WS 2000 Wireless Switch

System Reference
Chapter 3. LAN/Subnet Configuration

Enabling Subnets for the LAN Interface ....................................................... 3-2
Defining Subnets ......................................................................................... 3-2
Configuring Subnets .................................................................................... 3-3
The DHCP Configuration ............................................................................ 3-4
Advanced DHCP Settings ........................................................................... 3-5
Configuring Subnet Access .......................................................................... 3-6
The Access Overview Table ......................................................................... 3-6
The Access Exception Area .......................................................................... 3-6
Advanced Subnet Access Settings ................................................................. 3-8
Virtual LAN (VLAN) Configuration ............................................................... 3-11
Trunking VLANs Through the LAN Port ....................................................... 3-12
Configuring IP Filtering .............................................................................. 3-12

Chapter 4. WAN Configuration

Configuring the WAN Interface ................................................................. 4-2
Configuring WAN IP Information ............................................................... 4-2
Setting Up Point-to-Point over Ethernet (PPPoE) Communication ................. 4-3
Configuring the WS 2000 Firewall ............................................................. 4-5
Disabling the Firewall .................................................................................. 4-5
Setting the NAT Timeout ............................................................................ 4-5
Configurable Firewall Filters ...................................................................... 4-6
Configuring Network Address Translation (NAT) ......................................... 4-7
Configuring Static Routes ............................................................................ 4-10
Configuring the Default Gateway Interface ............................................... 4-10
Creating User Defined Routes .................................................................... 4-11
Setting the RIP Configuration .................................................................... 4-11
Configuring a Virtual Private Network (VPN) ............................................ 4-12
Creating a VPN Tunnel ............................................................................... 4-14
Setting Up VPN Security ............................................................................ 4-14
Configuring Manual Key Exchange ........................................................... 4-15
Setting Up Automatic Key Exchange ......................................................... 4-17
Setting Up Internet Key Exchange (IKE) .................................................... 4-18
VPN: Frequently Asked Questions ............................................................ 4-20
Configuring Content Filtering .................................................................... 4-23
Configuring DynDNS .................................................................................. 4-26
Enabling and Configuring DynDNS .............................................................. 4-26
Updating DynDNS ...................................................................................... 4-26

Chapter 5. Wireless Configuration

Enabling Wireless LANs (WLANs) .............................................................. 5-3
WLAN Summary ........................................................................................ 5-3
AP Adoption Configuration .......................................................................... 5-5
Configuring Wireless LANs ......................................................................... 5-6
Configuring Wireless LAN Security ............................................................ 5-7
Selecting the Authentication Method ............................................................ 5-7
Configuring 802.1x EAP Authentication ....................................................... 5-8
Configuring Kerberos Authentication .......................................................... 5-9
Setting the Encryption Method ................................................................. 5-10
Configuring WEP Encryption .................................................................... 5-10
Configuring WPA/WPA2-TKIP Encryption .................................................. 5-11
Configuring WPA2-CCMP (802.11i) Encryption ......................................... 5-12
KeyGuard ................................................................................................. 5-13
No Encryption ......................................................................................... 5-14
IP Filtering ............................................................................................... 5-14
Mobile Unit Access Control List (ACL) ..................................................... 5-14
Configuring Access Ports ........................................................................... 5-15
Setting Default Access Port Settings .......................................................... 5-18
Common Settings to All Radio Types ......................................................... 5-19
Radio-Specific Settings ............................................................................. 5-21
Advanced Access Port Settings ................................................................. 5-22
Radio Settings ......................................................................................... 5-24
Antenna Settings ..................................................................................... 5-24
Advanced Properties ............................................................................... 5-25
Quality of Service Configuration ............................................................... 5-26
Setting the Bandwidth Share Mode .............................................................. 5-27
Configuring Voice Prioritization and Multicast Address Settings .............. 5-28
Configuring WME Profiles ........................................................................ 5-28
To Add a WME Profile ............................................................................. 5-29
WME Priority Conversion ......................................................................... 5-30
Assigning WME Profiles to WLANs ......................................................... 5-30
Configuring WME Traffic Classification .................................................... 5-31
Setting Up Port Authentication for AP 300 Access Ports ............................. 5-33
Rogue Access Point (Port) Detection ............................................................ 5-33
Setting Up the Detection Method ............................................................... 5-34
Defining and Maintaining Approved AP List Rules .................................... 5-35
Examine the Approve and Rogue Access Ports ........................................ 5-35
Setting SNMP Traps for Rogue APs ............................................................ 5-38
Configuring Wireless Intrusion Protection System (WIPS) ......................... 5-38

Chapter 6. Administrator and User Access

Configuring Administrator Access ............................................................. 6-2
Selecting the Type of Admin Access .......................................................... 6-2
Configuring Secure Shell Connection Parameters ..................................... 6-3
Admin Authentication and RADIUS Server Authentication Setup ............. 6-3
Setting Up AirBEAM Software Access ...................................................... 6-3
Applet Timeout Specification .................................................................... 6-4
Changing the Administrator Password ...................................................... 6-4
Configuring User Authentication ............................................................... 6-4
Configuring the RADIUS Server ............................................................... 6-5
Configuring Lightweight Directory Access Protocol (LDAP) Authentication ................................................................................. 6-7
Setting Up a Proxy RADIUS Server .......................................................... 6-8
Managing the Local User Database ............................................................ 6-9
Setting the User Access Policy ................................................................. 6-10
Managing Digital Certificates ................................................................... 6-12
Chapter 7. Switch Administration

Overview of Administration Support ................................................................. 7-3
Restarting the WS 2000 Wireless Switch .......................................................... 7-3
Changing the Name of the Switch ................................................................. 7-4
Changing the Location and Country Settings of the WS 2000 .................... 7-4
Configuring Switch Redundancy ................................................................. 7-6
  Setting Up Switch Redundancy ............................................................... 7-6
  Redundancy Operations Status .............................................................. 7-7
Updating the WS 2000 Wireless Switch’s Firmware ................................... 7-7
  Checking for and Downloading Firmware Updates ..................................... 7-7
  Performing the Firmware Update ............................................................. 7-8
  Formatting a Compact Flash Card ............................................................ 7-9
  Setting Up DHCP Options for Firmware Upload ...................................... 7-9
Exporting and Importing Wireless Switch Settings .................................. 7-10
  To Import or Export Settings to an FTP or TFTP Site .............................. 7-11
  To Import Settings to a Local File .......................................................... 7-12
  To Export Settings to a Local File ......................................................... 7-12
  Sample Configuration File ........................................................................ 7-12
Configuring SNMP ......................................................................................... 7-20
  Setting the SNMP Version Configuration ................................................ 7-21
  Setting Up the Access Control List .......................................................... 7-22
  Setting the Trap Configuration ............................................................... 7-23
  Setting the Trap Configuration for SNMP v1/v2c .................................... 7-23
  Setting the Trap Configuration for SNMP V3 ........................................ 7-24
  Selecting Traps ......................................................................................... 7-24
  Setting RF Traps ...................................................................................... 7-27
Specifying a Network Time Protocol (NTP) Server .................................. 7-28
Setting Up and Viewing the System Log ................................................. 7-29
  Viewing the Log on the Switch ............................................................. 7-29
  Setting up a Log Server ........................................................................... 7-30

Chapter 8. Configuring HotSpot

Overview ......................................................................................................... 8-2
  Requirements ............................................................................................ 8-2
Configuring Hotspot ..................................................................................... 8-3
  Handling log-in’s and redirection ............................................................. 8-4
  Authentication (RADIUS) ......................................................................... 8-4
  Accounting (RADIUS) ............................................................................ 8-5

Chapter 9. Using DDNS

Overview ......................................................................................................... 9-2
Enabling DDNS .............................................................................................. 9-2
Updating DNS Entries using DDNS ............................................................ 9-4
  Updating DNS Entries for a Single Subnet .............................................. 9-4
Chapter 10. Trunking VLANs Through the WAN Port

Overview ................................................................................................................. 10-2
  Assigning VLAN Tags to Packets ........................................................................... 10-2
Installation Considerations and Default VLAN Settings ........................................... 10-2
Configuring VLAN Trunking .................................................................................... 10-3
  Mapping WLANs to VLANs ................................................................................... 10-4

Chapter 11. Status & Statistics

WAN Statistics ......................................................................................................... 11-2
Subnet Statistics ...................................................................................................... 11-3
  Interfaces .............................................................................................................. 11-5
Wireless LAN Statistics ........................................................................................... 11-6
  Displaying WLAN Summary Information .............................................................. 11-6
  Getting Statistics for a Particular WLAN ............................................................... 11-7
  General WLAN Information .................................................................................. 11-8
Access Port Statistics ............................................................................................... 11-9
  Access Port Statistics Summary Screen ................................................................. 11-9
  Detailed Information About a Particular Access Port ............................................ 11-10
  General Access Port Information .......................................................................... 11-11
Mobile Unit (MU) Statistics .................................................................................... 11-13
View Statistics in Graphic Form .............................................................................. 11-14

Chapter 12. WS 2000 Use Cases

Retail Use Case ....................................................................................................... 12-3
  A Retail Example ................................................................................................... 12-3
The Plan .................................................................................................................... 12-3
Contacting the Wireless Switch ............................................................................... 12-4
  Entering the Basic System Settings ...................................................................... 12-5
  Setting Access Control ......................................................................................... 12-6
  The IP Address Plan ............................................................................................. 12-7
Configuring POS Subnet ......................................................................................... 12-8
Configuring the Printer Subnet .............................................................................. 12-9
Configuring the Cafe Subnet ................................................................................... 12-11
Configuring the WAN Interface .............................................................................. 12-13
Configuring Network Address Translation (NAT) .................................................. 12-14
Inspecting the Firewall ......................................................................................... 12-16
Configuring the Access Ports ................................................................................ 12-16
  Setting Access Port Defaults ................................................................................ 12-17
  Naming the POS Access Port .............................................................................. 12-18
  Configuring the Printer Access Port ..................................................................... 12-19
  Configuring the Cafe Access Port ....................................................................... 12-20
  Associating the Access Ports to the WLANs ...................................................... 12-21
Configuring the Cafe WLAN .................................................................................. 12-22
Configuring the Printer WLAN .............................................................................. 12-24
Configuring the POS WLAN ................................................................................. 12-26
Configuring Subnet Access .................................................................................... 12-29
Configuring the Clients ......................................................................................... 12-31
Chapter 13. Command Line Interface Reference

Admin and Common Commands
- WS2000>admin> admin .................................................. 13-8
- WS2000>admin> help .................................................. 13-9
- WS2000>admin> passwd ............................................. 13-10
- WS2000>admin> quit .................................................. 13-11
- WS2000>admin> save ............................................... 13-12
- WS2000>admin> summary ......................................... 13-13
- WS2000>admin> / .................................................... 13-16
- WS2000>admin> .. .................................................. 13-17

Network Commands
- WS2000>admin> network ......................................... 13-18

Network AP Commands
- WS2000>admin(network.ap)> ap .............................. 13-19
- WS2000>admin(network.ap)> add ................................ 13-20
- WS2000>admin(network.ap)> copydefaults .................. 13-21
- WS2000>admin(network.ap)> delete ......................... 13-22
- WS2000>admin(network.ap)> list ......................... 13-23
- WS2000>admin(network.ap)> reset ....................... 13-24
- WS2000>admin(network.ap)> set .......................... 13-25
- WS2000>admin(network.ap)> show ..................... 13-27

Network AP Default Commands
- WS2000>admin(network.ap)> default ...................... 13-29
- WS2000>admin(network.ap.default)> set ............... 13-30
Network AP Test Commands .................................................. 13-33
WS2000>admin(network.ap.default)> show ................................13-32
WS2000>admin(network.ap)> test ............................................ 13-33
WS2000>admin/network.ap.test)> new ...................................... 13-34
Network DHCP Commands .................................................... 13-35
WS2000>admin(network.dhcp)> show ........................................ 13-37
WS2000>admin/network.dhcp)> set ........................................... 13-36
Network Firewall Commands ............................................... 13-38
WS2000>admin(network)> fw .................................................. 13-38
WS2000>admin/network.fw)> set .............................................. 13-39
WS2000>admin/network.fw)> show .......................................... 13-41
Network Firewall Policy Commands ..................................... 13-42
WS2000>admin/network.fw)> policy ......................................... 13-42
WS2000>admin/network.fw.policy)> import ............................. 13-43
Network Firewall Policy Inbound Commands ......................... 13-44
WS2000>admin/network.fw.policy.inb)> set ............................... 13-45
WS2000>admin/network.fw.policy.inb)> move ........................... 13-49
WS2000>admin/network.fw.policy.inb)> list .............................. 13-48
WS2000>admin/network.fw.policy.inb)> insert .......................... 13-47
WS2000>admin/network.fw.policy.inb)> delete ........................ 13-46
Network Firewall Policy Outbound Commands ....................... 13-51
WS2000>admin/network.fw.policy.outb)> set ............................. 13-57
WS2000>admin/network.fw.policy.outb)> list ........................... 13-55
WS2000>admin/network.fw.policy.outb)> insert ......................... 13-54
WS2000>admin/network.fw.policy.outb)> move ......................... 13-56
WS2000>admin/network.fw.policy.outb)> delete ........................ 13-53
Network Firewall Submap Commands .................................. 13-58
WS2000>admin/network.fw.submap)> show .............................. 13-63
WS2000>admin/network.fw.submap)> list ................................. 13-61
WS2000>admin/network.fw.submap)> delete ............................ 13-60
Network LAN Commands ...................................................... 13-64
WS2000>admin/network.lan)> lan ............................................ 13-64
Network LAN DHCP Commands ........................................... 13-67
WS2000>admin/network.lan.dhcp)> set ................................... 13-71
Network QoS Commands .................................................. 13-73

WS2000>admin(network)> qos ........................................ 13-73
WS2000>admin(network.qos)> clear ................................. 13-74
WS2000>admin(network.qos)> set .................................. 13-75
WS2000>admin(network.qos)> show ............................... 13-76

Network Router Commands ........................................... 13-77

WS2000>admin(network)> router .................................... 13-77
WS2000>admin(network.router)> add ............................ 13-78
WS2000>admin(network.router)> delete ......................... 13-79
WS2000>admin(network.router)> list ........................... 13-80
WS2000>admin(network.router)> set ........................... 13-81
WS2000>admin(network.router)> show ......................... 13-82

Network VLAN Commands ........................................... 13-83

WS2000>admin(network)> vlan ...................................... 13-83
WS2000>admin(network.vlan)> set ............................... 13-84
WS2000>admin(network.vlan)> show ............................ 13-85

Network VLAN Trunk Commands .................................... 13-86

WS2000>admin(network.vlan)> trunk ............................. 13-86
WS2000>admin(network.vlan.trunk)> clear ................. 13-87
WS2000>admin(network.vlan.trunk)> set .................... 13-88
WS2000>admin(network.vlan.trunk)> show ................ 13-89

Network WAN Commands ........................................... 13-90

WS2000>admin(network)> wan ...................................... 13-90
WS2000>admin(network.wan)> renew ......................... 13-91
WS2000>admin(network.wan)> set ........................... 13-92
WS2000>admin(network.wan)> show ......................... 13-93

Network WAN App Commands ....................................... 13-94

WS2000>admin(network.wan)> app .............................. 13-94
WS2000>admin(network.wan.app)> addcmd .................. 13-95
WS2000>admin(network.wan.app)> delcmd ................. 13-97
WS2000>admin(network.wan.app)> list ...................... 13-99

Network WAN NAT Commands ..................................... 13-100

WS2000>admin(network.wan)> nat .............................. 13-100
WS2000>admin(network.wan.nat)> add ...................... 13-101
WS2000>admin(network.wan.nat)> delete .................. 13-102
WS2000>admin(network.wan.nat)> list ...................... 13-103
WS2000>admin(network.wan.nat)> set ...................... 13-104
WS2000>admin(network.wan.nat)> show ................ 13-105

Network WAN VPN Commands ..................................... 13-106

WS2000>admin(network.wan)> vpn ............................. 13-106
WS2000>admin(network.wan.vpn)> add ...................... 13-107
WS2000>admin(network.wan.vpn)> delete .................. 13-108
WS2000>admin(network.wan.vpn)> ikestate ................. 13-109
WS2000>admin(network.wan.vpn)> list ...................... 13-110
WS2000>admin(network.wan.vpn)> reset .................... 13-111
WS2000>admin(network.wan.vpn)> set ...................... 13-112
WS2000>admin(network.wan.vpn)> stats .................... 13-116
Network WAN VPN Cmgr Commands ................................................................. 13-117
  WS2000>admin(network.wan.vn)> cmgr .................................................. 13-117
  WS2000>admin(network.wan.vn.cmgr)> delca ....................................... 13-118
  WS2000>admin(network.wan.vn.cmgr)> delprivkey ................................ 13-119
  WS2000>admin(network.wan.vn.cmgr)> delself ..................................... 13-120
  WS2000>admin(network.wan.vn.cmgr)> expcert .................................. 13-121
  WS2000>admin(network.wan.vn.cmgr)> genreq .................................... 13-122
  WS2000>admin(network.wan.vn.cmgr)> impcert ................................... 13-123
  WS2000>admin(network.wan.vn.cmgr)> listca .................................... 13-124
  WS2000>admin(network.wan.vn.cmgr)> listprivkey ................................ 13-125
  WS2000>admin(network.wan.vn.cmgr)> listself ................................... 13-126
  WS2000>admin(network.wan.vn.cmgr)> loadca .................................... 13-127
  WS2000>admin(network.wan.vn.cmgr)> loadself .................................. 13-128
  WS2000>admin(network.wan.vn.cmgr)> showreq ................................... 13-129

Network WLAN Commands ................................................................. 13-130
  WS2000>admin(network.wlan)> wlan ................................................... 13-130
  WS2000>admin(network.wlan)> add ...................................................... 13-131
  WS2000>admin(network.wlan)> del ...................................................... 13-132
  WS2000>admin(network.wlan)> list ..................................................... 13-133
  WS2000>admin(network.wlan)> set ...................................................... 13-134
  WS2000>admin(network.wlan)> show .................................................... 13-138

Network WLAN Rogue AP Commands ...................................................... 13-140
  WS2000>admin(network.wlan.rogueap)> set ......................................... 13-140
  WS2000>admin(network.wlan.rogueap)> show ..................................... 13-142

Network WLAN Rogue AP Approved AP List Commands .................................. 13-143
  WS2000>admin(network.wlan.rogueap.approvedlist)> approve .................... 13-145
  WS2000>admin(network.wlan.rogueap.approvedlist)> ageout .................... 13-144
  WS2000>admin(network.wlan.rogueap.approvedlist)> erase ..................... 13-146
  WS2000>admin(network.wlan.rogueap.approvedlist)> show ...................... 13-147

Network WLAN Rogue AP List Commands .................................................. 13-148
  WS2000>admin(network.wlan.rogueap)> roguelist ................................ 13-148
  WS2000>admin(network.wlan.rogueap.roguelist)> ageout ....................... 13-149
  WS2000>admin(network.wlan.rogueap.roguelist)> approve ...................... 13-150
  WS2000>admin(network.wlan.rogueap.roguelist)> erase ....................... 13-151
  WS2000>admin(network.wlan.rogueap.roguelist)> show ......................... 13-152

Network WLAN Rogue AP Locate Commands ............................................. 13-153
  WS2000>admin(network.wlan.rogueap.roguelist)> locate ......................... 13-153
  WS2000>admin(network.wlan.rogueap.roguelist.locate)> list .................. 13-154
  WS2000>admin(network.wlan.rogueap.roguelist.locate)> start ................ 13-155

Network WLAN Rogue AP MU Scan Commands ......................................... 13-156
  WS2000>admin(network.wlan.rogueap.roguelist.muscan)> muscan ................. 13-156
  WS2000>admin(network.wlan.rogueap.roguelist.muscan)> list .................. 13-157
  WS2000>admin(network.wlan.rogueap.roguelist.muscan)> start ................ 13-158

Network WLAN Rogue AP Rule List Commands ........................................ 13-159
  WS2000>admin(network.wlan.rogueap.rulelist)> rulelist ......................... 13-159
  WS2000>admin(network.wlan.rogueap.rulelist)> add ................................ 13-160
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS2000&gt;admin(system.authentication)&gt; authsymbolap</td>
<td>13-161</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.rogaueap.rulelist)&gt; delete</td>
<td>13-162</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.rogaueap.rulelist)&gt; show</td>
<td>13-163</td>
</tr>
<tr>
<td>Statistics Commands</td>
<td>13-164</td>
</tr>
<tr>
<td>WS2000&gt;admin(stats)&gt; show</td>
<td>13-164</td>
</tr>
<tr>
<td>WS2000&gt;admin(stats)&gt; send</td>
<td>13-165</td>
</tr>
<tr>
<td>Statistics RF Commands</td>
<td>13-167</td>
</tr>
<tr>
<td>WS2000&gt;admin(stats.rf)&gt; reset</td>
<td>13-167</td>
</tr>
<tr>
<td>WS2000&gt;admin(stats.rf)&gt; show</td>
<td>13-169</td>
</tr>
<tr>
<td>System Commands</td>
<td>13-172</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; system</td>
<td>13-172</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; lastpw</td>
<td>13-173</td>
</tr>
<tr>
<td>System Authentication Commands</td>
<td>13-174</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; authentication</td>
<td>13-174</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.authentication)&gt; set</td>
<td>13-175</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.authentication)&gt; show</td>
<td>13-176</td>
</tr>
<tr>
<td>System Authentication RADIUS Commands</td>
<td>13-177</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.authentication)&gt; radius</td>
<td>13-177</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.authentication.radius)&gt; set</td>
<td>13-178</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.authentication.radius)&gt; show</td>
<td>13-179</td>
</tr>
<tr>
<td>System Configuration Commands</td>
<td>13-180</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; config</td>
<td>13-180</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; default</td>
<td>13-181</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; export</td>
<td>13-182</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; import</td>
<td>13-184</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; partial</td>
<td>13-185</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; set</td>
<td>13-186</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; show</td>
<td>13-187</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; update</td>
<td>13-188</td>
</tr>
<tr>
<td>System Logs Commands</td>
<td>13-189</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; logs</td>
<td>13-189</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.logs)&gt; delete</td>
<td>13-190</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.logs)&gt; send</td>
<td>13-191</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.logs)&gt; set</td>
<td>13-192</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.logs)&gt; show</td>
<td>13-193</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.logs)&gt; view</td>
<td>13-194</td>
</tr>
<tr>
<td>System NTP Commands</td>
<td>13-195</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; ntp</td>
<td>13-195</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.ntp)&gt; set</td>
<td>13-196</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.ntp)&gt; show</td>
<td>13-197</td>
</tr>
<tr>
<td>System RADIUS Commands</td>
<td>13-198</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; radius</td>
<td>13-198</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.radius)&gt; set</td>
<td>13-199</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.radius)&gt; show</td>
<td>13-200</td>
</tr>
<tr>
<td>System RADIUS Client Commands</td>
<td>13-201</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.radius)&gt; client</td>
<td>13-201</td>
</tr>
</tbody>
</table>
WS2000>admin(system.snmp.traps)> set ................................. 13-242
WS2000>admin(system.snmp.traps)> show ............................... 13-245

System SSH Commands ..................................................... 13-248
WS2000>admin(system)> ssh .............................................. 13-248
WS2000>admin(system.ssh)> set ........................................ 13-249
WS2000>admin(system.ssh)> show ...................................... 13-250

System User Database Commands ....................................... 13-251
WS2000>admin(system)> userdb ........................................ 13-251

System User Database Group Commands ................................. 13-252
WS2000>admin(system.userdb)> group ................................ 13-252
WS2000>admin(system.userdb.group)> add ............................. 13-253
WS2000>admin(system.userdb.group)> create ......................... 13-254
WS2000>admin(system.userdb.group)> delete ......................... 13-255
WS2000>admin(system.userdb.group)> remove ....................... 13-256
WS2000>admin(system.userdb.group)> show ......................... 13-257

System User Database User Commands ................................ 13-258
WS2000>admin(system.userdb)> user .................................. 13-258
WS2000>admin(system.userdb.user)> add ............................. 13-259
WS2000>admin(system.userdb.user)> del ............................. 13-260
WS2000>admin(system.userdb.user)> set ............................. 13-261
WS2000>admin(system.userdb.user)> show ......................... 13-262

System WS2000 Commands .................................................. 13-263
WS2000>admin(system)> ws2000) ...................................... 13-263
WS2000>admin(system.ws2000)> restart ............................. 13-264
WS2000>admin(system.ws2000)> set .................................. 13-265
WS2000>admin(system.ws2000)> show ............................... 13-267

Chapter A. Appendix A: Syslog Messages

Informational Log Entries .................................................. A-2
Notice Log Entries .......................................................... A-4
Warning Log Entries ....................................................... A-6
Alert Log Entry ............................................................. A-9
Error-Level Log Entries ................................................... A-9
Debug-Level Log Entries ................................................. A-22
Emergency Log Entries ................................................... A-26
This guide is intended to support administrators responsible for understanding, configuring and maintaining the Wireless Switch. This document provides information for the system administrator to use during the initial setup and configuration of the system. It also serves as a reference guide for the administrator to use while updating or maintaining the system.

**About this Document**

We recommend viewing this online system reference guide with Internet Explorer 5.0 and higher or Netscape Navigator 4.7 or higher on a Microsoft Windows based PC. Viewing this document under other configurations may produce undesirable results.

**Document Conventions**

- **Notes**: Notes are displayed in blue text and indicate a tip or requirement.

- **GUI Screen Text**: Indicates monitor screen dialog/output from the graphical user interface accessed from any web browser on the network.
System Overview

The WS 2000 Wireless Switch provides a low-cost, feature-rich option for sites with one to six Access Ports. The WS 2000 Wireless Switch works at the center of a network’s infrastructure to seamlessly and securely combine wireless LANs (WLANs) and wired networks. The switch sits on the network. Wireless Access Ports connect to one of the six available ports on the switch and the external wired network (WAN) connects to a single 10/100 Mbit/sec. WAN port.

Mobile units (MUs) associate with the switch via an Access Port. When an MU contacts the switch, the switch cell controller services attempt to authenticate the device for access to the network.

The WS 2000 Wireless Switch acts as a WAN/LAN gateway and a wired/wireless switch.

Management of Access Ports

This wireless switch provides six 10/100 Mbit/sec. LAN ports for internal wired or wireless traffic. Four of these ports provide IEEE 802.3af-compliant Power over Ethernet (PoE) support for devices that require power from the Ethernet connection (such as Access Ports). Administrators can configure the six ports to communicate with a private LAN or with an Access Port for a wireless LAN (WLAN). The switch provides up to four extended service set identifiers (ESSIDs) for each Access Port connected to the switch.

Firewall Security

The LAN and Access Ports are placed behind a user-configurable firewall that provides stateful packet inspection. The wireless switch performs network address translation (NAT) on packets passing to and from the WAN port. This combination provides enhanced security by monitoring communication with the wired network.

Wireless LAN (WLAN) Security

Administrators can configure security settings independently for each ESSID. Security settings and protocols available with this switch include:

- Kerberos
- WEP-64
- WEP-128
- 802.1x with RADIUS
- 802.1x with Shared Key
- KeyGuard
- WPA/WPA2-TKIP
- WPA2/CCMP (802.11i)

VPN Security

Virtual Private Networks (VPNs) are IP-based networks that use encryption and tunneling to give users remote access to a secure LAN. In essence, the trust relationship is extended from one LAN across the public network to another LAN, without sacrificing security. A VPN behaves similarly to a private network; however, because the data travels through the public network, it needs several layers of security. The WS 2000 Wireless Switch acts as a robust VPN gateway.
Hardware Overview

The WS 2000 Wireless Switch provides a fully integrated solution for managing every aspect of connecting wireless LANs (WLANs) to a wired network. This wireless switch can connect directly to a cable or DSL modem, and can also connect to other wide area networks through a Layer 2/3 device (such as a switch or router). The switch includes the following features:

- One WAN (RJ-45) port for connection to a DSL modem, cable modem, or any other Layer 2/3 network device.
- Six 10/100 Mbit/sec. LAN (RJ-45) ports: four ports provide 802.3af “Power over Ethernet” (PoE) support; the other two do not provide power.
- Each port has two LEDs, one indicating the speed of the transmission (10 or 100 Mbit/sec.), the other indicating whether there is activity on the port. The four LAN ports with PoE have a third LED that indicates whether power is being delivered over the line to a power device (such as an Access Port). (See the WS 2000 Wireless Switch LED explanation for more information on the meaning of the different state of the LEDs.)
- A DB-9 serial port for direct access to the command-line interface from a PC. Use Symbol’s Null-Modem cable (Part No. 25-632878-0) for the best fitting connection.
- A CompactFlash slot that provides AirBEAM® support.

Technical Specifications

Physical Specifications

- Width: 203 mm
- Height: 38 mm
- Depth: 286 mm
- Weight: 0.64 kg

Power Specifications

- Maximum Power Consumption: 90-256 VAC, 47-63 Hz, 3A
- Operating Voltage: 48 VDC
- Operating Current: 1A
- Peak Current: 1.6A

Environmental Specifications

- Operating Temperature: 0°C to 40°C
- Storage Temperature: -40°C to 70°C
- Operating Humidity: 10% to 85% Non-condensing
- Storage Humidity: 10% to 85% Non-condensing
- Operating Altitude: 2.4 km
- Storage Altitude: 4.6 km
**WS 2000 Wireless Switch LED Functions**

The switch has a large blue LED on the right front that indicates that the switch is powered on.

Each port on the WS 2000 Wireless Switch has either two or three LEDs that indicate the status of the port. Ports 1-4, which supply 802.3af Power over Ethernet (PoE), have three LEDs. The remaining two non-powered LAN ports and the WAN port have two LEDs.

<table>
<thead>
<tr>
<th>Location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upper left LED</td>
<td>This LED is present on all ports and indicates the speed of the transmissions through the port. The LED is on when the transmission rate is 100 Mbit per second (100BaseT). The light is off when the transmission rate is 10 Mbit per second.</td>
</tr>
<tr>
<td>Upper right LED</td>
<td>This LED indicates activity on the port. This light is solid yellow when a link to a device is made. The light flashes when traffic is being transferred over the line.</td>
</tr>
</tbody>
</table>
| Lower LED      | This LED is only present on Ports 1-4. These ports provide 802.3af Power over Ethernet (PoE) support to devices (such as Access Ports). The LED has several states:  
OFF—A non-power device (or no device) is connected; no power is being delivered.  
GREEN—The switch is delivering 48 volts to the power device connected to that port.  
RED—There was a valid PoE connection; however, the switch has detected that the power device is faulty. The red light will remain until a non-faulty connection is made to the port. |
**Software Overview**

The WS 2000 Wireless Switch software provides a fully integrated solution for managing every aspect of connecting Wireless LANs (WLANs) to a wired network, and includes the following components:

**Operating System (OS) Services**

Operating System (OS) Services determine how the WS 2000 Wireless Switch communicates with existing network and operating system-centric software services, including:

- Dynamic Host Configuration Protocol (DHCP)
- Telnet and File Transfer Protocol (FTP/TFTP) servers
- The Simple Network Time Protocol (SNTP) client, used to keep switch time synchronized for Kerberos authentication
- A mechanism for setting up a redundant (secondary) switch that takes over if the primary switch fails

**Cell Controller Services**

The Cell Controller provides the ongoing communication between mobile units (MUs) on the Wireless LAN (WLAN) and the wired network. Cell Controller services perform the following:

- Initialize the Access Ports
- Maintain contact with Access Ports by sending a synchronized electronic “heartbeat” at regular intervals
- Track MUs when they roam from one location to another
- Manage security schemes based on system configuration
- Maintain system statistics
- Store policies and Access Port information
- Detect and manage rogue Access Ports
- Management of communications QoS

**Gateway Services**

Gateway services provide interconnectivity between the Cell Controller and the wired network, and include the following:

- System management through a Web-based Graphical User Interface (GUI) and SNMP
- 802.1x RADIUS client
- Security, including Secure Sockets Layer (SSL) and Firewall
- Network Address Translation (NAT), DHCP services, and Layer 3 Routing
- Virtual Private Network (VPN)
Getting Started with the WS 2000 Wireless Switch ......................................................... 2-2
Enable Subnet1 .................................................................................................................. 2-5
Communicating with the Outside World ......................................................................... 2-7
Setting Up Point-to-Point over Ethernet (PPPoE) Communication ................................. 2-8
Wireless Summary Area ...................................................................................................... 2-9
Setting the Authentication Method ...................................................................................... 2-10
Setting the Encryption Method ........................................................................................... 2-10
Mobile Unit Access Control List (ACL) ............................................................................ 2-11
Where to Go from Here? ...................................................................................................... 2-12
Getting Started with the WS 2000 Wireless Switch

This section provides just enough instruction to set up the WS 2000 Wireless Switch, connect an Access Port, and test communications with a single mobile unit (MU) and the wide area network (WAN). The configuration suggestions made here are just the minimum needed to test the hardware. Once finished with this section, additional configuration settings are required. This section covers the following topics:

- Step 1: Install the switch and connect it to the WAN, a standalone computer, and an Access Port
- Step 2: Set up administrative communication to the switch
- Step 3: Set the basic switch settings
- Step 4: Configure the LAN interface
- Step 5: Configure Subnet1
- Step 6: Configure the WAN Interface
- Step 7: Enable Wireless LANs (WLANs)
- Step 8: Configure WLAN Security
- Step 9: Test Connectivity

Step 1: Install the Switch

To install the WS 2000 Wireless Switch hardware, follow the directions in the WS 2000 Wireless Switch Quick Installation Guide found in the box with the switch and on the CD-ROM that is distributed with the switch. These instructions describe how to:

- Select a site (desk, wall, or rack) for the switch
- Install the switch using the appropriate accessories for the selected location
- Connect devices to WAN and LAN ports (using standard CAT-5 cables)
- Interpret the port LEDs on the front of the switch

After the switch is mounted and powered up, connect the following items to the switch:

1. Connect the WAN to the switch (using the WAN port) with a CAT-5 Ethernet cable. The LEDs for that port should start to flash.
2. Connect an Access Port to the switch using a CAT-5 Ethernet cable using one of the six LAN ports. If the Access Port requires PPPoE, connect the Access Port in ports 1, 2, 3, or 4. Ports 5 and 6 do not provide power.
3. Have a mobile “wireless” device available to test communication with the Access Port.

Access Ports must be connected to the LAN ports of the wireless switch to enable configuration of the Access Port related settings.

Step 2: Set Up Administrative Communication to the Switch

Before the configuration process can begin, establish a link with the wireless switch.

1. Connect a “wired” computer to the switch (in any one of the available LAN ports) using a standard CAT-5 cable.
2. Set up the computer for TCP/IP DHCP network addressing and make sure that the DNS settings are not hardcoded.
3. Start up Internet Explorer (with Sun Microsystems’ Java Runtime Environment (JRE) 1.4 or higher installed) and type the following IP address in the address field: 192.168.0.1

For optimum compatibility use Sun Microsystems’ JRE 1.4 or higher (available from Sun’s website), and be sure to disable Microsoft’s Java Virtual Machine if it is installed.

The following screen is displayed.
4. Log in using “admin” as the User ID and “symbol” as the Password.
5. If the login is successful, the following dialog window is displayed.

Enter a new admin password in both fields, and click the **Update Password Now** button. When the admin password has been updated, the System Settings screen is displayed.
Step 3: Set the Basic Switch Setting

1. Enter a **System Name** for the wireless switch. The specified name appears in the lower-left corner of the configuration screens, beneath the navigation tree. This name can be a useful reminder if multiple Symbol wireless switches are being administered.

2. Enter a text description of the location of the switch in the **System Location** field. This text is used as a reminder to the network administrator and is also used to set the location variable if the switch is administered using SNMP.

3. Enter an email address for the administrator in the **Admin Email Address** field. The switch uses this address for sending SNMP-related and other administration-related messages to the administrator.

4. Select the **Country** for the switch from the drop-down menu. Selecting the correct country is extremely important. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted by Access Ports. To ensure compliance with national and local laws, be sure to set this field accurately.

5. Click **Apply** to save changes. Unapplied changes are lost if the administrator navigates to a different screen.

---

**Note**

The WS 2000 switch is shipped with an open default SNMP configuration:

- **Community**: public, **OID**: 1.3.6.1, **Access**: Read-only
- **Community**: private, **OID**: 1.3.6.1, **Access**: Read-write

If your switch has these settings, it is important to change them immediately; otherwise, users on the same network will have read-write access to the switch through the SNMP interface. Select System Configuration --> SNMP Access from the left menu to examine the settings and change them, if necessary.
Step 4: Configure the LAN Interface

The first step of network configuration process is to figure out the topology of the LAN. The WS 2000 Wireless Switch allows the administrator to enable and configure four different subnets. The administrator can assign an IP address, port associations, and DHCP settings for each subnet.

**Enable Subnet1**

Select LAN under the Network Configuration group from the left menu. Use the LAN configuration screen to view a summary of physical-port addresses and wireless LANs (WLANs) associated with the four supported subnets, and to enable or disable each configured subnet.

1. In the LAN screen, the administrator can enable up to four subnets. Make sure that the checkbox to the left of the Subnet1 line is enabled.

   Each enabled subnet shows up in the directory tree in the left column of the configuration screens. Consider disabling a previously configured subnet if its assigned ports are no longer in use, or to consolidate the LAN’s communications on fewer subnets.

The rest of the information on this screen is summary information; it is collected from other screens (such as the subnet configuration screens) where the administrator can set the data.

| **Network** | Network (subnet) name is a descriptive string that should describe the subnet's function. The WS 2000 Network Management System uses subnet names throughout the configurations screens. |
| **Address** | This IP address allows users from outside the subnet (whether from the WAN or from another subnet from the same switch) to access the right subnet. An IP address uses a series of four numbers that are expressed in dot notation, for example, 194.182.1.1. |
| **Interfaces** | The Interfaces field displays which of the six physical LAN ports are associated with the subnet. The possible ports are: P1 (port 1), P2, P3, P4, P5, and P6 (from left to right facing the front of the switch). The administrator assigns a port to a subnet to enable access to the device(s) connected to that port. The administrator can assign a port to only one subnet. The Interfaces field also lists the WLANs that are associated with the subnet. |
Step 5: Configure Subnet1

The WS 2000 Network Management System allows the administrator to define and refine the configuration of the enabled subnets. Each of four subnets (short for “subnetworks”) can be configured as an identifiably separate part of the switch-managed local area network (LAN). Each subnet can include some combination of assigned ports and associated wireless LANs (WLANs).

1. Select Network Configuration --> LAN --> Subnet1 from the list on the left. The following screen appears for the selected subnet.

2. Check to make sure that all the ports and WLAN1 are selected for this subnet. WLAN1 should automatically be included if the switch and the Access Port are communicating properly. If WLAN1 is not present in the list, check the following:
   - The power to the Access Port
   - The connections between the switch and the Access Port
   - The LEDs to make sure that lights are on and flashing

3. For this initial configuration, ensure that This interface is a DHCP Server is enabled. If so, the switch sets the IP addresses automatically for the mobile devices. This value can be changed at any time in the future. All other default settings are fine for the system test.

   DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. The switch includes internal DHCP server and client features, and the subnet’s interface can use either capability.

4. Click the Apply button to save changes.

Step 6: Configure the WAN Interface

A wide area network (WAN) is a widely dispersed telecommunications network. In a corporate environment, the WAN port might connect to a larger corporate network. For a small business, the WAN port might connect to a DSL or cable modem to access the Internet.
The WS 2000 Wireless Switch includes one WAN port. In order to set up communications with the outside world, select **Network Configuration --> WAN** from the left menu. The following WAN configuration page appears.

![WAN Configuration Page](image)

**Communicating with the Outside World**

1. Click the **Enable WAN Interface** checkbox to enable a connection between the switch and a larger network or the outside world through the WAN port.

2. If this switch should be a DHCP client (get its IP address automatically from another server or switch), check the **This interface is a DHCP Client** checkbox. If **This interface is DHCP Client** is checked, the switch is limited to one WAN IP address. This choice is required when:
   - The host router or switch on the WAN is communicating with the WS 2000 Wireless Switch using DHCP.
   - The switch is interfacing with an Internet Service Provider (ISP) that uses DHCP addressing.

   **This setting is independent from the DHCP settings for the switch’s internal subnets.**

3. If **This interface is DHCP Client** is not checked, fill in the information in this area. To find out the information to enter into these fields, contact the network administrator or the ISP that provided the cable modem or DSL router. All the fields below take standard IP addresses of the form xxx.xxx.xxx.xxx.
   - The **IP Address** refers to the IP address that the outside world uses to address the WS 2000 Wireless Switch.
   - Click the **More IP Addresses** button to specify additional static IP addresses for the switch. Additional IP addresses are required when users within the LAN need dedicated IP addresses, or when servers in the LAN need to be accessed (addressed) by the outside world. The pop-up window allows the administrator to enter up to eight WAN IP addresses for the switch.
   - The **Subnet Mask** is the mask used for the WAN.
   - The **Default Gateway** is the address of the device that provides the connection to the WAN (often a cable modem or DSL router).
The two DNS Server fields specify DNS addresses of servers that can translate domain names, such as www.symbol.com, into IP addresses that the network uses when passing information. The Secondary DNS Server acts as a backup to the Primary DNS Server when the primary server is not responding.

Setting Up Point-to-Point over Ethernet (PPPoE) Communication

PPPoE provides the ability to connect a network of hosts through a simple device to a remote access concentrator. Many DSL providers require that their clients communicate using this protocol. The facility allows the ISP to control access, billing, and type of service provided to clients on a per-user or per-site basis. Check with the network administrator or ISP to determine whether to enable this feature, and, if so, find out the username and password required for authentication.

1. Check Enable in the PPP over Ethernet area to enable the PPPoE protocol for high-speed connections.
2. Enter the Username and Password required for authentication. The username and password are for the switch’s router to use when connecting to the ISP. When the Internet session starts, the ISP authenticates the username.
3. Set the Idle Time to an appropriate number. This number is the amount of time the PPPoE connection will be idle before it disconnects. The 10000 second (default idle time is appropriate for most situations).
4. Check Keep Alive to instruct the switch to continue occasional communications over the WAN even when client communications to the WAN are idle. Some ISPs terminate inactive connections, while others do not. In either case, enabling Keep-Alive mode keeps the switch’s WAN connection alive, even when there is no traffic. If the ISP drops the connection after so much idle time, the switch automatically reestablishes the connection to the ISP.
5. Select the appropriate WAN authentication method from the drop-down menu. Collect this information from the network administrator. Select between None, PAP, CHAP, or PAP or CHAP.

6. Click the Apply button to save changes.

Step 7: Enable Wireless LANs (WLANs)

The WS 2000 Wireless Switch works either in a wired or wireless environment; however, the power of the switch is associated with its support of wireless networks. In order to use the wireless features of the switch, the administrator needs to enable up to four wireless LANs (WLANs).

To start the WLAN configuration process, select the Network Configuration --> Wireless item from the left menu. The following Wireless summary screen appears.
Wireless Summary Area

The top portion of the window displays a summary of the WLANs that are currently defined. This is the screen in which the administrator can enable or disable a WLAN. At first, eight WLANs are listed: WLAN1, WLAN2, WLAN3, WLAN4, WLAN5, WLAN6, WLAN7, and WLAN8; however, only WLAN1 is enabled.

1. Verify that WLAN1 is enabled (checked) and associated with Subnet1.
2. Verify that Access Port 1 is shown in the Access Ports Adopted field to the right. If it is not, verify the connection between the switch and the Access Port.

The current settings for the associated Subnet and adopted Access Ports are displayed on this screen; however, the screen associated with each WLAN (under Network Configuration --> Wireless) is where the settings and rules for adopting Access Ports can be modified.

Use the AP Adoption Configuration tab to assign Access Ports to a particular WLAN. The switch can adopt up to six Access Ports at a time, but the list of allowed Access Port addresses (displayed in this area) can exceed six in number. A dual-radio 802.11a/b Access Port counts as one Access Port with respect to the maximum allowed; however, each radio is listed as a separate Access Port.

This adoption list identifies each Access Port by its Media Access Control (MAC) address. This address is the Access Port's hard-coded hardware number that is printed on the bottom of the device. An example of a MAC address is 00:09:5B:45:9B:07.

The default setting associates all adopted Access Ports with WLAN1.

Step 8: Configure WLAN Security

In the previous step, the administrator set parameters for each WLAN that fine tune the performance of the WLAN. In addition, the administrator can set the type and level of security for each WLAN. These security measures do not control communications from the WAN; instead, they control communication from the clients within the WLAN.
In the Network Configuration --> Wireless --> <WLAN name> --> <WLAN Name> --> Security screen, the administrator can set the user authentication method and the encryption method, as well as define a set of rules that control which MUs can communicate through the WLAN.

### Setting the Authentication Method

The authentication method sets a challenge-response procedure for validating user credentials such as username, password, and sometimes secret-key information. The WS 2000 Wireless Switch provides two methods for authenticating users: 802.1x EAP and Kerberos. The administrator can select between these two methods. For testing connectivity, WLAN security is not an issue, so there is not reason to enable authentication—the default setting (No Authentication) is sufficient.

### Setting the Encryption Method

Encryption applies a specific algorithm to data to alter its appearance and prevent unauthorized reading. Decryption applies the algorithm in reverse to restore the data to its original form. Sender and receiver employ the same encryption/decryption method.

Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN. WEP might be all that a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. An unauthorized person with a sniffing tool can monitor a network for less than a day and decode its encrypted messages.

For the connectivity test, set WEP 128 encryption. This ensures that communications with the switch are secure enough for this stage. Later on, increasing the security level might be necessary.

1. Select the WEP 128 (104-bit key) option.
2. To use WEP encryption with the No Authentication selection, click the WEP Key Settings button to display a sub-screen for entering keys.
3. Add a key to Key #1, and use that key with the mobile unit. The keys consist of 26 hexadecimal (0-9, A-E) characters. When finished, click the Ok button to close this screen an return to the WLAN Security screen.

4. Click the Apply button in the WLAN Security screen to save changes.

**Mobile Unit Access Control List (ACL)**

This list is used to specify which mobile units can or cannot gain access to the WLAN. The list employs an adoption rule for allowing or denying specific mobile units by way of exception. By default, all mobile units can gain access.

**Step 9: Test Connectivity**

At this point, the switch is set up to allow mobile units to access the LAN.

1. Go to the mobile unit and ensure that it is set up as a DHCP client.
2. Set the mobile unit for WEP 128 encryption and set the same key as the one that was entered in the WEP Key Settings dialog. It may be necessary to reboot the mobile unit after changing the settings.
3. Open a Web browser and type the IP address: 192.168.0.1. The WS 2000 Switch Management screen should appear. If not, go back to the wired system used to configure the switch and see if the mobile device appears in the MU Stats screen (**Status & Statistics** -> **MU Stats**). If it does not appear on the MU Stats screen, recheck the network and WEP settings on the mobile device.
4. In the Web browser, enter a URL for a site (such as www.symbol.com) on the WAN. If the site does not appear, go to the WAN Stats screen (**Status & Statistics** -> **WAN Stats**) to review the status of the WAN connection.
Where to Go from Here?

When full connectivity has been verified, the switch can be fully configured to meet the needs of the organization. Refer to the two case studies provided with this reference for specific installation examples. These case studies describe the environment, the desired features, and the configuration selections that were made in two different scenarios.

- Case 1: Retail Use Case
  (with handheld terminals, wireless printers, wired POS, secured access to in-store server, and public access to WAN)

- Case 2: Field Office Use Case
  (with 3 WAN IP addresses, VPN passthrough, RADIUS server, and full-access between subnets)
LAN/Subnet Configuration

Enabling Subnets for the LAN Interface .................................................. 3-2
Defining Subnets .................................................................................. 3-2
Configuring Subnets ............................................................................. 3-3
The DHCP Configuration ..................................................................... 3-4
Advanced DHCP Settings .................................................................... 3-5
Configuring Subnet Access .................................................................... 3-6
The Access Overview Table ..................................................................... 3-6
The Access Exception Area ..................................................................... 3-6
Advanced Subnet Access Settings .......................................................... 3-8
Virtual LAN (VLAN) Configuration ......................................................... 3-11
Trunking VLANs Through the LAN Port .................................................. 3-12
Configuring IP Filtering .......................................................................... 3-12
Enabling Subnets for the LAN Interface

The WS 2000 Wireless Switch allows the administrator to enable and configure four different subnets. The administrator can assign an IP address, port associations, DHCP settings, and security settings for each subnet. This System Reference provides two case studies that demonstrate how requirements for network access and capabilities drive the decisions of how to configure the subnets.

Defining Subnets

Select **LAN** under the **Network Configuration** group from the left menu. Use the LAN configuration screen to view a summary of physical-port addresses and Wireless LANs (WLANs) associated with the four supported subnets, and to enable or disable each configured subnet.

1. Check the box to the left of a subnet to enable that subnet. Up to four subnets can be enabled to use the wired and/or wireless connections of the switch-managed LAN. Enable multiple subnets to divide the communications of different business areas or operations. Each enabled subnet shows up in the directory tree in the left column of the configuration screens. Consider disabling a previously configured subnet if its assigned ports are no longer in use, or to consolidate the LAN’s communications on fewer subnets.

2. Click **Apply** to save changes. All “unapplied” changes are lost when the administrator moves to a new screen.

The rest of the information on this screen is summary information. It is collected from other screens (such as the subnet configuration screens) where the administrator can set the data.
To change features of a subnet select **Network Configuration --> LAN --> <subnet name>** from the menu on the left.

**Configuring Subnets**

The WS 2000 Network Management System allows the administrator to define and refine the configuration of the enabled subnets. Each of three subnets (short for "subnetworks") can be configured as an identifiably separate part of the switch-managed Local Area Network (LAN). Each subnet can include some combination of assigned ports and associated Wireless LANs (WLANs). To configure an enabled subnet, select the subnet name from the **Network Configuration --> LAN** list in the left. The following screen appears for the selected subnet.

1. Change the **Name** of the subnet to use a descriptive name that indicates something about the subnet. The name can contain seven characters, including spaces and numbers. It will appear in the left menu under the LAN menu item.
2. Set an **IP address** to be used for the subnet. This is how the switch will refer specifically to this subnet. This could be a WAN address; but more likely it will be a non-routable address. An IP address uses a series of four numbers that are expressed in dot notation, for example, 194.182.1.1.
3. Set the **Network Mask** for the IP address. A network mask uses a series of four numbers that are expressed in dot notation, similar to an IP number. For example, 255.255.255.0 is a network mask.
4. Select a port or WLAN from the Interfaces drop-down menu to associate it with the subnet. Six LAN ports are available on the switch. Assign from one to six ports to a subnet. Two subnets cannot use the same port. However, multiple ports can be assigned to one subnet.

Eight WLANs are available. WLAN assignments are logical designations. Associate from zero to three WLANs with a subnet. Two subnets cannot use the same WLAN. However, multiple WLANs can be associated with one subnet. If two or three WLANs are associated with one subnet, each port dedicated to that subnet can use any of the associated WLANs.

5. Click the Add button to add it to the Interfaces list.

Note that wireless devices cannot access the switch unless a WLAN is configured and associated with a subnet. (This process is described in Configuring Wireless LANs.)

The DHCP Configuration

DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, network mask, and gateway. The switch includes internal DHCP server and client features, and the subnet’s interface can use either capability.

1. Click the appropriate radio button to select one DHCP setting for the subnet’s interfaces:
   - Select This interface does not use DHCP to disable DHCP on this subnet and specify IP addresses manually.
   - Select This interface is a DHCP Client if this subnet obtains IP parameters from a DHCP server outside the switch.
   - Select This interface is a DHCP Server to enable the switch’s DHCP server features.
   - Select This interface is a DHCP Relay to use an external DHCP server to provide DHCP information to clients on this subnet. Use the associated field to enter the IP address for the external DHCP Server.

2. If This interface is a DHCP Server is the selected option, fill in the Address Assignment Range fields. These fields allow the administrator to assign a range of IP addresses to devices as they connect.

3. Set the Advanced Settings, if necessary.

4. Click the Apply button to save all changes.
Advanced DHCP Settings

1. Click the Advanced DHCP Server button to display a sub-screen to further customize IP address allocation.

2. If Dynamic DNS services are needed on the subnet, check the box labeled Enable Dynamic DNS.

   Enabling Dynamic DNS will allow domain name information to be updated when the IP address associated with that domain changes. When a MU associates and gets an IP address from the DHCP server, the DHCP server then updates the DNS server with the IP allotted to the corresponding hostname when DDNS is enabled.

   Any DHCP client can send the User Class Id either in the Single or Multiple user class ID format. The Single or Multiple User class option is provided to enable the switch to interpret the correct format in which the user class ID is sent by the client. The switch then retrieves the correct value of the user class ID sent by the DHCP client based on the selected format. This same user class ID format is used for the DDNS messages.

3. Specify the address of a Primary DNS Server. The Internet Server Provider (ISP) or a network administrator can provide this address.

   A DNS server translates a domain name, such as www.symbol.com, into an IP address that networks can use.

4. Specify the address of a Secondary DNS Server if one is available.

5. Specify the Default Gateway IP address for this subnet’s presence on the network, as used on the Subnet screen.

6. If your network has a Windows Internet Name Service (WINS) server specify the IP address in the WINS Server field.

   A WINS server allows you to map NetBIOS names to IP addresses.

7. Specify a DHCP Lease Time period in seconds for available IP addresses.

   The DHCP server grants an IP address for as long as it remains in active use. The lease time is the number of seconds that an IP address is reserved for re-connection after its last use. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. This is useful, for example, in education and customer environments where mobile-unit users change frequently. Use longer leases if there are fewer users.

8. If the MUs on this subnet are members of a domain, enter that name in the Domain Name field and it will be sent out via DHCP to all MUs associated with this subnet.

9. DNS Forward Zone is used for maintaining DomainName to Address mappings used by the DNS server.

10. Use the Static Mappings table to associate static (or fixed) IP addresses with MAC addresses of specific wireless devices. Every wireless, 802.11x-standard device has a unique Media Access Control (MAC) address.

   This address is the device’s hard-coded hardware number (shown on the bottom or back). An example of a MAC address is 00:09:5B:45:9B:07. This MAC table of specified devices provides corresponding static IP addresses for users, mobile units, and applications that may prefer or require such access.
Configuring Subnet Access

The WS 2000 Network Management System allows the administrator to set up access rules for subnet-to-subnet and subnet-to-WAN communication. These access rules control communication between subnets and the outside world (the WAN). Select Network Configuration --> Firewall --> Subnet Access to get to the Subnet Access screen.

The Access Overview Table

In the overview table, each of the rectangles represents a subnet association. The three possible colors indicate the current access level, as defined, for each subnet association.

<table>
<thead>
<tr>
<th>Color</th>
<th>Access Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Full Access</td>
<td>No protocol exceptions (rules) are specified. All traffic may pass between these two areas.</td>
</tr>
<tr>
<td>Yellow</td>
<td>Limited Access</td>
<td>One or more protocol rules are specified. Specific protocols are either enabled or disabled between these two areas. Click the table cell of interest and look at the exceptions area in the lower half of the screen to determine the protocols that are either allowed or denied.</td>
</tr>
<tr>
<td>Red</td>
<td>No Access</td>
<td>All protocols are denied, without exception. No traffic will pass between these two areas.</td>
</tr>
</tbody>
</table>

The Access Exception Area

In the lower half of the screen, the access is controlled by specific rules that control the protocols that are allowed or denied between the two subnets or the subnet and the WAN. All rules are added to the exception table. The Allow or Deny menu item applies to all entries in the table. There are two ways to add entries (access rules) to the table. The first is by checking the checkboxes for specific protocols (on the left). The second is by adding rules for specific port numbers by clicking the
Add button and filling in the necessary information. A combination of the two methods can be used to add multiple entries to the table.

You can allow or deny communication through specific protocols using the following process:

1. Click in a cell of the table that represents the subnet-to-subnet (or subnet-to-WAN) relationship to define. All access rules (if any are defined) appear in the table in the lower-half of the screen.
2. Use the pull-down menu above the list to Allow or Deny all the entries specified in the exception table. You cannot allow some protocols (or ports) and deny others.
3. From the list of checkboxes on the left side, select those protocols to allow or deny. The protocols are automatically added to the table with the relevant Name, Transport, Start Port, and End Port information. The available protocols are shown in the table below.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Transport, Port Used</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>TCP, 80</td>
<td>Hypertext Transfer Protocol (HTTP) is the protocol for transferring files on the World Wide Web. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols, the foundation protocols for the Internet.</td>
</tr>
<tr>
<td>TELNET</td>
<td>TCP, 23</td>
<td>TELNET is the terminal emulation protocol of TCP/IP. TELNET uses TCP to achieve a virtual connection between server and client, then negotiates options on both sides of the connection.</td>
</tr>
<tr>
<td>FTP</td>
<td>TCP, 21</td>
<td>File Transfer Protocol (FTP) is an application protocol that uses the Internet’s TCP/IP protocols. FTP provides a simple and efficient way to exchange files between computers on the Internet.</td>
</tr>
<tr>
<td>SMTP</td>
<td>TCP, 25</td>
<td>Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used for sending and receiving email. Due to its limited ability to queue messages at the receiving end, SMTP is often used with POP3 or IMAP. SMTP sends the email, and then POP3 or IMAP receives the email.</td>
</tr>
<tr>
<td>POP</td>
<td>TCP, 109:110</td>
<td>Post Office Protocol (POP3) is a TCP/IP protocol intended to permit a workstation to dynamically access a maildrop on a server host. A workstation uses POP3 to retrieve email that the server is holding for it.</td>
</tr>
<tr>
<td>DNS</td>
<td>TCP+UDP, 53</td>
<td>Domain Name Service (DNS) protocol searches for resources using a database that is distributed among different name servers.</td>
</tr>
</tbody>
</table>

- You can make changes to the information automatically filled into the table; however, note that changes in the selected transport type can change the port numbers that can be specified in the table.
4. To add an access rule for a protocol, port, or transport other than the ones available from the checkboxes on the left, click the **Add** button. An empty row is added to the table.
   - Specify a **Name** to identify the new access rule. This could be the name of a particular application, for example.
Select a transport type from the **Transport** column’s pull-down menu. The available transports are:

<table>
<thead>
<tr>
<th>Transport</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>This selection designates all of the protocols displayed in the table’s pull-down menu, as described below.</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol (TCP) is a set of rules used with Internet Protocol (IP) to send data as message units over the Internet. While IP handles the actual delivery of data, TCP keeps track of individual units of data called packets. Messages are divided into packets for efficient routing through the Internet.</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol (UDP) is mostly used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides very few error recovery services and methods. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol (ICMP) is tightly integrated with IP. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation. Because ICMP uses IP, ICMP packet delivery is unreliable. Hosts cannot count on receiving ICMP packets for a network problem.</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header (AH) is one of the two key components of IP Security Protocol (IPSec). The other key component is Encapsulating Security Protocol (ESP), described below. AH provides authentication, proving the packet sender really is the sender, and the data really is the data sent. AH can be used in transport mode, providing security between two end points. Also, AH can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Protocol (ESP) is one of the two key components of IP Security Protocol (IPSec). The other key component is Authentication Header (AH), described above. ESP encrypts the payload of packets, and also provides authentication services. ESP can be used in transport mode, providing security between two end points. Also, ESP can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).</td>
</tr>
<tr>
<td>GRE</td>
<td>General Routing Encapsulation (GRE) supports VPNs across the Internet. GRE is a mechanism for encapsulating network layer protocols over any other network layer protocol. Such encapsulation allows routing of IP packets between private IP networks across an Internet that uses globally assigned IP addresses.</td>
</tr>
</tbody>
</table>

Specify port information for the protocol. If the protocol uses only one port, enter the same port number in the **Start Port** and **End Port** columns, or leave the **End Port** column blank. Otherwise, use both columns for an entry that has a range of ports.

5. Click the **Apply** button to save changes.

**Advanced Subnet Access Settings**

There can be situations in which the standard subnet access setting process is not specific enough for the needs of an organization. Instead, access or firewall rules need to be defined based upon destination and source IP addresses, transport types, and ports. The Advanced Subnet Access screen allows the administrator to create more complicated inbound and outbound policies.
Select **Network Configuration** --> **Firewall** --> **Advanced Subnet Access** from the left menu. The screen consists of two areas. The Settings area enables or disables the data found on this screen. The Firewall Rules area displays the currently defined and active firewall rules. This area will display either the inbound or outbound rules. The rules are applied in the order that they are listed. The rules at the top of the list take precedence over the rules lower in the list.

1. To enable the advanced access settings, check the **Override Subnet Access and NAT settings** box. The rest of the screen will become active. When this box is not checked, the settings in both the Subnet Access screen (under Firewall) and the NAT screen (under WAN) are disabled; the switch will use the settings found on this screen instead.

2. If you want the application to translate the subnet access settings into Firewall Rules (displayed in the lower area), click the **Import rules from Subnet Access** button. This button removes the need for the administrator to reenter the information defined on the Subnet Access screen.

Next, add, delete, or modify rules in the Firewall Rules list, as necessary.

3. Select **Inbound** or **Outbound** from the pull-down menu at the top of the Firewall Rules area, to display either the inbound (data entering the LAN) or outbound (data exiting the LAN) rules.

4. To modify a rule, select the rule from the Firewall Rules list, then edit the fields by clicking in the field to modify. Often a dialog box will appear to facilitate the entry of the field data.

5. To add a rule, click the **Add** button and then add data to the six rule fields. Note that not all fields are required.

6. To delete a rule, select a rule from the list and click the **Del** button.

7. Move rules to a higher or lower precedence by clicking the **Move Up** or **Move Down** buttons, as necessary.

8. When you have finished defining the Firewall Rules, click the **Apply** button to save changes.

Use the following information to help set the Firewall Rule fields:

- **Index**—The index number determines the order in which firewall rules will be executed. The rules are executed in order from lowest index number to highest number. Use the **Move Up** and **Move Down** buttons to change the index number.
- **Source IP**—The Source IP range determines the origin address(es) for the firewall rule. To set the Source IP range, click the field and a new window will pop up to enter the IP address and a second number that indicates that number of IP numbers starting at the first address (the range). An IP address of 0.0.0.0 indicates all IP addresses.

- **Destination IP**—The Destination IP range determines the target address(es) for the firewall rule. To configure the Destination IP range, click the field and a new window will pop up to enter the IP address and range. An IP address of 0.0.0.0 indicates all IP addresses.

- **Transport**—To determine the transport protocol to be filtered in the firewall rule, click the field to choose from the list of protocols:

<table>
<thead>
<tr>
<th>Transport</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>This selection designates all of the protocols displayed in the table’s pull-down menu, as described below.</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol (TCP) is a set of rules used with Internet Protocol (IP) to send data as message units over the Internet. While IP handles the actual delivery of data, TCP keeps track of individual units of data called packets. Messages are divided into packets for efficient routing through the Internet.</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol (UDP) is mostly used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides very few error recovery services and methods. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol (ICMP) is tightly integrated with IP. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation. Because ICMP uses IP, ICMP packet delivery is unreliable. Hosts cannot count on receiving ICMP packets for a network problem.</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header (AH) is one of the two key components of IP Security Protocol (IPSec). The other key component is Encapsulating Security Protocol (ESP), described below. AH provides authentication, proving the packet sender really is the sender, and the data really is the data sent. AH can be used in transport mode, providing security between two end points. Also, AH can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Protocol (ESP) is one of the two key components of IP Security Protocol (IPSec). The other key component is Authentication Header (AH), described above. ESP encrypts the payload of packets, and also provides authentication services. ESP can be used in transport mode, providing security between two end points. Also, ESP can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).</td>
</tr>
<tr>
<td>GRE</td>
<td>General Routing Encapsulation (GRE) supports VPNs across the Internet. GRE is a mechanism for encapsulating network layer protocols over any other network layer protocol. Such encapsulation allows routing of IP packets between private IP networks across an Internet that uses globally assigned IP addresses.</td>
</tr>
</tbody>
</table>

- **Src. Ports (Source Ports)**—The source port range determines which ports the firewall rule applies to on the source IP address. To configure the source port range, click the field and a new window will pop up to enter the starting and ending ports in the range. For rules where only a single port is necessary, enter the same port in the start and end port fields.

- **Dst. Ports (Destination Ports)**—The destination port range determines which ports the firewall rule applies to on the destination IP address. To configure the destination port range, click the field and a new window will pop up to enter...
the starting and ending ports in the range. For rules where only a single port is necessary, enter the same port in the start and end port fields.

- **Rev. NAT (Reverse NAT) (inbound) / NAT (outbound)**—To enable NAT or reverse NAT for a firewall rule, enter this value.
  
  For Inbound, click the **Rev. NAT** field and a new window will pop up to enter the IP address and translation port for the reverse NAT host.
  
  For the Outbound direction, select the WAN (WAN1, WAN2, and so on) from the **NAT** field menu that is associated with the appropriate NAT definition. (See *Configuring Network Address Translation (NAT)*).

- **Action**—Choose **Allow** or **Deny** from the pull-down menu in this field to determine whether the firewall rule is to allow or deny the specified rule.

**Virtual LAN (VLAN) Configuration**

A Virtual Local Area Network or VLAN is a switched network that has been segmented by function or application rather than the traditional LAN segmentation, which is based on physical location. VLANs allow a greater level of flexibility than a standard LAN, and enable changes to be made to the network infrastructure without physically disconnecting network equipment. The WS 2000 Wireless Switch supports assigning one VLAN ID to each of the configured subnets.

To configure one or more VLAN, select **Network Configuration --> VLAN** from the navigation menu on the left. The VLAN Configuration screen will appear.

The upper part of the screen is use to set up the type of VLAN that will be used.

1. Use the pull-down menu to select a **VLAN Type** for this switch. The two options are **User Based** and **Port Based**. **User-based VLANS**, also known as MAC-based VLANS, partition traffic based on the MAC addresses of their users. The switch inspects frames and partitions information based on the VLAN associated with the MAC address. The advantage of this scheme is that it allows a user to move from one physical location to another and still be a member...
of the same VLAN. The disadvantage of user-based VLANs is that each client’s MAC address must be specified, which can be very time consuming for large network deployments.

**Port-based VLANs**, also known as Layer 3 VLANs, partition traffic based on protocol. The switch inspects each packet, extracts the VLAN membership information, and partitions the packet accordingly. The advantage of this scheme is that it allows partitioning based on protocol type, and each user does not have to be manually added to the VLAN. The disadvantage of port-based VLANs is that network performance is generally slower than user-based VLANs. This performance loss is due to the large amount of overhead required to inspect each packet for the VLAN ID.

Use the pull-down menu to select a **Trunk Port** for the switch. The WAN port or any one of the switch's six ports that is not associated with a subnet can be configured as the Trunk Port for a user-based VLAN.

- **Note** Ports that are associated with a subnet are not available in the Trunk Port pull-down menu. To disassociate a port from a subnet (so that is can be assigned as the trunk port), go to the appropriate subnet on the menu, select the desired port, and then click Delete. After clicking the Apply button on the subnet screen, return to the VLAN page, and the port will be available in the Trunk Port pull-down menu.

2. Enter a **VLAN Tag** between 1 and 4094. This tag will be associated with all VLAN traffic that goes out through the Trunk Port in a user-based VLAN. This tag should be the one used to share information between the various VLANs. This value should also be either one of the user-based or port-based VLANs.

**Trunking VLANs Through the LAN Port**

To configure VLAN trunking on the WAN port see Chapter 10, *Trunking VLANs Through the WAN Port*. To configure VLAN trunking on one of the LAN ports follow the instructions below.

A Trunk Port allows a type of VLAN partitioning that is transparent to the users connected to that port. All traffic passing through the Trunk Port is tagged with the default VLAN ID tag.

The next step is to specify the mapping between the available subnets and the VLANs that you are defining. In the mapping table, each of the four subnets are listed by name; however, only subnets that are currently active can be configured with a VLAN ID.

1. Enter the **VLAN ID** value for each subnet. The value must be between 1 and 4094. The WS 2000 Wireless Switch only supports VLANs numbered between 1 and 4094 in user-based VLANs. If your network uses a VLAN number higher than 4094, you will not be able to use VLAN trunking with this switch.

2. In the **Trunked VLANs** field, enter in the VLAN IDs for VLANs that you wish to configure as trunked VLANs. When entering multiple VLAN IDs, separate each ID with a comma. To qualify as a trunked VLAN, the VLAN ID must be associated with a configured subnet.

   The **Trunk Enable** box will be automatically checked on subnets for which VLAN IDs have been selected as trunked VLANs.

   3. **Click the Apply button** to save changes.

**Configuring IP Filtering**

IP based filtering allows administrators to configure Incoming and Outgoing IP filtering policies on packets within the same Subnet / WLAN and between wired and wireless hosts. Filters can be set up based on IP Address or as a default rule for all IPs in a given direction.
Select **Network Configuration** --> **IP Filtering** from the left navigation menu.

1. Click the **Add** button to create a new filter in the table. The new filter can then be edited by clicking on the corresponding fields in the table.

2. Click on the **Filter Name** field and provide a name or edit an existing name for the filter. The Filter Name should be unique for each filter rule that is added.

3. Select a **Protocol** for the filter from the pull-down menu. The available protocols are:

<table>
<thead>
<tr>
<th>Transport</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>This selection designates all of the protocols displayed in the table’s pull-down menu, as described below.</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol (TCP) is a set of rules used with Internet Protocol (IP) to send data as message units over the Internet. While IP handles the actual delivery of data, TCP keeps track of individual units of data called packets. Messages are divided into packets for efficient routing through the Internet.</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol (UDP) is mostly used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides very few error recovery services and methods. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol (ICMP) is tightly integrated with IP. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation. Because ICMP uses IP, ICMP packet delivery is unreliable. Hosts cannot count on receiving ICMP packets for a network problem.</td>
</tr>
<tr>
<td>Transport</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>PIM</td>
<td>Protocol Independent Multicast (PIM) is a collection of multicast routing protocols, each optimized for a different environment. There are two main PIM protocols, PIM Sparse Mode and PIM Dense Mode. A third PIM protocol, Bi-directional PIM, is less widely used.</td>
</tr>
<tr>
<td>GRE</td>
<td>General Routing Encapsulation (GRE) supports VPNs across the Internet. GRE is a mechanism for encapsulating network layer protocols over any other network layer protocol. Such encapsulation allows routing of IP packets between private IP networks across an Internet that uses globally assigned IP addresses.</td>
</tr>
<tr>
<td>RSVP</td>
<td>The RSVP protocol is used by a host to request specific qualities of service from the network for particular application data streams or flows. RSVP is also used by routers to deliver quality-of-service (QoS) requests to all nodes along the path(s) of the flows and to establish and maintain state to provide the requested service. RSVP requests will generally result in resources being reserved in each node along the data path.</td>
</tr>
<tr>
<td>IDP</td>
<td>Datagram Protocol (IDP) is a simple, unreliable datagram protocol, which is used to support the SOCK_DGRAM abstraction for the Internet Protocol (IP) family. IDP sockets are connectionless and normally used with the sendto and recvfrom subroutines.</td>
</tr>
<tr>
<td>PUP</td>
<td>It is the first open protocol, named the Public Unitary Protocol (PUP protocol). It was developed to standardize communications protocol among controls manufacturers in the facility automation industry. This protocol is generally understood to form the basis of the current BACnet protocol, which has become popular of late.</td>
</tr>
<tr>
<td>EGP</td>
<td>The Exterior Gateway Protocol (EGP) is an exterior routing protocol used for exchanging routing information with gateways in other autonomous systems.</td>
</tr>
<tr>
<td>IPIP</td>
<td>IPIP is a protocol which is used to encapsulate an IP packet within another IP packet.</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Protocol (ESP) is one of the two key components of IP Security Protocol (IPSec). The other key component is Authentication Header (AH), described above. ESP encrypts the payload of packets, and also provides authentication services. ESP can be used in transport mode, providing security between two end points. Also, ESP can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header (AH) is one of the two key components of IP Security Protocol (IPSec). The other key component is Encapsulating Security Protocol (ESP), described below. AH provides authentication, proving the packet sender really is the sender, and the data really is the data sent. AH can be used in transport mode, providing security between two end points. Also, AH can be used in tunnel mode, providing security like that of a Virtual Private Network (VPN).</td>
</tr>
<tr>
<td>IGMP</td>
<td>The Internet Group Management Protocol (IGMP) is used between IP hosts and their immediate neighbor multicast agents to support the creation of transient groups, the addition and deletion of members of a group, and the periodic confirmation of group membership. IGMP is an asymmetric protocol and is specified here from the point of view of a host, rather than a multicast agent.</td>
</tr>
<tr>
<td>IPV6</td>
<td>IPv6 is short for &quot;Internet Protocol Version 6&quot;. IPv6 is the &quot;next generation&quot; protocol designed by the IETF to replace the current version Internet Protocol, IP Version 4 (&quot;IPv4&quot;).</td>
</tr>
<tr>
<td>COMPR_H</td>
<td>COMPR_H is the Compressed Header Protocol.</td>
</tr>
<tr>
<td>RAW_IP</td>
<td>RAW IP is used when communication is done directly to the IP layer without using any additional protocols.</td>
</tr>
</tbody>
</table>
4. Select a Port from the pulldown menu for this IP Filtering rule to apply to. The default is All and will apply the filtering to all ports on the switch.

5. Enter the source IP range for the filtering rule in the Src Start and Src End fields.

6. Enter the destination IP range for the filtering rule in the Dst Start and Dst End fields.

7. The In Use field will display the current state of the filtering rule. When the rule is in use it will read YES. When the rule is not in use this field will read NO.
WAN Configuration

Configuring the WAN Interface ................................................. 4-2
  Configuring WAN IP Information ........................................... 4-2
  Setting Up Point-to-Point over Ethernet (PPPoE) Communication .............. 4-3
Configuring the WS 2000 Firewall ........................................... 4-5
  Disabling the Firewall .................................................. 4-5
  Setting the NAT Timeout ................................................ 4-5
  Configurable Firewall Filters .......................................... 4-6
Configuring Network Address Translation (NAT) ................................ 4-7
Configuring Static Routes ................................................ 4-10
  Configuring the Default Gateway Interface ................................ 4-10
  Creating User Defined Routes ......................................... 4-11
  Setting the RIP Configuration ........................................ 4-11
Configuring a Virtual Private Network (VPN) ................................ 4-12
  Creating a VPN Tunnel ................................................ 4-14
  Setting Up VPN Security .............................................. 4-14
  Configuring Manual Key Exchange ................................... 4-15
  Setting Up Automatic Key Exchange .................................. 4-17
  Setting Up Internet Key Exchange (IKE) ................................ 4-18
  VPN: Frequently Asked Questions .................................... 4-20
Configuring Content Filtering .............................................. 4-23
Configuring DynDNS ........................................................ 4-26
  Enabling and Configuring DynDNS ..................................... 4-26
  Updating DynDNS ....................................................... 4-26
Configuring the WAN Interface

A wide area network (WAN) is a widely dispersed telecommunications network. In a corporate environment, the WAN port might connect to a larger corporate network. For a small business, the WAN port might connect to a DSL or cable modem to access the Internet.

The administrator needs to enter the WAN configuration information. The WS 2000 Wireless Switch includes one WAN port. In order to set up communications with the outside world, select Network Configuration --> WAN from the left menu. The following WAN configuration page appears.

Configuring WAN IP Information

1. Check the Enable WAN Interface checkbox to enable a connection between the switch and a larger network or the outside world through the WAN port.

2. Check This interface is a DHCP Client checkbox to enable Dynamic Host Configuration Protocol (DHCP) for the WAN connection. If This interface is DHCP Client is checked, the switch is limited to one WAN IP address. This choice is required when:
   - The host router or switch on the WAN is communicating with the WS 2000 Wireless Switch using DHCP.
   - The switch is interfacing with an Internet Service Provider (ISP) that uses DHCP addressing.

   This setting is independent from the DHCP settings for the switch’s internal subnets.

   Note

3. It is not necessary to specify the IP Address or any of the other fields on the top section of this form when the WS 2000 Wireless Switch is set as a DHCP Client. The network host (router, switch, or modem) will provide these values each time it makes a connection with the switch.
4. If the DHCP setting is not checked, fill in the information in this area. To find out the information to enter into these fields, contact the network administrator or the ISP that provided the cable modem or DSL router. All the fields below take standard IP addresses of the form xxx.xxx.xxx.xxx.

- **The IP Address** refers to the IP address that the outside world will use to address the WS 2000 Wireless Switch.
- Click the **More IP Addresses** button to specify additional static IP addresses for the switch. Additional IP addresses are required when users within the LAN need dedicated IP addresses, or when servers in the LAN need to be accessed (addressed) by the outside world. The pop-up window allows the administrator to enter up to eight WAN IP addresses for the switch.
- **The Subnet Mask** is the mask used for the WAN.
- **The Default Gateway** is the address of the device that provides the connection to the WAN (often a cable modem or DSL router).
- **The two DNS Server fields** specify DNS addresses of servers that can translate domain names, such as www.symbol.com, into IP addresses that the network uses when passing information. The **Secondary DNS Server** acts as a backup to the **Primary DNS Server**, when the primary server is not responding.

