has read permission for GET to succeed.

Caution : Ensure that the same FTP user name, password and ftp health file works for every member ftp servers in FTP Server Group. This same set of parameters are used for health monitoring against each ftp server.

Click on ‘Add’ button to add this parameter.
Once FTP HM Configuration is completed, go to ‘Servers Health Monitoring’ → ‘Server Group HM’ menu to actually configure FTP server group for health monitoring.
Click on ‘Add/Modify’ to add FTP server group and a new window will appear.

Figure 110. Health Monitoring -> Server group HM , FTP HM configuration

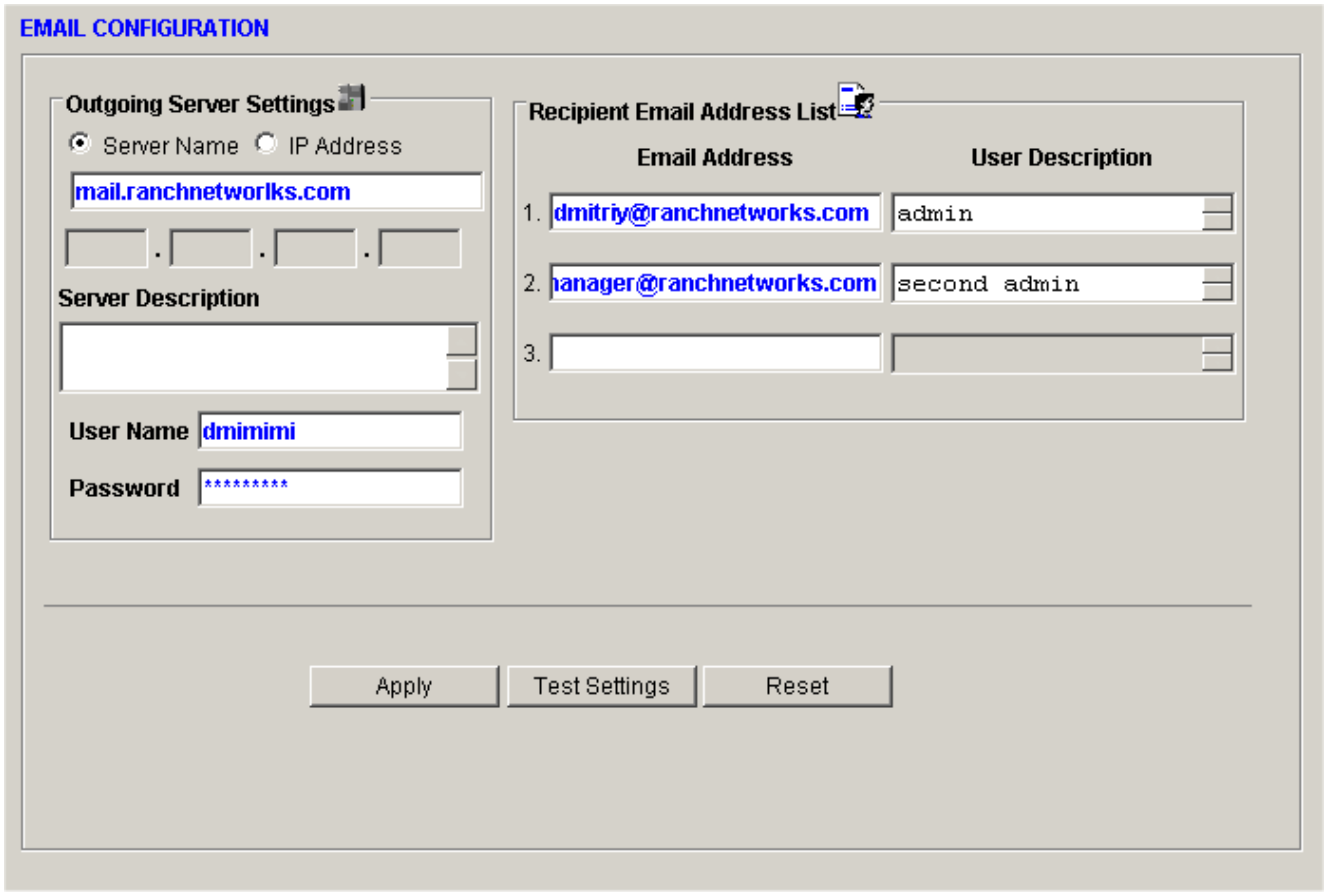


Select a Server Group ‘FTP Group’, Type of Server Group Health Monitoring ‘ftp’, port number ‘21’ and under FTP parameters configuration select a pre-configured ‘FTP Check’ parameter. Click on ‘Add Server Group’ to add this ‘FTP Group’ for monitoring.
Click on ‘Close Window’ when finished.

10.2.3 Email notification

One of the most important part of any monitoring process is to get the bad news as soon as possible. Any RNxx device will send the email notification in case of the server or servers group will change their status (DOWN or UP)
The email notification config :

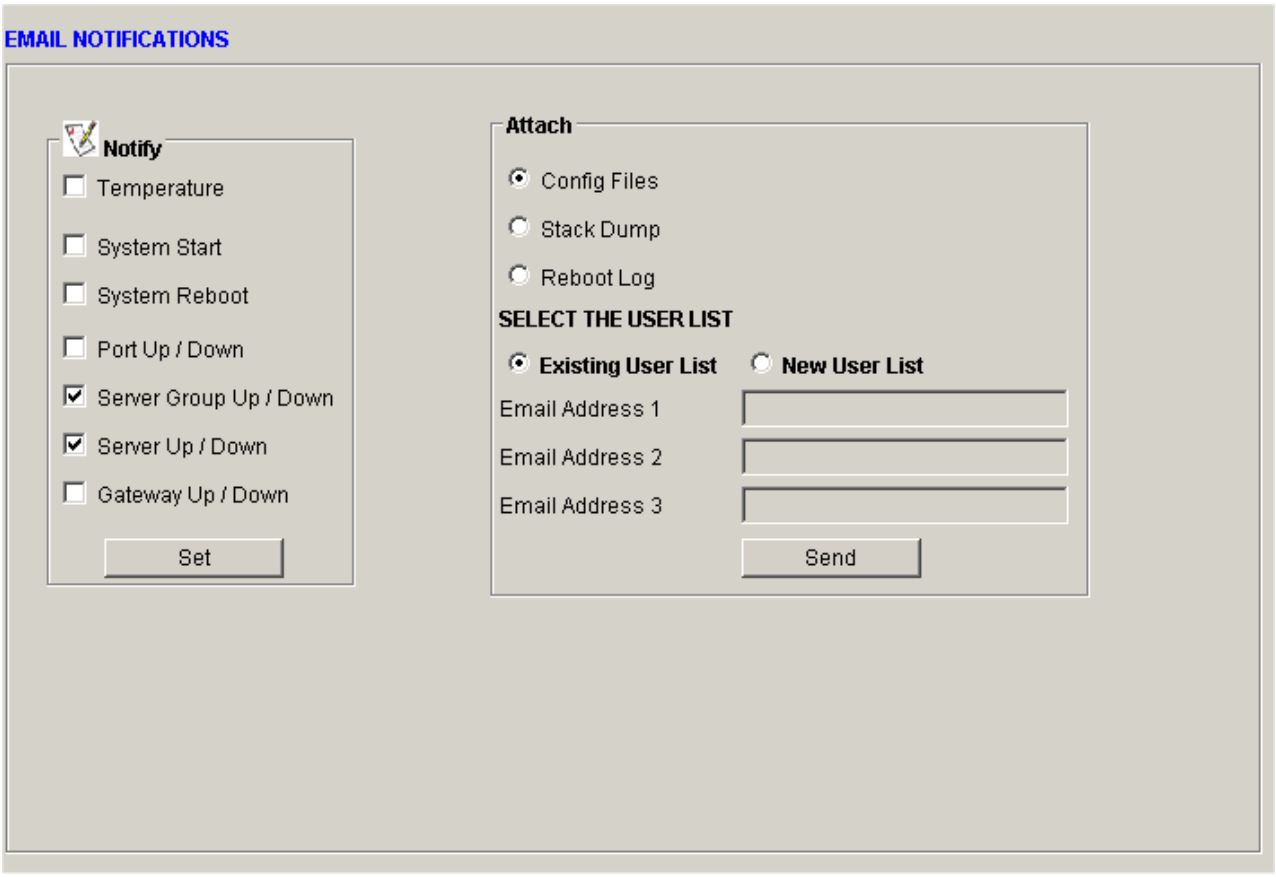
Go to System Configuration->Syslog & Alert Config->Email Configuration



This screen consists of the basic email configuration that will allow RNxx device to send the email notification

Outgoing Server – the email server that is used as to send the email (SMTP server)
Server Description - the description info for the SMTP server
User Name – the user name for the SMTP server (if the login required)
Password – the password for the SMTP server (if the login required)
Recipient Email Addresses List - the list of the recipients that should be notified .

Go to System Configuration->Syslog & Alert Config->Email Configuration->Email Notification



Check the options for the **Server Group UP/DOWN** and **Server UP/DOWN**

11.Multicast Configuration

(RN 5/20/40/41 models only)

Multicast is a traffic type which is originated from a single sender and destined for multiple receivers. Multicast-enabled networks allow users to receive streaming video and audio programs. Other emerging applications that heavily rely on multicasting are computer based video conferencing, corporate broadcasts, LAN TV, etc.

Traditional network applications involve communications between two end points. However, the newly emerged applications such as LAN TV, desktop conferencing, corporate broadcasts, and collaborative computing require simultaneous communication between groups of computers or in other words, point to multipoint communication.

There are three ways to explain multipoint networking: unicast, broadcast, and multicast transmission.

- **Unicast:** Applications based on unicast transmission send one copy of each packet to an individual node in the group. This method is easy to implement, but offers significant scaling restrictions if the group is large. Moreover, delivery time variations might be unacceptable from the application perspective.

- **Broadcast:** Applications based on broadcast transmission simply broadcast the packets in the network. This technique is even simpler to implement than unicast, but introduces a substantial risk of saturating the network. It is a palpable stress on the network resources, especially when the group destination nodes is small.

- **Multicast:** Multicast applications can send one copy of each packet to a whole group of nodes. Since only a single copy is transmitted to a set of destination, the multicast applications rely on the network to efficiently deliver it.

Multicast is a very efficient technology. It is easy on both the hosts and the networks. However, in order for multicast to work, the networking devices need to know which computers need to receive multicast traffic, and they need to be able to dynamically build efficient paths to the destinations.

11.1 Multicast Terms and Concepts

Multicast Group: Multicast is based on the concept of a group. An arbitrary group of receivers express an interest in getting a particular data stream. This group does not have any physical or geographical boundaries - the hosts can be located anywhere on the

Internet. Hosts that are interested in receiving traffic destined to a particular group must join that group.

IP Multicast Addressing: The IP address space is divided into four categories: Class A, Class B, Class C, and Class D. Classes A, B, and C are used for unicast traffic. Class D is reserved for multicast traffic. Class D addresses are allocated dynamically.

Host Extensions for IP Multicasting [RFC1112] specifies the extensions required from the host to support multicasting. The multicast addresses are in the range 224.0.0.0 through 239.255.255.255.

Note: This address range is only for group addresses or destination addresses of IP Multicast traffic. The source address for multicast datagrams is always the unicast source address.

IP Multicast Dynamic Registration: RFC 1112 defines the Internet Group Membership Protocol (IGMP). IGMP specifies how the host should inform the network that it is a member of a particular multicast group.

Multicast Routing: In unicast routing, traffic is routed through the network along a single path from a source to a destination host. A unicast router does not really care about the source address—it only cares about the destination address and how to forward the traffic towards that destination. The router scans through its routing table and forwards a single copy of the unicast packet via a selected interface in the direction of the destination.

In multicast routing, the source is sending traffic to an arbitrary group of hosts represented by a multicast group address. The multicast router must determine which direction is upstream (toward the source) and which direction (or directions) is downstream. If there are multiple downstream paths, the router replicates the packet and forwards the traffic down the appropriate downstream paths—which is not necessarily all the paths. This concept of forwarding multicast traffic away from the source, rather than towards the receiver, is called ‘reverse path forwarding’.

There are several standards available for routing IP Multicast traffic.

- **DVMRP** (Distance Vector Multicast Routing Protocol) – defined by RFC 1075
- **MOSPF** (Multicast Open Shortest Path First protocol) – an extension to OSPF that allows it to support IP Multicast – defined by RFC 1584
- **PIM** (Protocol Independent Multicast) – a multicast protocol that can be used in conjunction with all unicast IP routing protocols – described by Internet drafts. PIM can leverage whichever unicast routing protocols are used to populate the unicast routing table, including EIGRP, OSPF, BGP, or static routes. PIM uses

this unicast routing information to perform the multicast forwarding function, and although PIM is called a multicast routing protocol, it actually relies on the unicast routing table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing tables. PIM neither sends to nor receives multicast route updates from other routers.

IGMP (Internet Group Management Protocol): IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

IGMP Version 1, described in RFC 1112 has two different types of IGMP messages,

- Membership query
- Membership report

IGMP Version 2, defined inRFC 2236 has four types of IGMP messages,

- Membership query
- Version 1 membership report
- Version 2 membership report
- Leave group

IGMP Snooping: The default behavior for a Layer 2 switch is to forward all multicast traffic to every port that belongs to the destination LAN on the switch. This would defeat the purpose of the switch, which is to limit traffic to the ports that need to receive the data. The 'IGMP snooping' method can deal with multicast in a Layer 2 switching environment efficiently. IGMP snooping requires the LAN switch to examine, or snoop, the IGMP packets sent between the hosts and the router. When the switch hears the IGMP query message from a host to join a particular multicast group, the switch adds the host's port number to the associated multicast table entry. When the switch hears the IGMP leave group message from a host, it removes the host's port from the table entry.

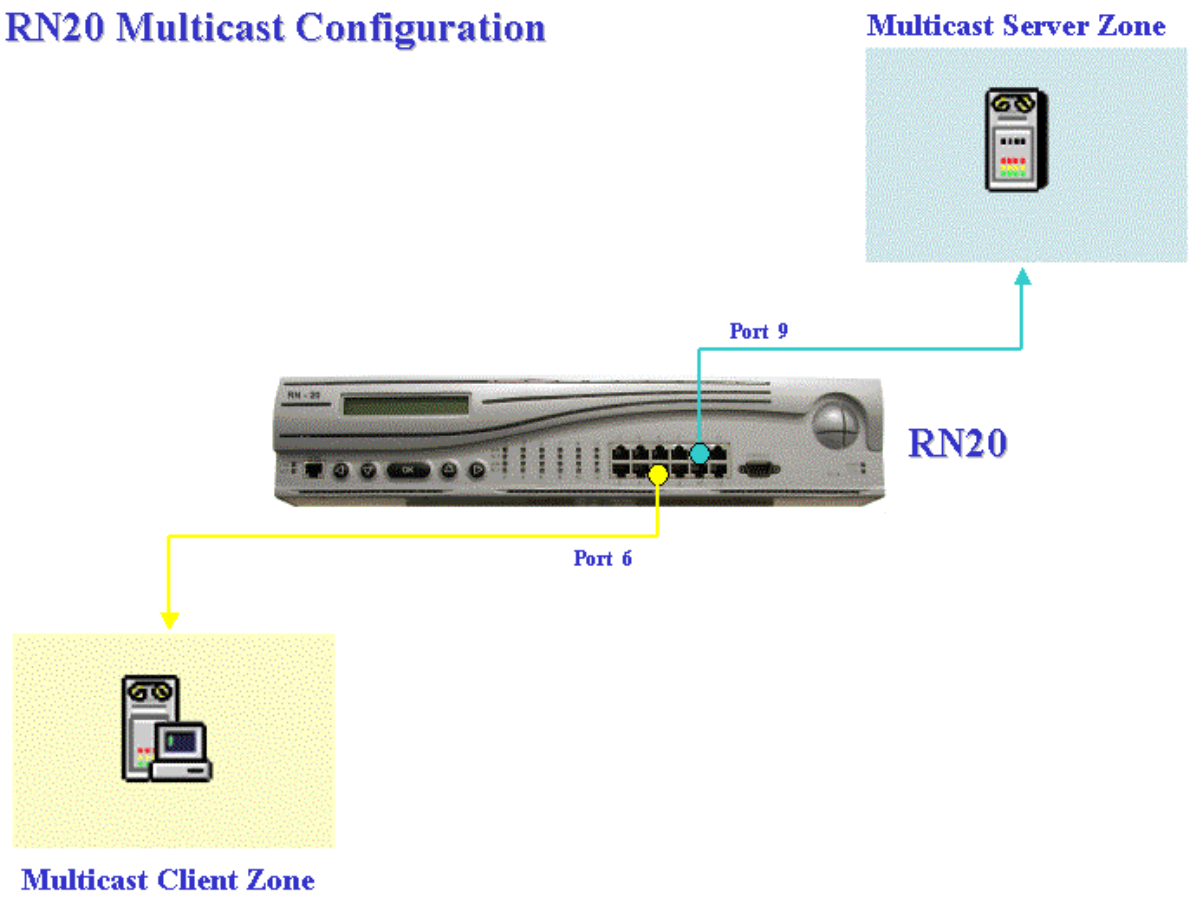
Because IGMP control messages are transmitted as multicast packets, they are indistinguishable from the general multicast data at Layer 2. A switch running IGMP snooping examines every multicast data packet to check whether it contains any pertinent IGMP control information. If IGMP snooping has been implemented on a low-end switch with a slow CPU, this could have a severe performance impact when data is transmitted at high rates.

11.2 Configuring RNxx device20 Multicasting

Many RNxx devices support multicast applications and is capable of IGMP snooping and multicast routing.
The following example using RN20 device shows a multicast server located in Multicast Server Zone (port 9) and a multicast client in Multicast Client Zone (port 6) of RN20. To

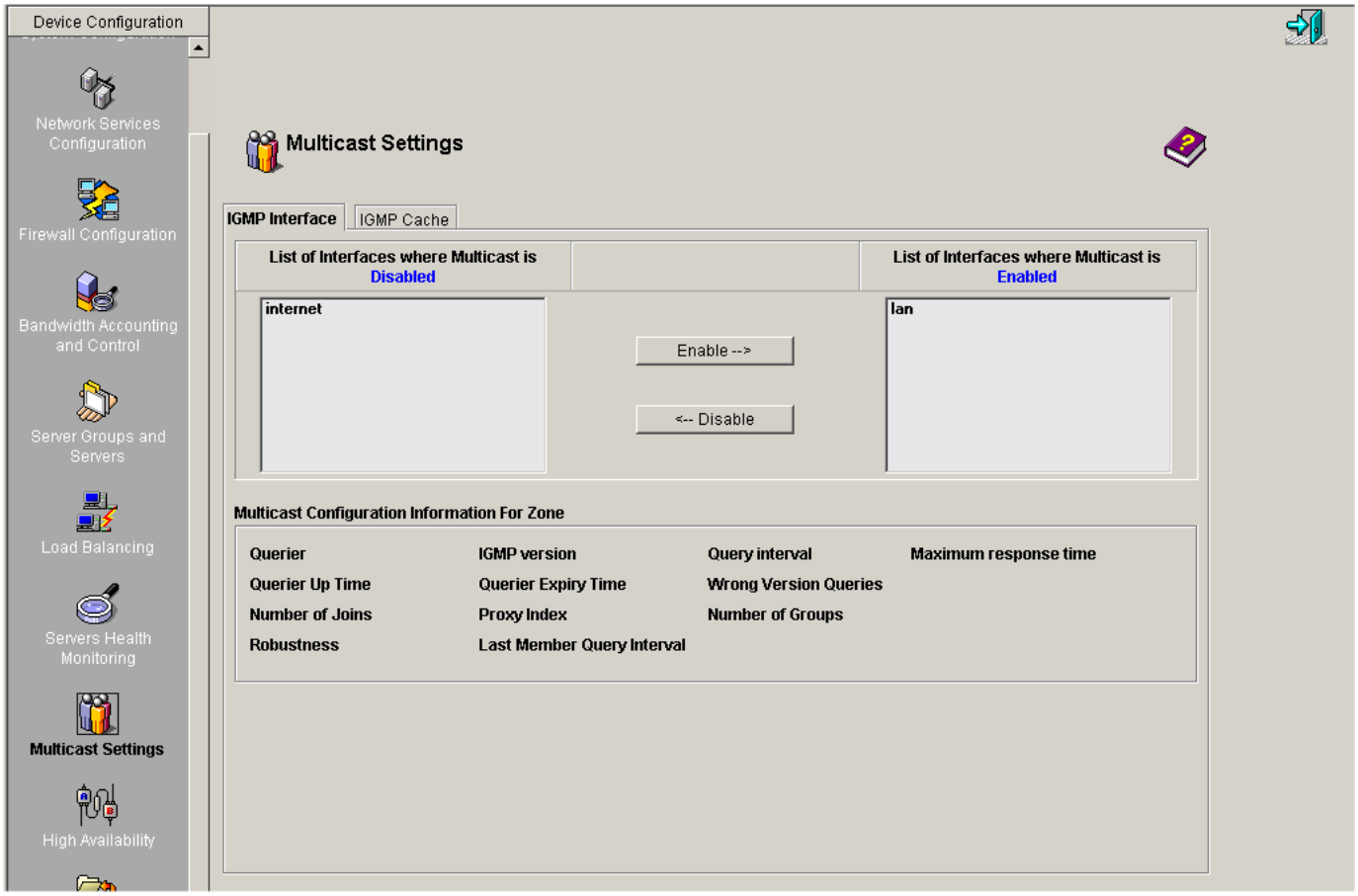
enable the server stream to be recognized by the client, IGMP forwarding is to be configured on RN20 across these two zones.

Figure 111. Mutlicast Setup



- Connect a multicast server and a client as shown on Figure 111, and configure zone firewall access rules to enable IGMP protocol in both multicast server and client zones.
- Go to Multicast Settings → IGMP Interface menu and add the client zone and the server zone to the Enabled list (select the zone and press Enable button)
- Start multicast stream application on the server side, and the IGMP cache values for this server will be automatically recognized by RN20 and listed under Multicast Settings → IGMP Cache menu.
- Start multicast client application on the client side to receive server audio/video stream.

Figure 112. Multicast Settings->IGMP Interface



Index: This is the VLAN interface over which multicast routing has to be enabled. An entry with the same index should exist in the VLAN Table.

Query intrvl: The frequency at which IGMP Host-Query packets are transmitted on this interface. Default – 125 seconds.

Ver: The version of IGMP, which is running on this interface. Default – 2.

Max Resp. Time: The maximum query response time advertised in IGMPv2 queries on this interface. Default – 100 seconds.

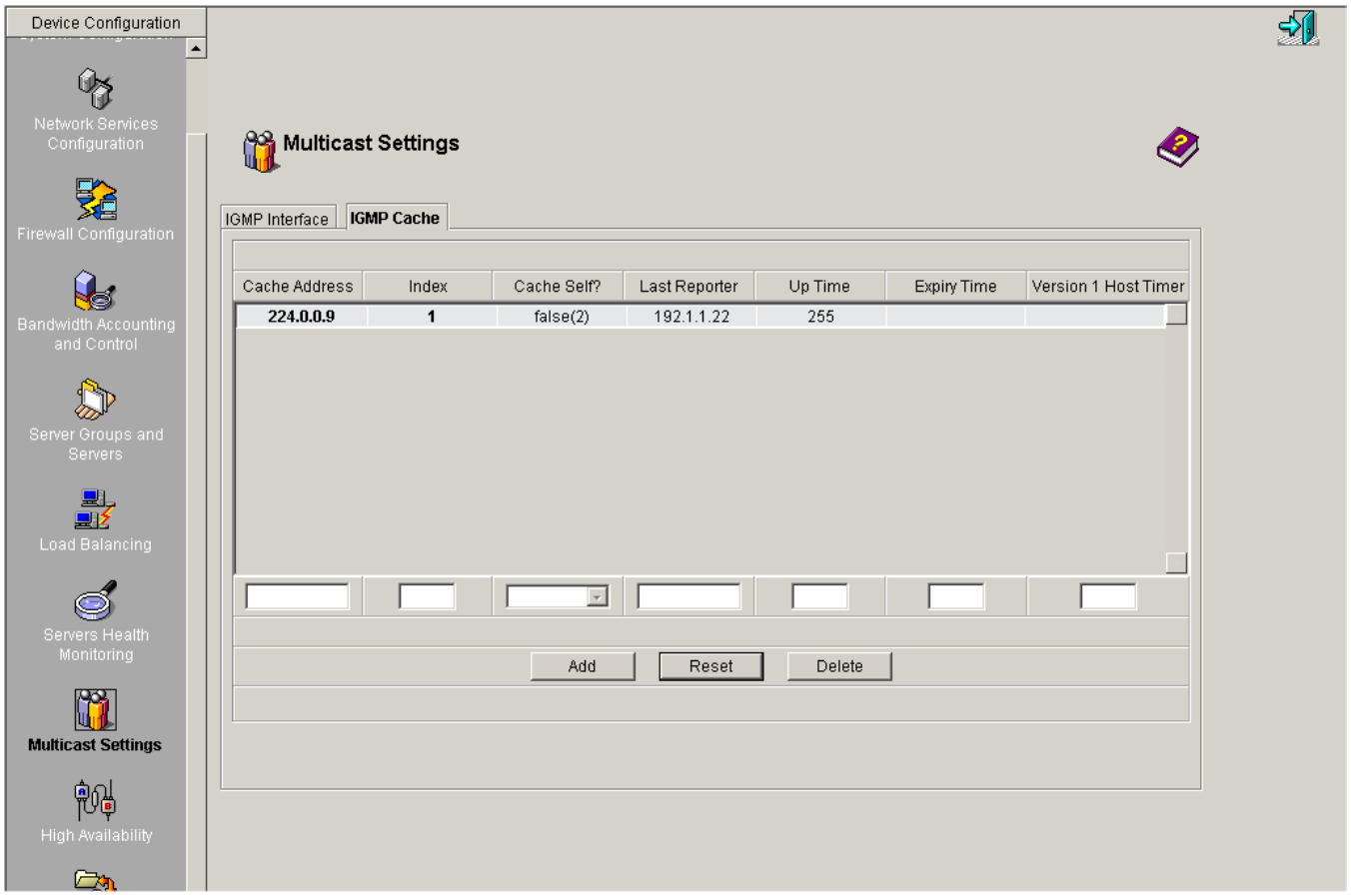
Proxy Indx : Ususally the value of is 0, indicating that no proxy function is being executed.

