

Management Software

AT-WA7400/EU

User's Guide

Copyright © 2007 Allied Telesyn, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc. Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

| | |
|---|----|
| Preface | 15 |
| Where to Find Web-based Guides | 16 |
| Contacting Allied Telesyn | 17 |
| Online Support | 17 |
| Email and Telephone Support | 17 |
| Returning Products | 17 |
| Sales or Corporate Information | 17 |
| Management Software Updates | 17 |
| Chapter 1: Preparing to Set Up the AT-WA7400 Wireless Access Point | 19 |
| Setting Up the Administrator's Computer | 20 |
| Setting Up the Wireless Client Computers | 22 |
| Understanding Dynamic and Static IP Addressing on the AT-WA7400 Management Software | 23 |
| Dynamic IP Addressing | 23 |
| Static IP Addressing | 23 |
| Recovering an IP Address | 24 |
| Chapter 2: Setting up the AT-WA7400 Management Software | 25 |
| Running KickStart to Find Access Points on the Network | 26 |
| Installing KickStart on the Administrator's PC | 30 |
| Logging in to the AT-WA7400 Management Software | 34 |
| Navigating the Web Pages | 36 |
| Links | 36 |
| Menu | 36 |
| Help | 36 |
| Configuring the Basic Settings and Starting the Wireless Network | 37 |
| Configuring the Basic Settings | 37 |
| Default Configuration | 40 |
| Next Steps | 41 |
| Make Sure the Access Point is Connected to the LAN | 41 |
| Test LAN Connectivity with Wireless Clients | 41 |
| Secure and Fine-Tune the Access Point Using Advanced Features | 41 |
| Logging in After the Initial Setup | 42 |
| Chapter 3: Managing Access Points and Clusters | 43 |
| Understanding Clustering | 44 |
| What is a Cluster? | 44 |
| How Many Access Points Can a Cluster Support? | 44 |
| What Kinds of Access Points Can Cluster Together? | 44 |
| What is the Relationship of the Master Access Point to Other Cluster Members? | 44 |
| Which Settings are Shared as Part of the Cluster Configuration and Which Are Not? | 45 |
| Settings Shared in the Cluster Configuration | 45 |
| Settings Not Shared by the Cluster | 45 |
| Cluster Mode | 46 |
| Standalone Mode | 46 |
| Cluster Formation | 47 |
| Cluster Size and Membership | 47 |
| Intra-Cluster Security | 47 |
| Auto-Synch of Cluster Configuration | 47 |
| Understanding and Changing Access Point Settings | 48 |
| Modifying the Location Description | 49 |

| | |
|---|------------|
| Removing an Access Point from the Cluster | 49 |
| Adding an Access Point to a Cluster | 50 |
| Navigating to Configuration Information for a Specific Access Point and Managing Standalone Access Points | 52 |
| Navigating to an Access Point by Using its IP Address in a URL..... | 52 |
| Configuring MAC Address Filtering..... | 53 |
| MAC Filtering of Rogue Access Points | 55 |
| Chapter 4: Managing User Accounts | 57 |
| Adding a User | 58 |
| Editing a User Account | 60 |
| Enabling a User Account | 60 |
| Disabling a User Account | 61 |
| Removing a User Account | 61 |
| Backing Up and Restoring a User Database | 62 |
| Backing Up the User Database | 62 |
| Restoring a User Database from a Backup File | 63 |
| Chapter 5: Session Monitoring | 65 |
| Viewing Sessions Information..... | 66 |
| Viewing Specific Session Information..... | 67 |
| Sorting Session Information | 68 |
| Chapter 6: Channel Management | 69 |
| Understanding Channel Management | 70 |
| How it Works in a Nutshell..... | 70 |
| Overlapping Channels | 70 |
| Example: A Network Before and After Channel Management..... | 71 |
| Displaying the Channel Management Settings..... | 72 |
| Configuring the Channel Management Settings | 73 |
| Stopping or Starting Automatic Channel Assignment..... | 73 |
| Viewing Current Channel Assignments and Setting Locks..... | 73 |
| Updating the Current Channel Settings Manually..... | 74 |
| Viewing the Last Proposed Set of Changes | 74 |
| Configuring Advanced Settings (Customizing and Scheduling Channel Plans) | 75 |
| Chapter 7: Wireless Neighborhoods | 79 |
| Understanding Wireless Neighborhood Information | 80 |
| Displaying the Wireless Neighborhood Information | 81 |
| Viewing Details of a Cluster Member..... | 84 |
| Chapter 8: Configuring Ethernet (Wired) Settings | 87 |
| Setting the DNS Name..... | 88 |
| Enabling or Disabling Guest Access..... | 90 |
| Configuring an Internal LAN and a Guest Network..... | 90 |
| Enabling or Disabling Guest Access..... | 90 |
| Enabling or Disabling Virtual Wireless Networks on the Access Point | 90 |
| Enabling or Disabling Spanning Tree | 92 |
| Configuring the Internal Interface Ethernet Settings | 93 |
| Configuring the Guest Interface Settings | 96 |
| Chapter 9: Configuring the Wireless Settings | 97 |
| Configuring 802.11d Regulatory Domain Support | 98 |
| Configuring the Radio Interface | 100 |
| Configuring Internal Wireless LAN Settings..... | 102 |
| Configuring the Guest Network Wireless Settings | 103 |
| Chapter 10: Configuring Security | 105 |
| Understanding Security Issues on Wireless Networks | 106 |
| How Do I Know Which Security Mode to Use?..... | 106 |
| Comparison of Security Modes for Key Management, Authentication and Encryption Algorithms | 107 |
| When to Use Plain Text..... | 107 |
| When to Use Static WEP | 107 |
| When to Use IEEE 802.1x..... | 108 |

| | |
|---|------------|
| When to Use WPA/WPA2 Personal (PSK) | 110 |
| When to Use WPA/WPA2 Enterprise (RADIUS)..... | 111 |
| Does Prohibiting the Broadcast SSID Enhance Security? | 113 |
| How Does Station Isolation Protect the Network? | 113 |
| Configuring Security Settings | 114 |
| Broadcast SSID, Station Isolation, and Security Mode | 114 |
| Plain Text | 115 |
| Guest Network | 116 |
| Static WEP | 116 |
| Rules to Remember for Static WEP | 119 |
| Example of Using Static WEP | 119 |
| Static WEP with Transfer Key Indexes on Client Stations | 120 |
| IEEE 802.1x | 121 |
| WPA/WPA2 Personal (PSK) | 123 |
| WPA/WPA2 Enterprise (RADIUS)..... | 125 |
| Configuring the IAPP Mapping Table | 129 |
| Configuring SNMP | 131 |
| Chapter 11: Setting Up Guest Access | 133 |
| Understanding the Guest Interface..... | 134 |
| Configuring the Guest Interface..... | 135 |
| Configuring a Guest Network on a Virtual LAN | 135 |
| Configuring the Welcome Screen (Captive Portal)..... | 136 |
| Using the Guest Network as a Client..... | 137 |
| Chapter 12: VLANs | 139 |
| Configuring VLANs..... | 140 |
| Configuring the Management VLAN..... | 143 |
| Chapter 13: Configuring Radio Settings | 145 |
| Understanding Radio Settings..... | 146 |
| Configuring Radio Settings..... | 147 |
| Configuring the Rate Sets | 152 |
| Chapter 14: Load Balancing | 155 |
| Understanding Load Balancing | 156 |
| Identifying the Imbalance: Overworked or Under-utilized Access Points | 156 |
| Specifying Limits for Utilization and Client Associations | 156 |
| Load Balancing and QoS | 156 |
| Configuring Load Balancing | 157 |
| Chapter 15: Configuring Quality of Service (QoS) | 161 |
| Understanding QoS | 162 |
| QoS and Load Balancing | 162 |
| 802.11e and WMM Standards Support | 162 |
| QoS Queues and Parameters to Coordinate Traffic Flow | 162 |
| QoS Queues and Type of Service (ToS) on Packets..... | 163 |
| EDCF Control of Data Frames and Arbitration Interframe Spaces | 164 |
| Random Backoff and Minimum / Maximum Contention Windows..... | 165 |
| Packet Bursting for Better Performance..... | 166 |
| Transmission Opportunity (TXOP) Interval for Client Stations | 166 |
| Configuring QoS Queues | 167 |
| Configuring AP EDCA Parameters..... | 168 |
| Enabling/Disabling Wi-Fi Multimedia | 170 |
| Configuring Station EDCA Parameters | 171 |
| Chapter 16: Configuring the Wireless Distribution System (WDS) | 173 |
| Understanding the Wireless Distribution System..... | 174 |
| Using WDS to Bridge Distant Wired LANs | 174 |
| Using WDS to Extend the Network Beyond the Wired Coverage Area..... | 174 |
| Backup Links and Unwanted Loops in WDS Bridges..... | 175 |
| Security Considerations Related to WDS Bridges..... | 175 |

| | |
|--|------------|
| WDS Guidelines | 176 |
| Configuring WDS Settings | 178 |
| Example of Configuring a WDS Link | 181 |
| Chapter 17: Maintenance and Monitoring | 183 |
| Monitoring Wired and Wireless LAN Settings | 184 |
| Viewing the Event Logs | 186 |
| Log Relay Host for Kernel Messages | 187 |
| Setting Up the Log Relay Host | 187 |
| Enabling or Disabling the Log Relay Host | 188 |
| Events Log | 188 |
| Viewing the Transmit/Receive Statistics | 190 |
| Viewing the Associated Wireless Clients | 192 |
| Link Integrity Monitoring | 192 |
| What is the Difference Between an Association and a Session? | 192 |
| Viewing the Status of Neighboring Access Points | 193 |
| Viewing System Information | 197 |
| Setting the Administrator Password | 199 |
| Enabling the Network Time Protocol (NTP) Server | 202 |
| Setting the HTTP Timeout | 204 |
| Rebooting the Access Point | 205 |
| Resetting the Configuration to Factory Defaults | 206 |
| Upgrading the Firmware | 207 |
| Verifying the Firmware Upgrade | 208 |
| SNMP Firmware Upgrade | 209 |
| Chapter 18: Backing Up and Restoring a Configuration | 211 |
| Backing up the Configuration Settings for an Access Point | 212 |
| Restoring Access Point Settings to a Previous Configuration | 213 |
| Appendix A: Management Software Default Settings | 215 |
| Appendix B: Configuring Security on Wireless Clients | 217 |
| Network Infrastructure and Choosing Between the Built-in or External Authentication Server | 219 |
| I Want to Use the Built-in Authentication Server (EAP-PEAP) | 219 |
| I Want to Use an External RADIUS Server with EAP-TLS Certificates or EAP-PEAP | 219 |
| Make Sure the Wireless Client Software is Up to Date | 220 |
| Accessing the Microsoft Windows Wireless Client Security Settings | 221 |
| Configuring a Client to Access an Unsecure Network (Plain Text mode) | 223 |
| Configuring Static WEP Security on a Client | 224 |
| Connecting to the Wireless Network with a Static WEP Client | 226 |
| Configuring IEEE 802.1x Security on a Client | 227 |
| IEEE 802.1x Client Using EAP/PEAP | 227 |
| IEEE 802.1x Client Using EAP/TLS Certificate | 231 |
| Configuring WPA/WPA2 Enterprise (RADIUS) Security on a Client | 236 |
| WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP | 236 |
| WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate | 241 |
| Configuring WPA/WPA2 Personal (PSK) Security on a Client | 245 |
| Configuring an External RADIUS Server to Recognize the AT-WA7400 Wireless Access Point | 248 |
| Obtaining a TLS-EAP Certificate for a Client | 253 |
| Appendix C: Troubleshooting | 259 |
| Wireless Distribution System (WDS) Problems and Solutions | 260 |
| Cluster Recovery | 261 |
| Reboot or Reset the Access Point | 261 |
| Stop Clustering and Reset Each Access Point in the Cluster | 261 |
| Appendix D: Command Line Interface (CLI) for Access Point Configuration | 265 |
| Comparison of Settings Configurable with the CLI and Web UI | 266 |
| Accessing the CLI for an Access Point | 269 |
| Telnet Connection to the Access Point | 269 |
| SSH Connection to the Access Point | 270 |