### Setting Up Point-to-Point over Ethernet (PPPoE) Communication

PPPoE provides the ability to connect a network of hosts through a simple device to a remote access concentrator. Many DSL providers require that their clients communicate using this protocol. The facility allows the ISP to control access, billing, and type of service provided to clients on a per-user or per-site basis. Check with the network administrator or ISP to determine whether to enable this feature, and, if so, find out the username and password required for authentication.

1. Check **Enable** in the **PPP over Ethernet** area to enable the PPPoE protocol for high-speed connections.
2. Enter the **Username** and **Password** required for authentication. The username and password is for the switch’s router to use when connecting to the ISP. When the Internet session starts, the ISP authenticates the username.
3. Set the **Idle Time** to an appropriate number. This number is the amount of time the PPPoE connection will be idle before it disconnects. The 10000 second (default idle time is appropriate for most situations).
4. Check Keep Alive to instruct the switch to continue occasional communications over the WAN even when client communications to the WAN are idle. Some ISPs terminate inactive connections, while others do not. In either case, enabling Keep-Alive mode keeps the switch’s WAN connection alive, even when there is no traffic. If the ISP drops the connection after so much idle time, the switch automatically reestablishes the connection to the ISP.

5. Select the appropriate WAN authentication method from the drop-down menu. Collect this information from the network administrator. Select between None, PAP, CHAP, or PAP or CHAP.

- **CHAP**
  A type of authentication in which the person logging in uses secret information and some special mathematical operations to come up with a number value. The server he or she is logging into knows the same secret value and performs the same mathematical operations. If the results match, the person is authorized to access the server. One of the numbers in the mathematical operation is changed after every login, to protect against an intruder secretly copying a valid authentication session and replaying it later to log in.

- **PAP**
  An identity verification method used to send a user name and password over a network to a computer that compares the user name and password to a table listing authorized users. This method of authentication is less secure, because the user name and password travel as clear text that a hacker could read.

6. Click the Apply button to save changes.

7. Once connected, the PPoE State section will display the provided IP Address, Default Gateway, Primary DNS Server and Secondary DNS Server.
Configuring the WS 2000 Firewall

The WS 2000 Wireless Switch provides a secure firewall/Network Address Translation (NAT) solution for the WAN uplink. The firewall includes a proprietary CyberDefense Engine to protect internal networks from known Internet attacks. It also provides additional protection by performing source routing, IP unaligned timestamp, and sequence number prediction. The firewall uses a collection of filters to screen information packets for known types of system attacks. Some of the switch’s filters are always enabled, and others are configurable.

To view or change the firewall settings, select Network Configuration --> WAN --> Firewall from the left menu.

Disabling the Firewall

The firewall can be enabled or disabled with one click. Check Disable Firewall if the filters should not be active. By default the firewall is enabled.

Setting the NAT Timeout

TCP Default Timeout

The TCP Default Timeout field is the NAT timeout value which user has to enter before NAT’s request is timed out by the switch. We now have table to enter the NAT timeout based on PORT and Protocol, hence if no matching record is found in this table then this default NAT value would be considered for all the TCP requests. Currently in WS2000 the NAT timeout configuration is a global configuration for any TCP/IP packets going through firewall. This configuration puts a restriction on the type of UDP or TCP applications can be used with WS2000. Hence a new table is introduced that allows user to enter the NAT timeout based on PORT and Protocol.

Enter a default timeout value (in seconds) for the switch to use as the timeout value when no matching records are found in the NAT Timeout Table below. This is a global configuration for any TCP/IP packets going through firewall that don’t match other values.
**NAT Timeout Table**

In addition to the **TCP Default Timeout** setting the WS2000 provides the ability to configure specific NAT timeout rules for specific TCP and UDP ports.

To add rules to the NAT Timeout Table:
1. Click the **Add** button to add a row to the table.
2. Select a Transport method from the pulldown menu. Available options are:
   - **TCP**
     - Transmission Control Protocol (TCP) is a set of rules used with Internet Protocol (IP) to send data as message units over the Internet. While IP handles the actual delivery of data, TCP keeps track of individual units of data called packets. Messages are divided into packets for efficient routing through the Internet.
   - **UDP**
     - User Datagram Protocol (UDP) is mostly used for broadcasting data over the Internet. Like TCP, UDP runs on top of Internet Protocol (IP) networks. Unlike TCP/IP, UDP/IP provides very few error recovery services and methods. UDP offers a way to directly connect, and then send and receive datagrams over an IP network.
3. Specify the **Port** number which the new timeout record will apply to.
4. Enter a **Timeout** value to specify the number of seconds before a NAT request is timed out by the switch’s firewall.
5. Click the **Apply** button to save the changes to this page.

**Configurable Firewall Filters**

The administrator can enable or disable the following filters. By default, all filters are activated. It is safe to turn the filters off if one of the following things is true:

- The switch is on a completely isolated network with no access to the Internet and is therefore secure.
- The switch is heavily loaded a slight increase in performance outweighs the safety of the network.
- Blocking these types of attacks would also block legitimate traffic on their network (although this scenario is highly unlikely).

**SYN Flood Attack Check**

A SYN flood attack requests a connection and then fails to promptly acknowledge a destination host’s response, leaving the destination host vulnerable to a flood of connection requests.

**Source Routing Check**

A source routing attack specifies an exact route for a packet’s travel through a network, while exploiting the use of an intermediate host to gain access to a private host.

**Winnuke Attack Check**

A “Win-nuking” attack uses the IP address of a destination host to send junk packets to its receiving port. This attack is a type of denial of service (DOS) attack that completely disables networking on systems Microsoft Windows 95 and NT. Because this attack is only affective on older systems, it may not be necessary to enable this feature on a LAN with newer Microsoft Windows operating systems or with systems that have the appropriate “Winnuke” patches loaded.

**FTP Bounce Attack Check**

An FTP bounce attack uses the PORT command in FTP mode to gain access to arbitrary ports on machines other than the originating client.
Click the Apply button to save changes made on this screen.

**Configuring Network Address Translation (NAT)**

NAT provides the translation of an Internet Protocol (IP) address within one network to a different, known IP address within another network. One network is designated the private network, while the other is the public. NAT provides a layer of security by translating private (local) network addresses to one or more public IP addresses. For example, when an administrator wants to allow individuals on the WAN side access to a particular FTP or web server that is located on one of the LAN subnets but does not want to permit any other access, NAT is the appropriate solution.

1. Select **Network Configuration --> WAN --> NAT** from the left menu. The following screen appears.
This screen displays the IP addresses specified in the WAN screen (Network Configuration --> WAN from the left menu). Up to eight WAN addresses can be associated with the switch. The NAT screen enables the administrator to set the type of translation and port forwarding required.

2. For each of the addresses, select the NAT type.
   - Select 1 to 1 from the pull-down menu to map a WAN IP address to a single local (subnet) IP address. This selection is useful in situations in which users require dedicated IP addresses or when public-facing servers are connected to the switch.
   - Select 1 to Many from the pull-down menu to map a WAN IP address to a range of local IP addresses. Use this option when there are fewer public IP addresses on the WAN than there are users on the LAN. 1 to Many NAT allows a single IP address to handle traffic from multiple private LAN IP addresses.
   - Select None from the pull-down menu when the administrator sets up routable IP addresses (set on the Network Configuration --> Routing screen).

3. If the NAT type is 1 to 1, the Outbound Mappings field allows the administrator to specify a single IP Address. This address specifies the 1-to-1 mapping between the WAN IP address and the specified LAN IP address.

4. If the NAT type is 1 to Many, the 1 to Many button in the adjacent Outbound Mappings field is active, allowing the administrator to specify address assignments for each subnet. If no translation should be done, none should be selected for the subnet.
5. Click the **Port Forwarding** button to display a sub-screen of port forwarding parameters for inbound traffic from the associated WAN IP address. When finished, click the **Ok** button to close the screen.

6. Click **Add** to add a new port forwarding entry and fill in the following fields.

   - **Name**: Enter a name for the service that is being forwarded. The name can be any alphanumeric string and is used for easy identification of the service.
   - **Transport**: Use this pull-down menu to specify the transport protocol used in this service. The choices are **ALL, TCP, UDP, ICMP, AH, ESP, and GRE**.
   - **Start Port / End Port**: Enter the port or ports used by this service. To specify a single port, enter the port number in the **Start Port** field. To specify a range of ports, use both the **Start Port** and **End Port** fields to enter the port numbers. For example, enter 110 in the **Start Port** field and 115 in the **End Port** field.
   - **IP Address**: Enter the **IP address** to which the specified service is forwarded. This address must be within the specified NAT range for the associated WAN IP address.

7. Click the **Forward all unspecified ports to** check box and then specify an IP address to enable port forwarding for incoming packets with unspecified ports.

8. Click the **Apply** button on the NAT screen to save changes.
Configuring Static Routes

A router uses routing tables and protocols to forward data packets from one network to another. The switch’s router manages traffic within the switch’s network, and directs traffic from the WAN to destinations on the switch-managed LAN. The WS 2000 Network Management System provides the Router screen to view and set the router’s connected routes. To view this screen, select **Network Configuration --> Router** from the menu on the left.

The **WS 2000 Route Table** area of the screen displays a list of currently connected routes between the enabled subnets, the WAN, and the router. The information here is generated from settings applied on the Subnet and WAN screens. The destination for each subnet is its IP address. The subnet mask (or network mask) and gateway settings are those belonging to each subnet, or to the WAN in general. To make changes to the information in the Connected Routes information, go to the appropriate subnet screen (**LAN --> <subnet name>** or the **WAN** screen).

### Configuring the Default Gateway Interface

The Default Gateway Interface allows you to specify which interface will be used as the default gateway for all unspecified routes on the WS2000. The available options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>None</strong></td>
<td>Selecting this option will not set a Default Gateway Interface for unspecified routes.</td>
</tr>
<tr>
<td><strong>WAN</strong></td>
<td>Sets the WAN interface as the Default Gateway Interface for all unspecified routes.</td>
</tr>
<tr>
<td><strong>Subnet 1</strong></td>
<td>If Subnet 1 is enabled, sets it as the Default Gateway Interface for all unspecified routes.</td>
</tr>
<tr>
<td><strong>Subnet 2</strong></td>
<td>If Subnet 2 is enabled, sets it as the Default Gateway Interface for all unspecified routes.</td>
</tr>
<tr>
<td><strong>Subnet 3</strong></td>
<td>If Subnet 3 is enabled, sets it as the Default Gateway Interface for all unspecified routes.</td>
</tr>
<tr>
<td><strong>Subnet 4</strong></td>
<td>If Subnet 4 is enabled, sets it as the Default Gateway Interface for all unspecified routes.</td>
</tr>
</tbody>
</table>
Creating User Defined Routes

The User Defined Routes area of the screen allows the administrator to view, add or delete internal static (dedicated) routes, and to enable or disable routes that are generated using the Routing Information Protocol (RIP). If RIP is enabled, this table can also include routes that RIP generates.

This table also includes internal static routes that the administrator adds. Internal static routes are dedicated routes for data that travels from the WAN, through the switch, and to a specified subnet. Such routes are supplemental to the default routes already set up for each of the subnets.

1. Click the Add button to create a new table entry.
2. Specify the destination IP address, subnet mask, and gateway information for the internal static route.
3. Select an enabled subnet from the Interface column’s drop-down menu to complete the table entry. Information in the Metric column is automatically generated, and is used by router protocols to determine the best hop routes.
4. The Source column automatically displays “User” for a user-added entry. An RIP-sourced entry displays “RIP.”
5. Click the Apply button to save changes.

Setting the RIP Configuration

Routing Information Protocol (RIP) is an interior gateway protocol that specifies how routers exchange routing-table information. The Routing screen also allows the administrator to select the type of RIP and the type of RIP authentication used by the switch. To set or view the RIP configuration, click the RIP Configuration button. The following subscreen appears.
1. Select the RIP Type from the pull-down menu to be one of the following values.

**No RIP** Depending on the RIP Direction setting, the No RIP option partially or completely disallows the switch's router from exchanging routing information with other routers. Routing information may not be appropriate to share, for example, if the switch manages a private LAN.

**RIP v1** RIP version 1 is a mature, stable, and widely supported protocol. It is well suited for use in stub networks and in small autonomous systems that do not have enough redundant paths to warrant the overhead of a more sophisticated protocol.

**RIP v2 (v1 compat)** RIP version 2 (compatible with version 1) is an extension of RIP v1's capabilities, but it is still compatible with RIP version 1. RIP version 2 increases the amount of packet information to provide the a simple authentication mechanism to secure table updates.

**RIP v2** RIP version 2 enables the use of a simple authentication mechanism to secure table updates. More importantly, RIP version 2 supports subnet masks, a critical feature that is not available in RIP version 1. This selection is not compatible with RIP version 1 support.

2. Select a routing direction from the RIP Direction drop-down menu. Both (for both directions), Rx only (receive only), and TX only (transmit only) are available options.

3. If RIP 2 or RIP 2 (v1 compat) is the selected RIP type, the RIP v2 Authentication area of the screen becomes active. Select the type of authentication to use from the Authentication Type drop-down menu. Available options are:

**None** This option disables the RIP authentication.

**Simple** This option enables RIP version 2's simple authentication mechanism. This setting activates the Password (Simple Authentication) field.

**MD5** This option enables the MD5 algorithm for data verification. MD5 takes as input a message of arbitrary length and produces a 128-bit fingerprint. The MD5 algorithm is intended for digital signature applications, in which a large file must be compressed in a secure manner before being encrypted with a private (secret) key under a public-key cryptographic system. The MD5 setting activates the RIP v2 Authentication settings for keys (below).

4. If the Simple authentication method is selected, specify a password of up to 15 alphanumeric characters in the Password (Simple Authentication) field.

5. If the MD5 authentication method is selected, fill in the Key #1 and Key #2 fields. Type in any numeric value between 0 and 256 into the MD5 ID field. Type in any string consisting of 16 alphanumeric characters into the MD5 Auth Key field.

6. Click the Ok button to return to the Routing screen.

### Configuring a Virtual Private Network (VPN)

VPNs are IP-based networks that use encryption and tunneling to give users remote access to a secure LAN. In essence, the trust relationship is extended from one LAN across the public network to another LAN, without sacrificing security. A VPN behaves similarly to a private network; however, because the data travels through the public network, three types of security mechanisms are required: confidentiality, integrity, and authentication.

- Confidentiality (through public-key or secret-key cryptology) ensures the privacy of information being exchanged between communicating parties.
- Integrity ensures that information being transmitted over the public Internet is not altered in any way during transit (by using hash codes, message authentication codes, or digital signatures).
Authentication (with password authentication or digital signatures) ensures the identity of all communicating parties.

A diagram of a typical VPN situation is shown below, where there is a VPN tunnel created between two WS 2000 switches across the WAN. The diagram shows the settings for both switches.

**VPN Tunnel Configuration Settings for WS 2000 (1):**
- **Tunnel Name:** Test
- **Local Subnet:** Subnet1
- **Local WAN IP:** 157.235.55.10
- **Remote Subnet:** 192.168.1.0 [for PC on WS 2000 (1)]
- **Remote Subnet Mask:** 255.255.255.0
- **Remote Gateway:** 157.235.55.10 [WAN IP of WS 2000 (2)]
- **Default Gateway:** 157.235.55.10 [Set in WAN config of WS 2000 (1)]

**VPN Tunnel Configuration Settings for WS 2000 (2):**
- **Tunnel Name:** Test
- **Local Subnet:** Subnet2
- **Local WAN IP:** 157.235.55.10
- **Remote Subnet:** 192.168.1.0 [for PC on WS 2000 (1)]
- **Remote Subnet Mask:** 255.255.255.0
- **Remote Gateway:** 157.235.55.10 [WAN IP of WS 2000 (1)]
- **Default Gateway:** 157.235.55.10 [Set in WAN config of WS 2000 (2)]

Note: When connecting the WS 2000 through a router the Default Gateway will be the interface of that router.

The WS 2000 Network Switch provides VPN technology with a variety of security and setup options. Select **Network Configuration --> WAN --> VPN** from the left menu to create a VPN tunnel.
Creating a VPN Tunnel

1. Click the Add button to create a VPN tunnel. The lower portion of the screen, which then appears, is used to configure the tunnel.

2. Type a name for the tunnel into the Tunnel Name field. Use a name that indicates the role of the tunnel.

3. Select the subnet that will be the local end of the tunnel from the Local Subnet menu.

4. Specify the IP address to use for the local WAN (Local Wan IP), which should be one of the (up to) eight IP address specified on the WAN screen.

5. Specify the IP address for the Remote Subnet along with its subnet mask (Remote Subnet Mask).

6. Specify the IP address for the Remote Gateway.

Setting Up VPN Security

The WS 2000 Wireless Switch provides several different options for VPN security, all based upon encryption key exchange:

1. Manual Key Exchange uses the Manual Key Settings screen to specify the transform sets that will be used for VPN access.

   A transform set is a combination of security protocols and algorithms that are applied to IPSec protected traffic. During security association (SA) negotiation, both gateways agree to use a particular transform set to protect the data flow. A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies which algorithms to use with the selected security protocol. If you specify an ESP protocol in a transform set, you can specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform. When the particular transform set is used during negotiations for IPSec SAs, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote end of the gateway.

2. Automatic Key Exchange enables the WS 2000 Wireless Switch to automatically set encryption and authentication keys for VPN access. The Auto Key Settings subscreen provides the means to specify the type of encryption and authentication, without specifying the keys.
3. **Internet Key Exchange (IKE)** protocol is an IPSec standard protocol used to ensure security for VPN negotiation, and remote host or network access. IKE provides an automatic means of negotiation and authentication for communication between two or more parties. IKE manages IPSec keys automatically for the parties.

Each of these options requires some configuration, as described below.

**Configuring Manual Key Exchange**

1. Select the **Manual Key Exchange** radio button.

2. Click the **Manual Key Settings** button to specify the encryption method and the following screen appears. The setup process requires specifying both the authentication and the encryption methods and keys.

3. Select the authentication and anti-replay method you wish to use for the tunnel from the **AH Authentication** menu.

   - **None** Disables AH authentication and the rest of the fields in this area will not be active.
   - **MD5** Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) authentication keys.
   - **SHA1** Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

4. If either **MD5** or **SHA1** is the authentication type, specify an **Inbound Authentication Encryption Key** and an **Outbound Authentication Encryption Key**. If **MD5** is the authentication type, specify 32-character hexadecimal keys. If **SHA1** is the authentication type, specify 40-character hexadecimal keys.

5. Provide up to an eight-character hexadecimal values for the **Inbound SPI** and **Outbound SPI** fields (minimum is 100). These fields are used to identify the inbound security association created by the AH algorithm. These values must match the corresponding outbound and inbound SPI values (respectively) configured on the remote security gateway. These values should also be unique across all tunnels on the system.
6. Select the **ESP Type** from the menu.

   - **None**: Disables ESP and the rest of the fields in this area will not be active.
   - **ESP**: Enables Encapsulating Security Payload encryption for this tunnel.
   - **ESP with Authentication**: Enables Encapsulating Security Payload encryption with authentication for this tunnel.

7. If **ESP** or **ESP with Authentication** is enabled, select an **Encryption Algorithm** from the menu.

   - **DES**: This option selects the DES encryption algorithm, which requires 64-bit (16-character hexadecimal) keys.
   - **3DES**: This option selects the 3DES encryption algorithm, which requires 192-bit (48-character hexadecimal) keys. When creating keys for 3DES, the first 8 bytes cannot equal the second 8 bytes, and the second 8 bytes cannot equal the third 8 bytes.
   - **AES 128-bit**: This option selects the Advanced Encryption Standard algorithm in use with 128-bit (32-character hexadecimal) keys.
   - **AES 192-bit**: This option selects the Advanced Encryption Standard algorithm in use with 192-bit (48-character hexadecimal) keys.
   - **AES 256-bit**: This option selects the Advanced Encryption Standard algorithm in use with 256-bit (64-character hexadecimal) keys.

8. Provide keys for both **Inbound ESP Encryption Key** and **Outbound ESP Encryption Key**. The length of the keys is mandated by the selected encryption algorithm. These keys must match the opposite keys at the remote gateway. The outbound key here must match the inbound key at the remote gateway, and the inbound key here must match the outbound key at the remote gateway.

9. If **ESP with Authentication** is enabled, an authentication algorithm must be selected to be used with ESP from the **ESP Authentication Algorithm** menu.

   - **MD5**: Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) authentication keys.
   - **SHA1**: Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

10. If **ESP with Authentication** is enabled, specify both the **Inbound** and **Outbound ESP Authentication Keys**.

11. Provide two (up to) eight-character hexadecimal values used to identify the inbound and outbound security association created by the encryption algorithm. These values must match the reciprocal inbound/outbound SPI values configured on the remote security gateway, so the local inbound key must match the remote outbound key, and so on. This value should also be unique across all tunnels on the system.

12. Select **Ok** to return to the VPN screen.
Setting Up Automatic Key Exchange

1. Select the Auto (IKE) Key Exchange radio button.

2. Click the Automatic Key Exchange button to set up this security scheme and the following screen appears.

3. Forward secrecy is a key-establishment protocol that guarantees that the discovery of a session key or a long-term private key will not compromise the keys of any other sessions. Select Yes from the Use Perfect Forward Secrecy menu to enable this option. Select No to disable Perfect Forward Secrecy.

4. If Perfect Forward Secrecy is enabled, select an IKE Authentication Algorithm.

   **G1 - 768bit**  Diffie-Hellman Group 1 Authentication uses a 768 bit algorithm for key exchange. Somewhat faster than the 1024-bit algorithm, but secure enough in most situations

   **G2 - 1024bit**  Diffie-Hellman Group 2 Authentication uses a 1024 bit algorithm for key exchange. Somewhat slower than the 768-bit algorithm, but much more secure and a better choice for extremely sensitive situations.

5. In the Security Association Life Time field, enter a value (in minutes) that indicates how long the association will last before the VPN client will need to reauthenticate.

6. Select the type of authentication from the AH Authentication menu. AH provides data authentication and anti-replay services for the VPN tunnel.

   **None**  Disables AH authentication and the rest of the fields in this area will not be active.

   **MD5**  Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) authentication keys.

   **SHA1**  Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

7. Select the ESP Type from the menu.

   **None**  Disables ESP and the rest of the fields in this area will not be active.

   **ESP**  Enables Encapsulating Security Payload encryption for this tunnel.

   **ESP with Authentication**  Enables Encapsulating Security Payload encryption with authentication for this tunnel.
8. If ESP or ESP with Authentication is enabled, select an Encryption Algorithm from the menu.

- **DES**: This option selects the DES encryption algorithm, which requires 64-bit (16-character hexadecimal) keys.
- **3DES**: This option selects the 3DES encryption algorithm, which requires 192-bit (48-character hexadecimal) keys. When creating keys for 3DES, the first 8 bytes cannot equal the second 8 bytes, and the second 8 bytes cannot equal the third 8 bytes.
- **AES 128-bit**: This option selects the Advanced Encryption Standard algorithm in use with 128-bit (32-character hexadecimal) keys.
- **AES 192-bit**: This option selects the Advanced Encryption Standard algorithm in use with 192-bit (48-character hexadecimal) keys.
- **AES 256-bit**: This option selects the Advanced Encryption Standard algorithm in use with 256-bit (64-character hexadecimal) keys.

9. If ESP with Authentication is selected for the ESP type, select the authentication algorithm to be used with ESP from the ESP Authentication Algorithm menu.

- **MD5**: Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) authentication keys.
- **SHA1**: Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.

10. Select Ok to return to the VPN screen.

**Setting Up Internet Key Exchange (IKE)**

1. Select the Auto (IKE) Key Exchange radio button.
2. Click the IKE Settings button to set up the Internet Key Exchange and the following screen appears.
3. Select the **Operation Mode** for IKE. The Phase I protocols of IKE are based on the ISAKMP identity-protection and aggressive exchanges. IKE main mode refers to the identity-protection exchange, and IKE aggressive mode refers to the aggressive exchange.

<table>
<thead>
<tr>
<th>Operation Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main</strong></td>
<td>This is the standard IKE mode for communication and key exchange.</td>
</tr>
<tr>
<td><strong>Aggressive</strong></td>
<td>Aggressive mode is faster and less secure than Main mode. Identities are not encrypted unless public key encryption is used. The Diffie-Hellman group cannot be negotiated; it is chosen by the initiator. Also, the authentication method cannot be negotiated if the initiator chooses to use public key encryption.</td>
</tr>
</tbody>
</table>

4. Select the type of ID to be used for the WS 2000 end of the tunnel from the **Local ID Type** menu.

<table>
<thead>
<tr>
<th>Local ID Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP</strong></td>
<td>Select this option if the local ID type is the IP address specified as part of the tunnel.</td>
</tr>
<tr>
<td><strong>FQDN</strong></td>
<td>Select this item if the local ID type is a fully qualified domain name (such as sj.symbol.com). The setting for this field does not have to be fully qualified, it just must match the setting of the field for the Certificate Authority.</td>
</tr>
<tr>
<td><strong>UFQDN</strong></td>
<td>Select this item if the local ID type is a user unqualified domain name (such as <a href="mailto:johndoe@symbol.com">johndoe@symbol.com</a>). The setting for this field does not have to be unqualified, it just must match the setting of the field of the Certificate Authority.</td>
</tr>
</tbody>
</table>

5. If **FQDN** or **UFQDN** are selected, specify the data (either the qualified domain name or the user name) in the **Local ID Data** field.

6. Repeat steps 4 and 5 for the **Remote ID Type** and **Remote ID Data** fields.

7. Choose the authentication mode to be used with the IKE algorithm from the **IKE Authentication Mode** menu.

<table>
<thead>
<tr>
<th>IKE Authentication Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre-shared key</strong></td>
<td>This option requires that you specify an authentication algorithm and passcode to be used during authentication.</td>
</tr>
<tr>
<td><strong>RSA Certificates</strong></td>
<td>Select this option to use RSA certificates for authentication purposes. See <em>Managing Digital Certificates</em> to create and import certificates into the system.</td>
</tr>
</tbody>
</table>

8. IKE provides data authentication and anti-replay services for the VPN tunnel. Select the desired authentication methods from the **IKE Authentication Algorithm** menu.

<table>
<thead>
<tr>
<th>IKE Authentication Algorithm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MD5</strong></td>
<td>Enables the Message Digest 5 algorithm, which requires 128-bit (32-character hexadecimal) authentication keys.</td>
</tr>
<tr>
<td><strong>SHA1</strong></td>
<td>Enables Secure Hash Algorithm 1, which requires 160-bit (40-character hexadecimal) keys.</td>
</tr>
</tbody>
</table>

9. If **Pre-Shared Key** is the authentication mode, provide a key in the **IKE Authentication Passphrase** field. If **MD5** is the selected authentication algorithm, provide a 32-character hexadecimal key. If **SHA1** is the selected algorithm, provide a 40-character hexadecimal key.
10. Use the **IKE Encryption Algorithm** menu to select the encryption and authentication algorithms for this VPN tunnel.

- **DES**
  - This option selects the DES encryption algorithm, which requires 64-bit (16-character hexadecimal) keys.
- **3DES**
  - This option selects the 3DES encryption algorithm, which requires 192-bit (48-character hexadecimal) keys. When creating keys for 3DES, the first 8 bytes cannot equal the second 8 bytes, and the second 8 bytes cannot equal the third 8 bytes.
- **AES 128-bit**
  - This option selects the Advanced Encryption Standard algorithm in use with 128-bit (32-character hexadecimal) keys.
- **AES 192-bit**
  - This option selects the Advanced Encryption Standard algorithm in use with 192-bit (48-character hexadecimal) keys.
- **AES 256-bit**
  - This option selects the Advanced Encryption Standard algorithm in use with 256-bit (64-character hexadecimal) keys.

11. Specify a **Key Lifetime**, which is the number of seconds that the key is valid. At the end of the lifetime, the key is renegotiated between the two parties.

12. Select the **Diffie-Hellman Group** to use. The Diffie-Hellman key agreement protocol allows two users to exchange a secret key over an insecure medium without any prior secrets. Two algorithms exist, one 768-bit and one 1024-bit algorithm.

- **Group 1 - 768 bit**
  - Somewhat faster than the 1024-bit algorithm, but secure enough in most situations.
- **Group 2 - 1024 bit**
  - Somewhat slower than the 768-bit algorithm, but much more secure and a better choice for extremely sensitive situations.

13. If you wish to delete the IPSEC Security Association (SA) with the IKE Security Association (SA) choose **Yes** from the **Delete IPSEC SA with IKE SA** menu. Otherwise select **No**.

14. Click the **Ok** button to return to the VPN screen.

---

**VPN: Frequently Asked Questions**

**Disclaimer:** Using a VPN connection over the WAN interface is subject to the limitations of your Internet Service Provider.

**My tunnel works fine when I use the Subnet Access page to configure my firewall. Now that I use Advanced Subnet Access, my VPN no longer works. What am I doing wrong?**

VPN requires certain packets to be passed through the firewall. Subnet Access automatically inserts these rules for you when you do VPN. Using Advanced Subnet Access requires the following rules to be in effect for each tunnel.

An **allow** inbound rule:

- **Src** <Remote Subnet IP range>
- **Dst** <Local Subnet IP range>
- **Transport** ANY
- **Src port** 1:65535
An *allow* outbound rule:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dst port</td>
<td>1:65535</td>
</tr>
<tr>
<td>Rev NAT</td>
<td>None</td>
</tr>
</tbody>
</table>

For IKE, an *allow* inbound rule:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src</td>
<td>&lt;Remote Gateway IP address&gt;</td>
</tr>
<tr>
<td>Dst</td>
<td>&lt;Wan IP address&gt;</td>
</tr>
<tr>
<td>Transport</td>
<td>UDP</td>
</tr>
<tr>
<td>Src port</td>
<td>1:65535</td>
</tr>
<tr>
<td>Dst port</td>
<td>500</td>
</tr>
<tr>
<td>Rev NAT</td>
<td>None</td>
</tr>
</tbody>
</table>

These rules must be above (higher in priority than) any default or other rules that would process these packets differently.

**Do I need to add any special routes on the WS 2000 switch to get my VPN tunnel to work?**

No. Packets for VPN are tunneled directly to the Remote VPN gateway. As long as a route exists to the Remote VPN gateway, no other routes are required.

Clients, however, might need extra routing information to tell them to use the WS 2000 switch as the gateway to reach the remote subnet. This is only required if the clients are not using the WS 2000 switch as their default gateway.

**Can I setup the WS 2000 Wireless Switch so that clients can both access the WAN normally and use the VPN when talking only to specific networks?**

Yes. Only packets that are going from the defined local subnet to the remote subnet will be send through the VPN tunnel. All other packets will be handled by whatever firewall rules are set.
How do I specify which certificates to use from the WS 2000 certificate manager to be used for an IKE policy?

When generating a certificate to be used with IKE, you must use one of the following fields: IP address, Domain Name, or Email address. Also make sure that you are using NTP when attempting use the certificate manager. Certificates are time sensitive.

On the IKE configuration page, Local ID type refers to the way that IKE selects a local certificate to use.

- IP tries to match the local WAN IP to the IP addresses specified in a local certificate.
- FQDM tries to match the user entered local ID data string to the domain name field of the certificate.
- UFQDM tries to match the user entered local ID data string to the email address field of the certificate.

Remote ID type refers to the way you identify an incoming certificate as being associated with the remote side.

- IP tries the match the remote gateway IP to the IP addresses specified in the received certificate.
- FQDM tries to match the user entered remote ID data string to the domain name field of the received certificate.
- UFQDM tries to match the user entered remote ID data string to the email address field of the received certificate.

I am using a direct cable connection between by two VPN gateways for testing and cannot get a tunnel established, yet it works when I setup them up across another network or router. What gives?

The packet processing architecture of the WS 2000 VPN solution requires a WAN default gateway to work properly. When connecting two gateways directly, you really do not need a default gateway when the two addresses are on the same subnet. As a workaround, you can point the WS 2000 switch’s WAN default gateway to be the other VPN gateway, and vice-versa.

My WS 2000 switch is a DHCP client on my WAN interface. How can I setup a tunnel without knowing my WAN IP address?

First of all, one end of a VPN tunnel must have a static IP address. Assuming the other end of your VPN tunnel has a static IP, here is how you configure your WS 2000 switch to use a DHCP WAN address with VPN.

1. Your VPN tunnel entry must have the Local WAN IP set to 0.0.0.0.
2. If you are using the IKE, the Local ID type (and corresponding Remote ID type on the other end) cannot be set to IP, since the IP address is not known.

How can I setup the WS 2000 switch to accept VPN tunnels from gateways that have a DHCP WAN address?

To accept a VPN tunnel from a unknown (DHCP) address, the WS 2000 Wireless Switch operates in what is called responder-only mode. That is, it cannot initiate the VPN connection. It can only wait for a VPN connection to come in. Clients behind a responder-only cannot connect to the remote subnet until the remote subnet has connected to them.
To setup responder-only mode, set the Remote Gateway to \textbf{0.0.0.0}. If you are using IKE the following restrictions are in place:

- Remote ID type cannot be \textbf{IP}. We do not know the IP of the remote since it is DHCP.
- IKE Authentication Mode cannot be set to \textbf{PSK} if IKE mode is set to \textbf{Main Mode}.
- You may not use \textbf{xAuth} for this tunnel.

\textbf{I have two WS 2000 switches and both have DHCP WAN addresses. Is there any possible way to open a VPN tunnel between them?}

Yes, but the configuration for each tunnel will need to change anytime a WAN IP lease expires. You can make this work temporarily by performing the following steps:

1. Set \textbf{0.0.0.0} as the local WAN IP for each gateway.
2. Configure the opposite WS 2000 switch's current DHCP address as the Remote Gateway. This is the field that needs to change every time the DHCP addresses change.
3. If using IKE, you cannot use ID type IP for either Local or Remote ID types.

\textbf{I have set up my tunnel and the status still says “Not Connected.” What should I do now?}

VPN tunnels are negotiated on an as-needed basis. If you have not sent any traffic between the two subnets, the tunnel will not be established. Once a packet is sent between the two subnets, the VPN tunnel setup will occur.

\textbf{I still can’t get my tunnel to work after attempting to initiate traffic between the 2 subnets. What now?}

Here are some troubleshooting tips:

1. Verify that you can ping each of the remote gateway IP addresses from clients on either side. Failed pings can indicate general network connection problems.
2. Pinging the internal gateway address of the remote subnet should run the ping through the tunnel as well. Allowing you to test even if there are no clients on the remote end.
3. Verify that your WAN IP address is not DHCP. VPN requires a static WAN IP address to work.

\textbf{Configuring Content Filtering}

Content filtering allows system administrators to block specific commands and URL extensions from going out through the WS 2000 switch’s WAN port. This feature allows blocking up to 10 files or URL extensions and allows blocking of specific outbound HTTP, SMTP, and FTP requests.

To configure content filtering, select \textbf{Network Configuration} \rightarrow \textbf{Content Filtering} from the left menu.
1. Select the type of blocking for outbound HTTP requests. Check one or both of the options:

- **Web Proxy** This selection blocks the use of web proxies by clients.
- **ActiveX** This selection blocks all outgoing ActiveX requests by clients.

2. Enter the Outbound URL extensions to block. Do this by typing one URL extension or file name (filename.ext) per line. Use an asterisk (*) as a wildcard in place of the filename to block all files with a specific extension (for example *.exe).

3. Simple Mail Transport Protocol (SMTP) is the Internet standard for host-to-host mail transport. SMTP generally operates over TCP on port 25. SMTP filtering allows the blocking of any or all outgoing SMTP commands. Choose which SMTP commands to block from the list, by checking those commands to block.

- **HELO** (Hello) This command is used to identify the SMTP sender to the SMTP receiver.
- **MAIL** (Mail) This command initiates a mail transaction where mail data is delivered to one or more mailboxes on the local server.
- **RCPT** (Recipient) This command is used to identify a recipient of mail data.
- **DATA** (Data) This command tells the SMTP receiver to treat the following information as mail data from the sender.
- **QUIT** (Quit) This command tells the receiver to respond with an OK reply and then terminate communication with the sender.
- **SEND** (Send) This command initiates a mail transaction where mail is sent to one or more remote terminals.
- **SAML** (Send and Mail) This command initiates a mail transaction where mail data is sent to one or more local mailboxes and remote terminals.
4. Specify the outbound FTP actions that should get blocked by checking the FTP action to block. File Transfer Protocol (FTP) is the Internet standard for host-to-host mail transport. FTP generally operates over TCP on port 21.

**Storing Files**
Blocks the request to transfer files sent from the client across the switch’s WAN port to the FTP server.

**Retrieving Files**
Blocks the request to retrieve files sent from the FTP server across the switch’s WAN port to the client.

**Directory List**
Blocks requests to retrieve a directory listing sent from the client across the switch’s WAN port to the FTP server.

**Create Directory**
Blocks requests to create directories sent from the client across the switch’s WAN port to the FTP server.

**Change Directory**
Blocks requests to change directories sent from the client across the switch’s WAN port to the FTP server.

**Passive Operation**
Blocks passive mode FTP requests sent from the client across the switch’s WAN port to the FTP server.

5. Click the **Apply** button to save changes made on this screen.
Configuring DynDNS

The WS 2000 Wireless Switch provides support for using the DynDNS service. Dynamic DNS is a feature offered by www.dyndns.com which allows the mapping of domain names to dynamically assigned IP addresses. When the dynamically assigned IP address of a client changes that new IP address is sent to the DynDNS servers and traffic for the specified domain(s) is routed to the new IP address.

To view or change the DynDNS settings, select Network Configuration --> WAN --> DynDNS from the left menu.

Enabling and Configuring DynDNS

1. Click Enable button activate DynDNS configuration. Enabling Dyn DNS will allow domain name information to be updated when the IP address associated with that domain changes. In order for changes to go through a username, password and hostname must be specified in the fields below.

2. Enter a your DynDNS Username for the DynDNS account you wish to use for the WS2000.

3. Enter your Password for the DynDNS account you wish to use for the WS2000.

4. Enter your Hostname for the DynDNS account you wish to use for the WS2000.

Updating DynDNS

Click the Update DynDNS button to update the WS2000’s current WAN IP address with the DynDNS service. After you have clicked the Update DynDNS button, click the Show Update Response button to open a dialogue which displays the hostname, IP address and any messages received during the update from the DynDNS servers.
Wireless Configuration

Enabling Wireless LANs (WLANs) ................................................................. 5-3
WLAN Summary ......................................................................................... 5-3
AP Adoption Configuration ............................................................... 5-5

Configuring Wireless LANs ................................................................. 5-6
Configuring Wireless LAN Security ................................................. 5-7
  Selecting the Authentication Method .......................................................... 5-7
  Configuring 802.1x EAP Authentication .................................................. 5-8
  Configuring Kerberos Authentication .................................................... 5-9
  Setting the Encryption Method ............................................................. 5-10
  Configuring WEP Encryption ............................................................... 5-10
  Configuring WPA/WPA2-TKIP Encryption ............................................ 5-11
  Configuring WPA2-CCMP (802.11i) Encryption .................................... 5-12
  KeyGuard ................................................................................................. 5-13
  No Encryption ........................................................................................ 5-14
  IP Filtering .............................................................................................. 5-14
  Mobile Unit Access Control List (ACL) ................................................ 5-14

Configuring Access Ports ...................................................................... 5-15
Setting Default Access Port Settings ......................................................... 5-18
  Common Settings to All Radio Types ....................................................... 5-19
  Radio-Specific Settings ............................................................................ 5-21
Advanced Access Port Settings ................................................................. 5-22
  Radio Settings ........................................................................................ 5-24
  Antenna Settings .................................................................................... 5-24
  Advanced Properties .............................................................................. 5-25
Quality of Service Configuration ................................................................. 5-26
  Setting the Bandwidth Share Mode ........................................................ 5-27
Configuring Voice Prioritization and Multicast Address Settings ........................................... 5-28
Configuring WME Profiles ........................................................................................................ 5-28
  To Add a WME Profile ............................................................................................................ 5-29
WME Priority Conversion ........................................................................................................... 5-30
Assigning WME Profiles to WLANs ....................................................................................... 5-30
Configuring WME Traffic Classification .................................................................................. 5-31
Setting Up Port Authentication for AP 300 Access Ports ......................................................... 5-33
Rogue Access Point (Port) Detection .......................................................................................... 5-33
  Setting Up the Detection Method ........................................................................................... 5-34
Defining and Maintaining Approved AP List Rules ................................................................. 5-35
Examine the Approve and Rogue Access Ports ..................................................................... 5-35
Setting SNMP Traps for Rogue APs ......................................................................................... 5-38
Configuring Wireless Intrusion Protection System (WIPS) ..................................................... 5-38
Enabling Wireless LANs (WLANs)

The WS 2000 Wireless Switch works either in a wired or wireless environment; however, the power of the switch is associated with its support of wireless networks. In order to use the wireless features of the switch, the administrator needs to enable one, two, or three wireless LANs (WLANs).

To start the WLAN configuration process, select the Network Configuration --- Wireless item from the left menu. The following Wireless summary screen appears.

WLAN Summary

The top portion of the window displays a summary of the WLANs that are currently defined. This is the screen in which the administrator can enable or disable a WLAN. By default, eight WLANs will be listed WLAN1, WLAN2, WLAN3, WLAN4, WLAN5, WLAN6, WLAN7 and WLAN8 however, only WLAN1 will be enabled.

1. To enable a WLAN, check the checkbox to the left of the WLAN name. When the administrator enables one of the WLANs, the name of an enabled WLAN shows up as an item on the list of WLANs that reside under Wireless in the left menu (after clicking the Apply button). When an administrator disables a WLAN, it disappears from the menu tree. A WLAN cannot be fully configured unless it is enabled.
2. To enable a WLAN as a hotspot, check the box marked **Hotspot** next to the WLAN(s) you wish to use as a hotspot. To configure hotspot settings see *Chapter 8, Configuring HotSpot*.

3. Assign the enabled WLANs descriptive names. The administrator can change the name of any of the WLANs in the **Name** field. This change will affect several other screens and the interface will change the name in the left menu tree.

4. By default, the switch assigns consecutive Extended Service Set Identification (ESSIDs). This is the name that users will see when accessing the wireless network. The **ESSID** can be given any recognizable alphanumeric string up to 32 characters in length.

5. An icon of a lock will appear under the **Security** heading if any wireless encryption or authentication is enabled for the WLAN.

The current settings for the associated Subnet and adopted Access Ports are also displayed on this screen; however, the screen associated with each WLAN (under **Network Configuration --> Wireless**) is where the settings and rules for adopting Access Ports can be modified.

### WEP Shared Mode

The **WEP Shared Mode** checkbox enables WEP Shared secret key authentication. IEEE802.11 defines two types of Authentication service: Open System and Shared Key. In Shared Key authentication service prior to Association phase STAs need to authenticate itself using the shared secret key. This authentication scheme is only available if the WEP option is implemented. The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEE802.11.

### SIP CAC Mode

The **SIP CAC Mode** checkbox enables or disables the SIP Call Admission Control feature which when used in conjunction with compatible VoIP hardware will test for network congestion before allowing VoIP calls to connect. This can help ensure call quality and connection when making VoIP calls.

### MU Inactivity Timeout and WEP Shared Mode Configuration

<table>
<thead>
<tr>
<th>MU Inactivity Timeout</th>
<th>Set the amount of time, in minutes, before inactive mobile units are disassociated with the WLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP Shared Mode</td>
<td>Enables WEP Shared secret key authentication. IEEE802.11 defines two types of Authentication service: Open System and Shared Key. In Shared Key authentication service prior to Association phase STAs need to authenticate itself using the shared secret key. This authentication scheme is only available if the WEP option is implemented. The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEE802.11.</td>
</tr>
</tbody>
</table>
**AP Adoption Configuration**

The AP Adoption Configuration screen allows for setting up default Access Port adoption rules as well as a deny list to prevent the adoption of specific Access Ports.

**AP Deny List**

The AP Deny List allows you to prevent individual Access Ports from associating with the switch. For each Access Port you wish to deny click the Add button and enter its MAC Address into the field provided.

To add an AP to the AP Deny List:
1. Click the Add button located below the AP Deny List table. A new row will be added to the table.
2. Enter the MAC Address of the Access Port you wish to deny.
3. Click the Apply button to save the changes.

**Access Port Adoption**

Use this list to adopt detected Access Ports and to assign them to a particular WLAN. The switch can adopt up to six Access Ports at a time, but the list of allowed Access-Port addresses (displayed in this area) can exceed six in number. A dual-radio 802.11a/b Access Port counts as one Access Port with respect to the maximum allowed; however, each radio will be listed as a separate Access Port.

This adoption list identifies each Access Port by its Media Access Control (MAC) address. This address is the Access Port’s hard-coded hardware number that is printed on the bottom of the device. An example of a MAC address is 00:09:5B:45:9B:07.

1. To adopt an Access Port, click the Add button to add a new criteria line to the table.
2. Specify the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start MAC</td>
<td>This field contains the lowest value in a range of MAC addresses that will use this particular adoption criteria. To specify a single MAC address instead of a range, enter it in this field as well as the End MAC field.</td>
</tr>
<tr>
<td>End MAC</td>
<td>This field contains that highest number in a range of MAC addresses that will use this particular adoption criteria. If this value is empty, the Access Port adopted by this criteria must match the Start MAC field exactly.</td>
</tr>
<tr>
<td>WLAN columns</td>
<td>The next four columns are associate with the eight WLANs that are shown in the upper portion of the screen. To the left, specify a range of Access Port MAC address for adoption. Then, click the checkboxes of the WLANs that need ability to adopt the Access Ports in the specified range.</td>
</tr>
</tbody>
</table>

The default setting for the switch has both the Start MAC and End MAC addresses set to “ANY”, and all enabled WLANs checked. This setting allows all the WLANs to adopt any Access Port that it detects, automatically.

3. Up to 20 entries can be added to the Access Port Adoption list. Click the Apply button to save changes.
Configuring Wireless LANs

The Network Configuration -> Wireless window (covered in Enabling Wireless LANs (WLANs)) is where WLANs are enabled; however, the Network Configuration -> Wireless -> <WLAN name> screen is where the administrator configures each WLAN, after it is enabled. The screen is titled with the name of the WLAN.

Within the WLAN window, the administrator changes both standard and advanced configuration features of the WLAN.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Rename the WLAN in this field, if desired. Character spaces are allowed. This change affects several other screens and the interface will also change the name in the left menu tree. Symbol Technologies recommends the use of descriptive names for WLANs.</td>
</tr>
<tr>
<td>ESSID</td>
<td>Specify an Extended Service Set Identification (ESSID) for the WLAN. The ESSID is a alphanumeric string up to 32 characters. Its purpose is to identify one or more Access Ports that are associated with the WLAN.</td>
</tr>
<tr>
<td>Subnet</td>
<td>This field provides a pull-down menu of the enabled subnets. Select the subnet to associate with the current WLAN.</td>
</tr>
<tr>
<td>VLAN</td>
<td>This is a read-only field which displays the VLAN ID of the VLAN associated with this WLAN. This setting can be changed on the VLAN Configuration screen.</td>
</tr>
</tbody>
</table>

Configuring Advanced WLAN Settings

The lower section of the WLAN screen provides several settings that the administrator might need to modify; however, the default settings are usually sufficient for most installations.

1. Check the Disallow MU to MU Communications box to enable a communication block between mobile units (MUs) using this WLAN. Such communication might be a security issue, for example, on a corporate network. Leave this checkbox unchecked (default setting) to allow MU-to-MU communications on this WLAN.
2. Check the **Answer Broadcast ESS** checkbox to enable adopted Access Ports to transmit the WLAN’s Extended Service Set Identification (ESSID). The purpose of allowing WLANs to answer the broadcast ESS is to identify Access Ports that are associated with the WLAN. This might be appropriate, for example, in a customer environment, such as a “hot spot.” Disable this option if broadcasting the WLAN’s ESSID poses a security risk, such as with a private, corporate network. The default setting is unchecked.

3. Click the **Apply** button to save changes.

For more advanced WLAN settings see *Quality of Service Configuration* or *Configuring Wireless LAN Security* later in this chapter.

**Configuring Wireless LAN Security**

The WS 2000 Wireless Switch allows the administrator to set the type and level of security for each WLAN. These security measures do not control communications from the WAN; instead, they control communication from the clients within the WLAN.

In the **Network Configuration --> Wireless --> <WLAN name> --> <WLAN Name> Security** screen, the administrator can set the user authentication method and the encryption method, as well as define a set of rules that control which MUs can communicate through the WLAN.

**Selecting the Authentication Method**

![Authentication Methods](image)

The authentication method sets a challenge-response procedure for validating user credentials such as username, password, and sometimes secret-key information. The WS 2000 Wireless Switch provides two methods for authenticating users: **802.1x EAP** and **Kerberos**. The administrator can select between these two methods. If WLAN security is not an issue, an administrator can decide not to enable authentication (**No Authentication**), because authentication protocols create overhead for the switch’s processor.
Configuring 802.1x EAP Authentication

The IEEE 802.1x is an authentication standard that ties EAP to both wired and wireless LAN applications. EAP provides effective authentication with or without IEEE 802.1x Wired Equivalent Privacy (WEP) encryption, or with no encryption at all. EAP supports multiple authentication measures. It requires that the site have an authentication (Remote Dial-In User Service, or RADIUS) server on the wired side of the Access Port. All other packet types are blocked until the authentication server verifies the client’s identity. To set up 802.1x EAP authentication:

1. On the Network Configuration --> Wireless --> <WLAN Name> --> <WLAN Name> Security screen, select the 802.1x EAP radio button to enable the 802.1x Extensible Authentication Protocol (EAP).
2. Click the 802.1x EAP Configuration button to display a sub-screen for specific authentication settings.

3. The administrator is required to specify the RADIUS Server Address of a primary RADIUS server for this type of authentication to work. Providing the IP address of a secondary server is optional. The secondary server acts as a failover server if the switch cannot successfully contact the primary server.
4. Specify the port on which the primary RADIUS server is listening in the RADIUS Port field. Optionally, specify the port of a secondary (failover) server. Older RADIUS servers listen on ports 1645 and 1646. Newer servers listen on ports 1812 and 1813. Port 1645 or 1812 is used for authentication. Port 1646 or 1813 is used for accounting. The ISP or a network administrator can confirm the appropriate primary and secondary port numbers.
5. The administrator can specify a RADIUS Shared Secret for authentication on the primary RADIUS server. Shared secrets are used to verify that RADIUS messages (with the exception of the Access-Request message) are sent by a RADIUS-enabled device that is configured with the same shared secret. The shared secret is a case-sensitive string that can include letters, numbers, or symbols. Make the shared secret at least 22 characters long to protect the RADIUS server from brute-force attacks.

Reauthentication Settings

6. Check the Enable Reauthentication checkbox to enable this authentication method.
7. In the **Period** field, set the EAP reauthentication period to match the appropriate level of security. A shorter time interval (~30 seconds or longer) provides tighter security on this WLAN’s wireless connections. A longer interval (5000-9999 seconds) relaxes security on wireless connections. The reauthentication period setting does not affect a wireless connection’s throughput. The engaged Access Port continues to forward traffic during the reauthentication process.

8. In the **Max. Retries** field, set the maximum number of retries for a client to successfully reauthenticate after failing to complete the EAP process. If the mobile unit fails the authentication process in specified number of retries, the switch will terminate the connection to the mobile unit.

**Advanced Settings**

9. The **MU Quiet Period** field allows the administrator to specify the idle time (in seconds) between a mobile unit’s authentication attempts, as required by the server.

10. The **MU Timeout** field allows the administrator to specify the time (in seconds) for the mobile unit’s retransmission of EAP-Request packets.

11. The **MU Tx Period** field allows the administrator to specify the time period (in seconds) for the server’s retransmission of the EAP-Request/Identity frame.

12. The **MU Max Retries** field allows the administrator to set the maximum number of times for the mobile unit to retransmit an EAP-Request frame to the server before it times out the authentication session. Note that this is a different value from the Max Retry field at the top of the window.

13. The **Server Timeout** field indicates the maximum time (in seconds) that the switch will wait for the server’s transmission of EAP Transmit packets.

14. The **Server Max Retries** field allows the administrator to set the maximum number of times for the server to retransmit an EAP-Request frame to the client before it times out the authentication session. Note that this is a different value from the **Max. Retries** field at the top of the window.

**Note**

*When changing the Server Max Retries setting to anything other than the default value, there is a known bug that can cause RADIUS authentication to fail.*

**RADIUS Client Accounting and Syslog Setup**

15. RADIUS accounting allows for the delivery of accounting packets from a Network Access Server (NAS) to the RADIUS accounting server where the information is stored. To enable this feature, click the **Enable Accounting** box.

16. If accounting is enabled, enter the maximum amount of time a client will wait for an acknowledgement from the RADIUS accounting server before resending the accounting packet in the **MU Timeout** field. In the **Retries** field, enter the maximum number of times for the client will resend the accounting packet to the RADIUS accounting server before giving up.

17. To enable 802.1x EAP message logging to an external Syslog server, check the **Enable Syslog** box and then specify the IP address of the syslog server in the **Syslog Server IP** field.

18. Click the **Ok** button to save changes.

**Configuring Kerberos Authentication**

Kerberos provides a strong authentication method for client/server applications by using secret-key cryptography. Using this protocol, a client can prove their identity to a server (and vice versa) across an insecure network connection. After a client and server use Kerberos to prove their identity, they can encrypt all communications to assure privacy and data integrity.

1. Select the **Kerberos** radio button to enable Kerberos authentication.
2. Click the **Kerberos Configuration** button to display a sub-screen for authentication settings.

3. A realm name functions similarly to a DNS domain name. In theory, the realm name is arbitrary; however, in practice a Kerberos realm is typically named using an uppercase version of the DNS domain name that is associated with hosts in the realm. Specify a realm name that is case-sensitive, for example, MyCompany.com.

4. Specify a **Username** for the Kerberos configuration.

5. Specify a **Password** for the Kerberos configuration.

   The Key Distribution Center (KDC) implements an authentication service and a ticket granting service, whereby an authorized user is granted a ticket that is encrypted with the user’s password. The KDC has a copy of every user password.

6. Specify a server IP address and a port to be used as the **Primary KDC**.

7. Optionally, specify a **Backup KDC** server by providing the IP address and port.

8. Optionally, specify a **Remote KDC** server by providing the IP address and port.

9. Make sure that NTP is enabled (go to **System Configuration** --> **NTP Servers** from the left menu). NTP is required for Kerberos Authentication. For more information, see *Specifying a Network Time Protocol (NTP) Server*.

10. Click **Ok** when done.

**Setting the Encryption Method**

Encryption applies a specific algorithm to data to alter its appearance and prevent unauthorized reading. Decryption applies the algorithm in reverse to restore the data to its original form. Sender and receiver employ the same encryption/decryption method.

The WS 2000 Wireless Switch provides four methods for data encryption: WEP, KeyGuard, WPA-TKIP, and WPA2-CCMP (802.11i). The WPA-TKIP and KeyGuard methods use WEP 104-bit key encryption. WPA-TKIP offers the highest level of security among the encryption methods available with the switch.

**Configuring WEP Encryption**

Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN. WEP might be all that a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. The existing 802.11 standard alone offers administrators no effective method to update keys. Key changes require the manual reconfiguration of each Access Port. An unauthorized person with a sniffing tool can monitor a network for less than a day and decode its encrypted messages.

WEP is available in two encryption modes: 40 bit (also called 64-bit) and 104 bit (also called 128 bit). The 104-bit encryption mode provides a longer algorithm that takes longer to decode than that of the 40-bit encryption mode.
The WEP 128 encryption mode allows devices using 104-bit key and devices using 40-bit keys to talk to each other using 40-bit keys, if the 104-bit devices permit this option.

1. Choose between the WEP 64 (40-bit key) and WEP 128 (104-bit key) option by selecting the appropriate radio button.
2. To use WEP encryption with the No Authentication selection, click the WEP Key Settings button to display a sub-screen for entering keys.
3. When finished, click the Ok button to close this screen.
4. Specify a Pass Key and click the Generate button. The pass key can be any alphanumeric string. The switch, other proprietary routers, and Symbol cards in mobile units (MUs) use an algorithm to convert an ASCII string to the same hexadecimal number, but this conversion is not required for a wireless connection.
5. Use the Key #1-4 fields to specify key numbers that use 26 hexadecimal characters. Select one of these keys for active use by selecting its radio button. Four different keys can be specified, allowing each WLAN to have a different key.
6. Click the Apply button on the WLAN Security screen to save changes.

Configuring WPA/WPA2-TKIP Encryption

Wi-Fi Protected Access (WPA) is specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i. This security standard provides more sophisticated data encryption than WEP. WPA is designed for corporate networks and small-business environments where more wireless traffic allows quicker discovery of encryption keys by an unauthorized person.

WPA’s encryption method is Temporal Key Integrity Protocol (TKIP). TKIP addresses WEP weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check, and an extended initialization vector. WPA/WPA2 also provides strong user authentication that is based on 802.1x EAP.

1. Select the WPA/WPA2-TKIP radio button to enable Wi-Fi Protected Access (WPA) with Temporal Key Integrity Protocol (TKIP).
2. To use WPA/WPA2-TKIP encryption with 802.1x EAP authentication or the No Authentication selection, click the WPA/WPA2-TKIP Settings button to display a sub-screen for key and key rotation settings.
3. To Enable WPA2 check the Use WPA2 checkbox to use WPA2 encryption in conjunction with WPA-TKIP.
4. If using WPA2 in conjunction with 802.1x EAP authentication you may enable Pre-Authentication and Opportunistic Key Caching by checking the corresponding checkboxes.
5. Check the Broadcast Key Rotation checkbox to enable or disable the broadcasting of encryption-key changes to mobile units.

6. Specify a time period in seconds for broadcasting encryption-key changes to mobile units. Set key broadcasts to a shorter time interval (at least 300 seconds) for tighter security on this WLAN’s wireless connections. Set key broadcasts to a longer time interval (at most, 80,000 seconds) to relax security on wireless connections.

A Pre-Shared Key (PSK) is an Internet Protocol security (IPSec) technology that uses a shared, secret key for authentication in IPSec policy. IPSec is a set of industry-standard, cryptography-based protection services and protocols. IPSec protects all protocols in the TCP/IP protocol suite and Internet communications by using Layer Two Tunneling Protocol (L2TP). Use pre-shared key authentication only in a WLAN environment intended for relaxed security. The administrator can specify the key either as an ASCII passphrase or as a 128-bit key. All WLAN clients must use the same PSK.

7. Select either the ASCII Passphrase or 256-bit Key radio button.

8. If ASCII Passphrase is selected, specify a 8 to 63 character alphanumeric string. The alphanumeric string allows character spaces. The switch converts the string to a numeric value.

9. To use the 256-bit Key option, enter 16 hexadecimal characters into each of four fields.

10. Click the Ok button to return to the WLAN security screen.

11. Click the Apply button on the WLAN Security screen to save changes.

**Configuring WPA2-CCMP (802.11i) Encryption**

WPA2 is a newer 802.11i standard that provides even stronger wireless security than WiFi Protected Access (WPA) and WEP. CCMP is the security protocol used by AES. It is the equivalent of TKIP in WPA. CCMP computes a Message Integrity Check (MIC) using the well known, and proven, Cipher Block Chaining Message Authentication Code (CBC-MAC) method. Changing even one bit in a message produces a totally different result.

WPA2-CCMP is based upon the concept of a robust security network (RSN), which defines a hierarchy of keys that have a limited lifetime, similar to TKIP. Also like TKIP, the keys that the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is encryption that is extremely secure.

1. Select the WPA2-CCMP radio button to enable Wi-Fi Protected Access (WPA) with Temporal Key Integrity Protocol (TKIP).

2. To use WPA-TKIP encryption with 802.1x EAP authentication or the No Authentication selection, click the WPA-TKIP Settings button to display a sub-screen for key and key rotation settings.
3. Check the **Broadcast Key Rotation** checkbox to enable or disable the broadcasting of encryption-key changes to mobile units.

4. Specify a time period in seconds for broadcasting encryption-key changes to mobile units. Set key broadcasts to a shorter time interval (at least 300 seconds) for tighter security on this WLAN's wireless connections. Set key broadcasts to a longer time interval (at most, 200,000 seconds) to relax security on wireless connections.

5. Select either the **ASCII Passphrase** or the **256-bit Key** radio button.

6. If **ASCII Passphrase** is selected, specify a 8 to 63 character ASCII string. The ASCII string allows character spaces. The switch converts the string to a numeric value.

7. To use the **256-bit Key** option, enter 16 hexadecimal characters into each of four fields.

8. **WPA2-CCMP Mixed Mode** enables WPA2-CCMP and WPA-TKIP Clients to operate simultaneously on the network. Enabling this option allows backwards compatibility for clients that support WPA-TKIP but do not support WPA2-CCMP.

9. The **Fast Roaming** area provides two fields. Enabling **Pre-Authentication** enables a client associated with one Access Port to carry out an 802.1x authentication with another Access Port before it roams over to it. The WS 2000 switch will cache the keying information of the client until it roams to the new Access Port. This enables the roaming the client to start sending and receiving data sooner by not having to do 802.1x authentication after it roams. Enabling **Opportunistic Key Caching** allows the switch to use a Pairwise Master Key (PMK) derived with a client on one Access Port with the same client when it roams over to another Access Port. Upon roaming the client does not have to do 802.1x authentication and can start sending/receiving data sooner.

10. Click the **Ok** button to return to the WLAN security screen.

11. Click the **Apply** button on the WLAN Security screen to save changes.

---

**KeyGuard**

KeyGuard is a proprietary encryption method developed by Symbol Technologies. KeyGuard is Symbol’s enhancement to WEP encryption and can work with any WEP device. This encryption method rotates WEP keys for devices that support the method. This encryption implementation is based on the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11i.

1. Select the **KeyGuard** radio button to enable the KeyGuard encryption method.

2. To use KeyGuard encryption with the No Authentication selection, click the **MCM Key Settings** button to display a sub-screen for entering keys. (Note that these are the same keys specified for WEP encryption.

3. Select a **Key #** radio button to enter to enter or change a passkey.

4. Specify a pass key string in the **Pass Key** field. The pass key can be any alphanumeric string. The switch, other proprietary routers, and Symbol cards in mobile units (MUs) use an algorithm to convert an ASCII string to the same hexadecimal number, but this conversion is not required for a wireless connection.

5. Click the **Generate** button and the pass key will be entered in the appropriate Key # field.

6. When finished entering pass keys, click the **Ok** button to close this screen.

7. Click the **Apply** button on the WLAN Security screen to save changes.
No Encryption

If No Authentication is selected, the No Encryption radio button can disable encryption on this WLAN. If security is not an issue, this setting avoids the overhead that an encryption protocol demands on the switch’s processor.

IP Filtering

IP based filtering allows administrators to configure Incoming and Outgoing IP filtering policies on packets within the same Subnet / WLAN and between wired and wireless hosts.

To Configure IP Filtering for the WLAN:
1. Check the box marked Enable IP Filtering to turn on IP Address based filtering for inbound and outbound traffic on the WLAN.
2. Click the IP Filtering button to display a sub-screen for filtering settings on the WLAN.
3. Click the Add button to create a new filter in the table. The new filter can then be edited by clicking on the corresponding fields in the table.
4. Click the Filter Name and provide a name or edit an existing name for the filter. The Filter Name should be unique for each filter rule that is added.
5. Click the Direction field for the corresponding filter to specify if the filter applies to traffic Inbound or Outbound on the WLAN. Inbound traffic refers to traffic coming from an MU to the AP. Outbound traffic refers to the traffic going from the AP to an MU.
6. Click the Action field for the corresponding filter to specify if the filter will be set to Allow or Deny traffic in the chosen direction. Allow will enable traffic to pass freely in the specified direction between the APs and MUs. Deny will prevent traffic from passing in the specified direction between the APs and MUs.
7. Check the Default Inbound Deny box to prevent traffic inbound on the WLAN from passing freely from the MUs to the APs.
8. Check the Default Outbound Deny box to prevent traffic outbound on the WLAN from passing freely from the APs to the MUs.
9. Click the OK button to return to the WLAN Security screen.
10. Click the Apply button the WLAN Security screen to commit the changes to the system.

Mobile Unit Access Control List (ACL)

Use this list to specify which mobile units can or cannot gain access to the WLAN. The list employs an adoption rule for allowing or denying specific mobile units by way of exception.

1. Select Allow or Deny from the pull-down menu. This rule applies to all mobile units except those listed in the table. If Allow is visible, the access criteria (MAC addresses) will be used to indicated which mobile units will be allowed access to the Access Port. If Deny is visible, the access criteria will be used to indicated which mobile units should not be allowed access.
2. Click the Add button to add a new entry to the list.
3. Each entry in the table specifies one or more MAC address to be used to match with a mobile unit’s MAC address that is attempting to gain access to the WLAN. Specify a single address (by specifying Start Address only) or a range of MAC access (by using both the Start Address and the End Address).

For example, if Allow is selected, all mobile units that match any of the specified MAC addresses or MAC address ranges in the table can be adopted by the WLAN. If Deny is selected, all mobile units that match any of the specified MAC addresses or MAC address ranges in the table cannot be adopted by the WLAN.

4. Click the Apply button to save changes.

**Configuring Access Ports**

The WS 2000 Wireless Switch automatically detects Access Ports when they are attached to one of the switch’s LAN ports. When the switch starts communication with an Access Port that can be adopted by the switch, it uploads the firmware appropriate for the Access Port. At this time, the Access Port becomes active. The switch also automatically adds the Access Port to the list of known ports under the left menu item, *Network Configuration* --> *Wireless* --> *Access Ports* --> <Access Port Name>.

For an Access Port to be adopted by the WS 2000 Wireless Switch, three things must be configured:

1. The **Country** field in the System Settings screen must be set.
2. The Access Port’s **MAC Address** must be set as one of the addresses that can be adopted by one of the enabled WLANs.
3. A WLAN that can adopt Access Port must be associated with an enabled subnet. (See *Configuring Wireless LANs*.)

The switch can adopt up to six Access Ports at a time, but the number of Access Ports listed can exceed six in number. A dual-radio 802.11a/b Access Port counts as one Access Port with respect to the maximum allowed; however, each radio will be listed as a separate Access Port in the list of Access Ports.
The switch creates a default name for a newly found switch consisting of “AP” and a unique number. During this detection process, the switch collects the following information from the Access Port:

**MAC address**
Each Access Port has a unique Media Access Control (MAC) address by which it is identified. This address is burned into the ROM of the Access Port. Also, this address appears on a sticker attached to the bottom of the Access Port.

**Serial Number**
Each Access Port has a unique serial number printed on the device at the time of manufacturing. This address is burned into the ROM of the Access Port.

**AP Type**
This field lists the model number of the Access Port (i.e. AP 100, AP 300)

**Radio type**
This field indicates the wireless protocol that the Access Port follows. The WS 2000 Wireless Switch supports 802.11b and 802.11 a/b dual-radio Access Ports.

**Adopted by**
This field contains a list of defined WLANs that have adopted this Access Port (see Configuring Wireless LANs and Access Port Adoption for the process of adopting an Access Port).

The switch also sets several default values for the channel and the power level based upon the Location information set in the System Settings screen and upon settings in the Access Port Default Settings screen for the radio type.

The WS 2000 Wireless Switch GUI also allows the administrator to refine the basic Access Port configuration that is set at the point of detection. To examine or change that information:

1. Select **Network Configuration --> Wireless --> Access Ports** from the left menu and then click the + to the left of the menu item. The detected Access Ports will be listed under the menu item, with the radio type listed in brackets (for example, [B]).

2. Select the Access Port item to examine or modify. There are two ways to distinguish between Access Ports when they are labeled with the default “AP#” name.
   - Look on the bottom of the Access Ports and take note of the MAC address (which looks like AA:BB:CC:DD EE:FF) and compare it with the MAC address in the Access Port windows.
   - Note the order in which Access Ports were plugged into the switch. The Access Port numbers are assigned in order, starting with AP1. When an Access Port has multiple radios, each radio is assigned an AP number.
The following screen is displayed with the settings for the selected Access Port.

3. From this screen, the administrator can change several pieces of information about each Access Port.

   - **Name**: Administrators can change the names of the Access Ports from Access Port# to something much more descriptive, so that they can easily identify which Access Port is being referenced in the various screens and in the left menu. The name is limited to a string of 13 characters.

   - **Location**: This field is a memory aid for the administrator. Enter text that describes where the Access Port is physically located. The name is limited to a string of 13 characters.

   - **Adopt this Access Port**: This button opens a dialogue box which allows you to adopt an Access Port into one or more WLANs.

4. In the **Radio Settings** area, the administrator can specify a number of characteristics of the radio.

   - **Placement**: Select either **Indoors** or **Outdoors** from the Placement pop-up menu. The setting will affect the selection available for several of the other advanced settings.
5. Click **Apply** to save changes.

This screen also provides the ability to change several advanced settings for the Access Ports. For more information, see *Advanced Access Port Settings*.

### Setting Default Access Port Settings

The WS 2000 Network Switch can support up to six Access Port. These Access Ports can be either a 802.11a or 802.11b radio type. When an Access Port associates with the wireless switch, the initial settings for that Access Port are taken from the Default Access Port Setting for the appropriate radio type. Select **Network Configuration** --> **Wireless** --> **Access Ports** to see the list of Default radio settings. Then select the Default settings screen for the appropriate radio type: one of **802.11a Defaults**, **802.11b Defaults**, or **802.11b/g Defaults**.

**Channel**

Specify a channel for communications between the Access Port and mobile units. The range of legally approved communications channels varies depending on the installation location. It is best to use a different channel number for each Access Port. Communications will be the clearest for nearby Access Ports if the channel numbers are 5 numbers apart (1, 6, 11).

**Power Level**

Specify a **Power Level** in milliwatts (mW) for RF signal strength. The optimal power level is best determined by a site survey prior to installation. Available settings include 1, 5, 15, 30, and 100. Consult the site survey for recommendations of the power level.

Set a higher power level to ensure RF coverage in WLAN environments that have more electromagnetic interference or greater distances between the Access Port and mobile units. Decrease the power level according to the proximity of other Access Ports. Overlapping RF coverage may cause lost packets and difficulty for roaming mobile units trying to engage an Access Port.
**Common Settings to All Radio Types**

Some of the settings are common to all three radio types.

**Channel Selection Mode**
Click the Channel Selection Mode button to configure how channel selection for the selected AP is determined. A window will open with the following selections:

**User Selection**
Select this radio button to enable manual channel selection. With this mode, channel can be selected from a drop down list in the parent window.

**Uniform Spreading (AP 300 Only)**
Select this radio button to enable the Uniform Spreading feature of the AP 300. To comply with Dynamic Frequency Selection (DFS) requirements in the European Union, the 802.11a radio on AP 300 Access Ports will come up on a random channel each time it is powered on.

**Note:** With this mode, channel can not be manually selected.

**Automatic Mode (Automatic Channel Selection)**
Select this radio button to enable Automatic Channel Selection (ACS) feature of WS2000/AP300. With this mode, the AP will scan the available channels and select the one in which least number of beacons is heard.

**Note:** With this mode, channel can not be manually selected.

**Placement**
Select either **Indoors** or **Outdoors** from the Placement pop-up menu. This setting will affect the power levels and channels available for selection.

**Channel**
Select a channel number from the Channel drop-down menu on which the Access Port should communicate with associated MUs.

*The available channels vary depending on the location setting of the switch.*

**Power Level**
Select a power level from the Power Level drop-down menu that will be used for radio communications between the Access Port and the MUs.

Set a higher power level to ensure RF coverage in WLAN environments that have more electromagnetic interference or greater distances between the Access Port and mobile units (MUs). Decrease the power level according to the proximity of other Access Ports. Overlapping RF coverage may cause lost packets and difficulty for roaming MUs trying to engage an Access Port.

**Antenna Diversity**
Use the drop-down menu to configure the Antenna Diversity settings for Access Ports that use external antennas.

**Full Diversity:** Utilizes both antennas to provide antenna diversity

**Primary Only:** Enables only the primary antenna

**Secondary Only:** Enables only the secondary antenna

*Antenna Diversity should only be enabled if the Access Port has two matching external antennas.*
**RTS Threshold**

Set the Request to Send Threshold (RTS Threshold) by specifying a number.

RTS is a transmitting station's signal that requests a Clear To Send (CTS) response from a receiving station. This RTS/CTS procedure clears the air when many mobile units (MUs) are contending for transmission time. Modifying this value allows the administrator to control the number of data collisions and thereby enhance communication with nodes that are hard to find because of other active nodes in the transmission path.

In this field, the administrator can specify a Request To Send (RTS) threshold (in bytes) for use by the WLAN's adopted Access Ports.

This setting initiates an RTS/CTS exchange for data frames that are larger than the threshold, and sends (without RTS/CTS) any data frames that are smaller than the threshold.

Consider the tradeoffs when setting an appropriate RTS threshold for the WLAN's Access Ports. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of the additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.

A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.

**Set Rates**

Click the **Set Rates** button to open a sub-screen where the default **Basic Rates** and **Supported Rates** for 802.11b/g Access Ports can be set.

A list of available Basic and Supported rates for the radio are listed in two columns with checkboxes next to each rate. Selecting a rate as a Basic Rate automatically selects that rate as a Supported Rate and disables the option in the Supported Rates column.

**Beacon Settings**

Set the Access Port beacon settings by clicking on the **Beacon Settings** button.

Set the following beacon values.

**Beacon Interval**—A beacon is a packet broadcast by the adopted Access Ports to keep the network synchronized. Included in a beacon is information such as the WLAN service area, the access-port address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a DTIM.

Specify a beacon interval in units of 1,000 microseconds (K-us). This is a multiple of the DTIM value, for example, 100 : 10. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decreasing this value (shorten the time) to support streaming-multicast audio and video applications that are jitter-sensitive.
**Radio-Specific Settings**

The fields below are only available for some radio types, as indicated in the second column.

**Uniform Spreading (AP 300 only)**

Check this checkbox to enable the Uniform Spreading feature of the AP 300. To comply with Dynamic Frequency Selection (DFS) requirements in the European Union, the 802.11a radio on AP 300 Access Ports will come up on a random channel each time it is powered on.

*To change the channel on the 802.11a radio for an AP 300 Access Port, this box MUST be unchecked.*

**Support Short Preamble b/g**

Check the **Support Short Preamble** box to allow the Access Port to communicate with the MUs using a short 56-bit preamble.

A preamble is the beginning part of a frame. The preamble comprises such elements as robust carrier sensing, collision detection, equalizer training, timing recovery, and gain adjustment. The administration can choose between a long or short preamble for data-frame transmission from the WLAN’s adopted Access Ports.

Use the long preamble setting (the default) for legacy wireless equipment that is not capable of dealing with short preambles. Use the short preamble setting where legacy equipment is not an issue and maximum throughput is desired, for example when streaming video or Voice-over-IP applications are used.

**DTIM Period**—A DTIM is periodically included in the beacon frame that is transmitted from adopted Access Ports. The DTIM period determines how often the beacon contains a DTIM, for example, 1 DTIM for every 10 beacons. The DTIM indicates that broadcast and multicast frames, buffered at the Access Port, are soon to arrive. These are simple data frames that require no acknowledgment, so nodes sometimes miss them.

In this field, the administrator can specify a period for the Delivery Traffic Indication Message (DTIM). This is a divisor of the beacon interval (in milliseconds); for example, 10 : 100. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decrease this setting (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive.

**Primary WLAN**—Select the primary WLAN when the 802.11a broadcast protocol is used. When a WLAN is associated with an 801.11a broadcaster, only one ESSID can be broadcast from the Access Port (even though three are supported by the switch). This field specifies which ESSID to broadcast.

**Security Beacon**—Check the **Security Beacon** box if the WLAN associated with the Access Port needs to be secure. If this feature is selected, the WLAN will not broadcast the ESSID. This selection eliminates the possibility of hackers tapping into the WLAN without authorization by “stealing” the ESSID.
Use this menu to set radio rates on the Access Port to one of the following settings:

- **B and G**: Clients that support 802.11b and/or 802.11g rates may associate with the Access Port.
- **G only**: Only clients that support 802.11g rates may associate with the Access Port.
- **B only**: Only clients that support 802.11b rates may associate with the Access Port.

**DTIM per BSS (AP 300 only)**

- **a/b/g**: DTIM Per BSS—A DTIM is periodically included in the beacon frame that is transmitted from adopted Access Ports. The DTIM period determines how often the beacon contains a DTIM, for example, 1 DTIM for every 10 beacons. The DTIM indicates that broadcast and multicast frames, buffered at the Access Port, are soon to arrive. These are simple data frames that require no acknowledgment, so nodes sometimes miss them.