Robust : The Robustness Variable allows tuning for the expected packet loss on a subnet

Last. Memb. Query Intrvl : The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group

messages, and is also the amount of time between Group-Specific Query messages.

Figure 113. Multicast Settings->IGMP Cache



The screen above shows existing entries in the IGMP cache. Each entry in this table represents an active multicast client.

Cache Address: This is the multicast group for which at least one active client exists on the VLAN specified by the index.

Index: The VLAN interface on which the client exists.

Cache Self: Whether RN20 is a client for this multicast group.

Last Reporter: This is the last active client that has replied to the IGMP query over this VLAN.

Up Time: This is the time in ticks (100^{th} of a second) elapsed since this entry was created.

Expiry time: Not applicable.

Version 1 Host Timer: Not applicable.

12.High Availability Configuration

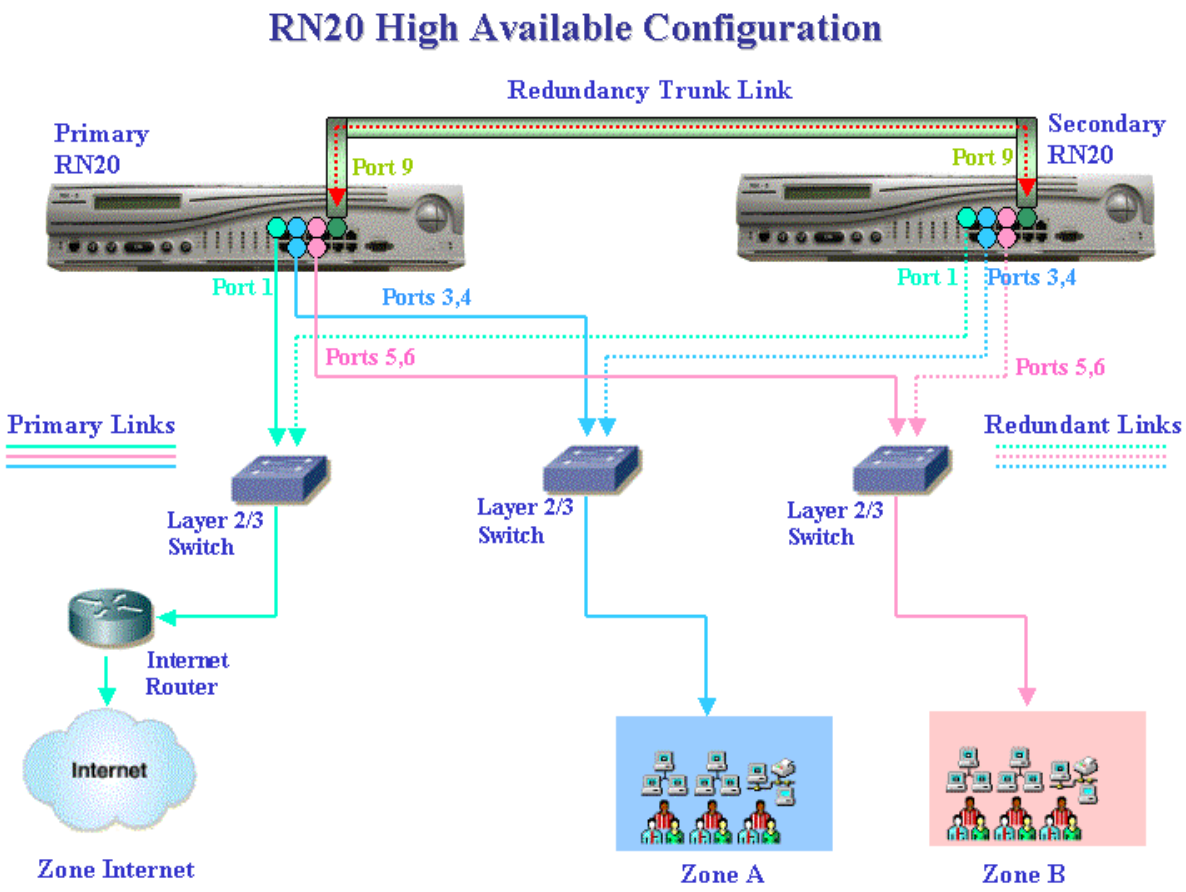
(RN 5/20/40/41 models only)

RNxx device allows one-to-one redundant configuration and supports the deployment of mission critical applications. This configuration consists of two RNxx devices working in tandem such that the network connectivity is not disrupted even if one of the units fails. RNxx supports two types of redundancy, namely port level and box level redundancy.

In such a configuration two devices are connected to the network in a symmetrical fashion and all the hosts/servers are reachable from either of the RNxx. The RN20 device is used as an example for High Availability feature.

If host A is reachable from the port 1 of one RN20, it should be reachable through the same port on the other RN20. The units are connected to each other using one or more ports. When several ports are used for RN20 connectivity, these ports are trunked. One of the RN20 is configured as the preferred primary and the other - as preferred secondary. In normal circumstances the preferred primary will be active and hence will handle all the traffic. The secondary RN20 will be dormant until a port on the primary RN20 goes down or the primary RN20 itself goes down, or the administrator manually starts the switchover process. The secondary RN20 will seamlessly take over the failed port in the first case or the entire network in the second and third cases. Picture below shows a redundant RN20 configuration.

Figure 114. High Availability Configuration



To create a redundant configuration:

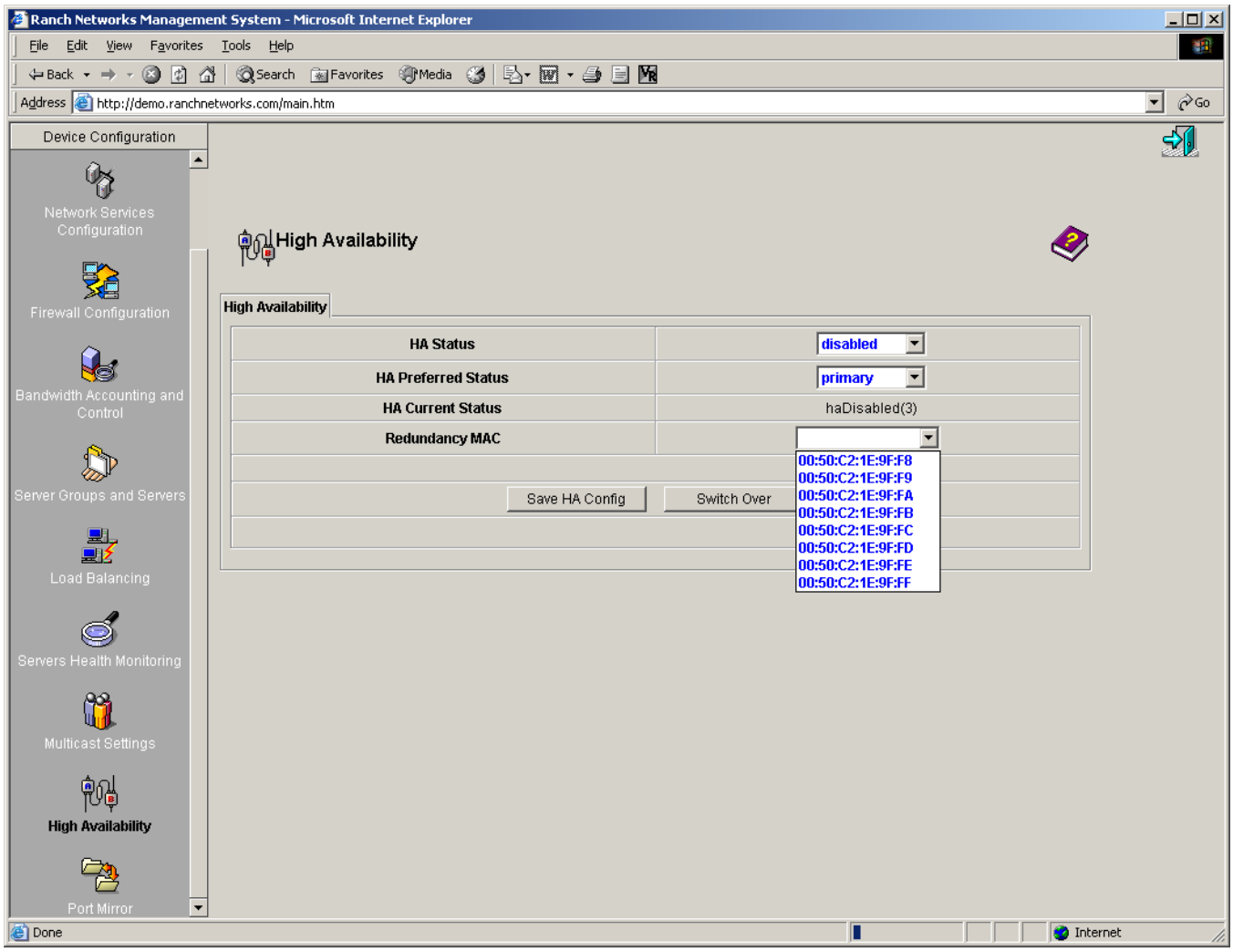
1. Connect two RN20s in symmetric fashion as shown and explained above. Please do not use port 9 on either RN20s for any of the data connections as it will be used later for inter-connecting the RN20s as redundant trunk link.
2. Power up one of the RN20s. Configure the RN20 according to the network topology requirements.
3. Configure the HA preferred status as ***secondary***, HA status as ***enable*** and enter Redundancy MAC that will be shared between the primary and secondary RN20s.
4. Configure the port 9 on the second RN20 as "highAvailability" port. Change admin status on port 9 to ***Up.*** Save this configuration.
5. Wait for HA current status to become ***primary.*** **Make sure the network connectivity is as expected**. If any changes in the configuration are done, make sure that it is saved on the RN20
6. Upload the configuration from this RN20 to an FTP server. Power down this RN20.
7. Power up the second RN20. Download the saved configuration file from the FTP server to the second RN20.
8. Modify the HA preferred status as ***primary*** and HA status as ***enable***. Save this configuration.

9. Wait for HA current status to become ***primary***. **Make sure the network connectivity is as expected**. THIS RN20 FROM NOW WILL ACT AS THE PRIMARY RN20.
10. Connect port 9 on the first RN20 to port 9 on the second RN20.
11. Power up the first RN20 now. After the system comes up make sure that both the HA preferred status & HA current status on this RN20 are ***secondary***. THIS RN20 FROM NOW WILL ACT AS THE SECONDARY RN20.
12. ALL CONFIGURATION CHANGES MADE ON THE PRIMARY (EXCEPT THOSE DONE ON THE MAINTENANCE TAB) MUST BE MANUALLY CONFIGURED ON THE SECONDARY SO THAT BOTH OF THEM ARE IN SYNC.

12.1 Configuring High Availability

Go to ‘High Availability’ menu to configure HA parameters.

Figure 115. High Availability Configuration Screen



HA status: HA can be enabled or disabled. Choose ‘enabled’ or ‘disabled’ from the pull down menu. Note: In order to enable HA at least one port (ex: port 9) MUST be configured as ‘HighAvailability’ and the redundancy MAC must be configured.
HA Preferred Status: This is used to set the preferred status of the RN20. This is only the intended HA status, the actual HA status of the unit is indicated by HA Current status. Choose ‘primary’ or ‘secondary’ from the pull down menu.
HA Current Status: This field shows the current HA status of RN20. It can be either primary, secondary or disabled. If it is primary, this device is actively handling traffic on

the network. If it is secondary, then the device is dormant and monitoring for any failures. It is disabled when the HA status is disabled.
Redundancy MAC: Redundancy MAC is required to be configured before HA can be enabled. This MAC is shared between the primary and secondary in such a way that when a switch over happens, all the hosts, switches connected to the primary that went down do not have to refresh their ARP.
There are eight preconfigured MAC. When configuring HA a user has to select one MAC address on the primary box and set the same address on the secondary box. The reason we provide eight different MAC addresses is that a user can install up to eight RNxx devices in one organization.

The button **Save HA Config** is used to save any changes to HA configuration.
The **Switch Over** button is used to initiate a manual switch over of the HA current status. The switch over can be initiated only from an RN20 where the ***preferred status*** is ***primary***. This action will cause the current primary to become secondary and vice versa.

13. Port Mirroring Configuration

(RN 5/20/40/41 models only)

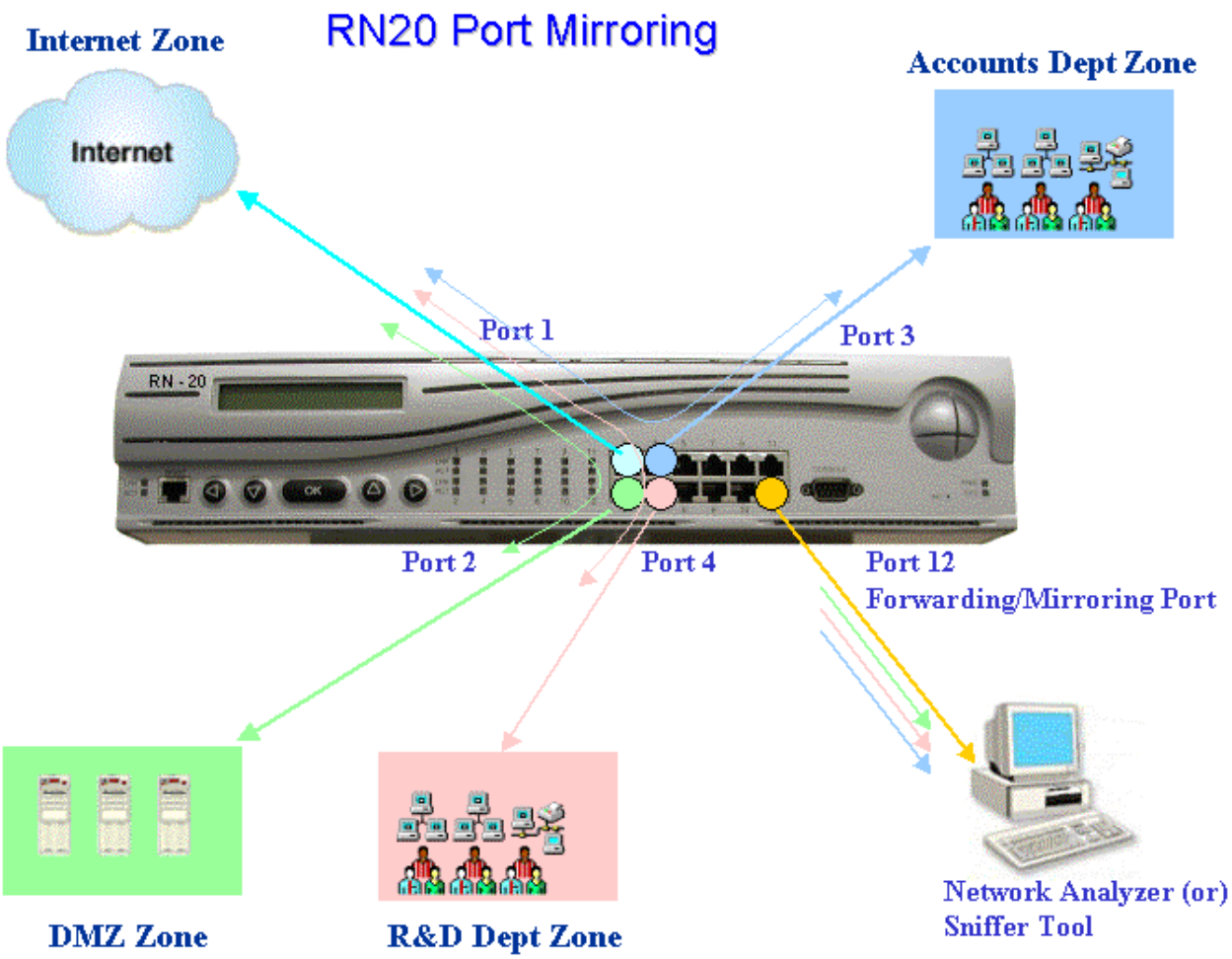
Port mirroring is a technique used to monitor network traffic in a switched environment. If port mirroring is enabled, a switch forwards a copy of each incoming and/or outgoing packet from one port to another port where the packet can be analyzed. Network administrator uses port mirroring as a diagnostic or debugging tool that helps him/her to determine the location of a network problem. This feature also enables administrator to closely track RNxx device performance and alter configuration if necessary.
RN20, RN40, RN500, RN700 devices, but RN300 support this feature. All "Port Mirroring" chapter uses RN20 device as an example.

In RN20 port mirroring can be configured by adding one or more ports to the list of 'Forwarding Ports' (also called Mirroring Ports) and then creating mirroring rules to define a set of source and/or destination ports from which the traffic will be copied to the mirroring ports. A protocol analyzer or a Sniffer connected to the forwarding/mirroring port will capture and evaluate the data without affecting the hosts on the source/destination ports.

The following example shows a typical port mirroring setup with internal departments such as DMZ, R&D and Accounts configured in different zones (ports 2, 3 and 4). All internal zones are connected to Internet via Internet Zone (port 1). Now the network administrator wants to monitor all packets entering and leaving the network through the Internet zone. His main goal is to closely monitor network utilization and effectively encounter attacks from Internet. He can designate an unused data port, for example, port 12 as forwarding / mirroring port where he would receive mirrored data.

Port 12 is added to the list of 'Forwarding Ports' in 'Port Mirror' Configuration menu. Two mirror rules are created. The first "port-to-any" rule with a source Internet zone (port 1) and any destination zone (ports 2, 3 and 4) to mirror all packets that are entering the enterprise from the Internet. The second rule, "any-to-port" establishes any zone as a source (ports 2, 3 and 4) and Internet zone (port 1) as the destination to mirror all packets that are leaving the enterprise through the Internet.

Figure 116. Port Mirroring Setup

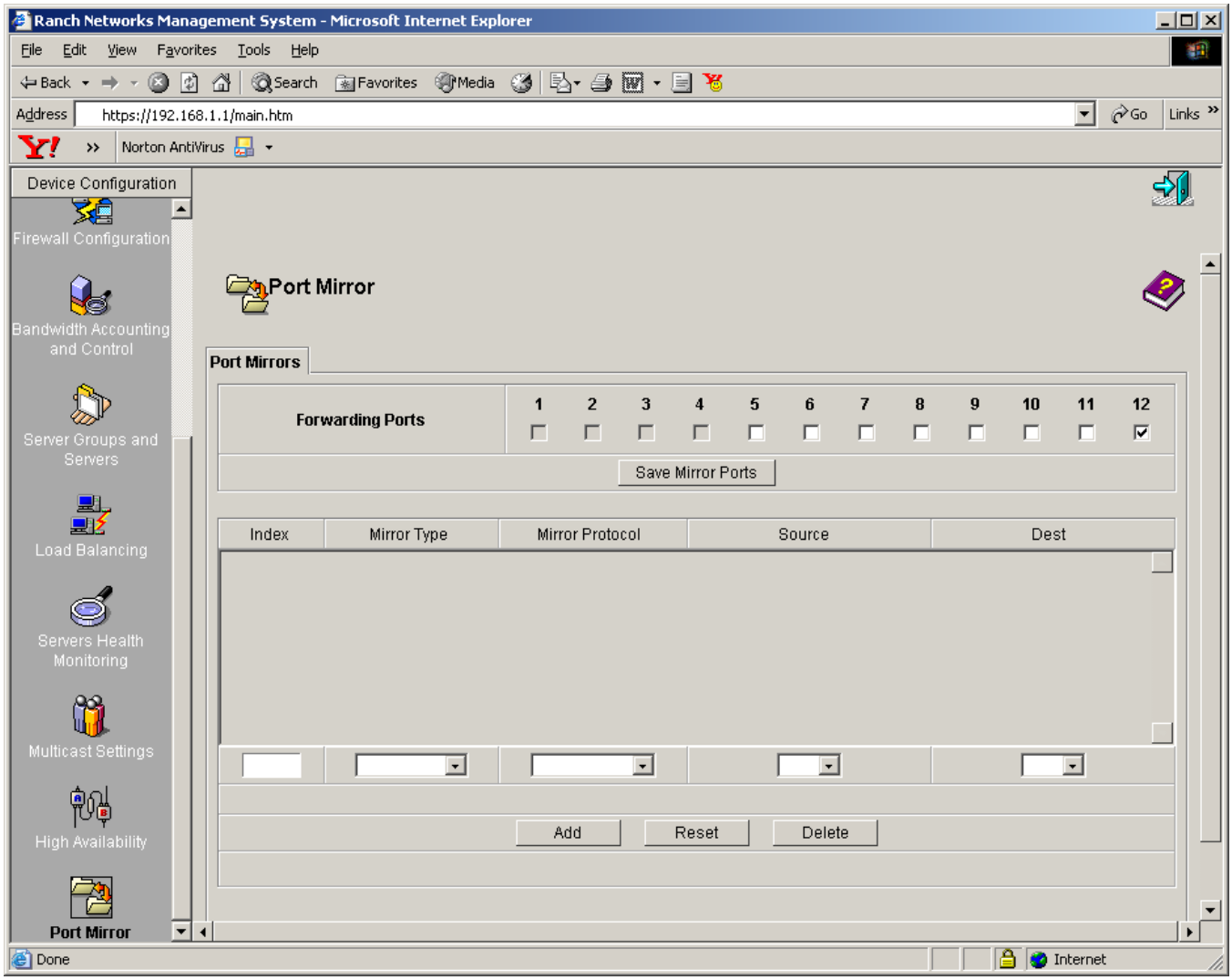


13.1 Steps to configure Port Mirroring on RN20

1. Ensure that the Internet, DMZ, R&D and Accounts Zones are created and physically connected to corresponding RN20 ports. All required firewall access rules are created enable intranet and internet communication.