| | |
|---|-----|
| Quick View of Commands and How to Get Help | 272 |
| Commands and Syntax | 272 |
| Getting Help on Commands at the CLI | 275 |
| Command Usage and Configuration Examples | 278 |
| Understanding Interfaces as Presented in the CLI | 278 |
| Saving Configuration Changes | 281 |
| Basic Settings | 282 |
| Get the IP Address for the Internal Interface on an Access Point | 283 |
| Get the MAC Address for an Access Point | 283 |
| Get Both the IP Address and MAC Address | 283 |
| Get Common Information on All Interfaces for an Access Point | 284 |
| Get the Firmware Version for the Access Point | 284 |
| Get the Location of the Access Point | 284 |
| Set the Location for an Access Point | 285 |
| Get the Current Password | 285 |
| Set the Password | 285 |
| Get the Wireless Network Name (SSID) | 285 |
| Set the Wireless Network Name (SSID) | 285 |
| Access Point and Cluster Settings | 285 |
| Determine if the Access Point is a Cluster Member or in Standalone Mode | 286 |
| Get MAC Addresses for all Access Points in the Cluster | 286 |
| Configure the Access Point as a Member of a Cluster | 286 |
| Configure the Access Point as a Standalone Device | 287 |
| User Accounts | 287 |
| Get All User Accounts | 287 |
| Add Users | 288 |
| Remove a User Account | 289 |
| Displaying Status | 289 |
| Get Common Information on the Internal Interface for the Access Point | 291 |
| Get Current Settings for the Ethernet (Wired) Internal Interface | 291 |
| Get All Wired Settings for the Wired Internal Interface | 292 |
| Get the MAC Address for the Wired Internal Interface | 292 |
| Get the Network Name (SSID) for the Wired Internal Interface | 292 |
| Get Current Settings for the Ethernet (Wired) Guest Interface | 292 |
| Get Current Wireless (Radio) Settings | 293 |
| Get the Current IEEE 802.11 Radio Mode | 293 |
| Get the Channel the Access Point is Currently Using | 293 |
| Get Basic Radio Settings for the Internal Interface | 293 |
| Get All Radio Settings on the Internal Interface | 294 |
| Get Status on Events | 295 |
| Enable Remote Logging and Specify the Log Relay Host for the Kernel Log | 295 |
| Prerequisites for Remote Logging | 295 |
| View Log Settings | 295 |
| Enable / Disable Log Relay Host | 296 |
| Specify the Relay Host | 296 |
| Specify the Relay Port | 297 |
| Review Log Settings After Configuring Log Relay Host | 297 |
| Get Transmit / Receive Statistics | 297 |
| Get Client Associations | 299 |
| Get Neighboring Access Points | 299 |
| Ethernet (Wired) Interface | 301 |
| Get Summary View of Internal and Guest Interfaces | 302 |
| Get the DNS Name | 302 |
| Set the DNS Name | 302 |
| Get Wired Internal Interface Settings | 302 |
| Get Wired Guest Interface Settings | 302 |
| Set DNS Nameservers to Use Static IP Addresses (Dynamic to Manual Mode) | 303 |
| Set DNS Nameservers to Use DHCP IP Addressing (Manual to Dynamic Mode) | 303 |
| Setting Up the Wireless Interface | 304 |
| Setting Up Security | 304 |

| | |
|--|-----|
| Get the Current Security Mode..... | 305 |
| Get Detailed Description of Current Security Settings..... | 305 |
| Set the Broadcast SSID (Allow or Prohibit)..... | 306 |
| Enable/Disable Station Isolation..... | 306 |
| Set Security to Plain Text..... | 307 |
| Set Security to Static WEP..... | 307 |
| Set the Security Mode..... | 307 |
| Set the Transfer Key Index..... | 307 |
| Set the Key Length..... | 307 |
| Set the Key Type..... | 308 |
| Set the WEP Keys..... | 308 |
| Set the Authentication Algorithm..... | 309 |
| Get Current Security Settings After Re-Configuring to Static WEP Security Mode..... | 309 |
| Set Security to IEEE 802.1x..... | 312 |
| Set the Security Mode..... | 312 |
| Set the Authentication Server..... | 312 |
| Set the RADIUS Key (For External RADIUS Server Only)..... | 313 |
| Enable RADIUS Accounting (External RADIUS Server Only)..... | 313 |
| Get Current Security Settings After Re-Configuring to IEEE 802.1x Security Mode..... | 314 |
| Set Security to WPA/WPA2 Personal (PSK)..... | 315 |
| Set Security to WPA/WPA2 Enterprise (RADIUS)..... | 318 |
| Set the Security Mode..... | 318 |
| Set the WPA Versions..... | 318 |
| Enable Pre-Authentication..... | 318 |
| Set the Cipher Suites..... | 319 |
| Set the Authentication Server..... | 320 |
| Set the RADIUS Key (For External RADIUS Server Only)..... | 320 |
| Enable RADIUS Accounting (External RADIUS Server Only)..... | 321 |
| Allow Non-WPA Clients..... | 321 |
| Get Current Security Settings After Reconfiguring to WPA/WPA2 Enterprise (RADIUS)..... | 321 |
| Enabling and Configuring the Guest Login Welcome Page..... | 323 |
| View Guest Login Settings..... | 323 |
| Enable/Disable the Guest Welcome Page..... | 324 |
| Set Guest Welcome Page Text..... | 324 |
| Review Guest Login Settings..... | 324 |
| Configuring Multiple BSSIDs on Virtual Wireless Networks..... | 325 |
| Configuring Virtual Wireless Network “One” on Radio One..... | 325 |
| Configure These Settings from the Web UI First..... | 325 |
| Use the CLI to Configure Security on the Interface..... | 325 |
| Use the CLI to set the Network Name (SSID) for the New Virtual Wireless Network..... | 326 |
| Creating WVN “Two” on Radio One with WPA security..... | 326 |
| Radio Settings..... | 326 |
| Get IEEE 802.11 Radio Mode..... | 326 |
| Get Radio Channel..... | 327 |
| Get Basic Radio Settings..... | 327 |
| Get All Radio Settings..... | 327 |
| Get Supported Rate Set..... | 328 |
| Get Basic Rate Set..... | 329 |
| Configure Radio Settings..... | 329 |
| Turn the Radio On or Off..... | 329 |
| Set the Radio Mode..... | 329 |
| Enable or Disable Super AG..... | 330 |
| Set the Radio Channel..... | 330 |
| Set the Beacon Interval..... | 330 |
| Set the DTIM Period..... | 330 |
| Set the Fragmentation Threshold..... | 331 |
| Set the RTS Threshold..... | 331 |
| Configure Basic and Supported Rate Sets..... | 331 |
| MAC Filtering..... | 333 |
| Specify an Accept or Deny List..... | 333 |

| | |
|---|------------|
| Add MAC Addresses of Client Stations to the Filtering List | 334 |
| Remove a Client Station's MAC Address from the Filtering List | 334 |
| Getting Current MAC Filtering Settings | 335 |
| Get the Type of MAC Filtering List Currently Set (Accept or Deny) | 335 |
| Get MAC Filtering List | 335 |
| Load Balancing | 335 |
| Quality of Service | 336 |
| Enable/Disable Wi-Fi Multimedia | 338 |
| About Access Point and Station EDCA Parameters | 338 |
| Understanding the Queues for Access Point and Station | 339 |
| Distinguishing between Access Point and Station Settings in QoS Commands | 339 |
| Get QoS Settings on the Access Point | 339 |
| Get QoS Settings on the Client Station | 340 |
| Set Arbitration Interframe Spaces (aifs) | 340 |
| Set AIFs on the Access Point | 340 |
| Set AIFs on the Client Station | 341 |
| Set Minimum and Maximum Contention Windows (cwmin, cwmax) | 341 |
| Set cwmin and cwmax on the Access Point | 342 |
| Set cwmin and cwmax on the Station | 342 |
| Set the Maximum Burst Length (burst) on the Access Point | 343 |
| Set Transmission Opportunity Limit (txop-limit) for WMM client stations | 344 |
| Wireless Distribution System | 344 |
| Configure a WDS Link | 345 |
| Enable the WDS interface (wlan0wds0) on the current access point: | 345 |
| Provide the MAC address of the remote access point to which you want to link: | 345 |
| Get Details on a WDS Configuration | 345 |
| Time Protocol | 347 |
| Rebooting the Access Point | 348 |
| Resetting the Access Point to the Factory Defaults | 348 |
| Keyboard Shortcuts and Tab Completion Help | 349 |
| Keyboard Shortcuts | 349 |
| Tab Completion and Help | 350 |
| CLI Classes and Fields Reference | 354 |
| Appendix E: Radio Bands | 357 |
| Index | 359 |

Figures

| | |
|--|-----|
| Figure 1. AT-WA7400 CD Main Page..... | 27 |
| Figure 2. KickStart Page..... | 27 |
| Figure 3. KickStart Welcome Dialog Box..... | 28 |
| Figure 4. KickStart Search Results Dialog Box..... | 28 |
| Figure 5. Administration Dialog Box..... | 29 |
| Figure 6. KickStart Setup Wizard Dialog Box..... | 30 |
| Figure 7. Select Installation Folder Dialog Box..... | 31 |
| Figure 8. KickStart Setup Disk Space Dialog Box..... | 31 |
| Figure 9. KickStart Installation Confirmation Dialog Box..... | 32 |
| Figure 10. Installing KickStart Dialog Box..... | 32 |
| Figure 11. KickStart Installation Complete Dialog Box..... | 33 |
| Figure 12. Login Dialog Box..... | 34 |
| Figure 13. Basic Settings Page..... | 35 |
| Figure 14. Navigational Aids..... | 36 |
| Figure 15. Summary of Settings Page..... | 40 |
| Figure 16. Default Web Page..... | 42 |
| Figure 17. Access Points Page..... | 48 |
| Figure 18. Settings of Access Point that Joined the Cluster..... | 50 |
| Figure 19. MAC Filtering Page..... | 53 |
| Figure 20. Configure Rogue MAC Filtering of Access Point Page..... | 55 |
| Figure 21. User Management Page..... | 58 |
| Figure 22. User Accounts Section..... | 60 |
| Figure 23. Backup or Restore User Database Page..... | 62 |
| Figure 24. Sessions Page..... | 66 |
| Figure 25. Without Automatic Channel Management: Access Points Can Broadcast on Overlapping Channels..... | 71 |
| Figure 26. With Channel Management Enabled: Access Points are Re-Assigned to Non-Interfering Channels..... | 71 |
| Figure 27. Channel Management Page..... | 72 |
| Figure 28. Wireless Neighborhood Page..... | 81 |
| Figure 29. Neighbor Details Information..... | 84 |
| Figure 30. Ethernet (Wired) Settings Page..... | 88 |
| Figure 31. Wireless Settings Page..... | 98 |
| Figure 32. Security Page..... | 114 |
| Figure 33. Static WEP Security Mode Settings..... | 117 |
| Figure 34. Setting the AP Transfer Key on the Access Point..... | 119 |
| Figure 35. Providing a Wireless Client with a WEP Key..... | 120 |
| Figure 36. Example of Using Multiple WEP Keys and Transfer Key Index on Client Stations..... | 121 |
| Figure 37. IEEE 802.1x Security Mode Settings..... | 122 |
| Figure 38. WPA/WPA2 Personal (PSK) Security Mode Settings..... | 124 |
| Figure 39. WPA/WPA2 Enterprise (RADIUS) Security Mode Settings..... | 126 |
| Figure 40. IAPP Map Table..... | 129 |
| Figure 41. SNMP Configuration Page..... | 131 |
| Figure 42. Guest Login Configuration Page..... | 136 |
| Figure 43. Virtual Wireless Networks Page..... | 140 |
| Figure 44. VLAN Management Page..... | 143 |
| Figure 45. Radio One Page..... | 147 |
| Figure 46. Radio One Rate Sets..... | 152 |
| Figure 47. Radio Two Rate Sets..... | 152 |
| Figure 48. Load Balancing Page..... | 158 |
| Figure 49. Quality of Service Page..... | 168 |
| Figure 50. Example Wireless Network..... | 174 |