  On the AP300, the administrator can specify a period for the Delivery Traffic Indication Message (DTIM) per BSSID. This is a divisor of the beacon interval (in milliseconds); for example, 10 : 100. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decrease this settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive.

Click the **Apply** button to save changes.

### Advanced Access Port Settings

The WS 2000 Wireless Switch GUI allows the administrator to configure the Access Port settings. To examine or change that information:

1. Select **Network Configuration --> Wireless --> Access Ports** from the left menu and then click the + to the left of the menu item. The detected Access Ports will be listed under the menu item.
2. Select the Access Port to examine or modify.

   When the Access Port Name menu item is selected, the following screen will appear:

   ![Wireless Switch Configuration Screen]

   The advanced Access Port settings are found at the bottom and right of the screen. For most installations, the default settings for the advanced settings are appropriate.
Radio Settings

Placement
Select either Indoors or Outdoors from the Placement pop-up menu. The setting will affect the selection available for several of the other advanced settings.

Channel
Select a channel number from the Channel drop-down menu on which the Access Port should communicate with associated MUs. (The available channels vary depending on the location setting of the switch.)

Power Level
Select a power level from the Power Level drop-down menu that will be used for radio communications between the Access Port and the MUs.

Set Rates
Click the Set Rates button to open a sub-screen where the default Basic Rates and Supported Rates for 802.11b/g Access Ports can be set.

A list of available Basic and Supported rates for the radio are listed in two columns with checkboxes next to each rate. Selecting a rate as a Basic Rate automatically selects that rate as a Supported Rate and disables the option in the Supported Rates column.

Antenna Settings

Internal/External Antenna
Specify whether the Access Port has internal antenna or external antenna. Depending on the antenna type selected certain options in the Radio Settings section may be disabled.

Antenna Diversity
Use the drop-down menu to configure the Antenna Diversity settings for Access Ports that use external antennas.

Full Diversity: Utilizes both antennas to provide antenna diversity.
Primary Only: Enables only the primary antenna.
Secondary Only: Enables only the secondary antenna.

Antenna Diversity should only be enabled if the Access Port has two matching external antennas.
**Advanced Properties**

**Support Short Preamble**

Check the **Support Short Preamble** checkbox to allow the Access Port to communicate with the MUs using a short 56-bit preamble.

A preamble is the beginning part of a frame. The preamble comprises such elements as robust carrier sensing, collision detection, equalizer training, timing recovery, and gain adjustment. The administration can choose between a long or short preamble for data-frame transmission from the WLAN's adopted Access Ports.

Use the long preamble setting (the default) for legacy wireless equipment that is not capable of dealing with short preambles. Use the short preamble setting where legacy equipment is not an issue and maximum throughput is desired, for example when streaming video or Voice-over-IP applications are used.

**RTS Threshold**

Set the Request to Send Threshold (**RTS Threshold**) by specifying a number.

RTS is a transmitting station's signal that requests a Clear To Send (CTS) response from a receiving station. This RTS/CTS procedure clears the air when many mobile units (MUs) are contending for transmission time. Modifying this value allows the administrator to control the number of data collisions and thereby enhance communication with nodes that are hard to find because of other active nodes in the transmission path.

In this field, the administrator can specify a Request To Send (RTS) threshold (in bytes) for use by the WLAN's adopted Access Ports.

This setting initiates an RTS/CTS exchange for data frames that are larger than the threshold, and sends (without RTS/CTS) any data frames that are smaller than the threshold.

Consider the tradeoffs when setting an appropriate RTS threshold for the WLAN's Access Ports. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of the additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold.

A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.
Beacon Settings

Set the Access Port beacon settings by clicking the **Beacon Settings** button.

**Beacon Interval**

A beacon is a packet broadcast by the adopted Access Ports to keep the network synchronized. Included in a beacon is information such as the WLAN service area, the access-port address, the broadcast destination addresses, a time stamp, and indicators about traffic and delivery such as a DTIM.

Specify a beacon interval in units of 1,000 microseconds (K-us). This is a multiple of the DTIM value, for example, 100 : 10. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decreasing this value (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive.

**DTIM Period**

A DTIM is periodically included in the beacon frame that is transmitted from adopted Access Ports. The DTIM period determines how often the beacon contains a DTIM, for example, 1 DTIM for every 10 beacons. The DTIM indicates that broadcast and multicast frames, buffered at the Access Port, are soon to arrive. These are simple data frames that require no acknowledgment, so nodes sometimes miss them.

In this field, the administrator can specify a period for the Delivery Traffic Indication Message (DTIM). This is a divisor of the beacon interval (in milliseconds); for example, 10 : 100. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decrease this settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive.

**DTIM Per BSSID (AP300 Only)**—On the AP300, the administrator can specify a period for the Delivery Traffic Indication Message (DTIM) per BSSID. This is a divisor of the beacon interval (in milliseconds); for example, 10 : 100. Increase the DTIM/beacon settings, lengthening the time, to let nodes sleep longer and preserve their battery life. Decrease this settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive.

**Secure Beacon**

Select the Secure Beacon checkbox if the WLAN associated with the Access Port needs to be secure. If this feature is selected, the WLAN will not broadcast the ESSID. This selection eliminates the possibility of hackers tapping in to the WLAN without authorization by “stealing” the ESSID.

Click **Ok** when finished setting the beacon settings.

AP SIP Call Admission Control

Specify the number of concurrent SIP sessions allowed for this Access Port.

SIP is the Session Initiation Protocol which controls sessions for multimedia and voice conferences.

Click **Apply** in the Access Port window to save changes.

### Quality of Service Configuration

Disruptions in service in a wireless environment can be a significant issue in environments that have high bandwidth demands (for example, when VoIP and video broadcasts are commonplace). Wireless Internet users can also suffer disruptions due to environmental conditions, such as adverse transmission situations or a large number of wireless devices that affect radio frequency communications. The WS 2000 Wireless Switch allows an administrator to adjust several parameters that can improve the quality of service (QoS) to wireless users.
Select **Wireless --> Wireless QoS** from the navigation menu on the left to specify how the bandwidth can be shared, how to distribute the bandwidth among the WLANs that are in service, or how to prioritize voice and multicast communications.

### Setting the Bandwidth Share Mode

First, specify how the networking resources will be shared. The Bandwidth Share Mode provides three allocation options:

- **Off**
  - Packets are served on a first-come-first-served basis. If this option is selected, the information in the **Bandwidth Share for Each WLAN** area is ignored.

- **Round Robin**
  - Bandwidth is equally shared among all active WLANs. If this option is selected, the Weight (%) in the **Bandwidth Share for Each WLAN** area is automatically set to be the same for all active WLANs, and the values are not editable.

- **Weighted Round Robin**
  - The bandwidth can be configured on a per WLAN basis. If **Weighted Round Robin** is the selected Bandwidth Share Mode, the weight for each WLAN can be set either using the **Weight** field or the **Weight (%)** field. When one is set, the application automatically adjusts the other field. Only the information for active WLANs can be edited.
Bandwidth Share for Each WLAN Table

The fields in this table are:

- **WLAN Name**: This field lists the WLANs on the switch by name (the same name that you see in the left menu). You cannot change the name of the WLAN in this field. Go to the Wireless screen to change a WLAN name.

- **Weight**: The Weight field specifies the relative amount of bandwidth provided to the given WLAN as compared to the other WLANs. For example, if WLAN1 has Weight set to 3 and WLAN2 has Weight set to 1, WLAN1 will get 3 times as much bandwidth as WLAN2. When the Weight field is changed, the weight percentage adjusts automatically to match.

- **Weight (%)**: This field is automatically calculated and cannot be edited. This field specifies the percentage of bandwidth allocated for each of the WLANs. If the Bandwidth Share Mode is set to **Round Robin**, the Weight (%) will be the same for all active WLANs. If the Bandwidth Share Mode is set to **Weighted Round Robin**, the value is calculated based upon the Weights set for each of the WLANs. For example, if WLAN1 has Weight set to 3 and WLAN2 has Weight set to 1, the application will automatically set the weight percentage to 75% for WLAN1 and 25% for WLAN2.

**Configuring Voice Prioritization and Multicast Address Settings**

To ensure better performance with Voice over IP (VoIP) broadcasts, the administrator can enable voice prioritization for particular multicast addresses within a WLAN. In the table, specify the multicast addresses by filling out the fields:

- **WLAN Name**: This field lists the WLANs on the switch by name (the same name that you see in the left menu). You cannot change the name of the WLAN in this field. Go to the Wireless screen to change a WLAN name.

- **Use Voice Prioritization**: Check this box to enable prioritization of voice over data for RF transmissions for the associated WLAN. This setting reduces the latency that might occur when data transmissions and VoIP transmissions compete for the same resources. Latency is usually experienced as broken or delayed speech or sound.

- **Multicast Address #1** and **Multicast Address #2**: Use the two Multicast Address fields to specify one or two MAC addresses to be used for multicast applications. Some VoIP devices make use of multicast addresses. Using this mechanism ensures that the multicast packets for these devices are not delayed by the packet queue.

**Note**: Voice prioritization and multicast addressing will only affect active WLANs. Applying these settings to an inactive WLAN will have no effect. To make a WLAN active, go to the Wireless screen.

**Configuring WME Profiles**

Wireless Multimedia Enhancements (WME) allow for custom Quality of Service (QoS) profiles to be created in order to manage specific types of traffic such as Voice over IP (VoIP) and Video traffic. These profiles can then be assigned to each of the 8 WLANs to allow for custom QoS for each WLAN.
To Add a WME Profile

Select **Network Configuration --> Wireless --> Wireless QoS --> WME Profile Configuration** from the navigation menu on the left.

1. In the **Profiles** section, click the **Add** button to add a new profile to the WME profiles table. Each profile contains a field for the Profile Name and an Edit button to customize the profile.

2. Enter a brief descriptive name for the WME Profile in the **Profile Name** field. The name should be unique among the WME profiles and is used to identify the WME profile on subsequent WME configuration pages.

3. Click the edit button to open a dialogue box where the WME profile options can be configured.

4. To start with a default template for either an Access Port (**AP**) or Mobile Unit (**STA**) choose a radio type (**B** or **AG**) click the appropriate button to populate the EDCA Parameters with default values for the chosen configuration.

5. Click the **Ok** button to save changes to the WME Profile.
**WME Priority Conversion**

Priority Conversion allows you to convert existing QoS priorities from non WME devices going to a WME device. The options allow the user to specify which field from which the priority of the packets is to be extracted.

From the radio buttons choose one of the following options:

- **DSCP**: If DSCP is selected, priority is determined from the DSCP field of the IP header.
- **VLAN Tag (Trunked Pkts)**: If VLAN tag is selected, packet priority is determined by looking at the VLAN tag of the packet.
- **None**: If ‘None’ is selected, packets are treated as BE packets. However, these values are not used if the packet matches a traffic classification entry. To disable Priority Conversion choose the None option.

**Assigning WME Profiles to WLANs**

The WME Configuration page enables you to map each of the switch’s 8 WLANs to specific WME Profiles.

Select **Network Configuration -> Wireless -> Wireless QoS -> WME Profile Configuration -> WME Configuration** from the navigation menu on the left.

1. Find the WLAN you wish to configure in the WLAN column.
2. Select the desired WME profile from the Profile pulldown menu.
3. Repeat steps 1 & 2 for each of the WLANs you wish to configure.
4. Click the Apply button to commit the changes.
**Configuring WME Traffic Classification**

The Traffic Classification screen is used to specify QoS settings for traffic from specific networks or specific source and/or destination ports. For each rule traffic can be set to have Best Effort, Background, Voice or Video QoS rules applied to them. The details of each of these QoS types are configured in the Edit sub-screen of WME Profile Configuration.

**To add a Traffic Classification Rule:**

Select Network Configuration --> Wireless --> Wireless QoS --> WME Profile Configuration --> WTraffic Classification from the navigation menu on the left.

1. Click the Add button to add a row for a new traffic classification rule. By default the new rule will be set to provide Best Effort QoS to all traffic on all ports.

2. Click on the Source field to bring up a screen where the source IP address and range can be configured for the rule. By default the source IP range for new traffic classifications is 0.0.0.0/32 making the rule apply to all source IP ranges.

3. Edit the Source IP Range as necessary and click the Ok button to return to the Traffic Classification page.
4. Click on the **Destination** field to bring up a screen where the destination IP address and range can be configured for the rule. By default the destination IP range for new traffic classifications is 0.0.0.0/32 making the rule apply to all destination IP ranges.

![Edit IP Range](image1)

5. Edit the **Destination IP Range** as necessary and click the **Ok** button to return to the **Traffic Classification** page.

6. Click on the **Source Ports** field to bring up a screen where the source port range can be configured for the rule. By default the source port range for new traffic classifications is 1:65535 making the rule apply to all source ports.

![Edit Port Range](image2)

7. Edit the **Source Port Range** as necessary and click the **Ok** button to return to the **Traffic Classification** page.

8. Click on the **Destination Ports** field to bring up a screen where the destination port range can be configured for the rule. By default the destination port range for new traffic classifications is 1:65535 making the rule apply to all destination ports.

![Edit Port Range](image3)

9. Edit the **Destination Port Range** as necessary and click the **Ok** button to return to the **Traffic Classification** page.

10. Select an **Access Category** to be associated with the traffic classification rule from the pulldown menu. This Access Category will determine what type of QoS settings will be applied to traffic matching the specified traffic classification rules. The options are Best Effort, Background, Voice and Video.

11. Click the **Apply** button to commit the changes.
Setting Up Port Authentication for AP 300 Access Ports

802.1x port authentication is used to provide security and authentication for all wired clients on a WLAN. The WS 2000 Wireless Switch supports 802.1x port authentication for the AP 300 Access Ports connected to it. It uses a username and password for all ports that can be configured from the wireless switch.

Select **Network Configuration --> [Access Ports] --> 802.1x Port Authentication** from the navigation menu on the left.

To set up Port Authentication for all adopted AP 300 Access Ports:

1. In the **Username** field, specify a 802.1x username for all AP 300 Access Ports adopted by the switch. To use the default username click the **<- Default** button next to the **Username** field.
2. In the **Password** field, specify a 802.1x password for all AP 300 Access Ports adopted by the switch. To use the default password click the **<- Default** button next to the **Password** field.
3. Click the **Set on all adopted AP 300** button to set the username and password specified in the **Username** and **Password** fields on all AP 300 Access Ports adopted by the switch.

Rogue Access Point (Port) Detection

Rogue Access Points (APs) are a hot area of concern with respect to LAN security. “Rogue AP” is a term used to describe an unauthorized access point that is connected to the production network or operating in a stand-alone mode (in a parking lot or in a neighbor’s building). Rogue APs, by definition, are not under the management of network administrators and do not conform to any network security policies.

Although 802.1x security settings should completely protect the LAN, organizations are not always fully compliant with the newest wireless-security best practices. In addition, organizations want to be able to detect and disarm rogue APs. The WS 2000 Wireless Switch provides a mechanism for detecting and reporting rogue APs.

Select **Network Configuration --> Wireless --> Rogue AP Detection** from the navigation menu on the left.
The Rogue AP Detection screen allows the administrator to determine how thoroughly the switch will search for rogue APs as well as list the approved APs.

**Setting Up the Detection Method**

The WS 2000 Wireless Switch provides three methods for detecting rogue Access Points (APs). Use the top part of the Rogue AP Detection screen to set the method or methods that the switch will use to detect rogue APs.

1. Check the **RF Scan by MU** box if you want the switch to work with mobile units (MUs) to detect a rogue AP. With this option selected, each MU reports whether it supports rogue AP detection mechanisms. If so, the switch sends WNMP requests, at regular intervals, to the MU to get a list of APs. The MU scans all the channels for APs in the vicinity. The MU then prepares a list of APs (BSSIDs) and sends it back to the switch using WNMP response message. The switch processes this information.

2. Check the **RF Scan by AP** box if you want the switch to work with the APs to detect a rogue AP. By default, this method is selected. With this option enabled, the switch sends a WISP configuration message to each adopted AP that indicates that rogue AP detection is needed. Each AP listens for beacons in its present channel and passes the beacons to the switch without modification. The switch then processes the beacons to determine whether any of them are rogues. This method is less disruptive than the RF Scan by MU mode.

3. Check the **RF Scan by Detector AP** box if you have set up a detector AP on the LAN and want the switch to work with that AP to detect rogue APs. To set an AP as a detector AP, go to the screen for the adopted AP under Access Ports in the navigation menu and check the appropriate box. Note that only some switches have the capability of being a Detector AP, including Symbol AP 100, AP 200, and AP 300 Access Ports.

4. In the **Scan Interval** field, enter a time interval (in minutes) between detection RF scans. Do this for each of the selected detection methods. By default, these scans are set at one hour intervals.
Defining and Maintaining Approved AP List Rules

The lower half of the Rogue AP Detection screen specifies rules that determine whether a detected AP can be approved or not. Each entry in the table works as an AP evaluation rule. You can specify a particular MAC address or a particular ESSID, or you can indicate that any MAC address or ESSID will work. However, if you select Any MAC and Any ESSID on the same line, all APs will be approved. Up to 20 rules can be defined.

1. Check the Approve Any AP Having a Symbol Defined MAC Address box to indicate that any Symbol AP (that is, one that has a known Symbol MAC address) is an approved AP.
2. Click the Add button to add a line in the rule table and then fill out the following table cells:

- **Any MAC**
  - Check this box to indicate that an AP with any MAC address matches the rule.
- **MAC Address**
  - Enter an approved MAC address to be used during the detection process. This field is only used when Any MAC (on the same line) is not checked.
- **Any ESSID**
  - Check this box to indicate that an AP with any ESSID matches the rule.
- **ESSID**
  - Enter an approved ESSID to be used during the detection process. This field is only used when Any ESSID (on the same line) is not checked.

3. To delete a particular rule from the table, select the rule and then click the Del button.
4. Click the Delete All button to clear the entire rule list.

Examine the Approve and Rogue Access Ports

This screen displays information about APs known to the switch. All approved APs are listed in the upper table. All rogue APs are listed in the lower table. This screen also allows the administrator to create detection rules from the information collected about approved or rogue APs.

To maintain the lists, select Network Configuration --> Wireless --> Rogue AP Detection --> AP List from the navigation menu on the left.
The Approved AP List

Each row of this table represents an approved AP that the switch has found. For each AP, both the MAC and the ESSID for the AP are listed. Use this portion of the screen to change the age out time or to add a rule to the rule list for a particular AP:

1. Enter a number in the **Approved AP’s Age Out Time** field to indicate the number of elapsed minutes before an AP will be removed from the approved list and reevaluated. A zero (0) in this field indicates that an AP can stay on the list permanently.
2. Click the **Add to Rule List** button to add a rule to the Approved APs’ Rule Management table on the Rogue AP Detection screen. The generated rule will use the MAC address and ESSID of the selected AP.
3. Click the **Add All to Rule List** button to add a rule to the Approved APs’ Rule Management table on the Rogue AP Detection screen for all the APs on the list. The generated rules will use the MAC addresses and ESSIDs of the APs.

The Rogue AP List

Each row of this table represents a rogue AP that the switch has found. For each AP, both the MAC and the ESSID for the AP is listed as well as some information about when the AP was first and last seen:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP MAC</td>
<td>This field is the MAC address for the rogue AP.</td>
</tr>
<tr>
<td>ESSID</td>
<td>This field is the ESSID for the rogue AP.</td>
</tr>
<tr>
<td>First Seen</td>
<td>This field indicates the number of elapsed hours since the rogue AP was first noticed on the network in hours:minutes:seconds.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>This field indicates the number of elapsed hours since the rogue AP was last noticed on the network in hours:minutes:seconds.</td>
</tr>
<tr>
<td>Reporting AP</td>
<td>This field shows the MAC address of the device that detected the rogue AP.</td>
</tr>
</tbody>
</table>
1. Enter a number in the **Rogue Entries Age Out Time** field to indicate the number of elapsed minutes before an AP will be removed from the rogue list and reevaluated. A zero (0) in this field indicates that an AP can stay on the list permanently.

2. Click the **Add to Approved AP Rule List** button to add a rule to the Approved APs’ Rule Management table of the Rogue AP Detection screen. The generated rule will use the MAC address and ESSID of the selected AP.

3. Click the **Add All to Approved AP Rule List** button to add a rule to the Approved APs’ Rule Management table on the Rogue AP Detection screen for all the APs on the list. The generated rules will use the MAC addresses and ESSIDs of the APs.

### Getting Detailed Information About a Rogue AP

The Rule List screen provides a means to get detailed information about a rogue Access Port as well as its detector to help an administrator track it down. To see detailed information:

1. Select a rogue AP from the **Rogue AP List**.
2. Click the **Detail** button to open a new window to view detailed information about the rogue AP and its detector.

### Details About the Rogue AP

The top of the Rogue AP Detail screen lists information about the rogue AP:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID/MAC</td>
<td>This field contains the BSSID or the MAC address for the rogue AP.</td>
</tr>
<tr>
<td>ESSID</td>
<td>This field is the ESSID for the rogue AP.</td>
</tr>
<tr>
<td>RSSI</td>
<td>This field displays the Receiver Signal Strength Indicator (RSSI) for the rogue AP. The value will be between 1 and 255. The larger the value, the better the signal strength and the closer the AP.</td>
</tr>
</tbody>
</table>

### Details About the Rogue Detector

The lower portion of the Rogue AP Detail screen displays information about the AP that detected the rogue. This information is provided to the administrator to help locate the rogue.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finder’s MAC</td>
<td>This is the MAC address for the AP that detected the rogue AP.</td>
</tr>
<tr>
<td>Closest AP MAC</td>
<td>This is the MAC address for the AP that is physically closest to the rogue AP.</td>
</tr>
<tr>
<td>Closest AP Name</td>
<td>This is the name of the AP that is physically closest to the rogue AP.</td>
</tr>
<tr>
<td>Scan Method</td>
<td>This is the scan method that was used to detect the rogue AP. The possible values are:</td>
</tr>
<tr>
<td>First Seen</td>
<td>This is the number of hours:minutes:seconds since the rogue AP was first noticed on the network.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>This is the number of hours:minutes:seconds since the rogue AP was last noticed on the network.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MU</td>
<td>(detected by a mobile unit)</td>
</tr>
<tr>
<td>Detector</td>
<td>(detected by the Detector AP)</td>
</tr>
<tr>
<td>On Channel</td>
<td>(detected by non-detector AP)</td>
</tr>
</tbody>
</table>
The WS 2000 Wireless Switch only reports rogue APs. It is up to the administrator to change security settings or disrupt the rogue AP’s connection.

**Setting SNMP Traps for Rogue APs**

It is also possible to set a trap for a rogue AP:

1. Go to [System Configuration] --> SNMP Access --> SNMP Traps from the navigation menu.

2. Check the Rogue AP box (in the lower right area of the screen) to generate a trap when a rogue (unauthorized) access port (AP) is detected. The detection process is non-disruptive and will not affect the performance of the switch. The detection functionality is greatly enhanced when the Approved AP list is filled out on the AP List screen under Rogue AP Detection.

**Configuring Wireless Intrusion Protection System (WIPS)**

The Wireless Intrusion Protection System (WIPS) provides additional wireless LAN security by monitoring the airwaves for any kind of Denial of Service (DoS) attacks. It is also able to actively suppress any rogue clients and APs in the network.

Symbol’s WIPS solution utilizes AP300s that act as dedicated sensors and send out relevant information to a centralized WIPS server. The WIPS server does all the data correlation and provides the threat mitigation services.
Go to **Network Configuration--> Wireless --> WIPS** from the navigation menu.

1. Click the **Enable WIPS** checkbox in the **WIPS mode** section.
2. Check the box next to each of the APs or Sensors which you wish to convert to a dedicated detector port.
3. Once all desired APs have been checked, click the **Convert** button to begin the conversion process.

*If no APs or Sensors are displayed in the tables, go to the properties page for each AP you wish to use as a WIPS detector and select the **Dedicate this AP as a Detector AP** option and return the the WIPS screen.*

4. Click the **Apply** button to save any changes made on this screen. Navigating away from the current screen without clicking the **Apply** button results in all changes to this screen being lost.
Administrator and User Access

Configuring Administrator Access ................................................................. 6-2
  Selecting the Type of Admin Access ............................................................. 6-2
  Configuring Secure Shell Connection Parameters ........................................ 6-3
  Admin Authentication and RADIUS Server Authentication Setup .................. 6-3
  Setting Up AirBEAM Software Access ......................................................... 6-3
  Applet Timeout Specification ....................................................................... 6-4
  Changing the Administrator Password .......................................................... 6-4
Configuring User Authentication ..................................................................... 6-4
  Configuring the RADIUS Server ................................................................ 6-5
  Configuring Lightweight Directory Access Protocol (LDAP) Authentication .... 6-7
  Setting Up a Proxy RADIUS Server ............................................................... 6-8
  Managing the Local User Database .............................................................. 6-9
  Setting the User Access Policy .................................................................... 6-10
Managing Digital Certificates ....................................................................... 6-12
  Importing CA Certificates .......................................................................... 6-12
  Creating Self Certificates ........................................................................... 6-13
Configuring Administrator Access

The WS 2000 Network Management System allows users to log in to perform administration tasks. The switch administrator can change any settings within the WS 2000 Network Management System. The default login name for the switch administrator is “admin” and the initial password is “symbol”.

To configure which interfaces the administrators can access the user interface or to change the passwords of the administrators, select System Configuration --> WS 2000 Access from the left menu.

Selecting the Type of Admin Access

The WS 2000 Network Management System runs from a standard Web browser. Any individual on an enabled subnet or over the WAN can access the log screen by specifying one of the IP addresses associated with the user interface. The WS 2000 Access screen allows the administrator to restrict access from different locations. By selecting the appropriate checkboxes, the administrator can allow or disallow specific types of access from the WAN port or from the LAN subnets.

When connected to the switch using multiple methods, i.e. SSH and HTTP, saving the configuration using one method will cause a disconnect from the other method.

Choose the types of access to allow by checking the associated checkbox.

<table>
<thead>
<tr>
<th>Access</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applet HTTP</td>
<td>80</td>
<td>Allows administrator access to the WS 2000 Management System through a standard HTTP web browser communication.</td>
</tr>
<tr>
<td>Applet HTTPS</td>
<td>443</td>
<td>Allows administrator access to the WS 2000 Management System through a HTTPS (secure) connection from a web browser.</td>
</tr>
<tr>
<td>CLI TELNET</td>
<td>23</td>
<td>Allows administrator access to the wireless switch through TELNET. Allows the administrator to access the switch through the command line interface.</td>
</tr>
</tbody>
</table>
If all the checkboxes in this section are disabled, the administrator will not be able to access the switch through the WS 2000 Management System user interface. The only access available is through a direct serial cable connection from a PC. All commands are given using the command line interface. If this situation occurs accidentally, you can restore the switch’s factory settings using the command line interface.

### Configuring Secure Shell Connection Parameters

If CLI SSH (port 22) is enabled either for either WAN or LAN, set the fields in the Secure Shell area:

1. Enter a value, in seconds, when a client connected via SSH must reauthenticate in the **Authentication Timeout** field. The default is 120 seconds (2 minutes).
2. Enter the amount of time, in seconds, when an inactive client using SSH will be disconnected in the **SSH Client Inactivity Timeout** field. The default is 120 seconds (2 minutes).

### Admin Authentication and RADIUS Server Authentication Setup

There are two methods available for authenticating administrators upon contacting the switch. This area provides a means to set up the desired authentication methods.

1. First choose an authentication method:
   - Select the **Local** radio button to have the administrator of the switch authenticate using the built-in password authentication process (that is, using the standard admin password).
   - Select the **RADIUS** radio button to have the administrator authenticate against a RADIUS database. If RADIUS is selected, the RADIUS server information can be entered in the **RADIUS Server for Admin Authentication** area.
2. If the RADIUS button is selected, specify the **RADIUS Server IP** address, the communication port for the authentication process, and the RADIUS server’s **Shared Secret** (password) that should be used.

### Setting Up AirBEAM Software Access

Symbol’s AirBEAM software suite is a comprehensive set of mobility management tools that maximize the availability, security and effectiveness of a wireless network. The fields in this section of the screen allow the administrator to enable access from the AirBEAM software suite and to set the AirBEAM password.

1. To enable AirBEAM access, check the **Enable AirBEAM** checkbox.
2. Specify a password for AirBEAM software access. Note that the AirBEAM login name is always “airbeam”.
3. Click the **Apply** button to save changes.
**Applet Timeout Specification**

This screen provides a method to set a timeout for an inactive connection from either an HTTP or HTTPs connection. Specify the maximum number of inactive minutes allowed in the **HTTP/S Timeout** field. A zero (0) value indicates that an inactive administrator connection will never be timed out.

**Changing the Administrator Password**

Click the **Change Admin/Manager Password** button (In the bottom right of the WS 2000 Access screen) to open a sub-screen that allows the administrator to change the switch administrator’s password.

1. Select **Admin** or **Manager** from the **User** field depending on which user’s password you wish to change.
2. Enter the new admin password in both fields, and click the **Update Password Now** button. The sub-screen will disappear and the focus will return to the WS2000 Access screen.

*If the administrator does not remember the current password, the administrator can contact Symbol Technical Support for directions on how to proceed.*

**Configuring User Authentication**

The WS 2000 Wireless Switch provides an integrated RADIUS server as well as the ability to work with external RADIUS and LDAP servers to provide user database information and user authentication. Several screens are available to configure the how the RADIUS server authentication works as well as set up the local user database and access policies.

- The RADIUS Server screen allows the administrator to set the data source, the authentication type, and associate digital certificates with the authentication (see *Configuring the RADIUS Server*).
- The LDAP screen allows the administrator to set up communication with an external LDAP server (see *Configuring Lightweight Directory Access Protocol (LDAP) Authentication*).
Configuring the RADIUS Server

The WS 2000 Wireless Switch provides an integrated RADIUS server as well as the ability to work with external RADIUS and LDAP servers to provide user database information and authentication. The RADIUS Server page allows the admin to set up data sources, as well as specify authentication information for the built-in RADIUS server.

Select [User Authentication] --> RADIUS Server to set up the RADIUS server configuration.

1. Use the Data Source pull-down menu to select the data source for the local RADIUS server.
   - If Local is selected, the internal User Database will serve as the data source. Use the User Database screen to enter the user data.
   - If LDAP is selected, the switch will use the data in an LDAP server. Configure the LDAP server settings on the LDAP screen under RADIUS Server on the menu tree.

2. Use the TTLS/PEAP Configuration check-boxes to specify the EAP types for the RADIUS server. TLS is selected by default and EAP and TTLS are selectable options.:
   - Protected EAP (PEAP) uses a TLS layer on top of EAP as a carrier for other EAP modules. PEAP is an ideal choice for networks using legacy EAP authentication methods.
   - Tunneled TLS EAP (EAP-TTLS) is similar to EAP-TLS, but the client authentication portion of the protocol is not performed until after a secure transport tunnel has been established. This allows EAP-TTLS to protect legacy authentication methods used by some RADIUS servers.

3. If PEAP is selected, specify a Default Auth Type for PEAP to use from the pull-down menu. The options are GTC and MSCHAP-V2:
   - EAP Generic Token Card (GTC) is a challenge handshake authentication protocol that uses a hardware token card to provide the response string.
   - Microsoft CHAP (MSCHAP-V2) is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.
4. If TTLS is selected, specify a Default Auth Type for TTLS to use from the pull-down menu. The options are MD5, PAP and MSCHAP-V2.
   - Message Digest 5 (MD5) is a secure hash function which converts a long data stream into a fixed size digest.
   - Password Authentication Protocol (PAP) is a protocol where the user sends an identifier and password pair to the server. This information is sent unencrypted.
   - Microsoft CHAP (MSCHAP-V2) is an encrypted authentication method based on Microsoft's challenge/response authentication protocol.

5. If you have a server certificate from a CA and wish to use it on the RADIUS server, select it from this pull-down menu. Only certificates imported to the switch will be available in the menu. To create a server certificate, select the Self Certificates screen from Certificate Mgmt in the navigation menu (see Creating Self Certificates).

6. You can also choose an imported CA Certificate to use on the RADIUS server. If using a server certificate signed by a CA, you will need to import that CA's root certificate using the CA certificates screen from the Certificate Mgmt menu. After a valid CA root certificate has been imported, it will be available from the CA Certificate pull-down menu.

7. Use the RADIUS Client Authentication table to set up multiple shared secrets based on the subnet or host that is trying to authenticate against the RADIUS server. Use the Add button to add entries to the list.

   **Subnet/Host**
   - This field contains the IP address of the subnet or host that will be authenticating with the RADIUS server.

   **Netmask**
   - This field contains the netmask (subnet mask) of the subnet or host that will be authenticating with the RADIUS server.

   **Shared Secret**
   - Set a shared secret to be used for each host or subnet that will be authenticating against the RADIUS server. The shared secret can be up to 7 characters in length.

8. Click Apply to save your changes.
Configuring Lightweight Directory Access Protocol (LDAP) Authentication

When the RADIUS Data Source is set to use an external LDAP server (see Configuring the RADIUS Server), the LDAP screen is used to provide information about the external LDAP server. Select [User Authentication] --> RADIUS Server --> LDAP. The fields on this screen are only available when LDAP is set as the data source for the RADIUS server.

1. Fill out the LDAP Configuration area to allow the switch to work with the LDAP server. Consult with the LDAP server administrator for details on how to set the values for the fields in this screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Server IP</td>
<td>Enter the IP address of the external LDAP server that will be acting as the data source for the RADIUS server. This server must be accessible from the WAN port or from an active subnet on the switch.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the TCP/IP port number for the LDAP server that will be acting as a data source. The default port is 389.</td>
</tr>
<tr>
<td>Login Attribute</td>
<td>Enter the login attribute used by your LDAP server for authentication. In most cases, the default value in this field should work.</td>
</tr>
<tr>
<td>Password Attribute</td>
<td>Enter the password attribute used by your LDAP server for authentication.</td>
</tr>
<tr>
<td>Bind Distinguished Name</td>
<td>Specify the distinguished name to bind with the LDAP server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a valid password for the LDAP server.</td>
</tr>
<tr>
<td>Base Distinguished Name</td>
<td>Specify a distinguished name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching.</td>
</tr>
<tr>
<td>Group Attribute</td>
<td>Specify the group attribute used by your LDAP server.</td>
</tr>
</tbody>
</table>
2. Click **Apply** to save your changes.

**Setting Up a Proxy RADIUS Server**

The WS 2000 Wireless Switch provides the capability to proxy authentication requests to a remote RADIUS server based upon the suffix of the user ID (such as myisp.com or company.com). Select [User Authentication] --> **RADIUS Server** --> **Proxy** to go to the RADIUS Proxy Configuration screen is where the definitions of proxies are made.

Up to 10 proxy servers are supported.

1. Enter a value between 3 and 6 in the **Retry Count** field to indicate the number of times the switch attempts to reach a proxy server before giving up.

2. Enter a value between 5 and 10 in the **Timeout** field to indicate the number of elapsed seconds that will cause the switch to time out on a request to a proxy server.

3. Use the **Add** button to add a new entry based upon a domain suffix to the Proxy Server Settings area. Then fill in the following information for each entry:

   - **Suffix**: Enter the domain suffix (such as myisp.com or mycompany.com) of the users to be sent to the specified proxy server.
   - **RADIUS Server IP**: Enter the IP address of the RADIUS server that will be acting as a proxy server.
Port Enter the TCP/IP port number for the RADIUS server that will be acting as a proxy server. The default port is 1812.

Shared Secret Set a shared secret to be used for each suffix that will be used for authentication with the RADIUS proxy server.

4. Click Apply to save changes.

To delete a server row, select the row corresponding to that entry and click the Del (Delete) button.

**Note**

If you are using a proxy server for RADIUS authentication, the Data Source field on the RADIUS Server screen (Configuring the RADIUS Server) must be set to Local. If it is set to LDAP, the proxy server will not be successful when performing the authentication.

**Managing the Local User Database**

The User Database screen is used to create users and groups for the local RADIUS server. This database is used when Local is selected as the Data Source from the RADIUS Server screen. The information in the database is ignored if an LDAP server is used for user authentication. Select [User Authentication] --> User Database to maintain the user entries.

Each user that is created is assigned their own password and is associated with one or more groups. Each group can be configured for its own access policy on the Access Policy configuration screen under the RADIUS Server menu.

**Adding Groups**

This Groups table displays a list of all groups in the local RADIUS server’s database. The groups are listed in the order that they are added. Although groups can be added and deleted, there is no capability currently to edit the name of a group.

1. To add a new group, click the Add button and enter the name of the group in the new blank field in the table.
2. Don’t forget to click Apply to save the changes.
Deleting Groups

To remove a group, select the group from the table and click the **Del** (Delete) key. A warning message will appear when you apply the change if there are users still assigned to the group. You can then remove the group from each user or add the group back to the group list.

Adding Users

The Users table displays the entire list of users. Up to 100 users can be entered here. The users are listed in the order that they are added. Although users can be added and deleted, there is no capability currently to edit the name of a group.

1. To add a new user, click the **Add** button at the bottom of the Users area.
2. In the new line, type a **User ID** (username).
3. Click the **Password** cell. A small window will appear. Enter a password for the user and then click **OK** to return to the User Database screen.
4. Click the **List of Groups** cell. A new screen will appear that will let you associate groups with the user. A user must belong to at least one group for the user to have access to the switch.
   - To add the user to a group, select the group in the Available list (on the right) and click the **<-Add** button.
   - To remove the user from a group, select the group in the Assigned list (on the left) and click the **Delete->** button.
5. Click **OK** when you are done.
6. Click **Apply** to save your changes.

Setting the User Access Policy

The RADIUS Access Policy screen allows you to set WLAN access based on a user group defined on the User Database screen. Select [User Authentication] --> RADIUS Server --> Access Policy to set group access.
Each Group ID defined in the User Database screen appears on the Access Policy screen as a single row in the table. Each wireless LAN represents a column in the table.

1. To enable group access to a particular WLAN, check the box for that WLAN in the row corresponding to the group. To disable access for a group, uncheck the box for the appropriate WLAN. A group must have at least one WLAN checked to have wireless access to the switch.

2. Click **Apply** when you have finished the changes.
Managing Digital Certificates

A digital certificate is an electronic identification card that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains a name, a serial number, expiration dates, a copy of the certificate holder’s public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

The WS 2000 Wireless Switch uses digital certificates for VPN access authentication and user authentication. The application provides two mechanisms for defining/importing digital certificates:

- CA certificates are those that a CA creates and signs with its own private key. These certificates are imported into the switch CA certificate library. (See Importing CA Certificates for directions.)
- Self certificates are those that an organization creates a certificate request, sends it off to a Certificate Authority (CA) to be signed, and then imports the signed certificate into the management system. (See Creating Self Certificates for directions.)

Importing CA Certificates

A certificate authority (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates that it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain this CA certificate in its “Trusted Root Library” so that it can trust certificates “signed” by the CA’s private key.

Depending on the public key infrastructure implementation, the digital certificate includes the owner’s public key, the expiration date of the certificate, the owner’s name, and other information about the public key owner.

The WS 2000 Management System provides the means to import and maintain a set of CA certificates to be used as an authentication option for VPN access. To use the certificate for a VPN tunnel, define a tunnel and select the IKE settings to use either RSA or DES certificates.

Before you import a certificate, you need to get one. Ask a CA for a certificate. They will typically send you the certificate information in an email message. You will need to import the content of the message into the WS 2000 Network Management System.

**Note:** Make sure that the WS 2000 is time synchronized with an NTP server before importing a certificate to avoid issues with conflicting date/time stamps.

To import a CA certificate perform the following steps:

1. Select **Network --> Certificates --> CA Certificates** from the left menu. The following screen appears.
2. Copy the content of the CA Certificate message and then click **Paste from Clipboard**. The content of the certificate will appear in the **Import Root CA Certificate** area.

3. Click the **Import Root CA Certificate** button to import it into the CA Certificate list.

4. Once in the list, select the certificate ID from the **View Imported CA Certificates** area to view information, such as the issuer name, subject, serial number, and data that the certificate expires.

5. Click the **Apply** button to save changes.

To delete a certificate, select the Id from the menu and then click the **Del** button.

### Creating Self Certificates

Self certificates are those for which the organization creates a certificate request, sends it off to a Certificate Authority (CA) to be signed, and then imports the signed certificate into the management system. To go through this process, select **System Configuration --> [Certificate Mgmt.]--> Self Certificates.**
1. To create the certificate request, click the Add button. The Certificate Request screen appears.

2. Fill out the request form with the pertinent information. Only 4 fields are required:

   **Key ID**
   Enter a name for the certificate to help distinguish between certificates. The name can be up to 7 characters in length.

   **Subject**
   This required field contains important information about the certificate. Contact the CA that will sign the certificate to determine the content of this field.

   **Signature Algorithm**
   Indicate the signature algorithm to use for the certificate. The settings are:
   - **MD5-RSA**: Message Digest 5 algorithm in combination with RSA encryption.
   - **SHA1-RSA**: Secure Hash Algorithm 1 in combination with RSA encryption.

   **Key Length**
   Indicate the desired length of the key. Possible values are 512, 1024, and 2048.
3. Fill in as many of the optional fields as desired or as required by the CA that will sign the certificate. The contact information is for the organization who is making the certificate request. The less obvious fields are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>Enter the email address to be used for identification purposes. Typically a CA requires either an email address, a domain name, or an IP address for identification purposes.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter the domain name to associate with the certificate. This field is often required by the CA.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the WAN IP of the WS 2000 Wireless Switch. Check with your CA to determine whether this information is necessary. Often it can be omitted if either the email or domain name information is provided.</td>
</tr>
</tbody>
</table>

4. When finished filling out the form, click Generate. The Certificate Request screen will disappear and the ID of the certificate request that was just generated will appear in the Requests ID list of the Self Certificates window.

5. Click the Export Request button. The generated certificate request appears in the large text box.

6. Click Copy to Clipboard and the content of request to be sent to the CA will be copied to the clipboard.

7. Create an email to your CA, paste the content into the body of the message, and send it off to the CA.

8. The CA will “sign” the certificate and send it back. At this point, copy the content from the email onto the clipboard. Then, click the Paste from Clipboard button and the content of the email will be displayed in the window.

9. Click the Import Certificate button to import the certificate and make it available for use as a VPN authentication option. The certificate ID will appear in the Signed list, where you can view information about it.

10. Apply your changes.

To use the certificate for a VPN tunnel, first define a tunnel and select the IKE settings to use either RSA or DES certificates.

**Note:** If the switch is rebooted after a certificate request has been generated but before the signed certificate is imported, the import will not execute properly. Please do not reboot the switch during this interval.
Switch Administration

Overview of Administration Support .................................................. 7-3
Restarting the WS 2000 Wireless Switch ............................................ 7-3
Changing the Name of the Switch .................................................... 7-4
Changing the Location and Country Settings of the WS 2000 ................. 7-4
Configuring Switch Redundancy ..................................................... 7-6
    Setting Up Switch Redundancy .................................................. 7-6
    Redundancy Operations Status ................................................ 7-7
Updating the WS 2000 Wireless Switch's Firmware ............................... 7-7
    Checking for and Downloading Firmware Updates .......................... 7-7
    Performing the Firmware Update ............................................. 7-8
    Formatting a Compact Flash Card ............................................. 7-9
    Setting Up DHCP Options for Firmware Upload ............................. 7-9
Exporting and Importing Wireless Switch Settings ................................ 7-10
    To Import or Export Settings to an FTP or TFTP Site ....................... 7-11
    To Import Settings to a Local File .......................................... 7-12
    To Export Settings to a Local File ........................................... 7-12
    Sample Configuration File .................................................... 7-12
Configuring SNMP ........................................................................ 7-20
    Setting the SNMP Version Configuration .................................... 7-21
    Setting Up the Access Control List ........................................... 7-22
    Setting the Trap Configuration ................................................ 7-23
    Setting the Trap Configuration for SNMP v1/v2c ............................ 7-23
    Setting the Trap Configuration for SNMP V3 ................................ 7-24
    Selecting Traps ......................................................................... 7-24
    Setting RF Traps ........................................................................ 7-27
Specifying a Network Time Protocol (NTP) Server ................................. 7-28
Setting Up and Viewing the System Log .................................................................7-29
  Viewing the Log on the Switch .......................................................................7-29
  Setting Up a Log Server ................................................................................7-30
Overview of Administration Support

The WS 2000 Network Management System provides several screens for administering the switch and monitoring activity on the switch. From the interface the administrator can:

- Change the general system settings, such as the name of the switch and the location of the switch
- Restart the switch
- Restore factory settings
- Export or import the switch’s configuration settings
- Find and install firmware updates
- Change the settings for who can access the switch for administration purposes
- Configure how log files are saved
- View system statistics for WAN communication, subnets, WLANS, Access Ports, and mobile units

Restarting the WS 2000 Wireless Switch

During the normal course of operations, the administrator might need to restart or reset the switch. For example, changing certain configuration settings can require restarting the switch for those settings to take effect.

1. Select System Configuration --> System Settings from the left menu.

2. Click the Restart WS 2000 button to restart the switch. A second window appears, asking for confirmation.

3. Select the Restart button. Upon confirming the restart, the switch reboots. Typically, normal communications with the switch are restored within a minute or two.
Changing the Name of the Switch

When the administrator first logs into the WS 2000 Network Management System, the System Settings screen appears. One of the fields in this screen is the System Name field. In this field, the administrator can specify the name of the switch. This name is used to distinguish the switch from others that are on the network and it is also used to set the device name in SNMP.

To examine and change the current name for the switch:
1. Select System Configuration --> System Settings from the left menu.

2. Find the System Name field and type a string of alphanumeric characters to create a name.
3. Select the Apply button to save the change.

Changing the Location and Country Settings of the WS 2000

When the administrator first logs into the WS 2000 Network Management System, the System Settings screen appears. One of the fields in this screen is the Country field. This field is set to the country in which the switch is installed. Setting this field appropriately ensures compliance with national and local laws concerning electromagnetic emissions and the power level of Access Port radio transmissions.

To examine and change the location setting for the switch:
1. Select **System Configuration --> System Settings** from the left menu.

2. Type in a description of the physical location of the switch within your facility into the **Location** field.

3. Find the **Country** field and use the drop down menu to select the correct country from the list.

4. Click **Apply** to save changes. The interface will ask you to confirm any changes you make to the Country selection.
Configuring Switch Redundancy

The WS 2000 Wireless Switch supports redundancy between two WS 2000 Wireless Switches, allowing a standby switch to take over if the primary switch stops responding. Use the WS 2000 Redundancy Settings to configure the Operational State and Redundancy Mode for the switch.

Setting Up Switch Redundancy

For each of the two switches, use the following procedure to set up redundancy.

1. Choose the redundancy mode in which the WS 2000 Wireless Switch will operate in.
   - **Stand-alone**: The switch has no redundancy capabilities and operates independently of any other WS 2000 switches on the network. This is the default setting.
   - **Redundancy**: Two WS 2000 switches are connected, with one set as a primary and the other as a standby. The primary switch will send heartbeat packets to the specified port of the standby switch at a specified interval. If the standby switch doesn’t receive a heartbeat packet in a specified amount of time, it will take over as the primary switch.

2. When redundancy is selected as the operational state, specify whether the current switch is the primary or standby switch by selecting the appropriate Redundancy mode radio button.
3. When redundancy is selected as the operational state, in the Heartbeat Interval field specify the amount of time between heartbeat packets being sent or received between the two switches.
4. When redundancy is selected as the operational state, in the Revert Delay field specify the amount of time after not receiving a heartbeat packet before the standby switch will take over.
5. When redundancy is selected as the operational state, check the Preempt Standby box to prevent system standby on the redundant switches.
6. Click the check boxes in the **Subnet Redundancy** to select which subnets are enabled for redundancy.
7. Click **Apply** to save changes.

**Redundancy Operations Status**

To see the Operational Mode status for switch redundancy, look at the bottom of the Redundancy screen. Click the **Refresh** button to update the Operational Mode status.

**Updating the WS 2000 Wireless Switch’s Firmware**

From time to time, Symbol will release updates to the WS 2000 Wireless Switch’s firmware. These updates will include:

- Information about how to communicate with newly released Access Ports
- Updates for security issues that have been identified
- Fixes to any software problems that have been identified

**Checking for and Downloading Firmware Updates**

The switch administrator should check for firmware updates for the WS 2000 Wireless Switch on a monthly basis, as follows:

1. Select **System Configuration --> Firmware Update** or **Network Configuration --> System Settings** from the left menu.

2. Examine the **WS 2000 Version** field to record the version number of the currently loaded software. It should be something like 2.0.0.0-20

4. Compare the WS 2000 Version with the most recent version listed on the site. All updates will be listed along with a description of what the update contains.

5. Check to see if an administrator has already downloaded the file. It might already be on an FTP server at the site. If not, download the update from http://www.symbol.com/services/downloads/. Put the file on an FTP server, on a system with a TFTP server, or on a CompactFlash card that is compatible with the switch.

**Performing the Firmware Update**

To perform the update, the update file must be available from an FTP or TFTP site, or it must be on the CompactFlash card in the CF slot of the switch. The administrator supplies the site information and the WS 2000 Network Management System will perform the update for the administrator.

1. Save the WS 2000 Network Switch’s current configuration settings (System Configuration --> Config Import/Export)
2. Select System Configuration --> Firmware Update from the left menu to view the Firmware Update screen.
3. Specify the Filename of the firmware file with the update (such as WS_22343.bin).
4. Specify a folder pathname for an FTP login, if necessary.
5. Select one of the FTP, TFTP, or CP Card radio buttons, as appropriate.

**If FTP is selected:**

1. Specify whether the FTP server is on the WAN or is on one of the subnets associated with the switch by selecting the appropriate choice from the FTP Server on drop-down menu to the right of the radio button.
2. Specify the IP Address of the FTP server that has the update.
3. Specify a Username and Password that will allow the FTP login and access to the file.

**If TFTP is selected:**

1. Specify whether the TFTP server is on the WAN or is on one of the subnets associated with the switch by selecting the appropriate choice from the TFTP Server on drop-down menu to the right of the radio button.
2. Specify the IP Address of the TFTP server that has the update.

**Note**

When using TFTP as the upgrade method, be sure the TFTP server you are using supports files larger than 16MB. The WS2000’s firmware files are over 20MB in size and will cause the upgrade to fail if your TFTP server does not support files larger than 16MB.

**If CF Card is selected:**

1. Click the Display CF button to open a dialogue where you can browse the Compact Flash card’s filesystem to find or verify the firmware file and path.

**To Finish:**

1. Click the Perform Update button to initiate the firmware update for the switch. The update process will take a few minutes.
2. After the switch reboots, return to the Firmware Update screen. Read the Status field to verify that the firmware update completed successfully. The WS 2000 Version number at the top of the screen should have been updated.
3. Confirm that the wireless switch’s configuration settings are the same as prior to the update. If not, restore the settings.

**Formatting a Compact Flash Card**

If you need to erase the contents of a Compact Flash card you can do so on the Firmware Update screen.
Formatting a Compact Flash card will erase all data on the card. There is no undo option for formatting cards. Be sure that you do not need any data on the Compact Flash card before formatting it.

To format a Compact Flash card:
1. Navigate to System Configuration --> Cfg/Firmware Mgt --> Firmware Update screen.
2. Verify that the Compact Flash card is firmly seated in the WS2000's Compact Flash slot.
3. Click the Format CF button.
4. Click Yes to continue formatting the card.

Setting Up DHCP Options for Firmware Upload

It is also possible to configure the switch to receive firmware and configuration files automatically from a server using the Dynamic Host Configuration Protocol (DHCP). This features allows quick and automatic rollouts of new configurations or firmware updates across the network without manually updating each switch. Select [System Configuration] --> [Cfg/Firmware Mgt] --> DHCP Options (Sys Update) to configure the switch to accept DHCL downloads.

Setting Up the Switch

1. Check Enable Automatic Firmware Update to allow the WS 2000 Wireless Switch to automatically receive firmware updates from a server using the DHCP protocol. By default this option is disabled.
2. Check Enable Automatic Configuration Update to allow the WS 2000 to automatically receive configuration file updates from a server using DHCP. By default this option is disabled.
3. Set the Auto Upgrade Interval (in seconds) for the WS2000 to check the server for automatic updates.
4. Use the Interface menu to select the interface from which Firmware and Configuration updates will be received. This interface can be either the WAN port or any of the configured subnets on the switch. By default this value is set to **WAN**.
5. Optional: If you wish to change or specify a DHCP Vendor Class Id enter it here. **DHCP Vendor class ID** is used by the onboard DHCP clients as a unique identifier for Firmware/Config upgrade parameters. The external DHCP server which handles the DHCP client needs to be configured with this option to provide TFTP/FTP server IP, firmware file name and config file to facilitate WS2000 for Auto FW/Config upgrade. Any string provided in the text field will be prefixed with a “SymbolWS.WS2K-" string.

6. Navigate to the **Firmware** or **Config Import/Export** screen depending on whether you are setting up the automatic firmware download or configuration settings download. Set the TFTP server IP address to the IP address of the server what will do the download. Also set the name of the file to download.

Setting Up the DHCP Server

The external DHCP server will also needs to be configured appropriately. On a Windows server, you will need to select the appropriate options in the server setup. For a Linux server, edit the /etc/dhcpd.conf file to have the appropriate settings.

Exporting and Importing Wireless Switch Settings

All of the configuration settings for the WS 2000 Wireless Switch can be saved to a configuration file and then either imported back into the same switch or transferred to another switch. This file-based configuration saving feature provides several benefits:

- It can speed the switch setup process significantly at sites using multiple WS 2000 Wireless switches.
- It allows an administrator to “backup” the current switch configuration before making significant changes, before restoring the default configuration, or for precautionary measures.

Select **System Configuration --> Config Import/Export** from the left menu to import or export the switch configuration settings.
To Import or Export Settings to an FTP or TFTP Site

Use the following procedure for exporting the switch’s configuration settings.

1. Specify the name of the log **Filename** (under Server Options) to be written to or read from the FTP server.
2. Specify the **Server IP** address of the FTP server to which the log file will be imported or exported.
3. Specify the **Username** to be used when logging in to the FTP server. The user account must be established on the FTP server that is targeted for importing or exporting file data.
4. Specify the **Password** that will allow the user access to the FTP server for the import or export operation.
5. Click the appropriate import or export button with the given filename and login information.
   - Click the **FTP Import** button to import the configuration file from an FTP server.
   - Click the **TFTP Import** button to import the configuration file from a TFTP server.
   - Click the **FTP Export** button to export the configuration to a file on the FTP server.
   - Click the **TFTP Export** button to export the configuration to a file on the TFTP server.

When importing configuration settings, the system will display a confirmation window indicating that you must log out of the switch after the operation completes for the changes to take effect.

6. After executing the export, check the **Status** field for messages about the success or errors in executing the specified operation.

To Import Settings to a Local File

1. Click the **Upload A File** button in the HTTP Import/Export area to specify a configuration file name that can be specified within the file system.
2. Type in the name of the file, or use the **Browse** button to find and select the file to import.
3. Once the upload is successful, click the **Apply Uploaded File** button to apply the new configuration to the switch. Check the **Status** area in the lower portion of the window for any errors generated during the import process.

To Export Settings to a Local File

1. Click the **Generate File** button in the HTTP Import/Export area to specify a name for the configuration file.
2. Type in the name of the file. Use the **Browse** button to navigate to the desired directory.
3. Once the name is accepted, click the **Download File** button to write the configuration settings to the file.
4. After executing the export, check the **Status** field for messages about the success or errors in executing the specified operation.

Sample Configuration File

All of the configuration settings for the WS 2000 Wireless Switch can be saved to a configuration file and then either imported back into the same switch or transferred to another switch.

Below is a sample configuration file that has been annotated using comment lines. All comment lines begin with //</wbr> and are blue in color. The configuration file is organized by function area, and most areas correspond directly to a menu item.

```
//
// WS2000 Configuration Command Script
// System Firmware Version: 01.09-01
//
```
system
ws2000
// WS2000 menu
set name WS2000
set loc '0'
set email '0'
set cc 'us'
set airbeam mode disable
set airbeam enc-passwd a11e00942773
set applet lan enable
set applet wan enable
set applet slan enable
set applet swan enable
set cli lan enable
set cli wan enable
set snmp lan enable
set snmp wan enable
/

system
config

// Config menu
set server 192.168.0.10
set user 'jhatashi'
set enc-passwd '930f0c9f3c2c'
set file cfg.txt
set fw file mf.bin
set fw path '0'
/

system
logs

// Logs menu
set mode disable
set level L6
set ipadr 0.0.0.0
/

system
ntp

// NTP menu
set mode disable
set server 1 0.0.0.0
set server 2 0.0.0.0
set server 3 0.0.0.0
set port 1 123
set port 2 123
set port 3 123
/

system
snmp
access

// SNMP ACL configuration
delete acl all
// SNMP v1/v2c configuration

delete v1v2c all
add v1v2c public ro 1.3.6.1
add v1v2c private rw 1.3.6.1

// SNMP v3 user definitions
delete v3 all

/
system
snmp
traps

// SNMP trap selection
set cold disable
set cfg disable
set acl disable
set auth disable
set adopt disable
set unadopt disable
set ap-deny disable
set assoc disable
set unassoc disable
set mu-deny disable

// SNMP v1/v2c trap configuration
delete v1v2c all

// SNMP v3 trap configuration
delete v3 all

/

network
wlan

// WLAN 1 configuration
set mode 1 enable
set ess 1 101
set enc 1 none
set auth 1 none
set wep-mcm index 1 1
set wep-mcm enc-key 1 1 c2767fe55c0a564f90f50a3989
set wep-mcm enc-key 1 2 f2464fd56c3a667fa0c53a09b9
set wep-mcm enc-key 1 3 e2565fc57c2a766fb0d52a19a9
set wep-mcm enc-key 1 4 92262fb50c5a061fc0a55696d9
set kerb user 1 0
set kerb enc-passwd 1 8e57
set kerb realm 1 0
set kerb server 1 1 0.0.0.0
set kerb server 1 2 0.0.0.0
set kerb server 1 3 0.0.0.0
set kerb port 1 1 88
set kerb port 1 2 88
set kerb port 1 3 88
set eap server 1 1 0.0.0.0
set eap server 1 2 0.0.0.0
set eap port 1 1 1812
set eap port 1 2 1812
set eap enc-secret 1 1 8e57
set eap enc-secret 1 2 8e57
set eap reauth mode 1 disable
set eap reauth retry 1 2
set eap reauth period 1 3600
set eap adv mu-quiet 1 10
set eap adv mu-tx 1 5
set eap adv mu-timeout 1 10
set eap adv mu-retry 1 2
set eap adv server-timeout 1 5
set eap adv server-retry 1 2
set tkip type 1 phrase
set tkip enc-password 1 a1e0042273343de8b04
set tkip enc-key 1 c2767fe5564fa8cd328034b3986e787257f4a80cd64cf32905735
set tkip interval 1 86400
set tkip rotate-mode 1 disable
set name 1 WLAN1
set no-mu-mu 1 disable
set vop 1 enable
set adopt 1 allow
set acl 1 allow
set mcast 1 1 01005e000000
set mcast 1 2 09000e000000
delete 1 all

// WLAN 2 configuration
set mode 2 disable
set ess 2 102
set enc 2 none
set auth 2 none
set wep-mcm index 2 1
set wep-mcm enc-key 2 1 c2767fe5564fa8cd328034b3986e787257f4a80cd64cf32905735
set wep-mcm enc-key 2 2 f2464fd56c3a667fa0c53a09b9
set wep-mcm enc-key 2 3 e2565fc57c2a766fbdd52a19a9
set wep-mcm enc-key 2 4 92262fb50c5a061fc0a5a69d9
set kerb user 2 "admin"
set kerb password 2 8e57
set kerb realm 2 "admin"
set kerb server 2 1 0.0.0.0
set kerb server 2 2 0.0.0.0
set kerb server 2 3 0.0.0.0
set kerb port 2 1 88
set kerb port 2 2 88
set kerb port 2 3 88
set eap server 2 1 0.0.0.0
set eap server 2 2 0.0.0.0
set eap port 2 1 1812
set eap port 2 2 1812
set eap enc-secret 2 1 8e57
set eap enc-secret 2 2 8e57
set eap reauth mode 2 disable
set eap reauth retry 2 2
set eap reauth period 2 3600
set eap adv mu-quiet 2 10
set eap adv mu-tx 2 5
set eap adv mu-timeout 2 10
set eap adv mu-retry 2 2
set eap adv server-timeout 2 5
set eap adv server-retry 2 2
set tkip type 2 phrase
set tkip enc-phrase 2 a11e00942773343deb84
set tkip enc-key 2 c2767fe55c0a564fa8cd3201b1984a33f8b8e78725727f40a80c6dcff32905735
set tkip interval 2 86400
set tkip rotate-mode 2 disable
set name 2 WLAN2
set no-mu-mu 2 disable
set vop 2 enable
set adopt 2 allow
set acl 2 allow
set mcast 2 1 01005E000000
set mcast 2 2 09000E000000
delete 2 all

// WLAN 3 configuration
set mode 3 disable
set ess 3 103
set enc 3 none
set auth 3 none
set wep-mcm index 3 1
set wep-mcm enc-key 3 1 c2767fe55c0a564f90f50a3f8b4
set wep-mcm enc-key 3 2 f2464fd56c3a667f5a53f409b6
set wep-mcm enc-key 3 3 e25b5f5c57c2a766f1fb052a15a9
set wep-mcm enc-key 3 4 922b2f95b565b6f1f0a55a6b9d9
set kerb user 3 0
set kerb enc-passwd 3 9e57
set kerb realm 3 0
set kerb server 3 1 0.0.0.0
set kerb server 3 2 0.0.0.0
set kerb server 3 3 0.0.0.0
set kerb port 3 1 1812
set kerb port 3 2 1812
set kerb port 3 3 1812
set eap server 3 1 0.0.0.0
set eap server 3 2 0.0.0.0
set eap port 3 1 1812
set eap port 3 2 1812
set eap adv mu-quiet 3 10
set eap adv mu-tx 3 5
set eap adv mu-timeout 3 10
set eap adv mu-retry 3 2
set eap adv server-timeout 3 5
set eap adv server-retry 3 2
set tkip type 3 phrase
set tkip enc-phrase 3 a11e00942773343deb84
set tkip enc-key 3 c2767fe55c0a564fa8cd3201b1984a33f8b8e78725727f40a80c6dcff32905735
set tkip interval 3 86400
set tkip rotate-mode 3 disable
set name 3 WLAN3
set no-mu-mu 3 disable
set vop 3 enable
set adopt 3 allow
set acl 3 allow
set mcast 3 1 01005E000000
set mcast 3 2 09000E000000
delete 3 all

/ network
ap
default

// Default 802.11 A radio configuration
set reg A in/out 149 100
set rate A 6 54
set div A enable
set beacon mode A disable
set beacon intvl A 100
set rts A 2341
set dtim A 10
set short-pre A enable
set primary A 1

// Default 802.11 B radio configuration
set reg B in/out 1 100
set rate B 1 11
set div B enable
set beacon mode B disable
set beacon intvl B 100
set rts B 2341
set dtim B 10
set short-pre B enable

/
// Access Port configuration
network
ap
delete 1 all
delete 2 all
delete 3 all

/
// LAN configuration
network
lan

// LAN configuration
set mode 1 enable
set name 1 Subnet1
set ipadr 1 192.168.0.1
set mask 1 255.255.255.0
set mode 2 disable
set name 2 Subnet2
set ipadr 2 192.168.1.1
set mask 2 255.255.255.0
set mode 3 disable
set name 3 Subnet3
set ipadr 3 192.168.2.1
set mask 3 255.255.255.0

// Port To Subnet Map configuration
set port 1 s1
set port 2 s1
set port 3 s1
set port 4 s1
set port 5 s1
set port 6 s1

// WLAN To Subnet Map configuration
set wlan 1 s1
set wlan 2 s2
set wlan 3 s3

/

network
lan
dhcp

// LAN DHCP configuration
set mode 1 server
set dgw 1 192.168.0.1
set dns 1 1 192.168.0.1
set dns 1 2 192.168.0.1
set lease 1 86400
set range 1 192.168.0.100 192.168.0.254
set mode 2 server
set dgw 2 192.168.1.1
set dns 2 1 192.168.1.1
set dns 2 2 192.168.1.1
set lease 2 86400
set range 2 192.168.1.100 192.168.1.254
set mode 3 server
set dgw 3 192.168.2.1
set dns 3 1 192.168.2.1
set dns 3 2 192.168.2.1
set lease 3 86400
set range 3 192.168.2.100 192.168.2.254

delete 1 all
delete 2 all
delete 3 all

/

network
wan

// WAN configuration
set dhcp enable
set mask 255.255.255.0
set dgw 0.0.0.0
set dns 1 0.0.0.0
set dns 2 0.0.0.0
set pppoe mode disable
set pppoe user '0'
set pppoe enc-passwd 8e57
set pppoe idle 600
set pppoe ka disable
set pppoe type pap/chap
set mode 1 enable
set ipadr 1 0.0.0.0
set mode 2 disable
set ipadr 2 0.0.0.0
set mode 3 disable
set ipadr 3 0.0.0.0
set mode 4 disable
set ipadr 4 0.0.0.0
set mode 5 disable
set ipadr 5 0.0.0.0
set mode 6 disable
set ipadr 6 0.0.0.0
set mode 7 disable
set ipadr 7 0.0.0.0
set mode 8 disable
set ipadr 8 0.0.0.0

/ network
wan
fw

// Firewall configuration
set syn enable
set src enable
set win enable
set ftp enable
set ip enable
set seq enable
set mime filter enable
set mime len 8192
set mime hdr 16

/ network
wan
nat

// NAT configuration
set type 1 1-to-many
set outb ip 1 0.0.0.0
set inb mode 1 disable
set inb ip 1 0.0.0.0
set type 2 none
set outb ip 2 0.0.0.0
set inb mode 2 disable
set inb ip 2 0.0.0.0
set type 3 none
set outb ip 3 0.0.0.0
set inb mode 3 disable
set inb ip 3 0.0.0.0
set type 4 none
set outb ip 4 0.0.0.0
set inb mode 4 disable
set inb ip 4 0.0.0.0
set type 5 none
set outb ip 5 0.0.0.0
set inb mode 5 disable
set inb ip 5 0.0.0.0
set type 6 none
set outb ip 6 0.0.0.0
set inb mode 6 disable
set inb ip 6 0.0.0.0
set type 7 none
set outb ip 7 0.0.0.0
set inb mode 7 disable
set inb ip 7 0.0.0.0
set type 8 none
set outb ip 8 0.0.0.0
set inb mode 8 disable
set inb ip 8 0.0.0.0

// Outbound 1-To-Many NAT configuration
set outb map s1 1
set outb map s2 1
set outb map s3 1

// Inbound NAT configuration
delete inb 1 all
delete inb 2 all
delete inb 3 all
delete inb 4 all
delete inb 5 all
delete inb 6 all
delete inb 7 all
delete inb 8 all
/

// Subnet map configuration
network
submap
set default s1 w allow
set default s1 s2 allow
set default s1 s3 allow
set default s2 w allow
set default s2 s1 allow
set default s2 s3 allow
set default s3 w allow
set default s3 s1 allow
set default s3 s2 allow
delete s1 all
delete s2 all
delete s3 all
/

// Router configuration
network
router
set type off
set dir both
set auth none
set enc-passwd Be57
set id 1 1
set enc-key 1 e2565fc57c2a76f6b075160d6f92952
set id 2 1
set enc-key 2 e2565fc57c2a76f6b075160d6f92952
delete all
/
save
Configuring SNMP

The Simple Network Management Protocol (SNMP) facilitates the exchange of management information between network devices. SNMP allows an administrator to manage network performance, find and solve network problems, and plan for network growth. The WS 2000 Wireless Switch includes SNMP management functions for gathering information from its network components, and communicating that information to specific users. For more background about SNMP, see SNMP Management Support. There are four different SNMP screens.

- Use the SNMP Access screen to define SNMP v1/v2c community definitions and SNMP v3 user definitions associated with access.
- Use the SNMP Trap Configuration screen to define SNMP v1/v2c community definitions and SNMP v3 user definitions associated with the traps themselves. Trap configuration depends on the network machine that receives the generated traps.
- Use the SNMP Traps screen to enable system, network, SNMP, mobile unit, and Access Port traps.
- Use the SNMP Rate Traps screen to enable traps by setting RF Rate thresholds.

Select System Configuration --> SNMP Access from the left menu to set up SNMP service.

Setting the SNMP Version Configuration

The SNMP Access screen allows the administrator to define SNMP v1/v2c community definitions and SNMP v3 user definitions. SNMP v1 and v2c provide a strong network management system, but their security is relatively weak. SNMP v3 provides greatly enhanced security protocols. SNMP v3 encrypts transmissions and provides authentication for users generating requests.

Setting Up SNMP v1/v2c Community Definitions

SNMP v1/v2c community definitions allow read-only or read/write access to switch-management information, as appropriate. The SNMP community, in this case, includes users whose IP addresses are specified on the SNMP Access
Control subscreen. A read-only community string allows a remote device to retrieve information, while a read/write community string also allows a remote device to modify settings. Set up a read/write definition to facilitate full access by the administrator.

1. To create a new community definition, click the Add button in the SNMP v1/v2c Community Configuration area.
2. Type in a site-appropriate name for the community.
3. Click in the OID cell of the table. Either use the OID (Object Identifier) pull-down menu to select the default OID or type in an OID number into the field. (The format is in a numerical dot notation, and valid numbers can be found within the MIB.)
   If is selected, the community will have access to all the OIDs (SNMP parameters) in the SNMP Management Information Base (MIB) file. If a custom OID is entered, the administrator can allow access to specific OIDs in the MIB to certain communities.
4. Use the Access pull-down menu to specify read-only (R) access or read/write (RW) access for the community. Read-only access allows a remote device to retrieve switch information, while read/write access also allows a remote device to modify switch settings.
5. Follow the directions for Setting up the Access Control List (below).

### Setting Up SNMP v3 Community Definitions

Setting up the v3 user definition is very similar to the v1/v2c community definitions. The difference is the addition of a user security level and a user password.

1. To create a new SNMP v3 user definition, click the Add button in the SNMP v3 User Definitions area.
2. Specify a user name in the Username field.
3. Select a security level from the Security pull-down menu. Select from the following choices:
   - noAuth (no authorization) Allows the user to access SNMP without authorization or encryption
   - AuthNoPriv (authorization without privacy) Requires the user to login, however no encryption is used
   - AuthPriv (authorization with privacy) Requires the user to login and encryption is used
4. Click in the OID cell of the table. Either use the OID (Object Identifier) pull-down menu to select the default OID or type in an OID number into the field. (The format is in a numerical dot notation, and valid numbers can be found within the MIB.)
   If is selected, the community will have access to all the OIDs (SNMP parameters) in the SNMP Management Information Base (MIB) file. If a custom OID is entered, the administrator can allow access to specific OIDs in the MIB to certain communities.
5. Click the **Password** button in the cell and the **Password Settings** screen appears.

6. Select an **Authentication Algorithm** from the drop-down menu, either **MD5** or **SHA1**.

7. Type in an **Authentication Password**.

8. Select a Privacy Algorithm from the drop-down menu. The options include:
   - **DES**
   - **AES 128-bit**

9. Type in a **Privacy Password** that matches the algorithm.

10. Click **Ok**, when done.

11. Use the **Access** pull-down menu to specify read-only (R) access or read/write (RW) access for the community. Read-only access allows a remote device to retrieve switch information, while read/write access also allows a remote device to modify switch settings.

12. Follow the directions for setting up the Access Control List (below).

**Setting Up the Access Control List**

To set up the Access Control list as specified by a range of IP addresses, click the **SNMP Access Control** button at the bottom of the SNMP Access screen. The SNMP Access Control screen appears:

1. Click the **Add** button to create a new entry in the Access Control table.

2. Specify the IP address for the user(s) that have access. Enter an IP address only in the **Starting IP Address** column to specify an address for a single SNMP user. Enter both the **Starting IP Address** and **Ending IP Address** columns to specify a range of addresses for SNMP users.

3. Click **Ok** to save changes and return to the SNMP Access screen.
**Setting the Trap Configuration**

To set the trap notification destination for SNMP, select *System Configuration --> SNMP Access --> SNMP Trap Configuration* from the left menu.

**Setting the Trap Configuration for SNMP v1/v2c**

To set the trap notification destination for the SNMP v1/v2c servers, add one or more entries to SNMP v1/v2c Trap Configuration table.

1. Click the **Add** button to add a new entry to the table.
2. Specify a **Destination IP** addresses for the systems that will receive notification when an SNMP trap is generated.
3. Specify a destination User Datagram Protocol (UDP) port for receiving the traps that are sent by SNMP agents. UDP offers direct connection for sending and receiving datagrams over an IP network.
4. Specify a **Community** name that matches one of the community names added on the SNMP Access screen.
5. Select the appropriate **SNMP Version (v1 or v2)** from the pull-down menu for this particular SNMP server.
6. Click the **Apply** button to save the entries.

**Setting the Trap Configuration for SNMP V3**

To set the trap notification destination for the SNMP v3 servers, add one or more entries to SNMP v3 Trap Configuration table.

1. Click the **Add** button to add a new entry to the table.
2. Specify a **Destination IP** addresses for the systems that will receive notification when an SNMP trap is generated.
3. Specify a destination User Datagram Protocol (UDP) port for receiving the traps that are sent by SNMP agents. UDP offers direct connection for sending and receiving datagrams over an IP network.
4. Specify a **Username** that matches one of the user names added on the SNMP Access screen.

5. Specify a **Security** level from *noAuth* (no authorization required), *AuthNoPriv* (authorization without encryption), or *AuthPriv* (authorization with encryption).

6. Specify a password for the user.

   **Note**

   When entering the same username on the SNMP Traps and SNMP Access screens, the password entered on the SNMP Traps page will overwrite the password entered on the SNMP Access page. To avoid this problem enter the same password on both pages.

7. Click the **Apply** button to save changes

### Selecting Traps

The SNMP Trap screen allow the administrator to specify the types of network events that generate traps, and who to notify regarding the events. SNMP traps are generated according to predefined types of network events that are considered important to manage. This information is asynchronously reported to the switch’s SNMP network-management system by switch-managed entities. Notification is sent to the responsible individuals whose IP addresses are listed for trap notification.

1. To set the SNMP traps, select **System Configuration --> SNMP Access --> SNMP Traps** from the left menu.

2. Check the type of traps to enable the generation of notification events.

<table>
<thead>
<tr>
<th>Trap Category</th>
<th>Trap Name</th>
<th>Generates a Trap whenever…</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Traps</strong></td>
<td><strong>System Cold Start</strong></td>
<td>The switch’s router reinitializes while transmitting, possibly altering the agent’s configuration or protocol entity implementation.</td>
</tr>
<tr>
<td></td>
<td><strong>Configuration Changes</strong></td>
<td>SNMP access or management functions are reconfigured.</td>
</tr>
<tr>
<td>Trap Category</td>
<td>Trap Name</td>
<td>Generates a Trap whenever…</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Network Traps</td>
<td>User Login Failure</td>
<td>A user fails to successfully login from the CLI or Applet.</td>
</tr>
<tr>
<td></td>
<td>Admin Password Change</td>
<td>A change is made to the Admin user password.</td>
</tr>
<tr>
<td></td>
<td>Low Compact Flash Memory</td>
<td>The Compact Flash card in the system falls below the amount specified.</td>
</tr>
<tr>
<td></td>
<td>Physical port status change</td>
<td>The status changes for one of the ports on the front of the WS 2000, such as if a device is plugged into or unplugged from the switch, or if the link is lost between the switch and the connected device.</td>
</tr>
<tr>
<td></td>
<td>Interface Status Change</td>
<td>An interface on the switch's status changes from its configured state.</td>
</tr>
<tr>
<td></td>
<td>DynDNS Update</td>
<td>If Dynamic DNS services are configured on the WAN a new trap is set when there is a Dynamic DNS update.</td>
</tr>
<tr>
<td></td>
<td>Denial of service (DOS) attempts</td>
<td>A Denial of Service attack is detected by the switch's firewall. A new trap will be sent at the interval specified until the attack has stopped.</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>SNMP authentication failures</td>
<td>An SNMP-capable client is denied access to the switch's SNMP management functions or data. This may result from incorrect login.</td>
</tr>
<tr>
<td></td>
<td>SNMP ACL violation</td>
<td>An SNMP client cannot access SNMP management functions or data due to an Access Control List (ACL) violation.</td>
</tr>
<tr>
<td>MU Traps</td>
<td>MU associated</td>
<td>An MU becomes associated with one of the switch's Wireless Local Area Networks (WLANs).</td>
</tr>
<tr>
<td></td>
<td>MU unassociated</td>
<td>An MU becomes unassociated with (or gets dropped from) one of the switch's WLANs.</td>
</tr>
<tr>
<td></td>
<td>MU denied association</td>
<td>An MU cannot associate with the switch-managed network, for example due to an absent or incorrectly specified MAC address on a WLAN Security screen.</td>
</tr>
<tr>
<td></td>
<td>MU denied authentication</td>
<td>An MU is denied authentication on one of the switch's WLANs, which can be caused by the MU being set for the wrong authentication type for the WLAN or by an incorrect key or password.</td>
</tr>
<tr>
<td>AP Traps</td>
<td>AP adopted</td>
<td>Any of the switch's Wireless Local Area Networks (WLANs) adopts an AP.</td>
</tr>
<tr>
<td></td>
<td>AP unadopted</td>
<td>Any of the switch's WLANs unadopts (or drops) an AP.</td>
</tr>
<tr>
<td></td>
<td>AP denied adoption</td>
<td>Any of the switch's WLANs deny the adoption of an AP.</td>
</tr>
<tr>
<td></td>
<td>AP detected radar (802.11a only)</td>
<td>An 802.11a AP 300 Access Port detects radar during its startup or ongoing radar scans. This trap only applies to the 802.11a radio of an AP 300 Access Port operating with Dynamic Frequency Selection and Transmit Power Control (DFS/TPC).</td>
</tr>
</tbody>
</table>
3. Click the **Apply** button to save the trap settings.
4. It is necessary to tell the switch where to send the notifications. Make sure to set the trap configuration to indicate where to send the notifications.