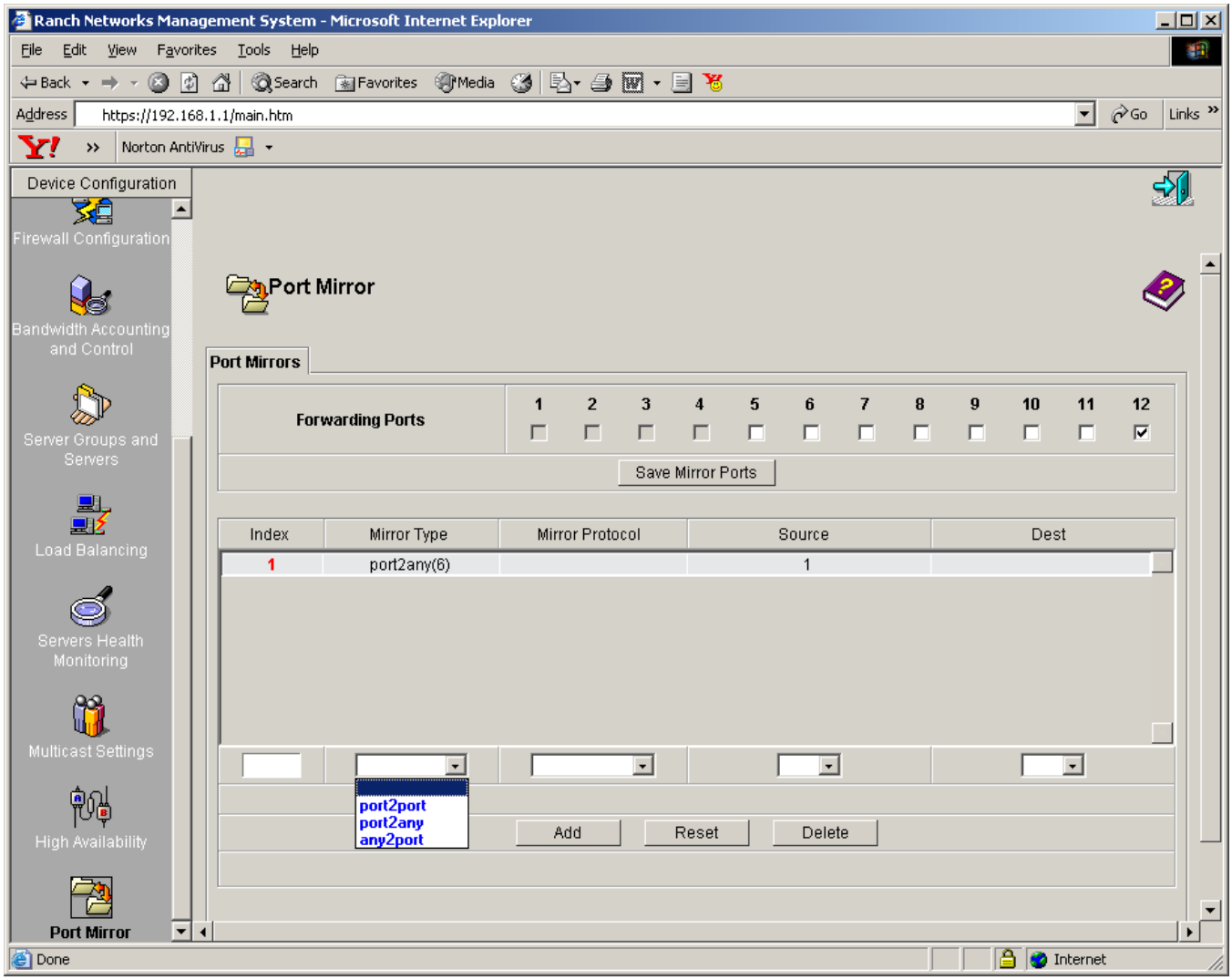
2. Logon to RN20 and go to 'Port Mirror' menu. Select port 12 and click on 'Save Mirror Ports' to designate as a Forwarding / Mirror port.

Figure 117 . Port Mirroring -> Port Mirrors Configuration



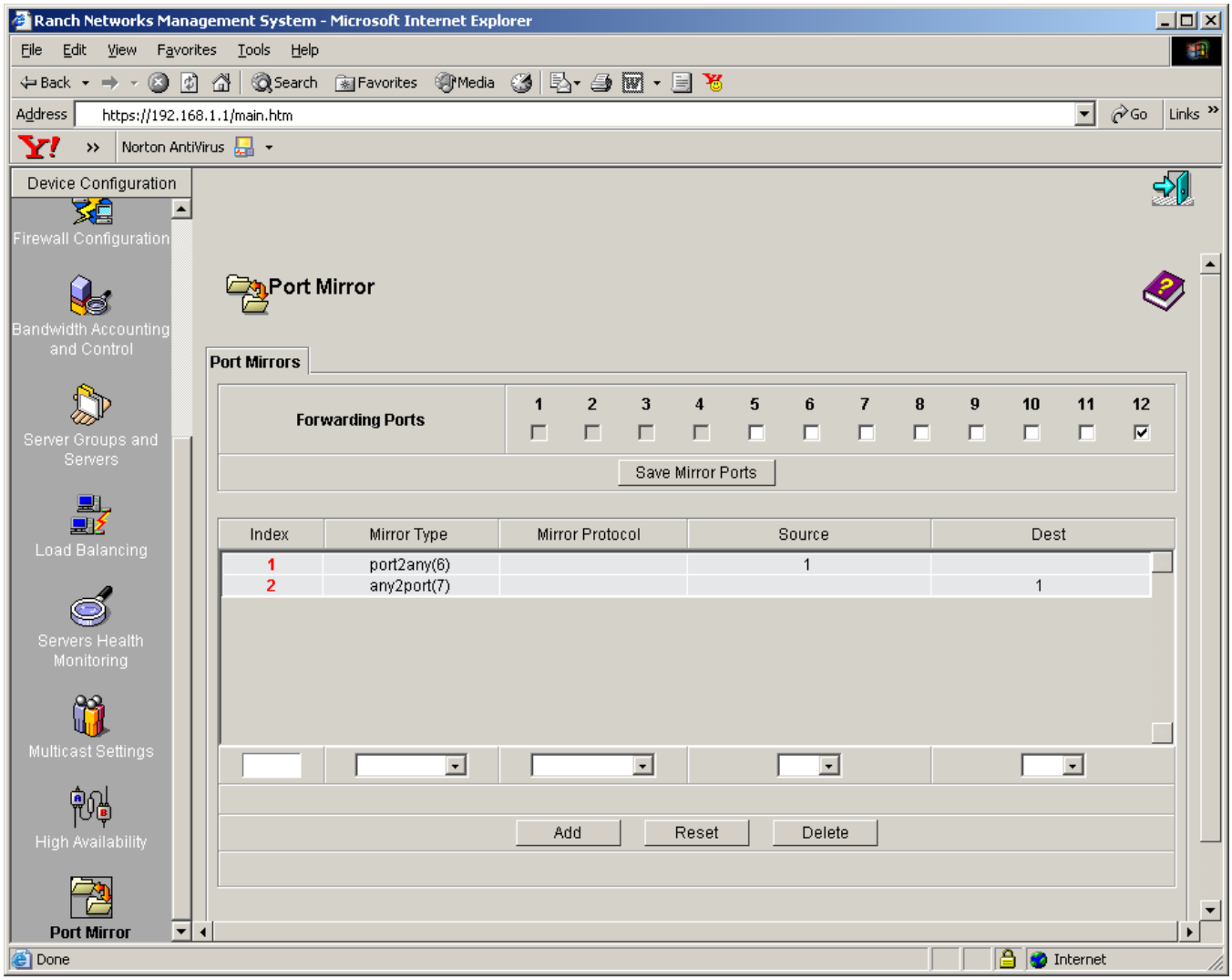
3. Add the first mirror rule with an index 1, mirror type ‘port2any’, mirror protocol ‘default’, and source ‘port 1’ from the selection lists.

Figure 118. Port Mirroring -> Port Mirrors Configuration (cont.)



4. Add the second rule with the index 2, mirror type ‘any2port’, mirror protocol ‘default’ and destination ‘port 1’

Figure 119. Port Mirroring -> Port Mirrors Configuration (cont.)



5. Go to System Config → Image Config → Update Config and click on 'Save Running Config' to permanently save these changes.
6. Connect a host which is running network analyzer or sniffer to port 12 to capture and analyze the mirrored packets.

14.Software Update Steps & Changing RN Models

The RN software update procedure is simple and straightforward, however, because the RN is the important and critical part of the network this event should be properly timed and planned.

Software Update:

The RN software update procedure is simple and straightforward, however, because the RN is the important and critical part of the network this event should be properly timed and planned.

Caution: Check with Ranch support whether you require any activation key for software update. Usually the updates for current major software revision does not require activation key. However, an activation key is required if the current major version (ex. Ranch OS-1.2.4) is being updated to next major software version (ex. Ranch OS-2.0).

14.1 Step 1 – Obtain the latest RN image.

To obtain the latest RN image please send the email to support@ranchnetworks.com . The reply message from the Ranch Networks Support Team will consist the URL of the FTP server where the software image should be downloaded from, and the login information. You also require latest activation key if the update involves major software version release.

It is strongly recommended to download the software image to the location different than RN device.

14.2 Step 2 – Backup the existing configuration.

Backup the existing configuration from RN to the backup FTP server.
(See User Administration Manual, Configuring RN for details)

14.3 Step 3 – Download the software image to RN

Choose non primary image for the update (for example if A image is currently used then B image should be selected for the update), program the new image, select this image as a default image.
(See User Administration Manual, Configuring RN for details)

14.4 Step 4 – Reboot RN with a new image

Reboot RN with a new image, check configuration.

In case of any problem related to the update the RN could be rolled back to the privies software image by selecting the backup image as a default.

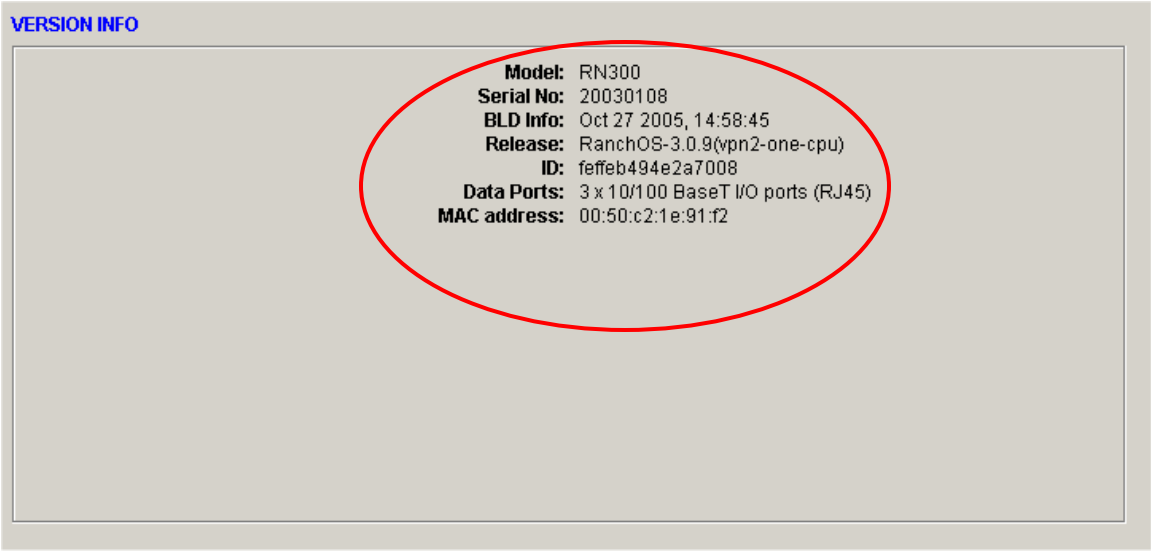
14.5 Step 5 – Enter Activation Key (if required)

Access the RN device GUI (https://management-IP) as usual and login with admin privilege. If activation key is required, a new screen will appear to enter the key. Type in the key and wait for while until the RN booting process completes.
(See User Administration Manual, Product Activation for more details.)

14.6 Step 6 – Check device is booted with new version

Go to System Configuration → Image Config → Version Info menu and check latest running image version.

Figure 120: System Configuration -> Image Config -> Version Info



14.7 Changing RN Models:

It may be required to upgrade from RN5 models (RN5A, RN5B or RN5C) to RN20, downgrade RN20 to any RN5 model or converting between different RN5 models. Any RN hardware unit is totally compatible to be configured as any model (RN20, RN5A, RN5B, RN5C) at any time depending on requirement. This can be achieved by downloading corresponding software image of the RN model and using it's activation key.

Caution: The existing configurations may not work properly after changing model numbers, as different models bring different feature set. Be sure to clear your browser settings (ex. Tools → Internet Options → delete files, delete cookies, clear history) as browser options will be changed between different models.

Converting RN5A to RN20:

1. These steps are valid for converting any RN5 model to RN20 model.
2. Boot RN5A. (ex. with Image A)
3. Take back up of running configuration.
4. Place existing RN5A image file (rn5a.bin) in safe place or different directory of your local FTP/TFTP server. It can be useful if your up grade process fails.
5. Download RN20 image file (rn20.bin) to Image A location from your local FTP/TFTP server.
6. Reboot RN device with default Image A, i.e. with newly downloaded RN20 image
7. Access the RN devices GUI from management interface (https://mgmt-IP)
8. Provide admin privilege username and password
9. You will be prompted to enter activation key in next screen. Type in activation key and wait while the booting process completes.
10. Go to System Config → Image Config → Version Info screen to check details of running image configuration and new model number as RN 20.
11. Once process is successful, download RN20 image file (rn20.bin) to Image B location also.

Converting RN20 to RN5A:

1. These steps are valid for converting any RN20 model to RN5 model.
2. Boot RN20. (ex. with Image A)
3. Take back up of running configuration.
4. Place existing RN20 image file (rn20.bin) in safe place or different directory of your local FTP/TFTP server. It can be useful if your up grade process fails.
5. Download RN5A image file (rn5a.bin) to Image A location from your local FTP/TFTP server.
6. Reboot RN device with default Image A, i.e. with newly downloaded RN5A image
7. Access the RN devices GUI from management interface (https://mgmt-IP)
8. Provide admin privilege username and password
9. You will be prompted to enter activation key in next screen. Type in activation key and wait while the booting process completes.
10. Go to System Configuration → Image Configuration → Version Info screen to check details of running image configuration and new model number as RN 20.
11. Once process is successful, download RN20 image file (rn20.bin) to Image B location also.

15.RN Network Configuration examples.

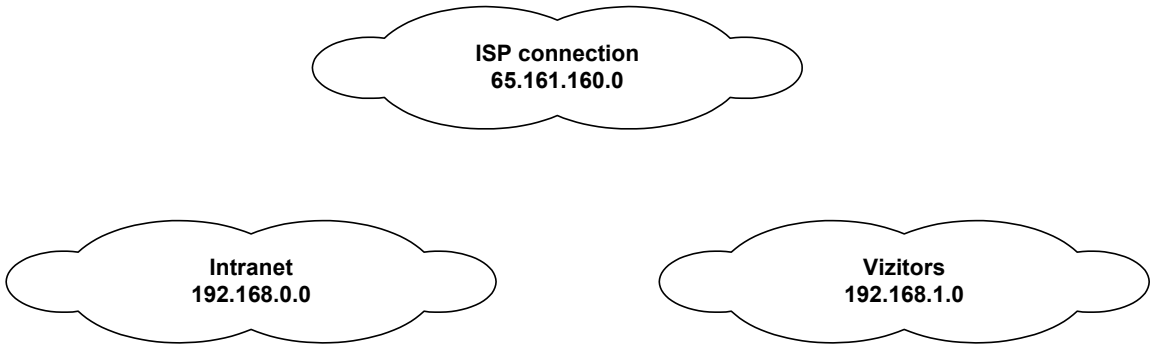
15.1 Example 1 : RN device with three physical zones

In this example the RN device is installed in the company that have the connection to ISP and two internal networks : one of them is the company's internal LAN another is the subnet that dedicated to the visiting consultants and sales representatives.
It is recommended to create the table of the network assets and relations between them .

Network Asset	IP subnet	Net. mask	NAT
ISP (internet)	65.161.160.0	255.255.240.0	No
Intranet	192.168.0.0	255.255.255.0	Yes
Visitors	192.168.1.0	255.255.255.0	Yes

The figure bellow shows the network assets listed in the table :

Figure 121. RN examples : Network Assets for the example



As usual, there is some limitation in the access between the networks:

Network	ISP (internet)	Intranet	Visitors
ISP (internet)	Access granted	No access	No access
Intranet	Access granted	Access granted	Access granted
Visitors	Access granted	No access	Access granted

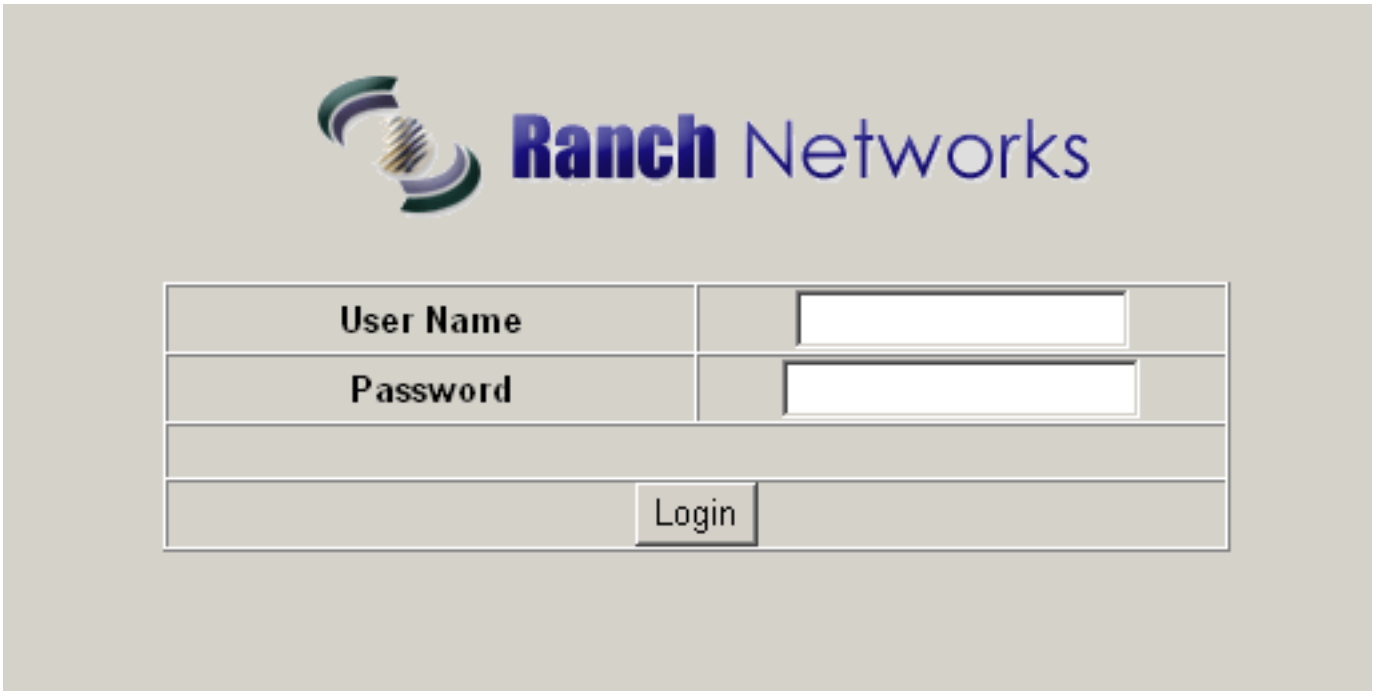
According to the table bellow three secure zones should be configured on RN device. There is no VLANS in the present configuration so all three zones will be considered as the physical zones

Pre configuration steps:

a) Power UP the RN device

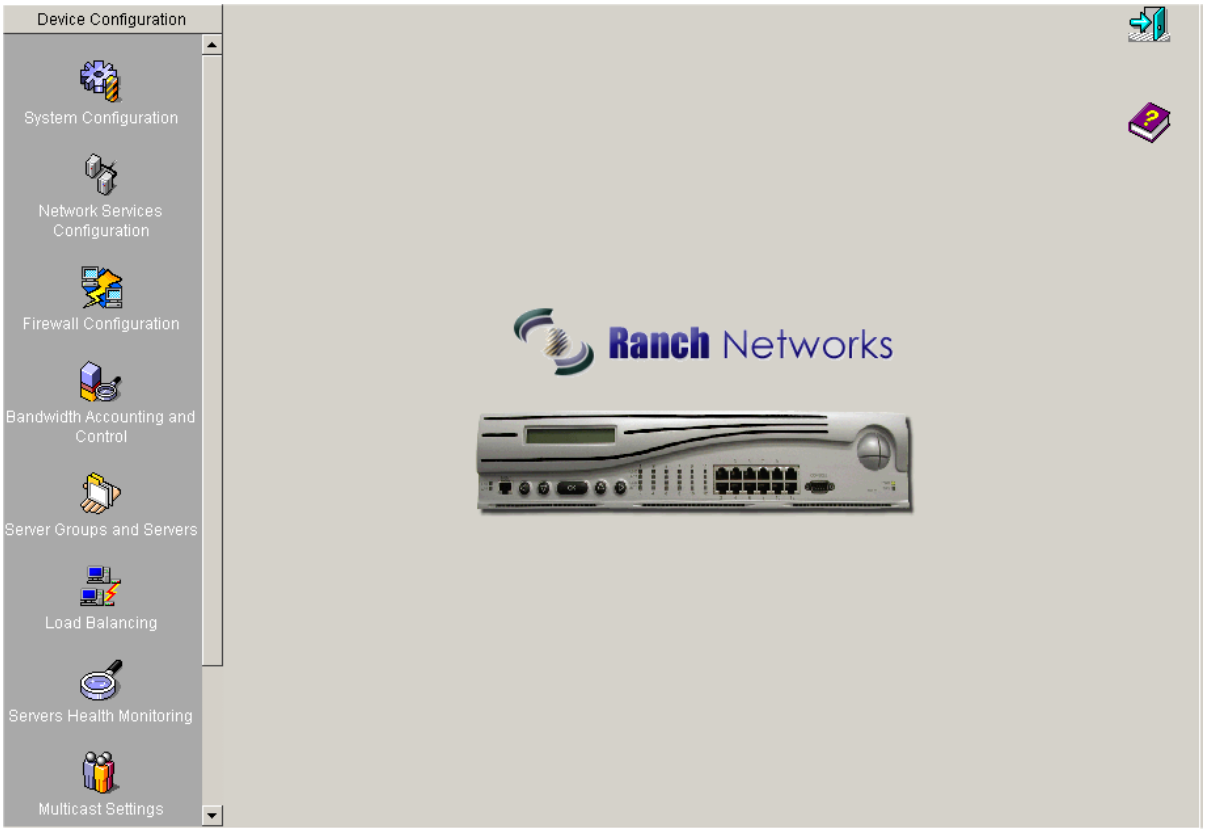
b) Using front panel key pad, read or configure the management interface IP Address, subnet address and default GW values. Refer to RN20 Installation Guide, Section 2.h for front panel keypad operational details. (For ex. IP Address: 192.168.2.1, subnet: 255.255.255.0 and default gateway: 192.168.2.100)
c) Connect administrator's management system directly to RN20's management interface. This is a simple local management method. Refer to RN20 Installation Guide, Section 3.b for various methods of connecting management station.
d) Configure IP Address properties of management station to be in the same subnet of RN20's management interface. (For ex, IP Address: 192.168.2.100, subnet: 255.255.255.0 and default gateway: 192.168.2.1)
e) Check the connectivity between management system and RN20 by using PING. For ex. ping to 192.168.2.1 should be successful.
f) Ensure the management station meets minimum requirements. Refer to RN20 Installation Guide, Section 3.b. The IE browser should be version 5.5 or higher.
    a. Start the browser on management station and type url https://management-interfaceIP. For ex. **https://192.168.2.1** or **http://192.168.2.1**

Figure 122. RN Login screen



g) Login with administrative privilege.

Figure 123. RN Web interface first screen



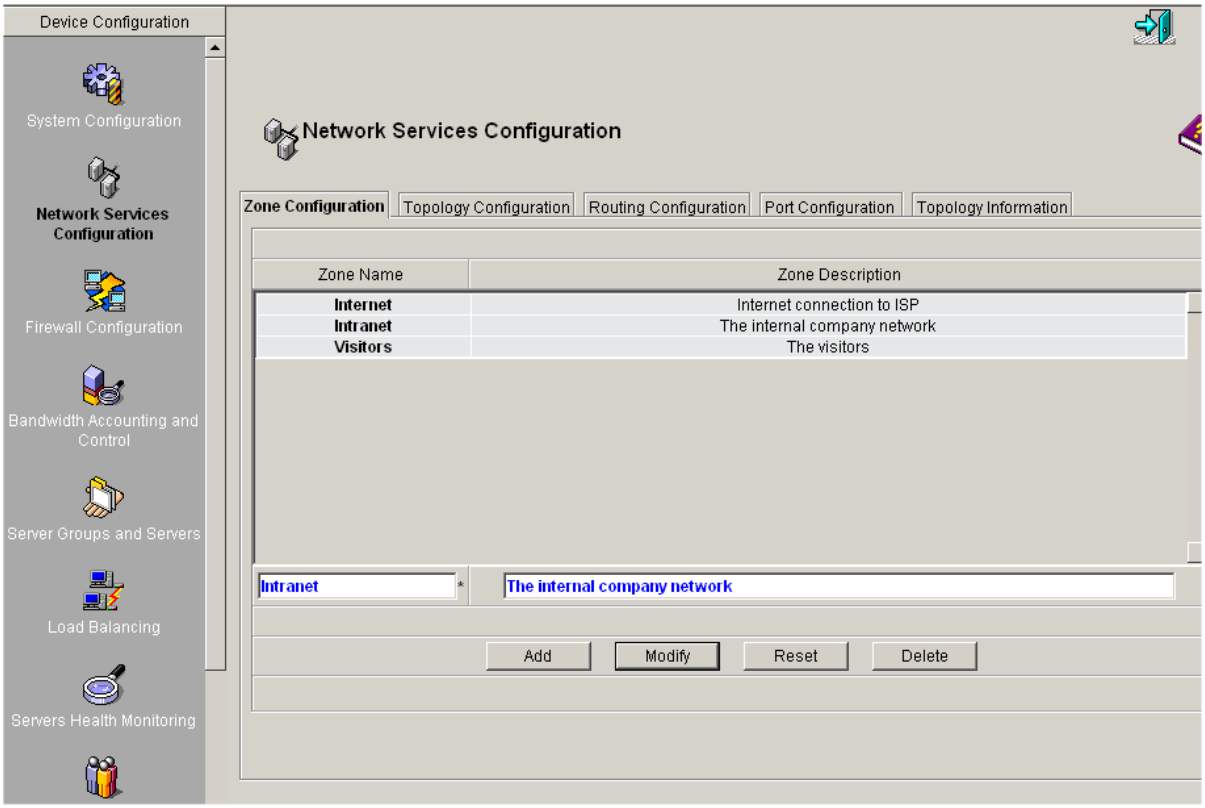
h) Check you have correct software image version. Go to System Configuration → Image Config → Version Info. Refer to RN 20 User Administration Guide, Section 5.1.3 for Image Management.

i) Be ready with your network topology and security rules to proceed configuring.