| | |
|--|-----|
| Figure 51. WDS Bridge..... | 175 |
| Figure 52. Wireless Distribution System Page..... | 179 |
| Figure 53. Interfaces Page | 184 |
| Figure 54. Events Page | 186 |
| Figure 55. Transmit/Receive Statistics Page..... | 190 |
| Figure 56. Client Associations Page..... | 192 |
| Figure 57. Neighboring Access Points Page | 193 |
| Figure 58. System Information Page | 197 |
| Figure 59. Basic Settings Page..... | 200 |
| Figure 60. Time Protocol Page..... | 202 |
| Figure 61. HTTP Timeout..... | 204 |
| Figure 62. Reboot Page..... | 205 |
| Figure 63. Reset Configuration Page..... | 206 |
| Figure 64. Upgrade Firmware Page..... | 208 |
| Figure 65. Configure SNMP Firmware Upgrade Page..... | 209 |
| Figure 66. Backup/Restore Page..... | 212 |
| Figure 67. Wireless Network Connections Properties Dialog Box..... | 222 |
| Figure 68. Wireless Network Properties Dialog Box..... | 223 |
| Figure 69. Wireless Network Properties Dialog Box..... | 224 |
| Figure 70. Security Settings Page | 225 |
| Figure 71. Wireless Network Properties Dialog Box..... | 226 |
| Figure 72. Security Settings Page | 228 |
| Figure 73. Association and Authentication Tabs..... | 228 |
| Figure 74. Protected EAP Properties Dialog Box and EAP Properties Dialog Box | 230 |
| Figure 75. Security Settings Page | 232 |
| Figure 76. Association and Authentication Tabs..... | 233 |
| Figure 77. Smart Card or other Certificate Properties Dialog Box..... | 234 |
| Figure 78. Security Settings Page | 237 |
| Figure 79. User Management Accounts Page..... | 238 |
| Figure 80. Wireless Network Properties Dialog Box..... | 239 |
| Figure 81. Protected AP Properties Dialog Box..... | 240 |
| Figure 82. Security Settings Page | 242 |
| Figure 83. Association and Authentication Tabs..... | 243 |
| Figure 84. Smart Card or other Certificate Properties Dialog Box..... | 244 |
| Figure 85. Security Settings Page | 245 |
| Figure 86. Association Tab | 246 |
| Figure 87. Security Settings Page | 249 |
| Figure 88. Internet Authentication Service Window..... | 250 |
| Figure 89. New RADIUS Client Dialog Box, Name and Address Dialog Box..... | 251 |
| Figure 90. New RADIUS Client Wizard Additional Information Dialog Box | 251 |
| Figure 91. Internet Authentication Service Window Showing Access Point | 252 |
| Figure 92. Security Alert Window..... | 254 |
| Figure 93. Certificate Server Welcome Page..... | 254 |
| Figure 94. RADIUS Server Login Window | 255 |
| Figure 95. Request a Certificate Page..... | 255 |
| Figure 96. Security Warning Dialog Box..... | 256 |
| Figure 97. User Certificate Dialog Box..... | 256 |
| Figure 98. Potential Scripting Violation Dialog Box..... | 256 |
| Figure 99. Certificate Issued Dialog Box..... | 257 |
| Figure 100. Potential Scripting Error Dialog Box | 257 |
| Figure 101. Root Certificate Store Dialog Box..... | 257 |
| Figure 102. Certificate Installed Confirmation Window | 258 |
| Figure 103. Stop Clustering Page..... | 262 |
| Figure 104. Reset Configuration Page..... | 263 |
| Figure 105. Cluster Management Page..... | 263 |
| Figure 106. PuTTY Configuration Dialog Box..... | 271 |
| Figure 107. CLI Class Relationships..... | 355 |

Tables

| | |
|---|-----|
| Table 1. Static WEP Configuration | 108 |
| Table 2. IEEE 802.1x Configuration | 109 |
| Table 3. WPA/WPA2 Configuration | 110 |
| Table 4. RADIUS Security | 111 |
| Table 5. Worldwide Frequencies for 802.11g and 802.11b Radios | 148 |
| Table 6. Management Software Default Settings | 215 |
| Table 7. Comparison of CLI to Web Browser Interface Settings | 266 |
| Table 8. Commands and Syntax | 273 |
| Table 9. Interfaces in the CLI | 279 |
| Table 10. Basic Settings Commands | 282 |
| Table 11. Cluster Functions and Commands | 286 |
| Table 12. User Account Commands | 287 |
| Table 13. Status Commands | 290 |
| Table 14. Wired Interface Commands | 301 |
| Table 15. Security Commands | 304 |
| Table 16. WEP Key Length Commands | 308 |
| Table 17. Key Type Commands | 308 |
| Table 18. Authentication Algorithm Commands | 309 |
| Table 19. Authentication Server Commands | 312 |
| Table 20. RADIUS Accounting Commands | 313 |
| Table 21. WPA Version | 315 |
| Table 22. Cipher Commands | 316 |
| Table 23. WPA Version Command | 318 |
| Table 24. Preauthentication Commands | 319 |
| Table 25. Cipher Commands | 319 |
| Table 26. Authentication Server Commands | 320 |
| Table 27. RADIUS Accounting Commands | 321 |
| Table 28. WPA Client Commands | 321 |
| Table 29. Guest Login and Welcome Page Commands | 323 |
| Table 30. Radio Settings Commands | 326 |
| Table 31. Radio Operation Commands | 329 |
| Table 32. Radio Mode Commands | 330 |
| Table 33. Rate Set Commands | 331 |
| Table 34. Accept and Deny List Commands | 334 |
| Table 35. QoS Commands | 337 |
| Table 36. Queue Commands | 339 |
| Table 37. WDS Commands | 345 |
| Table 38. Keyboard Shortcuts | 349 |

Preface

This guide contains instructions on how to configure and maintain an AT-WA7400 Wireless Access Point using its management software and contains the following sections:

- “Where to Find Web-based Guides” on page 16
- “Contacting Allied Telesyn” on page 17

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in portable document format (PDF) on our web site at **www.alliedtelesyn.com**. You can view the documents online or download them onto a local workstation or server.

Contacting Allied Telesyn

This section provides Allied Telesyn contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base: <http://kb.alliedtelesyn.com>. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesyn web site: www.alliedtelesyn.com.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesyn without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesyn Technical Support through our web site: www.alliedtelesyn.com.

Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information through our web site: www.alliedtelesyn.com. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Management Software Updates

New releases of management software for our managed products are available from either of the following Internet sites:

- Allied Telesyn web site: www.alliedtelesyn.com
- Allied Telesyn FTP server: <ftp://ftp.alliedtelesyn.com>

If you prefer to download new software from the Allied Telesyn FTP server from your workstation's command prompt, you will need FTP client software and you must log in to the server. Enter "anonymous" for the user name and your email address for the password.

Chapter 1

Preparing to Set Up the AT-WA7400 Wireless Access Point

Before you plug in and boot a new AT-WA7400 Wireless Access Point, review the following sections for a quick check of required hardware components, software, client configurations, and compatibility issues. Make sure you have everything you need ready to go for a successful launch and test of your new (or extended) wireless network.

This chapter contains the following sections:

- “Setting Up the Administrator’s Computer” on page 20
- “Setting Up the Wireless Client Computers” on page 22
- “Understanding Dynamic and Static IP Addressing on the AT-WA7400 Management Software” on page 23

Setting Up the Administrator's Computer

You configure and administer the AT-WA7400 Wireless Access Point with the KickStart utility (which you run from the CD), through a web-based user interface (UI), or through the command line interface. In order to successfully start the management software, the administrator's computer must be set up with the following hardware and software components:

- ❑ Ethernet connection
The computer used to configure the first AT-WA7400 Wireless Access Point with KickStart must be connected to the access point, either directly or through a hub, by an Ethernet cable.
- ❑ Wireless Connection to the Network
After you initially configure and launch the first AT-WA7400 Wireless Access Point, you can make further configuration changes through the management software using a wireless connection to the "internal" network. This configuration includes:
 - Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. (IEEE 802.11a, 802.11b, 802.11g, and 802.11a Turbo modes are supported.)
 - Wireless client software such as Microsoft Windows XP or Funk Odyssey wireless client configured to associate with the AT-WA7400 Management Software.

For more details about the Wi-Fi client setup, see "Setting Up the Wireless Client Computers" on page 22.

- ❑ Web browser/operating system
Configuration and administration of the AT-WA7400 Wireless Access Point is provided through a web-based user interface hosted on the access point. Allied Telesyn recommends using one of the following supported web browsers to access the AT-WA7400 management software:
 - Microsoft Internet Explorer version 5.5 or greater (with up-to-date patch level for either major version) on Microsoft Windows XP or Microsoft Windows 2000
 - Netscape Mozilla 1.7.x on Redhat Linux version 2.4

The administration web browser must have JavaScript enabled to support the interactive features of the administration interface. It must also support HTTP uploads to use the firmware upgrade feature.

- ❑ *AT-WA7400 Software and Documentation CD*
This CD contains the KickStart utility and the software documentation. You can run the KickStart utility on any Windows laptop or computer

that is connected to the access point (via wired or wireless connection). It detects AT-WA7400 Wireless Access Points on the network. The wizard steps you through initial configuration of new access points, and provides a link to the AT-WA7400 management software where you finish the basic setup process in a step-by-step mode and launch the network.

You can also download KickStart onto the administrator's computer which makes it unnecessary to have the CD.

For more about using KickStart, see "Running KickStart to Find Access Points on the Network" on page 26.

- ❑ **CD-ROM Drive**
The administrator's computer must have a CD-ROM drive to run the KickStart application on the *AT-WA7400 Wireless Access Point* CD or to download it to their computer.
- ❑ **Security Settings**
Ensure that security is disabled on the wireless client used to initially configure the access point.

Setting Up the Wireless Client Computers

The AT-WA7400 Wireless Access Point provides wireless access to any client with a properly configured Wi-Fi client adapter for the 802.11 mode in which the access point is running.

Multiple client operating systems are supported. Clients can be laptops or desktops, personal digital assistants (PDAs), or any other hand-held, portable or stationary device equipped with a Wi-Fi adapter and supporting drivers.

In order to connect to the access point, wireless clients need the following software and hardware:

- ❑ **Wi-Fi Client Adapter**
Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. (IEEE 802.11a, 802.11b, 802.11g, and 802.11a Turbo modes are supported.)

Wi-Fi client adapters vary considerably. The adapter can be a PC card built in to the client device, a portable PCMCIA or PCI card (types of NICs), or an external device such as a USB or Ethernet adapter that you connect to the client by means of a cable.

The AT-WA7400 Wireless Access Point supports 802.11a/g modes. The fundamental requirement for clients is that they all have configured adapters that match the 802.11 a/g mode.

- ❑ **Wireless Client Software**
Client software such as Microsoft Windows Supplicant or Funk Odyssey wireless client configured to associate with the AT-WA7400 Management Software.
- ❑ **Client Security Settings**
Security should be disabled on the client used to do initial configuration of the access point.

If the Security mode on the access point is set to anything other than plain text, wireless clients will need to set a profile to the authentication mode used by the access point and provide a valid username and password, certificate, or similar user identity proof. Security modes are Static WEP, IEEE 802.1x, WPA with RADIUS server, and WPA-PSK.

For information on configuring security on the access point, see Chapter 10, “Configuring Security” on page 105.

Understanding Dynamic and Static IP Addressing on the AT-WA7400 Management Software

Very little setup is required for the first access point and no configuration required for additional access points subsequently joining a pre-configured *cluster*.

When you run KickStart, it discovers the AT-WA7400 Wireless Access Points on the network and lists their IP addresses and MAC addresses. KickStart also provides a link to the administration web pages of each access point using the IP address in the URL. (For more information about the KickStart utility, see “Running KickStart to Find Access Points on the Network” on page 26.)

Dynamic IP Addressing

The AT-WA7400 Wireless Access Point generally expects that a DHCP server is running on the network where the access point is deployed. Most home and small business networks already have DHCP service provided either via a gateway device or a centralized server. However, if no DHCP server is present on the internal network, the access point will use the default static IP address in the Static IP address field for first time startup.

Similarly, wireless clients and other network devices (such as printers) will receive their IP addresses from the DHCP server, if there is one. If no DHCP server is present on the network, you must manually assign static IP addresses to your wireless clients and other network devices.

Static IP Addressing

The AT-WA7400 Wireless Access Point is shipped with a default static IP address of 192.168.1.230. (See Appendix A, “Management Software Default Settings” on page 215.) If no DHCP server is found on the network, the access point retains this static IP address at first-time startup.

After the access point starts up, you have the option of specifying a static IP addressing policy on AT-WA7400 Wireless Access Point and assigning static IP addresses to access points on the internal network using the management software. (See information about the Connection Type field and related fields in “Enabling or Disabling Guest Access” on page 90.)