**Setting RF Traps**

A screen is also available to specify traps caused when certain rates of activities either exceed or drop below a specified threshold. To set rate traps, select **System Configuration** --> **SNMP Access** --> **SNMP RF Traps** from the left menu.

<table>
<thead>
<tr>
<th>Trap Category</th>
<th>Trap Name</th>
<th>Generates a Trap whenever…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotspot Traps</td>
<td>Hotspot MU State Change</td>
<td>An MU using the switch’s Hotspot feature is authenticated, unauthenticated or dropped.</td>
</tr>
</tbody>
</table>

1. Select the threshold type for which you want a rate trap, such as Pkts/sec.
2. Determine whether you want the rate to apply to **Switch** (the switch as a whole), **Wlan** (for each WLAN enabled), **Ap** (each associated Access Port), or **Mu** (each mobile unit connected to the switch).
3. Type in the threshold rate into the field associated with the selected object.
4. Traps are only generated for those field where numbers exist. Explanation of the different threshold types are listed below.

- **Pkts/s**: The maximum threshold for the number of packets per second before a trap is sent.
- **Throughput**: The maximum threshold for the total throughput in Mbps (Megabits per second) for each of the devices before a trap is sent.
- **Average Bit Speed**: The minimum threshold for the average bit speed in Mbps (Megabits per second) for each of the devices before a trap is sent.
- **% Non-Unicast**: The maximum threshold for the total percentage of packets that are non-unicast for each of the devices before a trap is sent. Non-unicast packets include broadcast and multi-cast traffic.
- **Average Signal**: The minimum threshold for the average signal strength in dBm for each of the devices before a trap is sent.
- **Average Retries**: The maximum threshold for the average number of retries for each of the devices before a trap is sent.
- **% Gave Up**: The maximum threshold for the total percentage of packets that are given up for each of the devices before a trap is sent.
- **% Dropped**: The maximum threshold for the total percentage of packets that are dropped for each of the devices before a trap is sent.
- **% Undecryptable**: The maximum threshold for the total percentage of packets that are undecryptable for each of the devices before a trap is sent. Undecryptable packets can be the result of corrupt packets, bad CRC checks, or incomplete packets.
- **Associated MUs**: The maximum threshold for the total number of MUs associated with each of the devices before a trap is sent.

Enter the minimum number of packets that must pass through the device before an SNMP rate trap will be sent. It is recommended to set this value no less than 1000.

**Specifying a Network Time Protocol (NTP) Server**

Network Time Protocol (NTP) manages time and clock synchronization in a network environment. The switch, which acts as an NTP client, periodically synchronizes its clock with a master clock on an NTP server. Time synchronization is typically optional (although recommended) for the switch’s network operations; however, for sites using Kerberos authentication, time synchronization is required. Kerberos must synchronize the clocks of its Key Distribution Center (KDC) server(s).
Select **System Configuration --> NTP Servers** from the left menu to enable NTP. The NTP Server screen appars.

![NTP Server screenshot](image)

1. The field on the left of the Current Time area displays what the switch believes is the current time. Click the **Refresh** button to update that time. If an NTP server is configured, the switch will go out to the network to update its current time.

2. To enable time service on the switch, check the **Enable NTP on WS 2000** checkbox and continue with the rest of the steps below.

3. Specify a **Preferred Time Server**, and optionally a **First Alternate Time Server** and a **Second Alternate Time Server** by specifying the IP address and Port for the time service for each server. The default port is 123. The more NTP servers specified, the greatest assurance there is of uninterrupted time synchronization.

4. Specify a **Synchronization Interval** (in minutes). By default, the switch will synchronize the time every 15 minutes.

5. Click the **Apply** button to save any changes made on this screen.

**Setting Up and Viewing the System Log**

The WS 2000 Network Management System keeps a log of the events that happen on the switch. The switch has a modest of amount of memory to store events. If the administrator wishes to keep a more complete event history, the administrator needs to enable a log server.
To view the log or set up a log server, select **System Configuration -- Logs** from the left menu.

**Viewing the Log on the Switch**

To save a log of the most recent events that are retained on the switch, click the **View** button. The system will display a prompt asking for the administrator password. After the password has been entered, click the **Get File** button and a dialogue will be displayed with buttons to **Open** or **Save** the log.txt file. Click **Save** and specify a location to save the file.

To view the saved log.txt file on a Microsoft Windows based computer use the WordPad application. Viewing the log file with Notepad, the default text file view on most Windows based computers, will not properly display the formatting of the log file.

**Setting Up a Log Server**

To keep a complete history of the events that are logged by the switch, the administrator needs to set up an external system log on a server. The server listens for incoming switch-generated syslog messages on a UDP port (514 by default), and then decodes the messages into a log file appropriate for viewing and printing. Events are categorized into eight levels (0 through 7), with the lowest numbers representing the most critical issues.

1. Set the level of the errors to be logged from the **Logging Level** drop-down menu. All events associated with the selected level and events with levels lower than the selection will be recorded.
2. Check the **Enable logging in to an external syslog server** checkbox to enable logging.
3. Specify the Syslog server IP address for the server that will store the log.
4. Select **Apply** to save the changes.
5. Select **Network Configuration -- Subnet Access**. Work through all the combinations of subnet-to-WAN accesses to ensure that DNS communications are allowed. (UDP must be enabled to save the log entries.)
Configuring HotSpot

Overview ................................................................. 8-2
  Requirements ........................................................... 8-2
Configuring Hotspot ..................................................... 8-3
  Handling log-in’s and redirection .................................... 8-4
  Authentication (RADIUS) ............................................. 8-4
  Accounting (RADIUS) .................................................. 8-5
8.1 Overview

The hotspot feature enables the WS2000 Wireless Switch to act as a single on-site solution to provide wireless LAN hotspots and management.

The hotspot access controller enables hotspot operators to provide user authentication and accounting without a special client application. It enables a web browser as a secure authentication device. Instead of relying on the built-in security features of 802.11 to control privileges to an access port, you can configure a WLAN as an open network with hotspot authentication. The WS2000 Wireless Switch provides an IP address to the user through its built-in DHCP server, authenticates the user, and enables the user to access the Internet.

8.1.1 Requirements

The hotspot feature requires the following:

- HTTP redirection: Redirects unauthenticated users to a specific page specified by the Hotspot provider.
- User authentication: Authenticates users using a RADIUS server.
- Walled garden support: Enables a list of IP address (not domain names) to be accessed without authentication.
- Billing system integration: Sends accounting records to a RADIUS accounting server.
8.2 Configuring Hotspot

To configure the hotspot access controller on the WS2000 Wireless Switch:

1. Configure a subnet as outlined in the LAN/Subnet Configuration chapter and enable hotspot on that subnet.
2. Create a set of allowed destination IP addresses. These allowed destination IP addresses are also called a white list.

The login, welcome, and fail pages are maintained on a subnet-by-subnet basis. It can be hosted locally or remotely. To enable remote access to websites, you must enter a fully qualified URL.
8.2.1 Defining the Hotspot State of a Mobile Unit.

When configured as a hotspot, the switch tracks the hotspot-state of each mobile unit associated with the hotspot. The server maintains a list of all mobile units associated and tracks the state of these mobile units.

Mobile Units in a hotspot have one of the following two states:

- **REDIRECT state**—The associated mobile unit enters the REDIRECT state after 802.11 authentication and association. The mobile unit remains in this state until it successfully authenticates through the RADIUS server. After the mobile unit logs-off from the hotspot, it moves into the REDIRECT State.

- **RADIUS AUTHENTICATED state**—The mobile unit moves into the RADIUS AUTHENTICATED state after it successfully authenticates through the RADIUS server.

The RADIUS server provides the trigger to move the state of the mobile unit from REDIRECT to RADIUS AUTHENTICATED. There is a dedicated socket connection between the wireless switch and the RADIUS server for this purpose.

After the RADIUS server successfully authenticates the mobile unit, it sends a trigger to the wireless switch to change the hotspot-state of the mobile unit to RADIUS-AUTHENTICATED.

When the mobile unit requests the RADIUS server to log out, the RADIUS server again sends a trigger to the wireless switch to change the state of the mobile unit to REDIRECT.

8.2.2 Handling log-ins and redirection

When a client requests a URL from a web server, the login handler returns an HTTP redirection status code in the range 300-399 (for example, **301 Moved Permanently**), which indicates to the browser that it should look for the page at another URL.

This other URL can be a local or remote login page (based on the hotspot configuration). The login page URL is specified in the location HTTP header.

After the response with status code **301 Moved Permanently**, the client’s browser issues a request for the URL specified in the response header. The client’s browser, then displays the WS2000 login page.

To host a login page on the external web server, the IP address of that web server should be in the White list (list of IP addresses that are allowed to access the server) configuration. Ensure that the login page is designed so that the submit action always posts the login data on the WS2000 Wireless Switch.

When the login information is submitted to the WS2000 Wireless Switch, the login handler runs a CGI script that uses this data as input and sends the user the response from the CGI script.

8.2.3 Authentication (RADIUS)

The CGI script has a RADIUS client built in it, which receives the posted login data and initiates RADIUS authentication.

If the RADIUS authentication for that user is successful, the CGI script does the following:

1. Sends a command to wireless switch to change the MU state from REDIRECT to RADIUS-AUTHENTICATED.
2. Replies back to the login handler to generate an HTTP redirection response for Welcome page.
3. Starts the RADIUS accounting for the user.
4. Click the **Logout** button on the Welcome page to log out of the switch at any point.
The Welcome page will contain **Logout** button, which user can click at any point to logout from the system. Again the Remote Welcome page needs to be setup such that the logout request should be sent to WS2000. If the RADIUS authentication for that user is failed the CGI script will reply back to the Login Handler to generate an HTTP redirection response for Fail page.

Upon logout another CGI script is executed. The CGI script will use `REMOTE_ADDR` environment variable to get the IP address of the requester and verify its MAC address from ARP table. Then CGI script will stop the RADIUS accounting for that client and sends a command to wireless switch to change the MU state back to REDIRECT.

### 8.2.4 Accounting (RADIUS)

Upon successful login a CGI script will generate an Accounting Start packet describing the type of service being delivered and the client. The script will then send that information to the RADIUS Accounting server, which will reply with an acknowledgement that the packet has been received.

If a client logs out or an MU becomes unassociated an Accounting Stop packet will be generated describing the type of service that was delivered, statistics and elapsed time. That packet will be sent to the RADIUS accounting server, which will reply with an acknowledgement that the packet has been received.
Using DDNS

Overview ................................................................. 9-2
Enabling DDNS .......................................................... 9-2
Updating DNS Entries using DDNS ................................. 9-4
  Updating DNS Entries for a Single Subnet ......................... 9-4
9.1 Overview

When browsing web sites or sending E-mail messages a domain name is used. For example, the URL www.yahoo.com and the e-mail address user@yahoo.com contains the domain name yahoo.com. Domain names allow users to remember the address to a site without knowing the IP address. For traffic to be routed on a network those domain names must first be converted to an IP address. When a domain name is entered the domain is translated to an IP address by a Domain Name Server (DNS).

DNS translation poses the following challenges:

- There are a limited number of IP addresses currently available.
- Domain names and IP addresses are created and changed everyday.

Dynamic Domain Name System (DDNS) enables you to link a domain name to a changing IP address. When you connect to the Internet, your Internet service provider uses Dynamic Host Configuration Protocol (DHCP) and assigns the domain an unused IP address from a set pool of IP addresses. This IP address is only used for the duration of this specific connection. This method of dynamically assigning addresses, increases the pool of available IP addresses.

The DDNS service maintains a database to connect a domain name to an IP address on the Internet. Because the IP addresses change, it is necessary to update the DNS database with the current IP address for a given domain name. The DDNS service performs these updates.

Enabling Dynamic DNS will allow domain name information to be updated when the IP address associated with that domain changes. When a MU associates and gets and IP address from the DHCP server the DHCP server then updates the DNS server with the IP allocated to the corresponding hostname.

9.2 Enabling DDNS

Dynamic DNS is configured on a per-subnet basis and requires the subnet to be configured as a DHCP Server. DDNS is then enabled and configured in the Advanced DHCP Server screen for the corresponding subnet.
1. From the Subnet screen for the desired subnet select the radio button next to **This interface is a DHCP Server** and enter a range of IPs in the **Address Assignment Range** fields.

2. Click the **Advanced DHCP Server** button to open the Advanced DHCP window.

3. In the Advanced DHCP Server window check the box next to **Enable Dynamic DNS**.

4. Select either **Single User Class Option** or **Multiple User Class Option** depending on the settings of your DHCP clients.

   Any DHCP client can send the User Class Id either in the Single or Multiple user class ID format. The Single or Multiple User class option is provided to enable the switch to interpret the correct format in...
which the user class ID is sent by the client. The switch then retrieves the correct value of the user class ID sent by the DHCP client based on the selected format. This same user class ID format is used for the DDNS messages.

5. Enter IP Addresses in Primary DNS Server, Secondary DNS Server and Default Gateway and click the Ok button to return the Subnet configuration screen.

6. Click the Apply button on the Subnet configuration screen to save the changes and activate DDNS for that subnet.

9.3 Updating DNS Entries using DDNS

Once DDNS has been configured and enabled for a subnet it is possible to manually refresh the DNS entries for all active DHCP clients on a single subnet or on all active subnets.

9.3.1 Updating DNS Entries for a Single Subnet

The DNS entries for a single subnet can be updated using the following steps.

1. Select the subnet you wish to refresh from the menu tree on the left side of the screen.

2. From the Subnet configuration screen click the Update DNS button located in the DHCP section of the screen.

After the Update DNS button has been clicked, an ADD DNS message for all the active leases on the DHCP server for that subnet is sent to the DNS server. A DELETE DNS message for all the inactive leases on the DHCP server for that subnet is sent to the DNS server.
9.3.2 Updating DNS Entries for All Active Subnets

The DNS entries for all active subnets can be updated using the following steps.

1. Select **LAN** from menu tree on the left side of the screen.

2. From the DNS Update section of the screen click the **Update DNS for All Subnets** button located in the DHCP section of the screen.

After the **Update DNS for All Subnets** button has been clicked, an ADD DNS message for all the active leases on the DHCP servers for all active subnets is sent to the DNS server. A DELETE DNS message for all the inactive leases on the DHCP server for all active subnets is sent to the DNS server.
Trunking VLANs Through the WAN Port

Overview ........................................... 10-2
Assigning VLAN Tags to Packets ....................... 10-2
Installation Considerations and Default VLAN Settings ........................................... 10-2
Configuring VLAN Trunking ................................ 10-3
Mapping WLANs to VLANs ................................ 10-4
10.1 Overview

In previous versions of the WS2000 there was a limit of 31 VLAN IDs, from 1 to 31 due to limitations in the LAN port switch hardware. In the deployments which had existing VLAN configurations with VLAN ID above 31, it was difficult to make the WS2000 fit in seamlessly with the existing network topology.

To enable easier integration into networks with existing VLAN infrastructure, you can now configure the existing WAN port as a Trunk-Port and the user can configure any VLAN-IDs in the range 1-4094. With this setup, the WAN port can be configured either as a TRUNK port or as a WAN Link.

10.1.1 Assigning VLAN Tags to Packets

VLAN tag assignment to packets is achieved as follows:

- Wired hosts are assigned VLANs based on the Port to which they are connected.
- Wireless hosts, upon successful authentication, are assigned VLANs based on the WLAN through which they authenticate.

The WS2000 then maintains a table to store the hosts to VLAN mapping information.

Packets coming in from the LAN ports are handled as follows:

- For unicast packets destined to hosts on the same VLAN, the LAN switch handles the packet if both the hosts are wired.
- For unicast packets destined to hosts on the same VLAN, the WS2000 switches the packet.
- For broadcast packets, the same packet is duplicated and forwarded to all hosts on the same VLAN.

10.2 Installation Considerations and Default VLAN Settings

By default the WAN port is configured as a WAN LINK. This port has a default VLAN ID of 1.

After upgrading the WS2000 to version 2.1, the WAN port can be configured as either a WAN Link or as a TRUNK port. The user can configure any VLAN IDs between 1 and 4094.

- The Factory Setting for the WS2000 Version 2.1 would be as follows:
- Native VLAN by default is VLAN ID 1
- No Trunk Port is configured.
- The WAN port is configured as a WAN Link.
- No VLANs are enabled for Trunking.
10.3 Configuring VLAN Trunking

Use the following steps to configure VLAN trunking on the WAN port.

1. From Network Configuration section of the menu select VLAN to open the VLAN Configuration screen.

2. From the VLAN Type pulldown select either Port Based or User Based depending on your network’s existing VLAN settings.

   User Based VLANs, also known as MAC-based VLANs, partition traffic based on the MAC addresses of their members. The switch inspects frames and partitions information based on the VLAN associated with the MAC address. The advantage of this scheme is that it allows a client to move from one physical location to another and still be a member of the same VLAN. The disadvantage of User Based VLANs is that each client’s MAC address must be manually added to the VLAN, which can be very time consuming for large network deployments.

   Port Based VLANs, also known as Layer 3 VLANs, partitions traffic based on protocol. The switch inspects each packet, extracts the VLAN membership information, and partitions the packet accordingly. The advantage of this scheme is that it allows partitioning based on protocol type, and each client does not have to be manually added to the VLAN. The disadvantage of Port Based VLANs is that network performance is generally slower than with User Based VLANs. This performance loss is due to the large amount of overhead required to inspect each packet for the VLAN ID.

3. From the Trunk Port pulldown select Wan.

4. Enter a VLAN ID between 1 and 4094 in the Default VLAN ID field. Any untagged packet received on the Trunk Port, will be treated as belonging to this VLAN ID. This VLAN will be the one used to share information between the various VLANs.
5. Assign VLAN IDs to each of the active subnets you plan to use with VLAN tagging.

6. In the **Allowed VLANS** field enter the VLAN IDs that you wish to allow on the WS2000. The maximum allowed VLAN value is 4094. When entering multiple VLAN IDs, separate each ID with a comma. When entering a range of VLAN IDs, separate the starting and ending values with a "-".

### 10.3.1 Mapping WLANs to VLANS

Use the following steps to map a VLAN, that is not already a part of any subnet, to a WLAN:

1. Select the desired WLAN from the menu.
2. From the Subnet pulldown menu select **none**. The WLAN is now not associated with any subnet and the VLAN field can now be edited.
3. Enter a VLAN ID in the **VLAN** field to map that VLAN ID to the current WLAN.
4. Click the **Apply** button to save the changes.
WAN Statistics

The WS 2000 Network Management System provides a set of screens that allow the administrator to view real-time statistics for monitoring the switch’s activity. One of those screens displays statistics for the Wide Area Network (WAN) port. Selecting Status & Statistics --> WAN Stats displays the following screen.

The Information portion of the WAN Stats screen displays general information about the WAN. Much of this information is generated from settings on the WAN screen in the Network Configuration area.

- The Status field displays “Enabled” if the WAN interface is currently enabled on the WAN screen (Network Configuration --> WAN). If the WAN interface is disabled on the WAN screen, the WAN Stats screen does not display connection information and statistics.
- The HW address is the Media Access Control (MAC) address of the switch’s WAN port, which is set at the factory.
- The Mask field displays the subnet mask number for the switch’s WAN connection. This number is set on the WAN screen.
- The Link field displays “Up” if the WAN connection is active, and “Down” if the WAN connection is interrupted or lost.
- The WAN connection speed is displayed in Megabits per second (Mbps), for example, 100 Mbps.
- The IP addresses displayed here for the WAN connection are set on the WAN screen (Network Configuration --> WAN).

The Received and Transmitted portions of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted through the WAN interface, since the WAN was last enabled or the switch was last rebooted.

<table>
<thead>
<tr>
<th>Received Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Packets</td>
<td>The total number of data packets received over the WAN connection</td>
</tr>
<tr>
<td>RX Bytes</td>
<td>The total number of bytes of information received over the WAN connection</td>
</tr>
</tbody>
</table>
### Received Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Errors</td>
<td>The total number of errors including dropped data packets, buffer overruns, and frame errors on inbound traffic</td>
</tr>
<tr>
<td>RX Dropped</td>
<td>The number of data packets that failed to reach the WAN interface</td>
</tr>
<tr>
<td>RX Overruns</td>
<td>The total number of buffer overruns (when packets are received faster than the WAN interface can handle them)</td>
</tr>
<tr>
<td>RX Frame</td>
<td>The total number of TCP/IP data frame errors received</td>
</tr>
</tbody>
</table>

### Transmitted Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Packets</td>
<td>The total number of data packets sent over the WAN connection</td>
</tr>
<tr>
<td>TX Bytes</td>
<td>The total number of bytes of information sent over the WAN connection</td>
</tr>
<tr>
<td>TX Errors</td>
<td>The total number of errors including dropped data packets, buffer overruns, and carrier errors that fail on outbound traffic</td>
</tr>
<tr>
<td>TX Dropped</td>
<td>The number of data packets that fail to get sent from the WAN interface</td>
</tr>
<tr>
<td>TX Overruns</td>
<td>The total number of buffer overruns (when packets are sent faster than the WAN interface can handle them)</td>
</tr>
<tr>
<td>TX Carrier</td>
<td>The total number of TCP/IP data carrier errors received</td>
</tr>
</tbody>
</table>

### Subnet Statistics

The WS 2000 Network Management System provides a set of screens that allow the administrator to view real-time statistics for monitoring the switch's activity. One of those screens displays statistics for each of the subnets. Selecting **Status & Statistics --> Subnet Stats --> <Subnet Name> Stats** from the left menu displays the following screen.
The **Information** portion of the Subnet Stats screen displays general information about the subnet.

- The HW address is the Media Access Control (MAC) address of the switch’s WAN port, which is set at the factory.
- The IP addresses displayed here for the subnet connection are set on the subnet screen *(Network Configuration --> WLAN --> <subnet name>)*.

The Received and Transmitted portions of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted through the WAN interface since the WAN was last enabled or the switch was last rebooted.

<table>
<thead>
<tr>
<th>Received Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Packets</td>
<td>The total number of data packets received over the subnet</td>
</tr>
<tr>
<td>RX Bytes</td>
<td>The total number of bytes of information received over the subnet</td>
</tr>
<tr>
<td>RX Errors</td>
<td>The total number of errors including dropped data packets, buffer overruns, and frame errors on inbound traffic</td>
</tr>
<tr>
<td>RX Dropped</td>
<td>The number of data packets that failed to reach the subnet</td>
</tr>
<tr>
<td>RX Overruns</td>
<td>The total number of buffer overruns (when packets are received faster than the subnet can handle them)</td>
</tr>
<tr>
<td>RX Frame</td>
<td>The total number of TCP/IP data frame errors received</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transmitted Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Packets</td>
<td>The total number of data packets sent over the subnet</td>
</tr>
<tr>
<td>TX Bytes</td>
<td>The total number of bytes of information sent over the subnet</td>
</tr>
</tbody>
</table>
The interfaces section of the screen displays information about the ports and Access Ports associated with the subnet (set in Network Configuration --> Subnet --> <Subnet Name>).

The area shows the status of the port-subnet link and the speed of the connection. The Link field displays “Up” if the adjacent port is active, and “Down” if the adjacent port is inactive. When a port’s link status is “Up” the speed of the link (in Mbps) will be listed in the Speed field.

The area also shows the status of the port-WLAN associations. In this case, the adopted Access Ports for each of the associated WLANs are listed.

<table>
<thead>
<tr>
<th>Transmitted Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Errors</td>
<td>The total number of errors including dropped data packets, buffer overruns, and carrier errors that fail on outbound traffic</td>
</tr>
<tr>
<td>TX Dropped</td>
<td>The number of data packets that fail to get sent from the subnet</td>
</tr>
<tr>
<td>TX Overruns</td>
<td>The total number of buffer overruns (when packets are sent faster than the subnet can handle them)</td>
</tr>
<tr>
<td>TX Carrier</td>
<td>The total number of TCP/IP data carrier errors received</td>
</tr>
</tbody>
</table>
Wireless LAN Statistics

The WS 2000 Network Management System provides screens that display information about all of the switch’s wireless operations as well as information for each enabled wireless LAN (WLAN). Both screens are described in this section.

Displaying WLAN Summary Information

To see a summary information about wireless operations, select Status & Statistics --> Wireless Stats from the left menu.

The WLAN Summary section of the screen shows basic statistics about the currently enabled WLANs.

- **Name**: The WLAN name.
- **Subnet**: Displays the name of the subnet that is associated with the WLANs.
- **MUs**: Displays the number of mobile units associated with this WLAN.
- **T-put**: Displays the total throughput in Megabits per second (Mbps) for each of the active WLANs.
- **ABS**: Displays the Average Bit Speed (ABS) in Megabits per second (Mbps) for each of the active WLANs.
- **%NU**: Displays the percentage of the total packets for each active WLAN that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
- **Retries**: Displays the average number of retries per packet. A high number in this field could indicate possible network or hardware problems.
In the lower section of the screen, the **Total Switch RF Traffic** table gives summary information about RF traffic.

- **Total pkts per second**: Displays the average number of RF packets sent per second across all active WLANs on the wireless switch. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

- **Total bits per second**: Displays the average bits sent per second across all active WLANs on the wireless switch. The number in black displays this statistic for the last 30 seconds and the number in blue displays this statistic for the last hour.

- **Total associated MUs**: Displays current total number of Mobile Units associated with all the active WLANs on the wireless switch.

To clear the RF statistics, click the **Clear all RF Stats** button.

**Getting Statistics for a Particular WLAN**

To see a summary information about wireless operations, select **Status & Statistics --> Wireless Stats --> <WLAN name> Stats** from the navigation menu. A screen like the one shown for EngWLAN (below) will appear.

There are four areas on the screen. The Information area shows general information about the Access Port. The Received and Transmitted areas of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted through the Access Port. The Associated Mobile Units section lists the MUs and provides information on specific MUs that are currently transmitting through the Access Port.
**General WLAN Information**

**Information Section**

- **ESSID**: Displays the Extended Service Set Identification name that users will see when accessing the WLAN.
- **Subnet**: Displays the name of the subnet to which this WLAN is associated.
- **Num. Associated MUs**: Lists the number of mobile units (MUs) currently associated with the Access Port.
- **Authentication Type**: Displays the type of authentication used with this WLAN.
- **Encryption Type**: Displays type of encryption used with this WLAN.
- **Adopted APs**: Lists the Access Ports that have been adopted by this WLAN.

**Traffic Area**

- **Packets per second**: The Total column displays the average total packets per second that cross the selected WLAN. The Rx column displays the average total packets per second received on the selected WLAN. The Tx column displays the average total packets per second sent on the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

- **Throughput**: The Total column displays the average throughput in Mbps for a given time period on the selected WLAN. The Rx column displays the average throughput in Mbps for packets received on the selected WLAN. The Tx column displays the average throughput for packets sent on the WLAN WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

- **Avg. Bit Speed**: The Total column displays the average bit speed in Mbps for a given time period on the selected WLAN. This includes all packets that are sent and received. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

- **% Non-unicast pkts**: Displays the percentage of the total packets for the selected WLAN that are non-unicast packets. Non-unicast packets include broadcast and multicast packets. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

**RF Status**

- **Avg MU Signal**: Displays the average RF signal strength in dBm for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

- **Avg MU Noise**: Displays the average RF noise for all MUs associated with the selected WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

- **Avg MU SNR**: Displays the average Signal to Noise Ratio (SNR) for all MUs associated with the selected WLAN. The Signal to Noise Ratio is an indication of overall RF performance on your wireless networks.
Access Port Statistics

The WS 2000 Network Management System provides two screens, one that displays summary information for all associated access ports, and one that displays real-time statistics about the activity for each Access Port and its associated units.

Access Port Statistics Summary Screen

To see Access Port Summary information for the entire switch, select Status & Statistics --> Access Port Stats from the left menu.
Each Access Port associated with the switch is listed in the AP Summary area. For each AP, the following information is provided.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Displays the IP address of the Access Port.</td>
</tr>
<tr>
<td>WLAN</td>
<td>Displays the WLAN with which the Access Port is associated.</td>
</tr>
<tr>
<td>AP</td>
<td>Displays the name of the Access Port with which the Access Port is associated.</td>
</tr>
<tr>
<td>T-Put</td>
<td>Displays the total throughput in Megabits per second (Mbps) for the Access Port.</td>
</tr>
<tr>
<td>ABS</td>
<td>Displays the Average Bit Speed (ABS) in Megabits per second (Mbps) for the Access Port.</td>
</tr>
<tr>
<td>%NU</td>
<td>Displays the percentage of the total packets for the Access Port that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.</td>
</tr>
<tr>
<td>Retries</td>
<td>Displays the average number of retries per packet. A high number in this field could indicate possible network or hardware problems.</td>
</tr>
</tbody>
</table>

**Detailed Information About a Particular Access Port**

To see statistics about a particular Access Port, select `Status & Statistics --> Access Port Stats --> <Access Port Name>` from the left menu.

There are four areas on the screen. The Information area shows general information about the Access Port. The Received and Transmitted areas of the screen display statistics for the cumulative packets, bytes, and errors received and transmitted through the Access Port. The Associated Mobile Units section lists the MUs and provides information on specific MUs that are currently transmitting through the Access Port.
General Access Port Information

Information Section

**HW Address**
The Media Access Control (MAC) address of the Access Port. This value is typically set at the factory and can be found on the bottom of the Access Port.

**Placement**
Lists whether the Access Port is placed indoors or outdoors. This is determined by the placement setting in the Access Port configuration screen in the Network Configuration section.

**Current Channel**
This field indicates the channel for communications between the Access Port and mobile units. To specify the value, go to the corresponding Access Port screen.

**Adopted by**
The WLANs that currently adopt this Access Port (see Network Configuration -- Wireless for the Access Port Adoption List).

**Location**
The site location of the Access Port (an optional field that the administrator fills in on the Wireless --> Access Ports --> <Access Port Name> screen).

**Radio Type**
Displays the radio type of the selected Access Port. Radio types can be 802.11a, 802.11b, or 802.11b/g.

**Power**
The power level in milliwatts (mW) for RF signal strength is specified on the corresponding Access Port screen.

**Num. Associated MUs**
Lists the number of mobile units (MUs) currently associated with the Access Port.

**Active SIP Session Count**
Lists the number of currently active SIP Sessions on the selected Access Port. SIP is the Session Initiation Protocol which controls sessions for multimedia and voice conferences.

**Roamed SIP Sessions count**
Lists the number of SIP Sessions on the selected Access Port that have roamed to other Access Ports. SIP is the Session Initiation Protocol which controls sessions for multimedia and voice conferences.

Traffic Area

**Packets per second**
The Total column displays the average total packets per second that cross the selected Access Port. The Rx column displays the average total packets per second received on the selected Access Port. The Tx column displays the average total packets per second sent on the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

**Throughput**
The Total column displays the average throughput in Mbps for a given time period on the selected Access Port. The Rx column displays the average throughput in Mbps for packets received on the selected Access Port. The Tx column displays the average throughput for packets sent on the Access Port WLAN. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

**Avg. Bit Speed**
The Total column displays the average bit speed in Mbps for a given time period on the selected Access Port. This includes all packets that are sent and received. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.
### Approx RF Utilization
The approximate utilization of the Access Port’s RF port. This is calculated as Throughput divided by Average bit speed. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

### % Non-unicast pkts
Displays the percentage of the total packets for the selected Access Port that are non-unicast packets. Non-unicast packets include broadcast and multicast packets. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.

### RF Status

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avg MU Signal</strong></td>
<td>Displays the average RF signal strength in dBm for all MUs associated with the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.</td>
</tr>
<tr>
<td><strong>Avg MU Noise</strong></td>
<td>Displays the average RF noise for all MUs associated with the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.</td>
</tr>
<tr>
<td><strong>Avg MU SNR</strong></td>
<td>Displays the average Signal to Noise Ratio (SNR) for all MUs associated with the selected Access Port. The Signal to Noise Ratio is an indication of overall RF performance on your wireless networks.</td>
</tr>
</tbody>
</table>

### Errors

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Avg Num of Retries</strong></td>
<td>Displays the average number of retries for all MUs associated with the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.</td>
</tr>
<tr>
<td><strong>% Gave Up Pkts</strong></td>
<td>Displays the percentage of packets which the switch gave up on for all MUs associated with the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.</td>
</tr>
<tr>
<td><strong>% of Undecryptable Pkts</strong></td>
<td>Displays the percentage of undecryptable packets for all MUs associated with the selected Access Port. The number in black represents this statistic for the last 30 seconds and the number in blue represents this statistic for the last hour.</td>
</tr>
</tbody>
</table>
Mobile Unit (MU) Statistics

Each Access Port can have up to 32 associated mobile units. These units are listed in the Mobile Unit Access Control List of the WLAN Security screen (Network Configuration --> Wireless --> <WLAN Name> --> <WLAN Name> Security).

To see a summary of the associated mobile units and general information about each unit, select Status & Statistics --> MU Stats. The MU Stats Summary screen appears.

Field | Description
--- | ---
IP | Displays the IP address of the mobile unit.
WLAN | Displays the WLAN with which the mobile unit is associated.
AP | Displays the name of the Access Port with which the mobile unit is associated.
T-Put | Displays the total throughput in Megabits per second (Mbps) for the mobile unit.
ABS | Displays the Average Bit Speed (ABS) in Megabits per second (Mbps) for the mobile unit.
%NU | Displays the percentage of the total packets for the mobile unit that are non-unicast packets. Non-unicast packets include broadcast and multicast packets.
Retries | Displays the average number of retries per packet. A high number in this field could indicate possible network or hardware problems.
Detail | Clicking MU Detail will launch a new window with detailed statistics about the selected mobile unit. The MU Details screen is separated into four sections, MU Properties, MU Traffic, MU Signal, and MU Errors. The MU Properties section displays basic information such as hardware address, IP address, and associated WLAN and AP. The MU Traffic section displays statistics on RF traffic and throughput. The RF Status section displays information on RF signal averages from the MU. The Error section displays RF traffic errors based on retries, dropped packets and undecryptable packets.
View Statistics in Graphic Form

In the screens described by the previous sections of this chapter, the statistics for the WAN, LAN, WLAN, Access Ports, and mobile units are presented in a tabular format. However, administrators often want to see the trends of the activity on the LAN. To aid with that project, the WS 2000 Wireless Switch enables the administrator to view the statistics in a graphical format that is constantly updated.


To create a graph that will remain on your screen until you close it, follow these steps:

1. Select the type of Entity (WAN, SUBNET, WLAN, AP, or MU) that you want to display from the menu.
2. Select the particular member that you want to watch from the Member menu.
3. Select the data to monitor. Depending on the selected entity type, one or more of four radio buttons will become available to choose from. The radio button selection indicates what is being monitored (graphed on the X axis). Selections can be one of:

   **Pkts** If selected, the switch will monitor and graph packet traffic statistics. Select one or more of the eight values to monitor, including: packets received and transmitted, received and transmitted packets that were dropped, reception and transmission errors, and transmission and reception overruns.

   **RF** If selected, the switch will monitor radio frequency statistics. Select one or more of the different RF values to monitor, including: signal, noise, and signal-to-noise ratio (SNR).
Throughput
If selected, the switch will monitor the switches throughput. Select one or more of the different throughput values to monitor: total throughput, transmission received, transmitted throughput or the average bit speed.

PPS
If selected, information about packets per second will be graphed for the selected member. Select one or more of the three values to monitor: total packets per second, received packets, and transmitted packets.

4. Click the MONITOR button to open the graphics window. A window like the following will appear.

![WAN Statistics Graph]

5. Repeat Steps 1 through 4 to display as many statistics windows as you like.

A graphical statistics display window will stay available until you manually close it or Logout of the application.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail Use Case</td>
<td>12-3</td>
</tr>
<tr>
<td>A Retail Example</td>
<td>12-3</td>
</tr>
<tr>
<td>The Plan</td>
<td>12-3</td>
</tr>
<tr>
<td>Contacting the Wireless Switch</td>
<td>12-4</td>
</tr>
<tr>
<td>Entering the Basic System Settings</td>
<td>12-5</td>
</tr>
<tr>
<td>Setting Access Control</td>
<td>12-6</td>
</tr>
<tr>
<td>The IP Address Plan</td>
<td>12-7</td>
</tr>
<tr>
<td>Configuring POS Subnet</td>
<td>12-8</td>
</tr>
<tr>
<td>Configuring the Printer Subnet</td>
<td>12-9</td>
</tr>
<tr>
<td>Configuring the Cafe Subnet</td>
<td>12-11</td>
</tr>
<tr>
<td>Configuring the WAN Interface</td>
<td>12-13</td>
</tr>
<tr>
<td>Configuring Network Address Translation (NAT)</td>
<td>12-14</td>
</tr>
<tr>
<td>Inspecting the Firewall</td>
<td>12-16</td>
</tr>
<tr>
<td>Configuring the Access Ports</td>
<td>12-16</td>
</tr>
<tr>
<td>Setting Access Port Defaults</td>
<td>12-17</td>
</tr>
<tr>
<td>Naming the POS Access Port</td>
<td>12-18</td>
</tr>
<tr>
<td>Configuring the Printer Access Port</td>
<td>12-19</td>
</tr>
<tr>
<td>Configuring the Cafe Access Port</td>
<td>12-20</td>
</tr>
<tr>
<td>Associating the Access Ports to the WLANs</td>
<td>12-21</td>
</tr>
<tr>
<td>Configuring the Cafe WLAN</td>
<td>12-22</td>
</tr>
<tr>
<td>Configuring the Printer WLAN</td>
<td>12-24</td>
</tr>
<tr>
<td>Configuring the POS WLAN</td>
<td>12-26</td>
</tr>
<tr>
<td>Configuring Subnet Access</td>
<td>12-29</td>
</tr>
<tr>
<td>Configuring the Clients</td>
<td>12-31</td>
</tr>
<tr>
<td>Testing Connections</td>
<td>12-32</td>
</tr>
</tbody>
</table>
Retail Use Case

A Retail Example

Background

CCC clothing stores have, in the past, used POS terminals with a 10BaseT Ethernet connection to an in-house server. Management has decided to install wireless networking in the stores. Wireless point of sale (POS) terminals and printers will allow them to be more flexible with store layout. Wireless handheld terminals for inventory and price lookup will make inventory faster and more accurate. In some stores, management is adding a café with free wireless Internet access. The hope is that customers will visit more often and stay longer if their partners can use the Internet while they shop.

The following links show the tasks that the system administrator will carry out to complete the wireless upgrade.

The Plan

Clarisa is the employee assigned to implement the new network in San Jose. She needs three very different security policies. Wireless security policies are part of a WLAN configuration, so she will need three different WLANs.

- WLAN #1: Confidential information, such as credit card numbers and customer purchases, will travel over the links to wireless POS terminals. For these, she wants the strongest security measures possible. The two components of a wireless security policy are user authentication and data encryption. The corporation has a RADIUS server for user authentication and it is a logical choice for this application. If the corporation did not have a RADIUS server, an alternative would have been to install Kerberos on the in-store server and use Kerberos user authentication. As for data encryption, WEP is not secure enough for this traffic. A survey of the wireless POS terminals reveals that they all support WPA-TKIP, so Clarisa will use WPA-TKIP for data encryption.

- WLAN #2: The wireless printers are difficult to misuse - no keyboards - and the data stream to them does not include any information that needs strong encryption. On this WLAN, Clarisa can limit user access by limiting connections to just those devices which have their MAC addresses entered in the switch. The data will be WEP encrypted.

- WLAN #3: In the café, Clarisa wants an open network - no authentication or encryption. She believes that otherwise the support problems will be too difficult. But management wants to be absolutely certain that users of the café net cannot get access to the store computers or POS terminals. The WS 2000 allows the administrator to restrict access from one subnet to another, so Clarisa will create a subnet that is just for WLAN #3, and then restrict access from that subnet to the other subnets.
This plan covers all of the wireless devices—the POS terminals, the printers, and the customer laptops—except the wireless handheld terminals. Clarisa decides to put them on the WLAN with the POS terminals.

There are also some conventional, 100baseT wired devices to consider. There is the store server and two wired POS terminals. Clarisa will put all of these on the 100baseT ports on the WS 2000.

To keep things simple, Clarisa decides to define one subnet for each WLAN and assign one Access Port to each WLAN. The wired devices will be part of the POS subnet.

The WS 2000 will connect to the Internet through a DSL line.

**Contacting the Wireless Switch**

Clarisa sets up a direct network link between her laptop and the switch, plugging the cable into one of the local, non-WAN, ports. The switch defaults to having all the LAN ports on the first subnet and that subnet having an IP address of 192.168.0.1. So, as far as this connection is concerned, the switch comes up with an initial IP address of 192.168.0.1. She sets her laptop
to have an IP address of 192.168.0.2 and a netmask of 255.255.255.0. She also sets the gateway IP address to be 192.168.0.1, the WS 2000's IP address.

Clarisa starts her web browser and enters "http://192.168.0.1/" as the URL. The WS 2000 sends a login page to her browser. She logs in using "admin" for the username and "symbol" as the password. The system immediately asks her to change the password to something else. Clarisa does so.

### Entering the Basic System Settings

Clarisa selects System Settings from the left menu, located under the System Configuration heading.

Upon selecting this screen for the first time, the WS 2000 switch immediately asks her to choose a country. Different countries have different regulations for the use of these radio frequencies. Setting the location configures the switch to use only the channels, frequencies, and power levels that are legal for that country. She sets the country to United States - US.

The system name is used to distinguish between WS 2000 switches for remote configuration. She gives the switch a descriptive name, "SanJose-1". This name will appear in the footer for subsequent configuration windows for the switch. She does not need the name now, while she is in San Jose. But later, when she returns to corporate headquarters and wants to log into several switches remotely, it will help her to know which switch she is working on. She also enters a slightly longer description on the System Location field.

She enters her email address into the Admin Email Address box. CCC uses an SNMP manager that has the capability of monitoring network devices and sending email to the manager of a device that is in an unusual state. This is the email address that will be supplied to that SNMP manager for this switch.
Clarisa clicks the **Apply** button to save her changes.

### Setting Access Control

In the WS 2000 Access screen, Clarisa controls which network interfaces can be used to reconfigure the WS 2000 switch. She is currently using HTTP access on port 80 over the LAN, so she leaves that on. She may also want to make changes using the Command Line Interface (CLI), so she leaves on local CLI access. She wants to be able to manage the switch from corporate headquarters, but she does not want to leave the standard HTTP port, port 80, open over the WAN. She elects to leave port 443 open over the WAN instead. She knows she will want to monitor the switch from her SNMP system at corporate, so she leaves **SNMP WAN access** on.

AirBEAM is a Symbol Technology software system designed to simplify maintenance of wireless devices. CCC clothing recently purchased an AirBEAM license as part of a major commitment to Symbol Technology wireless bar code scanners for inventory. Clarisa would like to integrate the WS 2000 into the AirBEAM management system and she leaves AirBEAM access on.
Clarisa clicks the **Apply** button to save her changes.

Clarisa leaves the rest of the System Configuration screens for now, moves to the left menu, and clicks on **Network Configuration** so that she can begin to define the subnets.

**The IP Address Plan**

Subnets can be renamed, assigned an IP address, and have ports associated with them. Clarisa needs to plan how she is going to assign IP addresses to the subnets and the devices on them.

Clarisa only has one IP address from corporate for this store. She will use network address translation (NAT) for all of the devices, making request from those devices look to the outside world as if they came from the single static IP address that she has. For the devices, she plans to use IP numbers from the range 192.168.*.*, because IP addresses in that range are designated for internal use only.

She will assign them as follows:

<table>
<thead>
<tr>
<th>Subnet</th>
<th>IP Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.***</td>
<td>POS subnet</td>
</tr>
<tr>
<td>192.168.1.***</td>
<td>Printer subnet</td>
</tr>
<tr>
<td>192.168.2.***</td>
<td>Cafe subnet</td>
</tr>
</tbody>
</table>
And for each subnet:

- **192.168.**.1  The WS 2000 address on that subnet
- **192.168.**.2 to **192.168.**.10  Devices with static IP addresses
- **192.168.**.11 to **192.168.**.254  Devices with DHCP-supplied IP addresses

With this plan, she can begin to configure the individual subnets.

**Configuring POS Subnet**

Clarisa selects the first subnet from the LAN menu items in the left menu.

Clarisa renames this subnet “**POSsn**”, then gives the switch an IP address of 192.168.0.1 on that subnet and assigns a subnet mask of 255.255.255.0. The devices on this subnet are:

- Everything on the POS WLAN: wireless POS terminals and wireless handheld terminals
- One wired POS terminal on port 4 and one on port 5
- One in-store server on port 6

Using the Interfaces section of the screen on the right, she associates the first WLAN with this subnet, as well as Ports 1 (the one the POS WLAN is plugged into), 4 and 5 (the wired POS terminals), and 6 (the server). She activates the DHCP server and gives it an IP address range of 192.168.0.11 to 192.168.0.254.

After the Address Assignment Range is entered, Clarisa clicks **Advanced DHCP Server**.
The Default Gateway is already set to the subnet address. This is the IP address to which the DHCP clients on this subnet will forward their outbound traffic. Clarisa fills in the DNS Server addresses, which Corporate has specified. This will also be supplied to the DHCP clients. The DHCP Lease Time is the time an IP address will remain assigned to a client after there is no more activity. She leaves it at the default and clicks Ok to save her changes.

Then, in the subnet screen, she clicks Apply to save her overall changes.

Now she will configure the printer subnet.

**Configuring the Printer Subnet**

Clarisa selects the second subnet from the list of LAN menu items in the left menu.

She renames this subnet “Printsn”, then gives it an IP address of 192.168.1.1 and a subnet mask of 255.255.255.0. The only devices on this subnet are the wireless printers. Using the Interfaces section of the screen, she associates the second WLAN with this subnet. She activates the DHCP server with an IP address range of 192.168.1.11 to 192.168.1.254.
After the Address Assignment Range is entered, Clarisa clicks **Advanced DHCP Server**.
Clarisa enters the DNS server IP addresses and leaves the Default Gateway and DHCP Lease Time at their defaults. She clicks Ok in the Advanced DHCP Server window and then Apply in the Subnet window to save her changes.

Now Clarisa will configure the Cafe subnet.

**Configuring the Cafe Subnet**

Clarisa selects the third subnet in the LAN menu list under Network Configuration in the left menu.

She then renames this subnet “Cafesn” and gives it the IP address 192.168.2.1 and a subnet mask of 255.255.255.0. The only devices on this subnet are the customer’s laptops in the cafe.

Using the Interfaces section of the screen, she associates the third WLAN with this subnet, and activates the DHCP server with an IP address range of 192.168.2.11 to 192.168.2.254.
Clarisa clicks **Advanced DHCP Server** and enters the **DNS server IP addresses**. The **Default Gateway** is fine. However, Clarisa expects the cafe patrons to come and go frequently, so she reduces the **IP address lease time** to 1800 seconds. This means that a DHCP client mobile unit will give up its IP address if it is inactive on the network for more than half an hour. This seems about right for the usage patterns that she expects for the cafe. If she gets complaints, she will bump it to an hour.
Clarisa clicks the Ok button in the Advanced DHCP Server window, then on the Apply button in the subnet screen to save her choices. The subnets are now configured.

Next Clarisa configures the WAN interface.

**Configuring the WAN Interface**

Now Clarisa selects the WAN node in the left menu. Here she enters the static IP address assigned to this store by CCC corporate. She also enters the other information supplied to her by corporate: the gateway IP address, the subnet mask, and the DNS server IP addresses. She is connecting by a DSL modem, but because she has a static IP address, her Internet service provider (ISP) does not require PPP-over-Ethernet connection information. If her ISP required PPPoE account information, she would have entered that information in the PPP-over-Ethernet section of the screen.
If corporate had not paid their ISP for a static IP address for each store, she would have selected the **This interface is a DHCP Client** option and the WAN configuration information would have been assigned by the ISP each time they connected to the Internet.

Clarisa clicks the **Apply** button to save her changes.

### Configuring Network Address Translation (NAT)

Clarisa has only one public IP address for the whole store. She will use network address translation to make all requests from internal IP addresses to appear as if they came from the single public IP address.

She selects the **NAT** node under the WAN item in the left menu. The screen shows all IP addresses assigned to the switch in the WAN interface configuration step. In this case, there is one IP address shown. She selects **"1 to Many"** from the NAT Type menu to the right of the IP address.
After she makes this selection a new button appears, labelled "1 to Many Mappings". She selects the "1 to Many Mappings" button.

If Clarisa had more than one static IP address, she would have been able to assign several to the WAN interface. This screen would be used to choose how the internal IP addresses on each subnet translated into the selection of external IP addresses. However, she has only one external IP address. All requests from any IP address on the store network will be translated into a request using the single public IP address for the store.

Clarisa clicks the Ok button to confirm the mappings and then clicks the Apply button in the main screen to confirm the NAT choices and save her choices on the switch.
Inspecting the Firewall

Clarisa selects the **Firewall** item in the left menu. Each of the checkbox items represents a type of attack which the WS 2000 can filter out. She checks to see that all of the options are enabled.

[Image of the WS 2000 Wireless Switch Software interface showing the Firewall settings]

Clarisa clicks the **Apply** button to confirm that all attacks listed will be filtered.

Configuring the Access Ports

So far, Clarisa has been operating with the WS 2000 connected only to her laptop. To configure the Access Ports, she will need to connect them to the switch. She plans to use switch ports as follows:

<table>
<thead>
<tr>
<th>Switch Port</th>
<th>Connected to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 1</td>
<td>Access port for the POS WLAN</td>
</tr>
<tr>
<td>Port 2</td>
<td>Access port for the Printer WLAN</td>
</tr>
<tr>
<td>Port 3</td>
<td>Access port for the Cafe WLAN</td>
</tr>
<tr>
<td>Port 4</td>
<td>Wired POS terminal #1</td>
</tr>
<tr>
<td>Port 5</td>
<td>Wired POS terminal #1</td>
</tr>
<tr>
<td>Port 6</td>
<td>In-store server</td>
</tr>
</tbody>
</table>
Setting Access Port Defaults

The WS 2000 allows the user to specify the default settings for Access Ports. Clarisa expands the Access Ports node in the left menu and selects the 802.11b Defaults node. Clarisa has only 802.11b Access Ports.

All of the Access Ports will be indoors, so she specifies Placement as Indoors. She sets the Channel to one, though she will reset each Access Port to a different 802.11b channel later. She sets the Power Level to 20dB, the maximum level allowed in the US.

She does not change the supported rates—using the Set Rates button—but leaves them as they are. The switch will operate at the maximum rate allowed by radio conditions, scaling back as needed.

She also does not change the Antenna Diversity setting, Short Preamble setting, RTS Threshold, or the Beacon Settings. These parameters control some of the broadcast mechanics of an 802.11 conversation between mobile units and Access Ports. In most cases, there is no reason to change them.

Clarisa clicks Apply to save her changes.

After setting the default settings for 802.11a and 802.11b Access Ports, Clarisa removes the Access Ports from their packaging and labels each with the name of the WLAN which it will support. She connects the Access Ports to the switch, using the ports selected in her plan.
**Naming the POS Access Port**

Having specified the general Access Port defaults, Clarisa goes on to name and configure the Access Port for the POS WLAN. She selects the first Access Port in the left menu.

In the Properties section, Clarisa enters a new name for the Access Port and a brief description of its permanent location.

In the Radio Settings section, Clarisa sets the **Channel** to 3. She knows that the store uses cordless phones that transmit on channel 1. She also wants to maintain some separation between the channel used by this Access Port and the other Access Ports at this location.

She doesn’t change any of the other settings. She clicks the **Apply** button to save her changes.
Configuring the Printer Access Port

Clarisa configures the Printer Access Port in a similar way. She give it the name "Printer AP" and a location description. She assigns channel 6 to this Access Port, avoiding contention with the POS AP and the Cafe AP.

She clicks the Apply button to save her changes.
Configuring the Cafe Access Port

Finally, she names the third Access Port “Cafe AP” and gives it a channel of 9. In this case she makes sure Support Short Preamble is not selected. There are two preambles in use in the wireless world, an older, longer one and a newer, shorter one. Most wireless devices support both and use the shorter one by default. However, in the cafe, there will be older wireless devices coming in and rather than confuse them, she will stick with the longer preamble on this WLAN.

Again, she clicks the Apply button to save her changes.
**Associating the Access Ports to the WLANs**

Now Clarisa selects the **Wireless** item in the left menu. This screen indicates which Access Ports are associated with which WLANs.

First Clarisa looks in the Summary section of the screen to determine that all three WLANs are enabled.

In the Access Port Adoption List section, the screen begins with a single line with “ANY” as the Start MAC address, “ANY” as the End MAC address, and checks under all three of the WLANs. Clarisa removes the checks from the WLAN checkboxes.

Clarisa clicks the **Add** button and then enters the MAC address for the POS Access Port as the Start MAC address. She then selects the checkbox for **WLAN1**, the WLAN which supports the POS terminals. Similarly, Clarisa clicks the **Add** button and enters the MAC address for the Printer WLAN and puts it on WLAN2. Finally, she clicks the **Add** button a third time, enters the Start MAC address for the Access Port assigned to the Cafe WLAN and selects the checkbox for the **WLAN3**.

[Image of the wireless switch interface]

Clarisa clicks the **Apply** button to save her choices.
Configuring the Cafe WLAN

Clarisa clicks the button to the left of the Wireless menu item in the left menu. It opens up to show the individual WLANs. She selects the third WLAN. This is the WLAN which she plans to use for the cafe WLAN.

The WLAN name is used with in the WS 2000 configuration screens to make the interface easier to navigate. She names this WLAN from “WLAN3” to “Cafe”. She also gives it an ESSID of “CCC-Cafe”. The ESSID is broadcast to the users and will be what the cafe users see when they select a wireless network on their laptops. Finally, she uses the Subnet pull-down menu to make this WLAN part of the third subnet, the “Cafesn” subnet.

She leaves the Disallow MU to MU communications option unchecked. She is certain that some cafe users will want to communicate between themselves, so she does not choose the Disallow.

She turns on Answer Broadcast ESS for this WLAN. Some mobile units come with a default ESSID of “101”. This option allows the WLAN to respond to these mobile units even if the WLAN is set up with a different ESSID. Since the cafe is a public access WLAN, leaving this option on will make it easier for the cafe customer to associate with the WLAN. For the private WLANs on this switch, she will turn this option off.

She clicks the Apply button to save her choices.
Clarisa goes to the left menu and clicks the button to the left of the Cafe WLAN node. A menu item labeled “Cafe Security” is displayed and Clarisa selects it.

She confirms that the Cafe Security screen shows that no authentication and no encryption methods.

Clarisa clicks the Apply button to save her choices.
Configuring the Printer WLAN

For the printer WLAN, Clarisa makes the following selections:

Name: Printer
ESSID: CCC-Printer
Subnet: Prints
Disallow MU to MU Communication: Yes
Use Voice Prioritization: No
Answer Broadcast ESS: No

The wireless printers will never need to communicate with each other directly. MU-to-MU communications can be safely disallowed. Allowing "Answer Broadcast ESS" is a way to allow mobile units that are not configured with the network ESSID to associate with the WLAN. She knows that she will configure all of the mobile units on this WLAN with the correct ESSID, so she disallows this option, potentially keeping a cafe customer out of the printer WLAN.

Clarisa clicks the Apply button to confirm her choices.
Clarisa clicks the + to the left of the Printer WLAN menu item and selects the Printer Security item. In the screen that displays, Clarisa selects no authentication. She enters the MAC numbers of the wireless printers in the Mobile Access Control section. The MAC numbers are unique numbers assigned to every network-cable hardware device and are usually listed on the same label that shows the device’s model number and serial number. She enters each by clicking on the Add button and entering the MAC address in the Start MAC column of the new row.

She uses the Mobile Unit Access Control pull-down menu to select Deny. This specifies that the switch will deny access to any mobile unit that has a MAC address that is not listed.

In the Encryption Methods section, she selects WEP 128 (104-bit key). WEP encryption is weak compared with WPA-TKIP, but still requires a day or so of solid traffic samples and a fair amount of effort to break. There is no data transversing this link that a data thief couldn’t find in the trash. In any case, the store’s wireless printers only support WEP.

She clicks the WEP Key Settings button and enters the keys she will use:
She clicks the **Ok** button to confirm the WEP key selections, then the **Apply** button to confirm the screen selections.

### Configuring the POS WLAN

For the POS WLAN, she makes the following choices:

<table>
<thead>
<tr>
<th>Name</th>
<th>POS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESSID</td>
<td>CCC-POS</td>
</tr>
<tr>
<td>Subnet</td>
<td>POSsn</td>
</tr>
<tr>
<td>Disallow MU to MU Communication</td>
<td>No</td>
</tr>
<tr>
<td>Use Voice Prioritization</td>
<td>Yes</td>
</tr>
<tr>
<td>Answer Broadcast ESS</td>
<td>No</td>
</tr>
</tbody>
</table>

Allowing "**Answer Broadcast ESS**" is a way to allow mobile units which are not configured with the network ESSID to associate with the WLAN. She knows that she will configure all of the mobile units on this WLAN with the correct ESSID, so she disallows this option, potentially keeping a cafe customer out of the POS WLAN.

The options for **Multicast Addresses** are designed for compatibility with some VoIP phones. Clarisa doesn’t know if the voice handhelds will require it but, even if they do, she can’t know the required multicast addresses until they are purchased and arrive. She leaves the **Multicast Addresses** at the factory default.

![WS 2000 Wireless Switch Configuration](image)

Clarisa clicks the **Apply** button to save her choices.
Clarisa then clicks the “+” to the left of the POS WLAN in the left menu and selects **POS Security**.

In that screen, she selects **802.1x EAP** for authentication. This will allow her to use the corporate RADIUS server for user authentication. Under Encryption Methods, she selects **WPA-TKIP encryption**.

![WS 2000 Wireless Switch](image)

Then she selects the **“802.1x EAP Configuration”** key. In the next screen, she enters the corporate RADIUS server’s IP address, its port number, and the secret string needed to access it. In this case, her corporation is using a port number other than the standard one of 1812. She wants to allow the software to reauthenticate the users, but she is uncomfortable with the 3600 second (one hour) interval, and changes it to 10 minutes (600 seconds). She sees no reason to change the other 802.1x parameters.
She clicks the Ok button in the 802.1x-EAP configuration window. She then clicks the WPA-TKIP Settings button in the security screen.

TKIP encryption protocol calls for keys between two specific nodes to change with every packet. However, there is no standard with respect to how often one should change keys for broadcast packets. A very busy network with lots of broadcast packets could generate enough packets for successful decryption in about an hour. Clarisa sets the system to rotate the broadcast keys every five minutes.

TKIP requires an initial shared key to start, so that all messages can be encrypted, including the first one. This initial key setting would be entered in the lower half of this screen, if it were needed. However, if 802.1x EAP user authentication is enabled, the authentication server will provide the initial key to the client and the key settings will be grayed out. In this case, Clarisa is using 802.1x EAP user authentication, so she does not have it enter an initial shared key.
With this, Clarisa has finished configuring the basic WLAN configuration and the WLAN security. She clicks the **Ok** button in the WPA-TKIP window and then the **Apply** button in the WLAN security screen.

### Configuring Subnet Access

Clarisa wants the two internal subnets to have complete access to one another, but she wants the Cafe subnet to have access only to the WAN.

In the left menu, she opens the **Firewall** item under Network Configuration and selects the **Subnet Access** node.
To set the subnet access for a pair of subnets, she clicks the square for traffic from one subnet to another and then uses the detail section, which appears below, to determine the rules for traffic between those two subnets.

She allows the Cafe subnet to have full access to the WAN. For the Cafe subnet to or from any other internal subnet, she selects the appropriate square, then uses to the detail box below to “Deny” all protocols.

For the POS subnet and the Printer subnet, she selects “Allow” all protocols when going to the WAN, the POS subnet, and the Printer subnet.
After specifying all of the subnet access rules, she clicks the **Apply** button to save her changes.

### Configuring the Clients

Clarisa has now finished configuring the switch. Next she configures the wired clients.

Going to each device, she gives it the IP address and other networking information that it will need to communicate with the switch:

<table>
<thead>
<tr>
<th>Client</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Gateway</th>
<th>WS 2000 Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired POS terminal #1</td>
<td>192.168.0.4</td>
<td>255.255.255.0</td>
<td>192.168.0.1</td>
<td>4</td>
</tr>
<tr>
<td>Wired POS terminal #2</td>
<td>192.168.0.5</td>
<td>255.255.255.0</td>
<td>192.168.0.1</td>
<td>5</td>
</tr>
<tr>
<td>Server</td>
<td>192.168.0.6</td>
<td>255.255.255.0</td>
<td>192.168.0.1</td>
<td>6</td>
</tr>
</tbody>
</table>

Then she does the same thing with the wireless clients:

<table>
<thead>
<tr>
<th>Client type</th>
<th>WLAN ESSID</th>
<th>Wireless channel</th>
<th>Authentication</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless POS terminals</td>
<td>CCC-POS</td>
<td>3</td>
<td>802.1x EAP</td>
<td>WPA-TKIP</td>
</tr>
<tr>
<td>Handheld terminals</td>
<td>CCC-POS</td>
<td>3</td>
<td>802.1x EAP</td>
<td>WPA-TKIP</td>
</tr>
<tr>
<td>Wireless printers</td>
<td>CCC-Printers</td>
<td>7</td>
<td>None</td>
<td>WEP</td>
</tr>
</tbody>
</table>

The remaining tasks are to test the network and to put the Access Ports in their permanent locations.
Testing Connections

Clarisa powers up several sample devices and tests them, to be sure that they work as configured. She tests whether the devices can connect to the wireless switch and whether they can connect to devices on other subnets.

After she is confident that everything is working, she moves the Access Ports to their permanent locations. She connects the WS 2000 to the DSL modem. Finally, she tests the connection from each subnet to the WAN.

The store network is now complete.
Field Office Use Case

A Field Office Example

Background

Leo is the network administrator, system administrator, and IT professional for a field office with 60 employees. The users include sales people, sales engineers, office administration and customer support people. All of the sales personnel have laptops and many of them have personal digital assistants (PDAs).

The office is connected to the Internet and to corporate through a frame relay link. Between the office network and the frame relay, there is a router and a virtual private network (VPN) appliance. All traffic to corporate is encrypted by the VPN appliance. Traffic to other addresses passes straight through.

Leo installed a wireless access point about six months ago and quickly found that many employees preferred to use it. However, the throughput of the lone unit was not enough to service 40 or so users and coverage was weak in many areas of the building. In addition, Leo was doing user authentication by maintaining a list of permissible user MAC addresses on the access point. This required modifications to the list once or twice a week. Recently, when a laptop was stolen, Leo could not determine which MAC address to remove from the list for several hours. He concluded that a better method of user authentication was needed. Also, the data encryption on the old access point was WEP and WEP encryption can be broken with several hours of data encrypted with the same key. Leo changes the key every week, but some users complain when last week’s key does not work anymore.

Leo has decided to upgrade to a WS 2000 wireless switch. He will have four Access Ports, one in the administration office area, one in the sales office area, one in the sales engineering area, and one in the engineers’ demonstration room. Throughput and coverage will increase significantly. Leo will convert to 802.1x/EAP-TTLS user authentication through the corporate RADIUS server and convert to WPA2 encryption, improving security considerably and reducing maintenance significantly.

Leo’s company is also growing. Corporate has rented an expansion office for engineering in another part of the same building. Leo needs to establish secure communication with from the engineering subnet to this expansion office. The other office will also have a WS 2000, so Leo will establish a direct VPN link to that WS 2000 and use the VPN as the secure communication link.

The following links show the tasks that Leo will carry out to complete the wireless upgrade.

The Plan

Each WS 2000 WLAN has exactly one security policy, where a security policy is defined as a user authentication method and a data encryption method. Because each WLAN can have one and only one security policy, WLAN configuration is usually defined by the security needs of the installation. If two groups of users require different security policies, then they must associate to the WS 2000 through different WLANs. See the retail case study for an example of an installation where different security needs drive the need for separate WLANs.

In this situation, all of Leo’s users will use the same security system: 802.1x/EAP-TTLS user authentication and WPA data encryption. Leo can set up the WLANs in any way that is convenient.

Corporate has given Leo three static IP addresses for the wireless network. He will configure the WS 2000 as a DHCP server giving out internal-use-only IP addresses and use network address translation (NAT) in the switch to convert the outward-bound traffic to one of the static IP addresses.
To keep things simple, he will define one subnet for the administration users, one subnet for the sales and marketing users, and one subnet for the engineers. Each subnet will have one WLAN associated with it and one Access Port. The only exception is the engineering subnet, which will have one WLAN and two Access Ports. The marketing subnet will not have any access to the engineering or administration subnets. All of the subnets will be restricted to just HTTP, SMTP, and POP access to the WAN.

### Configuring the System Settings

**Contacting the Wireless Switch**

To begin configuration of the switch, Leo sets up a communication link to the switch. Leo starts with a direct network link between his laptop and the switch, plugging the cable into one of the local, non-WAN, ports. The switch defaults to having all the LAN ports on the first subnet and that subnet having an IP address of 192.168.0.1. So, as far as this connection is concerned, the switch comes up with an initial IP address of 192.168.0.1. He sets his laptop to have an IP address of
192.168.0.2 and a netmask of 255.255.255.0. He also sets the gateway IP address to be 192.168.0.1, the WS 2000's IP address.

Leo launches his web browser and enters "http://192.168.0.1/" as the URL. He logs in using admin for the username and symbol as the password.
As soon as he logs in, the WS 2000 asks him to set the password. He sets the administration password to something relatively secure.

He presses **Update Password Now** to record his selection.
**Entering the Basic System Settings**

The interface opens by displaying the System Setting screen. This screen is also accessible by clicking the toggle to the left of System Configuration in the left menu, then selecting **System Settings** in the left menu.

The first time System Settings are displayed, a dialog box is displayed, warning the administrator to select a country of operation.

Different countries have different regulations for the use of radio frequencies. Setting the location configures the switch to use only the channels, frequencies, and power levels that are legal for that country. Leo sets the location to United States - US.

The system name is used to distinguish between WS 2000 switches for remote configuration. Leo gives the switch a descriptive name, **Atlanta1**. This name will appear in the footer for subsequent configuration windows for the switch. He does not need the descriptive name, but he wants to put in something appropriate in case he needs it later. If the office eventually has more than one wireless switch, the name will help him to know which switch he is working on.

He also enters his email address into the **Admin Email Address** box. Leo's corporation uses an SNMP manager which has the capability of monitoring network devices and sending email to the manager of a device that is in an unusual state. This is the email address that will be supplied to that SNMP manager for this switch.
**Setting Access Control**

Leo then clicks the **WS 2000 Access** node in the left menu. This controls which subnet can be used to reconfigure the WS 2000 switch and how that reconfiguration can be accomplished. Leo will be inside the LAN, so he leaves on all means of reconfiguring from within the LAN. Corporate may want to have read access from outside the LAN, so Leo leaves on SNMP access from the WAN.

AirBEAM® is a Symbol Technology product for the management of software on wireless devices. Leo does not have a copy of AirBEAM yet, but he hopes to get one when the company purchases some Voice over IP (VoIP) phones. He also doesn’t expect to access the switch from the CompactFlash card slot. So, he turns **AirBEAM Access** off.

Leo clicks on the **Apply** button in the WS 2000 Access screen to save his changes.
Configuring the LAN

Leo clicks the toggle to the left of Network Configuration in the left menu. The tree expands and he selects the **LAN** item.

![LAN Configuration Screen]

This screen shows the subnets, their IP addresses, and the network interfaces (the 10/100BaseT ports and the WLANs) that are currently associated with each subnet. Only the first subnet is initially enabled, so Leo clicks on the check boxes to the left of **Subnet2** and **Subnet3** to enable them. He clicks the **Apply** button to record his changes.

Next Leo needs to configure each of the subnets. He clicks the toggle symbol to the left of **LAN** in the left menu to expand it.
Configuring the Engineering LAN

Leo selects Subnet1 from the choices under the LAN heading. He enters a new name for the subnet, Eng-SN, to make it easier to recognize this subnet throughout the WS 2000 interface.

He also selects the option This interface is a DHCP Server. Choosing this DHCP option means that the switch will pick IP addresses from the Address Assignment Range and assign them to network clients on this subnet, as needed.

This screen also sets the IP address for the switch’s interface to the subnet. Any address that starts with “192.168” is an internal-use-only IP address. That is, network administrators are free to use these IP addresses anyway they want, as long as the IP addresses are never visible to the outside world. The switch defaults to an address of 192.168.0.1 for the first subnet interface. Leo elects to use the range of IP addresses from 192.168.0.11 to 192.168.0.254 for the DHCP clients in this subnet.

Leo then selects the Advanced DHCP Server button. The DNS server IP addresses and the Gateway IP address entered here will be passed down the DHCP clients for this subnet for their own use while associated with this subnet. Leo enters the IP addresses that the corporation’s IT department has specified for the corporate primary and secondary DNS servers. For the gateway, Leo enters the IP address for the subnet, the same IP address that he entered for the IP Address in the IP Parameters section of the Subnet screen.

The DHCP Lease Time (sec) specifies how long in seconds a client may keep an IP address when that client is not active on the net. The lease time is currently set for 86,400 seconds, or 24 hours. Leo expects that people using these WLANs will connect for a work day or not. While in the office, he expects that their machines will initiate contact with the network every 10 or 15 minutes for email. When they unplug to go home, this lease time will hold their IP address for another full day and not return it to the usable pool until the end of the next day. Leo would prefer that the lease time expire sometime during the night. He figures a lease time of somewhere between 10,000 seconds and 30,000 seconds is appropriate for this application. Leo sets it to 10000 seconds and figures he will change it if anyone complains.
The **WINS Server** field is designed to supply the Windows Network Server IP address to any DHCP clients that request it. Leo supplies the IP number for the local WINS server.

The **Domain Name** field will be supplied to any DHCP clients that request it. Leo enters his company’s domain name.

![Advanced DHCP Server](image)

There is no reason to set up static DHCP mappings now. These would permanently lease an IP address to a client with a specific MAC address. Leo clicks the **Ok** button on the Advanced DHCP Server window, then the **Apply** button on the subnet window.
**Configuring the Sales Subnet**

The sales and marketing subnet is configured exactly the same way as the engineering subnet, though with a different name and a different IP address range.

Leo selects the Advanced DHCP Server button and follows the same procedures as he did for the engineering subnet. Leo clicks the **Ok** button on the Advanced DHCP Server window, then the **Apply** button on the subnet window.

The administration subnet is configured in the same way.
Again, Leo fills out the advanced DHCP screen as he did for the two previous subnets. Leo clicks the **Ok** button on the Advanced DHCP Server window, then the **Apply** button on the subnet window.

The next step is to configure the WAN interface.

**Configuring the WAN Interface**

Next Leo configures the WS 2000 WAN interface. This interface connects the WS 2000 switch to the VPN appliance and, through that appliance, to the Internet.

Leo enables the WAN interface, but leaves the DHCP Client option disabled. Instead of using DHCP to get address information for the switch, he enters the permanent information which he previously obtained from the corporate network administrator. He enters the IP address for the switch, the gateway address (in this case, the VPN appliance), and the IP addresses of the corporate primary and secondary DNS servers.

The corporation has a frame relay link between this office, the corporate network and the Internet. If the connection to the WAN had been through a DSL link, the account information would be entered in the PPP over Ethernet section on the bottom of this screen. Since it will not be needed, Leo makes sure that the **Enable** checkbox in the PPP Over Ethernet section is not checked.
Leo has three addresses for this switch. He plans to use one address for the traffic from each of the subnets. He clicks the **More IP Addresses** button and enters the other two IP addresses:

He clicks the **Ok** button in the address window, then the **Apply** button on the WAN window to save his changes.

The next step is to set up the network address translations (NAT).
Configuring the WAN Interface

Setting Up Network Address Translation

After entering the IP addresses for the WAN interface, Leo clicks the toggle to the left of the WAN item in the left menu to expand it. He then selects the NAT item. The WS 2000 displays the three IP addresses he entered when configuring the WAN.

Each of these IP addresses will serve as the alias for all of the traffic from its corresponding subnet. That is, each IP address will serve as the only alias for many internal-only IP addresses. Leo chooses 1 to Many in the pull-down menus to the right of each IP number. As he does so, a 1 to Many Mappings button appears to the right of the pull-down menus, in the Outbound Mappings column.
Leo clicks any of the **NAT Ranges** button to the right of the IP addresses. The 1 to Many Outbound Mappings window displays. Leo uses the pull-down menu to set the outbound IP address for each subnet. These are the same as the inbound IP addresses that he specified in the WAN configuration screen.

He clicks the **Ok** button to save his entries, then clicks the **Apply** button in the NAT screen.

The next step is to configure the firewall.
Confirm Firewall Configuration

After setting the NAT ranges, Leo selects Firewall under WAN in the left menu. The WS 2000 displays a series of Configurable Firewall Filters, all of which are currently enabled.

Leo examines the list and sees no reason to turn off any of the filters. He clicks the Apply button.

The next step is to determine which Access Ports each WLAN will use.

Adopting Access Ports

Now that the LAN and WAN interfaces are configured, Leo needs to specify which Access Ports will go with which wireless LANs (WLANs). To do this, Leo needs the MAC address for each Access Port. He removes them from their packaging and finds that they have consecutive MAC addresses: 00:A0:F8:BB:FC:94 through 00:A0:F8:BB:FC:97. He decides that he will install them as follows:

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Location</th>
<th>WLAN</th>
<th>Adoption List Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:A0:F8:BB:FC:94</td>
<td>Engineering offices</td>
<td>Engineering</td>
<td>WLAN1</td>
</tr>
<tr>
<td>00:A0:F8:BB:FC:95</td>
<td>Demonstration room, engineering area</td>
<td>Engineering</td>
<td>WLAN1</td>
</tr>
<tr>
<td>00:A0:F8:BB:FC:96</td>
<td>Sales and marketing area</td>
<td>Marketing</td>
<td>WLAN2</td>
</tr>
<tr>
<td>00:A0:F8:BB:FC:97</td>
<td>Administration area</td>
<td>Admin.</td>
<td>WLAN3</td>
</tr>
</tbody>
</table>

He marks each Access Port with its intended location and WLAN, so he will not get confused later.
Leo selects the **Wireless** item in the left menu. He sees that only the first wireless LAN is enabled. None of the WLANs have the names he would like them to have. He clicks on the checkboxes to the left of **WLAN2** and **WLAN3**, then on the **Apply** button to enable these two WLANs.

Now that the WLANs are enabled, Leo needs to specify which Access Ports go with which WLANs.

He goes to the section labeled **Access Port Adoption List** and deselects the check boxes to the right of the row in which the MAC address range is specified as ANY.

For the engineering WLAN, Leo selects the **Add** button, then enters a **Start MAC value** of 00:A0:F8:BB:FC:94 and an **End MAC value** of 00:A0:F8:BB:FC:95. Leo selects the **WLAN1** checkbox and makes sure that the other WLAN checkboxes are not checked.

To specify the marketing WLAN, Leo clicks again on the **Add** button. In the new line, he enters the same MAC address, 00:A0:F8:BB:FC:96, for both the **Start MAC** and the **End MAC**. Leo selects the **WLAN2** checkbox and makes sure that the other WLAN checkboxes are not checked.

Finally, for the administration WLAN, Leo again clicks the **Add** button. He enters 00:A0:F8:BB:FC:97 as both the **Start MAC** and the **End MAC** address. He selects the **WLAN3** checkbox and makes sure that the other WLAN checkboxes for that row are not selected.
Leo clicks the **Apply** button to save his changes.

The next step is configure the WLANs.