Step 1: Create the Zones

Click on **Network Services Configuration** , then on **Zone Configuration** Tab

Figure 124. RN Examples - Zone Configuration

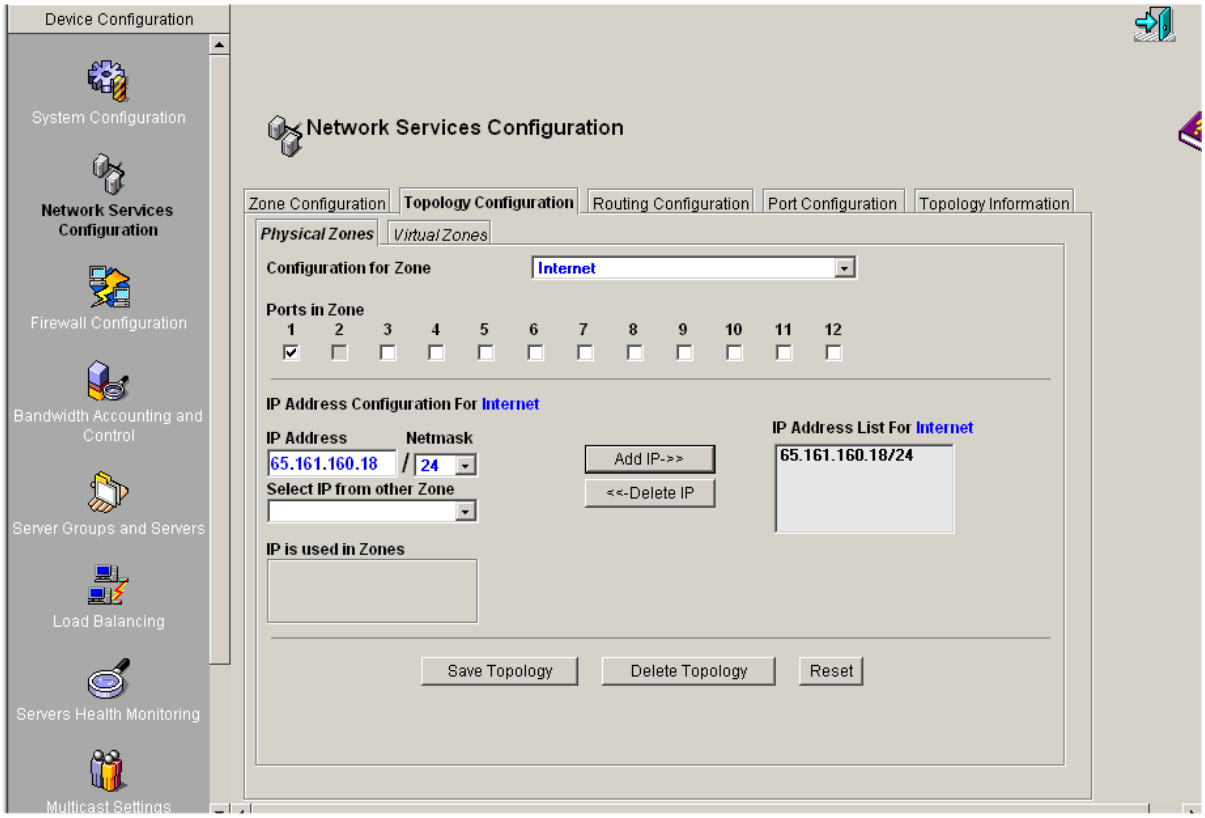


Create three zones – Internet(Internet) , Intranet(Company Network) and Visitors (The visitors)
To create the entry – type the values in the fields and press Add.

Step 2: Network Topology Configuration (IP settings for every zone)

Click on Topology Configuration Tab , select **Physical Zone** .
First lets create the Network topology for the Internet zone according to the networks assets table.
Select Internet zone from the drop-down menu .
Lets define 65.161.160.18 as the IP address of the Zone and the Zone is assigned to the physical data port number 1 (the IP address of the Zones interface will be the default router for all hosts that connected to this zone)

Figure 125. RN examples - Topology Configuration (Physical Zone)



Press **Save Topology** button

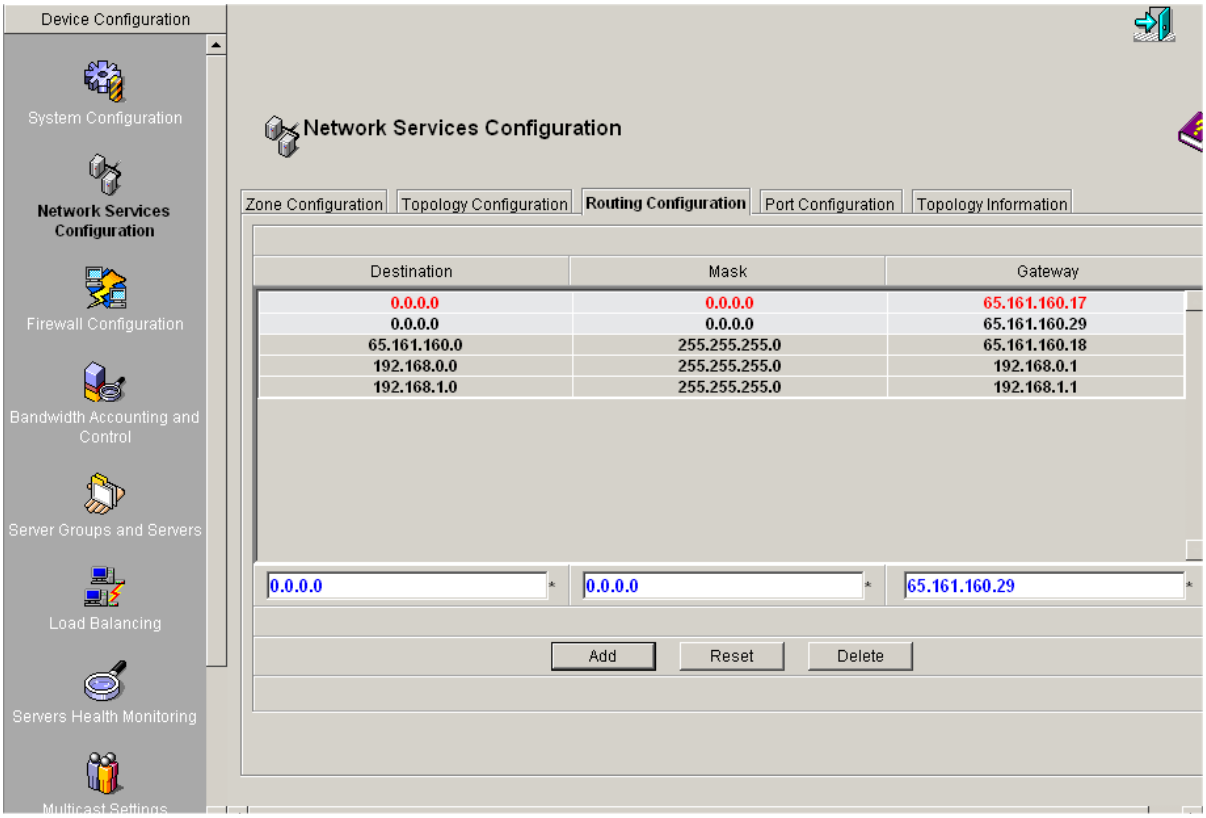
Repeat Step 2 for the rest of the zones using following parameters :

Intranet - port 2
192.168.0.1/24;
Visitors – port 3
192.168.1.1/24

Step 3: Check the routing configuration , add the route for the next hop.

Click on the Routing Configuration Tab
As the Zone is added the route record is created automatically , however the next hop for the RN device (the default route) should be added manually . The several default routes could added , the red color indicates the active route .

Figure 126. RN examples - Routing Configuration

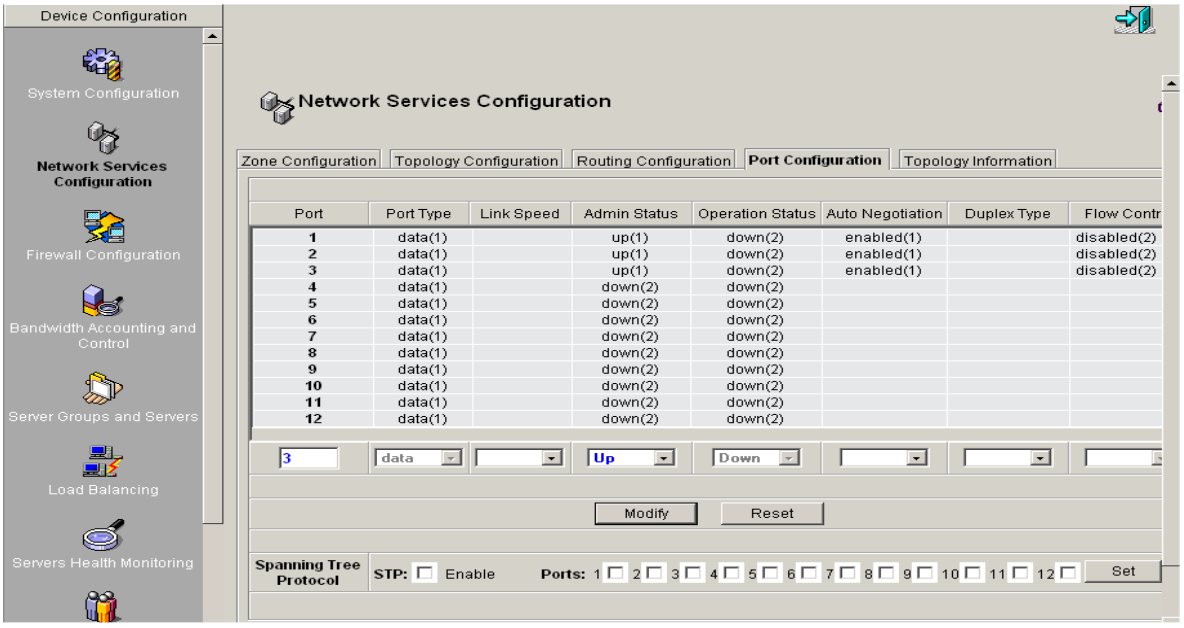


To create the entry – type the values in the fields and press Add.

15.1.1 Step 4 : Bring Up the physical ports assigned to the zones

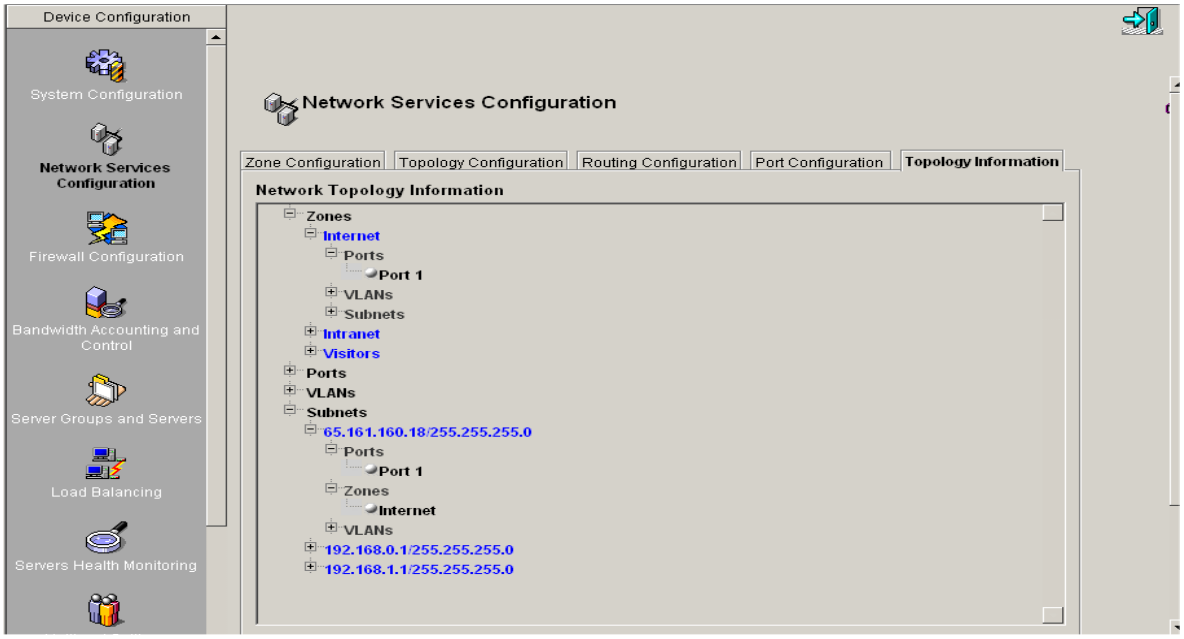
Click on Port Configuration Tab , Select the Admin Status UP for ports 1,2,3 and press **Modify** button

Figure 127. RN examples - Port Configuration



The **Topology Information** Tab serves the pure information purpose, so you can go over all network topology configuration that was done before

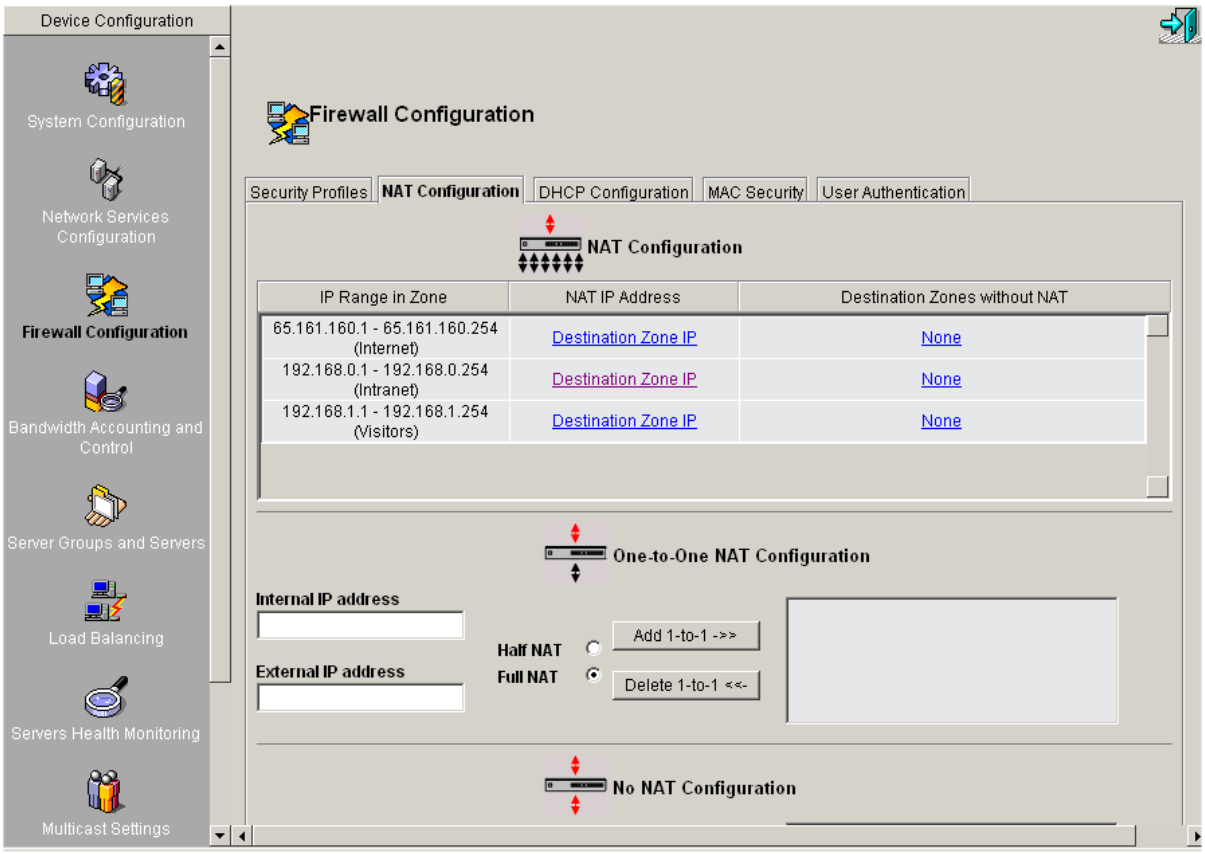
Figure 128. RN examples - Topology Information



Step 5: NAT and firewall configuration

The company , in this example , uses the private and the public IP addressing . In the case of the public IP addresses no further NAT configuration is required , but for the zones Intranet and Visitors NAT configuration is required .
Click on **Firewall Configuration** , then click on **NAT configuration** Tab

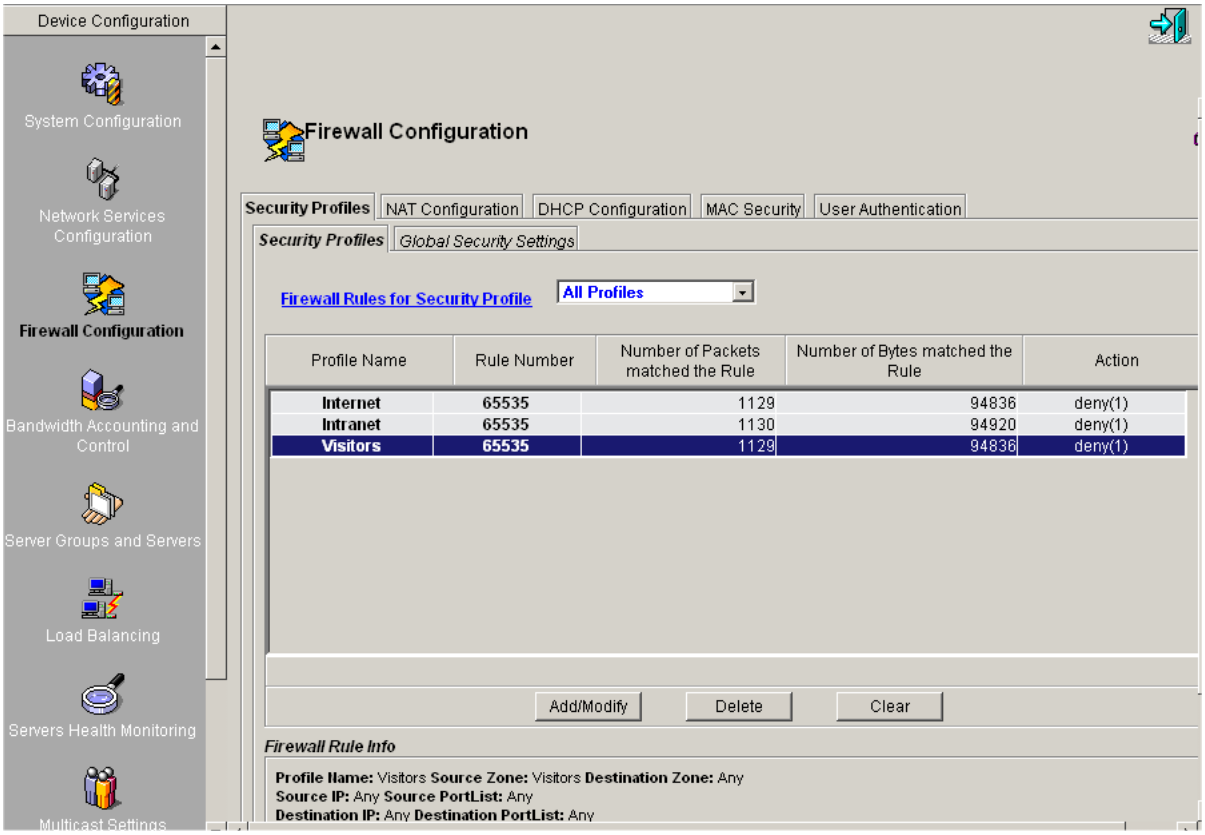
Figure 129. RN examples - Firewall configuration



For default the private IP will be NATed to the IP address of the destination zones interface. For example any IP Address that will go through Internet zone will be NATed to 656.161.160.18. (please see Users manual for NAT configuration details)

The security profiles for every of zones are created along with the zones. Because of the security concern the profiles consist only one default rule that denies all traffic related to the zone. The next screen shows the default rules for every zone (the start situation)

Figure 130. RN examples - Security Profile Configuration



Now, lets repeat the table of the access :

Network	ISP (internet)	Intranet	Visitors
ISP (internet)	Access granted	No access	No access
Intranet	Access granted	Access granted	Access granted
Visitors	Access granted	No access	Access granted

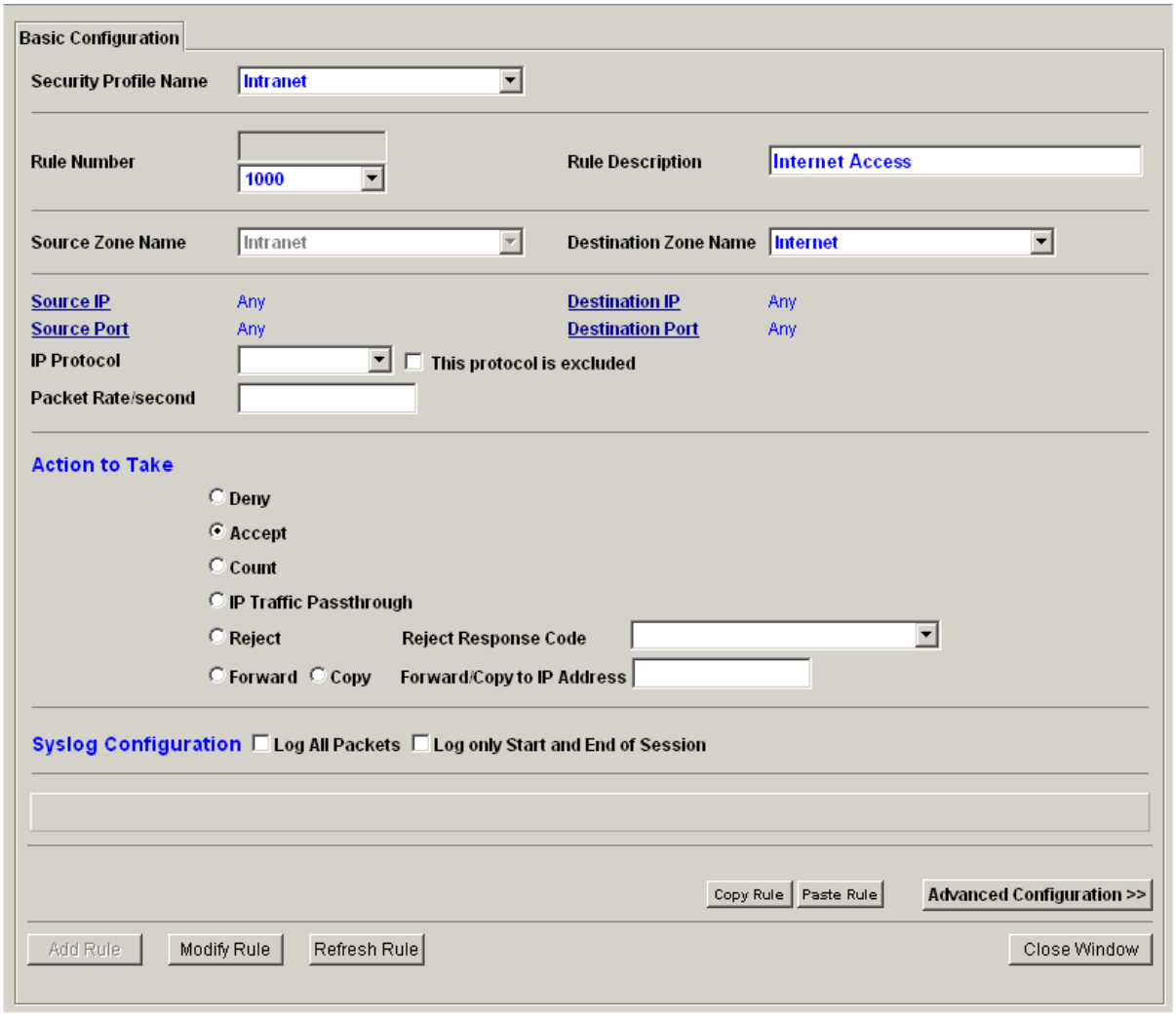
The first zone , Internet , can have only the default rule that prevent any access to the other zones , the rest of the zones must have more rules according to the table of access

The Intranet zone rules configuration :

Press Add/Modify button .