Caution

If you do not have a DHCP server on the internal network and do not plan to use one, the first thing you must do after bringing up the access point is to verify that the Connection Type is Static IP. You can either assign a new Static IP address to the access point or continue using the default address. Allied Telesyn recommends assigning a new Static IP address so that if later you bring up another AT-WA7400 Wireless Access Point on the same network, the IP address for each access point will be unique.

Recovering an IP Address

If you experience trouble communicating with the access point, you can recover a static IP address by resetting the access point configuration to the factory defaults (see “Resetting the Configuration to Factory Defaults” on page 206), or you can get a dynamically assigned address by connecting the access point to a network that has DHCP.

Chapter 2

Setting up the AT-WA7400 Management Software

Setting up and deploying one or more AT-WA7400 Wireless Access Points is in effect creating and launching a *wireless network*. The KickStart utility and corresponding AT-WA7400 Management Software Basic Settings web page simplify this process. This chapter contains procedures for setting up your AT-WA7400 Wireless Access Points and the resulting wireless network. Have the *AT-WA7400 Wireless Access Point* CD handy, and familiarize yourself with the default settings described in Appendix A, “Management Software Default Settings” on page 215.

This chapter includes the following procedures:

- ❑ “Running KickStart to Find Access Points on the Network” on page 26
- ❑ “Logging in to the AT-WA7400 Management Software” on page 34
- ❑ “Navigating the Web Pages” on page 36
- ❑ “Configuring the Basic Settings and Starting the Wireless Network” on page 37
- ❑ “Next Steps” on page 41
- ❑ “Logging in After the Initial Setup” on page 42

Running KickStart to Find Access Points on the Network

KickStart is an easy-to-use utility for discovering and identifying new AT-WA7400 Wireless Access Points. KickStart scans the network looking for access points, displays ID details on those it finds, and provides access to the AT-WA7400 Management Software.

Note

KickStart (and the other AT-WA7400 tools) recognizes and configures only AT-WA7400 Wireless Access Points. KickStart will not find or configure non-AT-WA7400 Wireless Access Points and will not find any other devices.

Note

Run KickStart only in the subnet of the internal network (SSID).

Note

KickStart finds only those access points that have IP addresses. IP addresses are dynamically assigned to access points if you have a DHCP server running on the network. If you deploy the access point on a network with no DHCP server, the default static IP address (192.168.1.230) is used.

**Caution**

Use caution with non-DHCP enabled networks: Do not deploy more than one new access point on a non-DHCP network because they will use the same default static IP addresses and conflict with each other. (For more information, see “Understanding Dynamic and Static IP Addressing on the AT-WA7400 Management Software” on page 23.)

To start the discovery process, perform the following procedure:

1. Do one of the following to create an Ethernet connection between the access point and your computer:
 - Connect one end of an Ethernet cable to the LAN port on the access point and the other end to the same hub where your PC is connected.
 - Connect one end of an Ethernet cable to the LAN port on the access point and the other end of the cable to the Ethernet port on your PC.

2. Insert the **AT-WA7400 Wireless Access Point** CD into the CD-ROM drive on your computer.

The CD's main page is shown in Figure 1.



Figure 1. AT-WA7400 CD Main Page

3. Click **KickStart Utility**.

The KickStart page, as shown in Figure 3, provides two options: Open KickStart and Install KickStart.

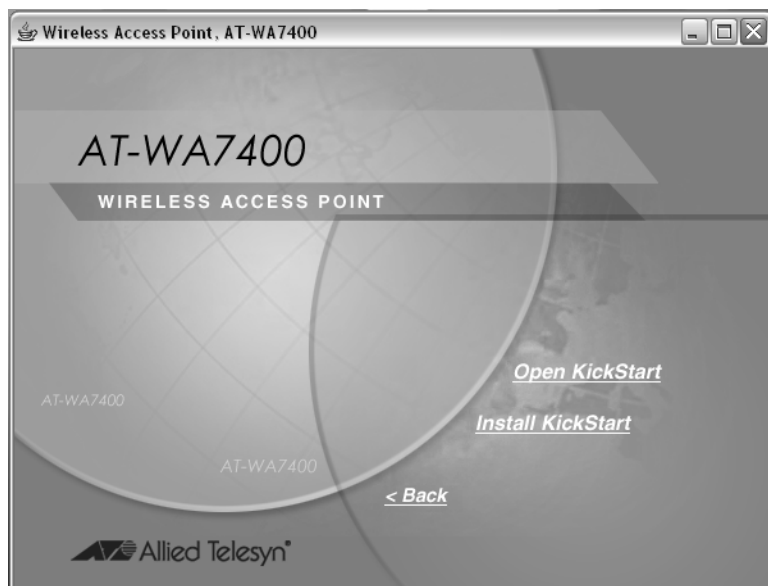


Figure 2. KickStart Page

For information about installing KickStart, refer to “Installing KickStart on the Administrator’s PC” on page 30. Otherwise, continue with this procedure.

- 4. Click **Open KickStart**.

The KickStart Welcome dialog box is displayed, as shown in Figure 3.

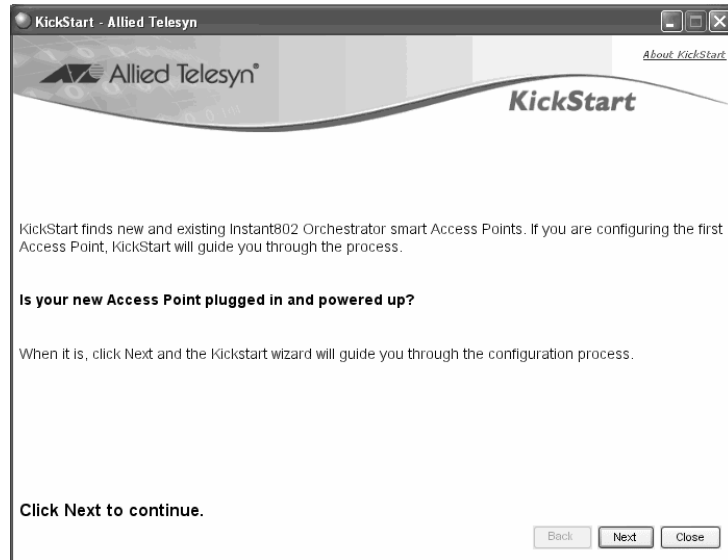


Figure 3. KickStart Welcome Dialog Box

- 5. Click **Next** to search for access points.

Wait for the search to complete, or until KickStart has found your new access points, as shown in Figure 4.



Figure 4. KickStart Search Results Dialog Box

Note

The KickStart utility only finds other AT-WA7400 Wireless Access Points.

If KickStart does not find the AT-WA7400 Wireless Access Point you just installed, an informational window is displayed with troubleshooting information about your LAN and power connections.

6. Review the list of access points that KickStart found, as shown in the example in Figure 4 on page 28..

The access points are listed with their locations, media access control (MAC) addresses, and IP addresses. If you are installing the first access point on a single-access-point network, only one entry is displayed on this page.

7. Verify the MAC addresses against the hardware labels for each access point. This will be especially helpful later in providing or modifying the descriptive Location name for each access point.
8. Click **Next**.

The Administration dialog box opens, as shown in Figure 5.



Figure 5. Administration Dialog Box

Note

KickStart provides a link to the AT-WA7400 management software web pages via the IP address of the first access point of each model. (For more information about model types and clustering see “What Kinds of Access Points Can Cluster Together?” on page 44.)

The AT-WA7400 management software is a centralized management tool that you can access through the IP address for any access point in a cluster.

After your other access points are configured, you can also link to the AT-WA7400 management software web pages using the IP address for any of the other AT-WA7400 Wireless Access Points, for example `http://IPAddressOfAccessPoint`.

Installing KickStart on the Administrator's PC

To install the KickStart utility on the administrator's PC, perform the following procedure:

1. Insert the **AT-WA7400 Wireless Access Point** CD into the CD-ROM drive on your computer.

The CD's main page is shown in Figure 1 on page 27. Click **KickStart Utility**.

The KickStart page, as shown in Figure 2 on page 27, provides two options: Open KickStart and Install KickStart.

The Open KickStart option is described in "Running KickStart to Find Access Points on the Network" on page 26.

2. Click **Install KickStart**.

The KickStart Setup Wizard dialog box is shown in Figure 6.



Figure 6. KickStart Setup Wizard Dialog Box

3. Click **Next**.

The Select Installation Folder dialog box is shown in Figure 7.

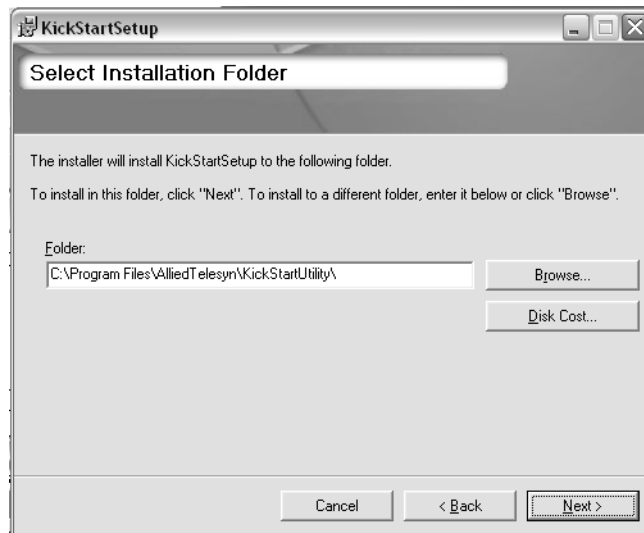


Figure 7. Select Installation Folder Dialog Box

4. Do one of the following:

- To see how much disk space the files require, click **Disk Cost**.

The KickStart Setup Disk Space window is shown in Figure 8.

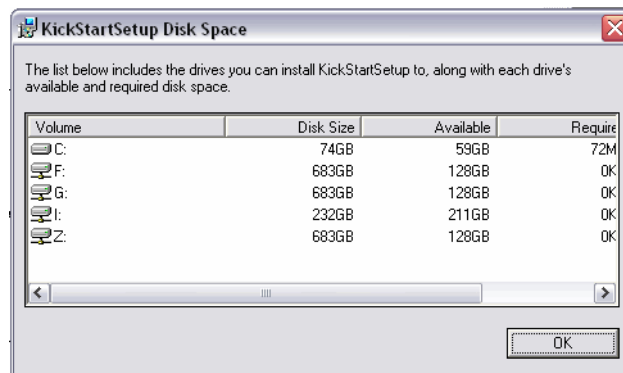


Figure 8. KickStart Setup Disk Space Dialog Box

Select the drive where you want to install KickStart, and then click **OK**.

- Click **Browse** to select a specific location for the KickStart utility.

The Browse for Folder window shows the default folder where the utility will be installed unless you select a different location. If this selection is OK, click **OK**. Otherwise, select a different folder and click **OK**.

5. Click **Next**.

The KickStart Setup confirmation dialog box is shown in Figure 9.

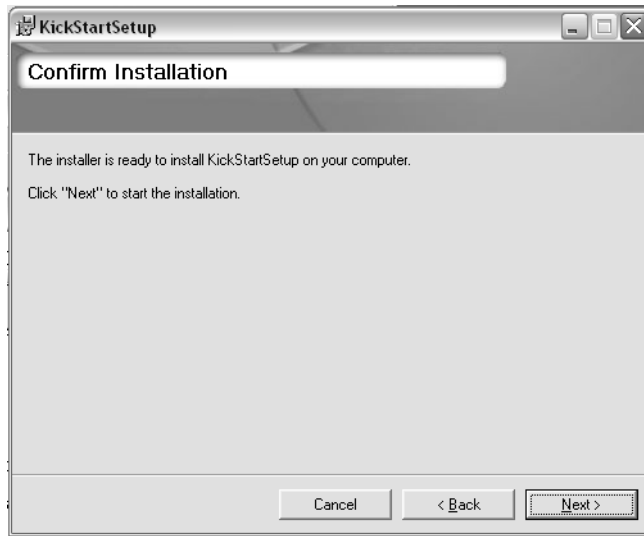


Figure 9. KickStart Installation Confirmation Dialog Box

6. Click **Next** to start the installation.

The Installing KickStart dialog box is shown in Figure 10.