**Configuring the WLANs**

Leo has specified which Access Ports go with which wireless LANs (WLANs). Now, he needs to name and configure each WLAN. He expands the **Wireless** node in the left menu, and selects the first WLAN listed.

Leo gives the WLAN the name **EngWLAN** so that subsequent screens in the WS 2000 interface will be a little easier to read. The ESSID is the identification string that his users will see, so he uses a name that will be easy for them to recognize, the string Engineering. The interface shows that this WLAN is already part of the Engineering subnet, so there is no reason to change it.
In the Advanced section of the screen, the **Disallow MU to MU Communications** setting would keep mobile units from communicating directly with each other. Leo believes that people sometimes share files directly, laptop to laptop, instead of using the file server. Leo does not want to prevent this type of communication, so he leaves this option disabled.

The **Use Voice Prioritization** option allows voice over IP (VoIP) devices, such as net phones, to have high priority access to the network. Without high priority access to the network, voice calls can rapidly degrade in quality when the network is busy. Leo does not think anyone is doing VoIP, but he is not sure, so he leaves that option turned on.

**Answer Broadcast ESS** instructs the Access Ports on this WLAN to respond to communications from mobile units that do not know what the ESSID for the wireless network is and which are using a default ESSID of 101. Leo knows that there are no such units in the office; if there were they would not have worked with the previous access point. Leo leaves this checkbox unchecked.

**Multicast Address 1** and **Multicast Address 2** are options included for compatibility with some VoIP phones which use multicast packets. Listing the multicast address allows the voice packets to avoid the usual multicast queue and improves the quality of the VoIP voice traffic. Leo doesn’t have any known need for these, so he leaves the addresses at the default.

Leo clicks the **Apply** button to save his changes.
Security

The next step to set security for the engineering WLAN. He selects the toggle to the left of EngWLAN in the left menu to display the EngWLAN Security item. Leo selects that item and the security screen is displayed. Leo selects 802.1x EAP as the authentication method and WPA2-CCMP as the encryption method.

Leo also needs to configure the 802.1x EAP system and the WPA2 encryption. Leo clicks 802.1x EAP Configuration. In the window that appears, he enters the RADIUS server information that he obtained from corporate system administration: the IP addresses of the RADIUS servers, the ports used for RADIUS communication, and the secret string used to start communication. He leaves the rest of the parameters at their default settings.
Leo clicks the **Ok** button to save the 802.1x EAP settings.

Leo then clicks the **WPA2-CCMP Settings** button. WPA2 constantly changes keys, but requires an initial key, known to both ends of the communication. If Leo was not using 802.1X EAP user authentication, that initial key would need to be entered here, in the Key Settings section. However, with 802.1x EAP, the RADIUS server supplies the initial key, so that Key Settings section is grayed out for Leo.

Leo does need to set the frequency with which the key for broadcast communication is changed. By default, the WS 2000 changes the broadcast every 84,600 seconds, i.e., every twenty-four hours. Breaking WEP encryption requires several hours of solid traffic, so Leo decides to change the broadcast key rotation to 3600 seconds, or once an hour.
Leo also selects **Allow WPA-TKIP clients** in the section labelled WPA-CCMP Mixed Mode. WPA-TKIP is an earlier version of the WPA encryption method. WPA2 is more secure, but not all wireless clients in Leo’s office are WPA2-capable. Selecting this option allows the older clients to use WPA-TKIP when they are not WPA2-CCMP-capable.

Leo also selects **Pre-Authentication and Opportunistic Key Caching** in the Fast Roaming section. These are options that are designed to make it easier for 802.1x wireless clients to roam within a WLAN. Under **Pre-Authentication**, a wireless client connected to one Access Port can communicate with other Access Ports and begin the authentication procedure before beginning to actual use that Access Port for network traffic. Under **Opportunistic Key Caching**, a wireless client which has agreed upon a given Pairwise Master Key (PMK) with one Access Port on a given WS 2000 is allowed to use that same PMK with other Access Ports connected to the same WS 2000. Both options increase the speed of roaming under 802.1x security and Leo enables both of them.

Leo clicks the **Ok** button to save his WPA2-CCMP settings, then the **Apply** button to confirm the WLAN configuration.

This completes configuration of the engineering WLAN. The sales and marketing WLAN and the administration WLAN are configured exactly the same way, with the sole exception that they take different names and ESSIDs.

<table>
<thead>
<tr>
<th>WLAN</th>
<th>WS 2000 Name</th>
<th>ESSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales and Marketing</td>
<td>MrkWLAN</td>
<td>Marketing</td>
</tr>
<tr>
<td>Administration</td>
<td>AdmWLAN</td>
<td>Administration</td>
</tr>
</tbody>
</table>

After these WLANs are configured, the next step is to configure the Access Ports.
Configuring the Access Ports

The WS 2000 allows the user to specify default settings for Access Ports. Leo expands the Access Ports node in the left menu and selects the **802.11b/g Defaults** node. Leo has four AP 300 ports and he will be able to set the defaults for these in this section.

All of the Access Ports will be indoors, so he specifies **Placement** as Indoors. He sets the default **Channel** as 1, even though all of his Access Ports will be using different 802.11b/g channels. He sets the **Power Level** to 20dBm. This will broadcast at 100 mW, the maximum level allowed in the US.

Leo leaves the **Slowest Supported Rate** and the **Fastest Supported Rate** as they are. The switch will operate at the maximum rate allowed by radio conditions, scaling back as needed. He sees no reason to change those parameters.

He does not change the settings for **Antenna Diversity**, **Support Short Preamble**, **RTS Threshold**, or **Beacon Settings**. These parameters control some of the broadcast mechanics of an 802.11 communication between mobile units and Access Ports. In most cases, there is no reason to change them. He clicks **Apply** to save his choices.

After configuring the default Access Port settings, Leo gets four short 100baseT cables and connects the four Access Ports to the switch. Just to make it easier to remember which port is which, he connects the one with the lowest MAC address to the first port number, the next lowest MAC address to the next port, and so on.

As he configures each Access Port, he will need to assign each Access Port to a channel. He can minimize radio interference if he has the radio channels for the different Access Ports separated as much as possible. He decides to use the following allocation:

<table>
<thead>
<tr>
<th>Access Port</th>
<th>Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering Offices</td>
<td>1</td>
</tr>
<tr>
<td>Demo Room</td>
<td>4</td>
</tr>
</tbody>
</table>
He clicks the toggle to the left of Access Ports in the left menu and selects the menu item labeled AP1. The WS 2000 has found and queried the Access Port for its MAC address. Leo enters a new name for the Access Port, Eng-AP1, and its location, Eng. Offices.

He sets the channel at 1, and notes the number. Access Ports channels should be separated as much as practical to minimize interference between them. The other engineering Access Port will use channel 4 and the marketing Access Port will use channel 7. He then sets the Power Level at the maximum setting of 100mW.

Leo leaves the Slowest Supported Rate and the Fastest Supported Rate as they are. The switch will operate at the maximum rate allowed by radio conditions, scaling back as needed. He sees no reason to change those parameters.

He also sees no reason to change the settings for Antenna Diversity, Support Short Preamble, RTS Threshold, or Beacon Settings. These parameters control some of the broadcast mechanics of an 802.11 conversation between mobile units and Access Ports. In most cases, there is no reason to change them.

He clicks the Apply button to save his changes.

Leo then selects AP2, the second engineering Access Port. He gives it a new name, a location, and assigns it channel 48.
Leo clicks the **Apply** button to save the configuration for this Access Port.

Leo then selects the third Access Port in the left menu. This will be the sales and marketing Access Port. Leo configures it similarly, but uses channel 7.
Leo clicks **Apply** to save his changes.

To avoid interference with the sales and marketing AP, Leo chooses channel 10 for the administration Access Port. He then enters the **Access Port Name** and **Location**.
Leo clicks the **Apply** button to save the changes for the administration Access Port.

The Access Ports are now configured. The next step is to specify access levels between the subnets.
Configuring Subnet Access

Leo selects the **Subnet Access** item in the left menu. This screen determines what subnet-to-subnet traffic can occur.

The subnet access defaults every subnet having access to every other subnet and full access to the WAN. Leo wants to restrict subnet access to that marketing has no access to the engineering subnet and no access to the administration subnet. He would also like to restrict all of the subnets to HTTP, SMTP, and POP access to the WAN.

First Leo will restrict access from the marketing subnet to the other subnets. He selects the cell in the matrix defined by **From Mrkt-SN** on the left and by **To Eng-SN** above. Then, in the Rules section, he pulls down the menu to the left of all protocols and selects **Deny**. This will block all traffic originating in the marketing subnet and going to the engineering subnet except the named protocols. No protocols were selected, so no traffic will be allowed.

Leo clicks on the **Apply** button to record this subnet access configuration.
Similarly, Leo restricts access from the marketing subnet to the administration subnet.

Leo would also like to restrict traffic from all subnets to the WAN to just HTTP, SMTP, and POP protocols. He selects the cell in the matrix defined by From Eng-SN on the left and To WAN above. Then he uses the Rules pull down menu to select Deny and specifies that HTTP, SMTP and POP are the exceptions.
Similarly, he restricts the marketing and administration subnets in their access to the WAN.

Leo clicks the **Apply** button to record his changes. The subnet access is configured.

Now Leo needs to set up VPN access to the Engineering Annex and test the installation.
Configuring the VPN

To configure a VPN link between WS 2000s, the following must be specified:

- The subnets on each end of the VPN link (tunnel)
- The authentication method for allowing a connection
- The encryption method for the content passed across the link

Both WS 2000s must be set up with complimentary information on each other.

Leo toggles open the **WAN** item in the left menu and selects **VPN**. Each VPN link between one subnet and another is called a **tunnel**.

---

**VPN Tunnel Configuration Settings for WS 2000 (1):**

- Tunnel Name: Eng2EngAnnex
- Local Subnet: Eng-SN
- Local LAN IP: 192.168.24.198
- Remote Subnet: 192.168.32.2 [For subnet defined on WS 2000 (2)]
- Remote Subnet Mask: 255.255.255.0
- Remote Gateway: 192.168.33.1 [LAN Port of WS 2000 (1)]

**VPN Tunnel Configuration Settings for WS 2000 (2):**

- Tunnel Name: Eng2EngAnnex
- Local Subnet: Anx-SN
- Local WAN IP: 192.168.33.1
- Remote Subnet: 192.168.32.1 [For Eng-SN on WS 2000 (1)]
- Remote Subnet Mask: 255.255.255.0
- Remote Gateway: 192.168.24.198 [LAN Port of WS 2000 (1)]
- Default Gateway: 192.168.24.198 [Set in WAN config of WS 2000 (2)]
Leo clicks the **Add** button to add a VPN tunnel.

Now Leo specifies the network parameters for the tunnel. The **Tunnel Name** is simply a name by which to distinguish one tunnel from another. Leo names the tunnel "Eng2EngAnnex."

The **Local Subnet** is the subnet that will be networked over the VPN, in this case, the Engineering subnet. The **Local WAN IP** is the IP address for the interface that this WS 2000 will show to the WS 2000 on the other side of the VPN. Leo enters an unused, internal IP address, 192.168.24.198.
The **Remote Subnet** specifies the subnet, on the other WS 2000, to which the engineering subnet will be connected. The **Remote Gateway** and the **Remote Subnet Mask** describe the network interface on the other WS 2000 switch. After Leo fills in these parameters, he clicks **Apply** to record the changes.

Now Leo needs to specify the authentication and encryption methods for the VPN link. He selects the simplest alternative, **Manual Key Settings**, since the link is so short and relatively unexposed.
The AH Authentication protocol is used between the two WS 2000 switches to authorize initialization of the VPN tunnel. The AH authentication method must match on both switches and the inbound key on one WS 2000 must match the outbound key on the other. Leo selects Secure Hash Algorithm 1 or SHA1 as the method and enters inbound and outbound 40 character authentication keys.

The inbound Security Parameter Index (SPI) for this WS 2000 must match the outbound SPI from the other switch and vice versa. Leo enters 100 for the Inbound SPI and 101 for the Outbound SPI.

The Encapsulating Security Payload or ESP is specified in the lower section. This specifies how the network packets will be encrypted between the two ends of the VPN tunnel. Leo chooses DES encryption and specifies the Inbound ESP Encryption Key so that it will match the Outbound ESP Encryption Key on the other WS 2000. He also specifies the Outbound ESP Encryption Key on this WS 2000 so that it will match the Inbound ESP Encryption Key on the other switch.

Finally, the Inbound and Outbound SPI fields in the encryption section on this WS 2000 must match the Outbound and Inbound SPIs on the other WS 2000. Leo enters 110 for the Inbound SPI and 111 for the Outbound SPI.

Leo clicks Ok to record the Manual Key Settings. Then he clicks the Apply button to confirm this configuration.

The switch is now configured!

Installing the Access Ports and Testing

The switch is now configured. Leo connects the switch’s WAN port to the VPN appliance that goes to the outside world. He gets three laptops and sets each of them to use DHCP for IP address assignment, 802.1x EAP for user authentication, and WPA-TKIP for data encryption over the wireless link. He uses the first laptop to connect to the engineering WLAN, the
second to connect to the sales and marketing WLAN, and the third laptop to connect to the administration WLAN. He makes sure that laptops on each WLAN can connect to the WAN and to each other.

After he has tested the three subnets, he installs the Access Ports in their permanent locations. He test coverage with the laptops, making sure each Access Port is covering its assigned area. He also unplugs each of the engineering Access Ports, in turn, to be sure that both are working properly. When everything seems to be working, he sends an email to the users telling them that the new wireless network is up and running!
<table>
<thead>
<tr>
<th>Command Line Interface Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin and Common Commands</strong></td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; admin</td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; help</td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; passwd</td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; quit</td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; save</td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; summary</td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; ..</td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; /</td>
</tr>
<tr>
<td><strong>Network Commands</strong></td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; network</td>
</tr>
<tr>
<td><strong>Network AP Commands</strong></td>
</tr>
<tr>
<td>WS2000&gt;admin(network)&gt; ap</td>
</tr>
<tr>
<td>WS2000&gt;admin(network.ap)&gt; add</td>
</tr>
<tr>
<td>WS2000&gt;admin(network.ap)&gt; copydefaults</td>
</tr>
<tr>
<td>WS2000&gt;admin(network.ap)&gt; delete</td>
</tr>
<tr>
<td>WS2000&gt;admin(network.ap)&gt; list</td>
</tr>
<tr>
<td>WS2000&gt;admin(network.ap)&gt; reset</td>
</tr>
<tr>
<td>WS2000&gt;admin(network.ap)&gt; set</td>
</tr>
<tr>
<td>WS2000&gt;admin(network.ap)&gt; show</td>
</tr>
<tr>
<td><strong>Network AP Default Commands</strong></td>
</tr>
<tr>
<td>WS2000&gt;admin(network.ap)&gt; default</td>
</tr>
<tr>
<td>WS2000&gt;admin(network.ap.default)&gt; set</td>
</tr>
<tr>
<td>WS2000&gt;admin(network.ap.default)&gt; show</td>
</tr>
<tr>
<td><strong>Network AP Test Commands</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
WS2000>admin(network.ap)> test ........................................... 13-33
WS2000>admin(network.ap.test)> new .................................. 13-34

Network DHCP Commands .................................................. 13-35
WS2000>admin(network)> dhcp ............................................ 13-35
WS2000>admin(network.dhcp)> set ....................................... 13-36
WS2000>admin(network.dhcp)> show ..................................... 13-37

Network Firewall Commands ............................................... 13-38
WS2000>admin(network)> fw ............................................. 13-38
WS2000>admin(network.fw)> set ......................................... 13-39
WS2000>admin(network.fw)> show ...................................... 13-41

Network Firewall Policy Commands ...................................... 13-42
WS2000>admin(network.fw)> policy ..................................... 13-42
WS2000>admin(network.fw.policy)> import .......................... 13-43

Network Firewall Policy Inbound Commands ............................ 13-44
WS2000>admin(network.fw.policy)> inb ................................ 13-44
WS2000>admin(network.fw.policy.inb)> add ............................ 13-45
WS2000>admin(network.fw.policy.inb)> delete ....................... 13-46
WS2000>admin(network.fw.policy.inb)> insert ....................... 13-47
WS2000>admin(network.fw.policy.inb)> list .......................... 13-48
WS2000>admin(network.fw.policy.inb)> move ....................... 13-49
WS2000>admin(network.fw.policy.inb)> set .......................... 13-50

Network Firewall Policy Outbound Commands ........................ 13-51
WS2000>admin(network.fw.policy)> outb .............................. 13-51
WS2000>admin(network.fw.policy.outb)> add ....................... 13-52
WS2000>admin(network.fw.policy.outb)> delete ................... 13-53
WS2000>admin(network.fw.policy.outb)> insert .................... 13-54
WS2000>admin(network.fw.policy.outb)> list ....................... 13-55
WS2000>admin(network.fw.policy.outb)> move .................... 13-56
WS2000>admin(network.fw.policy.outb)> set ....................... 13-57

Network Firewall Submap Commands ..................................... 13-58
WS2000>admin(network.fw)> submap ................................. 13-58
WS2000>admin(network.fw.submap)> add ......................... 13-59
WS2000>admin(network.fw.submap)> delete ....................... 13-60
WS2000>admin(network.fw.submap)> list ........................... 13-61
WS2000>admin(network.fw.submap)> set ........................... 13-62
WS2000>admin(network.fw.submap)> show ......................... 13-63

Network LAN Commands .................................................... 13-64
WS2000>admin(network)> lan ........................................... 13-64
WS2000>admin(network.lan)> set .................................... 13-65
WS2000>admin(network.lan)> show .................................. 13-66

Network LAN DHCP Commands ............................................ 13-67
WS2000>admin(network.lan)> dhcp ................................... 13-67
WS2000>admin(network.lan.dhcp)> add .............................. 13-68
WS2000>admin(network.lan.dhcp)> delete ......................... 13-69
WS2000>admin(network.lan.dhcp)> list ............................ 13-70
WS2000>admin(network.lan.dhcp)> set ............................ 13-71
WS2000>admin(network.lan.dhcp)> show ......................... 13-72

Network QoS Commands .................................................... 13-73
WS2000>admin(network.qos)> qos ................................................................. 13-73
WS2000>admin(network.qos)> clear ......................................................... 13-74
WS2000>admin(network.qos)> set ......................................................... 13-75
WS2000>admin(network.qos)> show ....................................................... 13-76

Network Router Commands ................................................................. 13-77
WS2000>admin(network.router)> router ............................................... 13-77
WS2000>admin(network.router)> add ................................................... 13-78
WS2000>admin(network.router)> delete ............................................... 13-79
WS2000>admin(network.router)> list ................................................... 13-80
WS2000>admin(network.router)> set ................................................... 13-81
WS2000>admin(network.router)> show ................................................. 13-82

Network VLAN Commands ................................................................. 13-83
WS2000>admin(network.vlan)> vlan .................................................... 13-83
WS2000>admin(network.vlan)> set .................................................... 13-84
WS2000>admin(network.vlan)> show .................................................. 13-85

Network VLAN Trunk Commands ......................................................... 13-86
WS2000>admin(network.vlan.trunk)> trunk ......................................... 13-86
WS2000>admin(network.vlan.trunk)> clear ......................................... 13-87
WS2000>admin(network.vlan.trunk)> set ............................................. 13-88
WS2000>admin(network.vlan.trunk)> show ......................................... 13-89

Network WAN Commands ................................................................. 13-90
WS2000>admin(network.wan)> wan ..................................................... 13-90
WS2000>admin(network.wan)> renew ............................................... 13-91
WS2000>admin(network.wan)> set ..................................................... 13-92
WS2000>admin(network.wan)> show .................................................. 13-93

Network WAN App Commands ........................................................... 13-94
WS2000>admin(network.wan.app)> app .............................................. 13-94
WS2000>admin(network.wan.app)> addcmd ....................................... 13-95
WS2000>admin(network.wan.app)> delcmd ....................................... 13-97
WS2000>admin(network.wan.app)> list .............................................. 13-99

Network WAN NAT Commands .......................................................... 13-100
WS2000>admin(network.wan)> nat ..................................................... 13-100
WS2000>admin(network.wan)> add .................................................... 13-101
WS2000>admin(network.wan)> delete ................................................ 13-102
WS2000>admin(network.wan)> list .................................................... 13-103
WS2000>admin(network.wan)> set .................................................... 13-104
WS2000>admin(network.wan)> show .................................................. 13-105

Network WAN VPN Commands .......................................................... 13-106
WS2000>admin(network.wan)> vpn ..................................................... 13-106
WS2000>admin(network.wan.vpn)> add ............................................ 13-107
WS2000>admin(network.wan.vpn)> delete ........................................ 13-108
WS2000>admin(network.wan.vpn)> ikestate ...................................... 13-109
WS2000>admin(network.wan.vpn)> list ............................................. 13-110
WS2000>admin(network.wan.vpn)> reset .......................................... 13-111
WS2000>admin(network.wan.vpn)> set ............................................. 13-112
WS2000>admin(network.wan.vpn)> stats ......................................... 13-116

Network WAN VPN Cmgr Commands .................................................. 13-117
WS2000>admin(network.wan.vpn)> cmgr ......................................... 13-117
WS2000>admin(network.wan.vpn.cmgr)> delca .................................................. 13-118
WS2000>admin(network.wan.vpn.cmgr)> delprivkey ............................................ 13-119
WS2000>admin(network.wan.vpn.cmgr)> delself ................................................... 13-120
WS2000>admin(network.wan.vpn.cmgr)> expcert ................................................ 13-121
WS2000>admin(network.wan.vpn.cmgr)> genreq .................................................. 13-122
WS2000>admin(network.wan.vpn.cmgr)> impcert ............................................... 13-123
WS2000>admin(network.wan.vpn.cmgr)> listca .................................................... 13-124
WS2000>admin(network.wan.vpn.cmgr)> listprivkey ........................................... 13-125
WS2000>admin(network.wan.vpn.cmgr)> listself ............................................... 13-126
WS2000>admin(network.wan.vpn.cmgr)> loadca ............................................... 13-127
WS2000>admin(network.wan.vpn.cmgr)> loadself ............................................. 13-128
WS2000>admin(network.wan.vpn.cmgr)> showreq ............................................. 13-129
WS2000>admin(network.wan.vpn.cmgr)> loadself ............................................. 13-128
WS2000>admin(network.wan.vpn.cmgr)> listself ............................................... 13-126
WS2000>admin(network.wan.vpn.cmgr)> listprivkey ........................................... 13-125
WS2000>admin(network.wan.vpn.cmgr)> impcert .............................................. 13-123
WS2000>admin(network.wan.vpn.cmgr)> delself ................................................ 13-120
WS2000>admin(network.wan.vpn.cmgr)> delprivkey .......................................... 13-119
WS2000>admin(network.wan.vpn.cmgr)> delca .................................................. 13-118

Network WLAN Commands ................................................................. 13-130
WS2000>admin(network.wan)> wlan ............................................................... 13-130
WS2000>admin(network.wan)> add ................................................................. 13-131
WS2000>admin(network.wan)> delete ............................................................ 13-132
WS2000>admin(network.wan)> list ................................................................. 13-133
WS2000>admin(network.wan)> set ................................................................. 13-134
WS2000>admin(network.wan)> show .............................................................. 13-138

Network WLAN Rogue AP Commands ....................................................... 13-140
WS2000>admin(network.wlan)> rogueap ......................................................... 13-140
WS2000>admin(network.wlan.rogueap)> set .................................................. 13-141
WS2000>admin(network.wlan.rogueap)> show ................................................ 13-142

Network WLAN Rogue AP Approved AP List Commands ............................... 13-143
WS2000>admin(network.wlan.rogueap.approvedlist)> approvedlist .................. 13-143
WS2000>admin(network.wlan.rogueap.approvedlist)> ageout ......................... 13-144
WS2000>admin(network.wlan.rogueap.approvedlist)> approve ....................... 13-145
WS2000>admin(network.wlan.rogueap.approvedlist)> erase ......................... 13-146
WS2000>admin(network.wlan.rogueap.approvedlist)> show ......................... 13-147

Network WLAN Rogue AP List Commands ................................................ 13-148
WS2000>admin(network.wlan.rogueap)> roguelist ........................................ 13-148
WS2000>admin(network.wlan.rogueap.roguelist)> ageout ............................ 13-149
WS2000>admin(network.wlan.rogueap.roguelist)> approve ......................... 13-150
WS2000>admin(network.wlan.rogueap.roguelist)> erase ............................ 13-151
WS2000>admin(network.wlan.rogueap.roguelist)> show ............................. 13-152

Network WLAN Rogue AP Locate Commands .............................................. 13-153
WS2000>admin(network.wlan.rogueap.roguelist)> locate .................................. 13-153
WS2000>admin(network.wlan.rogueap.roguelist.locate)> list ......................... 13-154
WS2000>admin(network.wlan.rogueap.roguelist.locate)> start ....................... 13-155

Network WLAN Rogue AP MU Scan Commands ........................................... 13-156
WS2000>admin(network.wlan.rogueap.muscan)> muscan .................................. 13-156
WS2000>admin(network.wlan.rogueap.muscanlist.muscan)> list .................... 13-157
WS2000>admin(network.wlan.rogueap.muscanlist.muscan)> start .................. 13-158

Network WLAN Rogue AP Rule List Commands .......................................... 13-159
WS2000>admin(network.wlan.rogueap)> rulelist ........................................... 13-159
WS2000>admin(network.wlan.rogueap.rulelist)> add ..................................... 13-160
WS2000>admin(network.wlan.rogueap.rulelist)> authsymbolap ...................... 13-161
WS2000>admin(network.wlan.rogueap.rulelist)> delete ............................... 13-162
<table>
<thead>
<tr>
<th>Command Line Interface Reference</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistics Commands</td>
<td>13-164</td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; stats</td>
<td>13-164</td>
</tr>
<tr>
<td>WS2000&gt;admin(stats)&gt; show</td>
<td>13-165</td>
</tr>
<tr>
<td>Statistics RF Commands</td>
<td>13-167</td>
</tr>
<tr>
<td>WS2000&gt;admin(stats)&gt; rf</td>
<td>13-167</td>
</tr>
<tr>
<td>WS2000&gt;admin(stats.rf)&gt; reset</td>
<td>13-168</td>
</tr>
<tr>
<td>System Commands</td>
<td>13-172</td>
</tr>
<tr>
<td>WS2000&gt;admin&gt; system</td>
<td>13-172</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; lastpw</td>
<td>13-173</td>
</tr>
<tr>
<td>System Authentication Commands</td>
<td>13-174</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; authentication</td>
<td>13-174</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.authentication)&gt; set</td>
<td>13-175</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.authentication)&gt; show</td>
<td>13-176</td>
</tr>
<tr>
<td>System Authentication RADIUS Commands</td>
<td>13-177</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.authentication)&gt; radius</td>
<td>13-177</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.authentication.radius)&gt; set</td>
<td>13-178</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.authentication.radius)&gt; show</td>
<td>13-179</td>
</tr>
<tr>
<td>System Configuration Commands</td>
<td>13-180</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; config</td>
<td>13-180</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; default</td>
<td>13-181</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; export</td>
<td>13-182</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; import</td>
<td>13-184</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; partial</td>
<td>13-185</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; set</td>
<td>13-186</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; show</td>
<td>13-187</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.config)&gt; update</td>
<td>13-188</td>
</tr>
<tr>
<td>System Logs Commands</td>
<td>13-189</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; logs</td>
<td>13-189</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.logs)&gt; delete</td>
<td>13-190</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.logs)&gt; send</td>
<td>13-191</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.logs)&gt; set</td>
<td>13-192</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.logs)&gt; show</td>
<td>13-193</td>
</tr>
<tr>
<td>System NTP Commands</td>
<td>13-195</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; ntp</td>
<td>13-195</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.ntp)&gt; set</td>
<td>13-196</td>
</tr>
<tr>
<td>System RADIUS Commands</td>
<td>13-198</td>
</tr>
<tr>
<td>WS2000&gt;admin(system)&gt; radius</td>
<td>13-198</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.radius)&gt; set</td>
<td>13-199</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.radius)&gt; show</td>
<td>13-200</td>
</tr>
<tr>
<td>System RADIUS Client Commands</td>
<td>13-201</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.radius)&gt; client</td>
<td>13-201</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.radius.client)&gt; add</td>
<td>13-202</td>
</tr>
<tr>
<td>WS2000&gt;admin(system.radius.client)&gt; del</td>
<td>13-203</td>
</tr>
</tbody>
</table>
WS2000>admin(system.radius.client)> show .................................................. 13-204

System RADIUS EAP Commands ......................................................... 13-205
  WS2000>admin(system.radius)> eap .................................................. 13-205
  WS2000>admin(system.radius.eap)> import .................................. 13-206
  WS2000>admin(system.radius.eap)> set ...................................... 13-207
  WS2000>admin(system.radius.eap)> show .................................. 13-208

System RADIUS EAP PEAP Commands ................................................. 13-209
  WS2000>admin(system.radius.eap)> peap .................................. 13-209
  WS2000>admin(system.radius.eap.peap)> set .............................. 13-210
  WS2000>admin(system.radius.eap.peap)> show ......................... 13-209

System RADIUS EAP TTLS Commands ................................................ 13-212
  WS2000>admin(system.radius.eap)> ttls .................................. 13-212
  WS2000>admin(system.radius.eap.ttls)> set .................................... 13-213
  WS2000>admin(system.radius.eap.ttls)> show .................................... 13-214

System RADIUS LDAP Commands ....................................................... 13-215
  WS2000>admin(system.radius)> ldap ........................................ 13-215
  WS2000>admin(system.radius.ldap)> set .................................. 13-216
  WS2000>admin(system.radius.ldap)> show .................................. 13-217

System RADIUS Policy Commands ..................................................... 13-218
  WS2000>admin(system.radius)> policy .................................. 13-218
  WS2000>admin(system.radius.policy)> set .................................. 13-219
  WS2000>admin(system.radius.policy)> show .................................. 13-220

System RADIUS Proxy Commands ...................................................... 13-221
  WS2000>admin(system.radius)> proxy ......................................... 13-221
  WS2000>admin(system.radius.proxy)> add .................................. 13-222
  WS2000>admin(system.radius.proxy)> del .................................. 13-223
  WS2000>admin(system.radius.proxy)> set .................................. 13-224
  WS2000>admin(system.radius.proxy)> show .................................. 13-225

System Redundancy Commands .......................................................... 13-226
  WS2000>admin(system)> redundancy ........................................ 13-226
  WS2000>admin(system.radius.redundancy)> set .......................... 13-227
  WS2000>admin(system.radius.redundancy)> show ...................... 13-228

System SNMP Commands ............................................................... 13-229
  WS2000>admin(system)> snmp .................................................. 13-229

System SNMP Access Commands ....................................................... 13-230
  WS2000>admin(system.snmp)> access ........................................ 13-230
  WS2000>admin(system.snmp.access)> add .................................. 13-231
  WS2000>admin(system.snmp.access)> delete .................................. 13-233
  WS2000>admin(system.snmp.access)> list .................................. 13-235
  WS2000>admin(system.snmp.access)> show .................................. 13-236

System SNMP Traps Commands ........................................................ 13-237
  WS2000>admin(system.snmp.traps)> traps .................................. 13-237
  WS2000>admin(system.snmp.traps)> add .................................. 13-238
  WS2000>admin(system.snmp.traps)> delete .................................. 13-240
  WS2000>admin(system.snmp.traps)> list .................................. 13-241
  WS2000>admin(system.snmp.traps)> set .................................. 13-242
  WS2000>admin(system.snmp.traps)> show .................................. 13-245
System SSH Commands .......................... 13-248
  WS2000>admin(system)> ssh .................... 13-248
  WS2000>admin(system.ssh)> set .................. 13-249
  WS2000>admin(system.ssh)> show ................. 13-250
System User Database Commands ............... 13-251
  WS2000>admin(system)> userdb ................. 13-251
System User Database Group Commands ......... 13-252
  WS2000>admin(system.userdb)> group ............ 13-252
  WS2000>admin(system.userdb.group)> add .......... 13-253
  WS2000>admin(system.userdb.group)> create .... 13-254
  WS2000>admin(system.userdb.group)> delete .... 13-255
  WS2000>admin(system.userdb.group)> remove .... 13-256
  WS2000>admin(system.userdb.group)> show ........ 13-257
System User Database User Commands .......... 13-258
  WS2000>admin(system.userdb)> user ............... 13-258
  WS2000>admin(system.userdb.user)> add ........ 13-259
  WS2000>admin(system.userdb.user)> del .......... 13-260
  WS2000>admin(system.userdb.user)> set .......... 13-261
  WS2000>admin(system.userdb.user)> show ........ 13-262
System WS2000 Commands ....................... 13-263
  WS2000>admin(system)> ws2000 ................. 13-263
  WS2000>admin(system.ws2000)> restart .......... 13-264
  WS2000>admin(system.ws2000)> set .............. 13-265
  WS2000>admin(system.ws2000)> show ............. 13-267
13.1 Admin and Common Commands

WS2000>admin> admin

Description:
Displays admin configuration options. The items available under this command are shown below.

Syntax:

- help: Displays general user interface help.
- passwd: Changes the admin password.
- summary: Shows a system summary.
- network: Goes to the network submenu
- stats: Goes to the stats submenu.
- system: Goes to the system submenu.
- save: Saves the configuration to system flash.
- quit: Quits the CLI.
- ..: Goes to the parent menu.
- /: Goes to the root menu.
WS2000>admin> help

Description:
Displays general CLI user interface help.

Syntax:
help Displays command line help.

Example:
admin> help

? : display command help - Eg. ?, show ?, s?
<ctrl-q> : go backwards in command history
<ctrl-p> : go forwards in command history
* Note : commands can be incomplete - Eg. sh = sho = show
WS2000>admin> passwd

Description:
Changes the password for the admin login.

Syntax:
passwd

Changes the admin password. This requires typing the old admin password. Passwords can be up to 11 characters.

Example:
admin>passwd

Old Admin Password:******
New Admin Password:******
Verify Admin Password:******
WS2000>admin> quit

Description:

Quits the command line interface.

This command appears in all of the submenus under admin. In each case, it has the same function, to exit out of the CLI.

Example:

ws2000>admin>quit
WS2000>admin> save

Description:

Saves the configuration to system flash.

This command appears in all of the submenus under admin. In each case, it has the same function, to save the configuration.

Syntax:

save       Saves configuration settings. This command works at all levels of the CLI. The save command must be issued before leaving the UI for the settings to be retained.

Example:

admin>save
admin>
WS2000>admin> summary

Description:
Displays the system summary.

Syntax:
summary Displays a summary of high-level characteristics and settings for the WAN, subnet, and WLAN.

Example:

    admin>summary

System Information

WS2000 firmware version : 1.5.0.0-160b
country code : us

WLAN 1 Information

ess identifier : 101
wlan mode : enable
enc type : none
auth type : none

WLAN 2 Information

ess identifier : 102
wlan mode : disable
enc type : none
auth type : none

WLAN 3 Information

ess identifier : 103
wlan mode : disable
enc type : none
auth type : none

WLAN 4 Information

ess identifier : 104
wlan mode : disable
enc type : none
auth type : none

Subnet 1 Information

subnet interface : enable
ip address : 192.168.0.1
network mask : 255.255.255.0
dhcp mode : server
default gateway : 192.168.0.1
ports : port1 port2 port3 port4 port5 port6
wlans : wlan1

Subnet 2 Information

subnet interface : disable
ip address : 192.168.1.1
network mask : 255.255.255.0
dhcp mode : server
default gateway : 192.168.1.1
ports :
wlans : wlan2

Subnet 3 Information

subnet interface : disable
ip address : 192.168.2.1
network mask : 255.255.255.0
dhcp mode : server
default gateway : 192.168.2.1
ports :
wlans : wlan3

Subnet 4 Information

subnet interface : disable
ip address : 192.168.3.1
network mask : 255.255.255.0
dhcp mode : server
default gateway : 192.168.3.1
ports :
wlans : wlan4
Primary WAN Information

wan interface : enable
ip address : 192.168.24.198
network mask : 255.255.255.0
default gateway : 192.168.24.1
dhcp mode : enable

admin>
**WS2000>admin> ..**

**Description:**

Displays the parent menu of the current menu.

This command appears in all of the submenus under admin. In each case, it has the same function, to move up one level in the directory structure.

**Example:**

```
admin(network.ap)>..
admin(network)>
```
WS2000>admin> /

**Description:**

Displays the root menu, that is, the top-level CLI menu.

This command appears in all of the submenus under admin. In each case, it has the same function, to move up to the top level in the directory structure.

**Example:**

```plaintext
admin(network.ap)>/
admin>
```
13.2 Network Commands

**WS2000>admin> network**

**Description:**
Displays the network submenu. The items available under this command are shown below.

- **ap**
  - Goes to the Access Port submenu.
- **lan**
  - Goes to the LAN submenu.
- **router**
  - Goes to the router submenu.
- **vlan**
  - Goes to the VLAN submenu.
- **wan**
  - Goes to the WAN submenu.
- **dhcp**
  - Goes to the DHCP submenu.
- **wlan**
  - Goes to the WLAN submenu.
- **fw**
  - Goes to the firewall submenu.
- **save**
  - Saves the configuration to system flash.
- **quit**
  - Quits the CLI.
- **qos**
  - Goes to the QoS submenu.
- **..**
  - Goes to the parent menu.
- **/**
  - Goes to the root menu.
13.3 Network AP Commands

WS2000>admin(network)> ap

Description:
Displays the Access Port submenu. The functionality provided by this menu is supplied by various screen under the Wireless menu item of the Web interface. The items available under this command are shown below.

- **add**: Adds entries to the Access Port adoption list.
- **delete**: Deletes entries from the Access Port adoption list.
- **list**: Lists entries in the Access Port adoption list.
- **set**: Sets Access Port parameters.
- **show**: Shows Access Port parameters.
- **copydefaults**: Copies default AP settings to a connected AP.
- **default**: Goes to the default submenu.
- **reset**: Resets an Access Port.
- **test**: Goes to the test submenu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- `..`: Goes to the parent menu.
- `/`: Goes to the root menu.
WS2000>admin(network.ap)> add

**Description:**

Adds entries to the Access Port adoption list. Performs functionality available in the Access Port Adoption List area of the Wireless screen.

**Syntax:**

```
add <idx> <mac1> <mac2>   Allows adoption of Access Ports with MAC addresses in the range of <mac1> to <mac2> associated with WLAN <idx> (WLAN 1–4).
```

**Example:**

```
admin(network.ap)>add 1 000000000000 00306542b965
admin(network.ap)>list 1
```

```
index  start mac  end mac
1 000000000000 00306542b965
```

**Related Commands:**

- `delete` Removes the MAC address range from the adoption list for the specified WLAN.
- `list` Displays entries in the Access Port adoption list.
WS2000>admin(network.ap)> copydefaults

Description:
Copies default Access Port settings to a connected Access Port. In the Web interface, the defaults are set on the Wireless, default AP screens (one for each radio type).

Syntax:
copydefaults <idx> Copies default Access Port settings to the connected AP specified by <idx>.

Example:
admin(network.ap) > copydefaults 1

Related Commands:
default  show  defaults Lists the current default settings for a selected Access Port type.
show  status Lists the index numbers for all currently connected Access Ports.
show  ap Gets information about a particular Access Port.
WS2000>admin(network.ap)> delete

Description:

Deletes entries from the Access Port adoption list. In the Web interface, this functionality is found on the Wireless screen in the Access Port Adoption list area.

Syntax:

```
delete  <idx>  <entry>     Deletes an entry in the Access Port adoption list as specified by <entry>, which is the number listed in the adoption list (use list command) for WAN <idx> (1-4).
<idx>  all     Deletes all entries in the Access Port adoption list.
```

Example:

The following example first lists out the adoption list entries for WLAN 1, deletes the second entry for WLAN 1, and finally displays the list for WLAN 1 showing that the entry has been deleted.

```
admin(network.ap)>list 1

index  start mac       end mac
-----------------------------
1      000000000000      00306542B965
2      004000000000      005000000000

admin(network.ap)>delete 1 2
admin(network.ap)>list 1

index  start mac       end mac
-----------------------------
1      000000000000      00306542B965
```

Related Commands:

- `add`          Adds entries to the adoption list.
- `list`         Lists entries in the Access Port adoption list.
WS2000>admin(network.ap)> list

**Description:**
Displays entries in the Access Port adoption list for a specified wireless LAN.

**Syntax:**

```
list <idx>   Lists the Access Port adoption entries for WLAN <idx> (1–4).
```

**Example:**

The following example shows the access port adoption list for WLAN 1.

```
admin(network.ap)>list 1

+-----------------------------------+--------+--------+
| index | start mac | end mac |
+-----------------------------------+--------+--------+
| 1     | 000000000000 | 00306542B965 |
| 2     | 004000000000 | 005000000000 |
```

**Related Commands:**

- **add**: Adds entries to the adoption list.
- **delete**: Deletes entries from the adoption list.
WS2000>admin(network.ap)> reset

Description:
Resets an Access Port.

Syntax:
reset ap <idx>   Resets the Access Port associated with index <idx>.

Example:
admin(network.ap)>reset ap 2
admin(network.ap)>?
Command Line Interface Reference

WS2000>admin(network.ap)> set

**Description:**

Sets Access Port parameters.

**Syntax:**

<table>
<thead>
<tr>
<th>set</th>
<th>beacon</th>
<th>mode</th>
<th>enable/disable</th>
<th>interval</th>
<th>ch_mode</th>
<th>fixed/random</th>
<th>div</th>
<th>&lt;idx&gt;</th>
<th>&lt;mode&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sets the beacon interval for Access Port <idx> (1–12) to <interval> in K-us (50–200).

Sets the channel mode for Access Port <idx> to fixed or random.

Sets the default antenna diversity to <mode> (one of full, primary, or secondary).

Sets the DTIM period for Access Port <idx> to <period> (number of beacons from 1–50).

Sets Access Port <idx> location description to <loc> (1–13 characters).

Sets Access Port <idx> name to <name> (1–13 characters).

Sets the primary WLAN <widx> (the WLAN index from 1 to 4) for 802.11a radio associated with Access Port <idx>. The ESS ID configured for this WLAN will be used in the 802.11a beacon as the primary ESS.

**Note:** This parameter is used only for AP200 APs with 802.11a radios

Sets Access Port <idx> basic and supported rates. <basic> and <supported> must be comma-separated lists of rates, such as 6,9,11,15 with no spaces. Basic rates are a subset of supported rates. The different types of radio support the following rates.

- **A** - 6|9|12|18|24|36|48|54
- **B** - 1|2|5.5|11
- **G** - 1|2|5.5|6|9|11|12|18|24|36|48|54

**Note:** For a G radio, basic rates must be a subset of B Rates in order to associate legacy B stations.

Sets Access Port <idx> regulatory parameters, which <indoor> is one of in or in/out; <ch> is the channel to use, and <pwr> is the power (in dB from 4 to 20). Select the value of <ch> from the appropriate list.

- **802.11b ch** -- 1 to 14
- **802.11a ch** -- 36,40,44,48,52,56,60,64,149,153,157,161

**Note:** Regulatory parameter values depend on country of operation and radio type. Refer to documentation for regulatory information.

Sets the RTS threshold for Access Port <idx> to <bytes> (e.g., 2341).

Enables or disables the short preamble mode for Access Port <idx>.
Example:

```
admin(network.ap)>set short-pre enable
admin(network.ap)>set shor 1 enable
admin(network.ap)>set name 1 BigOffice
admin(network.ap)>set dtim 1 25
admin(network.ap)>set loc 1 BigBldg
admin(network.ap)>show ap 1
```

```
ap name                  : BigOffice
ap location              : BigBldg
ap mac address           : 00A0F8565656
ap serial number         : 00A0F8565656
ap radio type            : 802.11 B
adopted by               : WLAN1

ap indoor use            : indoor/outdoor
ap channel               : 1
ap radio power           : 4 dB
antenna gain             : 0 dBi
rf power                 : 3 mW
antenna type             : external
ap diversity             : full

basic rates              : 1 2
supported rates          : 1 2 5.5 11

rts threshold            : 2341
beacon interval          : 100
dtim period              : 25
short preamble           : enable
security beacon (hide ess) : disable
primary wlan index       : wlan1
```

```
admin(network.ap)>
```
WS2000>admin(network.ap)> show

Description:

Shows Access Port parameters.

Syntax:

show ap <idx>  Shows Access Port <idx> radio parameters.
status  Shows a list of Access Ports and their status.

Example:

admin(network.ap)>show ap 1

ap name : BigOffice
ap location : BigBldg
ap mac address : 00A0F8565656
ap serial number : 00A0F8565656
ap radio type : 802.11 B
adopted by : WLAN1

ap indoor use : indoor/outdoor
ap channel : 1
ap radio power : 4 dB
antenna gain : 0 dBi
rf power : 3 mW

antenna type : external
ap diversity : full

basic rates : 1 2
supported rates : 1 2 5.5 11

rts threshold : 2341
beacon interval : 100
dtim period : 25
short preamble : enable
security beacon (hide ess) : disable
primary wlan index : wlan1
detector ap : disable

admin(network.ap)>show status

ap index : 1
ap status : connected
ap index : 2
ap status : not connected

ap index : 3
ap status : not connected

ap index : 4
ap status : not connected

ap index : 6
ap status : not connected

ap index : 7
ap status : not connected

ap index : 8
ap status : not connected

ap index : 9
ap status : not connected

ap index : 10
ap status : not connected

ap index : 11
ap status : not connected

ap index : 12
ap status : not connected

admin(network.ap)>

Related Commands:

set Sets Access Port parameters.
13.4 Network AP Default Commands

WS2000>admin(network.ap)> default

Description:

Displays the default Access Port (AP) submenu. The items available under this command are shown below.

set  Sets default Access Port parameters.
show Shows default Access Port parameters.
save Saves the configuration to system flash.
quit  Quits the CLI.
..  Goes to the parent menu.
/    Goes to the root menu.

The items in this menu are available in the Web interface under the three default Access Port screens (one for each radio type) within the Wireless menu area.
**WS2000>admin(network.ap.default)> set**

**Description:**
Sets the default Access Port parameters.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameter(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>beacon</td>
<td>Sets the default for secure beacons of specified type <code>&lt;type&gt;</code> (one of 802.11a, 802.11b, or 802.11b/g) to enable or disable.</td>
</tr>
<tr>
<td></td>
<td>mode</td>
<td>Sets the default beacon interval for specified radio type (one of 802.11a, 802.11b, or 802.11b/g) to <code>&lt;interval&gt;</code> in K-us (50–200).</td>
</tr>
<tr>
<td></td>
<td>intvl</td>
<td>Sets the default channel mode for radios of <code>&lt;type&gt;</code> (one of 802.11a, 802.11b, or 802.11b/g) to fixed or random.</td>
</tr>
<tr>
<td>ch-mode</td>
<td><code>&lt;type&gt;</code></td>
<td>Sets the default channel mode for radios of <code>&lt;type&gt;</code> (one of 802.11a, 802.11b, or 802.11b/g) to <code>&lt;mode&gt;</code> (one of full, primary, or secondary).</td>
</tr>
<tr>
<td>div</td>
<td><code>&lt;type&gt;</code></td>
<td>Sets the default antenna diversity for radios of <code>&lt;type&gt;</code> (one of 802.11a, 802.11b, or 802.11b/g) to <code>&lt;mode&gt;</code> (one of full, primary, or secondary).</td>
</tr>
<tr>
<td>dtim</td>
<td><code>&lt;type&gt;</code></td>
<td>Sets the default DTIM period for radios of specified <code>&lt;type&gt;</code> (one of 802.11a, 802.11b, or 802.11b/g) to <code>&lt;period&gt;</code> number of beacons (1–50).</td>
</tr>
<tr>
<td>primary</td>
<td><code>&lt;type&gt;</code></td>
<td>Sets the default primary WLAN <code>&lt;widx&gt;</code> (1 to 4) for 802.11a radios of specified <code>&lt;type&gt;</code> (one of 802.11a, 802.11b, or 802.11b/g). The ESS ID configured for this WLAN will be used in the 802.11a beacon as the primary ESS.</td>
</tr>
<tr>
<td>rate</td>
<td><code>&lt;type&gt;</code></td>
<td>Sets the default basic and supported rates for radios of specified <code>&lt;type&gt;</code> (one of 802.11a, 802.11b, or 802.11b/g). <code>&lt;basic&gt;</code> and <code>&lt;supported&gt;</code> must be a comma separated list of rates, such as 6,9,11,15 with no spaces. Basic rates are a subset of supported rates. The different types of radio support the following rates.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;basic&gt;</code></td>
<td>A - 6</td>
</tr>
<tr>
<td></td>
<td><code>&lt;supported&gt;</code></td>
<td>B - 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>G - 1</td>
</tr>
<tr>
<td>reg</td>
<td><code>&lt;type&gt;</code></td>
<td>Sets the default regulatory parameters for radios of specified type (one of 802.11a, 802.11b, or 802.11b/g), where <code>&lt;indoor&gt;</code> is one of in or in/out; <code>&lt;ch&gt;</code> is the channel to use, and <code>&lt;pwr&gt;</code> is the power (in dB from 4 to 20). Select the value of <code>&lt;ch&gt;</code> from the appropriate list.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;indoor&gt;</code></td>
<td>802.11b ch -- 1 to 14</td>
</tr>
<tr>
<td></td>
<td><code>&lt;ch&gt;</code></td>
<td>802.11a ch -- 36,40,44,48,52,56,60,64,149,153,157,161</td>
</tr>
<tr>
<td></td>
<td><code>&lt;pwr&gt;</code></td>
<td>Note: Regulatory parameter values depend on the country of operation and radio type. Refer to the documentation for specific regulatory information.</td>
</tr>
<tr>
<td>rts</td>
<td><code>&lt;type&gt;</code></td>
<td>Sets the default RTS threshold for radios of specified <code>&lt;type&gt;</code> (one of 802.11a, 802.11b, or 802.11b/g) to <code>&lt;bytes&gt;</code> (e.g., 2341).</td>
</tr>
<tr>
<td>short-pre</td>
<td><code>&lt;type&gt;</code></td>
<td>By default, enables or disables the short preamble mode for radios of specified <code>&lt;type&gt;</code> (one of 802.11a, 802.11b, or 802.11b/g).</td>
</tr>
</tbody>
</table>
Example:

```
admin(network.ap.default)>set ch_mode 802.11a fixed
admin(network.ap.default)>set dtim 802.11a 10
admin(network.ap.default)>set short 802.11b/g enable
admin(network.ap.default)>show default 802.11a
```

```
ap indoor use : indoor/outdoor
ap channel : 149
ap channel mode : fixed
ap radio power : 4 dB
power to antenna : 3 mW

ap diversity : full

basic rates : 6
supported rates : 6 9 12 18 24 36 48 54

rts threshold : 2341
beacon interval : 100
dtim period : 10
short preamble : disable
security beacon (hide ess) : disable
primary wlan index : wlan1
```

Related Commands:

- `show default` Displays the default AP settings for a particular radio type.
WS2000>admin(network.ap.default)> show

Description:
Shows the default Access Port parameters for a particular radio type.

Syntax:
show default  Shows the default Access Port parameters.

Example:
admin(network.ap.default)>set ch_mode 802.11a fixed
admin(network.ap.default)>set dtim 802.11a 10
admin(network.ap.default)>set short 802.11b/g enable
admin(network.ap.default)>show default 802.11a

ap indoor use : indoor/outdoor
ap channel : 149
ap channel mode : fixed
ap radio power : 4 dB
power to antenna : 3 mW

ap diversity : full

basic rates : 6
supported rates : 6 9 12 18 24 36 48 54

rts threshold : 2341
beacon interval : 100
dtim period : 10
short preamble : disable
security beacon (hide ess) : disable
primary wlan index : wlan1

Related Commands:
set Sets the default parameters for the specified radio type.
13.5 Network AP Test Commands

WS2000>admin(network.ap)> test

Description:

Displays the test submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>new</td>
<td>Switches the Access Port to a new channel.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(network.ap.test)> new

**Description:**

Switches the specified Access Port to a new channel.

**Syntax:**

```
new <idx> <ch>  Switches the Access Port indexed with <idx> (1–12) to channel <ch> (which must be a valid channel for the specified Access Port).
```

**Example:**

```
admin(network.ap.test)>new 2 15
admin(network.ap.test)>
```
13.6 Network DCHP Commands

WS2000>admin(network)> dhcp

Description:

Displays the DHCP submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets system updated flags.</td>
</tr>
<tr>
<td>show</td>
<td>Shows system updated flags.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(network.dhcp)> set

Description:
Sets parameters for automated firmware and configuration upgrades.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>firmwareupgrade 1 / 0</td>
<td>Enables (1) or disables (0) automatic switch firmware upgrade.</td>
</tr>
<tr>
<td>configupgrade 1 / 0</td>
<td>Enables (1) or disables (0) automatic switch configuration update.</td>
</tr>
<tr>
<td>interface &lt;int&gt;</td>
<td>Sets the interface for the upgrades to &lt;int&gt;:</td>
</tr>
<tr>
<td>s1</td>
<td>subnet 1</td>
</tr>
<tr>
<td>s2</td>
<td>subnet 2</td>
</tr>
<tr>
<td>s3</td>
<td>subnet 3</td>
</tr>
<tr>
<td>s4</td>
<td>subnet 4</td>
</tr>
<tr>
<td>w</td>
<td>WAN</td>
</tr>
</tbody>
</table>

Example:

admin(network.dhcp)> show all

Auto Firmware upgrade flag : 0
Auto Config upgrade flag    : 0
Interface                   : w

admin(network.dhcp)> set firmwareupgrade 1
admin(network.dhcp)> set con 1
admin(network.dhcp)> set inter s1
admin(network.dhcp)> show all

Auto Firmware upgrade flag : 1
Auto Config upgrade flag   : 1
Interface                   : s1

Related Commands:

show all               Shows the settings for all the automatic update parameters.
WS2000>admin(network.dhcp)> show

Description:
Displays system updated flags.

Syntax:
show all Displays all of the DHCP-related system update parameters.

Example:
admin(network.dhcp)>show all

Auto Firmware upgrade flag : 0
Auto Config upgrade flag : 0
Interface : w

Related Commands:
set Sets the DHCP-related parameters for updating system firmware and configuration.
13.7 Network Firewall Commands

WS2000>admin(network)> fw

Description:

Displays the firewall submenu. The items available under this command are shown below.

- **set**  Sets firewall parameters.
- **show** Shows firewall parameters.
- **submap** Goes to the subnet mapping submenu.
- **policy** Goes to the advanced subnet mapping submenu.
- **save** Saves the configuration to system flash.
- **quit** Quits the CLI.
- **..** Goes to the parent menu.
- **/** Goes to the root menu.

The commands in this menu are available in the Web interface on the Network>Firewall screen.
WS2000>admin(network.fw)> set

Description:
Sets firewall parameters. In the Web interface, this functionality is provided by the Network->Firewall screen.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set mode</td>
<td>Enables or disables the firewall.</td>
</tr>
<tr>
<td>override</td>
<td>Enables or disables subnet access override.</td>
</tr>
<tr>
<td>ftp</td>
<td>Enables or disables FTP bounce attack check.</td>
</tr>
<tr>
<td>ip</td>
<td>Enables or disables IP unaligned timestamp check.</td>
</tr>
<tr>
<td>mime</td>
<td>Enables or disables MIME flood attack check.</td>
</tr>
<tr>
<td>filter</td>
<td>Enables or disables MIME flood attack check.</td>
</tr>
<tr>
<td>hdr</td>
<td>Sets the max number of headers as specified in &lt;count&gt; (with value in range 12–34463).</td>
</tr>
<tr>
<td>len</td>
<td>Sets the max header length in bytes as specified by &lt;length&gt; (with value in range 256–34463).</td>
</tr>
<tr>
<td>seq</td>
<td>Enables or disables sequence number prediction check.</td>
</tr>
<tr>
<td>src</td>
<td>Enables or disables source routing check.</td>
</tr>
<tr>
<td>syn</td>
<td>Enables or disables SYN flood attack check.</td>
</tr>
<tr>
<td>timeout</td>
<td>Sets the firewall timeout to &lt;time&gt; minutes (1–90).</td>
</tr>
<tr>
<td>win</td>
<td>Enables or disables Winnuke attack check.</td>
</tr>
</tbody>
</table>

Example:

admin(network.fw)> set mode enable
admin(network.fw)> set override disable
admin(network.fw)> set ftp enable
admin(network.fw)> set mime hdr 3000
admin(network.fw)> show all

Firewall Status : enable
Subnet Access Override : disable

Configurable Firewall Filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp bounce attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>syn flood attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>unaligned ip timestamp filter</td>
<td>enable</td>
</tr>
<tr>
<td>source routing attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>winnuke attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>seq num prediction attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>mime flood attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>max mime header length</td>
<td>34463</td>
</tr>
<tr>
<td>max mime headers</td>
<td>3000</td>
</tr>
</tbody>
</table>

Always On Firewall Filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout</td>
<td>60</td>
</tr>
<tr>
<td>win</td>
<td>enable</td>
</tr>
</tbody>
</table>
ip spoofing attack filter : enable
land attack filter : enable
ping of death attack filter : enable
reassembly attack filter : enable

Related Commands:

show Show the current firewall settings.
WS2000>admin(network.fw)> show

**Description:**
Displays the firewall parameters.

**Syntax:**

```
show all
```

**Example:**

```plaintext
admin(network.fw)> show all

Firewall Status : enable
Subnet Access Override : disable

Configurable Firewall Filters

<table>
<thead>
<tr>
<th>Filter</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp bounce attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>syn flood attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>unaligned ip timestamp filter</td>
<td>enable</td>
</tr>
<tr>
<td>source routing attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>winnuke attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>seq num prediction attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>mime flood attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>max mime header length</td>
<td>34463</td>
</tr>
<tr>
<td>max mime headers</td>
<td>3000</td>
</tr>
</tbody>
</table>

Always On Firewall Filters

```plaintext
<table>
<thead>
<tr>
<th>Filter</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip spoofing attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>land attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>ping of death attack filter</td>
<td>enable</td>
</tr>
<tr>
<td>reassembly attack filter</td>
<td>enable</td>
</tr>
</tbody>
</table>
```

admin(network.fw)>}

**Related Commands:**

```
set
```

Sets firewall settings.
13.8 Network Firewall Policy Commands

WS2000>admin(network.fw)> policy

Description:

Displays the firewall policy submenu. The items available under this command are shown below.

- **inbound**: Goes to the inbound policy submenu.
- **outbound**: Goes to the outbound policy submenu.
- **import**: Imports subnet access rules.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
WS2000>admin(network.fw.policy)> import

Description:

Imports subnet access rules from current subnet access settings created in the GUI interface (Network-> Firewall -> Subnet Access menu item) or using the CLI submap menu commands. Previously set outbound firewall policies will be deleted.

Syntax:

import   Imports subnet access rules into the outbound policy list.

Example:

admin(network.fw.policy)>import
WARNING: You will lose all your current advanced access policies.
Do you want to continue [n/y]?y
admin(network.fw.policy)>
admin(network.fw.policy.outb)>list

<table>
<thead>
<tr>
<th>Idx</th>
<th>Src IP-Netmask</th>
<th>Dst IP-Netmask</th>
<th>Tp</th>
<th>Src Ports</th>
<th>Dst Ports</th>
<th>NAT</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.0.1-255.255.255.0</td>
<td>192.168.1.1-255.255.255.0</td>
<td>all</td>
<td>1:65535</td>
<td>1:65535</td>
<td>none</td>
<td>allow</td>
</tr>
<tr>
<td>2</td>
<td>192.168.0.1-255.255.255.0</td>
<td>192.168.2.1-255.255.255.0</td>
<td>all</td>
<td>1:65535</td>
<td>1:65535</td>
<td>none</td>
<td>allow</td>
</tr>
<tr>
<td>3</td>
<td>192.168.1.1-255.255.255.0</td>
<td>192.168.0.1-255.255.255.0</td>
<td>all</td>
<td>1:65535</td>
<td>1:65535</td>
<td>none</td>
<td>allow</td>
</tr>
<tr>
<td>4</td>
<td>192.168.1.1-255.255.255.0</td>
<td>192.168.2.1-255.255.255.0</td>
<td>all</td>
<td>1:65535</td>
<td>1:65535</td>
<td>none</td>
<td>allow</td>
</tr>
<tr>
<td>5</td>
<td>192.168.2.1-255.255.255.0</td>
<td>192.168.0.1-255.255.255.0</td>
<td>all</td>
<td>1:65535</td>
<td>1:65535</td>
<td>none</td>
<td>allow</td>
</tr>
<tr>
<td>6</td>
<td>192.168.2.1-255.255.255.0</td>
<td>192.168.1.1-255.255.255.0</td>
<td>all</td>
<td>1:65535</td>
<td>1:65535</td>
<td>none</td>
<td>allow</td>
</tr>
<tr>
<td>7</td>
<td>192.168.0.0-255.255.255.0</td>
<td>192.168.32.2-255.255.255.0</td>
<td>all</td>
<td>1:65535</td>
<td>1:65535</td>
<td>none</td>
<td>allow</td>
</tr>
<tr>
<td>8</td>
<td>192.168.0.0-255.255.255.0</td>
<td>0.0.0.0-255.255.255.0</td>
<td>all</td>
<td>1:65535</td>
<td>1:65535</td>
<td>wan1</td>
<td>allow</td>
</tr>
<tr>
<td>9</td>
<td>192.168.1.0-255.255.255.0</td>
<td>0.0.0.0-255.255.255.0</td>
<td>all</td>
<td>1:65535</td>
<td>1:65535</td>
<td>none</td>
<td>allow</td>
</tr>
<tr>
<td>10</td>
<td>192.168.2.0-255.255.255.0</td>
<td>0.0.0.0-255.255.255.0</td>
<td>all</td>
<td>1:65535</td>
<td>1:65535</td>
<td>none</td>
<td>allow</td>
</tr>
</tbody>
</table>

Related Commands:

submap > list   Lists the currently defined subnet to subnet/WAN communication rules into the outbound firewall policy list.
outb > list     Lists the current outbound firewall policies.
13.9 Network Firewall Policy Inbound Commands

**WS2000>admin(network.fw.policy)> inb**

**Description:**

Displays the inbound policy submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds a firewall policy.</td>
</tr>
<tr>
<td>set</td>
<td>Sets firewall policy parameters.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a firewall policy.</td>
</tr>
<tr>
<td>list</td>
<td>Lists firewall policies.</td>
</tr>
<tr>
<td>move</td>
<td>Moves a firewall policy to a different position in the list.</td>
</tr>
<tr>
<td>insert</td>
<td>Inserts a new firewall policy before an existing policy.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(network.fw.policy.inb)> add

Description:
Adds an inbound firewall policy.

Syntax:
add <sip> <snetmask> <dip> <dnetmask>  Adds a firewall policy to be effective on communications between <sip> with <snetmask> (an IP and associated netmask) and a destination site specified by <dip> and <dnetmask>.

Example:
admin(network.fw.policy.inb)>add 192.168.24.0 255.255.255.0 209.239.170.45 255.255.255.224
Inbound Policy Successfully added at index 1
admin(network.fw.policy.inb)>list

<table>
<thead>
<tr>
<th>Idx</th>
<th>Src IP-Netmask</th>
<th>Dst IP-Netmask</th>
<th>Tp</th>
<th>SPorts</th>
<th>DPorts</th>
<th>Rev. NAT</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.24.0-</td>
<td>209.239.170.45-</td>
<td>all</td>
<td>1:</td>
<td>1:</td>
<td>0.0.0.0</td>
<td>deny</td>
</tr>
<tr>
<td></td>
<td>255.255.255.0</td>
<td>255.255.255.224</td>
<td></td>
<td>65535</td>
<td>65535</td>
<td>nat port 0</td>
<td></td>
</tr>
</tbody>
</table>

Related Commands:
delete Deletes firewall policies from the inbound list.
move Moves firewall policies either up or down in the list of policies.
WS2000>admin(network.fw.policy.inb)> delete

Description:

Deletes a firewall policy.

Syntax:

delete  <idx>  Deletes inbound firewall policy <idx> from the policy list.
all      Deletes all inbound firewall policies.

Example:

admin(network.fw.policy.inb)>list
Idx  Src IP-Netmask  Dst IP-Netmask  Tp  SPorts  DPorts  Rev.  NAT  Action
--------------------------------------------------
1    209.239.179.52- 168.192.56.4-  all  1:  1:  0.0.0.0  deny
    255.255.255.224 255.255.255.0 65535  65535  nat port 0
2    209.239.160.202- 168.192.36.4-  gre 20:21 200: 0.0.0.0  allow
    255.255.255.224 255.255.255.0 201  nat port 0
admin(network.fw.policy.inb)>del 1
admin(network.fw.policy.inb)>list
Idx  Src IP-Netmask  Dst IP-Netmask  Tp  SPorts  DPorts  Rev.  NAT  Action
--------------------------------------------------
1    209.239.160.202- 168.192.36.4-  gre 20:21 200: 0.0.0.0  allow
    255.255.255.224 255.255.255.0 201  nat port 0
WS2000>admin(network.fw.policy.inb)> insert

Description:
Inserts a new firewall policy before an existing policy.

Syntax:
insert <idx> <sip> <snetsmask> <dip> <dnetmask>  Inserts a new policy into the inbound firewall policy list at spot <idx>, with source IP address and netmask of <sip> and <snetsmask>, and destination IP address and netmask of <dip> and <dnetmask>.

Example:
admin(network.fw.policy.inb)>list

<table>
<thead>
<tr>
<th>Idx</th>
<th>Src IP-Netmask</th>
<th>Dst IP-Netmask</th>
<th>Tp</th>
<th>SPorts</th>
<th>DPorts</th>
<th>Rev. NAT</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>209.239.170.88-192.168.42.2- all 1: 1: 0.0.0.0 deny</td>
<td>255.255.255.224 255.255.255.0</td>
<td>65535 65535 nat port 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

admin(network.fw.policy.inb)>insert 1 209.239.160.44 255.255.255.224 192.168.55.44 255.255.255.0

Inbound Policy Successfully inserted at index 1

admin(network.fw.policy.inb)>list

<table>
<thead>
<tr>
<th>Idx</th>
<th>Src IP-Netmask</th>
<th>Dst IP-Netmask</th>
<th>Tp</th>
<th>SPorts</th>
<th>DPorts</th>
<th>Rev. NAT</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>209.239.160.44-192.168.55.44- all 1: 1: 0.0.0.0 deny</td>
<td>255.255.255.224 255.255.255.0</td>
<td>65535 65535 nat port 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>209.239.170.88-192.168.42.2- all 1: 1: 0.0.0.0 deny</td>
<td>255.255.255.224 255.255.255.0</td>
<td>65535 65535 nat port 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**WS2000>admin(network.fw.policy.inb)> list**

**Description:**
Lists inbound firewall policies.

**Syntax:**

```
list
<iidx> Displays firewall policy with number <iidx>.
```

**Example:**

```
admin(network.fw.policy.inb)>add 192.168.24.0 255.255.255.0 209.239.170.45 255.255.255.224
Inbound Policy Successfully added at index 1

admin(network.fw.policy.inb)>list
```

<table>
<thead>
<tr>
<th>Idx</th>
<th>Src IP-Netmask</th>
<th>Dst IP-Netmask</th>
<th>Tp</th>
<th>SPorts</th>
<th>DPorts</th>
<th>Rev. NAT</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.24.0-255.255.255.0</td>
<td>209.239.170.45-255.255.255.224</td>
<td>all</td>
<td>1:1:0.0.0.0</td>
<td>65535 65535</td>
<td>nat port 0</td>
<td>deny</td>
</tr>
</tbody>
</table>
WS2000>admin(network.fw.policy.inb)> move

Description:
Moves a firewall policy to a different position in the list and renumbers all affected items in the list.

Syntax:
move up <idx>  Moves policy <idx> up one (to a lower number) in the policy list.
down <idx>  Moves policy <idx> down one (to a higher number) in the policy list.

Example:

admin(network.fw.policy.inb)>list
Idx Src IP-Netmask Dst IP-Netmask Tp SPorts DPorts Rev. NAT Action
-----------------------------------------------------------------------------------
1  209.239.160.202- 168.192.36.4- gre 20:21 200: 0.0.0.0 allow
   255.255.255.224 255.255.255.0 201 nat port 0
2  209.239.179.52- 168.192.56.4- all 1: 1: 0.0.0.0 deny
   255.255.255.224 255.255.255.0 65535 65535 nat port 0
admin(network.fw.policy.inb)>move up 2
admin(network.fw.policy.inb)>list
-----------------------------------------------------------------------------------
Idx Src IP-Netmask Dst IP-Netmask Tp SPorts DPorts Rev. NAT Action
-----------------------------------------------------------------------------------
1  209.239.179.52- 168.192.56.4- all 1: 1: 0.0.0.0 deny
   255.255.255.224 255.255.255.0 65535 65535 nat port 0
2  209.239.160.202- 168.192.36.4- gre 20:21 200: 0.0.0.0 allow
   255.255.255.224 255.255.255.0 201 nat port 0
**WS2000>admin(network.fw.policy.inb)> set**

**Description:**
Sets inbound firewall policy parameters.

**Syntax:**

- `set saddr <idx> <Ip Addr> <netmask>`: Sets source IP address and IP netmask for inbound firewall policy `<idx>`.
- `set daddr <idx> <Ip Addr> <netmask>`: Sets destination IP address and IP netmask for inbound firewall policy `<idx>`.
- `tp <idx> <tp>`: Sets transport protocol for inbound firewall policy `<idx>` to `<tp>` (one of `all, tcp, udp, icmp, ah, esp, gre`).
- `sport <idx> <port1> [<port2>]`: Sets source port range for inbound firewall policy `<idx>` from `<port1>` (1–65535) to `<port2>`. If `<port2>` is not specified, `<port1>` is used as the top end of the range.
- `dport <idx> <port1> [<port2>]`: Sets destination port range for inbound firewall policy `<idx>` from `<port1>` (1–65535) to `<port2>`. If `<port2>` is not specified, `<port1>` is used as the top end of the range.
- `rnat <idx> <Ip Addr>`: Sets reverse NAT IP address for inbound firewall policy `<idx>` to `<Ip Addr>` (a.b.c.d).
- `rport <idx> <rport>`: Sets reverse NAT port for inbound firewall policy `<idx>` to `<rport>` (0–65535).
- `action <idx> allow/deny`: Sets action of inbound firewall policy `<idx>` to allow or deny.

**Example:**

```
admin(network.fw.policy.inb)>set tp 1 gre
admin(network.fw.policy.inb)>list

Idx  Src IP-Netmask  Dst IP-Netmask  Tp  SPorts  DPorts  Rev. NAT  Action
---------------------------------------------------------------------------------------------
 1  209.239.160.202- 168.192.36.4- gre 1: 1: 0.0.0.0  deny
       255.255.255.224  255.255.255.0  65535  65535  nat port 0
```

```
admin(network.fw.policy.inb)>set sport 1 20 21
admin(network.fw.policy.inb)>set dport 1 200 201
admin(network.fw.policy.inb)>set action 1 allow
admin(network.fw.policy.inb)>list

Idx  Src IP-Netmask  Dst IP-Netmask  Tp  SPorts  DPorts  Rev. NAT  Action
---------------------------------------------------------------------------------------------
 1  209.239.160.202- 168.192.36.4- gre 20:21 200: 0.0.0.0  allow
       255.255.255.224  255.255.255.0  201  nat port 0
```
13.10 Network Firewall Policy Outbound Commands

WS2000>admin(network.fw.policy)> outb

Description:
Displays the outbound policy submenu. The items available under this command are shown below.

- **add**: Adds a firewall policy.
- **set**: Sets firewall policy parameters.
- **delete**: Deletes a firewall policy.
- **list**: Lists firewall policies.
- **move**: Moves a firewall policy to a different position in the list.
- **insert**: Inserts a new firewall policy before an existing policy.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
WS2000>admin(network.fw.policy.outb)> add

**Description:**

Adds an outbound firewall policy.

**Syntax:**

`add <sip> <snetmask> <dip> <dnetmask>`

Adds an outbound firewall policy to be effective on communications between
<sip> with <snetmask> (an IP and associated netmask) and a destination site
specified by <dip> and <dnetmask>.

**Example:**

    admin(network.fw.policy.outb)>add 192.168.24.0 255.255.255.0 209.239.170.45
    255.255.255.224

    Outbound Policy Successfully added at index 1
    admin(network.fw.policy.outb)>list

<table>
<thead>
<tr>
<th></th>
<th>Src IP-Netmask</th>
<th>Dst IP-Netmask</th>
<th>Tp</th>
<th>SPorts</th>
<th>DPorts</th>
<th>Rev. NAT</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.24.0-</td>
<td>209.239.170.45-</td>
<td>all</td>
<td>1:</td>
<td>1:</td>
<td>0.0.0.0</td>
<td>deny</td>
</tr>
<tr>
<td></td>
<td>255.255.255.0</td>
<td>255.255.255.224</td>
<td></td>
<td>65535</td>
<td>65535</td>
<td>nat port 0</td>
<td></td>
</tr>
</tbody>
</table>

**Related Commands:**

- **delete**
  - Deletes firewall policies from the outbound list.

- **move**
  - Moves policies either up or down in the list of policies.
WS2000>admin(network.fw.policy.outb)> delete

**Description:**

Deletes an outbound firewall policy.

**Syntax:**

```
delete <idx>       Deletes outbound firewall policy <idx> from the policy list.
  all             Deletes all outbound firewall policies.
```

**Example:**

```
admin(network.fw.policy.outb)>list
---------------------------------------------------------------------
Idx  Src IP-Netmask  Dst IP-Netmask  Tp  SPorts  DPorts  Rev. NAT  Action
---------------------------------------------------------------------
 1   209.239.179.52- 168.192.56.4-  all 1: 0.0.0.0  deny
      255.255.255.224  255.255.255.0  65535  65535 nat port 0
 2   209.239.160.202- 168.192.36.4-  gre 20:21 200: 0.0.0.0  allow
      255.255.255.224  255.255.255.0  201 nat port 0
```

```
admin(network.fw.policy.outb)>del 1
admin(network.fw.policy.outb)>list
---------------------------------------------------------------------
Idx  Src IP-Netmask  Dst IP-Netmask  Tp  SPorts  DPorts  Rev. NAT  Action
---------------------------------------------------------------------
 1   209.239.160.202- 168.192.36.4-  gre 20:21 200: 0.0.0.0  allow
      255.255.255.224  255.255.255.0  201 nat port 0
```
WS2000>admin(network.fw.policy.outb)> insert

Description:
Inserts a new outbound firewall policy before an existing policy.

Syntax:
insert <idx> <sip> <snetmask> <dip> <dnetmask> Inserts a new policy into the outbound firewall policy list at spot
<idx>, with source IP address and netmask of <sip> and <snetmask>,
and destination IP address and netmask of <dip> and <dnetmask>.

Example:

admin(network.fw.policy.outb)>list
---------------------------------------------------------------------
Idx Src IP-Netmask Dst IP-Netmask Tp SPorts DPorts Rev. NAT Action
---------------------------------------------------------------------
1 209.239.170.88- 192.168.42.2- all 1: 1: 0.0.0.0 deny
255.255.255.224 255.255.255.0 65535 65535 nat port 0

admin(network.fw.policy.outb)>insert 1 209.239.160.44 255.255.255.224 192.168.55.
44 255.255.255.0
Outbound Policy Successfully inserted at index 1

admin(network.fw.policy.outb)>list
---------------------------------------------------------------------
Idx Src IP-Netmask Dst IP-Netmask Tp SPorts DPorts Rev. NAT Action
---------------------------------------------------------------------
1 209.239.160.44- 192.168.55.44- all 1: 1: 0.0.0.0 deny
255.255.255.224 255.255.255.0 65535 65535 nat port 0
2 209.239.170.88- 192.168.42.2- all 1: 1: 0.0.0.0 deny
255.255.255.224 255.255.255.0 65535 65535 nat port 0
WS2000>admin(network.fw.policy.outb)> list

Description:

Lists outbound firewall policies.

Syntax:

list  
<idx>   

Lists all outbound firewall policies. 
Displays outbound firewall policy with number <idx>.

Example:

admin(network.fw.policy.outb)>add 192.168.24.0 255.255.255.0 209.239.170.45 255.255.224

Inbound Policy Successfully added at index 1

admin(network.fw.policy.outb)>list

------------------------------------------------------------------------------
|     |      |         |     |     |     |       |
------------------------------------------------------------------------------
| 1   | 192.168.24.0- | 209.239.170.45- | all | 1:  | 1: | 0.0.0.0 | deny |
|     | 255.255.255.0 | 255.255.255.224 |     | 65535 | 65535 | nat port 0 |
WS2000>admin(network.fw.policy.outb)> move

Description:

Moves an outbound firewall policy up or down in the policy list and renumbers the policy affected by the move.

Syntax:

**move up <idx>**  Moves a policy <idx> up one (to a lower number) in the outbound policy list.

**move down <idx>**  Moves a policy <idx> down one (to a higher number) in the outbound policy list.

Example:

```
admin(network.fw.policy.outb)> list
-----------------------------------------------------------------------------
Idx Src IP-Netmask Dst IP-Netmask Tp SPorts DPorts Rev. NAT Action          
-----------------------------------------------------------------------------
1 209.239.160.202-168.192.36.4- gre 20:21 200: 0.0.0.0  allow
   255.255.255.224 255.255.255.0          201 nat port 0
2 209.239.179.52-168.192.56.4- all 1: 1: 0.0.0.0  deny
   255.255.255.224 255.255.255.0 65535 65535 nat port 0
admin(network.fw.policy.outb)>move up 2
admin(network.fw.policy.outb)> list
-----------------------------------------------------------------------------
Idx Src IP-Netmask Dst IP-Netmask Tp SPorts DPorts Rev. NAT Action          
-----------------------------------------------------------------------------
1 209.239.179.52-168.192.56.4- all 1: 1: 0.0.0.0  deny
   255.255.255.224 255.255.255.0 65535 65535 nat port 0
2 209.239.160.202-168.192.36.4- gre 20:21 200: 0.0.0.0  allow
   255.255.255.224 255.255.255.0          201 nat port 0
```
WS2000>admin(network.fw.policy.outb)> set

Description:
Sets firewall policy parameters.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets firewall policy parameters.</td>
</tr>
<tr>
<td>saddr</td>
<td>Sets source IP address and IP netmask for outbound firewall policy &lt;idx&gt;.</td>
</tr>
<tr>
<td>daddr</td>
<td>Sets destination IP address and IP netmask for outbound firewall policy &lt;idx&gt;.</td>
</tr>
<tr>
<td>tp</td>
<td>Sets transport protocol for outbound firewall policy &lt;idx&gt; to &lt;tp&gt; (one of all, tcp, udp, icmp, ah, esp, or gre).</td>
</tr>
<tr>
<td>sport</td>
<td>Sets source port range for outbound firewall policy &lt;idx&gt; from &lt;port1&gt; (1-65535) to &lt;port2&gt;. If &lt;port2&gt; is not specified, &lt;port1&gt; is used as the top end of the range.</td>
</tr>
<tr>
<td>dport</td>
<td>Sets destination port range for outbound firewall policy &lt;idx&gt; from &lt;port1&gt; (1-65535) to &lt;port2&gt;. If &lt;port2&gt; is not specified, &lt;port1&gt; is used as the top end of the range.</td>
</tr>
<tr>
<td>nat</td>
<td>Sets NAT WAN ID for outbound firewall policy &lt;idx&gt; to &lt;wan idx&gt; (0–8), where 0 = none, 1 = WAN 1, 2 = WAN 2, etc.</td>
</tr>
<tr>
<td>action</td>
<td>Sets action of outbound firewall policy &lt;idx&gt; to allow or deny.</td>
</tr>
</tbody>
</table>

Example:

```
admin(network.fw.policy.outb)>set tp 1 gre
admin(network.fw.policy.outb)>list

Idx | Src IP-Netmask | Dst IP-Netmask | Tp | SPorts | DPorts | Rev. NAT | Action |
----|----------------|----------------|----|--------|--------|----------|--------|
1   | 209.239.160.202-168.192.36.4- | gre 1: 1: 0.0.0.0 deny | 255.255.255.224 | 255.255.255.0 | 65535 | 65535 | nat port 0 |
```

```
admin(network.fw.policy.outb)>set sport 1 20 21
admin(network.fw.policy.outb)>set dport 1 200 201
admin(network.fw.policy.outb)>set action 1 allow
admin(network.fw.policy.outb)>list

Idx | Src IP-Netmask | Dst IP-Netmask | Tp | SPorts | DPorts | Rev. NAT | Action |
----|----------------|----------------|----|--------|--------|----------|--------|
1   | 209.239.160.202-168.192.36.4- | gre 20:21 200: 0.0.0.0 allow | 255.255.255.224 | 255.255.255.0 | 201 | nat port 0 |
```
13.11 Network Firewall Submap Commands

WS2000>admin(network.fw)> submap

Description:
Displays the subnet mapping submenu. The items available under this command are shown below.

- **add**: Adds subnet access exception rules.
- **delete**: Deletes subnet access exception rules.
- **list**: Lists subnet access exception rules.
- **set**: Sets subnet access parameters.
- **show**: Shows subnet access parameters.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
**WS2000>admin(network.fw.submap)> add**

**Description:**
Adds subnet access exception rules.

**Syntax:**
```
add <from> <to> <name> <tran> <port1> <port2>  
```
Adds a subnet access exception rule for communication from `<from>` (one of `s1 = subnet1, s2 = subnet2, s3 = subnet3, s4 = subnet4`) to `<to>` (s1 = subnet1, s2 = subnet2, s3 = subnet3, s4 = subnet4, w = the WAN), that has the name `<name>` (1 to 7 characters), which denies `<tran>` (one of the following transport protocols: tcp, udp, icmp, ah, esp, gre, or all) for ports in the range `<port1>` to `<port2>`.

**Example:**
```
admin(network.fw.submap)> add s1 w test gre 21 101
admin(network.fw.submap)> list s1

<table>
<thead>
<tr>
<th>index</th>
<th>from</th>
<th>to</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>subnet1 wan</td>
<td>test</td>
<td>gre</td>
<td>21</td>
<td>101</td>
<td></td>
</tr>
</tbody>
</table>

admin(network.fw.submap)> add s1 s2 test2 ah 20 80
admin(network.fw.submap)> add s2 s3 test3 all 20 300

admin(network.fw.submap)> list s1

<table>
<thead>
<tr>
<th>index</th>
<th>from</th>
<th>to</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>subnet1 wan</td>
<td>test</td>
<td>gre</td>
<td>21</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>subnet1 subnet2 test2</td>
<td>ah</td>
<td>20</td>
<td>80</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

admin(network.fw.submap)> list s2

<table>
<thead>
<tr>
<th>index</th>
<th>from</th>
<th>to</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>subnet2 subnet3 test3</td>
<td>all</td>
<td>20</td>
<td>300</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

admin(network.fw.submap)> delete s2 all
admin(network.fw.submap)> list s2

<table>
<thead>
<tr>
<th>index</th>
<th>from</th>
<th>to</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
WS2000> admin(network.fw.submap) > delete

Description:

Deletes subnet access exception rules.