Select the Intranet zone from the drop-down menu;
Enter the number of the rule (lets make it 1000);
Enter " Internet Access " at the rule description ;
Choose Internet zone as a Destination zone;
Select Accept as the Action to Take;
Press Add Rule;

Figure 131. RN examples - Internet Zone rules



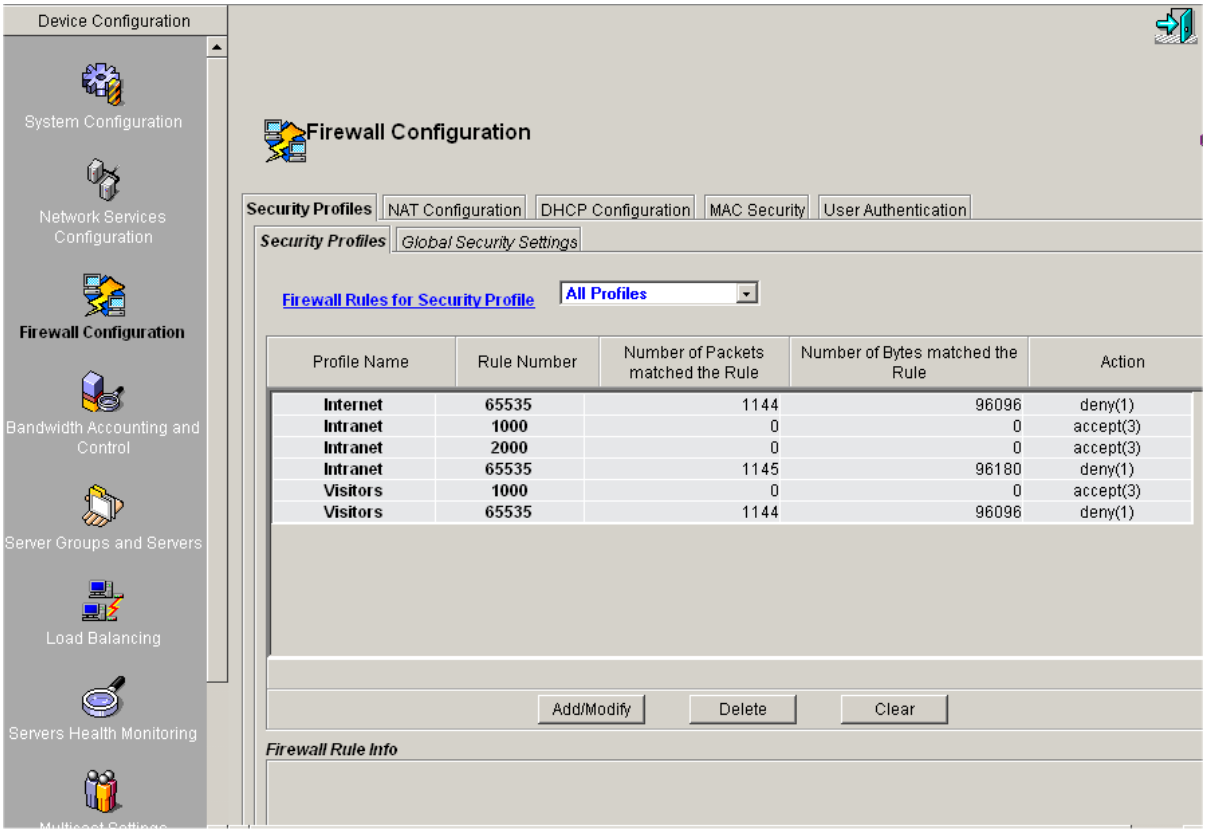
At this point the traffic from Intranet zone to Internet zone is permitted .

Using the procedure above and the setting from the table bellow create the rest of the rules

Profile Name	Rule Number	Description	Destination Zone	Action to Take
Intranet	2000	Access to Visitors	Visitors	Accept
Visitors	1000	Internet Access	Internet	Accept

The next screen shows the summary for the rules after configuration

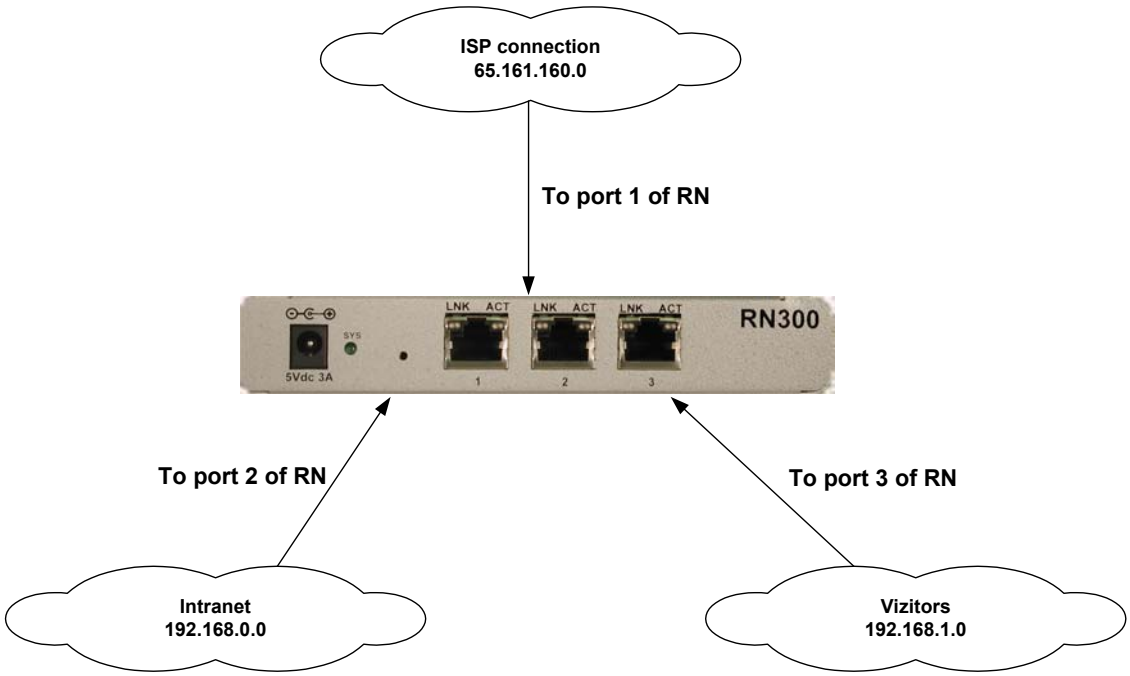
Figure 132. RM examples - Security profiles



At this point the basic network configuration of RN for this example is done.

The configured network topology for this example

Figure 133. RN examples - The configured topology



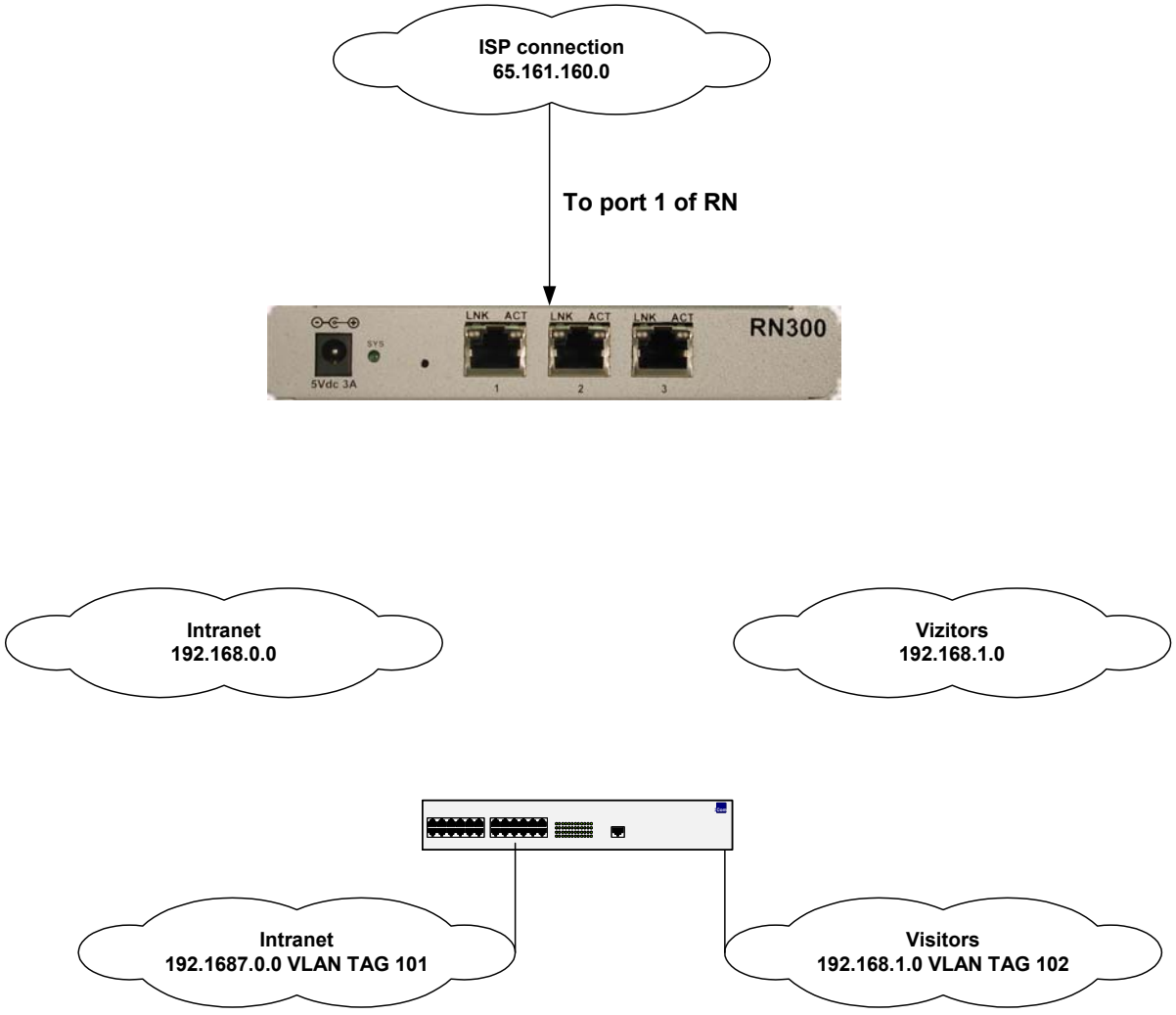
The summary of the configuration steps:

Step 1: Create the Zones
Step 2: Network Topology Configuration (IP settings for every zone)
Step 3: Check the routing configuration , add the route for the next hop.
Step 4: Bring Up the physical ports assigned to the zones
Step 5: NAT and firewall configuration

15.2 Example 2 : RN device with virtual zones.

In this example the company has the part of the Intranet and Visitors subnets connected trough the switch using VLANS . To secure the network and to give the internet access to the internet the virtual zones sould be configured on RN device .

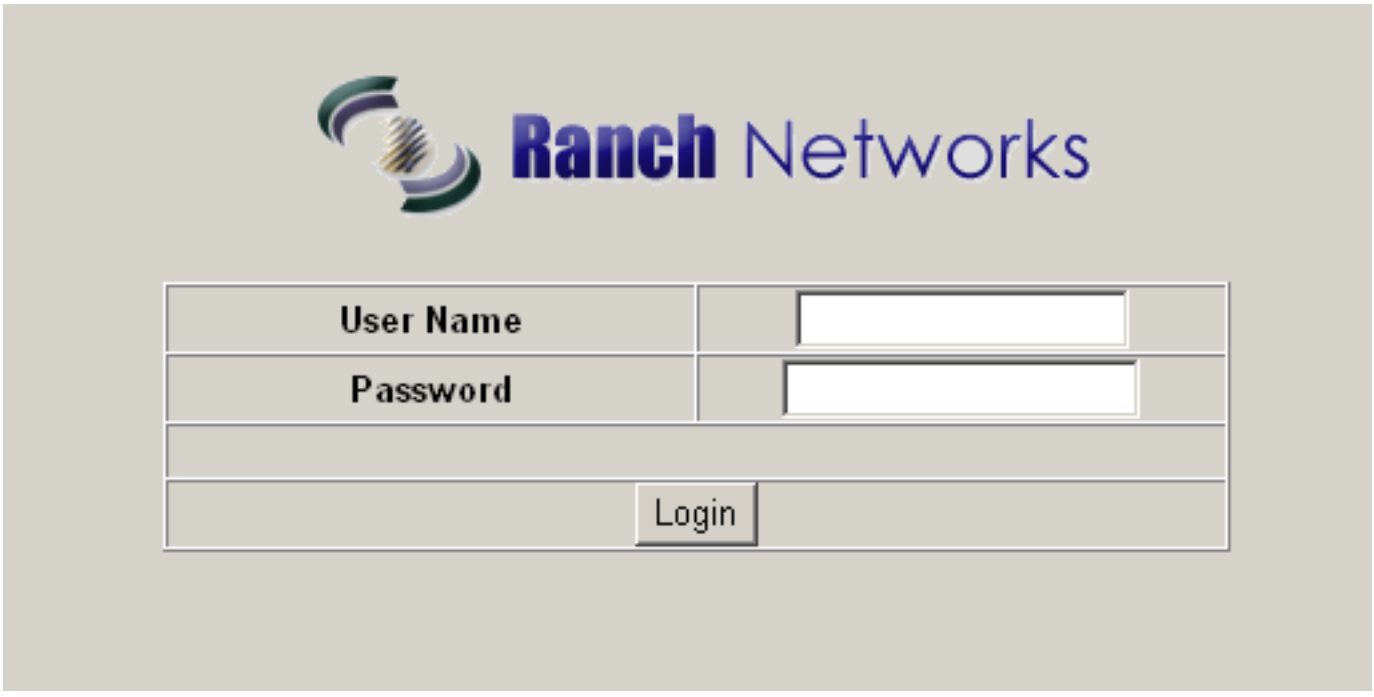
Figure 134. The initial picture for Virtual topology example



Pre configuration steps:

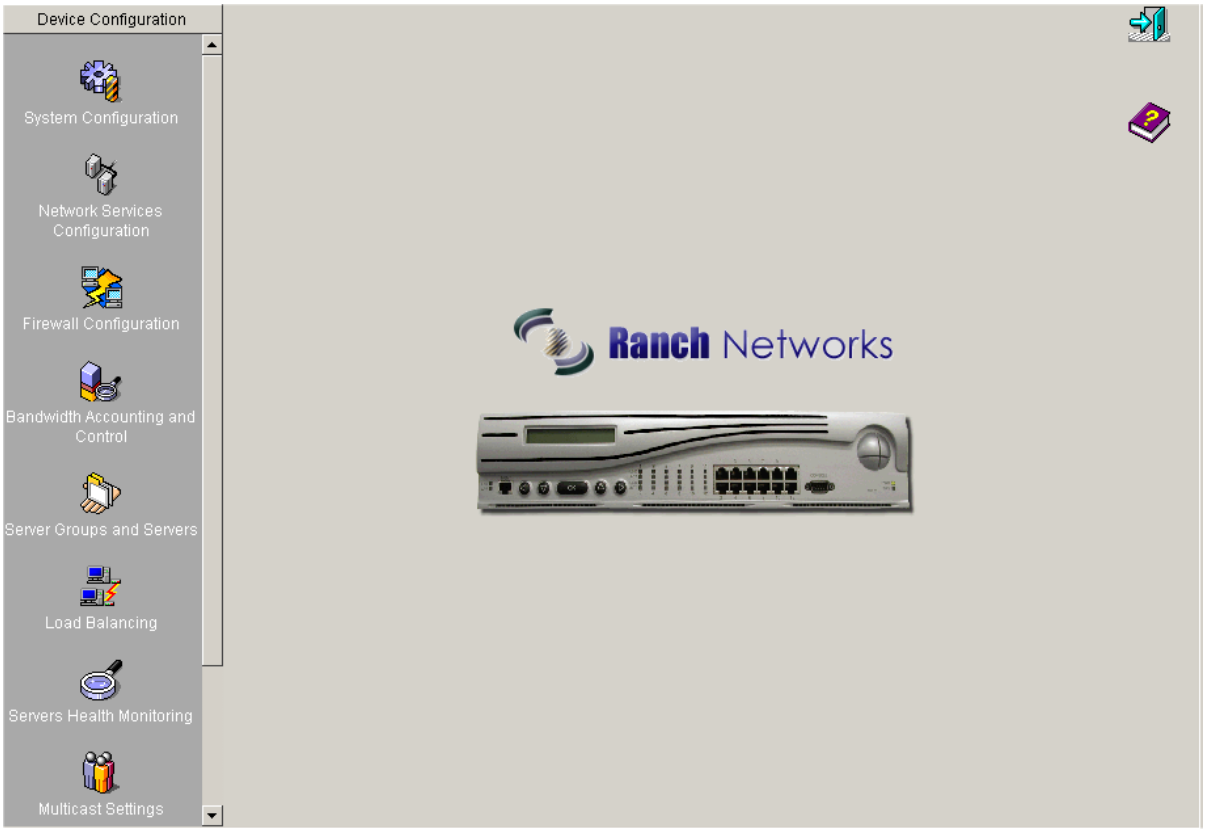
g) Power UP the RN device
h) Using front panel key pad, read or configure the management interface IP Address, subnet address and default GW values. Refer to RN20 Installation Guide, Section 2.h for front panel keypad operational details. (For ex. IP Address: 192.168.2.1, subnet: 255.255.255.0 and default gateway: 192.168.2.100)
i) Connect administrator's management system directly to RN20's management interface. This is a simple local management method. Refer to RN20 Installation Guide, Section 3.b for various methods of connecting management station.
j) Configure IP Address properties of management station to be in the same subnet of RN20's management interface. (For ex, IP Address: 192.168.2.100, subnet: 255.255.255.0 and default gateway: 192.168.2.1)
k) Check the connectivity between management system and RN20 by using PING. For ex. ping to 192.168.2.1 should be successful.
l) Ensure the management station meets minimum requirements. Refer to RN20 Installation Guide, Section 3.b. The IE browser should be version 5.5 or higher.
    a. Start the browser on management station and type url https://management-interfaceIP. For ex. **https://192.168.2.1** or **http://192.168.2.1**

Figure 135. RN examples - Login screen



g) Login with administrative privilege.

Figure 136. RN examples - the RN interface first page



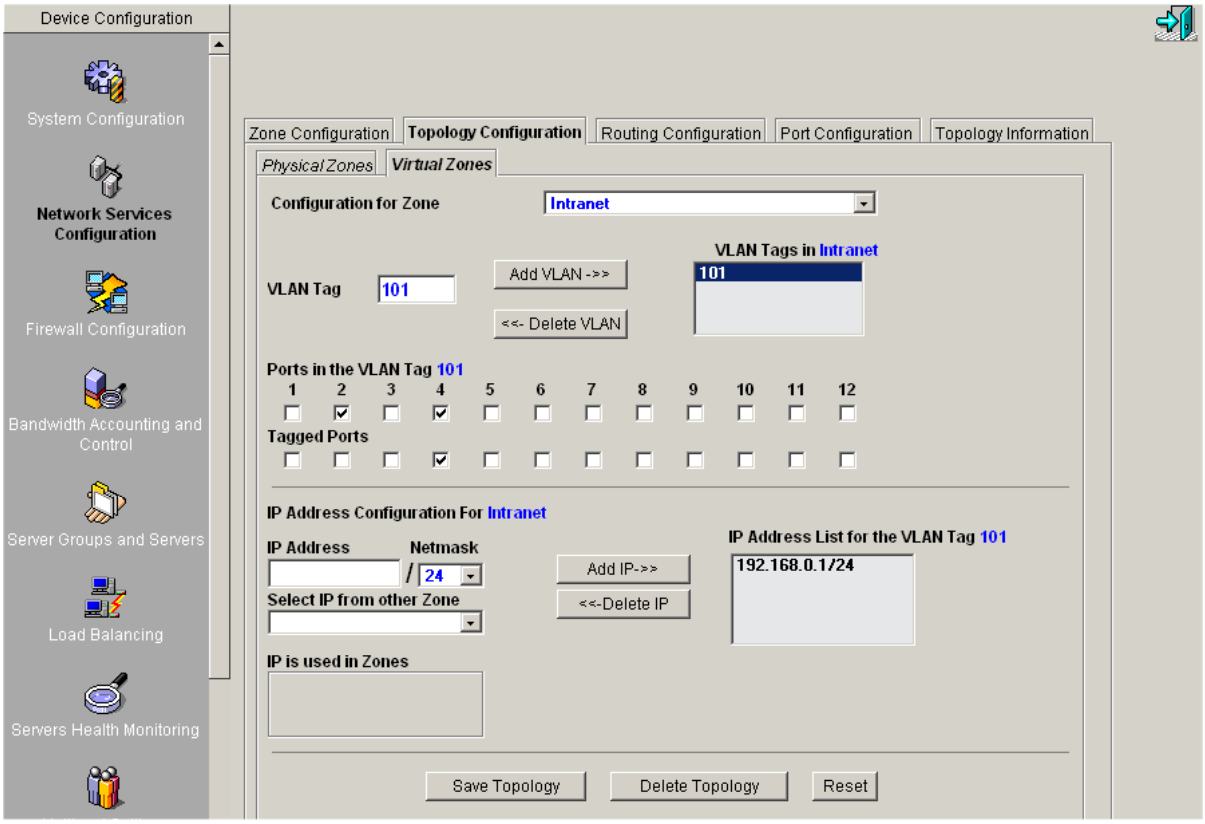
j) Check you have correct software image version. Go to System Configuration → Image Config → Version Info. Refer to RN 20 User Administration Guide, Section 5.1.3 for Image Management.
k) Be ready with your network topology and security rules to proceed configuring.

Step 1 (see the Example 1)

Step 2 : Network Topology Configuration (IP settings for every zone)

Click on Topology Configuration Tab , select **Virtual Zone** .
First , lets create the network topology for the Intranet zone .
One part of the Internet zone will be connected to the physical port 2 , another part will be connected to the physical port 4 , but the traffic that is coming to this port is tagged so only VLAN tag 101 will be assigned to the Intranet zone .

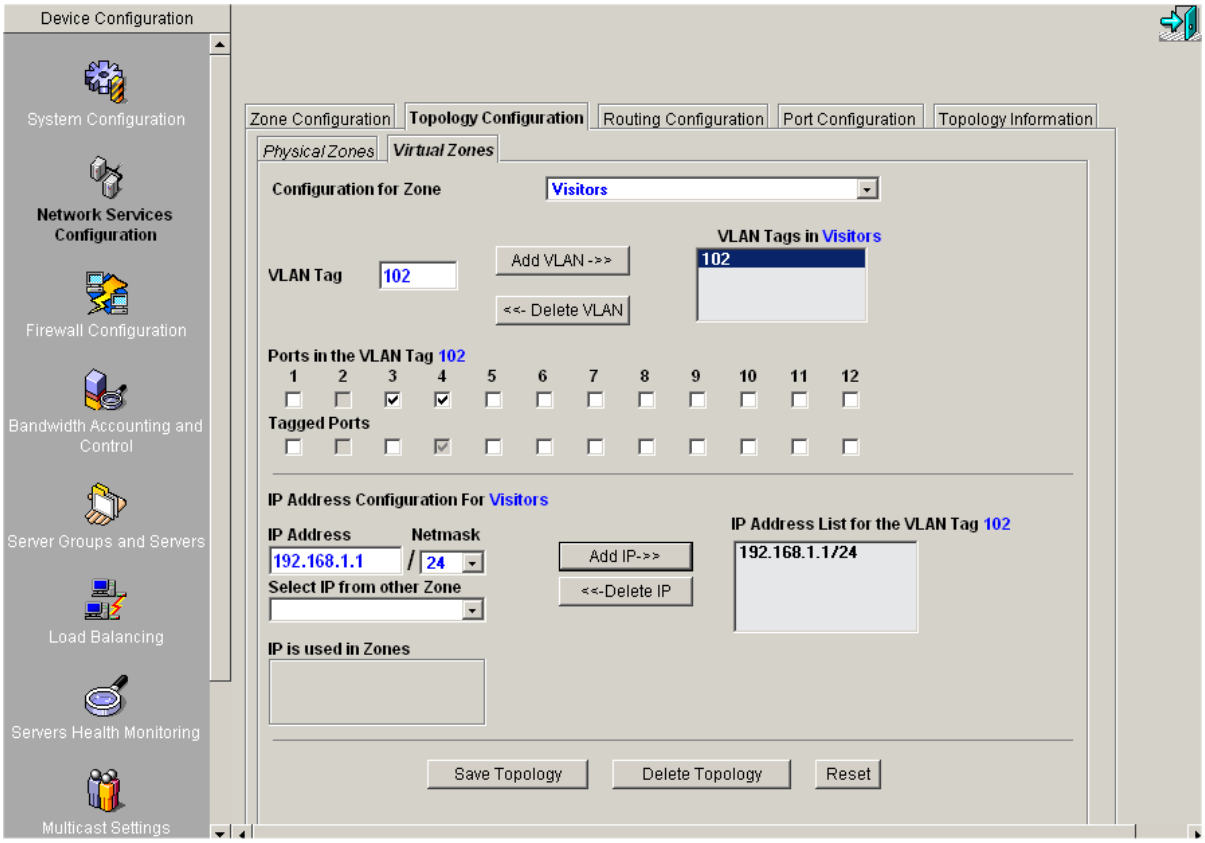
Figure 137. RN examples - Topology with the virtual zones



As it shown on the picture above the virtual zone Intranet consists of one physical port 2 and one tagged port 4 , only the traffic with VLAN tag 101 from port 4 belongs to this virtual zone

Next , , lets create the network topology for the Visitors zone .
One part of the Internet zone will be connected to the physical port 3 , another part will be connected to the physical port 4 , but the traffic that is coming to this port is tagged so only VLAN tag 102 will be assigned to the Visitors zone .