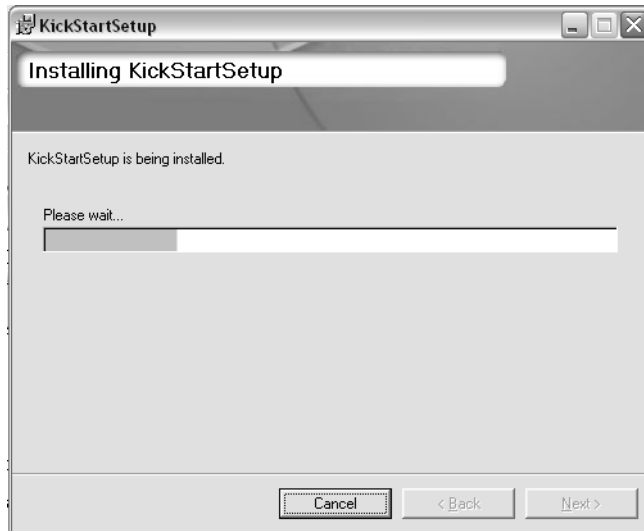


Figure 10. Installing KickStart Dialog Box

When the installation is complete, the Installation Complete dialog box is displayed, as shown in Figure 11.

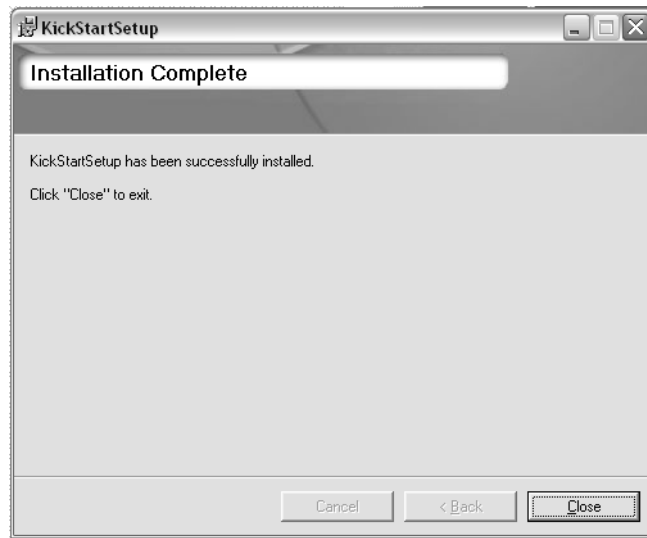


Figure 11. KickStart Installation Complete Dialog Box

7. Click **Close**.

You can now run KickStart from the Programs folder under Allied Telesyn.

Logging in to the AT-WA7400 Management Software

To access the AT-WA7400 management software, perform the following procedure:

1. In the KickStart Administration dialog box, click **Administration**.

You are prompted for a user name and password, as shown in Figure 12.



Figure 12. Login Dialog Box

The defaults for user name and password are:

Username

manager

Password

friend

Note

You cannot modify the user name.

2. Enter the username and password and click **OK**.

When you log in for the first time, the Basic Settings page is displayed, as shown in Figure 13. This page displays the global settings for all access points that are members of the cluster and, if you specify automatic configuration, for any new access points that you add later.

Provide basic settings

1 Review Description of this Access Point ...


These fields show information specific to this access point.


IP Address: 10.10.20.230


MAC Address: 00:0c:46:f2:d7:64

Firmware Version: wa7400 ver 1.11.06c_DUAL (Jan 24 2006 10:45:53)

Location

Clustered 

0 Access Points 

0 User Accounts 

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster if the policy for adding new access points is set to "configure automatically".

Current Password

New Password

Confirm New Password

Wireless Network Name (SSID)

3 Set Configuration Policy for New Access Points ...

If you choose "configure automatically" as the policy for adding new access points, new access points will join the cluster when they are powered up and inherit the settings specified on this page. (If you choose to ignore new access points, you must configure them manually.)

New Access Points

This access point is in standalone mode. If you need to change these settings, click the "Access Points" tab.

4 Settings ...

Click "update" to save the new settings.

Figure 13. Basic Settings Page

Navigating the Web Pages

The web pages provide several ways that you can navigate through the software, as shown in Figure 14.

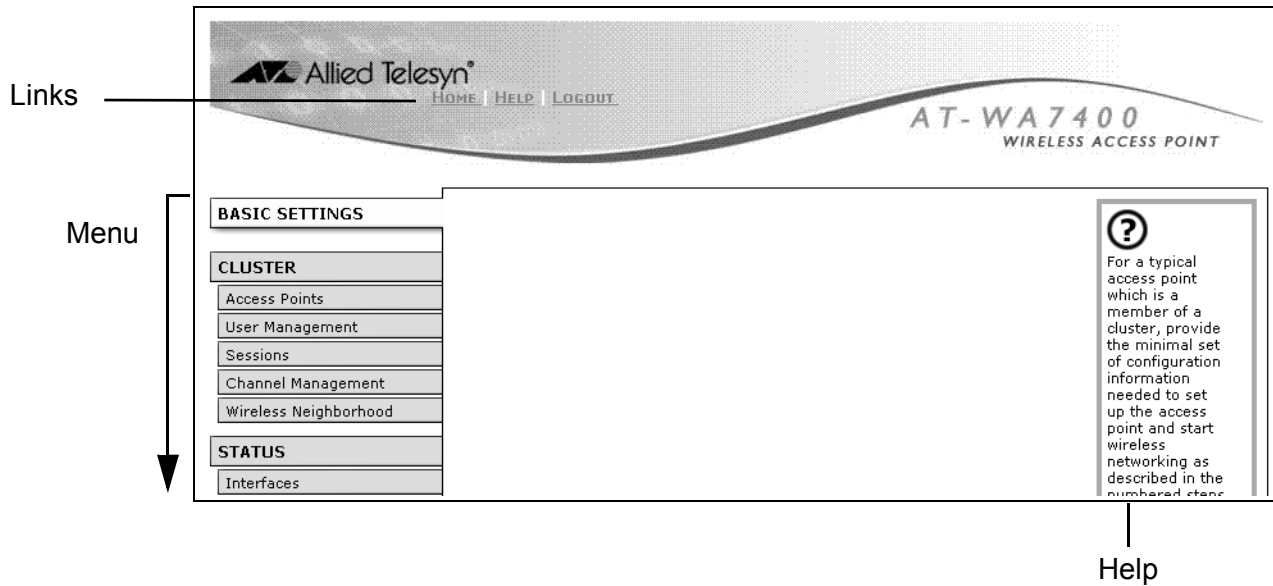


Figure 14. Navigational Aids

- Links** The three links at the top of all the pages allow you to navigate to the following locations:
- Home - The home page for the access point showing the Basic Settings page.
 - Help - The entire help system for the access point.
 - Logout - Opens the logout page so that you can log out from the AT-WA7400 management software. The Logout page is also available on the Advanced menu, and is automatically displayed when your HTTP connection times out.
- Menu** The menu is located along the left side of the page. The Advanced section is always collapsed until you click the plus sign (+) to make a selection from that menu. When you go to one of the other menus, the section is collapsed again.
- Help** The help text along the right side provides help related to the specific management software function for the menu item you chose. Click one of the links within the help to display information about that topic. To see all the help topics, click the Help link at the top of the page.

Configuring the Basic Settings and Starting the Wireless Network

Provide a minimal set of configuration information by defining the basic settings for your wireless network. These settings are all available on the Basic Settings page in the AT-WA7400 management software, and are categorized into steps 1-4 on the web page.

Configuring the Basic Settings

To configure initial settings, perform the following procedure:

1. In the Review Description of this Access Point section, configure the following parameters as necessary:

IP Address

The IP address assigned to this access point. You cannot edit this field because the IP address is already assigned (either through DHCP or statically through the Ethernet (wired)) settings as described in "Enabling or Disabling Guest Access" on page 90.

MAC Address

Shows the MAC address of the access point.

A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface.

The address shown here is the MAC address for the bridge (br0). This is the address by which the access point is known externally to other networks.

Firmware Version

Version information about the firmware currently installed on the access point.

As new versions of the firmware become available, you can upgrade the firmware on your access points to take advantages of new features and enhancements.

For instructions on how to upgrade the firmware, see "Upgrading the Firmware" on page 207.

Location

Specify a location description for this access point.

2. In the Provide Network Settings section, configure the following parameters as necessary:

Current Password

As an immediate first step in securing your wireless network, Allied

Telesyn recommends that you change the administrator password from the default which is “friend.” Enter the current administrator password.

New Password

Enter a new administrator password. The characters you enter are displayed as “*” characters to prevent others from seeing your password as you type.

The Administrator password must be an alphanumeric string of up to 8 characters. Do not use special characters or spaces.

Confirm New Password

Retype the new administrator password to confirm that you typed it as you intended.

Network Name (SSID)

Enter a name for the wireless network as a character string. This name will apply to all access points on this network. As you add more access points, they will share this SSID.

The *Service Set Identifier* (SSID) is an alphanumeric string of up to 32 characters.

If you are connected as a wireless client to the same access point that you are administering, resetting the SSID causes you to lose connectivity to the access point. You will need to reconnect to using the new SSID after you save the new Network Name.

Note

The AT-WA7400 Management Software is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple access points, and more than one administrator is logged on to the AT-WA7400 Management Software’s web pages and making changes to the configuration, all access points in the cluster will stay in synch but there is no guarantee that all configuration changes specified by multiple users will be applied.

3. In the Set Configuration Policy for New Access Points section, configure the following parameter as necessary:

New Access Points

Choose the policy you want to put in effect for adding new access points to the network.

If you choose “are configured automatically,” then when a new access point is added to the network it automatically joins the existing *cluster*. The cluster configuration is copied to the new access point, and no manual configuration is required to deploy it.

If you choose “are ignored,” new access points will not join the cluster; they will be considered *standalone*. You need to configure standalone access points manually using KickStart and the AT-WA7400 management software residing on the standalone access points. (To get to the web page for a standalone access point, use its IP address in a URL as follows: `http://IPAddressOfAccessPoint.`)

Note

If you change the policy so that new access points “are ignored,” then any new access points you add to the network will not join the cluster. Existing clustered access points will not be aware of these standalone access points. Therefore, if you are viewing the AT-WA7400 management software web pages through the IP address of a clustered access point, the new standalone access points will not show up in the list of access points on the Cluster > Access Points page. The only way to see a standalone access point is to browse to it directly by using its IP address in the URL.

If you later change the policy to cluster so that new access points “are configured automatically,” all subsequent new access points will automatically join the cluster. Standalone access points, however, will stay in standalone mode until you explicitly add them to the cluster.

For information on how to add standalone access points to the cluster, see “Adding an Access Point to a Cluster” on page 50

4. In the Settings section, click **Update** to apply these settings and deploy the access point as a wireless network.

A summary of the settings is shown in Figure 15.

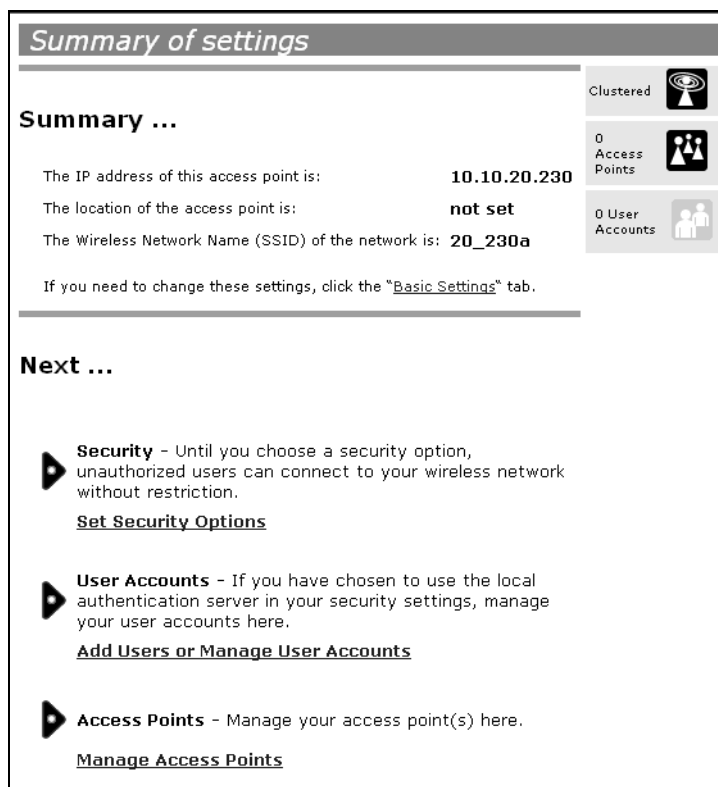


Figure 15. Summary of Settings Page

At initial startup, no security is in place on the access point. An important next step is to configure security, as described in Chapter 10, “Configuring Security” on page 105.