Syntax:

delete <from> <idx> Deletes access exception rule entry <idx> from <from> (one of s1 = subnet1, s2 = subnet2, s3 = subnet3, s4 = subnet4).
<from> all Deletes all access exception rule entries from <from> (s1 = subnet1, s2 = subnet2, s3 = subnet3, s4 = subnet4).

Example:

admin(network.fw.submap) > list s1

<table>
<thead>
<tr>
<th>index</th>
<th>from</th>
<th>to</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>subnet1 wan</td>
<td>test</td>
<td>gre</td>
<td>21</td>
<td>101</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>subnet1 subnet2 test2</td>
<td>ah</td>
<td>20</td>
<td>80</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

admin(network.fw.submap) > delete s1 2

admin(network.fw.submap) > list s1

<table>
<thead>
<tr>
<th>index</th>
<th>from</th>
<th>to</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>subnet1 wan</td>
<td>test</td>
<td>gre</td>
<td>21</td>
<td>101</td>
<td></td>
</tr>
</tbody>
</table>

admin(network.fw.submap) > list s2

<table>
<thead>
<tr>
<th>index</th>
<th>from</th>
<th>to</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>subnet2 subnet3 test3</td>
<td>all</td>
<td>20</td>
<td>300</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

admin(network.fw.submap) > delete s2 all

admin(network.fw.submap) > list s2

<table>
<thead>
<tr>
<th>index</th>
<th>from</th>
<th>to</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
</tr>
</thead>
</table>
WS2000>admin(network.fw.submap)> list

Description:
Lists subnet access exception rules.

Syntax:
list <from>  Lists the access exception entries for <from> (one of s1 = subnet1, s2 = subnet2, s3 = subnet3, s4 = subnet4).

Example:

```
admin(network.fw.submap)>list s1

index  from  to  name  prot  start port  end port
-------------------------------------------------------------------------------
1  subnet1 wan  test  gre  21  101

admin(network.fw.submap)>add s1 s2 test2 ah 20 80
admin(network.fw.submap)>add s2 s3 test3 all 20 300

admin(network.fw.submap)>list s1

-------------------------------------------------------------------------------
index  from  to  name  prot  start port  end port
-------------------------------------------------------------------------------
1  subnet1 wan  test  gre  21  101
2  subnet1 subnet2 test2  ah  20  80

admin(network.fw.submap)>list s2

-------------------------------------------------------------------------------
index  from  to  name  prot  start port  end port
-------------------------------------------------------------------------------
1  subnet2 subnet3 test3  all  20  300

admin(network.fw.submap)>delete s2 all

admin(network.fw.submap)>list s2

-------------------------------------------------------------------------------
index  from  to  name  prot  start port  end port
```
**Description:**

Sets a default subnet access rule to allow or deny communication.

**Syntax:**

```
set default <from> <to> deny/allow
```

Creates a default subnet access rule to deny or allow communication `<from>` one of the subnets (one of `s1` = subnet1, `s2` = subnet2, `s3` = subnet3, `s4` = subnet4) and `<to>` is a destination (one of `s1` = subnet1, `s2` = subnet2, `s3` = subnet3, `s4` = subnet4, `w` = the WAN).

**Example:**

```
admin(network.fw.submap)> set default s2 w deny

admin(network.fw.submap)> show default s1

+-----------+-----------+-----------+-----------+-----------+
|          | subnet1   | subnet2   | subnet3   | subnet4   |
|----------+-----------+-----------+-----------+-----------|
| wan      | allow     | allow     | allow     | deny      |
+-----------+-----------+-----------+-----------+-----------+

admin(network.fw.submap)>
```
WS2000>admin(network.fw.submap)> show

Description:
Displays default subnet access exception rules for indicated subnet.

Syntax:
show default <from>  Shows all default access exception rules for subnet <from> (one of s1 = subnet1, s2 = subnet2, s3 = subnet3, s4 = subnet4) to all other subnets.

Example:
admin(network.fw.submap)>set default s2 w deny

admin(network.fw.submap)>show default s1

<table>
<thead>
<tr>
<th>wan</th>
<th>subnet1</th>
<th>subnet2</th>
<th>subnet3</th>
<th>subnet4</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow</td>
<td>allow</td>
<td>allow</td>
<td>allow</td>
<td>deny</td>
</tr>
</tbody>
</table>

admin(network.fw.submap)>
13.12 Network LAN Commands

WS2000>admin(network)> lan

Description:

Displays the LAN submenu. The items available under this command are shown below.

- **dhcp**: Goes to the DHCP submenu.
- **set**: Sets LAN parameters.
- **show**: Shows LAN parameters.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
WS2000>admin(network.lan)> set

Description:
Sets the LAN parameters for the four subnets.

Syntax:

- **set ipadr** <idx> <IPaddr>
  - Sets the IP address of subnet <idx> (1–4) to the IP address <IPaddr> in the form a.b.c.d.
- **mask** <idx> <IPmask>
  - Sets the netmask of subnet <idx> (1–4) to IP address mask <IPmask> in the form a.b.c.d.
- **mode** <idx> enable/disable
  - Enables or disables the subnet identified by <idx> (1–4).
- **name** <idx> <name>
  - Sets the name of the subnet to <name> (can be up to 7 characters).
- **port** <port#> <subnet>
  - Assigns port <port#>(1–6) to the subnet indicated by (s1, s2, s3, s4). Unassigns a port with <subnet> = none.
- **wlan** <wlan#> <subnet>
  - Assigns WLAN number <wlan#> to the subnet indicated by (s1, s2, s3, s4). Unassigns a WLAN with <subnet> = none.

Example:

```
admin(network.lan)>show lan 1

subnet name : Subnet1
subnet interface : enable
ip address : 192.168.0.1
network mask : 255.255.255.0
ports : port1 port2 port3 port4 port5 port6
wlan : wlan1

admin(network.lan)>set name 1 newName
admin(network.lan)>set port 4 none
admin(network.lan)>set wlan 2 s1
admin(network.lan)>show lan 1

subnet name : NewName
subnet interface : enable
ip address : 192.168.0.1
network mask : 255.255.255.0
ports : port1 port2 port3 port5 port6
wlan : wlan1 wlan2

admin(network.lan)>
```

Related Commands:

- **show lan**  Shows the current settings for the specified subnet (LAN).
**WS2000>admin(network.lan)> show**

**Description:**
SHOWS THE LAN PARAMETERS.

**Syntax:**

`show lan <idx>` SHOWS THE SETTINGS FOR THE SUBNET <idx> (1–4).

**Example:**

```
admin(network.lan)>show lan 1

subnet name : Subnet1
subnet interface : enable
ip address : 192.168.0.1
network mask : 255.255.255.0
ports : port1 port2 port3 port4 port5 port6
wlans : wlan1
```

```
admin(network.lan)>set name 1 NewName
admin(network.lan)>set port 4 none
admin(network.lan)>set wlan 2 s1
admin(network.lan)>show lan 1

subnet name : NewName
subnet interface : enable
ip address : 192.168.0.1
network mask : 255.255.255.0
ports : port1 port2 port3 port5 port6
wlans : wlan1 wlan2
```

```
admin(network.lan)>`
```
13.13 Network LAN DHCP Commands

WS2000>admin(network.lan)> dhcp

Description:
Displays the DHCP submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds static DHCP address assignments.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes static DHCP address assignments.</td>
</tr>
<tr>
<td>list</td>
<td>Lists static DHCP address assignments.</td>
</tr>
<tr>
<td>set</td>
<td>Sets DHCP parameters.</td>
</tr>
<tr>
<td>show</td>
<td>Shows DHCP parameters.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(network.lan.dhcp)> add

Description:

Adds static DHCP address assignments.

Syntax:

add <idx> <mac> <ip> Adds a static DHCP address assignment for subnet <idx> where the device with the MAC address <mac> (00A0F8F01234) assigned to the IP address <ip>.

Example:

```
admin(network.lan.dhcp)>add 1 00A0F8F01234 192.160.24.6
admin(network.lan.dhcp)>add 1 00A1F1F24321 192.169.24.7
admin(network.lan.dhcp)>list 1

------------------------------------------------------------------------------
index   mac address     ip address
------------------------------------------------------------------------------
1       00A0F8F01234    192.160.24.6
2       00A1F1F24321    192.169.24.7

admin(network.lan.dhcp)>```

WS2000>admin(network.lan.dhcp)> delete

Description:

Deletes static DHCP address assignments.

Syntax:

```
delete <idx> <entry> Deletes the static DHCP address entry <entry> for subnet <idx>.
<idx> all Deletes all static DHCP addresses for subnet <idx>.
```

Example:

```
admin(network.lan.dhcp)>list 1

<table>
<thead>
<tr>
<th>index</th>
<th>mac address</th>
<th>ip address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

admin(network.lan.dhcp)>add 1 0011223344FF 191.168.0.42
admin(network.lan.dhcp)>add 1 4433221100AA 191.168.0.43
admin(network.lan.dhcp)>list 1

<table>
<thead>
<tr>
<th>index</th>
<th>mac address</th>
<th>ip address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0011223344FF</td>
<td>191.168.0.42</td>
</tr>
<tr>
<td>2</td>
<td>4433221100AA</td>
<td>191.168.0.43</td>
</tr>
</tbody>
</table>

admin(network.lan.dhcp)>delete 1 1
admin(network.lan.dhcp)>list 1

<table>
<thead>
<tr>
<th>index</th>
<th>mac address</th>
<th>ip address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
WS2000>admin(network.lan.dhcp)> list

Description:
Lists static DHCP address assignments.

Syntax:
list <idx>  Lists the static DHCP address assignments for subnet <idx> (1–4).

Example:

admin(network.lan.dhcp)>add 1 00A0F8F01234 192.168.63.5
admin(network.lan.dhcp)>list 1

index mac address ip address
1 00A0F8F01234 192.168.63.5

admin(network.lan.dhcp)>add 1 12332244AABB 192.168.64.3
admin(network.lan.dhcp)>list 1

index mac address ip address
1 00A0F8F01234 192.168.63.5
2 12332244AABB 192.168.64.3
WS2000>admin(network.lan.dhcp)> set

Description:
Sets DHCP parameters for the subnets.

Syntax:

```
set   <idx>   <ip>       Sets the default gateway for subnet <idx> (1–4) to the IP address <ip>.
dns   <idx>   1  <ip>    Sets the 1 = primary or 2 = secondary DNS server for subnet <idx> (1–4) to the IP address <ip>.
      2                  
wins  <idx>   <ip>       Sets the WINS server for subnet <idx> (1–4) to the IP address <ip>.
lease <idx>   <lease>    Sets the DHCP lease time for subnet <idx> (1–4) to <lease> seconds (1–999999).
domain <idx>  <dname>    Sets the domain name for subnet <idx> (1–4) to the domain name <dname> (1 to 63 characters).
mode   <idx>   none     Sets the DHCP mode for subnet <idx> (1–4) to:
        client   -- enables the subnet to be a DHCP client
        server   -- enables the subnet to be a DHCP server
range <idx>   <ip1>   <ip2>  Sets the DHCP assignment range for subnet <idx> (1–4) from IP address <ip1> to another IP address <ip2>.
```

Example:

```
admin(network.lan.dhcp)>set dns 1 1 209.160.0.18
admin(network.lan.dhcp)>set dns 1 2 209.160.0.218
admin(network.lan.dhcp)>show dhcp 1
  dhcp mode     : server
  default gateway : 192.168.0.1
  primary dns server : 209.160.0.18
  secondary dns server : 209.160.0.218
  wins server      : 192.168.0.254
  starting ip address : 192.168.0.11
  ending ip address : 192.168.0.254
  lease time       : 10000
  domain name      :
admin(network.lan.dhcp)>set domain 1 BigFishCo
admin(network.lan.dhcp)>show dhcp 1
  dhcp mode     : server
  default gateway : 192.168.0.1
  primary dns server : 209.160.0.18
  secondary dns server : 209.160.0.218
  wins server      : 192.168.0.254
  starting ip address : 192.168.0.11
  ending ip address : 192.168.0.254
  lease time       : 10000
  domain name      : BigFishCo
admin(network.lan.dhcp)>
```
WS2000>admin(network.lan.dhcp)> show

Description:
Shows DHCP parameter settings for specified subnets.

Syntax:

`show dhcp <idx>`  Show the DHCP parameter settings for subnet <idx> (1–4). These parameters are set with the `set` command.

Example:

```
admin(network.lan.dhcp)>set dns 1 1 209.160.0.18
admin(network.lan.dhcp)>set dns 1 2 209.160.0.218
admin(network.lan.dhcp)>show dhcp 1

dhcp mode : server
default gateway : 192.168.0.1
primary dns server : 209.160.0.18
secondary dns server : 209.160.0.218
wins server : 192.168.0.254
starting ip address : 192.168.0.11
ending ip address : 192.168.0.254
lease time : 10000
domain name :

admin(network.lan.dhcp)>set domain 1 BigFishCo

admin(network.lan.dhcp)>show dhcp 1

dhcp mode : server
default gateway : 192.168.0.1
primary dns server : 209.160.0.18
secondary dns server : 209.160.0.218
wins server : 192.168.0.254
starting ip address : 192.168.0.11
ending ip address : 192.168.0.254
lease time : 10000
domain name : BigFishCo

admin(network.lan.dhcp)>`
13.14 Network QoS Commands

WS2000>admin(network)> qos

Description:
Displays the quality of service (QoS) submenu. The items available under this command are shown below.

- **set**: Sets QoS parameters.
- **show**: Shows QoS parameters.
- **clear**: Clears QoS parameters.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- `..`: Goes to the parent menu.
- `/`: Goes to the root menu.
WS2000>admin(network.qos)> clear

Description:
Clears QoS radio statistics.

Syntax:

```
clear        queuing        Clears the radio QoS queuing statistics.
```

Example:
```
admin(network.qos)> clear queue
```

Related Commands:
```
set          Shows the QoS parameters and the QoS queuing statistics.
show
```
WS2000>admin(network.qos)> set

Description:
Sets QoS parameters.

Syntax:

```
set bw-share mode none / static / weighted
weight <idx> <weight>
```

Set bandwidth share mode to one of none, static, or weighted.

Set the weight for WLAN <idx> (1–4) to <weight> (1–10). A weight can only be set if the mode is set to weighted.

Example:

```
admin(network.qos)>set bw-share mode weighted
admin(network.qos)>set bw weight 1 4
admin(network.qos)>
```

Related Commands:

```
show
clear
```

Shows the bandwidth settings and the queuing statistics.

Clears the queuing statistics.
WS2000>admin(network.qos)> show

Description:

Shows QoS parameters and queuing statistics.

Syntax:

    show bw-share <idx>
    queuing <idx>

    Shows the bandwidth sharing settings.
    Displays the radio QoS queuing statistics.

Example:

    admin(network.qos)>show bw
    BW Share Mode:static

    admin(network.qos)>show qu 1
    BW Share Mode:static

    +-----------------+-------+-------+-------+
    | Priority | In   | Out   | Dropped |
    +-----------------+-------+-------+-------+
    | 0            | 0     | 0     | 0      |
    | 1            | 0     | 0     | 0      |
    | 2            | 0     | 0     | 0      |

    admin(network.qos)> 

Related Commands:

    set
    clear

    Sets the QoS parameters.
    Clears the QoS queuing statistics.
13.15 Network Router Commands

WS2000>admin(network)> router

Description:
Displays the router submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds user-defined routes.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes user-defined routes.</td>
</tr>
<tr>
<td>list</td>
<td>Lists user-defined routes.</td>
</tr>
<tr>
<td>set</td>
<td>Sets RIP parameters.</td>
</tr>
<tr>
<td>show</td>
<td>Shows routes/RIP parameters.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000> admin(network.router)> add

Description:

Adds user-defined routes.

Syntax:

`add` `<dest>` `<netmask>` `<gw>` `<iface>` `<metric>` Adds a route with destination IP address `<dest>`, IP netmask `<netmask>`, gateway IP address `<gw>`, interface subnet or WAN set to `<iface>` (one of `s1` = subnet1, `s2` = subnet2, `s3` = subnet3, `s4` = subnet4, or `w` = WAN), and metric set to `<metric>` (1-15).

Example:

```
admin(network.router)> add 202.57.42.6 255.255.255.224 202.57.42.1 s2 3
admin(network.router)> list
------------------------------------------------------------------
index  destination  netmask  gateway  interface  metric
------------------------------------------------------------------
 1  202.57.42.6  255.255.255.224  202.57.42.1  subnet2  3

admin(network.router)> add 234.44.33.212 255.255.255.234 234.44.33.2 s3 5
admin(network.router)> list
------------------------------------------------------------------
index  destination  netmask  gateway  interface  metric
------------------------------------------------------------------
 1  202.57.42.6  255.255.255.224  202.57.42.1  subnet2  3
 2  234.44.33.212  255.255.255.234  234.44.33.2  subnet3  5
```
WS2000>admin(network.router)> delete

Description:

Deletes user-defined routes.

Syntax:

delete  <idx> Deletes the user-defined route <idx> (1–20) from the list.
all       Deletes all user-defined routes.

Example:

admin(network.router)> list
------------------------------------------------------------------
index destination netmask gateway interface metric
------------------------------------------------------------------
1  202.57.42.6  255.255.255.224  202.57.42.1  subnet2  3
2  234.44.33.212  255.255.255.234  234.44.33.2  subnet3  5
admin(network.router)> delete 2
admin(network.router)> list
------------------------------------------------------------------
index destination netmask gateway interface metric
------------------------------------------------------------------
1  202.57.42.6  255.255.255.224  202.57.42.1  subnet2  3
WS2000> admin(network.router)> list

Description:

Lists user-defined routes.

Syntax:

list

Displays a list of user-defined routes.

Example:

admin(network.router)> add 234.44.33.212 255.255.255.234 234.44.33.2 s3 5
admin(network.router)> list

-------------------------------------------------------------------------------
index destination netmask gateway interface metric
-------------------------------------------------------------------------------
 1 202.57.42.6 255.255.255.224 202.57.42.1 subnet2 3
 2 234.44.33.212 255.255.255.234 234.44.33.2 subnet3 5
-------------------------------------------------------------------------------
**WS2000>admin(network.router)> set**

**Description:**
Sets routing information protocol (RIP) parameters.

**Syntax:**

- `set auth <auth>` Sets RIP authentication type to `<auth>` (one of `none`, `simple`, or `md5`).
- `set dir <dir>` Sets RIP direction to `<dir>` (one of `rx` = receive, `tx` = transmit, or both).
- `set id <idx> <keyid>` Sets MD5 authentication ID for key `<idx>` (1–2) to the MD5 `<keyid>` (1–256).
- `set key <idx> <key>` Sets the MD5 authentication ID for key `<idx>` (1–2) to MD5 key `<key>` (1 to 16 characters).
- `set passwd <passwd>` Sets password for simple authentication to `<passwd>` (1 to 16 characters).
- `set type <type>` Sets RIP type to `<type>` (one of `off`, `ripv1`, `ripv2`, or `ripv1v2`).

**Example:**

```plaintext
admin(network.router)>set auth md5
admin(network.router)>set key 1 12345678
admin(network.router)>set key 2 87654321
admin(network.router)>show rip

rip type : off
rip direction : both
rip authentication type : md5
rip simple auth password : ********
rip md5 id 1 : 1
rip md5 key 1 : ********
rip md5 id 2 : 1
rip md5 key 2 : ********
```

**Warning:** Having RIP enabled compromises your Subnet to Subnet firewall.

```plaintext
admin(network.router)>set type ripv1
admin(network.router)>show rip

rip type : ripv1
rip direction : both
rip authentication type : md5
rip simple auth password : ********
rip md5 id 1 : 1
rip md5 key 1 : ********
rip md5 id 2 : 1
rip md5 key 2 : ********
```
WS2000>admin(network.router)> show

Description:

Shows connected routes and routing information protocol (RIP) parameters.

Syntax:

show rip routes

  Shows RIP parameters.
  Shows connected routes.

Example:

admin(network.router)> show rip
rip type : off
rip direction : both
rip authentication type : md5
rip simple auth password : ********
rip md5 id 1 : 1
rip md5 key 1 : ********
rip md5 id 2 : 1
rip md5 key 2 : ********
admin(network.router)> show routes

<table>
<thead>
<tr>
<th>index</th>
<th>destination</th>
<th>netmask</th>
<th>gateway</th>
<th>interface</th>
<th>metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.2.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>subnet3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>192.168.1.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>subnet2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>192.168.0.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>subnet1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>192.168.24.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>wan</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.24.1</td>
<td>wan</td>
<td>0</td>
</tr>
</tbody>
</table>
13.16 Network VLAN Commands

WS2000>admin(network)> vlan

Description:
Displays the VLAN submenu. The items available under this command are shown below.

- **trunk**: Goes to the trunk submenu.
- **set**: Sets VLAN parameters.
- **show**: Shows VLAN parameters.
- **save**: Saves the configuration to system flash.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
WS2000>admin(network.vlan)> set

Description:
Sets VLAN parameters.

Syntax:

```
set assign-mode user / port
set default <vlan-id>
set vlan-id s1 / s2 / s3 / s4
```

Assigns the VLAN assignment mode to one of **user** or **port**.

Assigns the default VLAN ID to `<vlan-id>`, which is a number between 1 and 4094.

Sets the VLAN ID for subnet (one of s1, s2, s3, or s4) to `<vlan-id>` (1–4094).

Example:
```
admin(network.vlan)> set assign-mode user
admin(network.vlan)> set default 3
admin(network.vlan)> show vlan 3
```

```
VLAN assignment mode : user
VLAN ID : 3
VLAN Mapped Subnet : Subnet3
Default VLAN ID : Yes
```

Related Commands:

```
show
```
Displays the VLAN settings.
WS2000>admin(network.vlan)> show

Description:

Shows VLAN parameters.

Syntax:

show vlan <id> Displays the VLAN settings for the VLAN specified by <id> (1–4094).

Example:

admin(network.vlan)>show vlan 3

VLAN assignment mode : user
VLAN ID : 3
VLAN Mapped Subnet : Subnet3
Default VLAN ID : Yes

admin(network.vlan)>show vlan 2

VLAN assignment mode : user
VLAN ID : 2
VLAN Mapped Subnet : Subnet1
Default VLAN ID : No

Related Commands:

set Sets the VLAN parameters.
13.17 Network VLAN Trunk Commands

**WS2000>admin(network.vlan)> trunk**

**Description:**
Displays the trunk submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets trunk parameters.</td>
</tr>
<tr>
<td>show</td>
<td>Shows trunk parameters.</td>
</tr>
<tr>
<td>clear</td>
<td>Clears options.</td>
</tr>
<tr>
<td>.</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
**WS2000>admin(network.vlan.trunk)> clear**

**Description:**
Clears VLANs that are trunked.

**Syntax:**

```
clear trunked
```
Clears all the VLANs that are being trunked.

**Example:**

```
admin(network.vlan.trunk)> clear trunked
```

**Related Commands:**

- **set**  Sets the VLAN trunking parameters.
- **show**  Displays the VLAN trunking settings.
WS2000> admin(network.vlan.trunk)> set

Description:
Sets trunk parameters.

Syntax:

<table>
<thead>
<tr>
<th></th>
<th>trunk-port</th>
<th>enable / disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>&lt;port idx&gt;</td>
<td></td>
</tr>
<tr>
<td>trunked</td>
<td>add</td>
<td></td>
</tr>
<tr>
<td>all</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enables or disables the trunk port for the VLAN to be <port id> (1–6) as numbered on the switch.

Adds the VLANs in <vlan list> to be trunked. Specify a VLAN by number (1–4094), separated by commas.

Assigns all VLANs to be trunked.

Example:

```
admin(network.vlan.trunk)> set trunked add 3,4
admin(network.vlan.trunk)> ```
WS2000>admin(network.vlan.trunk)> show

Description:
Displays VLAN trunk settings.

Syntax:

show trunk Displays VLAN trunking settings.

Example:

admin(network.vlan.trunk)>show trunk

Trunk Port : None
VLAN's Trunked : None

Related Commands:

set Sets trunking parameters.
13.18 Network WAN Commands

WS2000>admin(network)> wan

Description:

Displays the WAN submenu. The items available under this command are shown below.

- vpn: Goes to the VPN submenu.
- nat: Goes to the NAT submenu.
- app: Goes to the outbound content filtering submenu.
- renew: Renews the IP address.
- set: Sets WAN parameters.
- show: Shows WAN parameters.
- save: Saves the configuration to system flash.
- quit: Quits the CLI.
- ..: Goes to the parent menu.
- /: Goes to the root menu.
WS2000>admin(network.wan)> renew

Description:
Renews the IP address.

Syntax:

renew
Renews the switch’s DHCP lease of the IP address if it is a DHCP client.

Example:

admin(network.wan)>renew
admin(network.wan)>
WS2000>admin(network.wan)> set

Description:
Sets the WAN parameters. In the Web interface, this functionality if provided by the Network->WAN screen.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set dhcp</td>
<td>Enables or disables the switch as a DHCP client.</td>
</tr>
<tr>
<td>dgw</td>
<td>Sets the default gateway IP address to &lt;a.b.c.d&gt;.</td>
</tr>
<tr>
<td>dns</td>
<td>Sets the IP address of one or two DNS servers, where &lt;idx&gt; indicates either the primary (1) or secondary (2) server, and &lt;a.b.c.d&gt; is the IP address of the server.</td>
</tr>
<tr>
<td>ipadr</td>
<td>Sets up to 8 (using &lt;idx&gt; from 1 to 8) IP addresses &lt;a.b.c.d&gt; for the WAN interface of the switch.</td>
</tr>
<tr>
<td>mask</td>
<td>Sets the subnet mask.</td>
</tr>
<tr>
<td>mode</td>
<td>Enables or disables the WAN interface associated with the given &lt;idx&gt; as set using the set ipadr command.</td>
</tr>
<tr>
<td>pppoe</td>
<td>Enables or disables PPPoE.</td>
</tr>
<tr>
<td>idle</td>
<td>Sets PPPoE idle time to &lt;val&gt; (an integer in the range 1–65535), which indicates the number of seconds.</td>
</tr>
<tr>
<td>password</td>
<td>Enables or disables PPPoE keepalive.</td>
</tr>
<tr>
<td>type</td>
<td>Sets PPPoE authentication to &lt;type&gt;, where &lt;type&gt; can be one of the following values: none, pap/chap, pap, or chap.</td>
</tr>
<tr>
<td>user</td>
<td>Sets PPPoE user name to &lt;userID&gt; (1–47 characters).</td>
</tr>
</tbody>
</table>

Example:

```
admin(network.wan)> set dhcp enable
admin(network.wan)> set dgw 192.168.122.25
admin(network.wan)> set pppoe mode enable
admin(network.wan)> set pppoe type chap
admin(network.wan)> set pppoe user JohnDoe
admin(network.wan)> set pppoe password @#$goodpassword%$#
admin(network.wan)> set pppoe keepalive enable
```

Related Commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip</td>
<td>Shows the IP settings for the WAN.</td>
</tr>
<tr>
<td>pppoe</td>
<td>Shows the PPPoE settings for the WAN.</td>
</tr>
</tbody>
</table>
WS2000>admin(network.wan)> show

Description:
Shows the WAN parameters.

Syntax:

`show ip  <idx>` Shows the general IP parameters for the WAN along with settings for the WAN interface associated with `<idx>` (where `<idx>` is in the range 1–8).

**Note:** If the WAN interface IP addresses have not been specified for `<idx>`, the IP and Mask values will be shown as 0.0.0.0.

`pppoe` Shows all PPPoE settings.

Example:

```
admin(network.wan)>show ip 3

wan interface : enable
ip address : 0.0.0.0
network mask : 0.0.0.0
default gateway : 192.168.24.1
dhcp mode : enable
primary dns server : 209.142.0.2
secondary dns server : 209.142.0.218
```

```
admin(network.wan)>show pppoe

pppoe mode : enable
pppoe keepalive mode : disable
pppoe authentication type : chap
pppoe idle time : 600
pppoe user name : JohnDoe
pppoe password : ********
```
13.19 Network WAN App Commands

WS2000>admin(network.wan)> app

Description:
Displays the outbound content filtering submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addcmd</td>
<td>Adds app control commands to the deny list.</td>
</tr>
<tr>
<td>delcmd</td>
<td>Deletes app control commands from the deny list.</td>
</tr>
<tr>
<td>list</td>
<td>Lists app control records.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>.</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(network.wan.app)> addcmd

Description:

Adds app control commands to the deny list.

Syntax:

```
addcmd  web  file  <filename>.<ext> Denies specified web file name. <filename> can be up to 15 characters and "*" can be used to match any string. <ext> can be up to 10 characters (such as htm, html, or java). Up to 10 files can be specified.
proxy
activex
ftp  put  Adds put command to the deny list.
get  Adds get command to the deny list.
ls  Adds list directory command to the deny list.
mkdir  Adds make directory command to the deny list.
cd  Adds connect directory command to the deny list.
pasv  Adds passive mode command to the deny list.
smtp  helo  Adds helo SMTP command to the deny list.
mail  Adds mail SMTP command to the deny list.
rcpt  Adds rcpt SMTP command to the deny list.
data  Adds data SMTP command to the deny list.
quit  Adds quit SMTP command to the deny list.
send  Adds send SMTP command to the deny list.
saml  Adds saml SMTP command to the deny list.
reset  Adds reset SMTP command to the deny list.
vrfy  Adds vrfy SMTP command to the deny list.
expn  Adds expn SMTP command to the deny list.
```

Example:

```
admin(network.wan.app)>addcmd ftp ?

put  : store command
get  : retrieve command
ls  : directory list command
mkdir  : create directory command
cd  : change directory command
pasv  : passive mode command

admin(network.wan.app)>addcmd ftp put
admin(network.wan.app)>addcmd ftp cd
admin(network.wan.app)>addcmd ftp pasv

admin(network.wan.app)>list ftp
```

FTP Commands
Storing Files               : deny
Retrieving Files            : allow
Directory List              : allow
Create Directory            : allow
Change Directory            : deny
Passive Operation           : deny

admin(network.wan.app) > addcmd smtp helo
admin(network.wan.app) > addcmd smtp vrfy
admin(network.wan.app) > list smtp

SMTP Commands

HELO                      : deny
MAIL                      : allow
RCPT                      : allow
DATA                      : allow
QUIT                      : allow
SEND                      : allow
SAML                      : allow
RESET                     : allow
VRFY                      : deny
EXPN                      : allow

Related Commands:

delcmd                     Removes a file or command from the deny list.
WS2000>admin(network.wan.app)> delcmd

Description:

Deletes application control commands from the deny list.

Syntax:

delcmd web file <filename>.<ext> Deletes specified web file name from deny list. <filename> can be up to 15 characters and "***" can be used to match any string. <ext> can be up to 10 characters (such as htm, html, or java). Up to 10 files can be specified.

delcmd all Deletes all files from the deny list.

delcmd proxy Allows web proxies.

delcmd activex Allows ActiveX files.

delcmd ftp put Deletes put command from the deny list.
delcmd get Deletes get command from the deny list.
delcmd ls Deletes list directory command from the deny list.
delcmd mkdir Deletes make directory command from the deny list.
delcmd cd Deletes connect directory command from the deny list.
delcmd pasv Deletes passive mode command from the deny list.

delcmd smtp helo Deletes helo SMTP command from the deny list.
delcmd mail Deletes mail SMTP command from the deny list.
delcmd rcpt Deletes rcpt SMTP command from the deny list.
delcmd data Deletes data SMTP command from the deny list.
delcmd quit Deletes quit SMTP command from the deny list.
delcmd send Deletes send SMTP command from the deny list.
delcmd saml Deletes saml SMTP command from the deny list.
delcmd reset Deletes reset SMTP command from the deny list.
delcmd vrfy Deletes vrfy SMTP command from the deny list.
delcmd expn Deletes expn SMTP command from the deny list.

Example:

admin(network.wan.app)>list ftp

FTP Commands

Storing Files : deny
Retrieving Files : allow
Directory List : allow
Create Directory : allow
Change Directory : deny
Passive Operation : deny

admin(network.wan.app)>delcmd ftp put
admin(network.wan.app)>delcmd ftp cd

admin(network.wan.app)>list ftp
FTP Commands

<table>
<thead>
<tr>
<th>Storing Files</th>
<th>allow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieving Files</td>
<td>allow</td>
</tr>
<tr>
<td>Directory List</td>
<td>allow</td>
</tr>
<tr>
<td>Create Directory</td>
<td>allow</td>
</tr>
<tr>
<td>Change Directory</td>
<td>allow</td>
</tr>
<tr>
<td>Passive Operation</td>
<td>deny</td>
</tr>
</tbody>
</table>

admin(network.wan.app)>list smtp

SMTP Commands

<table>
<thead>
<tr>
<th>HELO</th>
<th>deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAIL</td>
<td>allow</td>
</tr>
<tr>
<td>RCPT</td>
<td>allow</td>
</tr>
<tr>
<td>DATA</td>
<td>allow</td>
</tr>
<tr>
<td>QUIT</td>
<td>allow</td>
</tr>
<tr>
<td>SEND</td>
<td>allow</td>
</tr>
<tr>
<td>SAML</td>
<td>allow</td>
</tr>
<tr>
<td>RESET</td>
<td>allow</td>
</tr>
<tr>
<td>VRFY</td>
<td>deny</td>
</tr>
<tr>
<td>EXPN</td>
<td>allow</td>
</tr>
</tbody>
</table>

admin(network.wan.app)>delcmd smtp helo
admin(network.wan.app)>list smtp

SMTP Commands

<table>
<thead>
<tr>
<th>HELO</th>
<th>allow</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAIL</td>
<td>allow</td>
</tr>
<tr>
<td>RCPT</td>
<td>allow</td>
</tr>
<tr>
<td>DATA</td>
<td>allow</td>
</tr>
<tr>
<td>QUIT</td>
<td>allow</td>
</tr>
<tr>
<td>SEND</td>
<td>allow</td>
</tr>
<tr>
<td>SAML</td>
<td>allow</td>
</tr>
<tr>
<td>RESET</td>
<td>allow</td>
</tr>
<tr>
<td>VRFY</td>
<td>deny</td>
</tr>
<tr>
<td>EXPN</td>
<td>allow</td>
</tr>
</tbody>
</table>

Related Commands:

**addcmd**  
Adds a file or command to the deny list.
WS2000>admin(network.wan.app) > list

Description:
Lists the app control records.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Lists Web/HTTP app control settings.</td>
</tr>
<tr>
<td>ftp</td>
<td>Lists FTP app control settings.</td>
</tr>
<tr>
<td>smtp</td>
<td>Lists SMTP app control record.</td>
</tr>
</tbody>
</table>

Example:

```
admin(network.wan.app) > list web

HTTP Files/Commands

Web Proxy : deny
ActiveX    : deny
filename   :
```

```
admin(network.wan.app) > list ftp

FTP Commands

Storing Files : allow
Retrieving Files : allow
Directory List : allow
Create Directory : deny
Change Directory : deny
Passive Operation : deny
```

```
admin(network.wan.app) > list smtp

SMTP Commands

HELO      : deny
MAIL      : allow
RCPT      : allow
DATA      : allow
QUIT      : allow
SEND      : allow
SAML      : allow
RESET     : allow
VRFY      : deny
EXPN      : allow
```

```
admin(network.wan.app) >
```
13.20 Network WAN NAT Commands

WS2000>admin(network.wan)> nat

Description:

Displays the nat submenu. The items available under this command are shown below.

- **add**: Adds NAT records.
- **delete**: Deletes NAT records.
- **list**: Lists NAT records.
- **set**: Sets NAT parameters.
- **show**: Shows NAT parameters.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
WS2000>admin(network.wan.nat)> add

**Description:**

Adds NAT records.

**Syntax:**

```
add inb <idx> <name> <tran> <port1> <port2> <ip> <dst_port>
```

Sets an inbound network address translation (NAT) for WAN address <idx>, where <name> is the name of the entry (1 to 7 characters), <tran> is the transport protocol (one of tcp, udp, icmp, ah, esp, gre, or all), <port1> is the starting port number in a port range, <port2> is the ending port number in a port range, <ip> is the internal IP address, and <dst_port> is the (optional) internal translation port.

**Example:**

```
admin(network.wan.nat)>add inb 2 special tcp 20 21 192.168.42.16 21
```

```
admin(network.wan.nat)>list inb 2
                        index  name  prot  start port  end port  internal ip  translation port
                        1  special  tcp  20   21  192.168.42.16    21
```

**Related Commands:**

- **delete inb** Deletes one of the inbound NAT entries from the list.
- **list inb** Displays the list of inbound NAT entries.
WS2000>admin(network.wan.nat)> delete

Description:

Deletes NAT records.

Syntax:

delete inb <idx> <entry> Deletes a NAT entry <entry> (1–20) that is associated with WAN <idx> (1–8).
delete inb <idx> all Deletes all NAT entries associated with WAN <idx> (1–8).

Example:

admin(network.wan.nat)>list inb 2

<table>
<thead>
<tr>
<th>index</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
<th>internal ip</th>
<th>translation port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>special</td>
<td>tcp</td>
<td>20</td>
<td>21</td>
<td>192.168.42.16</td>
<td>21</td>
</tr>
</tbody>
</table>

admin(network.wan.nat)>delete inb 2 all

admin(network.wan.nat)>list inb 2

Related Commands:

add inb Adds entries to the list of inbound NAT entries.
list inb Displays the list of inbound NAT entries.
WS2000>admin(network.wan.nat)> list

Description:
Lists NAT records.

Syntax:
list inb <idx> Lists the inbound NAT entries associated with WAN port <idx> (1–8).

Example:
admin(network.wan.nat)>add inb 2 special tcp 20 21 192.168.42.16 21

admin(network.wan.nat)>list inb 2

<table>
<thead>
<tr>
<th>index</th>
<th>name</th>
<th>prot</th>
<th>start port</th>
<th>end port</th>
<th>internal ip</th>
<th>translation port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>special</td>
<td>tcp</td>
<td>20</td>
<td>21</td>
<td>192.168.42.16</td>
<td>21</td>
</tr>
</tbody>
</table>

Related Commands:
delete inb Deletes one of the inbound NAT entries from the list.
add inb Adds entries to the list of inbound NAT entries.
WS2000>admin(network.wan.nat)> set

Description:
Sets NAT inbound and outbound parameters.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Enables or disables port forwarding for WAN IP address index &lt;idx&gt; (1–8).</td>
</tr>
<tr>
<td>ip</td>
<td>Forwards unspecified ports associated with WAN address &lt;idx&gt; to the specified IP address &lt;ip&gt; (1–8).</td>
</tr>
<tr>
<td>outb ip</td>
<td>Sets 1-to-1 NAT IP mapping associated with WAN address &lt;idx&gt; to the specified IP address &lt;ip&gt; (1–8).</td>
</tr>
<tr>
<td>map</td>
<td>Sets the subnet to WAN mapping for 1-to-many NAT relationship where &lt;from&gt; is the subnet (s1, s2, s3, or s4) and &lt;to&gt; is the WAN address index (1–8) or “none”.</td>
</tr>
<tr>
<td>type</td>
<td>Sets the type of NAT translation for WAN address index &lt;idx&gt; (1–8) to one of none, 1-to-1, or 1-to-many.</td>
</tr>
</tbody>
</table>

Example:

```
admin(network.wan.nat)>set type 1 1-to-1
admin(network.wan.nat)>set outb ip 1 209.239.44.36
admin(network.wan.nat)>set inb mode 1 enable
admin(network.wan.nat)>show nat 1

nat type : 1-to-1
one to one nat ip address : 209.239.44.36
port forwarding mode : enable
port forwarding ip address : 0.0.0.0
one to many nat mapping : subnet1 subnet2 subnet3 subnet4
```
WS2000>admin(network.wan.nat)> show

Description:

Shows NAT parameters.

Syntax:

show nat <idx>  Shows NAT settings for WAN <idx> (1–8).

Example:

admin(network.wan.nat)>set inb mode 1 enable
admin(network.wan.nat)>show nat 1

nat type : 1-to-1
one to one nat ip address : 209.239.44.36
port forwarding mode : enable
port forwarding ip address : 0.0.0.0
one to many nat mapping : subnet1 subnet2 subnet3 subnet4
13.21 Network WAN VPN Commands

WS2000>admin(network.wan)> vpn

Description:
Displays the VPN submenu. The items available under this command are shown below.

- cmgr: Goes to the cmgr (Certificate Manager) submenu.
- add: Adds an security policy database (SPD) entry.
- set: Sets SPD parameters.
- list: Lists SPD entries.
- delete: Deletes SPD entries.
- stats: Lists statistics for all active tunnels.
- ikestate: Lists statistics for all active tunnels.
- reset: Resets all VPN tunnels.
- save: Saves the configuration to system flash.
- quit: Quits the CLI.
- ..: Goes to the parent menu.
- /: Goes to the root menu.
WS2000>admin(network.wan.vpn)> add

Description:
Adds an security policy database (SPD) entry.

Syntax:
add <name> <LSubnet> <LWanIP> <RSubnetIP> <RSubnetMask> <RGatewayIP>

 Creates a tunnel named <name> (1 to 13 characters) to gain access to local subnet <LSubnet> (1, 2, 3, 4), through local WAN IP <LWanIP> from the remote subnet with address <RSubnetIP> and subnet mask <RSubnetMask> using the remote gateway <RGatewayIP>.

Example:
admin(network.wan.vpn)>add Bob 1 209.239.160.55 206.107.22.45 255.255.255.224 206.107.22.2
If tunnel type is Manual, proper SPI values and Keys must be configured after adding the tunnel

admin(network.wan.vpn)>list

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Type</th>
<th>Remote IP/Mask</th>
<th>Remote Gateway</th>
<th>Local WAN IP</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eng2EngAnnex</td>
<td>Manual</td>
<td>192.168.32.2/24</td>
<td>192.168.33.1</td>
<td>192.168.24.198</td>
<td>1</td>
</tr>
<tr>
<td>Bob</td>
<td>Manual</td>
<td>206.107.22.45/27</td>
<td>206.107.22.2</td>
<td>209.239.160.55</td>
<td>1</td>
</tr>
</tbody>
</table>

admin(network.wan.vpn)>
WS2000>admin(network.wan.vpn)> delete

Description:

Deletes security policy database (SPD) entries.

Syntax:

delete * Deletes all SPD entries.
<name> Deletes SPD entries named <name>.

Example:

admin(network.wan.vpn)>list

+-----------------+-----------------+-----------------+-----------------+-----------------+---------+
| Tunnel Name     | Type            | Remote IP/Net   | Remote Gateway  | Local WAN IP    | Subnet  |
+-----------------+-----------------+-----------------+-----------------+-----------------+---------+
| Eng2EngAnnex    | Manual          | 192.168.32.2/24 | 192.168.33.1     | 192.168.24.198  | 1       |
| Bob             | Manual          | 206.107.22.45/27| 206.107.22.2     | 209.239.160.55  | 1       |

admin(network.wan.vpn)>delete Bob

admin(network.wan.vpn)>list

+-----------------+-----------------+-----------------+-----------------+-----------------+---------+
| Tunnel Name     | Type            | Remote IP/Net   | Remote Gateway  | Local WAN IP    | Subnet  |
+-----------------+-----------------+-----------------+-----------------+-----------------+---------+
| Eng2EngAnnex    | Manual          | 192.168.32.2/24 | 192.168.33.1     | 192.168.24.198  | 1       |

admin(network.wan.vpn)>
WS2000>admin(network.wan.vpn)> ikestate

**Description:**
Displays statistics for all active tunnels using Internet Key Exchange (IKE).

**Syntax:**
ikestate 

**Example:**
admin(network.wan.vpn)> ikestate

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>IKE State</th>
<th>Dest IP</th>
<th>Remaining Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eng2EngAnnex</td>
<td>Not Connected</td>
<td>----</td>
<td>---</td>
</tr>
<tr>
<td>Bob</td>
<td>Not Connected</td>
<td>----</td>
<td>---</td>
</tr>
</tbody>
</table>

admin(network.wan.vpn)>
WS2000>admin(network.wan.vpn)> list

Description:
Lists security policy database (SPD) entries.

Syntax:
list
<name>  Lists detailed information about tunnel named <name>. Note that the <name> must match case with the name in the SPD entry. “Bob” is not equal to “bob”, as shown in the example below.

Example:
admin(network.wan.vpn)>list

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Type</th>
<th>Remote IP/Mask</th>
<th>Remote Gateway</th>
<th>Local WAN IP</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eng2EngAnnex</td>
<td>Manual</td>
<td>192.168.32.2/24</td>
<td>192.168.33.1</td>
<td>192.168.24.198</td>
<td>1</td>
</tr>
<tr>
<td>Bob</td>
<td>Manual</td>
<td>206.107.22.45/27</td>
<td>206.107.22.2</td>
<td>209.239.160.55</td>
<td>1</td>
</tr>
</tbody>
</table>

admin(network.wan.vpn)>list bob

bad index value

admin(network.wan.vpn)>list Bob

Detail listing of VPN entry:

Name : Bob
Local Subnet : 1
Tunnel Type : Manual
Remote IP : 206.107.22.45
Remote IP Mask : 255.255.255.224
Remote Security Gateway : 206.107.22.2
Local Security Gateway : 209.239.160.55
AH Algorithm : None
Encryption Type : ESP
Encryption Algorithm : DES
ESP Inbound SPI : 0x0000000100
ESP Outbound SPI : 0x0000000100
WS2000>admin(network.wan.vpn)> reset

Description:
Resets all VPN tunnels.

Syntax:

reset Resets all VPN tunnels.

Example:

admin(network.wan.vpn)>reset

VPN tunnels reset.

admin(network.wan.vpn)>
**WS2000>admin(network.wan.vpn)> set**

**Description:**
Sets security policy database ( SPD) entry parameters.

**Syntax:**

```
set ike myidtype <name> <idtype>  
  Sets the Local ID type for IKE authentication for SPD <name> (1 to 13 characters) to <idtype> (one of IP, FQDN, or UFQDN).

remidtype <name> <idtype>  
  Sets the Remote ID type for IKE authentication for SPD <name> to <idtype>. This value is not required when the ID type is set to IP.

myiddata <name> <iddata>  
  Sets the Local ID data for IKE authentication for SPD <name> to <iddata>. This value is not required when the ID type is set to IP.

remiddata <name> <iddata>  
  Sets the Remote ID data for IKE authentication for SPD <name> to <iddata>.

opmode <name> Main/Aggr  
  Sets the Operation Mode of IKE for SPD <name> to Main or Aggr(essive).

authtype <name> <authtype>  
  Sets the IKE Authentication type for SPD <name> to <authtype> (one of PSK or RSA).

authalgo <name> MD5/SHA1  
  Sets the IKE Authentication Algorithm for SPD <name> to MD5 or SHA1.

psk <name> <psk>  
  Sets the IKE Pre-Shared Key for SPD <name> to <psk> (1–49 characters).

encalgo <name> <encalgo>  
  Sets the IKE Encryption Algorithm for SPD <name> to <encalgo> (one of DES, 3DES, AES128, AES192, or AES256).

lifetime <name> <lifetime>  
  Sets the IKE Key life time in seconds for SPD <name> to <lifetime>.

group <name> G768/G1024  
  Sets the IKE Diffie-Hellman Group for SPD <name> to either G768 or G1024.

type <name> Auto/Manual  
  Sets the authentication type of SPD <name> to Auto or Manual.

sub <name> <sub>  
  Sets the Local Subnet (1, 2, 3, or 4) for SPD <name> to subnet number <sub> (1, 2, 3, or 4).

remip <name> <remip>  
  Sets the IP address for the remote end of SPD <name> to <remip> (a.b.c.d).

remmask <name> <remmask>  
  Sets the IP Mask for the remote end of SPD <name> to <remmask> (a.b.c.d).

remgw <name> <remgw>  
  Sets the Remote IP gateway for SPD <name> to be <remgw> (a.b.c.d).

authalgo <name> <authalgo>  
  Sets the authentication algorithm for SPD <name> to <authalgo> (one of None, MD5, or SHA1).
```
authkey <name> IN/OUT <authkey>
Sets the AH authentication key (if SPD type is Manual) for tunnel <name> with the direction set to IN or OUT, and the manual authentication key set to <authkey>. (The key size is 32 hex characters for MD5, and 40 hex characters for SHA1).

certype <name> <encotype>
Sets the Encryption type for SPD <name> to <encotype> (one of None, ESP, or ESP-AUTH).

calgo <name> <encalgo>
Sets the Encryption Algorithm for SPD <name> to <encalgo> (one of DES, 3DES, AES128, AES192, or AES256).

spauthalgo <name> MD5/SHA1
Sets ESP Authentication Algorithm for SPD <name> to MD5 or SHA1.

ckey <name> IN/OUT <enckey>
Sets the Manual Encryption Key in ASCII for SPD <name> and direction IN or OUT to the key <enckey>. The size of the key depends on the encryption algorithm.
- 16 hex chars for DES
- 48 hex chars for 3DES
- 32 hex chars for AES128
- 48 hex chars for AES192
- 64 hex chars for AES256

spauthkey <name> IN/OUT<spauthkey>
Sets Manual ESP Authentication Key for SPD <name> either for IN or OUT direction to <spauthkey>, an ASCII string of hex characters. If authalgo is set to MD5, the provide 32 hex characters. If authalgo is set to SHA1, provide 40 hex characters.

spi <name> AUTH/ESP IN/OUT <spi>
Sets IN(bound) or OUT(bound) SPI for AUTH (Manual Authentication) or ESP for SPD <name> to <spi> (a hex value more than 0xFF).

localgw <name> <ip>
Sets the Local WAN IP to <ip> (a.b.c.d).

usepf <name> enable/disable
Enables or disables Perfect Forward Secrecy for SPD <name>.

services <name> <lifetime>
Sets SA life time to <lifetime> seconds (minimum 300).

Example:

```
admin(network.wan.vpn)>list Bob
```

---

**Detail listing of VPN entry:**

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Subnet</td>
<td>1</td>
</tr>
<tr>
<td>Tunnel Type</td>
<td>Manual</td>
</tr>
<tr>
<td>Remote IP</td>
<td>206.107.22.45</td>
</tr>
<tr>
<td>Remote IP Mask</td>
<td>255.255.255.224</td>
</tr>
<tr>
<td>Remote Security Gateway</td>
<td>206.107.22.2</td>
</tr>
<tr>
<td>Local Security Gateway</td>
<td>209.239.160.55</td>
</tr>
<tr>
<td>AH Algorithm</td>
<td>None</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>ESP</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>DES</td>
</tr>
</tbody>
</table>
ESP Inbound SPI : 0x00000100
ESP Outbound SPI : 0x00000100

admin(network.wan.vpn)>set usepfs Bob enable
admin(network.wan.vpn)>set spi Bob ESP IN abcde
admin(network.wan.vpn)>set spi Bob ESP OUT cdef23
admin(network.wan.vpn)>list Bob

-------------------------------------------
Detail listing of VPN entry:
-------------------------------------------
Name : Bob
Local Subnet : 1
Tunnel Type : Manual
Remote IP : 206.107.22.45
Remote IP Mask : 255.255.255.224
Remote Security Gateway : 206.107.22.2
Local Security Gateway : 209.239.160.55
AH Algorithm : None
Encryption Type : ESP
Encryption Algorithm : DES
ESP Inbound SPI : 0x000ABCDE
ESP Outbound SPI : 0x00CDEF23

admin(network.wan.vpn)>set authalgo Bob MD5
admin(network.wan.vpn)>list Bob

-------------------------------------------
Detail listing of VPN entry:
-------------------------------------------
Name : Bob
Local Subnet : 1
Tunnel Type : Manual
Remote IP : 206.107.22.45
Remote IP Mask : 255.255.255.224
Remote Security Gateway : 206.107.22.2
Local Security Gateway : 209.239.160.55
AH Algorithm : MD5
Encryption Type : ESP
Encryption Algorithm : DES
Auth Inbound SPI : 0x00000100
Auth Outbound SPI : 0x00000100
ESP Inbound SPI : 0x000ABCDE
ESP Outbound SPI : 0x00CDEF23
```
admin(network.wan.vpn)>set authkey Bob IN 12345678901234567890123456789012
admin(network.wan.vpn)>set authkey Bob OUT 11111111112222222222333333333344
admin(network.wan.vpn)>set spi Bob AUTH IN 2233445
admin(network.wan.vpn)>set spi Bob AUTH OUT 33344
admin(network.wan.vpn)>list Bob
```

Detail listing of VPN entry:

<table>
<thead>
<tr>
<th>Name</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Subnet</td>
<td>1</td>
</tr>
<tr>
<td>Tunnel Type</td>
<td>Manual</td>
</tr>
<tr>
<td>Remote IP</td>
<td>206.107.22.45</td>
</tr>
<tr>
<td>Remote IP Mask</td>
<td>255.255.255.224</td>
</tr>
<tr>
<td>Remote Security Gateway</td>
<td>206.107.22.2</td>
</tr>
<tr>
<td>Local Security Gateway</td>
<td>209.239.160.55</td>
</tr>
<tr>
<td>AH Algorithm</td>
<td>MD5</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>ESP</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>DES</td>
</tr>
<tr>
<td>Auth Inbound SPI</td>
<td>0x2233445</td>
</tr>
<tr>
<td>Auth Outbound SPI</td>
<td>0x00333444</td>
</tr>
<tr>
<td>ESP Inbound SPI</td>
<td>0x00ABCDEF</td>
</tr>
<tr>
<td>ESP Outbound SPI</td>
<td>0x00CDEF23</td>
</tr>
</tbody>
</table>
WS2000>admin(network.wan.vpn)> stats

Description:

Lists statistics for all active tunnels.

Syntax:

stats

Display statistics for all active VPN tunnels.

Example:

admin(network.wan.vpn)>stats

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Status</th>
<th>SPI(OUT/IN)</th>
<th>Life Time</th>
<th>Bytes(Tx/Rx)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eng2EngAnnex</td>
<td>Not Active</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>Not Active</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
13.22 Network WAN VPN Cmgr Commands

WS2000>admin(network.wan.vpn)> cmgr

Description:
Displays to the Certificate Manager submenu. The items available under this command are shown below.

- genreq: Generates a Certificate Request.
- loadca: Loads a trusted certificate from CA.
- loadself: Loads a self certificate signed by CA.
- showreq: Displays a certificate request in PEM format.
- listprivkey: Lists names of private keys.
- listself: Lists the self certificate loaded.
- listca: Lists the trusted certificate loaded.
- delprivkey: Deletes the private key.
- delself: Deletes the self certificate.
- delca: Deletes the trusted certificate.
- expcert: Exports the certificate file.
- impcert: Imports the certificate file.
- save: Saves the configuration to system flash.
- quit: Quits the CLI.
- ..: Goes to the parent menu.
- /: Goes to the root menu.
WS2000>admin(network.wan.vpn.cmgr)> delca

Description:

 Deletes a trusted certificate.

Syntax:

delca <IDname> Deletes the trusted certificate <IDname>.

Example:

 admin(network.wan.vpn.cmgr)>delca CAfinance
 admin(network.wan.vpn.cmgr)>
WS2000>admin(network.wan.vpn.cmgr)> delprivkey

**Description:**

Deletes a private key.

**Syntax:**

`delprivkey <IDname>`

Deletes private key named `<IDname>`.

**Example:**

```
admin(network.wan.vpn.cmgr)>delprivkey <IDname>
admin(network.wan.vpn.cmgr)>
```
WS2000>admin(network.wan.vpn.cmgr)> delself

**Description:**

Deletes a self certificate.

**Syntax:**

delself <IDname>  Deletes the self certificate named <IDname>.

**Example:**

```
admin(network.wan.vpn.cmgr)>delself<IDname>
admin(network.wan.vpn.cmgr)>
```
WS2000>admin(network.wan.vpn.cmgr)> expcert

Description:
Exports the certificate file.

Syntax:
expcert  ftp / tftp  <file name>  Exports the certificate with specified filename <file name> by either ftp or tftp. The tftp or ftp options for this file transfer will use the settings for the configuration file settings. See System Configuration Commands for information on how to set the tftp/ftp options.

Example:
admin(system.config)>set server 192.168.22.12
admin(system.config)>set user myadmin
admin(system.config)>set passwd

admin(network.wan.vpn.cmgr)>expcert ftp mycertificate
admin(network.wan.vpn.cmgr)>}

Related Commands:
impcert  Imports a certificate.
WS2000>admin(network.wan.vpn.cmgr)> genreq

**Description:**
Generates a Certificate Request.

**Syntax:**
```
genreq <Idname> <Subject> ...optional arguments...
```
Generates a self-certificate request for a Certification Authority (CA), where <Idname> is the private key ID (up to 7 characters) and <subject> is the subject name (up to 49 characters). A number of optional arguments can also be specified as indicated below.

- `-ou <OrgUnit>` Organization Unit (up to 49 chars)
- `-on <OrgName>` Organization Name (up to 49 chars)
- `-cn <City>` City Name of Organization (up to 49 chars)
- `-st <State>` State Name (up to 49 chars)
- `-p <PostCode>` Postal code (9 digits)
- `-cc <CCode>` Country code (2 chars)
- `-e <Email>` E-mail Address (up to 49 chars)
- `-d <Domain>` Domain Name (up to 49 chars)
- `-i <IP>` IP Address (a.b.c.d)
- `-sa <SAalgo>` Signature Algorithm (one of MD5-RSA or SHA1-RSA)
- `-k <KSize>` Key size in bits (one of 512, 1024, or 2048)

**Note:** The parameters in [square brackets] are optional. Check with the CA to determine what fields are necessary. For example, most CAs require an email address and an IP address, but not the address of the organization.

**Example:**
```
admin(network.wan.vpn.cmgr)>genreq MyCert2 MySubject -ou MyDept -on MyCompany
Please wait. It may take some time...

-----BEGIN CERTIFICATE REQUEST-----
MIHzMIGeAgEAMDkxEjAQBgNVBAoTCU15Q29tcGFueTEPMA0GA1UECxMGTXlEZXB0
MRIwEAYDVQQDEw1NeVN1YmplY3QwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAtKcX
plKFCFAJymTFX7lyuxY1fdS7UEhKjBsH7pdqnJnsASk6ZQGAqerjRpKScWlzmzn4
1q2+mgGnCvaZULIo7wIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCC1Q5LHdbG/C1f
Bj8AszttSo/bA4dcX3vHvhJcmuuWO9LHS2imPA3xhX/d6+Q1SMbs+tG4RP01RSr
iWDyuvwx
-----END CERTIFICATE REQUEST-----
WS2000>admin(network.wan.vpn.cmgr)> impcert

Description:
Imports the certificate file.

Syntax:

```
impcert  ftp / tftp  <file name>  Imports the certificate with specified filename <file name> by either ftp or tftp. The tftp or ftp options for this file transfer will use the settings for the configuration file settings. See System Configuration Commands for information on how to set the tftp/ftp options.

Example:
```
```
admin(system.config)>set server 192.168.22.12
admin(system.config)>set user myadmin
admin(system.config)>set passwd

admin(network.wan.vpn.cmgr)>impcert ftp mycertificate
admin(network.wan.vpn.cmgr)>
```

Related Commands:

```
expcert  Exports a certificate.
```
WS2000>admin(network.wan.vpn.cmgr)> listca

Description:
Lists the loaded trusted certificate.

Syntax:
listca
Lists the loaded trusted certificates.

Example:
admin(network.wan.vpn.cmgr)>listca
Trusted Certificate List:
WS2000>admin(network.wan.vpn.cmgr)> listprivkey

Description:

Lists the names of private keys.

Syntax:

listprivkey  Lists all private keys.

Example:

admin(network.wan.vpn.cmgr)>listprivkey

-------------------------------
Private Key Name       Certificate Associated
-------------------------------
**WS2000>admin(network.wan.vpn.cmgr)> listself**

**Description:**
Lists the loaded self certificates.

**Syntax:**

`listself` Lists all self certificates that are loaded.

**Example:**

```
admin(network.wan.vpn.cmgr)> listself
```

**Self Certificate List:**
WS2000>admin(network.wan.vpn.cmgr)> loadca

Description:

Loads a trusted certificate from the Certificate Authority.

Syntax:

loadca

Example:

admin(network.wan.vpn.cmgr)>loadca

Currently Only certificates in PEM format can be uploaded
Paste the certificate:
WS2000>admin(network.wan.vpn.cmgr)> loadself

**Description:**

Loads a self certificate signed by the Certificate Authority.

**Syntax:**

`loadself <IDname>` Loads the self certificate signed by the CA with name `<IDname>`.

**Example:**

```
admin(network.wan.vpn.cmgr)> loadself MyCert
Currently Only certificates in PEM format can be uploaded.
Paste the certificate:
```
WS2000>admin(network.wan.vpn.cmgr)> showreq

**Description:**

Displays a certificate request in PEM format.

**Syntax:**

```
showreq  <IDname>  Displays a certificate request named <IDname> generated from the genreq command.
```
13.23 Network WLAN Commands

WS2000>admin(network)> wlan

Description:
Displays the WLAN submenu. The items available under this command are shown below.

- **add**: Adds MU access control list entries.
- **delete**: Deletes MU access control list entries.
- **list**: Lists MU access control list entries.
- **rogueap**: Goes to the rogue AP submenu.
- **set**: Sets WLAN parameters.
- **show**: Shows WLAN parameters.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
WS2000>admin(network.wlan)> add

Description:
Add entries to the mobile unit (MU) access control list.

Syntax:
add <idx> <mac1> <mac2> Adds an entry to the MU access control list, where <idx> is the WLAN index (1–4), 
<mac1> is the starting MAC address (e.g., 001122334455), and <mac2> is ending MAC address in the acceptable range.

Example:
admin(network.wlan)>add 1 000000000000 112233445566
admin(network.wlan)>list 1
------------------------------------------------------------------------------
index  start mac  end mac
------------------------------------------------------------------------------
1  000000000000  112233445566
admin(network.wlan)>

Related Commands:
delete Deletes entries from the MU access control list.
list Shows entries in the MU access control list.
WS2000>admin(network.wlan)> delete

Description:

Deletes specified entry or entries from mobile unit (MU) access control list.

Syntax:

```
delete  <idx>  <entry>    Deletes MU access control list entry <entry> (1–30) for WLAN <idx> (1–4).
delete  <idx>  all        Deletes all access control list entries for the WLAN specified by <idx>.
```

Example:

```
admin(network.wlan)>add 1 223344556677 334455667788
admin(network.wlan)>list 1

<table>
<thead>
<tr>
<th>index</th>
<th>start mac</th>
<th>end mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>000000000000</td>
<td>112234455666</td>
</tr>
<tr>
<td>2</td>
<td>223344556677</td>
<td>334455667788</td>
</tr>
</tbody>
</table>

admin(network.wlan)>delete 1 2
admin(network.wlan)>list 1

<table>
<thead>
<tr>
<th>index</th>
<th>start mac</th>
<th>end mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>000000000000</td>
<td>112234455666</td>
</tr>
</tbody>
</table>

admin(network.wlan)>`

Related Commands:

- **add** Adds entries to the MU access control list.
- **list** Displays entries in the MU access control list.
WS2000>admin(network.wlan)> list

Description:

Lists the entries in the mobile unit (MU) access control list.

Syntax:

```
list <idx>       Displays the entries in the MU access control list for WLAN <idx> (1–4).
```

Example:

```
admin(network.wlan)> list 1

+----------+----------+----------+
| index    | start    | end      |
|----------+----------+----------|
| 1        | 000000000000 | 112233445566 |
```

Related Commands:

- **add**       Adds entries to the MU access control list.
- **delete**    Deletes entries from the MU access control list.
WS2000>admin(network.wlan)> set

Description:
Sets WLAN parameters.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set acl</td>
<td>Sets the default MU access control mode to allow or deny for WLAN &lt;idx&gt;.</td>
</tr>
<tr>
<td>adopt</td>
<td>Sets default Access Port adoption to allow or deny for WLAN &lt;idx&gt;.</td>
</tr>
<tr>
<td>auth</td>
<td>Sets the authentication type for WLAN &lt;idx&gt; to &lt;type&gt; (none, eap, or kerberos).</td>
</tr>
<tr>
<td>bcast</td>
<td>Enables or disables the broadcast ESS answer.</td>
</tr>
<tr>
<td>eap adv</td>
<td>Sets the EAP MU/supplicant quiet period for WLAN &lt;idx&gt; to &lt;period&gt; seconds (1–65535).</td>
</tr>
<tr>
<td></td>
<td>Sets the EAP MU/supplicant TX period for WLAN &lt;idx&gt; to &lt;period&gt; seconds (1–65535).</td>
</tr>
<tr>
<td></td>
<td>Sets the EAP MU/supplicant timeout for WLAN &lt;idx&gt; to &lt;timeout&gt; seconds (1–255).</td>
</tr>
<tr>
<td></td>
<td>Sets the EAP maximum number of MU retries to &lt;retry&gt; (1–10) for WLAN &lt;idx&gt;.</td>
</tr>
<tr>
<td></td>
<td>Sets the server timeout for WLAN &lt;idx&gt; to &lt;timeout&gt; seconds (1–255).</td>
</tr>
<tr>
<td></td>
<td>Sets the maximum number of server retries for WLAN &lt;idx&gt; to &lt;retry&gt; (1–10).</td>
</tr>
<tr>
<td>server</td>
<td>Sets the RADIUS server &lt;rsidx&gt; (1-primary or 2-secondary) for WLAN &lt;idx&gt; to IP address &lt;ip&gt;.</td>
</tr>
<tr>
<td>port</td>
<td>Sets the RADIUS server &lt;rsidx&gt; (1-primary or 2-secondary) for WLAN &lt;idx&gt; to &lt;port&gt;.</td>
</tr>
<tr>
<td>rad-acct</td>
<td>Enables/disables RADIUS accounting for WLAN &lt;idx&gt;.</td>
</tr>
<tr>
<td></td>
<td>Sets RADIUS accounting retry count to &lt;count&gt; (1–10) for WLAN &lt;idx&gt;.</td>
</tr>
<tr>
<td></td>
<td>Sets RADIUS accounting retry timeout to &lt;time&gt; seconds (1–255).</td>
</tr>
<tr>
<td>reauth</td>
<td>Enables or disables the EAP reauthentication parameters for WLAN &lt;idx&gt;.</td>
</tr>
<tr>
<td></td>
<td>Sets the reauthentication period for WLAN &lt;idx&gt; to &lt;period&gt; seconds (30–9999).</td>
</tr>
<tr>
<td></td>
<td>Sets the maximum number of reauthentication retries to &lt;retry&gt; (1–99) for WLAN &lt;idx&gt;.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>secret</strong></td>
<td>&lt;idx&gt; &lt;rsidx&gt; &lt;secret&gt; &lt;idx&gt; &lt;secret&gt; &lt;rsidx&gt;</td>
</tr>
<tr>
<td><strong>syslog</strong></td>
<td>ip &lt;idx&gt; &lt;ip&gt;</td>
</tr>
<tr>
<td><strong>enc</strong></td>
<td>&lt;idx&gt; &lt;type&gt;</td>
</tr>
<tr>
<td><strong>ess</strong></td>
<td>&lt;idx&gt; &lt;ess&gt;</td>
</tr>
<tr>
<td><strong>kerb</strong></td>
<td>passwd &lt;idx&gt; &lt;password&gt;</td>
</tr>
<tr>
<td><strong>port</strong></td>
<td>&lt;idx&gt; &lt;ksidx&gt; &lt;port&gt;</td>
</tr>
<tr>
<td><strong>realm</strong></td>
<td>&lt;idx&gt; &lt;realm&gt;</td>
</tr>
<tr>
<td><strong>server</strong></td>
<td>&lt;idx&gt; &lt;ksidx&gt; &lt;ip&gt;</td>
</tr>
<tr>
<td><strong>user</strong></td>
<td>&lt;idx&gt; &lt;name&gt;</td>
</tr>
<tr>
<td><strong>mcast</strong></td>
<td>&lt;idx&gt; &lt;midx&gt; &lt;mic&gt;</td>
</tr>
<tr>
<td><strong>mode</strong></td>
<td>&lt;idx&gt; enable/disable</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>&lt;idx&gt; &lt;name&gt;</td>
</tr>
<tr>
<td><strong>no-mu-mu</strong></td>
<td>&lt;idx&gt; &lt;mode&gt;</td>
</tr>
<tr>
<td><strong>vop</strong></td>
<td>&lt;idx&gt; &lt;mode&gt;</td>
</tr>
</tbody>
</table>
### Examples:

- **Example 1:**
  ```
  admin(network.wlan)>set name 1 store
  admin(network.wlan)>set name 2 backoff
  admin(network.wlan)>set auth 1 kerberos
  ```

  Kerberos requires WEP 104 or Keyguard. The encryption type has been changed to WEP 104.

- **Example 2:**
  ```
  admin(network.wlan)>set no-mu-mu 1 enable
  admin(network.wlan)>show wlan 1
  ```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan name</td>
<td>store</td>
</tr>
<tr>
<td>ess identifier</td>
<td>101</td>
</tr>
<tr>
<td>wlan mode</td>
<td>enable</td>
</tr>
<tr>
<td>enc type</td>
<td>wep104</td>
</tr>
<tr>
<td>auth type</td>
<td>kerberos</td>
</tr>
<tr>
<td>voice prioritization</td>
<td>enable</td>
</tr>
<tr>
<td>disallow mu to mu</td>
<td>enable</td>
</tr>
<tr>
<td>answer broadcast ess</td>
<td>disable</td>
</tr>
<tr>
<td>default mu acl mode</td>
<td>allow all</td>
</tr>
<tr>
<td>default ap adopt mode</td>
<td>allow all</td>
</tr>
<tr>
<td>multicast address 1</td>
<td>01005E000000</td>
</tr>
<tr>
<td>multicast address 2</td>
<td>09000E000000</td>
</tr>
</tbody>
</table>

### Table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>type &lt;idx&gt;</td>
<td>phrase/key</td>
</tr>
<tr>
<td>phrase &lt;idx&gt;</td>
<td>&lt;phrase&gt;</td>
</tr>
<tr>
<td>rotate-mode &lt;idx&gt;</td>
<td>enable/disable</td>
</tr>
<tr>
<td>interval &lt;idx&gt;</td>
<td>&lt;interval&gt;</td>
</tr>
<tr>
<td>mixed-mode &lt;idx&gt;</td>
<td>enable/disable</td>
</tr>
<tr>
<td>preauth &lt;idx&gt;</td>
<td>enable/disable</td>
</tr>
<tr>
<td>opp-pmk &lt;idx&gt;</td>
<td>enable/disable</td>
</tr>
</tbody>
</table>

- **Sets the CCMP key type to phrase or key for WLAN <idx>**.
- **Sets the CCMP ASCII pass phrase for WLAN <idx> to <phrase> (8–63 characters).** Must be specified when type parameter is set to phrase.
- **Enables or disables the broadcast key rotation for WLAN <idx>**.
- **Sets the broadcast key rotation interval for WLAN <idx> to <interval> (300–604800) seconds.**
- **Enables or disables mixed mode (allowing WPA-TKIP clients) for WLAN <idx>**.
- **Enables or disables preauthentication (fast roaming) for WLAN <idx>**.
- **Enables or disables opportunistic PMK caching (fast roaming) for WLAN <idx>**.