Figure 138. RN examples - Topology for the "Visitors" Zone

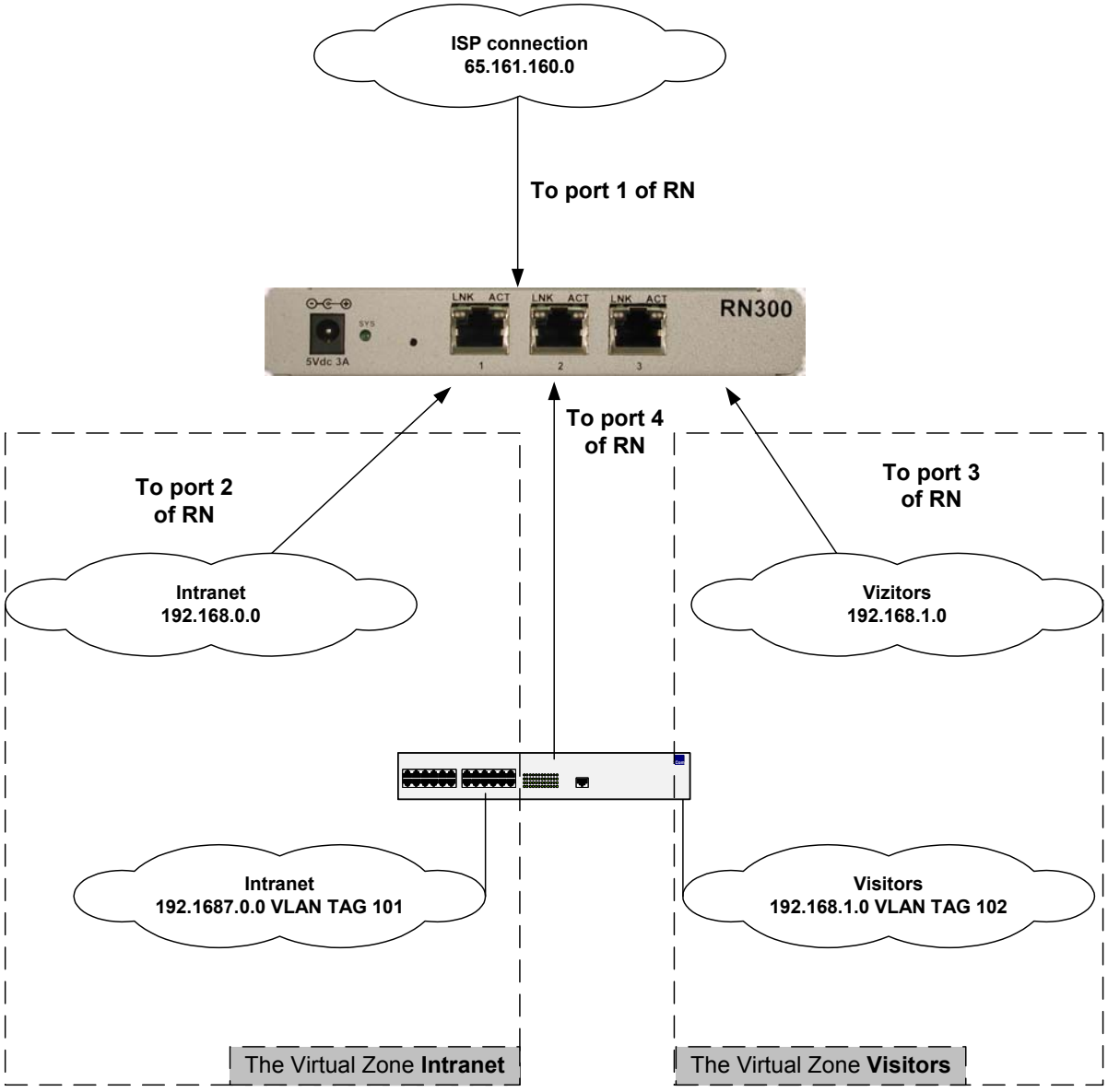


As it shown on the picture above the virtual zone Visitorst consists of one physical port 3 and one tagged port 4 , only the traffic with VLAN tag 102 from port 4 belongs to this virtual zone

Assuming that the security requirements are the same as for **Example 1** of this manual perform **Steps 3 to 5** from **Example 1** to complete the configuration procedure

The final network topology

Figure 139. RN examples - The final network topology (Virtual zones)

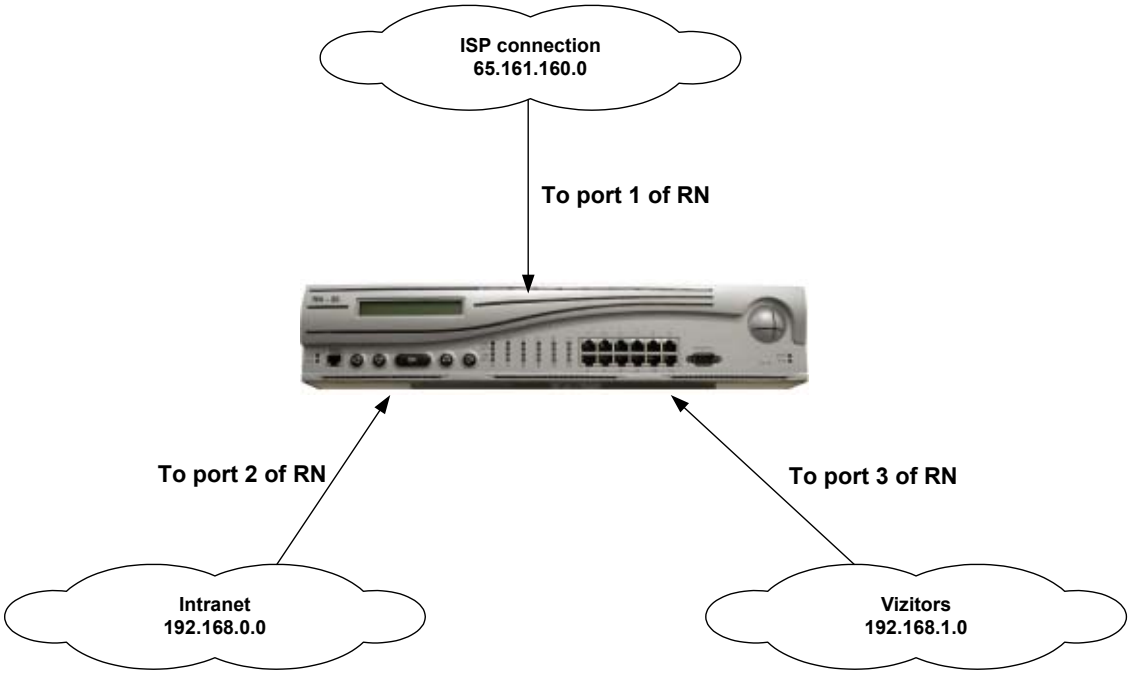


16.Example 3 : Different NAT configurations examples

RN device implements the several different types of NAT :
NAT, one-to-one Full NAT, one-to-one Half NAT and no-Nat.

The following examples is omitting the NAT options (see Example 1 of this manual) and assuming the following configuration:

Figure 140. Example 3 - Network Topology



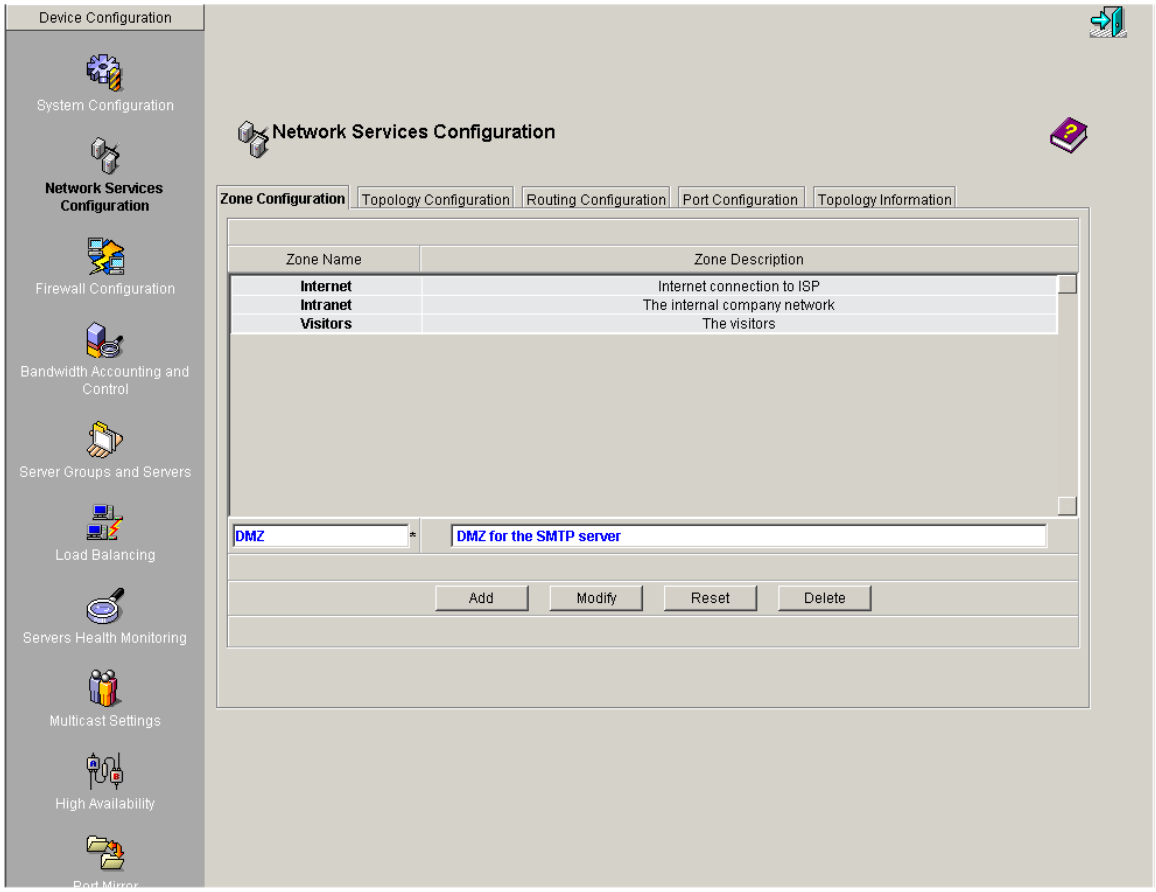
The network administrator was asked to install several public accessed servers. Some of them should be installed in the DMZ , another part of the servers already exists in the Intranet zone and should have restricted access from public network . The next table shows the network assets that will be used in this example.

Server IP Address	Service Type	Zone Name	Type of NAT
65.161.160.24	SMTP forward server	Will be installed at new DMZ zone	No Nat
192.168.0.24	HTTP	Exists in Intranet zone	One-to-one full NAT
192.168.0.27	FTP	Exists in Intranet zone	One-to-one half NAT

No NAT configuration

To establish the DMZ zone the new zone should be created

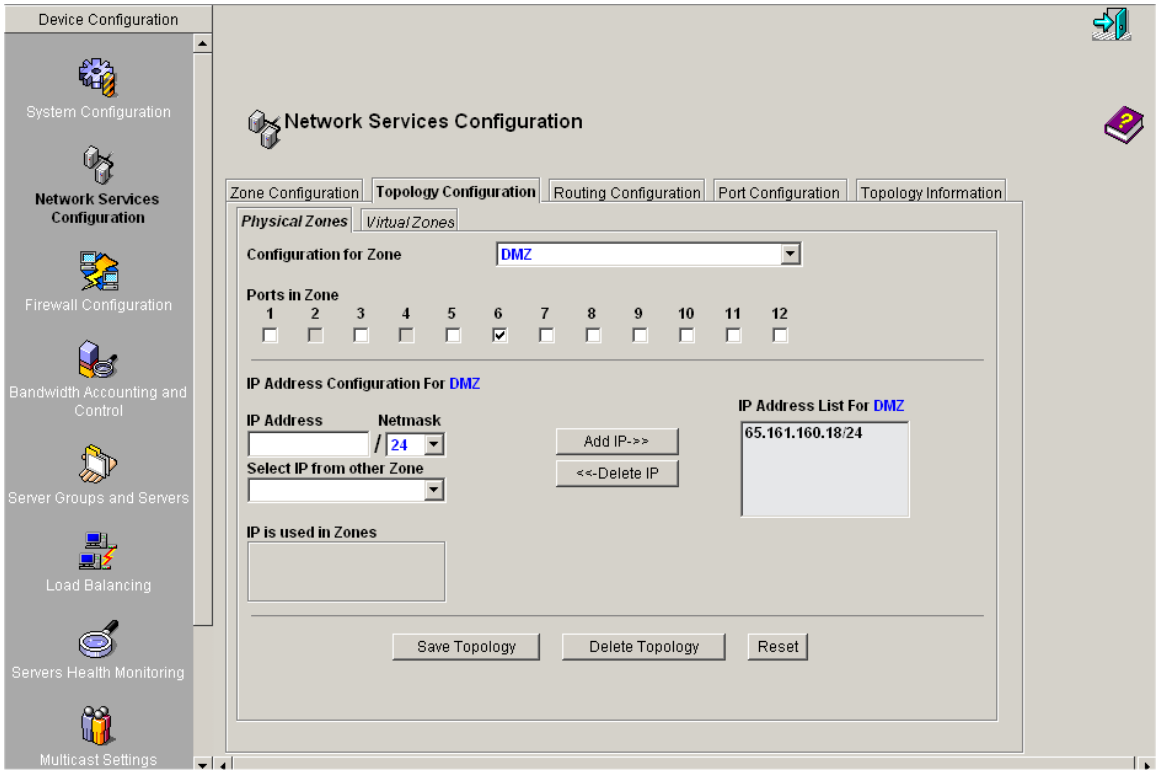
Figure 141. Example 3 - Zone Configuration



Press **Add** button to complete.

Proceed to Topology configuration for a new zone

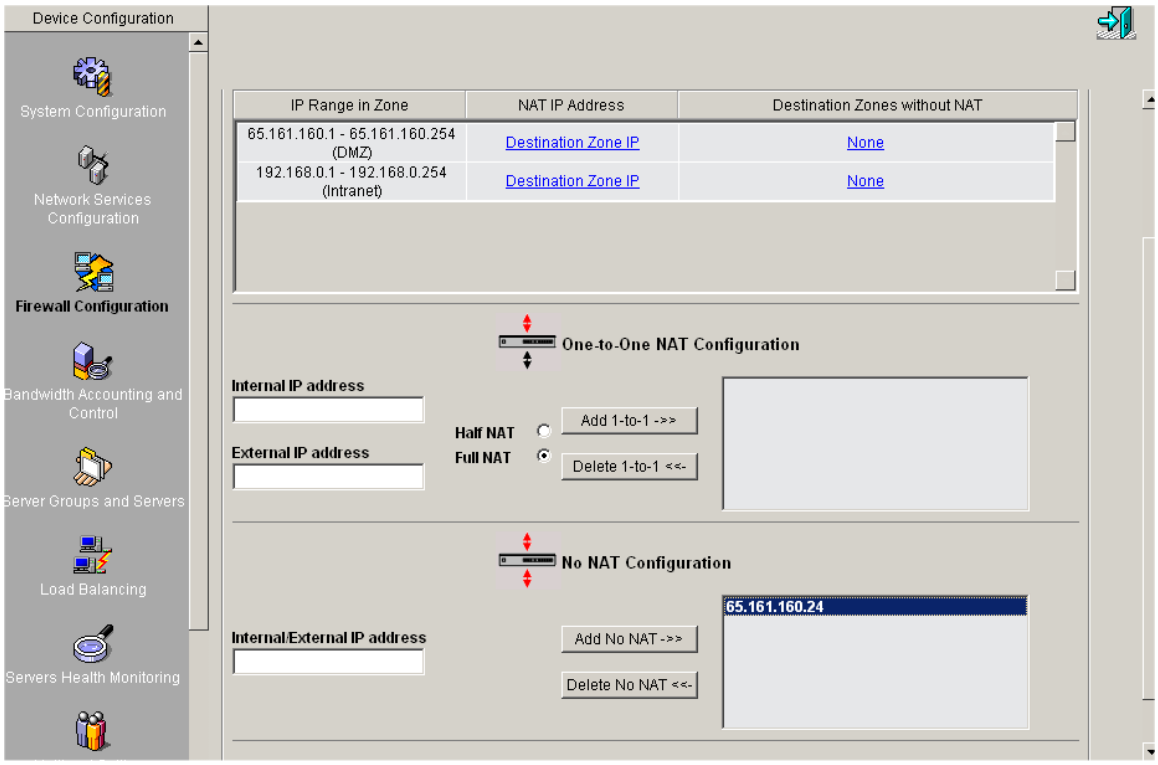
Figure 142. Example 3 - Zone Topology Configuration



The DMZ zone has 65.161.160.18 as the interface IP Address and was assigned to port 6. The SMTP server , according to the network assets table, has a public IP Address so it does not need to be NATed.

To configure no-NAT for this address , go to Firewall Configuration , then click on NAT configuration Tab

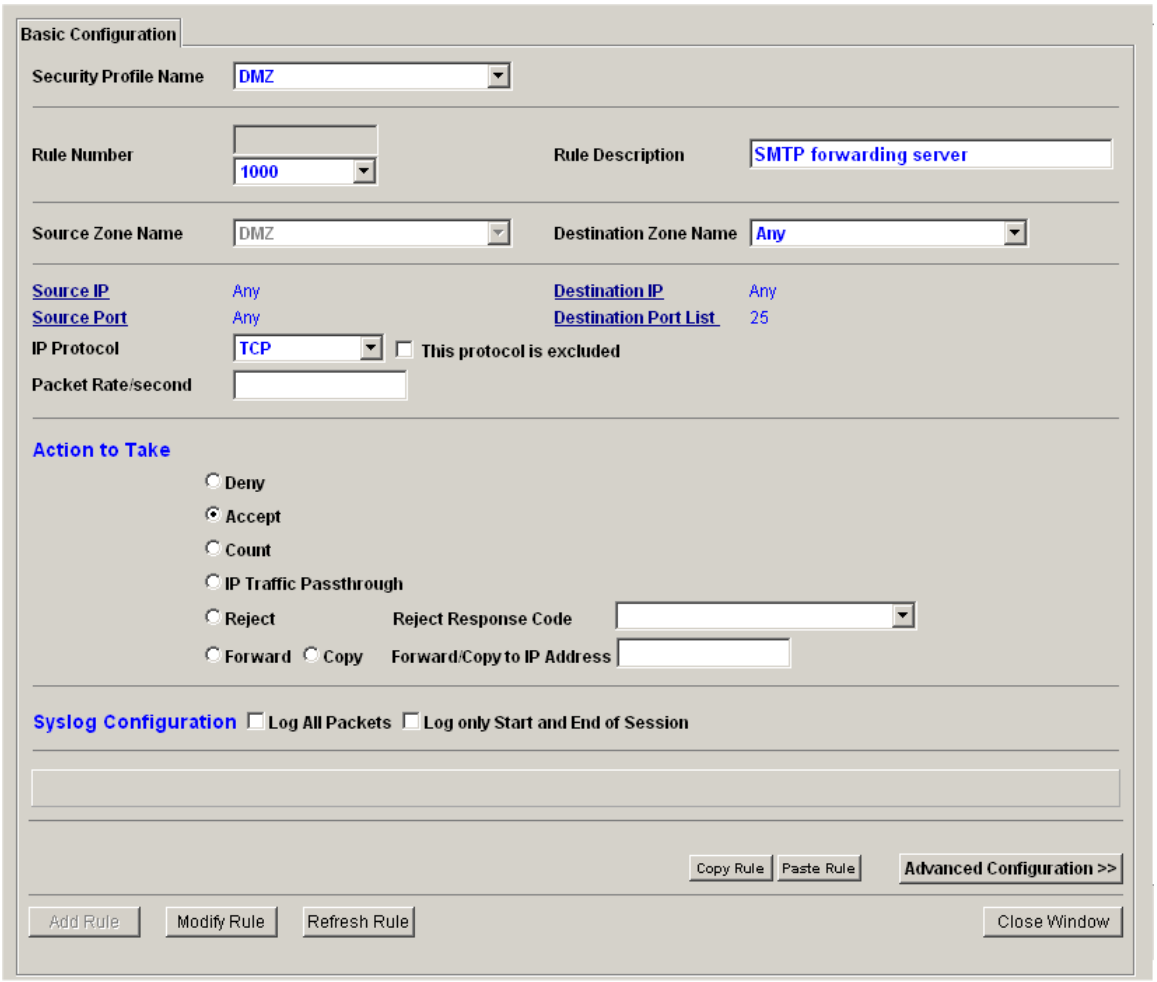
Figure 143. Example 3 - NAT Configuration



At this point the server 65.161.160.24 is configured as no-NAT , but still , it is the part of the secured zone and DMZ zone has only one rule that denies any traffic .

To complete the task click on **Security profiles** TAB , than press Add/Modify button . Create the rule as it shows on the next picture and press Add Rule

Figure 144. Example 3 - Security Profiles -> Rules Configuration



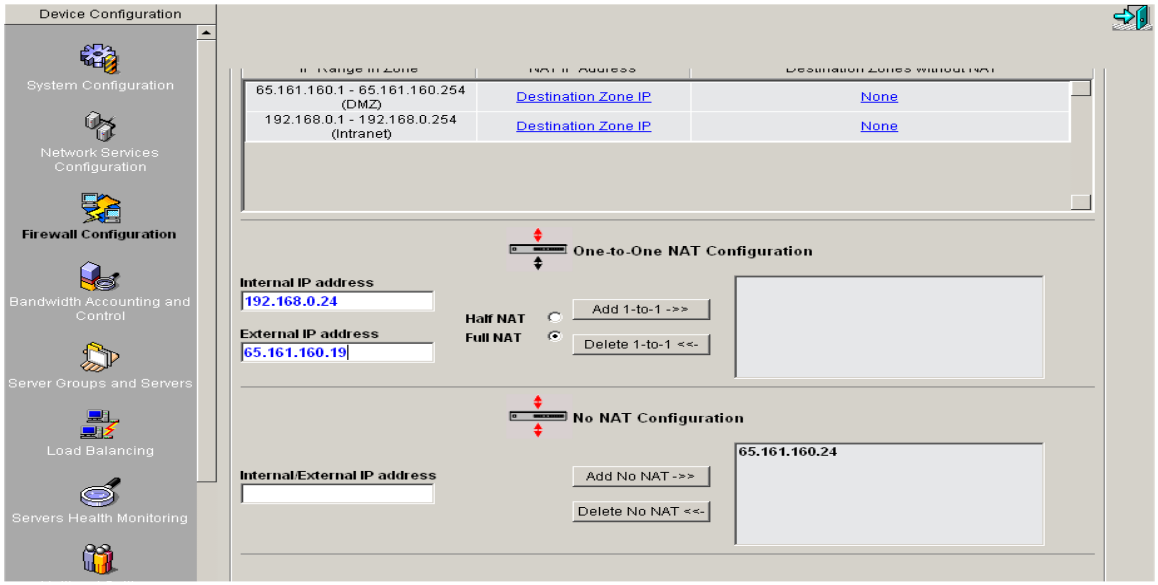
The first tasks is done

Server IP Address	Service Type	Zone Name	Type of NAT
65.161.160.24	**SMTP forward server**	**Will be installed at new DMZ zone**	**No Nat**
192.168.0.24	HTTP	Exists in Intranet zone	One-to-one full NAT
192.168.0.27	FTP	Exists in Intranet zone	One-to-one half NAT

The next tasks is to create one-to-one NAT to the internal servers.