At this point, if you click Basic Settings again, the summary of settings page is replaced by the standard Basic Settings configuration options.

If you chose to *ignore new access points*, then as you add new access points they will run in standalone mode. In standalone mode, an access point does not share the cluster configuration with other access points; it must be configured manually.

You can always update the settings on a standalone access point to have it join the cluster. You can also remove an access point from a cluster thereby switching it to run in standalone mode.

5. Click **Update** to activate the wireless network with these new settings.

Default Configuration

If you follow the steps above and accept all the defaults, the access point will have the default configuration described in Appendix A, “Management Software Default Settings” on page 215.

Next Steps

To make sure the access point is connected to the LAN, bring up some wireless clients and connect the clients to the network. After you have tested the basics of your wireless network, you can enable more security and fine-tune the setup by modifying advanced configuration features on the access point.

Make Sure the Access Point is Connected to the LAN

If you configured the access point and administrator PC by connecting both into a network hub, then your access point is already connected to the LAN. That's it—you're up and running! The next step is to test some wireless clients.

If you configured the access point using a direct wired connection using a crossover cable from your computer to the access point, do the following:

1. Disconnect the crossover cable from the computer and the access point.
2. Connect a regular Ethernet cable from the access point to the LAN.
3. Connect your computer to the LAN either via an Ethernet cable or wireless client card.

Test LAN Connectivity with Wireless Clients

Test the AT-WA7400 Wireless Access Point by trying to detect it and associate it with some wireless client devices.

Secure and Fine-Tune the Access Point Using Advanced Features

After you have the wireless network up and running and have tested against the access point with some wireless clients, you can add in more layers of security, add users, configure a guest interface, and fine-tune performance settings. These features are described in the rest of this guide.

Logging in After the Initial Setup

When you log in again after you complete the initial setup, the default web page is the Interfaces page, as shown in Figure 16.

The screenshot shows the web interface for the AT-WA7400 Wireless Access Point. The header includes the Allied Telesyn logo, navigation links (HOME, HELP, LOGOUT), and the device name 'AT-WA7400 WIRELESS ACCESS POINT'. The main content area is titled 'View settings for network interfaces' and is divided into sections for Wired and Wireless settings. On the left, there is a sidebar menu with categories like BASIC SETTINGS, CLUSTER, STATUS, and ADVANCED. On the right, there is a help box with a question mark icon and instructions on how to configure Ethernet and Wireless settings.

| View settings for network interfaces | |
|--------------------------------------|-------------------------|
| Wired Settings (Configure) | |
| Internal Interface | |
| MAC Address | 00:0C:46:F2:E2:BC |
| VLAN ID | |
| IP Address | 149.35.8.241 |
| Subnet Mask | 255.255.255.0 |
| Guest Interface | |
| MAC Address | 00:00:00:00:00:00 |
| VLAN ID | |
| Subnet | n/a |
| Wireless Settings (Configure) | |
| Radio One | |
| MAC Addresses | 00:0C:46:F2:E2:BC / n/a |
| Mode | IEEE 802.11a |
| Wireless Network Name (SSID) | allied |
| Channel | 52 (5260 MHz) |
| Radio Two | |
| MAC Addresses | 00:0C:46:F2:E2:C0 / n/a |
| Mode | IEEE 802.11g |
| Wireless Network Name (SSID) | allied |
| Channel | 6 (2437 MHz) |

Help Box:
 This page displays current Ethernet (Wired) and Wireless settings on the access point.
 To configure Ethernet Settings, go to the [Ethernet \(Wired\) Settings](#) tab.
 To configure Wireless Settings, go to the [Wireless Settings](#) tab.
[More ...](#)

Figure 16. Default Web Page

Chapter 3

Managing Access Points and Clusters

The AT-WA7400 Management Software shows current basic configuration settings for clustered access points (location, IP address, MAC address, status, and availability) and provides a way of navigating to the full configuration for specific access points if they are cluster members.

Standalone access points or those which are not members of this cluster do not show up in this listing. To configure standalone access points, you must discover (via KickStart) or know the IP address of the access point and by using its IP address in a URL (<http://IPAddressOfAccessPoint>).

Note

The AT-WA7400 Management Software is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple access points, and more than one administrator is logged on to the web pages and making changes to the configuration, all access points in the cluster will stay in synch but there is no guarantee that all configuration changes specified by multiple users will be applied.

This chapter contains the following sections:

- ❑ “Understanding Clustering” on page 44
- ❑ “Understanding and Changing Access Point Settings” on page 48
- ❑ “Navigating to Configuration Information for a Specific Access Point and Managing Standalone Access Points” on page 52
- ❑ “Configuring MAC Address Filtering” on page 53
- ❑ “MAC Filtering of Rogue Access Points” on page 55

Understanding Clustering

A key feature of the AT-WA7400 Management Software is the ability to form a dynamic, configuration-aware group (called a *cluster*) with other AT-WA7400 Wireless Access Points in a network in the same subnet. Access points can participate in a self-organizing cluster which makes it easier for you to deploy, administer, and secure your wireless network. The cluster provides a single point of administration and lets you view the deployment of access points as a single wireless network rather than a series of separate wireless devices.

What is a Cluster?

A cluster is a group of access points which are coordinated as a single group through the AT-WA7400 Management Software. You cannot create multiple clusters on a single wireless network (SSID). Only one cluster per wireless network is supported.

How Many Access Points Can a Cluster Support?

Up to eight access points are supported in a cluster at any one time. If a new access point is added to a network with a cluster that is already at full capacity, the new access point is added in *standalone mode*. Note that when the cluster is full, extra access points are added in standalone mode regardless of the configuration policy in effect for new access points.

For related information, see “Cluster Mode” on page 46 and “Standalone Mode” on page 46.

What Kinds of Access Points Can Cluster Together?

A single AT-WA7400 Wireless Access Point can form a cluster with itself (a “cluster of one”) and with other AT-WA7400 Wireless Access Points of the same model.

What is the Relationship of the Master Access Point to Other Cluster Members?

You use a *master* access point, which you choose from among the cluster members, to change the cluster configuration, share configuration updates, and track new access points joining or leaving the group. If a master access point becomes unavailable, a new cluster member is assigned master responsibilities. This process is fully automated based on a ruleset that takes into account seniority, cluster size, and other factors to determine which access point is best suited to the task at any given time.

There is no need to track or attend to which access point is the master because this status is subject to change at any time depending on the needs of the cluster. This concept is important because you may notice slight differences between configuration information displayed on AT-WA7400 Management Software web pages for a master access point versus other cluster members.

Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?

Most configuration settings that you define using the AT-WA7400 Management Software are propagated to cluster members as a part of the cluster configuration.

Settings Shared in the Cluster Configuration

The cluster configuration includes:

- Network name (SSID)
- Administrator password
- Configuration policy
- User accounts and authentication
- Wireless interface settings
- Guest Welcome screen settings
- Network Time Protocol (NTP) settings
- Radio settings

Only Mode, Channel, Fragmentation Threshold, RTS Threshold and Rate Sets are synchronized across the cluster. Beacon Interval, DTIM Period, Maximum Stations, and Transmit Power do not cluster.

Note

When Channel Planning is enabled, the radio Channel is not synched across the cluster. See "Stopping or Starting Automatic Channel Assignment" on page 73.

- Security settings
- QoS queue parameters
- MAC address filtering

Settings Not Shared by the Cluster

The settings *not* shared among clustered access points are the following, most of which, by nature, must be unique:

- IP addresses
- MAC addresses
- Location descriptions
- Load balancing settings
- WDS bridges
- Ethernet (Wired) settings, including enabling or disabling guest access
- Guest interface configuration

Settings that are not shared must be configured individually on the AT-WA7400 Management Software web pages for each access point. To access the AT-WA7400 Management Software web pages for an access point that is a member of the current cluster, click on its IP Address link on the Cluster > Access Points page of the current access point.

Cluster Mode

When an access point is a cluster member, it is considered to be in cluster mode. You define whether you want new access points to join the cluster or not via the configuration policy you set in the Basic Settings. You can re-set an access point in cluster mode to standalone mode. (See “Removing an Access Point from the Cluster” on page 49.)

Note

When the cluster is full (eight access points is the limit), extra access points are added in standalone mode regardless of the configuration policy in effect for new access points. See “How Many Access Points Can a Cluster Support?” on page 44.

Standalone Mode

The AT-WA7400 Wireless Access Point can be configured in standalone mode. In standalone mode, an access point is not a member of the cluster and does not share the cluster configuration, but rather requires manual configuration that is not shared with other access points. (See “Removing an Access Point from the Cluster” on page 49.)

Standalone access points are not listed on the Cluster > Access Points page in the web pages of access points that are cluster members. You need to know the IP address of a standalone access points in order to configure and manage it directly. (See “Navigating to an Access Point by Using its IP Address in a URL” on page 52.)

The Basic Settings page for a standalone access point indicates only that the current mode is standalone and provides a button for adding the access point to a cluster (group). If you click on any of the Cluster page in the web pages for an access point in standalone mode, you are redirected to the Join Cluster page because Cluster settings do not apply to standalone access points.

Note

When the cluster is full (eight access points is the limit), extra access points are added in *standalone mode* regardless of the configuration policy in effect for new access points. See “How Many Access Points Can a Cluster Support?” on page 44.

You can re-enable cluster mode on a standalone access point. (See “Adding an Access Point to a Cluster” on page 50.)

Cluster Formation

A cluster is formed when the first AT-WA7400 Wireless Access Point is configured. (See “Configuring the Basic Settings and Starting the Wireless Network” on page 37.)

If a cluster configuration policy is in place when a new access point is deployed, it attempts to rendezvous with an existing cluster.

If it is unable to locate a cluster, then it establishes a new cluster on its own.

If it locates a cluster but is rejected because the cluster is full, or the clustering policy is to ignore new access points, then the access point deploys in standalone mode.

Cluster Size and Membership

The upper limit of a cluster is eight access points. The Cluster web administration pages provides a real-time, visual indicator of the number of access points in the current cluster and warn when the cluster has reached access point capacity.

If a cluster is present but is already full, new access points are deployed in standalone mode.

Intra-Cluster Security

To ensure that the security of the cluster as a whole is equivalent to the security of a single access point, communication of certain data between access points in a cluster is done using Secure Sockets Layer with private key encryption.

Both the cluster configuration file and the user database are transmitted among access points using SSL.

Auto-Synch of Cluster Configuration

If you are making changes to the access point configuration that require a relatively large amount of processing (such as adding several new users), you may encounter a synchronization progress bar after clicking Update on any of the AT-WA7400 Management Software web pages. The progress bar indicates that the system is busy performing an auto-synch of the updated configuration to all access points in the cluster. The AT-WA7400 Management Software is not available during the auto-synch.

Note that auto-synchronization always occurs during configuration updates that affect the cluster, but the processing time is usually negligible. The auto-synch progress bar is displayed only for longer-than-usual wait times.

Understanding and Changing Access Point Settings

The Access Points page provides information about all access points in the cluster.

From this page, you can view location descriptions, IP addresses, enable (activate) or disable (deactivate) *clustered* access points, and remove access points from the cluster. You can also modify the location description for an access point.

The IP address links provide a way to navigate to configuration settings and data on an access point.

Standalone access points (those which are not members of the cluster) are not shown on this page.

To view or edit information on access points in a cluster, perform the following procedure:

1. From the main menu, select **Cluster > Access Points**.

The Access Points page is shown in Figure 17. This page shows any access points that are connected to a cluster.