**Note:** The WEP authentication mechanism saves up to four different keys (one for each WLAN). It is not requirement to set all keys, but you must associate a WLAN with the appropriate key.

- **Selects the WEP/KeyGuard key (from one of the four potential values of <kidx> (1–4) for WLAN <idx>.**
- **Sets the WEP/KeyGuard key for key index <kidx> (1–4) for WLAN <idx> to <key> 1 to 26 (hex digits).**
admin(network.wlan)>
WS2000>admin(network.wlan)> show

Description:
Displays the WLAN parameters.

Syntax:

show eap <idx> Shows the EAP parameters for WLAN <idx>.
show kerb <idx> Shows the Kerberos parameters for WLAN <idx>.
show tkip <idx> Shows the TKIP parameters for WLAN <idx>.
show ccmp <idx> Shows the CCMP parameters for WLAN <idx>.
show wep-mcm <idx> Shows the WEP/Keyguard parameters for WLAN <idx>.
show wlan <idx> Shows the basic WLAN parameters for WLAN <idx>.

Example:

admin(network.wlan)>show tkip 1

  tkip key type : phrase
  tkip phrase   : ********
  tkip key     : ********
  tkip rotate mode : disable
  tkip rotate interval : 86400

admin(network.wlan)>show ccmp 1

  ccmp key type   : phrase
  ccmp phrase    : ********
  ccmp key       : ********
  ccmp rotate mode : disable
  ccmp rotate interval : 86400
  ccmp mixed mode (allow WPA) : disable
  802.11i preauthentication : disable
  Opportunistic PMK Caching : enable

admin(network.wlan)>show wep-mcm 1

  wep key index : 1
  wep key 1     : ********
  wep key 2     : ********
  wep key 3     : ********
  wep key 4     : ********

admin(network.wlan)>show wlan 1

  wlan name : WLAN1
ess identifier : 101
wlan mode : enable
enc type : none
auth type : none
voice prioritization : enable
disallow mu to mu : disable
answer broadcast ess : disable
default mu acl mode : allow all
default ap adopt mode : allow all
multicast address 1 : 01005E000000
multicast address 2 : 09000E000000

Related Commands:

set Sets WLAN parameters.
### 13.24 Network WLAN Rogue AP Commands

**WS2000>admin(network.wlan)> rogueap**

**Description:**

Displays the rogue AP submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Shows current rogue AP configuration.</td>
</tr>
<tr>
<td>set</td>
<td>Sets rogue AP parameters.</td>
</tr>
<tr>
<td>rulelist</td>
<td>Goes to the rule list submenu.</td>
</tr>
<tr>
<td>approvedlist</td>
<td>Goes to the approved AP list submenu.</td>
</tr>
<tr>
<td>roguelist</td>
<td>Goes to the rogue AP list submenu.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(network.wlan.rogueap)> set

Description:
Sets rogue access point parameters.

Syntax:

set muscan mode enable / disable
Sets the MU scan interval to <interval> (5–65535) minutes. Enables or disables mobile unit scanning.

set apscan mode enable / disable
Sets the AP scan interval to <interval> (5–65535) minutes. Enables or disables AP scanning.

set detscan mode enable / disable
Sets the detector AP scan interval to <interval> (5–65535) minutes. Enables or disables detector AP scanning. For this feature to be fully functional, you must also set one of the Access Ports as a detector AP. See the WS2000>admin(network.ap)> set command.

interval <interval>
Sets the detector AP scan interval to <interval> (5–65535) minutes.

Example:

admin(network.wlan.rogueap)>set apscan mode enable
admin(network.wlan.rogueap)>set apscan int 60

Related Commands:

show Displays the rogue AP parameters.
WS2000>admin(network.wlan.rogueap)> show

Description:
Shows the current rogue AP configuration.

Syntax:
show
Displays the rogue AP scanning settings.

Example:
admin(network.wlan.rogueap)>show

mu scan               : disabled
mu scan interval      : 60 minutes
ap scan               : disabled
ap scan interval      : 60 minutes
detector ap scan      : disabled
detector ap scan interval : 60 minutes

Related Commands:
set
Sets the rogue AP scanning parameters.
13.25 Network WLAN Rogue AP Approved AP List Commands

WS2000>admin(network.wlan.rogueap)> approvedlist

Description:

Displays the approved AP list submenu. The items available under this command are shown below.

- **show**: Shows the approved AP list.
- **ageout**: Displays the ageout time for an approved list entry.
- **approve**: Approves an AP.
- **erase**: Erases the list.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
WS2000>admin(network.wlan.rogueap.approvedlist)> ageout

Description:
Displays ageout time for an approved list entry.

Syntax:

    ageout <interval>  Sets the number of minutes, <interval> (0–1000) before an entry in the approved list is automatically removed.

Example:

    admin(network.wlan.rogueap.approvedlist)>ageout 30
    admin(network.wlan.rogueap.approvedlist)>

Related Commands:

    erase  Erases the approved AP list.
WS2000>admin(network.wlan.rogueap.approvedlist)> approve

Description:
Approves an AP.

Syntax:
approve <idx>          Approves an access point from the list.
all                     Approves all access points in the list.

Example:
admin(network.wlan.rogueap.approvedlist)> approve 1
admin(network.wlan.rogueap.approvedlist)> approve all
admin(network.wlan.rogueap.approvedlist)>

Related Commands:
erase  Erases all access points in the list.
WS2000>admin(network.wlan.rogueap.approvedlist)> erase

Description:

Erases the approved AP list.

Syntax:

erase all  Erases all entries in the approved list.

Example:

admin(network.wlan.rogueap.approvedlist)>erase all
admin(network.wlan.rogueap.approvedlist)>show

    approved ap list
    +++++++++++++++++

    approved list ageout : 30 minutes

    index     ap     essid
    ----     --     ------

Related Commands:

approve   Adds an Access Port to the approved list.
show      Displays the approved list.
WS2000>admin(network.wlan.rogueap.approvedlist)> show

Description:

Shows the approved AP list.

Syntax:

show 
Displays the list of approved APs.

Example:

admin(network.wlan.rogueap.approvedlist)> show

approved ap list
++++++++++++++++

approved list ageout : 30 minutes

index ap essid
----- -- ------

Related Commands:

approve 
Adds an AP to the approved list.
13.26 Network WLAN Rogue AP List Commands

WS2000>admin(network.wlan.rogueap)> roguelist

Description:
Displays the rogue AP list submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays the rogue list entries.</td>
</tr>
<tr>
<td>locate</td>
<td>Goes to the submenu for locating a rogue AP.</td>
</tr>
<tr>
<td>muscan</td>
<td>Goes to the submenu for on-demand MU polling.</td>
</tr>
<tr>
<td>ageout</td>
<td>Displays the ageout time for a rogue list entry.</td>
</tr>
<tr>
<td>approve</td>
<td>Approves a rogue AP.</td>
</tr>
<tr>
<td>erase</td>
<td>Erases the list.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(network.wlan.rogueap.roguelist)> ageout

Description:
Displays the ageout time for a rogue list entry.

Syntax:

```
ageout <time>
```
Sets the ageout time for the entry associated to <time> (1–1000) minutes.

Example:

```
admin(network.wlan.rogueap.roguelist)>ageout 50
```

Related Commands:

- `locate` Locates a rogue AP.
- `show` Shows the rogue AP list parameters and entries.
**WS2000>admin(network.wlan.rogueap.roguelist)> approve**

**Description:**
Moves a rogue AP into the approved AP list.

**Syntax:**

```
approve  <idx>   Puts the rogue AP <idx> into the approved AP list.
   all       Puts all the entries of the rogue list into the approved AP list.
```

**Example:**

```
admin(network.wlan.rogueap.approvedlist)>approve all
```

**Related Commands:**

```
show       Shows the rogue list entries.
```

WS2000>admin(network.wlan.rogueap.roguelist)> erase

Description:
Erases the rogue AP list.

Syntax:
 erase all

Example:
admin(network.wlan.rogueap.roguelist)> erase all

Related Commands:
 show Lists all entries in the rogue AP list.
WS2000>admin(network.wlan.rogueap.roguelist)> show

Description:
Displays the rogue list entries.

Syntax:
show all  Displays the list of rogue APs.
<idx>    Displays detailed information for the rogue AP with index number <idx>.

Example:
  admin(network.wlan.rogueap.roguelist)> show all

    rogue ap list
    +++++++++++++++++++

    rogue list ageout : 0 minutes

    Idx  AP                Essid                Channel
    +---------------------------------------------------------------------+

Related Commands:
locate    Locates a rogue AP.
approve   Approves a rogue AP.
13.27 Network WLAN Rogue AP Locate Commands

WS2000>admin(network.wlan.rogueap.roguelist)> locate

Description:

Displays the locate submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Starts locating a rogue AP.</td>
</tr>
<tr>
<td>list</td>
<td>Lists results of the locate rogue AP scan.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>.</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
**list**

**Description:**
Lists the results of the locate rogue AP scan.

**Syntax:**

```
list
```

Lists the results of the locate rogue AP scan.

**Example:**

```
admin(network.wlan.rogueap.roguelist.locate)>list
```

**Related Commands:**

- **start**: Starts the rogue AP location process.
WS2000>admin(network.wlan.rogueap.roguelist.locate)> start

Description:
Locates a rogue AP.

Syntax:

```
start <mac> <essid>
```

Starts locating a rogue AP where `<mac>` is the MAC address (or BSSID) of the rogue AP, and `<essid>` is the ESSID for the rogue AP.

Example:

```
admin(network.wlan.rogueap.roguelist.locate)>start 00A0f8fe2344 wlan-engg
```

Related Commands:

```
list
```
Lists information for the rogue AP found during the scan.
13.28 Network WLAN Rogue AP MU Scan Commands

WS2000>admin(network.wlan.rogueap.roguelist)> muscan

Description:
Displays the MU scan submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Starts a rogue AP scan using on-demand MU polling.</td>
</tr>
<tr>
<td>list</td>
<td>Lists the rogue APs found during the scan.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(network.wlan.rogueap.roguelist.muscan)> list

Description:
Lists the results of the locate rogue AP scan.

Syntax:
list          Lists the results of the locate rogue AP scan.

Example:
admin(network.wlan.rogueap.roguelist.muscan)> list

Related Commands:
start       Starts the MU scan process.
**WS2000>admin(network.wlan.rogueap.roguelist.muscan)> start**

**Description:**
Starts an on-demand MU polling for rogue APs.

**Syntax:**
```
start <mac>       Starts locating a rogue AP where <mac> is the MAC address (or BSSID) of the rogue AP, and <essid> is the ESSID for the rogue AP.
```

**Example:**
```
admin(network.wlan.rogueap.roguelist.muscan)> start 00A0f8fe2344
```

**Related Commands:**
```
list            Lists information for the rogue AP found during the scan.
```
13.29 Network WLAN Rogue AP Rule List Commands

WS2000>admin(network.wlan.rogueap)> rulelist

Description:
Displays the rule list submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Displays the rule list.</td>
</tr>
<tr>
<td>add</td>
<td>Adds an entry to the rule list.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes an entry from the rule list.</td>
</tr>
<tr>
<td>authsymbolap</td>
<td>Authorizes all Symbol APs.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(network.wlan.rogueap.rulelist)> add

Description:
Adds an entry to the rule list.

Syntax:
add <mac> <essid>   Adds an entry into the rule list to allow an AP with the mac address <mac> and the ESSID <essid>.

Example:
admin(network.wlan.rogueap.rulelist)>add 00a0f8f31212 mywlan
admin(network.wlan.rogueap.rulelist)>show

    rule list
    ++++++++  

    symbol ap authorization : disabled

    index ap essid
    ---- -- -------
    1 00:a0:f8:f3:12:12 mywlan

admin(network.wlan.rogueap.rulelist)>?

Related Commands:

show      Shows the entries in the rule list.
**WS2000>admin(network.wlan.rogueap.rulelist)> authsymbolap**

**Description:**

Authorizes all Symbol APs.

**Syntax:**

```
authsymbolap enable / disable
```

Enables or disables automatic authorization of all Symbol APs.

**Example:**

```
admin(network.wlan.rogueap.rulelist)> auth enable
admin(network.wlan.rogueap.rulelist)> show
```

```
rule list
+++++++++
symbol ap authorization : enabled

index ap essid
----- -- -------
1 00:a0:f8:f3:12:12 mywlan
```

**Related Commands:**

```
show
```

Shows all the rules in the rule list and shows status of the Symbol AP automatic authorization.
WS2000>admin(network.wlan.rogueap.rulelist)> delete

Description:
Deletes an entry from the rule list.

Syntax:

delete  all     Deletes all entries in the rule list.
<idx>       Deletes the <idx> entry in the rule list.

Example:

admin(network.wlan.rogueap.rulelist)>delete all
admin(network.wlan.rogueap.rulelist)>show

        rule list
        ++++++++,

            symbol ap authorization : enabled

index  ap  essid
------  --  ------

Related Commands:

show     Displays the entries in the rule list.
WS2000>admin(network.wlan.rogueap.rulelist)> show

Description:
Displays the rule list.

Syntax:

show
Displays all entries in the rule list.

Example:

admin(network.wlan.rogueap.rulelist)> show

rule list
+++++++  

symbol ap authorization   : enabled

index ap essid
---- -- ------
1 00:a0:f8:f3:12:12 mywlan

Related Commands:

delete Deletes entries from the rule list.
add Adds entries to the rule list.
13.30 Statistics Commands

WS2000>admin)> stats

Description:

Displays statistics and status for different switch entities. The items available under this command are shown below.

- **show**: Shows system status and statistics.
- **rf**: Goes to the RF statistics submenu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
**WS2000>admin(stats)> show**

**Description:**

Displays the system status and statistics for either the specified subnet or the WAN.

**Syntax:**

```
show lease subnet wan
```

- `show`  Show the leases issued by the switch.
- `subnet <idx>` Shows subnet status, where `<idx>` is the index number of the subnet (LAN) to show.
- `wan` Shows WAN status.

**Example:**

```
show subnet example
admin(stats)> show subnet 1
LAN Interface Information
subnet interface 1 : enable
ip address 1 : 192.168.0.1
network mask : 255.255.255.0
ethernet address : 00A0F86FD8FD
LAN Rx Information
rx packets : 236530
rx bytes : 31581419
rx errors : 0
rx dropped : 0
rx overruns : 0
rx frame errors : 0
LAN Tx Information
tx packets : 100101
tx bytes : 40811508
tx errors : 0
tx dropped : 0
tx overruns : 0
tx carrier errors : 0
Port 1
link status : up
speed : 100 Mbps
Port 2
link status : up
speed : 100 Mbps
Port 3
link status : down
Port 4
link status : down
Port 5
link status : down
Port 6
link status : down
WLAN Interfaces
wlans : wlan1
```
show wan example

admin(stats) > show wan

WAN Interface Information
wan interface 1 : enable
ip address 1 : 192.168.24.198
wan interface 2 : disable
ip address 2 : 192.168.24.198
wan interface 3 : disable
ip address 3 : 192.168.24.198
wan interface 4 : disable
ip address 4 : 192.168.24.198
wan interface 5 : disable
ip address 5 : 192.168.24.198
wan interface 6 : disable
ip address 6 : 192.168.24.198
wan interface 7 : disable
ip address 7 : 192.168.24.198
wan interface 8 : disable
ip address 8 : 192.168.24.198
network mask : 255.255.255.0
ethernet address : 00A0F86FD8FC
link status : up
speed : 100 Mbps

WAN Rx Information
rx packets : 226809
rx bytes : 311719105
rx errors : 1
rx dropped : 0
rx overruns : 0
rx frame errors : 1

WAN Tx Information
tx packets : 5499
tx bytes : 559567
tx errors : 0
tx dropped : 0
tx overruns : 0
tx carrier errors : 0
13.31 Statistics RF Commands

WS2000>admin(stats)> rf

Description:
Displays the RF statistics submenu. The items available under this command are shown below.

- **show**: Shows RF statistics.
- **reset**: Resets/clears all RF statistics.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
**WS2000>admin(stats.rf)> reset**

**Description:**
Resets/clears all RF statistics.

**Syntax:**
```
reset
```
Resets RF statistics.

**Example:**
```
admin(stats.rf)> reset
```
WS2000>admin(stats.rf)> show

Description:
Shows radio frequency (RF) statistics.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>Shows all WLAN status.</td>
</tr>
<tr>
<td>all</td>
<td>Shows all Access Port status.</td>
</tr>
<tr>
<td>wlan</td>
<td>Shows all mobile unit (MU) status.</td>
</tr>
<tr>
<td>ap &lt;idx&gt;</td>
<td>Shows the specified Access Port's statistics, where &lt;idx&gt; is the index number of the Access Port (1–12).</td>
</tr>
<tr>
<td>mu &lt;mu&gt;</td>
<td>Shows the specified mobile unit's statistics, where &lt;mu&gt; is the index number of the mobile unit (1–200).</td>
</tr>
<tr>
<td>total</td>
<td>Shows total switch statistics.</td>
</tr>
</tbody>
</table>

Example:

admin(stats.rf)> show all wlan example

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WLAN1</td>
<td>Enabled</td>
</tr>
<tr>
<td>2</td>
<td>WLAN2</td>
<td>Disabled</td>
</tr>
<tr>
<td>3</td>
<td>WLAN3</td>
<td>Disabled</td>
</tr>
<tr>
<td>4</td>
<td>WLAN4</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

admin(stats.rf)> show wlan 1 example

<table>
<thead>
<tr>
<th>Name</th>
<th>ESSID</th>
<th>Subnet</th>
<th>Adopted APs</th>
<th>Number of Associated MUs</th>
<th>Packets per second</th>
<th>Throughput</th>
<th>Average Bit Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN1</td>
<td>101</td>
<td>Subnet1</td>
<td>2</td>
<td>0</td>
<td>0.00 pps</td>
<td>0.00 Mbps</td>
<td>0.00 Mbps</td>
</tr>
</tbody>
</table>

admin(stats.rf)> show wlan 2 example

<table>
<thead>
<tr>
<th>Name</th>
<th>ESSID</th>
<th>Subnet</th>
<th>Adopted APs</th>
<th>Number of Associated MUs</th>
<th>Packets per second</th>
<th>Throughput</th>
<th>Average Bit Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN2</td>
<td>102</td>
<td>Subnet2</td>
<td>3</td>
<td>0</td>
<td>0.00 pps</td>
<td>0.00 Mbps</td>
<td>0.00 Mbps</td>
</tr>
</tbody>
</table>

admin(stats.rf)> show wlan 3 example

<table>
<thead>
<tr>
<th>Name</th>
<th>ESSID</th>
<th>Subnet</th>
<th>Adopted APs</th>
<th>Number of Associated MUs</th>
<th>Packets per second</th>
<th>Throughput</th>
<th>Average Bit Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN3</td>
<td>103</td>
<td>Subnet3</td>
<td>4</td>
<td>0</td>
<td>0.00 pps</td>
<td>0.00 Mbps</td>
<td>0.00 Mbps</td>
</tr>
</tbody>
</table>

admin(stats.rf)> show wlan 4 example

<table>
<thead>
<tr>
<th>Name</th>
<th>ESSID</th>
<th>Subnet</th>
<th>Adopted APs</th>
<th>Number of Associated MUs</th>
<th>Packets per second</th>
<th>Throughput</th>
<th>Average Bit Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN4</td>
<td>104</td>
<td>Subnet4</td>
<td>5</td>
<td>0</td>
<td>0.00 pps</td>
<td>0.00 Mbps</td>
<td>0.00 Mbps</td>
</tr>
</tbody>
</table>
Non-Unicast Packets : 0.00 %

Signal : 0.0 dBm
Noise : 0.0 dBm
Signal-to-Noise : 0.0 dBm

Average Number of Retries : 0.00 Retries
Dropped Packets : 0.00 %
Undecryptable Packets : 0.00 %

admin(stats.rf)>show all ap example
ap index : 1
ap status : not connected

ap index : 2
ap status : connected

ap index : 3
ap status : not connected

ap index : 4
ap status : not connected

ap index : 5
ap status : not connected

ap index : 6
ap status : not connected

ap index : 7
ap status : not connected

ap index : 8
ap status : not connected

ap index : 9
ap status : not connected

ap index : 10
ap status : not connected

ap index : 11
ap status : not connected

ap index : 12
ap status : not connected

admin(stats.rf)>show ap 2 example
Name : AP2
Location :
Radio Type : 802.11 B
Current Channel : 1
Adopted By : WLAN1
Number of Associated Mus : 0

Packets per second : 0.13 pps
Throughput : 0.00 Mbps
Average Bit Speed : 0.00 Mbps
Approximate Utilization : 0.00 %
Non-Unicast Packets : 100.00 %

Signal : 0.0 dBm
Noise : 0.0 dBm
Signal-to-Noise : 0.0 dBm

Average Number of Retries : 0.00 Retries
Dropped Packets : 0.00 %
Undecryptable Packets : 0.00 %
13.32 System Commands

WS2000>admin)> system

Description:
Displays the system submenu. The items available under this command are shown below.

lastpw          Displays the last debug password.
config          Goes to the config submenu.
logs            Goes to the logs submenu.
ntp             Goes to the NTP submenu.
snmp            Goes to the SNMP submenu.
userdb          Goes to the userdb submenu.
radius          Goes to the RADIUS submenu.
ws2000          Goes to the WS2000 submenu.
authentication  Goes to the authentication submenu.
ssh             Goes to the SSH submenu.
redundancy      Goes to the redundancy submenu.
save            Saves the configuration to system flash.
quit            Quits the CLI.
..              Goes to the parent menu.
/               Goes to the root menu.
WS2000>admin(system)> lastpw

Description:

This command displays the MAC address for the switch, the previous admin password for the switch, and the number of times the current admin password has been used along with how many more times it will be valid.

Syntax:

lastpw  Gets the last password of the system.

Example:

    admin(system)> lastpw

    WS2000  MAC Address is 00:a0:f8:6f:d8:fc
    Last Password was symbol12
    Current password used 0 times, valid 4 more time(s)
13.33 System Authentication Commands

WS2000>admin(system)> authentication

Description:

Displays the authentication submenu. The items available under this command are shown below.

radius       Goes to the RADIUS submenu.
save         Saves the configuration to system flash.
show         Shows the authentication parameters.
..            Goes to the parent menu.
/             Goes to the root menu.
WS2000>admin(system.authentication)> set

Description:

Sets the parameter that specifies how user authentication is taking place.

Syntax:

set mode local / radius  Sets the authentication mode. If set to local, the internal User Database will serve as the data source. If set to radius, the switch will use an external LDAP server for the information. If radius is the mode, then the parameters under the radius submenu must to be set.

Example:

admin(system.authentication)> set mode local
admin(system.authentication)> show all
  authentication mode : local
admin(system.authentication)>

Related Commands:

radius--> set  Sets the parameters to specify that the external RADIUS server is used for user authentication.
WS2000>admin(system.authentication)> show

Description:

Shows the main user authentication parameters.

Syntax:

show all          Displays the user authentication settings.

Example:

admin(system.authentication)>set mode local
admin(system.authentication)>show all
  authentication mode : local
admin(system.authentication)> 

Related Commands:

set          Sets the authentication parameters.
13.34 System Authentication RADIUS Commands

WS2000>admin(system.authentication)> radius

Description:

Displays the RADIUS submenu. The items available under this command are shown below.

- **set**: Sets the RADIUS authentication parameters.
- **show**: Shows the RADIUS authentication parameters.
- **save**: Saves the configuration to system flash.
- ..: Goes to the parent menu.
- /: Goes to the root menu.
WS2000>admin(system.authentication.radius)> set

**Description:**
Sets the RADIUS proxy server authentication parameters.

**Syntax:**
- **set auth-server-ip** `<IP>`
- **auth-server-port** `<port>`
- **shared-secret** `<password>`

- Sets the IP address for the RADIUS authentication proxy server.
- Specifies the TCP/IP port number for the RADIUS server that will be acting as a proxy server. The default port is 1812.
- Sets a shared secret to be used for each suffix that will be used for authentication with the RADIUS proxy server.

**Example:**
```
admin(system.authentication.radius)>set auth-server-ip 192.168.0.4
admin(system.authentication.radius)>set auth-server-port 1812
admin(system.authentication.radius)>set shared mysecret
admin(system.authentication.radius)>
admin(system.authentication.radius)>show all
  radius server ip          : 192.168.0.4
  radius server port        : 1812
  radius server shared secret : ********
```
WS2000>admin(system.authentication.radius)> show

Description:

Shows the RADIUS authentication parameters.

Syntax:

show       Displays the RADIUS proxy server parameters.

Example:

admin(system.authentication.radius)>set auth-server-ip 192.168.0.4
admin(system.authentication.radius)>set auth-server-port 1812
admin(system.authentication.radius)>set shared mysecret

admin(system.authentication.radius)>show all
  radius server ip      : 192.168.0.4
  radius server port    : 1812
  radius server shared secret : ********

Related Commands:

set       Sets the RADIUS authentication parameters.
13.35 System Configuration Commands

WS2000>admin(system)> config

Description:
Displays the config submenu.

Syntax:

default  Restores default configuration.
default  Exports configuration from the system.
import   Imports configuration to the system.
import   Restores partial default configuration.
set      Sets import/export parameters.
show     Shows import/export parameters.
update   Performs firmware update.
save     Saves the configuration to system flash.
quit     Quits the CLI.
..       Goes to the parent menu.
/        Goes to the root menu.
WS2000>admin(system.config)> default

**Description:**
Restores the factory default configuration.

**Syntax:**
default  
Restores the switch to the original (factory default) configuration.

**Example:**
admin(system.config)>default

******************************************************************************
System will now restore default configuration. You will need to set the
country code for correct operation.
******************************************************************************
WS2000>admin(system.config)> export

**Description:**

Exports the configuration from the system.

**Syntax:**

`export`  
Exports the configuration to the FTP server. Use the set command to set the server, user, password, and file name before using this command.

`tftp`  
Exports the configuration to the TFTP server. Use the set command to set the IP address for the TFTP server before using the command.

`terminal`  
Exports the configuration to the terminal.

**Example:**

Export FTP Example:

```
admin(system.config)>set server 192.168.22.12
admin(system.config)>set user myadmin
admin(system.config)>set passwd
```

```
admin(system.config)>export ftp
Export operation : [ Started ]
Building configuration file : [ Done ]
File transfer : [ In progress ]
File transfer : [ Done ]
Export operation : [ Done ]
```

Export TFTP Example:

```
admin(system.config)>set server 192.168.0.101
admin(system.config)>export tftp
```

```
Export operation : [ Started ]
Building configuration file : [ Done ]
File transfer : [ In progress ]
File transfer : [ Done ]
Export operation : [ Done ]
```

Export Terminal Example:

```
admin(system.config)>export terminal
//
// WS2000 Configuration Command Script
// System Firmware Version: 1.5.0.0-160b
//
system
```
ws2000
// WS2000 menu
set name WS2000
set loc Extra\20office
set email fred@symbol.com
set cc us
set airbeam mode disable
set airbeam enc-passwd a11e00942773
set applet lan enable
set applet wan enable
set applet slan enable
set applet swan enable
set cli lan enable
set cli wan enable
set snmp lan enable
set snmp wan enable
/
system
config
--More--
...<several pages of settings>
/
// Router configuration
network
router
set type off
set dir both
set auth none
set enc-passwd 8e57
set id 1 1
set enc-key 1 e2565fc57c2a766fb0d55160d6f92952
set id 2 1
set enc-key 2 e2565fc57c2a766fb0d55160d6f92952
delete all
/
save
**WS2000>admin(system.config)> import**

**Description:**
Imports the configuration to the system.

**Syntax:**

```
import ftp
```
Imports the configuration from the FTP server. Use the set command to set the server, user, password, and file.

```
tftp
```
Imports the configuration from the TFTP server. Use the set command to set the server and file.

**Example:**

Import FTP Example

```bash
admin(system.config)> set server 192.168.22.12
admin(system.config)> set user myadmin
admin(system.config)> set passwd mysecret
admin(system.config)> import ftp
```

Import operation : [ Started ]
File transfer : [ In progress ]
File transfer : [ Done ]
Import operation : [ Done ]

Import TFTP Example

```bash
admin(system.config)> set server 192.168.0.101
admin(system.config)> import tftp
```

Import operation : [ Started ]
File transfer : [ In progress ]
File transfer : [ Done ]
Import operation : [ Done ]
WS2000>admin(system.config)> partial

Description:

Resets the switch’s configuration to the factory default settings for all settings except the WAN and some SNMP related settings. The following settings will remain intact when using Restore Partial Default Configuration:

- All settings on the WAN page
- SNMP access to the WS 2000 on the WS 2000 Access page
- All settings on the SNMP Access page

Before using this feature, consider exporting the current configuration for safekeeping.

Syntax:

- partial Restores part of the system configuration.

Related Commands:

- export Exports system configuration settings.
WS2000>admin(system.config)> set

Description:

Sets the import/export parameters.

Syntax:

`set server <ipaddress>`
Sets the FTP/TFTP server IP address (a.b.c.d).

`user <username>`
Sets the FTP user name (up to 47 characters).

`passwd <pswd>`
Sets the FTP password (up to 39 characters).

`file <filename>`
Sets the configuration file name (up to 39 characters).

`fw file <filename>`
Sets the firmware filename (up to 39 characters).

`path <pathname>`
Sets the firmware file path (up to 39 characters).

Example:

FTP Set Example

admin(system.config)> set server 192.168.22.12
admin(system.config)> set user myadmin
admin(system.config)> set passwd

admin(system.config)> export ftp

Export operation : [ Started ]
Building configuration file : [ Done ]
File transfer : [ In progress ]
File transfer : [ Done ]
Export operation : [ Done ]

Firmware Example

admin(system.config)> set fw file mf_0105000160B.bin
admin(system.config)> set fw path /tftp/myadmin/
admin(system.config)> update tftp s1
**WS2000>admin(system.config)> show**

**Description:**

Shows the import/export parameters.

**Syntax:**

`show all` Shows all import/export parameters.

**Example:**

```
admin(system.config)>show all

ftp/tftp server ip address : 192.168.0.101
ftp user name : myadmin
ftp password : ********
cfg filename : cfg.txt
firmware filepath : /tfpt/myadminplace/
firmware filename : mf.bin
```
WS2000>admin(system.config)> update

Description:
Performs a firmware update.

Syntax:

update tftp/ftp <iface>  
Sets how firmware updates will occur. Select between ftp and tftp. 
<iface> specifies the interface (location), as follows:
s1 = subnet1
s2 = subnet2
s3 = subnet3
s4 = subnet4
w = wan

Note: Before using this command, use set server to set the IP address for the FTP/TFTP server. If using the ftp mode, also use set user and set passwd to allow login to the FTP server.

cf  
Indicates that firmware updates will occur from the switch’s compact flash slot. (Undoes an ftp/tftp setting.)

Example:

admin(system.config)>set fw file mf_01050000200B.bin
admin(system.config)>set fw path /tftp/myadmin/
admin(system.config)>update tftp s1
13.36 System Logs Commands

**WS2000>admin(system)> logs**

**Description:**
Displays the logs submenu.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>delete</td>
<td>Deletes core files.</td>
</tr>
<tr>
<td>set</td>
<td>Sets log options and parameters.</td>
</tr>
<tr>
<td>send</td>
<td>Sends log and core files.</td>
</tr>
<tr>
<td>show</td>
<td>Shows logging options.</td>
</tr>
<tr>
<td>view</td>
<td>Views system log.</td>
</tr>
<tr>
<td>save</td>
<td>Saves configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(system.logs)> delete

**Description:**

Deletes the core log files.

**Syntax:**

`delete` Deletes the core system log files.

**Example:**

```
admin(system.logs)>delete
```
WS2000>admin(system.logs)> send

**Description:**
Sends log and core files.

**Syntax:**
```
send
```
Sends the system log file via FTP to a location specified with the set command. Use the set command to set the FTP login and site information.

**Example:**
```
admin(system.logs)>set user fred
admin(system.logs)>set passwd mygoodness
admin(system.logs)>show all

log level : L6 Info
ext syslog server logging : disable
ext syslog server ip address : 0.0.0.0
ftp/tftp server ip address : 192.168.0.10
ftp user name : fred
ftp password : ********

admin(system.logs)>send

File transfer : [ In progress ]

File transfer : [ Done ]

admin(system.logs)>
```

**Related Commands:**
- `set`  Sets the parameters associated with log operations, such as send.
- `show all`  Displays the log related settings.
**WS2000>admin(system.logs)> set**

**Description:**
Sets log options and parameters.

**Syntax:**
```
set ipadr <ip>          Sets the external syslog server IP address to <ip> (a.b.c.d).
set level <level>      Sets the level of the events that will be logged. All event with a level at or above <level> (L0–L7) will be saved in the system log.
                        L0:Emergency
                        L1:Alert
                        L2:Critical
                        L3:Errors
                        L4:Warning
                        L5:Notice
                        L6:Info
                        L7:Debug
set mode enable/disable Enables or disables ext syslog server logging.
set server <a.b.c.d>  Sets the FTP server IP address.
set user <username>   Sets the FTP user name (1–47 characters).
set passwd <password> Sets the FTP password (1–39 characters).
```

**Example:**

```
admin(system.logs)>set user fred
admin(system.logs)>set passwd mygoodness
admin(system.logs)>show all

log level                : L6 Info
ext syslog server logging: disable
ext syslog server ip address : 0.0.0.0
ftp/tftp server ip address : 192.168.0.10
ftp user name             : fred
ftp password              : ********
```
WS2000>admin(system.logs)> show

Description:

Shows logging options.

Syntax:

show all Displays all of the logging options.

Example:

admin(system.logs)>set user fred
admin(system.logs)>set password mygoodness

unknown input before marker
set password mygoodness
^
admin(system.logs)>set passwd mygoodness
admin(system.logs)>show all

log level : L6 Info
ext syslog server logging : disable
ext syslog server ip address : 0.0.0.0
ftp/tftp server ip address : 192.168.0.10
ftp user name : fred
ftp password : ********

Related Commands:

set Sets logging parameters to be used with send.
**Description:**

Views the system log file.

**Syntax:**

```plaintext
view
```

Views the system log file.

**Example:**

```
admin(system.logs)> view

Jan  7 16:14:00 (none) syslogd 1.4.1: restart (remote reception).
Jan  7 16:14:10 (none) klogd: :ps log:fc: queue maintenance
Jan  7 16:15:43 (none) last message repeated 2 times
Jan  7 16:16:01 (none) CC:  4:16pm  up 6 days, 16:16, load average: 0.00, 0.01, 0.0
Jan  7 16:16:01 (none) CC:  Mem:   62384   32520   29864
Jan  7 16:16:01 (none) CC:        0        0
Jan  7 16:16:01 (none) CC: 0000077e  0012e95b 0000d843 00000000 00000003 0000121
Jan  7 16:16:01 (none) CC: 00000000 00000000 0037ebf7 000034dc 00000000 00000000 00000000
Jan  7 16:17:15 (none) klogd: :ps log:fc: queue maintenance
Jan  7 16:17:15 (none) klogd: :ps log:fc: queue maintenance

...
13.37 System NTP Commands

WS2000>admin(system)> ntp

Description:
Displays the NTP submenu.

Syntax:

show     Shows NTP parameters settings.
set      Sets NTP parameters.
save     Saves the configuration to system flash.
quit     Quits the CLI.
..       Goes to the parent menu.
/        Goes to the root menu.
**WS2000>admin(system.ntp)> set**

**Description:**
Sets NTP parameters.

**Syntax:**

```
set mode enable/disable
intrvl <time>
server <idx> <ip>
port <idx> <port>
```

- `set mode enable/disable`: Enables or disables NTP.
- `intrvl <time>`: Sets the length of time `<time>`, in minutes, for the switch to synchronize its time with an NTP server.
- `server <idx> <ip>`: Sets the NTP server IP address `<ip>` (a.b.c.d); specify one of the three NTP servers with `<idx>` (1, 2, or 3).
- `port <idx> <port>`: Sets the NTP port for the indicated server `<idx>` to `<port>` (1–65535).

**Example:**

```
admin(system.ntp)> set mode enable
admin(system.ntp)> set server 1 203.21.37.18
admin(system.ntp)> set port 1 345

admin(system.ntp)> show all
```

```
ntp mode : enable
server ip 1 : 203.21.37.18
server ip 2 : 0.0.0.0
server ip 3 : 0.0.0.0
server port 1 : 345
server port 2 : 123
server port 3 : 123
current time : 1970-01-07 23:29:05
```

`admin(system.ntp)>`
WS2000>admin(system.ntp)> show

Description:
Shows NTP parameters.

Syntax:
show all Shows all NTP server settings.

Example:

    admin(system.ntp)> show all

    ntp mode : enable
    server ip 1 : 114.233.112.4
    server ip 2 : 0.0.0.0
    server ip 3 : 0.0.0.0
    server port 1 : 123
    server port 2 : 123
    server port 3 : 123
    current time : 2004-10-07 22:58:24

Related Commands:
set Sets NTP parameters.
13.38 System RADIUS Commands

**WS2000>admin(system)> radius**

**Description:**

Displays the RADIUS submenu. The items available under this command are shown below.

- **eap**  
  Goes to the EAP submenu.

- **policy**  
  Goes to the access policy submenu.

- **ldap**  
  Goes to the LDAP submenu.

- **proxy**  
  Goes to the proxy submenu.

- **client**  
  Goes to the client submenu.

- **set**  
  Sets the RADIUS parameters.

- **show**  
  Shows the RADIUS parameters.

- **save**  
  Saves the configuration to system flash.

- **quit**  
  Quits the CLI.

- **..**  
  Goes to the parent menu.

- **/**  
  Goes to the root menu.
WS2000>admin(system.radius)> set

Description:
Sets the RADIUS database.

Syntax:
set database local / ldap

Sets the RADIUS server to either the local database or an LDAP server.

Example:
admin(system.radius)>set database ldap
admin(system.radius)>show all
Database : ldap

Related Commands:

show all  Shows the top-level RADIUS parameters.
WS2000>admin(system.radius)> show

**Description:**

Shows the RADIUS parameters.

**Syntax:**

```
show all
```

Displays the RADIUS database setting.

**Example:**

```
admin(system.radius)>set database ldap
admin(system.radius)>show all
```

```
Database : ldap
```

**Related Commands:**

```
set
```

Sets the RADIUS database source.
13.39 System RADIUS Client Commands

WS2000>admin(system.radius)> client

Description:

Displays the client submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds a RADIUS client.</td>
</tr>
<tr>
<td>del</td>
<td>Deletes a RADIUS client.</td>
</tr>
<tr>
<td>show</td>
<td>Displays a list of configured clients.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(system.radius.client)> add

Description:

Adds a RADIUS client.

Syntax:

add <ip> <mask> <secret> Adds a RADIUS client with IP address <ip>, netmask <mask>, and shared secret <secret>.

Example:

admin(system.radius.client)> add 192.168.46.4 225.225.225.0 mysecret
admin(system.radius.client)> show

List of Radius Clients:

<table>
<thead>
<tr>
<th>Idx</th>
<th>Subnet/Host</th>
<th>Netmask</th>
<th>SharedSecret</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.46.4</td>
<td>225.225.225.0</td>
<td>****</td>
</tr>
</tbody>
</table>

Related Commands:

del Deletes a RADIUS client.
show Shows a list of RADIUS clients.
WS2000>admin(system.radius.client)> del

Description:
Deletes a RADIUS client.

Syntax:
del <ip> Deletes the RADIUS client with IP address <ip>.

Example:
admin(system.radius.client)> show
List of Radius Clients:

<table>
<thead>
<tr>
<th>Idx</th>
<th>Subnet/Host</th>
<th>Netmask</th>
<th>SharedSecret</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.46.4</td>
<td>225.225.225.0</td>
<td>****</td>
</tr>
<tr>
<td>2</td>
<td>192.168.101.43</td>
<td>225.225.225.0</td>
<td>****</td>
</tr>
</tbody>
</table>

admin(system.radius.client)> del 192.168.46.4
admin(system.radius.client)> show
List of Radius Clients:

<table>
<thead>
<tr>
<th>Idx</th>
<th>Subnet/Host</th>
<th>Netmask</th>
<th>SharedSecret</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.101.43</td>
<td>225.225.225.0</td>
<td>****</td>
</tr>
</tbody>
</table>

Related Commands:
add  Adds a RADIUS client to the list.
show Displays the list of RADIUS clients.
WS2000>admin(system.radius.client)> show

Description:
Displays a list of configured clients.

Syntax:

Example:

admin(system.radius.client)>show
List of Radius Clients :

<table>
<thead>
<tr>
<th>Idx</th>
<th>Subnet/Host</th>
<th>Netmask</th>
<th>SharedSecret</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.46.4</td>
<td>225.225.225.0</td>
<td>*****</td>
</tr>
<tr>
<td>2</td>
<td>192.168.101.43</td>
<td>225.225.225.0</td>
<td>*****</td>
</tr>
</tbody>
</table>

Related Commands:

add    Adds a RADIUS client to the list.

del    Deletes a RADIUS client from the list.
13.40 System RADIUS EAP Commands

WS2000>admin(system.radius)> eap

Description:

Displays the EAP submenu. The items available under this command are shown below.

- `peap`        Goes to the PEAP submenu.
- `ttls`        Goes to the TTLS submenu.
- `import`      Imports the EAP certificates.
- `set`         Sets the EAP parameters.
- `show`        Shows the EAP parameters.
- `save`        Saves the configuration to system flash.
- `quit`        Quits the CLI.
- `..`          Goes to the parent menu.
- `/`           Goes to the root menu.
**WS2000>admin(system.radius.eap)> import**

**Description:**
Imports the EAP certificates.

**Syntax:**

```
import server <cert id>  Imports a server certificate with the certificate ID <cert id>.
sacert <cert id>       Imports a Trusted Certificate with certificate ID <cert id>.
```

**Example:**

```
admin(system.radius.eap)>import server mycert
admin(system.radius.eap)>import cacert NETE3443
```

**Related Commands:**

```
show cert  Show the list of certificates.
```
WS2000>admin(system.radius.eap)> set

Description:

Sets the EAP parameters.

Syntax:

```
set auth peap/ttls
```

Sets the default authorization type to one of **PEAP** or **TTLS**. When selected, go to the submenu associated with the selection to finish the setup.

Example:

```
admin(system.radius.eap)>set auth peap
admin(system.radius.eap)>show all
Default EAP Type : peap
```

Related Commands:

```
show all
```

Shows the EAP settings.
WS2000>admin(system.radius.eap)> show

**Description:**

Shows the EAP parameters.

**Syntax:**

```
show all            Displays the default EAP authentication settings.
cert               Displays a list of certificates.
```

**Example:**

```
admin(system.radius.eap)>set auth peap
admin(system.radius.eap)>show all
Default EAP Type : peap
```

**Related Commands:**

```
set                Sets the EAP parameters.
```
13.41 System RADIUS EAP PEAP Commands

WS2000>admin(system.radius.eap)> peap

Description:

Displays the PEAP submenu. The items available under this command are shown below.

- **set**: Sets the PEAP authentication type.
- **show**: Shows the PEAP authentication type.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
WS2000>admin(system.radius.eap.peap)> set

Description:
Sets the PEAP authentication type.

Syntax:
set auth gtc / mschapv2  
Sets the authentication type for PEAP to one of GTC or MTCHAPv2.

Example:
admin(system.radius.eap.peap)>set auth gtc
admin(system.radius.eap.peap)>show
PEAP Auth Type : gtc

Related Commands:
show                 Displays the PEAP authentication type.
**WS2000>admin(system.radius.eap.peap)> show**

**Description:**

Shows the PEAP authentication type.

**Syntax:**

```
show
```

Displays the PEAP authentication type.

**Example:**

```
admin(system.radius.eap.peap)>set auth gtc
admin(system.radius.eap.peap)>show
```

```
PEAP Auth Type : gtc
```

**Related Commands:**

```
set
```

Sets the PEAP authentication type.
13.42 System RADIUS EAP TTLS Commands

WS2000>admin(system.radius.eap)> ttls

Description:

Displays the TTLS submenu. The items available under this command are shown below.

- **set**: Sets the TTLS authentication type.
- **show**: Shows the TTLS authentication type.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- `..`: Goes to the parent menu.
- `/`: Goes to the root menu.
WS2000>admin(system.radius.eap.ttls)> set

Description:
Sets the TTLS authentication type.

Syntax:
```
set auth pap / md5 / mschapv2
```
Sets the authentication type for TTLS to one of PAP, MD5, or MSCHAPv2.

Example:
```
admin(system.radius.eap.ttls)>set auth md5
admin(system.radius.eap.ttls)>show
TTLS Auth Type : md5
```

Related Commands:
```
show       Show the TTLS authentication type.
```
WS2000>admin(system.radius.eap.ttls)> show

Description:
Shows the TTLS authentication type.

Syntax:

**show**
Displays the TTLS authentication type.

Example:

```
admin(system.radius.eap.ttls)>set auth md5
admin(system.radius.eap.ttls)>show
TTLs Auth Type : md5
```

Related Commands:

**set**
Sets the TTLS authentication type.
13.43 System RADIUS LDAP Commands

WS2000>admin(system.radius)> ldap

Description:

Displays the LDAP submenu. The items available under this command are shown below.

- **set**  Sets the LDAP parameters.
- **show** Shows the LDAP parameters.
- **save**  Saves the configuration to system flash.
- **quit**  Quits the CLI.
- **..**    Goes to the parent menu.
- **/**     Goes to the root menu.
WS2000>admin(system.radius.ldap)> set

Description:
Sets the LDAP parameters.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set ipadr &lt;ip&gt;</td>
<td>Sets LDAP server IP address to &lt;ip&gt;.</td>
</tr>
<tr>
<td>port &lt;port&gt;</td>
<td>Sets LDAP server port to &lt;port&gt;.</td>
</tr>
<tr>
<td>binddn &lt;binddn&gt;</td>
<td>Sets LDAP bind distinguished name to &lt;binddn&gt; (a string of characters).</td>
</tr>
<tr>
<td>basedn &lt;basedn&gt;</td>
<td>Sets LDAP Base distinguished name to &lt;basedn&gt; (a string of characters).</td>
</tr>
<tr>
<td>passwd &lt;password&gt;</td>
<td>Sets LDAP server password to &lt;password&gt; (a string of characters).</td>
</tr>
<tr>
<td>login &lt;logattr&gt;</td>
<td>Sets LDAP login attribute to &lt;logattr&gt; (a string of characters).</td>
</tr>
<tr>
<td>pass_attr &lt;passattr&gt;</td>
<td>Sets LDAP password attribute to &lt;passattr&gt; (a string of characters).</td>
</tr>
<tr>
<td>groupname &lt;gname attr&gt;</td>
<td>Sets LDAP group name attribute to &lt;gname attr&gt; (a string of characters).</td>
</tr>
<tr>
<td>filter</td>
<td>Sets LDAP membership filter with appropriate settings</td>
</tr>
<tr>
<td>membership &lt;groupattr&gt;</td>
<td>Sets LDAP membership attribute to &lt;groupattr&gt; (a string of characters).</td>
</tr>
</tbody>
</table>

Example:

```
admin(system.radius.ldap)>set ipadr 192.168.42.23
admin(system.radius.ldap)>set port 356
admin(system.radius.ldap)>show all
LDAP Server IP : 192.168.42.23
LDAP Server Port : 56
LDAP Bind DN : dfkjkkj
LDAP Base DN : o=mobion
LDAP Login Attribute : (uid=%{Stripped-User-Name:-%{User-Name}})
LDAP Password Attribute : userPassword
LDAP Group Name Attribute : cn
LDAP Group Membership Filter : 
LDAP Group Membership Attribute : mygroup
admin(system.radius.ldap)>
```

Related Commands:

show Displays the set of LDAP server settings.
WS2000>admin(system.radius.ldap)> show

Description:

Shows the LDAP parameters.

Syntax:

show all Displays the list of LDAP parameters.

Example:

admin(system.radius.ldap)>set ipadr 192.168.42.23
admin(system.radius.ldap)>set port 356
admin(system.radius.ldap)>show all
LDAP Server IP : 192.168.42.23
LDAP Server Port : 356
LDAP Bind DN : dfkJkKj
LDAP Base DN : o=mobion
LDAP Login Attribute : (uid=%{Stripped-User-Name:-%{User-Name}})
LDAP Password Attribute : userPassword
LDAP Group Name Attribute : cn
LDAP Group Membership Filter :
LDAP Group Membership Attribute : mygroup
admin(system.radius.ldap)>

Related Commands:

set Sets the LDAP parameters.
13.44 System RADIUS Policy Commands

WS2000>admin(system.radius)> policy

Description:
Displays the policy submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Sets the group’s access policy.</td>
</tr>
<tr>
<td>show</td>
<td>Shows the group’s access policy.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(system.radius.policy)> set

Description:
Sets the group’s access to WLANs.

Syntax:

set <group> <idx list> Gives group <group> access to WLAN with a list of indexes <idx list>. The list can be either a single index or several indexes separated by spaces. The group must be already defined. See System User Database Group Commands for information about adding groups.

Example:

admin(system.radius.policy)> set g1 2 3 4
admin(system.radius.policy)> show
List of Access Policies :
   g1                   : 2 3 4
   g2                   : No Wlans

Related Commands:

show Displays the group’s access policies.
WS2000>admin(system.radius.policy)> show

Description:

Shows the group's access policy.

Syntax:

show Displays the group access settings.

Example:

admin(system.radius.policy)>set g1 2 3 4
admin(system.radius.policy)>show

List of Access Policies :

g1 : 2 3 4

g2 : No Wlans

Related Commands:

set Sets the group WLAN access settings.
### 13.45 System RADIUS Proxy Commands

**WS2000>admin(system.radius)> proxy**

**Description:**
Displays the proxy submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds a proxy realm.</td>
</tr>
<tr>
<td>del</td>
<td>Deletes a proxy realm.</td>
</tr>
<tr>
<td>set</td>
<td>Sets the proxy server parameters.</td>
</tr>
<tr>
<td>show</td>
<td>Shows the proxy server parameters.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(system.radius.proxy)> add

Description:

Adds a proxy realm.

Syntax:

add <realm> <ip> <port> <secret>  Add a proxy realm with realm name <realm>, RADIUS server IP address <ip>, port <port>, and shared secret <secret>.

Example:

admin(system.radius.proxy)>add realm1 192.168.102.42 225 realmpass
admin(system.radius.proxy)>show realm
Proxy Realms :

<table>
<thead>
<tr>
<th>Idx</th>
<th>Suffix</th>
<th>RadiusServerIP</th>
<th>Port</th>
<th>SharedSecret</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>realm1</td>
<td>192.168.102.42</td>
<td>225</td>
<td>*****</td>
</tr>
</tbody>
</table>

Related Commands:

show realm  Displays this list of defined proxy servers.
del  Deletes a proxy server from the list.
**WS2000>admin(system.radius.proxy)> del**

**Description:**

Deletes a proxy realm.

**Syntax:**

```
del <realm>  Deletes a proxy server realm with name <realm>.
```

**Example:**

```
admin(system.radius.proxy)>add realm1 192.168.102.42 225 realmpass
admin(system.radius.proxy)>show realm
Proxy Realms:

Idx  Suffix        RadiusServerIP    Port  SharedSecret
-------------------------------------------------------------------------------
1    realm1        192.168.102.42    225   *****
```

```
admin(system.radius.proxy)>del realm1
admin(system.radius.proxy)>show realm
Proxy Realms:

Idx  Suffix        RadiusServerIP    Port  SharedSecret
-------------------------------------------------------------------------------
```

**Related Commands:**

- **add** Adds a proxy server realm.
- **show** Displays the list of proxy servers.
**WS2000>admin(system.radius.proxy)> set**

**Description:**
Sets the proxy server parameters.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set delay &lt;delay&gt;</td>
<td>Sets the retry delay of the proxy server to &lt;delay&gt; minute (5–10).</td>
</tr>
<tr>
<td>count &lt;count&gt;</td>
<td>Sets the retry count of the proxy server to &lt;count&gt; (3–6).</td>
</tr>
</tbody>
</table>

**Example:**

```plaintext
admin(system.radius.proxy)> set delay 7
admin(system.radius.proxy)> set count 4
admin(system.radius.proxy)> show proxy
Proxy Server Retry Count : 4
Proxy Server Retry Delay : 7
```

**Related Commands:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show proxy</td>
<td>Shows the proxy server retry settings.</td>
</tr>
</tbody>
</table>
WS2000>admin(system.radius.proxy)> show

Description:

Shows the proxy server parameters.

Syntax:

show proxy realms

Displays the proxy server parameters.

Displays proxy server realm information.

Example:

admin(system.radius.proxy)>add realm1 192.168.102.42 225 realmpass
admin(system.radius.proxy)>show realm
Proxy Realms :

<table>
<thead>
<tr>
<th>Idx</th>
<th>Suffix</th>
<th>RadiusServerIP</th>
<th>Port</th>
<th>SharedSecret</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>realm1</td>
<td>192.168.102.42</td>
<td>225</td>
<td>****</td>
</tr>
</tbody>
</table>

admin(system.radius.proxy)>set delay 7
admin(system.radius.proxy)>set count 4
admin(system.radius.proxy)>show proxy
Proxy Server Retry Count : 4
Proxy Server Retry Delay : 7

Related Commands:

set Sets the proxy server retry parameters.
add Adds a proxy server realm to the list.
13.46 System Redundancy Commands

WS2000>admin(system)> redundancy

Description:
Displays the redundancy submenu. The items available under this command are shown below.

- **set**: Sets redundancy parameters.
- **show**: Shows redundancy settings.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
WS2000>admin(system.redundancy) > set

**Description:**

Sets the parameters for redundant switch mode.

**Syntax:**

```
set mode primary / standby
op-state upgrade / standalone / redundancy
heartbeat <interval>
revertdelay <delay>
hb_interface <port>
```

**Example:**

```
admin(system.redundancy) > set mode standby

can not set the value when the op_state is either upgrade or standalone

admin(system.redundancy) > set op-state redundancy
admin(system.redundancy) > set mode standby
admin(system.redundancy) >
```

**Related Commands:**

```
show
```

Displays the redundancy settings.
**WS2000>admin(system.redundancy)> show**

**Description:**
Displays the switch redundancy settings.

**Syntax:**

```
show all
```

Displays the switch redundancy settings.

**Example:**

```
admin(system.redundancy)>show all
```

- redundancy configured mode : primary
- redundancy operational mode : VRRP daemon not running
- redundancy operational state : standalone
- heart beat interval : 3 seconds
- revert delay : 5 minutes
- heart beat interface : 1

**Related Commands:**

```
set
```
Sets the redundancy settings.
13.47 System SNMP Commands

WS2000>admin(system)> snmp

Description:
Displays the SNMP submenu. The items available under this command are shown below.

- **access**: Goes to the SNMP access submenu.
- **traps**: Goes to the SNMP traps submenu.
- **save**: Saves the configuration to system flash.
- **quit**: Quits the CLI.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
13.48 System SNMP Access Commands

WS2000>admin(system.snmp)> access

Description:

Displays the SNMP access menu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds SNMP access entries.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes SNMP access entries.</td>
</tr>
<tr>
<td>list</td>
<td>Lists SNMP access entries.</td>
</tr>
<tr>
<td>show</td>
<td>Shows SNMP v3 engine ID.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(system.snmp.access)> add

Description:

Adds SNMP access entries.

Syntax:

add acl <ip1> <ip2> Adds an entry to the SNMP access control list with <ip1> as the starting IP address and <ip2> and the ending IP address.

v1v2c <comm> ro/rw <oid>/all

Adds an SNMP v1/v2c configuration with <comm> as the community (1–31 characters), the read/write access set to ro (read only) or rw (read/write), and the Object Identifier <oid> (a string of 1–127 numbers separated by dot, such as 2.3.4.5.6 or all for all objects).

v3 <user> ro/rw <oid>/all <sec> des/aes <pass1> <pass2>

Adds an SNMP v3 user definition with the username <user> (1–31 characters), access set to ro (read only) or rw (read/write), the object ID set to <oid> (1–127 chars in dot notation, such as 1.3.6.1 or all for all objects), the security type <sec> set to one of none, auth, or auth/priv.

The following parameters must be specified if <sec> is set to auth/priv:
- Privacy algorithm set to des or aes
- Privacy password <pass2> (8–31 chars)

Example:

admin(system.snmp.access)>add acl 209.236.24.1 209.236.24.46
admin(system.snmp.access)>list acl

------------------------------------------------------------------
index start ip end ip
------------------------------------------------------------------
1 209.236.24.1 209.236.24.46
------------------------------------------------------------------

admin(system.snmp.access)>add v3 fred rw 1.3.6.6 none
admin(system.snmp.access)>list v3 all

index : 1
username : fred
access permission : read/write
object identifier : 1.3.6.6
security level : none
auth algorithm : md5
auth password : ********
privacy algorithm : des
privacy password : ********
admin(system.snmp.access)>add v3 judy rw 1.3.6.1 auth/priv md5 changeme des changemetoo

admin(system.snmp.access)>list v3 2

<table>
<thead>
<tr>
<th>index</th>
<th>: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>: judy</td>
</tr>
<tr>
<td>access permission</td>
<td>: read/write</td>
</tr>
<tr>
<td>object identifier</td>
<td>: 1.3.6.1</td>
</tr>
<tr>
<td>security level</td>
<td>: auth/priv</td>
</tr>
<tr>
<td>auth algorithm</td>
<td>: md5</td>
</tr>
<tr>
<td>auth password</td>
<td>: ********</td>
</tr>
<tr>
<td>privacy algorithm</td>
<td>: des</td>
</tr>
<tr>
<td>privacy password</td>
<td>: ********</td>
</tr>
</tbody>
</table>
WS2000>admin(system.snmp.access)> delete

Description:
Deletes SNMP access entries.

Syntax:

delete acl <idx> Deletes entry <idx> from the access control list.
all Deletes all entries from the access control list.

v1v2c <idx> Deletes entry <idx> from the v1/v2 configuration list.
all Deletes all entries from the v1/v2 configuration list.

v3 <idx> Deletes entry <idx> from the v3 user definition list.
all Deletes all entries from the v3 user definition list.

Example:
admin(system.snmp.access)>list acl
INDEX  START IP  END IP
--- ------------------ ------------------
1  209.236.24.1  209.236.24.46

admin(system.snmp.access)>delete acl all
admin(system.snmp.access)>list acl
INDEX  START IP  END IP
--- ------------------ ------------------

admin(system.snmp.access)>list v3 all
INDEX USER NAME  ACCESS PERMISSION  OBJECT IDENTIFIER  SECURITY LEVEL  AUTH ALGORITHM  AUTH PASSWORD  PRIVACY ALGORITHM  PRIVACY PASSWORD
--- ------------------ ------------------ ------------------ ------------------ ------------------ ------------------ ------------------ ------------------
1 fred read/write 1.3.6.6 none md5 ******** des ********
2 judy read/write 1.3.6.1 auth/priv md5 ********
auth password : *******
privacy algorithm : des
privacy password : *******

admin(system.snmp.access)>delete v3 2
admin(system.snmp.access)>list v3 all

index : 1
username : fred
access permission : read/write
object identifier : 1.3.6.6
security level : none
auth algorithm : md5
auth password : *******
privacy algorithm : des
privacy password : *******

admin(system.snmp.access)>
WS2000>admin(system.snmp.access)> list

Description:
Lists SNMP access entries.

Syntax:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Lists SNMP access control list entries.</td>
</tr>
<tr>
<td>v1v2c</td>
<td>Lists SNMP v1/v2c configuration.</td>
</tr>
<tr>
<td>v3 &lt;idx&gt;</td>
<td>Lists SNMP v3 user definition with index &lt;idx&gt;.</td>
</tr>
<tr>
<td>all</td>
<td>Lists all SNMP v3 user definitions.</td>
</tr>
</tbody>
</table>

Example:

```shell
admin(system.snmp.access)>list acl
----------------------------------------------------------------
<table>
<thead>
<tr>
<th>index</th>
<th>start ip</th>
<th>end ip</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>209.236.24.1</td>
<td>209.236.24.46</td>
</tr>
</tbody>
</table>

admin(system.snmp.access)>list v3 all

index : 1
username : fred
access permission : read/write
object identifier : 1.3.6.6
security level : none
auth algorithm : md5
auth password : ********
privacy algorithm : des
privacy password : ******
```

```shell
admin(system.snmp.access)>list v3 2

index : 2
username : judy
access permission : read/write
object identifier : 1.3.6.1
security level : auth/priv
auth algorithm : md5
auth password : ********
privacy algorithm : des
privacy password : ******
```
WS2000>admin(system.snmp.access)> show

Description:
Shows the SNMP v3 engine ID.

Syntax:
show   eid  Shows the SNMP v3 Engine ID.

Example:
admin(system.snmp.access)>show eid

WS2000 snmp v3 engine id  : 0000018457D71CDFF86FD8FC

admin(system.snmp.access)>
13.49 System SNMP Traps Commands

WS2000>admin(system.snmp)> traps

Description:

Displays the SNMP traps submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds SNMP trap entries.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes SNMP trap entries.</td>
</tr>
<tr>
<td>list</td>
<td>Lists SNMP trap entries.</td>
</tr>
<tr>
<td>set</td>
<td>Sets SNMP trap parameters.</td>
</tr>
<tr>
<td>show</td>
<td>Shows SNMP trap parameters.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>quit</td>
<td>Quits the CLI.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
WS2000>admin(system.snmp.traps)> add

Description:

Adds SNMP trap entries.

Syntax:

```
add v1v2 <ip> <port> <comm> v1/v2
```

Adds an entry to the SNMP v1/v2 access list with the destination IP address set to <ip>, the destination UDP port set to <port>, the community string set to <comm> (1 to 31 characters), and the SNMP version set to v1 or v2.

```
v3 <ip> <port> <user> <sec> <auth> <pass1> <priv> <pass2>
```

Adds an entry to the SNMP v3 access list with the destination IP address set to <ip>, the destination UDP port set to <port>, the username set to <user> (1–31 characters), and the security type set to one of none, auth, or auth/priv.

The following parameters must be specified if <sec> is auth or auth/priv:

- Authentication type <auth> set to md5 or sha1
- Authentication password <pass1> (8–31 chars)

The following parameters must be specified if <sec> is set to auth/priv:

- Privacy algorithm set to des or aes
- Privacy password <pass2> (8–31 chars)

Example:

```
admin(system.snmp.traps)>add v1v2 203.223.24.2 333 mycomm v1
```

```
admin(system.snmp.traps)>list v1v2c
```

```
+--------------------+----------------+-----------------+-----------------+---------+
<table>
<thead>
<tr>
<th>index</th>
<th>dest ip</th>
<th>dest port</th>
<th>community</th>
<th>version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>203.223.24.2</td>
<td>333</td>
<td>mycomm</td>
<td>v1</td>
</tr>
</tbody>
</table>
```

```
admin(system.snmp.traps)>add v1v2 209.255.32.1 334 jumbo v2
```

```
admin(system.snmp.traps)>list v1v2c
```

```
+--------------------+----------------+-----------------+-----------------+---------+
<table>
<thead>
<tr>
<th>index</th>
<th>dest ip</th>
<th>dest port</th>
<th>community</th>
<th>version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>203.223.24.2</td>
<td>333</td>
<td>mycomm</td>
<td>v1</td>
</tr>
<tr>
<td>2</td>
<td>209.255.32.1</td>
<td>334</td>
<td>jumbo</td>
<td>v2</td>
</tr>
</tbody>
</table>
```

```
admin(system.snmp.traps)>add v3 201.232.24.33 555 BigBoss none md5
```

```
admin(system.snmp.traps)>list v3 all
```

```
index : 1
destination ip : 201.232.24.33
destination port : 555
username : BigBoss
security level : none
auth algorithm : md5
auth password : ********
privacy algorithm : des
privacy password : ********
WS2000>admin(system.snmp.traps)> delete

Description:

Deletes SNMP trap entries.

Syntax:

deatle v1v2c <idx>         Deletes entry <idx> from the v1v2c access control list.
deatle all                  Deletes all entries from the v1v2c access control list.
deatle v3 <idx>            Deletes entry <idx> from the v3 access control list.
deatle all                  Deletes all entries from the v3 access control list.

Example:

    admin(system.snmp.traps)>list v3 all

    index : 1
    destination ip : 201.232.24.33
    destination port : 555
    username : BigBoss
    security level : none
    auth algorithm : md5
    auth password : ********
    privacy algorithm : des
    privacy password : ********
WS2000>admin(system.snmp.traps)> list

Description:
Lists SNMP trap entries.

Syntax:

<table>
<thead>
<tr>
<th>list</th>
<th>v1v2c</th>
<th>v3</th>
<th>all</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lists SNMP v1/v2c access entries.</td>
<td>Lists SNMP v3 access entry &lt;idx&gt;.</td>
<td>Lists all SNMP v3 access entries.</td>
</tr>
</tbody>
</table>

Example:

```
admin(system.snmp.traps)>add v1v2 203.223.24.2 333 mycomm v1
admin(system.snmp.traps)>list v1v2c

index  dest ip  dest port  community  version
----------------------------------------------------------------------
1  203.223.24.2  333  mycomm  v1

admin(system.snmp.traps)>add v3 201.232.24.33 555 BigBoss none md5
admin(system.snmp.traps)>list v3 all

index : 1
destination ip : 201.232.24.33
destination port : 555
username : BigBoss
security level : none
auth algorithm : md5
auth password : ********
privacy algorithm : des
privacy password : ********
```
**WS2000>admin(system.snmp.traps)> set**

**Description:**
Sets SNMP trap parameters.

**Syntax:**

```
set cold enable / disable
set cfg enable / disable
set lowcf enable / disable
set port enable / disable
set dos-attack enable / disable
set snmp-auth enable / disable
set snmp-acl enable / disable
set mu-assoc enable / disable
set mu-unassoc enable / disable
set mu-deny-assoc enable / disable
set mu-deny-auth enable / disable
set ap-adopt enable / disable
set ap-unadopt enable / disable
set ap-denied-adopt enable / disable
set ap-radar enable / disable
set cf-thresh <memory>
set min-pkt <pkt>
set dos-rate-limit <seconds>
set rate <rate> <scope> <value>
```

**Notes:**
- `<value>` can be a number with up to two decimal places, except for assoc_mus, which must be an integer.
- `<memory>` sets the threshold for low compact flash memory trap to `<memory>` (0–2147483647 kb).
- `<pkt>` sets the minimum number of packets required for rate traps to fire (1–65535).
- `<seconds>` sets the rate limit in seconds for DOS traps to `<seconds>` per trap (0–2147483647).
- `<rate>` choices, `Interpretation`, and `Allowed Range for <value>`:
  - `pkts`: Packets/second, `<value>`: 0-9999.99, `<scope>` switch, wlan, ap, mu
  - `mbps`: Throughput, `<value>`: 0-108.00, `<scope>` switch, wlan, ap, mu
  - `avg-bps`: Average bit speed in mbps, `<value>`: 0-108.00, `<scope>` wlan, ap, mu
  - `pct-nu`: % not UNICAST, `<value>`: 0-100.00, `<scope>` wlan, ap, mu
  - `avg-signal`: Negative average signal, `<value>`: 0-100.00, `<scope>` wlan, ap, mu
  - `avg-retries`: Average retries, `<value>`: 0-16.00, `<scope>` wlan, ap, mu
  - `pct-dropped`: % dropped packets, `<value>`: 0-100.00, `<scope>` wlan, ap, mu
  - `pct-undecrypt`: % undecryptable, `<value>`: 0-100.00, `<scope>` wlan, ap, mu
  - `assoc-mus`: Number of associated MUs, `<value>`: 0-200, `<scope>` switch, wlan, ap

**Note:** `<value>` can be a number with up to two decimal places, except for assoc_mus, which must be an integer.
Example:

admin(system.snmp.traps)>show trap

SNMP System Traps

snmp cold start : disable
snmp config changed : disable
low compact flash memory : disable

SNMP Network Traps

physical port status change : disable
denial of service : disable

SNMP Traps

snmp auth failure : disable
snmp acl violation : disable

SNMP MU Traps

mu associated : disable
mu unassociated : disable
mu denied association : disable
mu denied authentication : disable

SNMP AP Traps

ap adopted : disable
ap unadopted : disable
ap denied adoption : disable
ap radar detection : disable

SNMP Trap Threshold

compact flash memory threshold : 1024
min packets required for rate trap: 800
denial of service trap rate limit : 10

admin(system.snmp.traps)>set cold enable
admin(system.snmp.traps)>set port enable
admin(system.snmp.traps)>set dos-attack enable
admin(system.snmp.traps)>set mu-unassoc enable
admin(system.snmp.traps)>set ap-radar enable
admin(system.snmp.traps)>set min-pkt 1000
admin(system.snmp.traps)>show trap

SNMP System Traps

<table>
<thead>
<tr>
<th>Trap Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp cold start</td>
<td>enable</td>
</tr>
<tr>
<td>snmp config changed</td>
<td>disable</td>
</tr>
<tr>
<td>low compact flash memory</td>
<td>disable</td>
</tr>
</tbody>
</table>

SNMP Network Traps

<table>
<thead>
<tr>
<th>Trap Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>physical port status change</td>
<td>enable</td>
</tr>
<tr>
<td>denial of service</td>
<td>enable</td>
</tr>
</tbody>
</table>

SNMP Traps

<table>
<thead>
<tr>
<th>Trap Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp auth failure</td>
<td>disable</td>
</tr>
<tr>
<td>snmp acl violation</td>
<td>disable</td>
</tr>
</tbody>
</table>

SNMP MU Traps

<table>
<thead>
<tr>
<th>Trap Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>mu associated</td>
<td>disable</td>
</tr>
<tr>
<td>mu unassociated</td>
<td>enable</td>
</tr>
<tr>
<td>mu denied association</td>
<td>disable</td>
</tr>
<tr>
<td>mu denied authentication</td>
<td>disable</td>
</tr>
</tbody>
</table>

SNMP AP Traps

<table>
<thead>
<tr>
<th>Trap Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap adopted</td>
<td>disable</td>
</tr>
<tr>
<td>ap unadopted</td>
<td>disable</td>
</tr>
<tr>
<td>ap denied adoption</td>
<td>disable</td>
</tr>
<tr>
<td>ap radar detection</td>
<td>enable</td>
</tr>
</tbody>
</table>

SNMP Trap Threshold

<table>
<thead>
<tr>
<th>Trap Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>compact flash memory threshold</td>
<td>1024</td>
</tr>
<tr>
<td>min packets required for rate trap</td>
<td>1000</td>
</tr>
<tr>
<td>denial of service trap rate limit</td>
<td>10</td>
</tr>
</tbody>
</table>

admin(system.snmp.traps)>
WS2000>admin(system.snmp.traps)> show

Description:

Shows SNMP trap parameters.

Syntax:

show trap rate-trap

Example:

admin(system.snmp.traps)>show trap

SNMP System Traps

snmp cold start : enable
snmp config changed : disable
low compact flash memory : disable

SNMP Network Traps

physical port status change : enable
denial of service : enable

SNMP Traps

snmp auth failure : disable
snmp acl violation : disable

SNMP MU Traps

mu associated : disable
mu unassociated : enable
mu denied association : disable
mu denied authentication : disable

SNMP AP Traps

ap adopted : disable
ap unadopted : disable
ap denied adoption : disable
ap radar detection : enable

SNMP Trap Threshold
compact flash memory threshold : 1024
min packets required for rate trap: 1000
denial of service trap rate limit : 10

admin(system.snmp.traps)>show rate-trap

SNMP Switch Rate Traps

pkts/s greater than : disable
throughput(Mbps) greater than : disable
num of associated mu greater than : disable

SNMP Wlan Rate Traps

pkts/s greater than : disable
throughput(Mbps) greater than : disable
avg bit speed(Mbps) less than : disable
pct non-unicast greater than : disable
-average signal worse than : disable
average retry greater than : disable
pct dropped greater than : disable
pct undecryptable greater than : disable
num of associated mu greater than : disable

SNMP Portal Rate Traps

pkts/s greater than : disable
throughput(Mbps) greater than : disable
avg bit speed(Mbps) less than : disable
pct non-unicast greater than : disable
-average signal worse than : disable
average retry greater than : disable
pct dropped greater than : disable
pct undecryptable greater than : disable
num of associated mu greater than : disable

SNMP Mu Rate Traps

pkts/s greater than : disable
throughput(Mbps) greater than : disable
avg bit speed(Mbps) less than : disable
pct non-unicast greater than : disable
-average signal worse than : disable
average retry greater than : disable
pct dropped greater than : disable
pct undecryptable greater than : disable

admin(system.snmp.traps)>

13.50 System SSH Commands

WS2000>admin(system)> ssh

Description:
Displays the secure shell (SSH) submenu. The items available under this command are shown below.

- **set**: Sets SSH parameters
- **show**: Shows SSH parameters.
- **save**: Saves the configuration to system flash.
- **..**: Goes to the parent menu.
- **/**: Goes to the root menu.
WS2000>admin(system.ssh)> set

Description:
Sets secure shell parameters for system access.

Syntax:

set auth-timeout <time>       Sets the maximum time <time> (0–65535 seconds) allowed for SSH authentication to occur before executing a timeout.
set inactive-timeout <time>   Sets the maximum amount of inactive time <time> (0–65535 seconds) for an SSH connection before a timeout occurs and the user is dropped.

Example:

admin(system.ssh)> set auth-timeout 60
admin(system.ssh)> set inactive-timeout 2000
admin(system.ssh)> show all
Authentication Timeout : 60
SSH Client Inactivity Timeout : 2000

Related Commands:

show all     Shows the SSH parameter values.
WS2000>admin(system.ssh)> show

Description:
Shows secure shell timeout parameters.

Syntax:

show all  Display the SSH parameter settings.

Example:

admin(system.ssh)> set auth-timeout 60
admin(system.ssh)> set inactiv 2000
admin(system.ssh)> show all
    Authentication Timeout : 60
    SSH Client Inactivity Timeout : 2000

Related Commands:

set         Sets the values for the secure shell timeout parameters.
13.51 System User Database Commands

WS2000>admin(system)> userdb

Description:

Displays the userdb submenu. The items available under this command are shown below.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>Goes to the user submenu.</td>
</tr>
<tr>
<td>group</td>
<td>Goes to the group submenu.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the configuration to system flash.</td>
</tr>
<tr>
<td>..</td>
<td>Goes to the parent menu.</td>
</tr>
<tr>
<td>/</td>
<td>Goes to the root menu.</td>
</tr>
</tbody>
</table>
13.52 System User Database Group Commands

**WS2000>admin(system.userdb)> group**

**Description:**
Displays the group submenu. The items available under this command are shown below.

- **create** Creates a new group.
- **delete** Deletes a group.
- **add** Adds a user to a group.
- **remove** Removes a user from a group.
- **show** Shows the existing groups.
- **save** Saves the configuration to system flash.
- **..** Goes to the parent menu.
- **/** Goes to the root menu.
WS2000>admin(system.userdb.group)> add

Description:

Add a user to a group.

Syntax:

```
add <userID> <groupID>
```

Adds the user specified by <userID> to the group <groupID>. The userID must already be defined in the database. Use the add command from the (system.userdb.users) menu to add a new user.

Example:

```
admin(system.userdb.group)> add fred g1
admin(system.userdb.group)> add joe g1
admin(system.userdb.group)> add joe g2
admin(system.userdb.group)> show user g1
List of Users of Group:
    fred
    joe
admin(system.userdb.group)> show user g2
List of Users of Group:
    joe
```

Related Commands:

```
show users
```

Displays a list of users in a group.
WS2000>admin(system.userdb.group)> create

Description:

Creates a new group.

Syntax:

create <groupId>       Creates a new group with the ID <groupId>. The <groupId> can be an alphanumeric string.

Example:

admin(system.userdb.group)>create g1
admin(system.userdb.group)>create g2
admin(system.userdb.group)>create g3
admin(system.userdb.group)>show groups
List of Group Names :
    g1
    g2
    g3

Related Commands:

delete            Deletes a group.
show groups       Displays a list of groups in the database.
WS2000>admin(system.userdb.group)> delete

Description:

Deletes a group from the database.

Syntax:

delete  <groupID>  Deletes the group named <groupID> from the database. A warning will occur if there are still users assigned to that group.

Example:

```
admin(system.userdb.group)>show group
List of Group Names   :
   g1
   g2
   g3

admin(system.userdb.group)>delete g3
admin(system.userdb.group)>show group
List of Group Names   :
   g1
   g2
```

Related Commands:

add       Adds users to a group.
show user  Displays a list of users in a group.
WS2000>admin(system.userdb.group)> remove

Description:
Removes a user from a group.