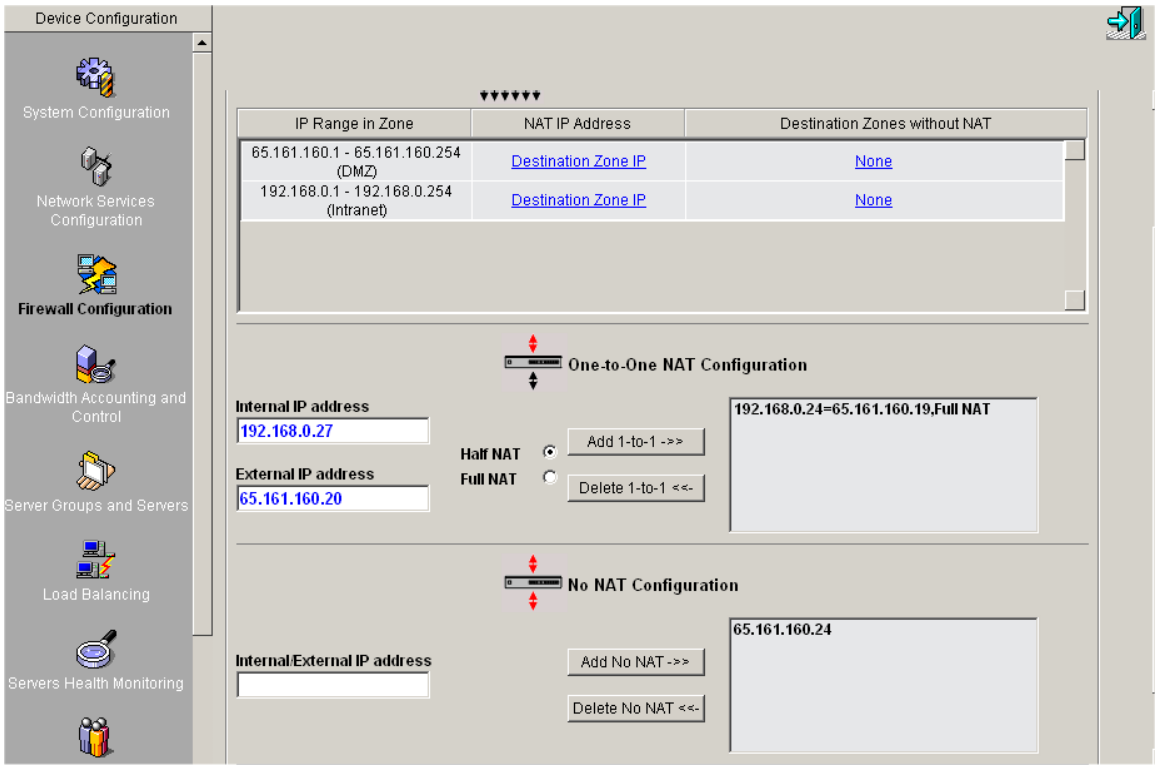
Click on NAT Configuration TAB
Configure the servers as it shown on the next picture

Figure 145. Example 3 - One-to-One NAT Configuration



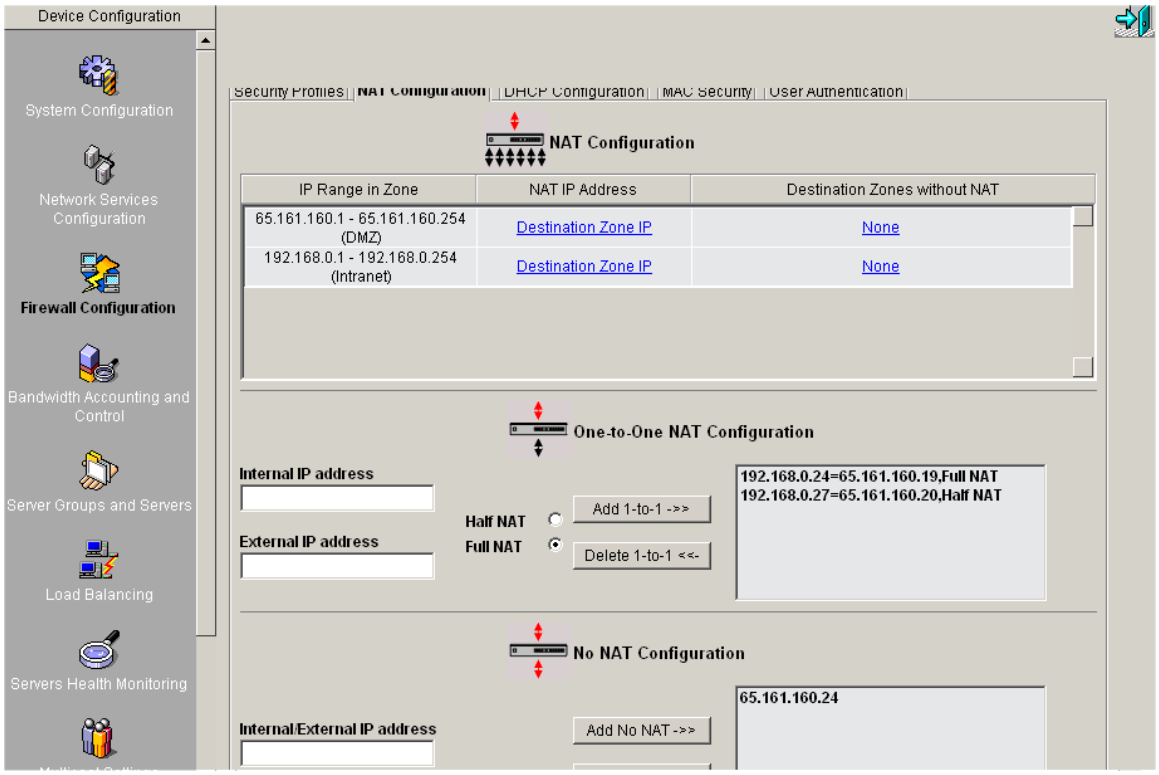
press **Add 1-to-1 ->**

Figure 146.Example 3 - One-to-One NAT Configuration (cont.)



press **Add 1-to-1 ->**

Figure 147.Example 3 - One-to-One NAT Configuration (cont)



The internal servers are configured with one-to-one NAT options and their private IP Addresses are taking out from the regular NAT range.

192.168.0.24 Was NATed 1-to-1 full NAT to 65.161.160.19 - means all source addresses for incoming traffic will be changed to 65.161.160.19

192.168.0.25 192.168.0.27 Was NATed 1-to-1 half NAT to 65.161.160.19 - means all source addresses for incoming traffic will have the original values (this will allow the Security Admin to keep track who is trying to login to FTP server)

To complete the configuration the rules that permit traffic to the public part of 1-to-1 NAT should be created at Internet zone (or at any zones that public IP addresses are assigned to)

17.Example 4: RN syslog configuration

If the syslog options is enabled (see **RN Configuration -> Syslog Config** part of the Users Manual) the RN device will log , for default, the following activities :

- All RN20 configuration changes
- All Administrator logins attempts
- All User authentication logins/logouts attempts

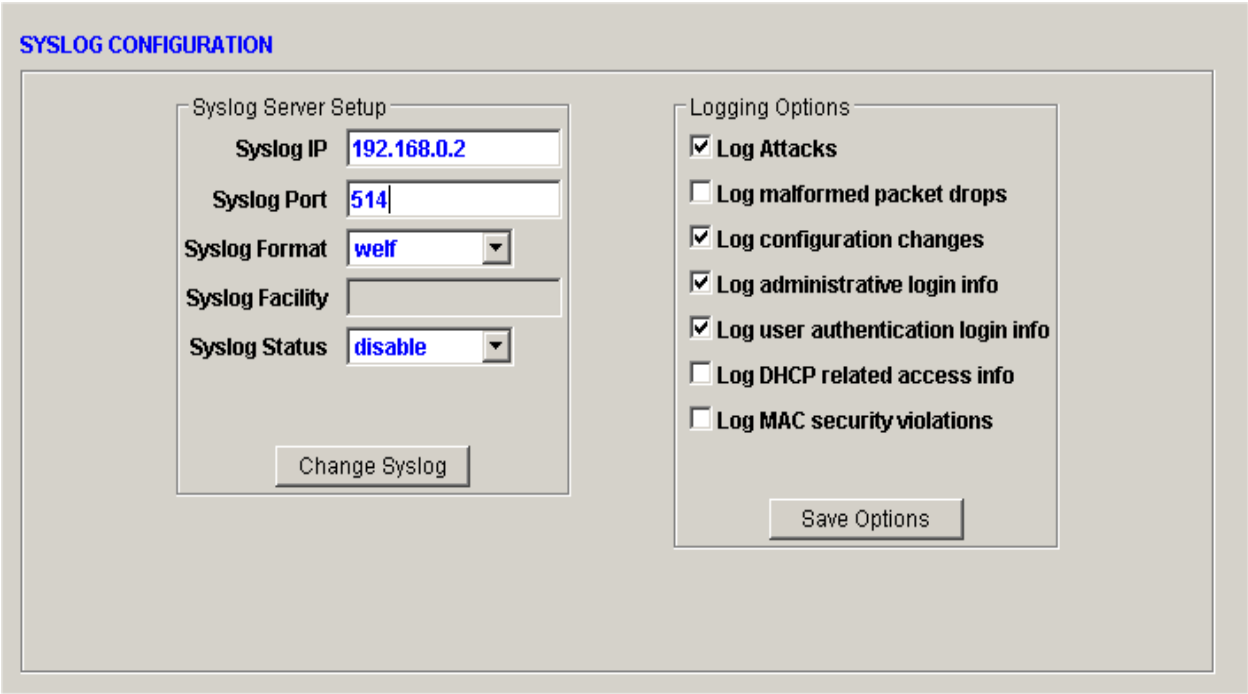
In addition to the options that are listed above the System Administrator can configure:

- All malformed Packets
- All DHCP related messages
- All MAC security violations, if MAC security is configured.

This example assumes that the syslog server (with the IP Address and port 514) is configured and accessible from the RN device management port.

Enable Syslog on RN device:

Figure 148. RN Syslog Configuration



Press **Change Syslog** to enable logging .

Make some changes in RN configuration and check the log file on the syslog server. Some examples of the log file messages(all records are shown in **WELF** format) :

The Configuration was changed

The date and time were changed then the next record will be sent to the log file:

```
Feb  5 11:41:47 192.1.1.159  id=firewall time="Feb 05 2004 12:43:58" fw=192.1.1.159 serial=20030026 pri=1 src=192.1.1.105
dst=192.1.1.159 dstport=443 proto=TCP type=local-mgmt user=root  msg="DATE-TIME mm/dd/yy=02/05/2004 11:43:17
modified"
```

The highlighted part of the message shows the new values for DATE-TIME settings.

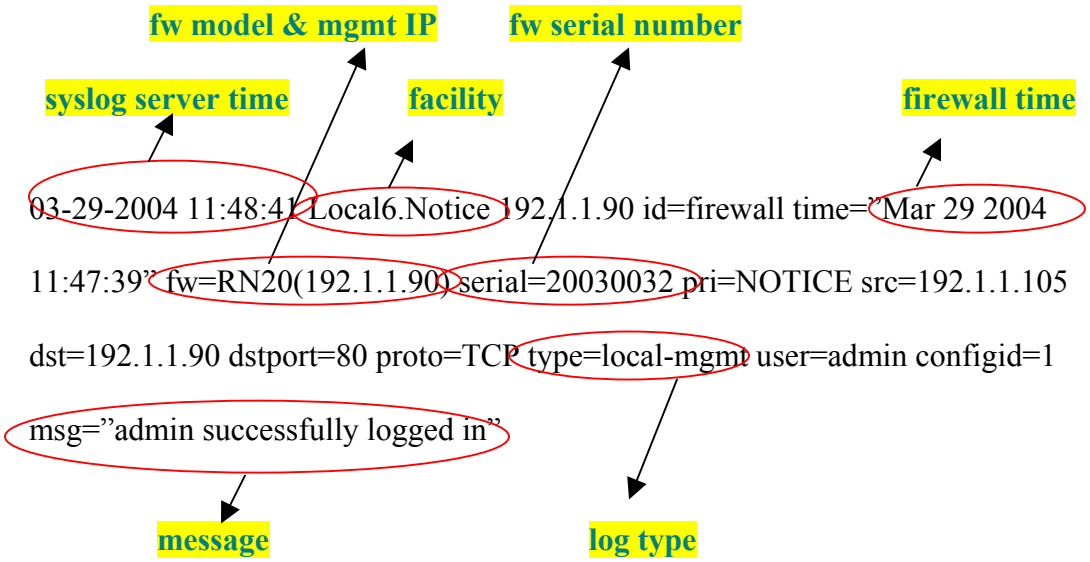
Users login
The user started the RN administration session:

```
Feb  6 10:54:15 192.1.1.159  id=firewall time="Feb 06 2004 10:57:50" fw=192.1.1.159 serial=20030026 pri=1 src=192.1.1.105
dst=192.1.1.159 dstport=443 proto=TCP type=local-mgmt user=root  msg=" successfully logged in "
```

The highlighted part of the message shows that the users "*root*" started to work.

18.RNxx log messages definitions

18.1 The fields of the RNxx log message



facility : Syslog facility default is 22.
Supports eight facilities LOCAL0(16) to LOCAL7(23)

id : firewall
vpn

time : Time stamp of firewall unit when event occurred

fw : model(mgmt-ip)

serial : Serial Number of RN unit (ex. 200300xx). This field is unique identifier.

pri : 0 → EMERGENCY (System in emergency state & unusable)
1 → ALERT (Immediate response required)
2 → CRITICAL (Critical condition)
3 → ERROR (Error condition)
4 → WARNING (Warning condition)
5 → NOTICE (Normal but significant condition)
6 → INFO (Information message)
7 → DEBUG (Debugging information)

src : Source IP Address

dst : Destination IP Address

srcport : Source port

dstport : Destination port

proto : IP protocol name (TCP, UDP, ICMP etc)

type : local-mgmt (Accessing RN device from dedicated management interface)
remote-mgmt (Accessing RN device from data port network)

user : session involved with user logged in

configid :

msg : Detailed message of the event

section : CTRL, LAN, WAN

18.2 Log Message categories

- Login / Logout related
- Front Panel settings modifications
- Reboot messages
- FW service status
- RNxx Management settings modifications
- Image file changes
- Configuration file changes
- FW user administration
- Zone configuration
- Topology configuration
- Routing configuration
- Port configuration
- FW Rule administration
- Security Profile administration
- NAT administration
- DHCP Relay configuration
- MAC Security administration

18.3 The log messages list and description

18.3.1 Login / Logout related

Event: FW Admin login from GUI (through the management port)
Log message:

07-22-2004 12:37:43 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:35:12" fw=**RN20(172.16.1.108)** serial=20030043 pri=NOTICE category=CONFIG subcat=LOGIN src=**10.1.2.105** dst=172.16.1.108 dstport=**443** type=local-mgmt proto=**TCP** user=**root** configid=0 Msg=Success Info=[Operation=Login] section=CTRL

Description: User root (from 10.1.2.105) performed the successful login to the RNxx (172.161.1.108 using port tcp:443) management GUI

Event: FW Admin logout from GUI (through the management port)
Log message:

07-22-2004 12:38:15 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:35:44" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=LOGIN src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Success Info=[Operation=Logout] section=CTRL

Description: User **root** (from **10.1.2.105**) performed the successful logout from the RNxx (**172.161.1.108** using port tcp:**443**) management GUI

Event: FW Admin login failed (invalid password) (through the management port)
Log message:

07-22-2004 12:38:36 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:36:05" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=LOGIN src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Failed Info=[Operation=Login Type="Invalid Password"] section=CTRL

Description: User **root** (from **10.1.2.105**) failed to login to the RNxx (**172.161.1.108** using port tcp:**443**) management GUI because of the wrong password (**Operation=Login Type="Invalid Password**")

Event: FW Admin login failed, invalid user (through the management port)
Log message:

07-22-2004 12:38:56 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:36:25" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=LOGIN src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=gytuytu configid=0 Msg=Failed Info=[Operation=Login Type="Invalid User"] section=CTRL

Description: User gytuytu (from **10.1.2.105**) failed to login to the RNxx (**172.161.1.108** using port tcp:**443**) management GUI because of the wrong user name (**Operation=Login Type="Invalid User"**)

Event: FW Admin login from GUI (Remote Mgmt through the data ports)
Log message:

07-22-2004 17:21:12 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 17:18:42" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=LOGIN src=172.16.8.2 dst=172.16.8.1 dstport=8443 type=remote-mgmt proto=TCP user=root configid=0 Msg=Success Info=[Operation=Login] section=CTRL

Description: User root (from **172.16.8.2**) performed the successful login to the RNxx (**172.161.1.108** using port tcp:**8443**)

Event: FW Admin logout from GUI (Remote Mgmt)
Log message:

07-22-2004 17:23:10 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 17:20:40" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=LOGIN src=172.16.8.2 dst=172.16.8.1 dstport=8443 type=remote-mgmt proto=TCP user=root configid=0 Msg=Success Info=[Operation=Logout] section=CTRL

Description: User root (from **172.16.8.2**) performed the successful logout from the RNxx (**172.161.1.108** using port tcp:**8443**)

Event: FW Admin login failed - invalid password (Remote Mgmt)
Log message:

07-22-2004 17:24:15 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 17:21:45" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=LOGIN src=172.16.8.2 dst=172.16.8.1 dstport=8443 type=remote-mgmt proto=TCP user=root configid=0 Msg=Failed Info=[Operation=Login Type="Invalid Password"] section=CTRL

Description: User **root** (from **172.16.8.2**) failed to login to the RNxx (**172.161.1.108** using port tcp:**8443**) management GUI because of the wrong password (**Operation=Login Type="Invalid Password**")

18.3.2 Front Panel settings modifications

Event: Front Panel Disable
Log message:

07-22-2004 12:18:04 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:15:34" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=MGMT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Logout Info=[Operation=Modified] section=CTRL

Description: User root disabled the write access to the LCD keyboard

---

18.3.3 Reboot messages

Event : Reboot from GUI
Log message:

07-22-2004 14:01:24 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 13:58:54" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=REBOOT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Success Info=[Operation=reboot] section=CTRL

Description : User **root** initiated the system reboot (Operation=reboot)

Event : Reboot from Reset or Power Cycle
Log message:

07-22-2004 14:29:22 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:26:52" fw=RN20(172.16.1.108) serial=20030043 pri=ALERT category=STATE subcat=NONE Msg=Alert Info=[Improper Shutdown Detected] section=CTRL

Description : The electrical power outage occurred.

18.3.4 FW service status

Event: FW Started successfully
Log message:

07-22-2004 14:03:10 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:00:39" fw=RN20(172.16.1.108) serial=20030043 pri=ALERT category=STATE subcat=NONE Msg=Up Info=[Firewall Service is UP] section=CTRL

Description: The FW service was started on RNxx device

18.3.5 RNxx Management settings modifications

Event: Management IP default GW modified
Log message:

07-22-2004 12:21:36 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:19:06" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=MGMTIP src=0.0.0.0 dst=0.0.0.0 dstport=0 type=LCD proto=NA user= configid=0 Msg=Success Info=[Operation="Modify Management IP"gateway=172.16.1.1] section=CTRL

Description: The default gateway for the management port was changed.

Event: Zone enabled for Remote Mgmt Access
Log messages:

07-22-2004 12:18:45 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:16:15" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=ZONE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Modified Info=[zone=Zone WebServer3] section=CTRL

Description: The user **root** has enabled the secure zone **WebServer3** for the remote management.

Event: Zone disabled for Remote Mgmt Access
Log message:

07-22-2004 12:19:48 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:17:18" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=ZONE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Modified Info=[zone=Zone WebLoad2] section=CTRL

Description: The user **root** has disabled the secure zone **WebServer2** for the remote management.

18.3.6 Image file changes

Event: Image download successful
Log messages:

07-22-2004 12:22:17 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:19:47" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=IMAGE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Success Info=[Operation="Image Download" Type="Download Started"server=192.1.1.79, login=hari, dir=/hari, file=r] section=CTRL

Description: The user **root** has successfully downloaded the software image to the RNxx device

---

Event: Image download failed
Log message:

07-22-2004 12:32:44 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:30:14" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=IMAGE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Failed Info=[Operation="Image Download" Type="Invalid Params"server=192.1.1.79, login=hari, dir=/hari1, file=r] section=CTRL

Description: The software image download failed .

18.3.7 Configuration file changes

Event: Configuration upload
Log message:

07-22-2004 12:23:23 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:20:53" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=CONFIG src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Success Info=[Operation=Upload server=192.1.1.79 type=configB] section=CTRL

Description: The user **root** has successfully uploaded the configuration file from the RNxx device

---

Event: Configuration download
Log message:

07-22-2004 12:40:29 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:37:58" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=CONFIG src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Success Info=[Operation=Download server=192.1.1.79 type=configA] section=CTRL

Description: The user **root** has successfully downloaded the configuration file to the RNxx device

---

18.3.8 FW user administration

Event: User added
Log message

07-22-2004 12:40:57 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:38:26" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=MGMT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Modified Info=[Operation="Add New user" user=admin2 group=admin] section=CTRL

Description: The user **admin2** was successfully added with the admin privilege (Operation="Add New user" user=admin2 group=admin)

Event: User deleted
Log message:

07-22-2004 12:41:16 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:38:45" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=MGMT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Modified Info=[Operation="Delete User" user=admin2] section=CTRL

Description: The user **admin2** was deleted

18.3.9 Zone configuration

Event: Zone Added
Log message:

07-22-2004 12:41:40 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:39:09" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=ZONE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Created Info=[zone=Zone Test] section=CTRL

Description: The secure zone **Test** was created.

Event: Zone Modified
Log message:

07-22-2004 12:41:59 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:39:28" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=ZONE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Modified Info=[zone=Zone Test] section=CTRL

Description: The secure zone **Test** was modified.

Event: Zone Deleted
Log message:

07-22-2004 12:42:16 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:39:45" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=ZONE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=0 Msg=Deleted Info=[zone=Zone Test] section=CTRL

Description: The secure zone **Test** was deleted.

18.3.10 Topology configuration

Event: Zone Topology Created
Log messages:

07-22-2004 12:43:53 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:41:23" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=NAT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=2 Msg=Created section=CTRL

07-22-2004 12:43:53 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:41:22" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=TOPO src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=2 Msg=Created Info=[ip=172.16.50.1 vlanid=12] section=CTRL

07-22-2004 12:43:53 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:41:22" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=TOPO src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=2 Msg=Created Info=[ip=172.16.50.1 mask=255.255.255.0] section=CTRL

07-22-2004 12:43:53 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:41:22" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=TOPO src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=2 Msg=Created Info=[vlanid=12 port=12] section=CTRL

07-22-2004 12:43:53 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:41:22" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=TOPO src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=2 Msg=Created Info=[vlanid=12] section=CTRL

Description: The topology for the secure zone was created on the RNxx device

---

Event: Zone Topology Deleted
Log messages:

07-22-2004 12:45:05 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:42:34" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=TOPO src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=3 Msg=Deleted Info=[vlanid=12] section=CTRL

07-22-2004 12:45:05 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:42:34" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=TOPO src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=3 Msg=Deleted Info=[vlanid=12 port=12] section=CTRL

07-22-2004 12:45:05 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:42:34" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=TOPO src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=3 Msg=Deleted Info=[ip=172.16.50.1 mask=255.255.255.0] section=CTRL

07-22-2004 12:45:05 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:42:34" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=TOPO src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=3 Msg=Deleted Info=[ip=172.16.50.1 vlanid=12] section=CTRL

07-22-2004 12:45:05 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:42:34" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=NAT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=3 Msg=Modified section=CTRL

Description: The topology for the secure zone was deleted form the RNxx device

---

18.3.11 Routing configuration

Event: Static Route Added
Log messages:

07-22-2004 12:45:53 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:43:22" fw=RN20(172.16.1.108) serial=20030043 pri=ALERT category=STATE subcat=NONE Msg=Up Info=[Gateway 172.16.1.1 is now reachable.] section=CTRL

07-22-2004 12:45:39 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:43:09" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=ROUTE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=3 Msg=Created Info=[dest=0.0.0.0 mask=0.0.0.0 gateway=172.16.1.1] section=CTRL

Description: The static route 0.0.0.0 172.16.1.1. was added to RNxx routing table .

Event: Static Route Deleted
Log messages:

07-22-2004 12:45:37 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:43:06" fw=RN20(172.16.1.108) serial=20030043 pri=ALERT category=STATE subcat=NONE Msg=Down Info=[No default gateways available!] section=CTRL

07-22-2004 12:45:37 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:43:06" fw=RN20(172.16.1.108) serial=20030043 pri=CRITICAL category=STATE subcat=NONE Msg=Down Info=[Gateway 172.16.1.1 is unreachable.] section=CTRL

07-22-2004 12:45:37 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:43:06" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=ROUTE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=3 Msg=Deleted Info=[dest=0.0.0.0 mask=0.0.0.0 gateway=172.16.1.1] section=CTRL

Description: The static route 0.0.0.0 172.16.1.1. was deleted from RNxx routing table .