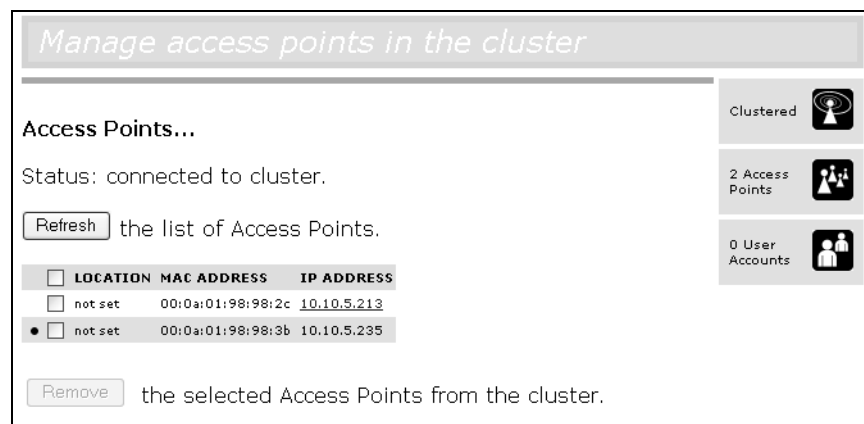


Figure 17. Access Points Page

2. Click **Refresh** to update the access points list.

The Access Points page provides the following information:

Location

Description of where the access point is physically located.

MAC Address

The media access control (MAC) address of the access point.

A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point.

The address shown here is the MAC address for the bridge (br0). This is the address by which the access point is known externally to other networks.

IP Address

The IP address of the access point. Each IP address is a link to the AT-WA7400 Management Software web pages for that access point. You can use the links to navigate to the web pages for a specific access point. This is useful for viewing data on a specific access point to make sure a cluster member is picking up cluster configuration changes, to configure advanced settings on a particular access point, or to switch a standalone access point to cluster mode. To see MAC addresses for guest and internal interfaces on the access point, see the Status > Interfaces page.

Modifying the Location Description

To change the location description for an access point:

1. From the main menu, select **Basic Settings**.

The Basic Settings page is shown in Figure 13 on page 35.

2. Update the Location description in section 1 under "Review Description of this Access Point."
3. Click **Update** to apply the changes.

Removing an Access Point from the Cluster

To remove an access point from the cluster, do the following.

1. From the main menu, select **Cluster > Access Point**.

The Access Points page is shown in Figure 17 on page 48.

2. Click the checkbox next to the access point so that the box is checked.
3. Click **Remove**.

The change is under Status for that access point; the access point will now show as standalone (instead of cluster).

Note

In some situations it is possible for the cluster to become out of sync. If after removing an access point from the cluster, the access point list still reflects the deleted access point or shows an incomplete display; refer to the information on cluster recovery in “Cluster Recovery” on page 261.

Adding an Access Point to a Cluster

To add an access point that is currently in standalone mode back into a cluster, do the following.

1. Go to the AT-WA7400 Management Software web pages for the standalone access point. (See “Navigating to an Access Point by Using its IP Address in a URL” on page 52.)

The web pages for the standalone access point are displayed.

2. From the main menu, select **Cluster > Access Points**.
3. Click **Join Cluster**.

The Summary of Settings page is redisplayed, as shown in Figure 18, with the settings of the access point that is now part of the cluster.

The screenshot shows a web interface titled "Summary of settings". On the right side, there are three status indicators: "Clustered" with a wireless antenna icon, "0 Access Points" with a group of people icon, and "0 User Accounts" with a single person icon. The main content area is titled "Summary ..." and lists the following information:

- The IP address of this access point is: **10.10.20.230**
- The location of the access point is: **not set**
- The Wireless Network Name (SSID) of the network is: **20_230a**

Below this information, it says: "If you need to change these settings, click the ['Basic Settings'](#) tab."

The "Next ..." section contains three items:

- Security** - Until you choose a security option, unauthorized users can connect to your wireless network without restriction. [Set Security Options](#)
- User Accounts** - If you have chosen to use the local authentication server in your security settings, manage your user accounts here. [Add Users or Manage User Accounts](#)
- Access Points** - Manage your access point(s) here. [Manage Access Points](#)

Figure 18. Settings of Access Point that Joined the Cluster

The access point is now a cluster member. Its Status (Mode) on the Cluster > Access Points page now indicates "Clustered."

Note

In some situations it is possible for the cluster to become out of sync. If, after removing an access point from the cluster, the access point list still reflects the deleted access point or shows an incomplete display; refer to the information on cluster recovery in "Cluster Recovery" on page 261.

Navigating to Configuration Information for a Specific Access Point and Managing Standalone Access Points

In general, the AT-WA7400 Management Software is designed for central management of *clustered* access points. For access points in a cluster, all access points in the cluster reflect the same configuration. In this case, it does not matter which access point you actually connect to for administration.

There may be situations, however, when you want to view or manage information on a particular access point. For example, you might want to check status information such as client associations or events for an access point. Or you might want to configure and manage features on an access point that is running in *standalone* mode. In these cases, you can navigate to the AT-WA7400 Management Software web interface for individual access points by clicking the IP address links on the Access Points page.

All clustered access points are shown on the Cluster > Access Points page. To navigate to clustered access points, you can simply click on the IP address for a specific cluster member shown in the list.

Navigating to an Access Point by Using its IP Address in a URL

You can also link to the web pages of a specific access point by entering the IP address for that access point as a URL directly into a web browser address bar in the following form:

```
http://IPAddressOfAccessPoint
```

where *IPAddressOfAccessPoint* is the address of the particular access point you want to monitor or configure.

This is the only way to navigate to configuration information for a standalone access point.

If you do not know the IP address of a standalone access point, use KickStart to find all access points on the network and you should be able to derive which ones are standalone by comparing KickStart findings with access points listed on the Cluster > Access Points page. The access points that KickStart finds that are not shown on the this page are probably standalone access points. (For more information on using KickStart, see “Running KickStart to Find Access Points on the Network” on page 26.)

Configuring MAC Address Filtering

A media access control (MAC) address is a hardware address that uniquely identifies each node of a network. All IEEE 802 network devices share a common 48-bit MAC address format, usually displayed as a string of 12 hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

Each wireless network interface card (NIC) used by a wireless client has a unique MAC address.

You can control client access to your wireless network by switching on MAC filtering and specifying a list of approved MAC addresses. When MAC filtering is on, only clients with a listed MAC address can access the network.

Based on how you set the MAC filter, you can *allow* only client stations with a listed MAC address or *prevent* access to the stations listed. For the guest interface, MAC Filtering settings apply to both BSSes. On a two-radio access point, MAC Filtering settings apply to both radios.

To set the DNS name, perform the following procedure:

1. From the main menu, select **Advanced > MAC Filtering**.

The MAC Filtering page is shown in Figure 19.

Configure MAC Filtering of client stations

Filter Allow only stations in list
 Allow any station unless in list

Stations List

FE:DA:BD:09:87:65

Remove

: : : : : Add

Update

Figure 19. MAC Filtering Page

2. Configure the following settings:

Filter

Click one of the following radio buttons:

- Allow only stations in the list
- Allow any station unless in list

Stations List

To add a MAC Address to Stations List, enter its 48-bit MAC address into the lower text boxes, then click **Add**.

The MAC Address is added to the Stations List.

To remove a MAC Address from the Stations List, select its 48-bit MAC address, then click **Remove**.

The stations in the list will either be allowed or prevented from accessing the access point based on how you set the Filter.

3. Click **Update** to save your settings.

MAC Filtering of Rogue Access Points

When an access point is not listed in the access points list, the MAC filtering of rogue access points feature sends an SNMP trap to alert you to the unregistered (rogue) access point.

To enable MAC filtering of rogue access points, perform the following procedure:

1. From the main menu, select **Advanced > Pre-Config Rogue AP**.

The Configure MAC Filtering of Rogue Access Points page is shown in Figure 20.

Configure Rogue MAC Filtering of Access Point

Access Points List

Remove

[] : [] : [] : [] : [] : []

Add

Update

Figure 20. Configure Rogue MAC Filtering of Access Point Page

2. To add an access point to the list:
 - a. Type its MAC address in the fields above the Add button.
 - b. Click **Add**.
 - c. Click **Update**.
3. To remove an access point from the list:
 - a. Select the MAC address of the access point in the Access Points List.

- b. Click **Add**.
- c. Click **Update**.

Chapter 4

Managing User Accounts

The AT-WA7400 Management Software includes user management capabilities for controlling client access to access points.

User management and authentication must always be used in conjunction with the following two security modes, which require use of a RADIUS server for user authentication and management.

- IEEE 802.1x mode
- WPA with RADIUS mode

You have the option of using either the internal RADIUS server embedded in the AT-WA7400 Wireless Access Point or an external RADIUS server that you provide. If you use the embedded RADIUS server, use the management software on the access point to set up and manage user accounts. If you are using an external RADIUS server, you will need to set up and manage user accounts on the Administrative interface for that server.

On the User Management page, you can create, edit, remove, and view client user accounts. Each user account consists of a user name and password. The set of users specified here represent approved *clients* that can log in and use one or more access points to access local and possibly external networks via your wireless network.

Note

Users specified here are clients of the access point(s) that use the access points as a connectivity hub, not administrators of the wireless network. Only those with the administrator username and password and knowledge of the administration URL can log in as an administrator and view or modify configuration settings.

This chapter contains the following sections:

- “Adding a User” on page 58
- “Editing a User Account” on page 60
- “Backing Up and Restoring a User Database” on page 62

Adding a User

To add a new user, perform the following procedure:

1. From the main menu, select **Cluster > User Management**.

The User Management page is shown in Figure 21.

The screenshot shows a web interface titled "Manage user accounts". It features a sidebar on the right with icons for "Clustered", "2 Access Points", and "3 User Accounts". The main content area is divided into two sections: "User Accounts..." and "Add a user...".

User Accounts...

To edit a user account, click a user name.

To enable or disable a user, click the "enable" or "disable" button. Likewise, to remove a user, click the "remove" button. Ensure that you have selected at least one user prior to any of these actions.

Note: These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

| <input type="checkbox"/> Edit | User Name | Real Name | Status |
|---------------------------------|-----------|----------------------|---------|
| <input type="checkbox"/> [Edit] | samantha | Elizabeth Montgomery | enabled |
| <input type="checkbox"/> [Edit] | endora | Agnes Moorhead | enabled |
| <input type="checkbox"/> [Edit] | darren | Dick York | enabled |

Selected users:

[\[backup or restore the user database\]](#)

Add a user...

To add a user, fill in the fields below and click "add account".

User Name

Real Name

Password

Password (again for safety)

Figure 21. User Management Page

User accounts are shown at the top of the page under User Accounts. The user name, real name and status (enabled or disabled) are shown.

2. In the Add a User section, provide the following information:

User Name

User names are alphanumeric strings of up to 237 characters. Do not use special characters or spaces.

Real Name

For information purposes, provide the user's full name, up to 256 characters.

Password

Specify a password for this user. Passwords are alphanumeric strings of up to 256 characters. Do not use special characters or spaces. You must retype the password.

3. Click **Add Account** to add the account.

The new user is then displayed in the User Accounts list. The user account is enabled by default when you first create it.

Note

A limit of 100 user accounts per access point is imposed by the web user interface. Network usage may impose a more practical limit, depending upon the demand from each user.

Editing a User Account

After you create a user account, it is displayed in the User Accounts section at the top of the Cluster > User Management page.

To edit an existing user account, perform the following procedure:

1. From the main menu, select **Cluster > User Management**.

The User Management page is shown in Figure 21 on page 58.

2. In the User Accounts section, click the checkbox next to the user name so that the box is checked, as shown in Figure 22.

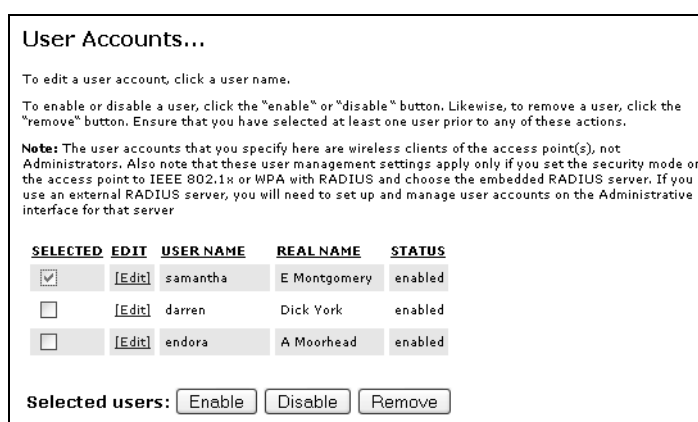


Figure 22. User Accounts Section

A user account must be enabled for the user to log on as a client and use the access point.