Syntax:
remove <userID> <groupID> Removes user <userID> from the group <groupID>.

Example:
admin(system.userdb.group)>remove joe g1
admin(system.userdb.group)>show users g1
List of Users of Group:

  fred

admin(system.userdb.group)>

Related Commands:
add Adds a user to a group.
show users Shows a list of users in a group.
WS2000>admin(system.userdb.group)> show

Description:

Shows the existing groups.

Syntax:

```
show     groups       Displays a list of the defined groups.
users    <groupId>    Displays a list of users in group <groupId>.
```

Example:

```
admin(system.userdb.group)> create g1
admin(system.userdb.group)> create g2
admin(system.userdb.group)> create g3
admin(system.userdb.group)> show groups
List of Group Names    :
                          g1  
                          g2  
                          g3  
admin(system.userdb.group)> show users g1
List of Users of Group  :
                          fred
```

Related Commands:

- **create**  Creates a new group.
- **delete**  Deletes a group.
13.53 System User Database User Commands

WS2000>admin(system.userdb)> user

Description:

Displays the user submenu. The items available under this command are shown below.

- **add**: Adds a new user to the database.
- **del**: Deletes a user from the database.
- **set**: Sets the password for a user.
- **show**: Shows a list of users and group information about a user.
- **save**: Saves the configuration to system flash.
- ..: Goes to the parent menu.
- /: Goes to the root menu.
WS2000>admin(system.userdb.user)> add

Description:

Adds a new user to the database.

Syntax:

add  <userID>  <password>    Adds a user to the database with the ID <userID> and password <password>. Password is limited to 8 alphanumeric characters.

Example:

admin(system.userdb.user)>add fred fredpass
admin(system.userdb.user)>add joe joepass
admin(system.userdb.user)>add sally sallypa
admin(system.userdb.user)>
List of User Ids : 
    fred
    joe
    sally

Related Commands:

show users    Show a list of the users in the database.
del           Deletes a user from the database.
WS2000> admin(system.userdb.user)> del

Description:

Deletes a user from the database.

Syntax:

```
del <userID>  Deletes the user with the ID <userID> from the database.
```

Example:

```
admin(system.userdb.user)> add fred fredpass
admin(system.userdb.user)> add joe joepass
admin(system.userdb.user)> add sally sallypa
admin(system.userdb.user)> show users
List of User Ids :  
   fred
   joe
   sally

admin(system.userdb.user)> del sally
admin(system.userdb.user)> show users
List of User Ids :  
   fred
   joe
```

Related Commands:

```
add  Adds a user to the database.
show users  Displays a list of users in the database.
```
WS2000>admin(system.userdb.user)> set

Description:
Sets the password for a user.

Syntax:
set <userID> <newpassword>  Resets the password for user with <userID> to <newpassword>.

Example:
admin(system.userdb.user)>set fred frednew

Related Commands:
add         Adds a new user.
WS2000>admin(system.userdb.user)> show

Description:
Shows a list of users and group membership for a particular user.

Syntax:
show   groups   <userId>   Displays the list of groups that a user with <userId> belongs to.
users   Displays a list of all defined users in the database.

Example:
admin(system.userdb.user)>add fred fredpass
admin(system.userdb.user)>add joe joepass
admin(system.userdb.user)>show users
List of User Ids
    fred
    joe
admin(system.userdb.user)>..
admin(system.userdb.user)>group
admin(system.userdb.group)>create g1
admin(system.userdb.group)>add joe g1
admin(system.userdb.group)>..
admin(system.userdb.user)>user
admin(system.userdb.user)>show groups joe
List of Groups of user
    g1

Related Commands:
add   Add a user to the database.
13.54 System WS2000 Commands

WS2000>admin(system)> ws2000)

Description:

Displays the WS 2000 submenu. The items available under this command are shown below.

restart  Restarts the WS 2000 Wireless Switch.
set      Sets WS 2000 system parameters.
show     Shows WS 2000 system parameter settings.
save     Saves the configuration to system flash.
quit     Quits the CLI.
..       Goes to the parent menu.
/        Goes to the root menu.
WS2000>admin(system.ws2000)> restart

Description:
Restarts the WS 2000 Wireless Switch.

Syntax:
restart
  Restarts the switch from the firmware.

Example:
admin(system.ws2000)> restart

Restarting system.

WS 2000 Boot Firmware Version 1.5.0.0-160b
Copyright(c) Symbol Technologies Inc. 2003. All rights reserved.

Press escape key to run boot firmware ........

Power On Self Test

testing ram : pass
testing nor flash : pass
testing nand flash : pass
testing ethernet : pass

...

Starting iGateway Apps(1)....
Starting iGateway Apps(2)....
Using switch.o
Starting Wireless Switch....
Configuring iGateway....
Starting SNMP....
Using led.o
Starting WS2000 CLI....

Login:
**WS2000>admin(system.ws2000)> set**

**Description:**
Sets WS 2000 system parameters.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set airbeam mode enable/disable</td>
<td>Enables/disables airbeam access.</td>
</tr>
<tr>
<td>passwd &lt;passwd&gt;</td>
<td>Sets the airbeam password to &lt;passwd&gt; (1–39 characters).</td>
</tr>
<tr>
<td>applet lan enable/disable</td>
<td>Enables/disables http applet access from LAN.</td>
</tr>
<tr>
<td>wan enable/disable</td>
<td>Enables/disables http applet access from WAN.</td>
</tr>
<tr>
<td>slan enable/disable</td>
<td>Enables/disables https applet access from LAN.</td>
</tr>
<tr>
<td>swan enable/disable</td>
<td>Enables/disables https applet access from WAN.</td>
</tr>
<tr>
<td>cc &lt;cc&gt;</td>
<td>Sets the WS2000 country code to two-letter &lt;cc&gt;.</td>
</tr>
<tr>
<td>cli lan enable/disable</td>
<td>Enables/disables CLI telnet access from LAN.</td>
</tr>
<tr>
<td>wan enable/disable</td>
<td>Enables/disables CLI telnet access from WAN.</td>
</tr>
<tr>
<td>email &lt;email&gt;</td>
<td>Sets the WS2000 admin email address to &lt;email&gt; (1–59 characters).</td>
</tr>
<tr>
<td>ftp lan enable/disable</td>
<td>Enables/disables FTP access from the LAN.</td>
</tr>
<tr>
<td>wan enable/disable</td>
<td>Enables/disables FTP access from the WAN.</td>
</tr>
<tr>
<td>loc &lt;loc&gt;</td>
<td>Sets the WS2000 system location to &lt;loc&gt; (1–59 characters).</td>
</tr>
<tr>
<td>name &lt;name&gt;</td>
<td>Sets the WS2000 system name to &lt;name&gt; (1–59 characters).</td>
</tr>
<tr>
<td>ssh lan enable/disable</td>
<td>Enables/disables secure shell access from the LAN.</td>
</tr>
<tr>
<td>wan enable/disable</td>
<td>Enables/disables secure shell access from the WAN.</td>
</tr>
<tr>
<td>snmp lan enable/disable</td>
<td>Enables/disables SNMP access from LAN.</td>
</tr>
<tr>
<td>wan enable/disable</td>
<td>Enables/disables SNMP access from WAN.</td>
</tr>
<tr>
<td>timeout &lt;time&gt;</td>
<td>Sets the idle timeout to &lt;time&gt; minutes (0–1440). Setting the value to 0 indicates not to timeout.</td>
</tr>
</tbody>
</table>

**Example:**

```
admin(system.ws2000)>show all
```

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>system name</td>
<td>Atlanta</td>
</tr>
<tr>
<td>system location</td>
<td>Atlanta Field Office</td>
</tr>
<tr>
<td>admin email address</td>
<td><a href="mailto:LeoExample@symbol.com">LeoExample@symbol.com</a></td>
</tr>
<tr>
<td>system uptime</td>
<td>0 days 4 hours 33 minutes</td>
</tr>
<tr>
<td>WS2000 firmware version</td>
<td>1.5.0.0-200b</td>
</tr>
<tr>
<td>country code</td>
<td>us</td>
</tr>
<tr>
<td>applet http access from lan</td>
<td>enable</td>
</tr>
<tr>
<td>applet http access from wan</td>
<td>disable</td>
</tr>
<tr>
<td>applet https access from lan</td>
<td>enable</td>
</tr>
<tr>
<td>applet https access from wan</td>
<td>disable</td>
</tr>
<tr>
<td>cli telnet access from lan</td>
<td>enable</td>
</tr>
<tr>
<td>cli telnet access from wan</td>
<td>disable</td>
</tr>
<tr>
<td>snmp access from lan</td>
<td>enable</td>
</tr>
<tr>
<td>snmp access from wan</td>
<td>enable</td>
</tr>
<tr>
<td>airbeam access mode</td>
<td>disable</td>
</tr>
<tr>
<td>airbeam access user name</td>
<td>airbeam</td>
</tr>
</tbody>
</table>
```
airbeam access password : ********

admin(system.ws2000)>set name BldgC
admin(system.ws2000)>set email johndoe@mycompany.com
admin(system.ws2000)>set applet lan enable
admin(system.ws2000)>set airbeam mode enable
admin(system.ws2000)>set airbeam passwd changeme
admin(system.ws2000)>show all

system name : BldgC
system location : Atlanta Field Office
admin email address : johndoe@mycompany.com
system uptime : 0 days 4 hours 41 minutes
WS2000 firmware version : 1.5.0.0-200b
country code : us
applet http access from lan : enable
applet http access from wan : disable
applet https access from lan : enable
applet https access from wan : disable
cli telnet access from lan : enable
cli telnet access from wan : disable
snmp access from lan : enable
snmp access from wan : enable
airbeam access mode : enable
airbeam access user name : airbeam
airbeam access password : ********

admin(system.ws2000)>
**WS2000> admin(system.ws2000)> show**

**Description:**

Shows WS 2000 system information.

**Syntax:**

```
show all
```

Shows all of the WS 2000 system information.

**Example:**

```
admin(system.ws2000)> show all

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>system name</td>
<td>Atlantal</td>
</tr>
<tr>
<td>system location</td>
<td>Atlanta Field Office</td>
</tr>
<tr>
<td>admin email address</td>
<td><a href="mailto:LeoExample@symbol.com">LeoExample@symbol.com</a></td>
</tr>
<tr>
<td>system uptime</td>
<td>0 days 4 hours 33 minutes</td>
</tr>
<tr>
<td>WS2000 firmware version</td>
<td>1.5.0.0-200b</td>
</tr>
<tr>
<td>country code</td>
<td>us</td>
</tr>
<tr>
<td>applet http access from lan</td>
<td>enable</td>
</tr>
<tr>
<td>applet http access from wan</td>
<td>disable</td>
</tr>
<tr>
<td>applet https access from lan</td>
<td>enable</td>
</tr>
<tr>
<td>applet https access from wan</td>
<td>disable</td>
</tr>
<tr>
<td>cli telnet access from lan</td>
<td>enable</td>
</tr>
<tr>
<td>cli telnet access from wan</td>
<td>disable</td>
</tr>
<tr>
<td>snmp access from lan</td>
<td>enable</td>
</tr>
<tr>
<td>snmp access from wan</td>
<td>enable</td>
</tr>
<tr>
<td>airbeam access mode</td>
<td>disable</td>
</tr>
<tr>
<td>airbeam access user name</td>
<td>airbeam</td>
</tr>
<tr>
<td>airbeam access password</td>
<td>********</td>
</tr>
</tbody>
</table>
```

admin(system.ws2000)>
Appendix A: Syslog Messages

Informational Log Entries .............................................................. A-2
Notice Log Entries ................................................................. A-4
Warning Log Entries .............................................................. A-6
Alert Log Entry ................................................................ A-9
Error-Level Log Entries .............................................................. A-9
Debug-Level Log Entries .............................................................. A-22
Emergency Log Entries .............................................................. A-26
## A.1 Informational Log Entries

<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Module</td>
<td>LOG_INFO</td>
<td>802.1x: 802.1x Authentication success for MU [MAC_ADDR]</td>
</tr>
<tr>
<td>802.1X Module</td>
<td>LOG_INFO</td>
<td>Tried max eap-id requests for MU [MAC_ADDR].</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_INFO</td>
<td>CFG portal exists called with null mac</td>
</tr>
<tr>
<td>Cell Controller Module</td>
<td>LOG_INFO</td>
<td>Caught Signal [Number] ignoring it sig</td>
</tr>
<tr>
<td>Cell Controller Module</td>
<td>LOG_INFO</td>
<td>ccmain: no free ccb for tx</td>
</tr>
<tr>
<td>Cell Controller Module</td>
<td>LOG_INFO</td>
<td>mu remove ioctl failed</td>
</tr>
<tr>
<td>Cell Controller Module</td>
<td>LOG_INFO</td>
<td>portal remove ioctl failed</td>
</tr>
<tr>
<td>Cell Controller Module</td>
<td>LOG_INFO</td>
<td>Starting</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_INFO</td>
<td>Out of turn eap id ([Number]), expected ([Number]), Ignoring</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_INFO</td>
<td>rcvd eap-logoff from [MAC_ADDR] usmu-&gt;mu-&gt;addr</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_INFO</td>
<td>rcvd eap-notif from supplicant [MAC_ADDR] usmu-&gt;mu-&gt;addr</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_INFO</td>
<td>rcvd eap-start from [MAC_ADDR] usmu-&gt;mu-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_INFO</td>
<td>kerberos preauth required by KDC [IP_ADDR] from_ip</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_INFO</td>
<td>krb5: sending ap_rep (fail) to MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>Inactivity timer expired for MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>MU [MAC_ADDR] Associated to [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>MU [MAC_ADDR] DisAssociated from [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>mu [MAC_ADDR] is a voice mu mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>mu [MAC_ADDR] needs proxy arp mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>MU lock period expired. Removing MU [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>no ccbs to tx disassoc to mu [MAC_ADDR] from [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>No CCBs. MU [MAC_ADDR] DeAuthenticated from [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>No RFP. MU [MAC_ADDR] DeAuthenticated from [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>Removing MU [MAC_ADDR]mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>Scheduling MU [MAC_ADDR] for deletion from [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_INFO</td>
<td>tx disassoc to mu [MAC_ADDR] on bss [MAC_ADDR] mu_addr bss_addr</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_INFO</td>
<td>local clock is synchronized with ntp server</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_INFO</td>
<td>ntp: system clock updated to [%s]</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_INFO</td>
<td>[Pairwise Transient Key] Unable to get free CC buffer</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_INFO</td>
<td>[Pairwise Transient Key] Group rekey after %u seconds gk_timeout</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_INFO</td>
<td>rcvd access-accept from [IP_ADDR] for [MAC_ADDR]</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_INFO</td>
<td>rcvd access-reject from [IP_ADDR] for [MAC_ADDR]</td>
</tr>
<tr>
<td>RF Port Module</td>
<td>LOG_INFO</td>
<td>Radio [MAC_ADDR] acs done ch=[Number]</td>
</tr>
<tr>
<td>RF Port Module</td>
<td>LOG_INFO</td>
<td>Radio [MAC_ADDR] acs in progress addr</td>
</tr>
<tr>
<td>RF Port Module</td>
<td>LOG_INFO</td>
<td>Radio [MAC_ADDR] adopted addr</td>
</tr>
<tr>
<td>RF Port Module</td>
<td>LOG_INFO</td>
<td>Radio [MAC_ADDR] inactive prtl_ptr-&gt;addr</td>
</tr>
<tr>
<td>RF Port Module</td>
<td>LOG_INFO</td>
<td>Radio [MAC_ADDR] removed prtl_ptr-&gt;addr</td>
</tr>
<tr>
<td>Rogue AP Detection Module</td>
<td>LOG_INFO</td>
<td>Number of known APs: %u count</td>
</tr>
<tr>
<td>Statistics Module</td>
<td>LOG_INFO</td>
<td>Resetting</td>
</tr>
<tr>
<td>VLAN Module</td>
<td>LOG_INFO</td>
<td>Mapped port [Number] to subnet [Number]</td>
</tr>
<tr>
<td>VLAN Module</td>
<td>LOG_INFO</td>
<td>Mapped wlan [Number] to subnet [Number]</td>
</tr>
<tr>
<td>VLAN Module</td>
<td>LOG_INFO</td>
<td>Port [Number] has no subnet mapping port_idx</td>
</tr>
<tr>
<td>VLAN Module</td>
<td>LOG_INFO</td>
<td>Subnet [Number] disabled subnet_idx</td>
</tr>
<tr>
<td>VLAN Module</td>
<td>LOG_INFO</td>
<td>Subnet [Number] enabled subnet_idx</td>
</tr>
<tr>
<td>VLAN Module</td>
<td>LOG_INFO</td>
<td>Wlan [Number] has no subnet mapping wlan_idx</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_INFO</td>
<td>SIP: Max number of SIP sesions reached on portal [ address ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_INFO</td>
<td>&quot;SIP: Create a new SIP session for call id [ identifier ], set state to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>initiated&quot;</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_INFO</td>
<td>SIP: Decrementing the number of Active SIP sessions of portal [ address ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to [ number ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_INFO</td>
<td>SIP: Incrementing the number of Active SIP sessions of portal [ address ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to [ number ]</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_INFO</td>
<td>WIPS is disabled</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_INFO</td>
<td>WIPS : Detection in progress</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_INFO</td>
<td>Could not send configuration to [ MAC ] Sensor was not found</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_INFO</td>
<td>WIPS : Max number of sensors detected. Not adding any more</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_INFO</td>
<td>AP [ MAC ] is converted to sensor</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_INFO</td>
<td>Sensor [ MAC ] is successfully reverted</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_INFO</td>
<td>&quot;Sensor [ MAC ] is no longer responding, removed&quot;</td>
</tr>
</tbody>
</table>
### Notice Log Entries

<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WIPS module</strong></td>
<td>LOG_INFO</td>
<td>Sensor [MAC] timed out waiting for [command]</td>
</tr>
<tr>
<td><strong>AP Revert</strong></td>
<td>LOG_INFO</td>
<td>AP [MAC] Reverting to AP4131</td>
</tr>
<tr>
<td><strong>AP Revert</strong></td>
<td>LOG_INFO</td>
<td>AP [MAC] Reverting to AP4121</td>
</tr>
<tr>
<td><strong>AP Revert</strong></td>
<td>LOG_INFO</td>
<td>old rf image = [name] new rf image = [name] load_now = [truth value]</td>
</tr>
<tr>
<td><strong>Port Configuration</strong></td>
<td>LOG_INFO</td>
<td>Port config changed for port idx = [idx]</td>
</tr>
<tr>
<td><strong>Port Configuration</strong></td>
<td>LOG_INFO</td>
<td>Port config changed for Wan: port idx = [idx]</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>LOG_INFO</td>
<td>Subnet [idx] : DHCP Client is already running</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>LOG_INFO</td>
<td>Subnet [idx] : Stopping DHCP Client</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>LOG_INFO</td>
<td>Adding the DGW as Subnet [idx]</td>
</tr>
<tr>
<td><strong>CF Format</strong></td>
<td>LOG_INFO</td>
<td>CF card Formatted</td>
</tr>
</tbody>
</table>

### System Component Debug Log Entries

<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.1X Module</strong></td>
<td>LOG_NOTICE</td>
<td>8021x: final timeout on server [IP_ADDR]. old_ip</td>
</tr>
<tr>
<td><strong>802.1X Module</strong></td>
<td>LOG_NOTICE</td>
<td>8021x: Starting WPA/Tkip keying for MU [MAC_ADDR]</td>
</tr>
<tr>
<td><strong>802.1X Module</strong></td>
<td>LOG_NOTICE</td>
<td>8021x: WEP keys sent. Starting Keyguard</td>
</tr>
<tr>
<td><strong>802.1X Module</strong></td>
<td>LOG_NOTICE</td>
<td>8021x: WEP[Number] keys transmitted to MU [MAC_ADDR]</td>
</tr>
<tr>
<td><strong>EAP Module</strong></td>
<td>LOG_NOTICE</td>
<td>EAP code [Number] != EAP_RESPONSE from MU [MAC_ADDR]. Ignoring</td>
</tr>
<tr>
<td><strong>EAP Module</strong></td>
<td>LOG_NOTICE</td>
<td>invalid eapol length [Number] from [MAC_ADDR]. ignoring</td>
</tr>
<tr>
<td><strong>EAP Module</strong></td>
<td>LOG_NOTICE</td>
<td>invalid eapol version [Number] from [MAC_ADDR].</td>
</tr>
<tr>
<td><strong>EAP Module</strong></td>
<td>LOG_NOTICE</td>
<td>invalid etherType 0x%04X from [MAC_ADDR].</td>
</tr>
<tr>
<td><strong>Kerberos Client Module</strong></td>
<td>LOG_NOTICE</td>
<td>krb: ess [%s] authenticated with kdc [IP_ADDR]</td>
</tr>
<tr>
<td><strong>Kerberos Proxy Module</strong></td>
<td>LOG_NOTICE</td>
<td>krb: mu [MAC_ADDR] ticket expired. deauthenticating</td>
</tr>
<tr>
<td><strong>Kerberos Proxy Module</strong></td>
<td>LOG_NOTICE</td>
<td>krb5: MU [MAC_ADDR] authenticated. Ticket valid for %02u:%02u:%02u hh:mm:ss</td>
</tr>
<tr>
<td><strong>Encryption Key Exchange Module</strong></td>
<td>LOG_NOTICE</td>
<td>[Pairwise Transient Key] Bad ack bit %x %x [MAC_ADDR] *U08 *) &amp;eap_pkt-&gt;skd.info_h</td>
</tr>
<tr>
<td><strong>Encryption Key Exchange Module</strong></td>
<td>LOG_NOTICE</td>
<td>[Pairwise Transient Key] Bad key type [MAC_ADDR] mu-&gt;addr</td>
</tr>
</tbody>
</table>
| **Encryption Key Exchange Module** | LOG_NOTICE | [Pairwise Transient Key] Bad replay ctr [MAC_ADDR] Rcvd %x %x Expected %x %x
<p>| |
| |
| <strong>Encryption Key Exchange Module</strong> | LOG_NOTICE | [Pairwise Transient Key] Bad version [MAC_ADDR] mu-&gt;addr                   |</p>
<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_NOTICE</td>
<td>[Pairwise Transient Key] Funny pkt!! [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_NOTICE</td>
<td>[Pairwise Transient Key] IE no match [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_NOTICE</td>
<td>[Pairwise Transient Key] Ignore packet [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_NOTICE</td>
<td>[Pairwise Transient Key] Ignore packet [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_NOTICE</td>
<td>[Pairwise Transient Key] Ignore packet [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_NOTICE</td>
<td>[Pairwise Transient Key] MIC Error [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_NOTICE</td>
<td>[Pairwise Transient Key] MIC Error [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_NOTICE</td>
<td>[Pairwise Transient Key] req bit set [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_NOTICE</td>
<td>SSN IE too big - [Number] bytes [MAC_ADDR] eap_pkt-&gt;skd.mlen mu-&gt;addr</td>
</tr>
</tbody>
</table>
## Warning Log Entries

<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Module</td>
<td>LOG_WARNING</td>
<td>8021x: MU [MAC_ADDR] in unknown PAE state [[Number]].</td>
</tr>
<tr>
<td>802.1X Module</td>
<td>LOG_WARNING</td>
<td>8021x: no rsp from server [IP_ADDR] count: [Number]</td>
</tr>
<tr>
<td>802.1X Module</td>
<td>LOG_WARNING</td>
<td>8021x: Using backup server [IP_ADDR]</td>
</tr>
<tr>
<td>802.1X Module</td>
<td>LOG_WARNING</td>
<td>Unable to send EAPOL keys. MPPE keys</td>
</tr>
<tr>
<td>802.1X Module</td>
<td>LOG_WARNING</td>
<td>Unable to send EAPOL keys. MPPE keys</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WPA/TKIP keying failure. MPPE keys not</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_WARNING</td>
<td>atable initialize</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_WARNING</td>
<td>eapol length [Number]) from [MAC_ADDR] is invalid</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_WARNING</td>
<td>ignoring eap frame from MU [MAC_ADDR].</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_WARNING</td>
<td>Username in eap-id-rsp from [MAC_ADDR] too long [Number] bytes</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_WARNING</td>
<td>kerberos services waiting for</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_WARNING</td>
<td>krb: authentication failure from KDC [IP_ADDR] from_ip</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_WARNING</td>
<td>krb: error [Number] in krb5_process_padata) retval</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_WARNING</td>
<td>krb: error [Number] reported by decode_krb5_as_rep) retval</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_WARNING</td>
<td>krb: kerberos error code: [Number] err_reply-&gt;error</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_WARNING</td>
<td>krb: principal not known on kdc</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_WARNING</td>
<td>krb: rcvd krb_error from [IP_ADDR] from_ip</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>Bad Encryption Type from KDC. Check that the</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>Client name not known to KDC. MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>Clock skew reported by KDC for MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>KDC reported ecode %u for MU [MAC_ADDR] ecode mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: Client name for MU [MAC_ADDR] not known on KDC</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: clock skew reported for MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: error code = [Number] in decode_krb error</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: error [Number] in decode_krb5_ap_req) retval</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: Error [Number] in encode_krb5_ap_rep</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: Error [Number] in encode_krb5_ap_rep_enc_part)</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: error [Number] in encode_krb5_error) retval</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: Error [Number] in krb5_encrypt_helper</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: error [Number] in krb5_rd_req_decoded) retval</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: key generation failure!</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: Server name for MU [MAC_ADDR] not known to KDC</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: switch auth not done. ignoring</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: switch auth not done. Ignoring ap_req</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: switch auth not done. Ignoring as_req from</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: switch auth not done. Ignoring sk_req</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: Ticket from MU [MAC_ADDR] already expired.</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: Ticket from MU [MAC_ADDR] not yet valid.</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>krb5: unknown WNMP msg [Number]) from MU [MAC_ADDR]</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>Server name not known to KDC. MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>Ticket for AP has expired. MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_WARNING</td>
<td>Ticket for AP not yet valid. MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_WARNING</td>
<td>\nUnrecognized subtype %04x ignored sub_type</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_WARNING</td>
<td>Assoc denied to MU [MAC_ADDR]. Capability [Number]) not supp</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_WARNING</td>
<td>Bad SSID from MU [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_WARNING</td>
<td>Bad Tx_Rates [Number]) for MU [MAC_ADDR]</td>
</tr>
</tbody>
</table>
| MU Association Module        | LOG_WARNING | Incorrect Seq Num [Number]) in Auth_Req from [MAC_ADDR]
<p>| MU Association Module        | LOG_WARNING | Invalid WPA elem from MU [MAC_ADDR] Rejecting Assoc_Req. |
| MU Association Module        | LOG_WARNING | Max MU capacity reached. Denying Auth to [MAC_ADDR] |
| MU Association Module        | LOG_WARNING | mu [MAC_ADDR] not in acl mu_ptr-&gt;addr |
| MU Association Module        | LOG_WARNING | No WPA elem from MU [MAC_ADDR] Rejecting Assoc_Req. |
| MU Association Module        | LOG_WARNING | rx assoc for unknown mu [MAC_ADDR] pkt_ptr-&gt;src |
| MU Association Module        | LOGWARNING   | SSID too long [Number]) from MU [MAC_ADDR] |
| MU Association Module        | LOG_WARNING | Unsupported auth algorithm [Number]) from MU [MAC_ADDR] |
| NTP Client Module            | LOG_WARNING | ntp:li-field in ntp header indicates server is not synced |
| NTP Client Module            | LOG_WARNING | rcvd ntp rsp from unknown server [IP_ADDR]. Ignoring |
| RF Port Configuration Module | LOG_WARNING | portal [MAC_ADDR] bad radio type [Number] |
| RF Port Configuration Module | LOG_WARNING | portal [MAC_ADDR] bad radio type [Number] |
| RF Port Configuration Module | LOG_WARNING | Portal [MAC_ADDR] can't be defaulted prtl_ptr-&gt;addr |
| RF Port Configuration Module | LOG_WARNING | Portal [MAC_ADDR] denied adoption in acl prtl_ptr-&gt;addr |
| RF Port Configuration Module | LOG_WARNING | portal [MAC_ADDR] found at idx [Number] |
| RF Port Configuration Module | LOG_WARNING | portal [MAC_ADDR] not connected &amp; not in acl |
| RF Port Configuration Module | LOG_WARNING | portal [MAC_ADDR] not found using idx [Number] |</p>
<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF Port Configuration Module</td>
<td>LOG_WARNING</td>
<td>Portal [MAC_ADDR] replaced by [MAC_ADDR] in slot [Number]</td>
</tr>
<tr>
<td>RF Port Configuration Module</td>
<td>LOG_WARNING</td>
<td>Portal [MAC_ADDR]: no country code</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_WARNING</td>
<td>Radius ID mismatch in rsp from [IP_ADDR]. Ignoring from ip</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_WARNING</td>
<td>Radius validation failed for rsp from [IP_ADDR] for [MAC_ADDR]</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_WARNING</td>
<td>rcvd unexpected rsp from [IP_ADDR] from_ip</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_WARNING</td>
<td>Unable to read System Name from configuration</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_WARNING</td>
<td>unexpected Type [[Number]] in rsp from [IP_ADDR] Ignoring!</td>
</tr>
<tr>
<td>SecurityPolicy.cpp</td>
<td>LOG_WARNING</td>
<td>Error reading configuration. Not starting Kerberos</td>
</tr>
<tr>
<td>Statistics Module</td>
<td>LOG_WARNING</td>
<td>unable to read location for portal [Number] p_idx</td>
</tr>
<tr>
<td>Statistics Module</td>
<td>LOG_WARNING</td>
<td>unable to read name for portal [Number] p_idx</td>
</tr>
<tr>
<td>Statistics Module</td>
<td>LOG_WARNING</td>
<td>unable to read tx_power for portal [Number] p_idx</td>
</tr>
<tr>
<td>Statistics Module</td>
<td>LOG_WARNING</td>
<td>unable to read wlan_map for portal [Number] p_idx</td>
</tr>
</tbody>
</table>
### Alert Log Entry

<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP Client Module</td>
<td>LOG_ALERT</td>
<td>errno [Number] updating system clock to ntp time errno</td>
</tr>
</tbody>
</table>

### Error-Level Log Entries

<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Module</td>
<td>LOG_ERR</td>
<td>Config error! EAP enabled but no valid</td>
</tr>
<tr>
<td>Access Control List Module</td>
<td>LOG_ERR</td>
<td>ACL adopt all read failed</td>
</tr>
<tr>
<td>Access Control List Module</td>
<td>LOG_ERR</td>
<td>ACL adopt all read failed</td>
</tr>
<tr>
<td>Access Control List Module</td>
<td>LOG_ERR</td>
<td>ACL entry count read failed</td>
</tr>
<tr>
<td>Access Control List Module</td>
<td>LOG_ERR</td>
<td>ACL entry count read failed</td>
</tr>
<tr>
<td>Access Control List Module</td>
<td>LOG_ERR</td>
<td>ACL read from cfg failed</td>
</tr>
<tr>
<td>Access Control List Module</td>
<td>LOG_ERR</td>
<td>ACL radio [Number] adopt write fail cfg_list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>ACL cannot read radio [Number] cfg mac radio_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>ACL cannot write radio [Number] cfg mac cfg_list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>ACL cannot write radio [Number] cfg mac cfg_list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>ACL cannot write radio [Number] cfg status cfg_list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read cfg wlan mode</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read cfg wlan mode</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t get beacon interval</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t get bss primary ess</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t get bss primary ess</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t get bss primary ess</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t get dtim period</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t read cfg bss radio idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t read cfg bss radio idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t read cfg bss radio idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t read cfg bss radio idx</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t set bss mac</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t set bss radio idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: can’t set bss radio idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: rates configured incorrectly</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: unable to read cfg basic rates</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: unable to read cfg supported rates</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: unknown radio type in rate cfg</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read [Number] indoor setting list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read cfg country code</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read cfg country code</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read cfg ess</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read cfg mu-mu disallow</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read cfg wlan mode</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read mcast addr1</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read mcast addr2</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read radio [Number] channel cfg_list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read radio [Number] diversity cfg_list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read radio [Number] power cfg_list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot read reg [Number] indoor setting list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: cannot set radio [Number] channel cfg_list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: country code is null in cfg</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>altable: radio [Number] conn status is [Number] cfg_list_idx status</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>cfg cannot read radio [Number] cfg mac radio_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>cfg cannot read radio [Number] cfg mac radio_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>cfg cannot write radio [Number] cfg type cfg_list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>cfg cannot write radio [Number] cfg type cfg_list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>cfg default failed:index [Number] radio type [Number] invalid: bad rgltry info list_idx</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>cfg of radio [Number] not allowed rtype</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>cfg radio type [Number] not allowed rtype</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>rfport list is full</td>
</tr>
<tr>
<td>Address Lookup Table Module</td>
<td>LOG_ERR</td>
<td>wlan [Number]: addr1 = [MAC_ADDR] addr2 = [MAC_ADDR] wlan_idx</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cell Controller Module</td>
<td>LOG_ERR</td>
<td>Error [Number] initing sig handlers errno</td>
</tr>
<tr>
<td>Cell Controller Module</td>
<td>LOG_ERR</td>
<td>Error [Number] initing stats.cpp errno</td>
</tr>
<tr>
<td>Cell Controller Module</td>
<td>LOG_ERR</td>
<td>no shmem!!</td>
</tr>
<tr>
<td>Cell Controller Utility Module</td>
<td>LOG_ERR</td>
<td>Get_Mem: errno [Number] opening %s errno str</td>
</tr>
<tr>
<td>Cell Controller Utility Module</td>
<td>LOG_ERR</td>
<td>Get_Mem: errno [Number] reading file %s errno str</td>
</tr>
<tr>
<td>Cell Controller Utility Module</td>
<td>LOG_ERR</td>
<td>Get_Mem: error parsing file %s str</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_ERR</td>
<td>Unable to read ESS from config</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_ERR</td>
<td>Unable to read Sys-Name from config</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb: error [Number] in decrypt_as_reply) retval</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb: error [Number] in stash_as_reply) retval</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb: error [Number] in verify_as_reply) retval</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb: error [Number] reported by decode_krb5_error) retval</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb: error [Number] reported by encode_krb5_as_req) retval</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb: error [Number] reported by krb5_obtain_padata) retval</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb: socket bind error. errno [Number] errno</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb: socket creation error. errno [Number] errno</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb: socket recv. fd [Number]. errno [Number] fd errno</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb: socket send error on fd [Number]. errno [Number] kdc_fd errno</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_ERR</td>
<td>krb5: error [Number] reported by</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_ERR</td>
<td>krb5: socket rcv. error. errno-[Number] errno</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_ERR</td>
<td>krb5: socket send error. errno-[Number] errno</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_ERR</td>
<td>Socket bind error. errno: [Number] errno</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_ERR</td>
<td>Socket creation error. errno: [Number] errno</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_ERR</td>
<td>ntp enabled but no valid IP address configured</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_ERR</td>
<td>ntp rsp [Number] bytes) from [IP_ADDR] is too small</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_ERR</td>
<td>ntp: error reading configuration</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_ERR</td>
<td>ntp:socket bind error. errno-[Number] errno</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_ERR</td>
<td>ntp:socket create error. errno-[Number] errno</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_ERR</td>
<td>ntp:socket recv error. errno-[Number] errno</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_ERR</td>
<td>ntp:socket send error. errno-[Number] errno</td>
</tr>
<tr>
<td>portalcfg.cpp</td>
<td>LOG_ERR</td>
<td>rfport: error: ess cannot map to multiple bss</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| RADIUS Module                    | LOG_ERR     | eap code [Number] != EAP-RSP for [MAC_ADDR]. Ignoring
RADIUS Module                    | LOG_ERR     | errno [Number] reading Radius rsp errno                                                                                                        |
| RADIUS Module                    | LOG_ERR     | errno [Number] sending radius request to [IP_ADDR]:[Number].                                                                                   |
| RADIUS Module                    | LOG_ERR     | Invalid MPPE key size [Number] bytes) ptext[0]                                                                                                  |
| RADIUS Module                    | LOG_ERR     | MPPE Key decrypt failed. Server: [IP_ADDR]                                                                                                    |
| RADIUS Module                    | LOG_ERR     | MPPE key rcvd is too big [Number] bytes len                                                                                                  |
| RADIUS Module                    | LOG_ERR     | Over [Number] attributes in rsp from [IP_ADDR] Dropping!                                                                                     |
| RF Port Image Module             | LOG_ERR     | bad size %ld of RFP Image img_ptr->len                                                                                                        |
| RF Port Image Module             | LOG_ERR     | bad header len in RFP Image                                                                                                                    |
| RF Port Image Module             | LOG_ERR     | bad magic value in RFP Image                                                                                                                   |
| RF Port Image Module             | LOG_ERR     | can’t allocate %ld bytes img_ptr->len + RFP_IMG_CHECKSUM_SIZE                                                                               |
| RF Port Image Module             | LOG_ERR     | Can’t allocate image %s img_ptr->img_name                                                                                                     |
| RF Port Image Module             | LOG_ERR     | can’t find eof in RFP Image                                                                                                                    |
| RF Port Image Module             | LOG_ERR     | can’t read RFP Image file                                                                                                                     |
| RF Port Image Module             | LOG_ERR     | can’t reset stream offset for %s img_ptr->img_name                                                                                            |
| RF Port Image Module             | LOG_ERR     | Image header check failed %s img_ptr->img_name                                                                                                |
| RF Port Module                   | LOG_ERR     | bad cfg seq for [MAC_ADDR]. expected [Number] got [Number].                                                                                   |
| RF Port Module                   | LOG_ERR     | Cfg rejected by [MAC_ADDR] err=[Number] addr cfg_err                                                                                           |
| RF Port Module                   | LOG_ERR     | error:[MAC_ADDR] is doing unconfigured acs addr                                                                                                |
| RF Port Module                   | LOG_ERR     | old status for [MAC_ADDR]. expected [Number] got [Number].                                                                                     |
| Rogue AP Detection Module        | LOG_ERR     | no ccb cannot send WNMP msg                                                                                                                    |
| Rogue AP Detection Module        | LOG_ERR     | Unable to read rogue-detection timeout from cfg                                                                                              |
| Rogue AP Detection Module        | LOG_ERR     | Unable to read watched_mac from cfg                                                                                                             |
| Rogue AP Detection Module        | LOG_ERR     | Unable to read watchedssid from cfg                                                                                                            |
| Receive Packets Module           | LOG_ERR     | rx data frame of unexpected ethernet                                                                                                           |
| Receive Packets Module           | LOG_ERR     | rxpkts:bad ctl %04x from [[MAC_ADDR]] pkt_ptr->ctl pkt_ptr->src                                                                               |
| Receive Packets Module           | LOG_ERR     | rxpkts:bad dest [[MAC_ADDR]] from [[MAC_ADDR]] pkt_ptr->src pkt_ptr->src                                                                         |
| Statistics Module                | LOG_ERR     | errno [Number] sending trap to SNMPD
errno                                                                                                                        |
| Statistics Module                | LOG_ERR     | errno [Number] sending trap to SNMPD
errno                                                                                                                        |
<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistics Module</td>
<td>LOG_ERR</td>
<td>stats driver rcvd unexpected cmd: [Number]n stats-&gt;cmd</td>
</tr>
<tr>
<td>VLAN Module</td>
<td>LOG_ERR</td>
<td>%s:cannot open %s <strong>FILE</strong> __SW_DEV_PATH_NAME</td>
</tr>
<tr>
<td>VLAN Module</td>
<td>LOG_ERR</td>
<td>Error: Port [Number] assigned to [Number] vlans</td>
</tr>
<tr>
<td>VLAN Module</td>
<td>LOG_ERR</td>
<td>Invalid subnet value [Number] in cfg</td>
</tr>
<tr>
<td>VLAN Module</td>
<td>LOG_ERR</td>
<td>Invalid subnet value [Number] in cfg</td>
</tr>
<tr>
<td>Wireless Switch Protocol Module</td>
<td>LOG_ERR</td>
<td>deleting prev rfport instance [MAC_ADDR] rx_wh-&gt;src</td>
</tr>
<tr>
<td>Wireless Switch Protocol Module</td>
<td>LOG_ERR</td>
<td>portal [[MAC_ADDR][Number] not allowed in cfg prtl_ptr-&gt;addr prtl_ptr-&gt;state</td>
</tr>
<tr>
<td>Wireless Switch Protocol Module</td>
<td>LOG_ERR</td>
<td>resetting rf port [[MAC_ADDR]] rfp_ptr-&gt;addr</td>
</tr>
<tr>
<td>Wireless Switch Protocol Module</td>
<td>LOG_ERR</td>
<td>RF Port [MAC_ADDR] no free rfp rx_wh-&gt;src</td>
</tr>
<tr>
<td>Wireless Switch Protocol Module</td>
<td>LOG_ERR</td>
<td>Rx device info from [MAC_ADDR] rx_wh-&gt;src</td>
</tr>
<tr>
<td>Wireless Switch Protocol Module</td>
<td>LOG_ERR</td>
<td>wisp:could not find rport image</td>
</tr>
<tr>
<td>RF Port Image Module</td>
<td>LOG_ERR</td>
<td>can’t open image file</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>Cannot create any more SIP sessions - max limit reached</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Invite received with NULL call id</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Cancel received with NULL call id</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Cancel received for an invalid call id [ identifier ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Ack received with NULL call id</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Ack received for an invalid call id [ identifier ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Bye received for an invalid call id [ identifier ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Bye received with NULL call id</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Status message received with NULL status code</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Status message received with NULL call id</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Status message received for an invalid call id [ identifier ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Status message received at invalid state for call id [ identifier ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:Status message received at invalid state for call id [ identifier ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_ERR</td>
<td>SIP:status message received with invalid error code [ number ]</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Could not read WIPS state</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Could not open socket</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Could not bind to socket</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Could not set socket options</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Error in receiving command</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Bad sensor command received</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>WIPS : Invalid AD command [command] received</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Invalid AP MAC. Can not convert to sensor</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Can not convert the non-existing AP300 [MAC] to sensor</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Invalid AP MAC. Can not revert to AP</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Could not revert. Sensor [MAC] was not found</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Could not get free buffer</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Invalid AP MAC. Can not send cfg to sensor</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>AD packet with invalid MAC is received</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Ack from an unknown sensor</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Could not remove sensor [MAC]</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Config from an unknown sensor</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Configuration with bad length is received from [MAC]</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Unexpected config reply from [MAC]</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Could not send back data</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Error reading configuration</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Could not find RF port [MAC]</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_ERR</td>
<td>Invalid AP MAC. Can not get sensor config</td>
</tr>
<tr>
<td>AP Revert</td>
<td>LOG_ERR</td>
<td>RF Port [MAC] no free rfp</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_ERR</td>
<td>Port Auto-neg Get failed for port [port idx]</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_ERR</td>
<td>Port Speed Get failed for port [port idx]</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_ERR</td>
<td>Port Duplex Get failed for port [port idx]</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_ERR</td>
<td>ioctl Read failed for Lan Port [port idx]</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_ERR</td>
<td>Read failed for Wan registers</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_ERR</td>
<td>Write failed for Wan registers</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_ERR</td>
<td>&quot;GET ERR in port cfg, sw registers may not set for port = [idx]&quot;</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_ERR</td>
<td>&quot;GET ERR in port cfg, sw registers may not set for wan.&quot;</td>
</tr>
<tr>
<td>CF Format</td>
<td>LOG_ERR</td>
<td>Could not format cf card</td>
</tr>
<tr>
<td>CF Format</td>
<td>LOG_ERR</td>
<td>Error in sending the CF format message</td>
</tr>
<tr>
<td>CF Format</td>
<td>LOG_ERR</td>
<td>Could not open cf format status file</td>
</tr>
<tr>
<td>CF Format</td>
<td>LOG_ERR</td>
<td>Could not lock cf format status file</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CF Format</td>
<td>LOG_ERR</td>
<td>Could not read cf format status file</td>
</tr>
<tr>
<td>CF Format</td>
<td>LOG_ERR</td>
<td>Could not unlock cf format status file</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalid Row returning -1</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error reading config id [config id value]</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Bad parameters passed</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Could not get total entries from WLAN_TRUNK Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Could not get entries from WLAN_TRUNK Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Invalid context</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Could not get total entries from Global IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Could not get entries from Global IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Config read error for WLAN default incoming deny</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Config read error for WLAN default outgoing deny</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Config read error for TRUNK default incoming deny</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Config read error for TRUNK default outgoing deny</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Config read error for WLAN IP Filter Mode</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error: Config read error for TRUNK IP Filter Mode</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not get total entries from Global IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not get Global IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]: Invalid pointer passed</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]: Invalid pointer passed</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalid Length Passed for IP Filter table [length]</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Error reading config id</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalid Length Passed for WLAN Filter table [length]</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]: error getting tot entries glob ipf</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]: error getting glob ipf</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to allocate memory for handler registration</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to allocate memory for table registration info</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to allocate memory for iterator info</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:WLAN index is other than type int</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:WLAN index out of bound</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:tmp-&gt;next_variable NULL pointer</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:list index is other than type int</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:list index out of bound</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>problem encountered in ccWlanFilterTable_Handler: unknown column</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:reqinfo-&gt;mode = MODE_SET_FREE</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:reqinfo-&gt;mode = MODE_SET_UNDO</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>problem encountered in ccWlanFilterTable_Handler: unknown column</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to allocate memory for handler registration</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to allocate memory for table registration info</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to allocate memory for iterator info</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get total entries from WLAN IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get total entries from WLAN IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get total entries from WLAN IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not get total entries from WLAN IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Duplicate filter name in WLAN [wlan-index] IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not get filter policy name required for deletion</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not get filter policy direction required for deletion</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not check whether the entry present in the Global IP Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not write Global IP Filter into the configuration</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get config IDs for the WLAN IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get total entries from WLAN IP Filter Table</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get total entries from WLAN IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not delete entry from WLAN IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>problem encountered in ccWlanIpFilterPolicyTable: unknown column</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not write Global IP Filter into the configuration</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalid index supplied.</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>problem encountered in ccWlanIpFilterPolicyTable_Handler: unknown column</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config read/write error in ccWanTrunkIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:IP Filter mode is disabled on WLAN [wlan-index] Enable it before adding/deleting any entries</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>No such row.</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Row already exists.</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to process set request in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column [column-number] in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column [column-number] in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column [column-number] in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column [column-number] in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Problem encountered in ccWlanIpFilterPolicyTable_Handler: unsupported mode</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config read/write error in ccWanTrunkIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config read/write error in ccWanTrunkIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config read/write error in ccWanTrunkIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config read/write error in ccWanTrunkIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config read/write error in ccWanTrunkIpFilter</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config read/write error in ccWanTrunkIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get TRUNK IP Filter Mode</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get TRUNK IP Filter default incoming action</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get TRUNK IP Filter default outgoing action</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unknown param [magiv value decimal](magic value in hex) requested from ccWanTrunkIpFilterMIB</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to allocate memory for handler registration</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to allocate memory for table registration info</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to allocate memory for iterator info</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWanTrunkIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in cclpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Duplicate filter name in TRUNK IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>&quot;Invalid filter name, add corresponding entry in the Global IP Filter Table&quot;</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWanTrunkIpFilterTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not get filter name at index[filter policy index]</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Duplicate filter name in TRUNK IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWanTrunkIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWanTrunkIpFilterTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not get filter policy name required for deletion</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not get filter policy direction required for deletion</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not check whether the entry present in the Global IP Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not write Global IP Filter into the configuration</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get Trunk IP Filter Table config Ids</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not delete entry from Trunk IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>problem encountered in ccWanTrunkIpFilterTable: unknown column</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not write Global IP Filter into the configuration</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalid index supplied.</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWlanIpFilterPolicyTable</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>problem encountered in ccWanTrunkIpFilterTable_Handler: unknown column</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config read/write error in ccWanTrunkIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>IP Filter mode is disabled on the TRUNK Port Enable it before adding/deleting any entries</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWanTrunkIpFilter</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>No such row.</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccWanTrunkIpFilterTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Row already exists.</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to process set request in ccWanTrunkIpFilterTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column[column number] in ccWanTrunkIpFilterTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column[column number] in ccWanTrunkIpFilterTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column[column number] in ccWanTrunkIpFilterTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column[column number] in ccWanTrunkIpFilterTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Problem encountered in [Function Name]: unsupported mode</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Could not get total entries from TRUNK IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>[Function Name]:Could not get total entries from TRUNK IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Duplicate filter name in TRUNK IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to register ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to register ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to register ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>The filter name is used by either WLAN/TRUNK IP Filter Table's delete before deleting from Global IP Filter Table</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>&quot;Config GET/SET error in ccIpFilterPolicyTable&quot;***</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Start IP is greater than the End IP of either SRC or DEST\</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>problem encountered in ccIpFilterPolicyTable: unknown column</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalid index supplied.</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>problem encountered in ccIpFilterPolicyTable_Handler: unknown column</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>No such row.</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Config GET/SET error in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Row already exists.</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Unable to process set request in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column[wlan-index]\in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column[wlan-index]\in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column[wlan-index]\in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>Invalidation request rcvd for column[wlan-index]\in ccIpFilterPolicyTable</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_ERR</td>
<td>problem encountered in ccIpFilterPolicyTable_Handler: unsupported mode</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR while Get CFG_ID_TEST_INT5 (periodic interval)</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR while Get DYNDNS_USERNAME</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR while Get DYNDNS_PASSWORD</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR Adding DynDNS Service Result: [ Result ]</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR while Get DYNDNS_MODE</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR while Get PPPPOE_MODE</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR while Get DYNDNS_HOSTNAME</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR Adding DynDNS Interface Result [ Result ]</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR in getting wan ip address</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR Adding DynDNS Service Result: %d</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR Delete Interface record</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR Delete Service record</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR while retrieving DynDNS MODE</td>
</tr>
<tr>
<td>DynDNS module</td>
<td>LOG_ERR</td>
<td>ERROR adding Interface record</td>
</tr>
</tbody>
</table>
## Debug-Level Log Entries

<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X Module</td>
<td>LOG_DEBUG</td>
<td>Deauthenticating MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Cell Controlled Module</td>
<td>LOG_DEBUG</td>
<td>Not catching signal [Number] i</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_DEBUG</td>
<td>rcvd [Number] bytes of EAP payload from [MAC_ADDR]</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_DEBUG</td>
<td>sending eap-%s to [MAC_ADDR]</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_DEBUG</td>
<td>sending eap-id-req to [MAC_ADDR] usmu-&gt;mu-&gt;addr</td>
</tr>
<tr>
<td>EAP Module</td>
<td>LOG_DEBUG</td>
<td>sending eapol-key to [MAC_ADDR] usmu-&gt;mu-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_DEBUG</td>
<td>krb: AS_REQUEST sent  to [IP_ADDR] sa.sin_addr.s_addr</td>
</tr>
<tr>
<td>Kerberos Client Module</td>
<td>LOG_DEBUG</td>
<td>krb: received AS_RESPONSE from [IP_ADDR] from_ip</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_DEBUG</td>
<td>krb5: as_request sent to [IP_ADDR] ip</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_DEBUG</td>
<td>krb5: error desc from KDC: %s err_reply-&gt;text.data</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_DEBUG</td>
<td>krb5: rcvd ap_req from MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_DEBUG</td>
<td>krb5: rcvd sk_req from MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_DEBUG</td>
<td>krb5: rcvd tgs_req from MU [MAC_ADDR] mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_DEBUG</td>
<td>krb5: tgs_request sent to [IP_ADDR] ip</td>
</tr>
<tr>
<td>Kerberos Proxy Module</td>
<td>LOG_DEBUG</td>
<td>rcvd WNMP message of type: [Number] from MU [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_DEBUG</td>
<td>Ignoring Assoc_EID Field [Number]) from MU [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_DEBUG</td>
<td>MU [MAC_ADDR] not present in MU table pkt_ptr-&gt;src</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_DEBUG</td>
<td>MU [MAC_ADDR] not present in MU table pkt_ptr-&gt;src</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_DEBUG</td>
<td>MU [MAC_ADDR] not present in MU table pkt_ptr-&gt;src</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_DEBUG</td>
<td>Received Association-Req from [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_DEBUG</td>
<td>Received Authentication-Req from [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_DEBUG</td>
<td>Received DeAuthentication from [MAC_ADDR]</td>
</tr>
<tr>
<td>MU Association Module</td>
<td>LOG_DEBUG</td>
<td>Received ReAssociation-Req from [MAC_ADDR]</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_DEBUG</td>
<td>ntp is disabled in configuration</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_DEBUG</td>
<td>ntp request sent to [IP_ADDR] sa.sin_addr.s_addr</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_DEBUG</td>
<td>ntp server version [Number]) not same as our version</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_DEBUG</td>
<td>ntp: local: %ld.%ld server:%ld.%ld Drift = %ld.%ld\n</td>
</tr>
<tr>
<td>NTP Client Module</td>
<td>LOG_DEBUG</td>
<td>rcvd ntp response from [IP_ADDR] sa.sin_addr.s_addr</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_DEBUG</td>
<td>[Pairwise Transient Key] recv message #2 [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_DEBUG</td>
<td>[Pairwise Transient Key] recv message #4 [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_DEBUG</td>
<td>[Pairwise Transient Key] recv message #6 [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_DEBUG</td>
<td>[Pairwise Transient Key] starting key exchange a) [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_DEBUG</td>
<td>[Pairwise Transient Key] starting key exchange b) [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_DEBUG</td>
<td>[Pairwise Transient Key] xmit message #1 [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_DEBUG</td>
<td>[Pairwise Transient Key] xmit message #3 [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>Encryption Key Exchange Module</td>
<td>LOG_DEBUG</td>
<td>[Pairwise Transient Key] xmit message #5 [MAC_ADDR] mu-&gt;addr</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_DEBUG</td>
<td>access-req sent to [IP_ADDR]:[Number] for [MAC_ADDR]</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_DEBUG</td>
<td>Msg-Auth absent in rsp from [IP_ADDR] from_ip</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_DEBUG</td>
<td>radius rsp from [IP_ADDR] for [MAC_ADDR] rcvd after timeout</td>
</tr>
<tr>
<td>RADIUS Module</td>
<td>LOG_DEBUG</td>
<td>rcvd access-challenge from [IP_ADDR] for [MAC_ADDR]</td>
</tr>
<tr>
<td>Rogue AP Detection Module</td>
<td>LOG_DEBUG</td>
<td>Adding AP: [MAC_ADDR] ESS: %s to reported_ap_list</td>
</tr>
<tr>
<td>Rogue AP Detection Module</td>
<td>LOG_DEBUG</td>
<td>Sent rogue-list req to [MAC_ADDR]! mu_ptr-&gt;addr</td>
</tr>
<tr>
<td>Rogue AP Detection Module</td>
<td>LOG_DEBUG</td>
<td>starting rogue detection requests</td>
</tr>
<tr>
<td>Security Policy Module</td>
<td>LOG_DEBUG</td>
<td>Wlan %x; ESS %s; Auth %s; Enc %s i+1 ess</td>
</tr>
<tr>
<td>Statistics Module</td>
<td>LOG_DEBUG</td>
<td>errno [Number] sending trap to SNMPD\n errno</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP:Decrementing the number of Inactive SIP sessions of portal [address ] to [number ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP:Decrementing the number of Roamed SIP sessions of portal [address ] to [number ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP:Decrementing the number of SIP sessions of MU [address ] to [number ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP:Incrementing the number of SIP sessions of MU [address ] to [number ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP:Cancel received in invalid state for call id [identifier ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP:Changing the state of the SIP session call id [identifier ] to completed</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP:Ack received in invalid state for call id [identifier ]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP:Changing the state of the SIP session call id [identifier ] to terminated</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP: Changing the state of the SIP session call id [identifier] to processed</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP: Removing the SIP session call id [identifier]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP: Timer expired for call id [identifier]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP: MU [addr] associated with different portal [addr]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP: SIP clean up timer called for MU [addr]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP: SIP clean up timer registered for MU [addr]</td>
</tr>
<tr>
<td>SIP Module</td>
<td>LOG_DEBUG</td>
<td>SIP: SIP clean up timer de-registered for MU [addr]</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS : Converting to sensors .....</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS : Resetting [MAC] .....</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS : Sending REVERT command to sensor [MAC] ...</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS : Detection started .....</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>Sending configuration to [MAC].....</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS: ACK received</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS: PINGREPLY received</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS: CONFIGREPLY received</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS: Unknown AD packet is received</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS : Adding sensor [MAC]</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS: Sensor already exists</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>&quot;WIPS : Newly detected sensor, getting configuration...&quot;</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>Configuration updated for [MAC]</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>Unexpected Ack received</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>Configuration received from [MAC]</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>&quot;Converted AP [MAC] did not respond for unicast pings, removing from AP list&quot;</td>
</tr>
<tr>
<td>WIPS module</td>
<td>LOG_DEBUG</td>
<td>WIPS : Unicast ping is sent to [MAC]</td>
</tr>
<tr>
<td>AP Deny List</td>
<td>LOG_DEBUG</td>
<td>RF Port [MAC] is denied for adoption</td>
</tr>
<tr>
<td>AP2AP Beaconing</td>
<td>LOG_DEBUG</td>
<td>Num MUs data received for MU probe request = [num mus]</td>
</tr>
<tr>
<td>AP Revert</td>
<td>LOG_DEBUG</td>
<td>Revert image sent successfully for AP [MAC]</td>
</tr>
<tr>
<td>AP Revert</td>
<td>LOG_DEBUG</td>
<td>&quot;Image found: img_id1 = [image name], id received = [image name]&quot;</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_DEBUG</td>
<td>Register value received for Port [idx] = [register value]</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_DEBUG</td>
<td>Register value to be set for Port [idx] = [register value]</td>
</tr>
<tr>
<td>System Component</td>
<td>Debug Level</td>
<td>Log Message</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_DEBUG</td>
<td>Writing Register values for Wan = [register value]</td>
</tr>
<tr>
<td>Port Configuration</td>
<td>LOG_DEBUG</td>
<td>Setting Wan port configuration.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>LOG_DEBUG</td>
<td>Deleting Default gateway Interface [interface name]</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>LOG_DEBUG</td>
<td>Adding Default gateway: Executing command [cmd]</td>
</tr>
<tr>
<td>CF Format</td>
<td>LOG_DEBUG</td>
<td>CF format message sent ot msg task</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IP Filtering is called from TRUNK OUTGOING context</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>Dropping packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>Allowing packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IP Filtering is called before BCMC_LAN from TRUNK INCOMING context</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IPF: Dropping packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IP Filtering is called from TRUNK INCOMING context</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IPF: Dropping packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IP Filtering is called from WLAN[wlan-index]OUTGOING context</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IPF: Dropping packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IP Filtering is called from PS_Switch_Defrag_Data WLAN[wlan-index] INCOMING context</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IPF: Dropping packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IP Filtering is called from WLAN[wlan-index]OUTGOING context</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IPF: Dropping packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IP Filtering is called from WLAN[wlan-index]INCOMING context</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IPF: Dropping packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IP Filtering is called from BCMC_LAN WLAN[wlan_index]OUTGOING context</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IPF: Dropping packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IP Filtering is called from BCMC_ESS WLAN OUTGOING context</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IPF: Dropping packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>IP Filter Hash Table is locked dropping packet</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>match found</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>ip address mismatch</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>Port mismatch</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>Protocol mismatch</td>
</tr>
<tr>
<td>IP Filter Module</td>
<td>LOG_DEBUG</td>
<td>direction mismatch[incoming/outgoing]</td>
</tr>
</tbody>
</table>
### Emergency Log Entries

<table>
<thead>
<tr>
<th>System Component</th>
<th>Debug Level</th>
<th>Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cell Controller Module</strong></td>
<td>LOG_EMERG</td>
<td>Caught Signal [Number] Aborting with core dump!</td>
</tr>
<tr>
<td><strong>Cell Controller Module</strong></td>
<td>LOG_EMERG</td>
<td>Assertion failed. Aborting with core dump!</td>
</tr>
<tr>
<td><strong>Cell Controller Module</strong></td>
<td>LOG_EMERG</td>
<td>bind failure: address in use. Check</td>
</tr>
<tr>
<td><strong>Cell Controller Utility Module</strong></td>
<td>LOG_EMERG</td>
<td>Assert Fail File %s Line [Number]; Exiting\n file</td>
</tr>
<tr>
<td><strong>Rogue AP Detection Module</strong></td>
<td>LOG_EMERG</td>
<td>memory allocation failure!</td>
</tr>
<tr>
<td><strong>Rogue AP Detection Module</strong></td>
<td>LOG_EMERG</td>
<td>Memory allocation failure!</td>
</tr>
<tr>
<td><strong>Security Policy Module</strong></td>
<td>LOG_EMERG</td>
<td>Config read failure. File: %s Line: [Number] \</td>
</tr>
<tr>
<td><strong>Security Policy Module</strong></td>
<td>LOG_EMERG</td>
<td>Couldn't init Security Policy for WLAN [Number] reverting to defaults</td>
</tr>
<tr>
<td><strong>AP2AP Beaconing</strong></td>
<td>LOG_EMERG</td>
<td>memory allocation failure!</td>
</tr>
</tbody>
</table>
Index

Numerics
1 to 1 NAT ............................................. 4-8
1 to Many NAT ....................................... 4-8
802.11 b/g mode ..................................... 5-22
802.11i encryption .................................. 5-12
802.1x EAP authentication
  advanced settings .................................. 5-9
  configuring ....................................... 5-8
  RADIUS accounting ................................ 5-9
  reauthentication settings ....................... 5-9
  Syslog setup ...................................... 5-9

A
access
  administrator ...................................... 6-2
  configuring for subnets ......................... 3-6
  control, setting ................................. 12-6, 12-38
  points, rogue, see rogue APs.................. 6-2
  types ............................................. 6-2
  user policy ...................................... 6-10
Access Control List, see ACL
Access Ports
  adopting ......................................... 5-5, 12-47
  adoption requirements ......................... 5-15
  advanced properties ............................ 5-25
  advanced radio settings ....................... 5-24
  advanced settings ................................ 5-22
  allowed number per switch .................... 5-15
  antenna settings ................................ 5-24
  approved list .................................... 5-36
  associating to WLANs ............................ 12-21
  authentication ................................... 5-33
  changing name and location .................... 5-17
  configuring ..................................... 5-15, 12-16, 12-54
  error information ................................ 11-12
  general information ................................ 11-11
  installing and testing ......................... 12-65
  interfaces information ......................... 11-5
  managing ........................................ 1-3
  POS ................................................ 12-18
  printer ............................................ 12-19
  radio settings .................................... 5-17, 5-19
  RF status ........................................ 5-17
  rogue, see rogue APs ............................ 6-2
  setting defaults ................................ 5-18, 12-17
  setting rates .................................... 5-20
  specialized radio settings ..................... 5-21
  specifications .................................... 1-3
  statistics ....................................... 11-9
  summary information ............................ 11-9
  traffic information .............................. 11-11
  traps ............................................. 7-26
ACL
  MU access to WLAN ............................... 2-11, 5-14
  setting up ....................................... 7-22
  administration support overview ............... 7-3
  administrator access
    AirBEAM software ................................ 6-3
    authentication .................................. 6-3
    changing password ................................ 6-4
    configuring ..................................... 6-2
Index-2

<table>
<thead>
<tr>
<th>Section</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS setup</td>
<td>8-3</td>
</tr>
<tr>
<td>settings</td>
<td>8-2</td>
</tr>
<tr>
<td>aggressive mode</td>
<td>4-19</td>
</tr>
<tr>
<td>AirBEAM software</td>
<td></td>
</tr>
<tr>
<td>CF Card access</td>
<td>6-3</td>
</tr>
<tr>
<td>description</td>
<td>12-6</td>
</tr>
<tr>
<td>setting up access</td>
<td>8-3</td>
</tr>
<tr>
<td>settings</td>
<td>12-38</td>
</tr>
<tr>
<td>allow rules</td>
<td>4-20</td>
</tr>
<tr>
<td>antenna settings</td>
<td>5-19, 5-24</td>
</tr>
<tr>
<td>AP 300 Access Port authentication</td>
<td>5-33</td>
</tr>
<tr>
<td>API listing</td>
<td>13-1</td>
</tr>
<tr>
<td>attacks, types</td>
<td>4-6</td>
</tr>
<tr>
<td>authentication</td>
<td></td>
</tr>
<tr>
<td>802.1x EAP</td>
<td>5-8</td>
</tr>
<tr>
<td>administrator</td>
<td>6-3</td>
</tr>
<tr>
<td>CHAP</td>
<td>2-8, 4-4</td>
</tr>
<tr>
<td>EAP types</td>
<td>6-5</td>
</tr>
<tr>
<td>EAP-TTLS</td>
<td>5-5</td>
</tr>
<tr>
<td>GTC</td>
<td>6-5, 6-6</td>
</tr>
<tr>
<td>header</td>
<td>3-8, 3-10, 3-14</td>
</tr>
<tr>
<td>iKE</td>
<td>4-19</td>
</tr>
<tr>
<td>Kerberos</td>
<td>5-9</td>
</tr>
<tr>
<td>LDAP</td>
<td>8-7</td>
</tr>
<tr>
<td>MSCHAP-V2</td>
<td>6-5, 6-6</td>
</tr>
<tr>
<td>none</td>
<td>5-14</td>
</tr>
<tr>
<td>PAP</td>
<td>2-8, 4-4</td>
</tr>
<tr>
<td>RADIUS server</td>
<td>6-3, 6-5, 6-6</td>
</tr>
<tr>
<td>RIP</td>
<td>4-12</td>
</tr>
<tr>
<td>setting method</td>
<td>2-10</td>
</tr>
<tr>
<td>setting up for AP 300</td>
<td>5-33</td>
</tr>
<tr>
<td>user, configuring</td>
<td>8-4</td>
</tr>
<tr>
<td>WAN methods</td>
<td>2-8, 4-4</td>
</tr>
<tr>
<td>WLANs</td>
<td>5-7</td>
</tr>
<tr>
<td>authorization levels</td>
<td>7-22</td>
</tr>
<tr>
<td>automatic key exchange</td>
<td></td>
</tr>
<tr>
<td>description</td>
<td>4-14</td>
</tr>
<tr>
<td>setting up</td>
<td>4-17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td></td>
</tr>
<tr>
<td>bandwidth, Share Mode settings</td>
<td>5-27</td>
</tr>
<tr>
<td>beacon settings</td>
<td>5-20, 5-26</td>
</tr>
<tr>
<td>blocking</td>
<td></td>
</tr>
<tr>
<td>outbound FTP actions</td>
<td>4-25</td>
</tr>
<tr>
<td>outbound HTTP requests</td>
<td>4-24</td>
</tr>
<tr>
<td>SMTP commands</td>
<td>4-24</td>
</tr>
<tr>
<td>broadcast ESS, answering</td>
<td>5-7</td>
</tr>
<tr>
<td>browser recommendations</td>
<td>1-2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Cell Controller services</td>
<td>1-6</td>
</tr>
<tr>
<td>certificates</td>
<td></td>
</tr>
<tr>
<td>importing CA</td>
<td>6-12</td>
</tr>
<tr>
<td>managing digital</td>
<td>6-12</td>
</tr>
<tr>
<td>request form</td>
<td>6-14</td>
</tr>
<tr>
<td>selecting</td>
<td>6-6</td>
</tr>
<tr>
<td>self, see self certificates</td>
<td></td>
</tr>
<tr>
<td>specifying for IKE</td>
<td>4-22</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td></td>
</tr>
<tr>
<td>DATA command</td>
<td>4-24</td>
</tr>
<tr>
<td>database, local</td>
<td>6-9</td>
</tr>
<tr>
<td>destination ports, description</td>
<td>3-10</td>
</tr>
<tr>
<td>DHCP</td>
<td></td>
</tr>
<tr>
<td>advanced settings</td>
<td>3-5</td>
</tr>
<tr>
<td>configuration</td>
<td>3-4</td>
</tr>
<tr>
<td>description</td>
<td>2-6</td>
</tr>
<tr>
<td>firmware upload options</td>
<td>7-9</td>
</tr>
<tr>
<td>setting up server</td>
<td>7-10</td>
</tr>
<tr>
<td>Diffie-Hellman groups</td>
<td>4-20</td>
</tr>
<tr>
<td>digital certificates, managing</td>
<td>6-12</td>
</tr>
<tr>
<td>dimensions</td>
<td>1-4</td>
</tr>
<tr>
<td>Domain Name Service (DNS) protocol</td>
<td>3-7</td>
</tr>
<tr>
<td>downloads, updated firmware</td>
<td>7-7</td>
</tr>
<tr>
<td>DTIM period</td>
<td>5-21, 5-22, 5-26</td>
</tr>
<tr>
<td>Dynamic Host Configuration Protocol, see DHCP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td></td>
</tr>
<tr>
<td>EAP</td>
<td></td>
</tr>
<tr>
<td>configuring authentication</td>
<td>5-8</td>
</tr>
<tr>
<td>Protected EAP</td>
<td>6-5</td>
</tr>
<tr>
<td>Tunneled TLS EAP</td>
<td>6-5</td>
</tr>
<tr>
<td>type options</td>
<td>6-5</td>
</tr>
<tr>
<td>email address, administrator</td>
<td>2-4</td>
</tr>
<tr>
<td>Encapsulating Security Protocol (ESP)</td>
<td>3-8, 3-10, 3-14</td>
</tr>
<tr>
<td>encryption</td>
<td></td>
</tr>
<tr>
<td>algorithm types</td>
<td>4-16</td>
</tr>
<tr>
<td>KeyGuard</td>
<td>5-13</td>
</tr>
<tr>
<td>none</td>
<td>5-14</td>
</tr>
<tr>
<td>setting method</td>
<td>2-10, 5-10</td>
</tr>
<tr>
<td>WEP</td>
<td>2-10, 5-10</td>
</tr>
<tr>
<td>WPA2-CCMP</td>
<td>5-12</td>
</tr>
</tbody>
</table>
NAT
- 1 to 1 ........................................... 4-8
- 1 to Many ..................................... 4-8
- configuring .................................. 4-7, 12-14
- forward vs. reverse ......................... 3-11
- selecting type ................................. 4-8
- setting timeout ............................... 4-5
- setting up ..................................... 12-45

Network Address Translation, see NAT

network traps .................................... 7-25

NTP server, specifying .......................... 7-28

O
- operating system services ...................... 1-6

P
- PAP authentication ............................. 2-8, 4-4
- passwords
  - AirBEAM ...................................... 6-3
  - changing for administrator ............... 8-4
  - default ...................................... 8-2
  - entering ..................................... 2-3
  - settings ..................................... 7-22
- placement, radio .................................. 5-19
- Point-to-Point Protocol over Ethernet, see PPPoE
- port-based VLANs ............................... 3-12
- ports
  - destination, description .................... 3-10
  - forwarding options ......................... 4-9
  - hardware configuration ........................ 1-4
  - source, description ......................... 3-10
- POS subnet, configuring ...................... 12-8
- Post Office Protocol (POP) ................... 3-7
- power level, radio ............................. 5-19
- power specifications .......................... 1-4
- PPPoE, setting up .............................. 2-8, 4-3
- preamble length ................................ 5-21, 5-25
- Pre-Shared Key (PSK) ......................... 5-12
- primary WLAN .................................. 5-21
- printer subnet, configuring .................. 12-9
- Protected EAP (PEAP) authentication .......... 6-5
- proxy configuration, setting up ............... 6-8

Q
- quality of service (QoS)
  - Bandwidth Share Mode ....................... 5-27
  - configuration ................................ 5-26
  - QUIT command ................................ 4-24

R
- radio settings
  - Access Port options ........................... 5-17, 5-19
  - advanced .................................... 5-24
  - specialized ................................... 5-21
  - RADIUS server
    - accounting .................................. 5-9
    - administrator access ....................... 6-3
    - authentication options ..................... 6-5
    - client authentication ....................... 6-6
    - configuring .................................. 6-5
    - data source .................................. 6-5
    - LDAP settings ................................. 6-7
    - local user database ......................... 6-9
    - proxy configuration ........................... 6-8
    - shared secret ................................ 5-8
    - user access policy ............................ 6-10
  - resetting the switch ......................... 3-11
- RF status
  - Access Ports .................................. 11-12
  - WLAN ........................................ 11-8
- robust security network (RSN) ................. 5-12
- rogue APs
  - detection ..................................... 5-33
  - examining and approving ..................... 5-35
  - getting details ................................ 5-37
  - listing ........................................ 5-36
  - maintaining rule list ....................... 5-35
  - setting SNMP traps ............................ 5-38
  - setting up detection ........................ 5-34
  - traps .......................................... 7-26

S
- SA negotiation .................................. 4-14
- SA negotiation ................................. 4-14
- SA negotiation ................................. 4-14
- setting up ..................................... 12-51
- SAML command .................................. 4-24
- security
  - authorization levels ......................... 7-22
  - available settings and protocols .......... 1-3
  - beacon settings ............................... 5-21
  - firewall ....................................... 1-3
  - SA negotiation ................................ 4-14
- self certificates
SNMP
software
SNMP traps, setting
settings, exporting and importing
SEND command
sequence number prediction attacks
settings, step by step
shared secrets, setting up
short preamble
SMTP
blocking commands
protocol description
SNMP
access
configuring
default configuration
setting version configuration
v1/v2 community definitions
v3 community definitions
SNMP traps, setting
categories and descriptions
configuration
rate traps
rogue APs
selecting
threshold types
v1/v2
v3
software
Cell Controller
gateway services
operating system
overview
source ports, description
source routing attacks
specifications
Access Ports
dimensions
hardware overview
power and environment
SSH, configuring connection parameters
stand-alone mode
static routes, configuring
statistics
Access Ports
interfaces
mobile units
received fields
subnet
transmitted fields
viewing in graph form
WAN
WLAN
subnet access
advanced settings
allowing or denying
configuring
level descriptions
protocols
subnets
access, see subnet access
changing features
configuring
configuring Subnet1
defining
enabling Subnet1
interface information
mapping to VLANs
POS
printer
statistics
summary information
SYN flood attacks
text, command
Syslog setup
system
basic information
basic settings
changing name
configuring settings
overview
settings
traps
updating firmware
viewing log
T
technical specifications
TELNET protocol
Temporal Key Integrity Protocol (TKIP)
TFTP
exporting and importing settings
firmware updates
timeout settings
transform sets
Transmission Control Protocol (TCP)
transport protocol descriptions
traps, see SNMP traps, setting
Tunneled TLS EAP (EAP-TTLS) authentication
tunnels
Advanced Subnet Access
DHCP addresses
setting up without WAN address
trouble establishing
VPN, creating
TX fields, statistics
typographical conventions
U
UFQDN ID type
uniform spreading
URL extensions, blocking
use cases
field office example
retail example
User Datagram Protocol (UDP)
user-based VLANs ........................................ 3-11
user-defined routes, creating .................. 4-11
users
  access policy ...................................... 6-10
  adding to database .............................. 6-10
  authentication, configuring .......... 6-4
  database, managing ......................... 6-9
  ID, entering .................................. 2-3
  RADIUS server settings ................. 6-5

V
Virtual Local Area Networks, see VLANs
Virtual Private Networks, see VPNs
VLANs
  configuration .................................. 3-11
  description .................................. 3-11
  mapping to subnets ......................... 3-12
  types ....................................... 3-11
voice prioritization, configuring .......... 5-28
VPNs
  allow rules .................................. 4-20
  configuring .................................. 4-12, 12-62
  creating tunnels .............................. 4-14
  FAQs ......................................... 4-20
  security ...................................... 1-3
  setting up security ......................... 4-14
  troubleshooting ............................. 4-20
VRFY command .................................. 4-25

W
WAN
  configuring interface ......................... 2-6, 4-2, 12-13, 12-43
  description .................................. 4-2
  external communication .................... 2-7, 4-2
  statistics .................................... 11-2
Weighted Round Robin ......................... 5-27
WEP encryption
  configuring .................................. 5-10
  key settings .................................. 5-11
  modes ....................................... 5-10
  selecting ..................................... 2-10
Wide Area Network, see WAN
Winnuiking attacks ............................... 4-6
Wired Equivalent Privacy, see WEP encryption
Wireless Local Area Networks, see WLANs
WLANs
  advanced settings ............................ 5-6
  assigning Access Ports ..................... 5-5
  authentication ................................ 5-7
  bandwidth share ............................. 5-28
  basic information ............................ 5-3
  configuring .................................. 5-6, 12-22, 12-49
  configuring security ......................... 2-9
  displaying summary information ............ 11-6
  enabling ..................................... 2-8, 5-3
  error information ............................ 2-8, 5-3
  ESSID ....................................... 5-6
  general information ......................... 11-8
  primary ...................................... 5-21
  RF status ..................................... 11-8
  security ...................................... 1-3, 5-7
  statistics .................................... 11-6
  summary of settings ......................... 2-9
  traffic information ......................... 11-8
  voice prioritization ......................... 5-28
  WPA2-CCMP (802.11i) encryption, configuring .... 5-12
  WPA-TKIP encryption, configuring .............. 5-11