18.3.12 Port configuration

Event: Port Admin UP
Log message:

07-22-2004 12:47:00 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:44:29" fw=RN20(172.16.1.108) serial=20030043 pri=ALERT category=STATE subcat=NONE Msg=Up Info=[Port=12] section=CTRL

07-22-2004 12:46:58 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:44:28" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=PORT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=4 Msg=Modified Info=[port=12] section=CTRL

Description: The admin status for the port 12 was changed from Down to Up.

Event: Port Admin Down
Log message:

07-22-2004 12:47:29 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:44:58" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=PORT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=4 Msg=Modified Info=[port=12] section=CTRL

Description: The admin status for the port 12 was changed from Up to Down.

18.3.13 FW Rule administration

Event: FW rule added
Log message:

07-22-2004 12:48:08 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:45:37" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=FW src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=4 Msg=Created Info=[from-zone=Zone Test rule=100] section=CTRL

Description: The rule number **100** was added for the secure zone **Test** by the user **root**

Event: FW rule modified
Log messages:

07-22-2004 12:48:33 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:46:02" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=FW src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=4 Msg=Modified Info=[from-zone=Zone Test rule=100] section=CTRL

Description: The rule number **100** that belongs to the secure zone **Test** was modified by the user **root.**

Event: FW rule deleted
Log message:

07-22-2004 12:49:00 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 12:46:30" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=FW src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=4 Msg=Deleted Info=[from-zone=Zone Test rule=100] section=CTRL

Description: The rule number **100** that used to belong to the secure zone **Test** was deleted by the user **root.**

18.3.14 Security Profile administration

Event: Security Profile created
Log message:

07-22-2004 14:51:14 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:48:44" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=PROFILE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=7 Msg=Created Info=[profile=p1] section=CTRL

Description: The security profile **p1** was created by the user root

---

Event: Security Profile deleted
Log message:

07-22-2004 14:52:32 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:50:02" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=PROFILE src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=7 Msg=Deleted Info=[profile=p1] section=CTRL

Description: The security profile **p1** was deleted by the user root

---

Event: Security Profile – FW rule added
Log message:

07-22-2004 14:54:57 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:52:27" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=FW src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=7 Msg=Created Info=[profile=p1 rule=105] section=CTRL

Description: The firewall rule number **105** was added to the security profile **p1** by the user root

---

Event: Security Profile – FW rule modified
Log message:

07-22-2004 14:57:24 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:54:54" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=FW src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=7 Msg=Modified Info=[profile=p1 rule=105] section=CTRL

Description: The firewall rule number **105** that belongs to the security profile **p1** was modified by the user root

---

Event: Security Profile – FW rule deleted
Log message:

id=firewall time="July 22 2004 14:55:29" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=FW src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=7 Msg=Deleted Info=[profile=p1 rule=105] section=CTRL

Description: The firewall rule number **105** that used to belong to the security profile **p1** was deleted by the user root

---

18.3.15 NAT administration

Event: Full NAT Rule added
Log message:

07-22-2004 14:31:33 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:29:03" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=NAT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=1 Msg=Created section=CTRL

Description: The full NAT rule was added to the RNxx configuration by the user **root**.

Event: Full NAT Rule deleted
Log message:

07-22-2004 14:32:15 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:29:45" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=NAT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=2 Msg=Modified section=CTRL

Description: The full NAT rule was deleted from the RNxx configuration by the user **root**.

Event: No NAT Rule added
Log message:

07-22-2004 14:34:22 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:31:52" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=NAT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=4 Msg=Created section=CTRL

Description: The No NAT rule was added to the RNxx configuration by the user **root**. .

Event: No NAT Rule deleted
Log message

07-22-2004 14:35:25 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:32:55" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=NAT src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=5 Msg=Modified section=CTRL

Description: The No NAT rule was deleted from the RNxx configuration by the user **root**. .

18.3.16 DHCP Relay configuration

Event: DHCP Relay configuration added
Log message

07-22-2004 14:37:20 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:34:50" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=DHCP src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=6 Msg=Modified Info=[status, zone-list, serv-addr] section=CTRL

Description: The DHCP relay rule was added to the RNxx configuration by the user **root**. .

Event: DHCP Relay configuration modified
Log message

07-22-2004 14:38:04 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:35:34" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=DHCP src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=6 Msg=Modified Info=[status, zone-list, serv-addr] section=CTRL

Description: The DHCP relay rule was modified by the user **root**. .

18.3.17 MAC Security administration

MAC Security "Allowed" configured for a zone

07-22-2004 14:38:55 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:36:25" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=MAC src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=6 Msg=Created Info=[zone=Zone MC-Client mac=00:00:00:01:11:00] section=CTRL

07-22-2004 14:38:48 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:36:18" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=MAC src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=6 Msg=Modified Info=[zone=Zone MC-Client mac=aa:aa:aa:aa:aa:aa] section=CTRL

MAC Security "Allowed" configuration modifed for a zone

07-22-2004 14:40:12 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:37:42" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=MAC src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=6 Msg=Modified Info=[zone=Zone MC-Client mac=00:00:00:11:11:00] section=CTRL

MAC Securityy "Deny" configuration created for a zone

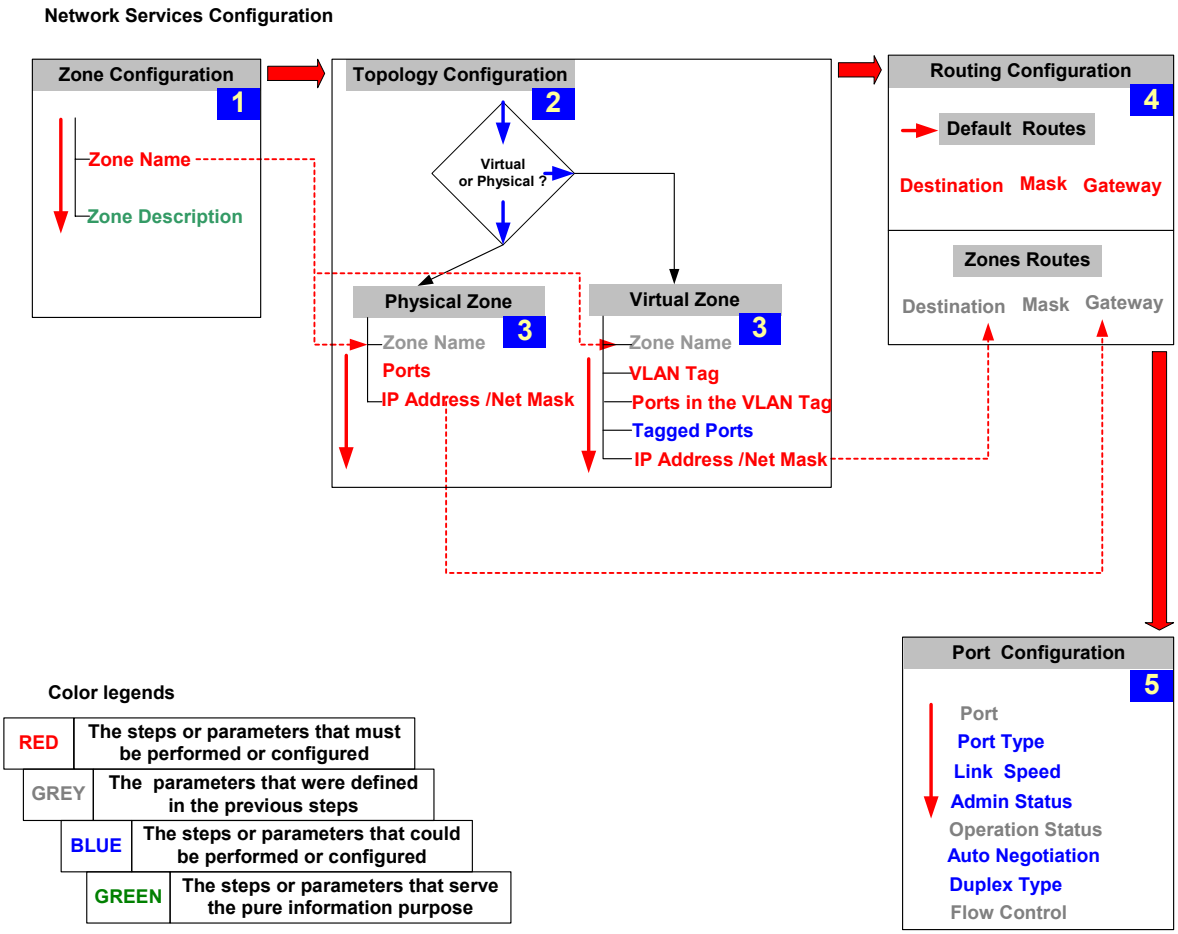
07-22-2004 14:41:08 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:38:38" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=MAC src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=6 Msg=Created Info=[zone=Zone Nessus1 mac=00:00:11:11:11:00] section=CTRL

MAC Securityy "Deny" configuration modified for a zone

07-22-2004 14:41:54 Local7.Debug 172.16.1.108 id=firewall time="July 22 2004 14:39:24" fw=RN20(172.16.1.108) serial=20030043 pri=NOTICE category=CONFIG subcat=MAC src=10.1.2.105 dst=172.16.1.108 dstport=443 type=local-mgmt proto=TCP user=root configid=6 Msg=Modified Info=[zone=Zone Nessus1 mac=00:00:11:12:11:00] section=CTRL

19.RN Services Configuration routes

19.1 Networks Services Configuration route

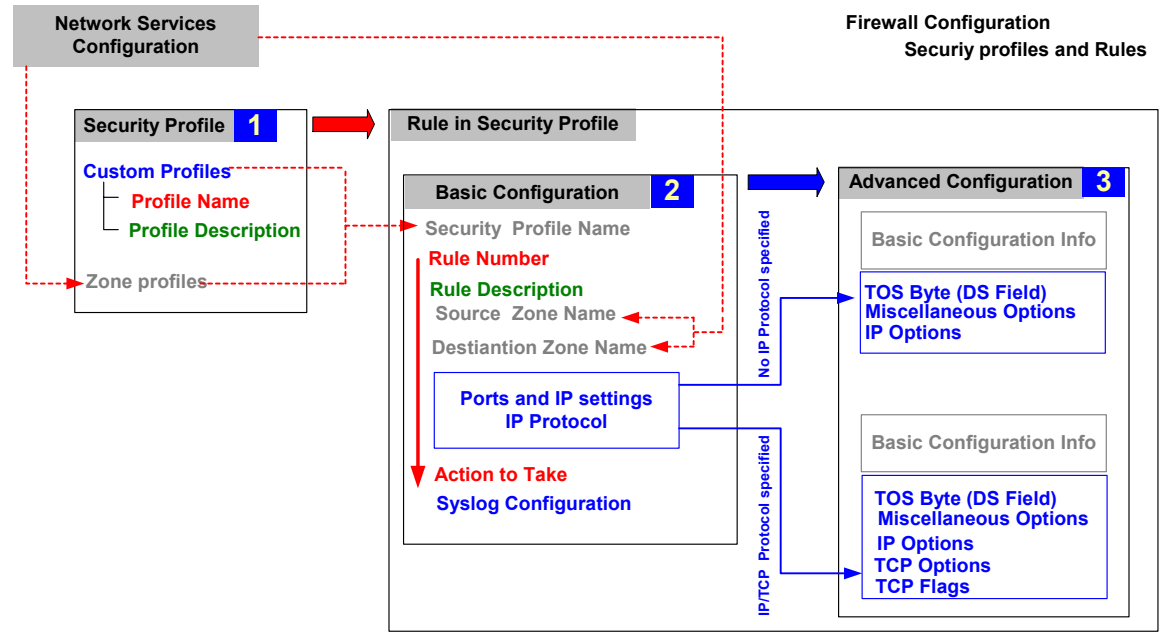


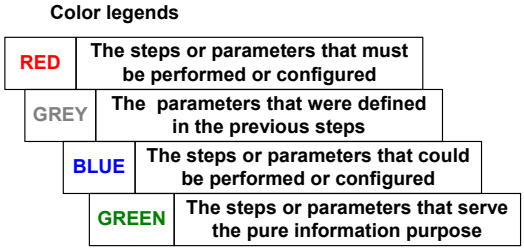
For more information about Network Services Configuration please refer to the chapter

"Network Services Configuration" of the RN Users manual .

19.2 Firewall Configuration Route

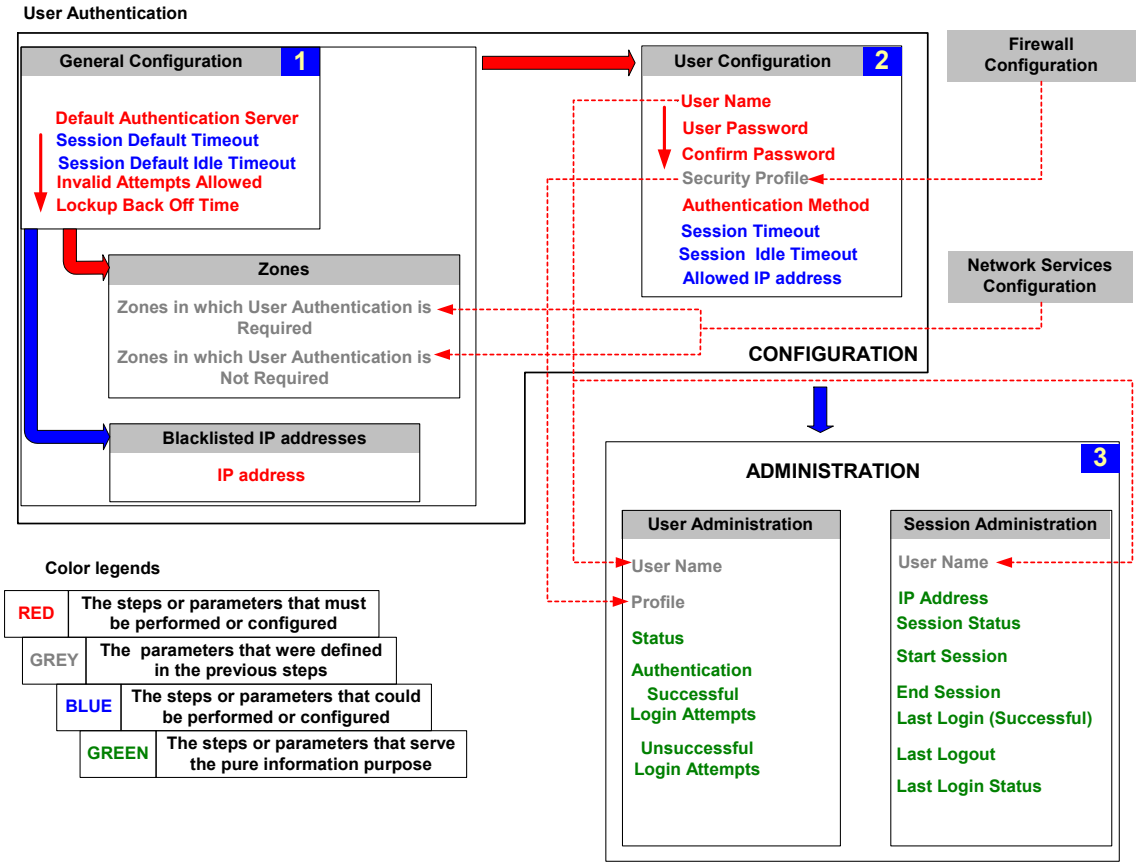
19.2.1 Security profiles and Rules Configuration





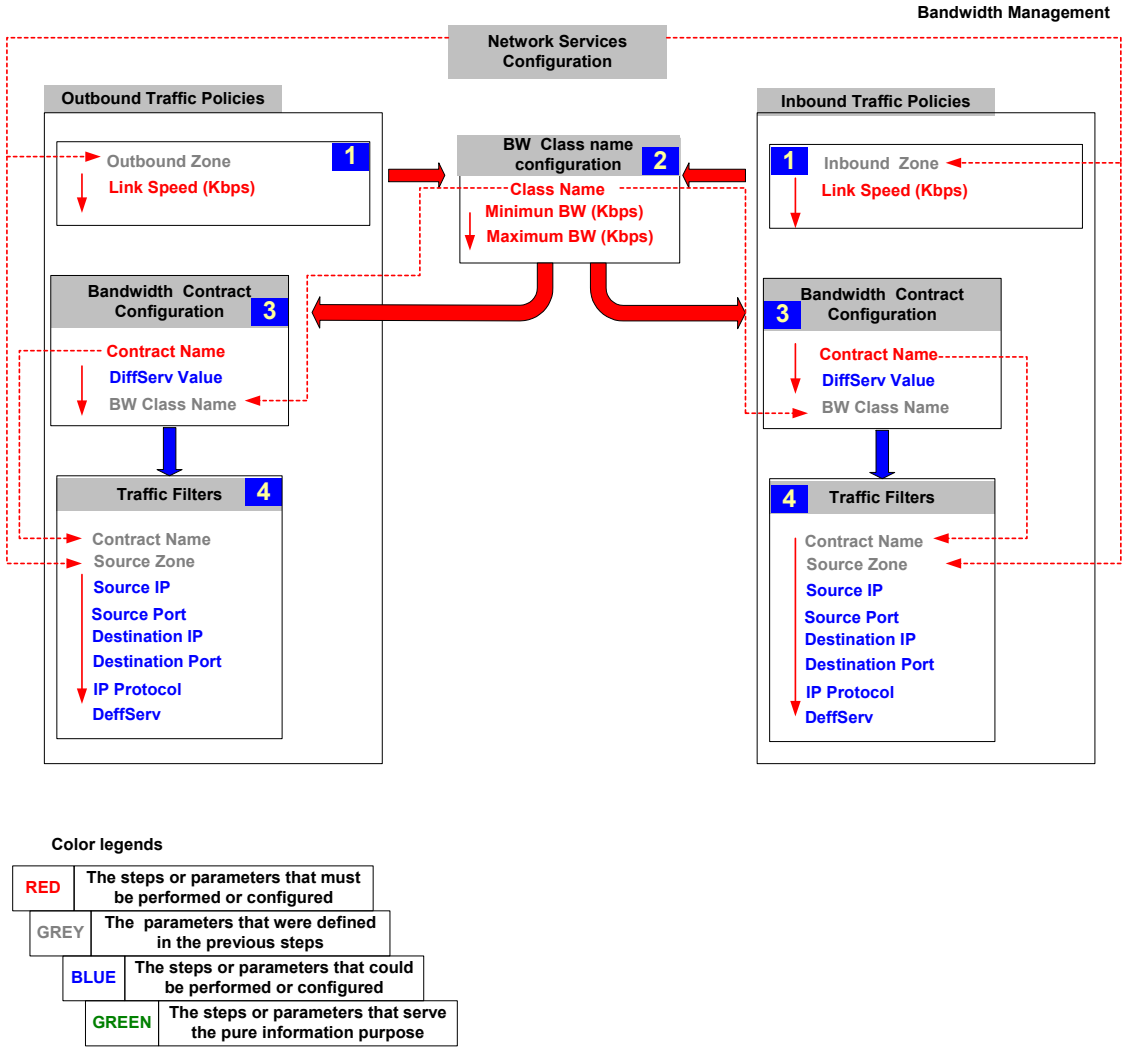
For more information about Firewall Configuration please refer to the chapter "Firewall Configuration" of the RN Users manual .

19.2.2 User Authentication Configuration



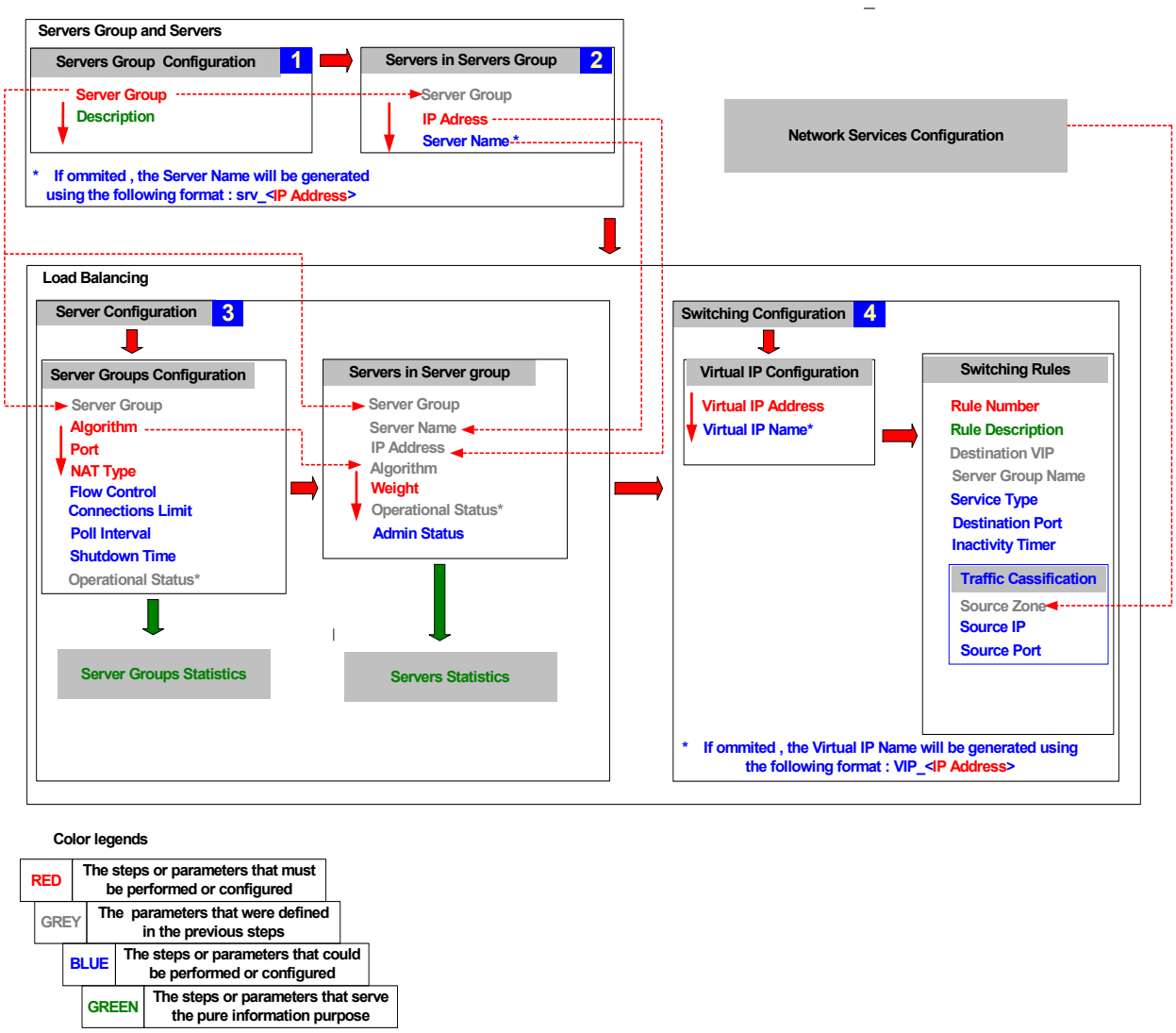
For more information about User Authentication Configuration please refer to the chapter "User Authentication Configuration" of the RN Users manual .

19.3 Bandwidth Accounting and Control Configuration route



For more information about Firewall Configuration please refer to the chapters "Bandwidth Accounting and Control Configuration" of the RN Users manual .

19.4 Servers Group and Load Balancing Configuration route



For more information about Servers and Load Balancing Configuration please refer to the chapters “Server Groups and Servers Configuration” and “Load Balancing” of the RN Users manual.

20.Dictionary

20.1 NAT

NAT is a method by which IP addresses are mapped from one address space to another to provide transparent routing to the end hosts.

20.2 Interface (zone topology)

The IPv4 format IP Address (for example 192.168.1.1) that assigned to the secure zone One secure zone can be configured with the multiple interfaces (IP Addresses)

20.3 Port (zone topology)

The physical port on RNxx device.

20.4 Rule

The policy that regulates network traffic. There are several types of the rules on RNxx device: firewall rule, switching rule (load balancing).

20.5 Rule (firewall)

The policy that is used by RNxx firewall to control network traffic

20.6 Rule (load balancing)

The policy that is used by RNxx load balancer (switching rule)

20.7 Secure profile

The set of the firewall rules that controls network traffic for the certain zone or the user (see user authentication)

20.8 Secure zone

A collection of objects such as: physical ports, subnets, virtual LANs and more .All of the mentioned above objects are regulated by the set of the rules that created for the zone.

20.9 Secure physical zone

The secure zone with the topology that includes ports and subnets.

20.10 Secure virtual zone

The secure zone with the topology that includes ports, subnets and VLANs.

20.11 Subnet

The IPv4 subnet

20.12 VPN

Virtual private network .