You can enable or disable any user account. With this feature, you can maintain a set of user accounts and authorize or prevent users from accessing the network without having to remove or re-create accounts. This can come in handy in situations where users have an occasional need to access the network. For example, contractors who do work for your company on an intermittent but regular basis might need network access for 3 months at a time, then be off for 3 months, and back on for another assignment. You can enable and disable these user accounts as needed, and control access as appropriate.

Enabling a User Account

To enable a user account, perform the following procedure:

1. From the main menu, select **Cluster > User Management**.

The User Management page is shown in Figure 21 on page 58.

2. In the User Accounts section, click the checkbox next to the user name you want to enable.
3. Click **Enable**.

A user with an account that is enabled can log on to the wireless access points in your network as a client.

Disabling a User Account

To disable a user account, perform the following procedure:

1. From the main menu, select **Cluster > User Management**.

The User Management page is shown in Figure 21 on page 58.

2. In the User Accounts section, click the checkbox next to the user name you want to disable.
3. Click **Disable**.

A user with an account that is *disabled* cannot log on to the wireless access points in your network as a client. However, the user remains in the database and can be enabled later as needed.

Removing a User Account

To remove a user account, perform the following procedure:

1. From the main menu, select **Cluster > User Management**.

The User Management page is shown in Figure 21 on page 58.

2. In the User Accounts section, click the checkbox next to the user name you want to remove.
3. Click **Remove**.

If you think you might want to add this user back in at a later date, consider *disabling* the user rather than removing the account altogether.

Backing Up and Restoring a User Database

You can save a copy of the current set of user accounts to a backup configuration file. You can use the backup file at a later date to restore the user accounts on the access point to the previously saved configuration.

Backing Up the User Database

To create a backup copy of the user accounts for this access point, perform the following procedure:

1. From the main menu, select **Cluster > User Management**.

The User Management page is shown in Figure 21 on page 58.

2. In the User Accounts section, click the **backup or restore the user database** link.

The Backup or restore the user database for this access point page is displayed, as shown in Figure 23.

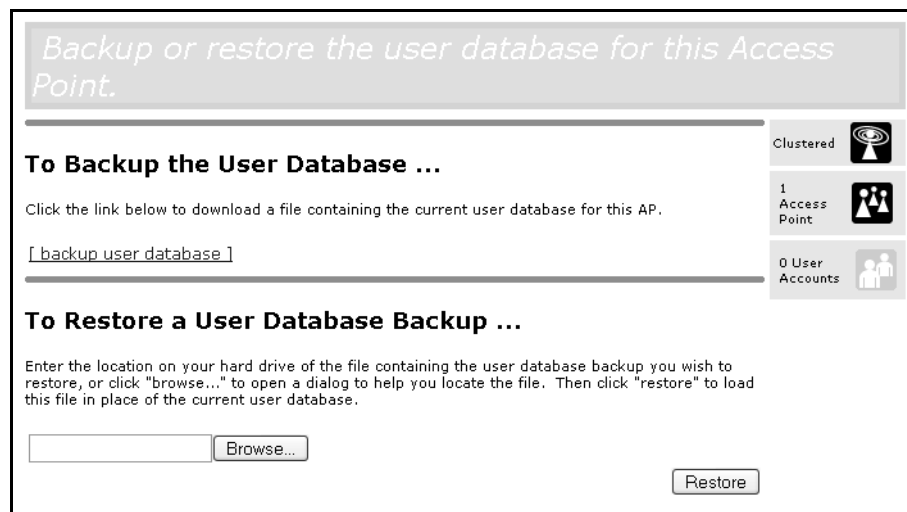


Figure 23. Backup or Restore User Database Page

3. Choose the **Save** option in this first dialog box.

This opens a file browser.

4. Use the file browser to navigate to the directory where you want to save the file, and click **OK** to save the file.

You can keep the default file name (`wirelessUsers.ubk`) or rename the backup file, but be sure to save the file with a `.ubk` extension.

Restoring a User Database from a Backup File

To restore a user database from a backup file, perform the following procedure:

1. From the main menu, select **Cluster > User Management**.

The User Management page is shown in Figure 21 on page 58.

2. In the User Accounts section, click the **backup or restore the user database** link.

The Backup or restore the user database for this access point page is displayed, as shown in Figure 23 on page 62.

3. Select the backup configuration file you want to use, either by typing the full path and file name in the Restore field or by clicking **Browse** and selecting the file.

(Only those files that were created with the User Database Backup function and saved as .ubk backup configuration files are valid to use with Restore; for example, wirelessUsers.ubk.)

4. Click **Restore**.

When the backup restore process is complete, a message is shown to indicate that the user database has been successfully restored. (This process is not time-consuming; the restore should complete almost immediately.)

From the main menu, select **Cluster > User Management** to see the restored user accounts.

Chapter 5

Session Monitoring

The AT-WA7400 Management Software provides real-time session monitoring information including which clients are associated with a particular access point, data rates, transmit/receive statistics, signal strength, and idle time.

A session in this context is the period of time in which a user on a client device (station) with a unique MAC address maintains a connection with the wireless network. The session begins when the client logs on to the network, and the session ends when the client either logs off intentionally or loses the connection for some other reason.

Note

A session is not the same as an association, which describes a client connection to a particular access point. A client network connection can shift from one clustered access point to another within the context of the same session. A client station can roam between access points and maintain the session.

Note

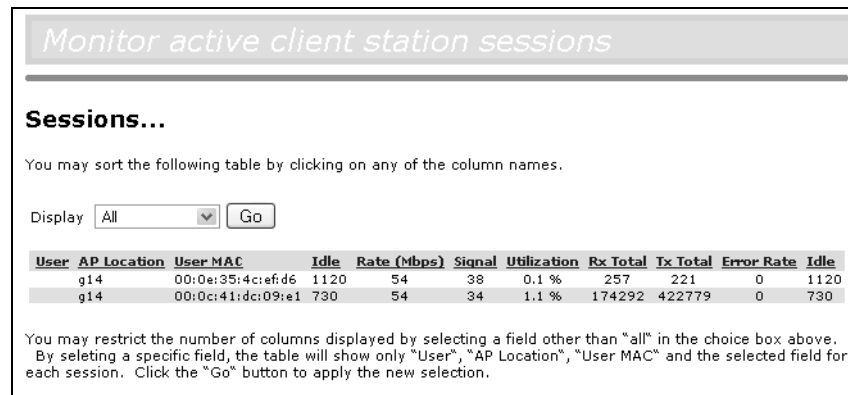
For information about monitoring associations and link integrity monitoring, see “Viewing the Associated Wireless Clients” on page 192.

Viewing Sessions Information

To view session monitoring information, perform the following procedure:

1. From the main menu, select **Cluster > Sessions**.

The Sessions page is shown in Figure 24



The screenshot shows a web interface for monitoring active client station sessions. At the top, there is a header "Monitor active client station sessions". Below this, the section is titled "Sessions...". A message states: "You may sort the following table by clicking on any of the column names." Below the message is a "Display" dropdown menu set to "All" and a "Go" button. The table below has the following columns: User, AP Location, User MAC, Idle, Rate (Mbps), Signal, Utilization, Rx Total, Tx Total, Error Rate, and Idle. Two rows of data are shown:

| User | AP Location | User MAC | Idle | Rate (Mbps) | Signal | Utilization | Rx Total | Tx Total | Error Rate | Idle |
|------|-------------|-------------------|------|-------------|--------|-------------|----------|----------|------------|------|
| g14 | | 00:0e:35:4c:ef:d6 | 1120 | 54 | 38 | 0.1 % | 257 | 221 | 0 | 1120 |
| g14 | | 00:0c:41:dc:09:e1 | 730 | 54 | 34 | 1.1 % | 174292 | 422779 | 0 | 730 |

Below the table, a note states: "You may restrict the number of columns displayed by selecting a field other than 'all' in the choice box above. By selecting a specific field, the table will show only 'User', 'AP Location', 'User MAC' and the selected field for each session. Click the 'Go' button to apply the new selection."

Figure 24. Sessions Page

The Sessions page displays the following information about client stations associated with access points in the cluster:

User Name

Indicates the client user name of IEEE 802.1x clients.

Note

This field is relevant only for clients that are connected to access points using IEEE 802.1x security mode *and* local authentication server. (For more information about this mode, see "IEEE 802.1x" on page 121.) No user name is shown for clients of access points using IEEE 802.1x with RADIUS server or other security modes.

AP Location

Indicates the location of the access point.

This is derived from the location description specified on the Basic Settings page.

User MAC Address

Indicates the MAC address of the user's client device (station).

A MAC address is a hardware address that uniquely identifies each node of a network.

Idle Time

Indicates the amount of time this station has remained inactive.

A station is considered to be idle when it is not receiving or transmitting data.

Data Rate

The speed at which this access point is transferring data to the specified client.

The data transmission rate is measured in *megabits per second* (Mbps).

This value should fall within the range of the advertised rate set for the IEEE 802.1x mode in use on the access point. For example, 6 to 54Mbps for 802.11a,

Signal

Indicates the strength of the radio frequency (RF) signal the client receives from the access point.

The measure used for this is an IEEE 802.1x value known as Received Signal Strength Indication (RSSI), and will be a value between 0 and 100.

RSSI is determined by a an IEEE 802.1x mechanism implemented on the network interface card (NIC) of the client station.

Utilization

Utilization rate for this station.

For example, if the station is active (transmitting and receiving data) 90% of the time and inactive 10% of the time, its utilization rate is 90%.

Receive Total

Indicates number of total packets received by the client during the current session.

Transmit Total

Indicates number of total packets transmitted to the client during this session.

Error Rate

Indicates the percentage of time frames are dropped during transmission on this access point.

Viewing Specific Session Information

To view only specific information about a session, perform the following procedure:

1. On the Sessions page, from the Display list, choose the field you want to display and click **Go**.

The page is refreshed and displays the User, AP Location, and User MAC information in addition to the field you selected.

Sorting Session Information

To sort the information in the session list, perform the following procedure:

1. On the Sessions page, click the column label by which you want to sort the sessions.

The display is refreshed to show the sessions in the order you chose.

Chapter 6

Channel Management

This chapter contains the following sections:

- ❑ “Understanding Channel Management” on page 70
- ❑ “Displaying the Channel Management Settings” on page 72
- ❑ “Configuring the Channel Management Settings” on page 73

Understanding Channel Management

When channel management is enabled, the AT-WA7400 Management Software automatically assigns radio channels used by clustered access points to reduce mutual interference (or interference with other access points outside of its cluster). This maximizes WiFi bandwidth and helps maintain the efficiency of communication over your wireless network.

Note

You must start channel management to get automatic channel assignments; it is disabled by default on a new access point. See “Stopping or Starting Automatic Channel Assignment” on page 73.

How it Works in a Nutshell

At a specified interval (the default is one hour) or on demand (click Update), the Channel Manager maps access points to channel use and measures interference levels in the cluster. If significant channel interference is detected, the Channel Manager automatically reassigns some or all of the access points to new channels per an efficiency algorithm (or automated channel plan).

Overlapping Channels

The radio frequency (RF) broadcast channel defines the portion of the radio spectrum that the radio on the access point uses for transmitting and receiving. The range of available channels for an access point is determined by the IEEE 802.11 mode (also referred to as band) of the access point.

IEEE 802.11b/802.11g modes (802.11 b/g) support use of channels 1 through 11 inclusive, while IEEE 802.11a mode supports a larger set of non-consecutive channels (36,40,44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165).

Interference can occur when multiple access points within range of each other are broadcasting on the same or overlapping channels. The impact of this interference on network performance can intensify during busy times when a large amount of data and media traffic competing for bandwidth.

The Channel Manager detects which bands (b/g or a) clustered access points are on, and uses a predetermined collection of channels that will not mutually interfere. For the “b/g” radio band, the classical set of non-interfering channels is 1, 6, 11. Channels 1, 4, 8, 11 produce minimal overlap. A similar set of non-interfering channels is used for the “a” radio band, which includes all channels for that mode since they are not overlapping.

**Example: A
Network Before
and After
Channel
Management**

Without automated channel management, channel assignments to clustered access points might be made on *consecutive channels*, which would overlap and cause interference. For example, access point1 could be assigned to channel 6, access point2 to channel 6, and access point3 to channel 5 as shown in Figure 25.

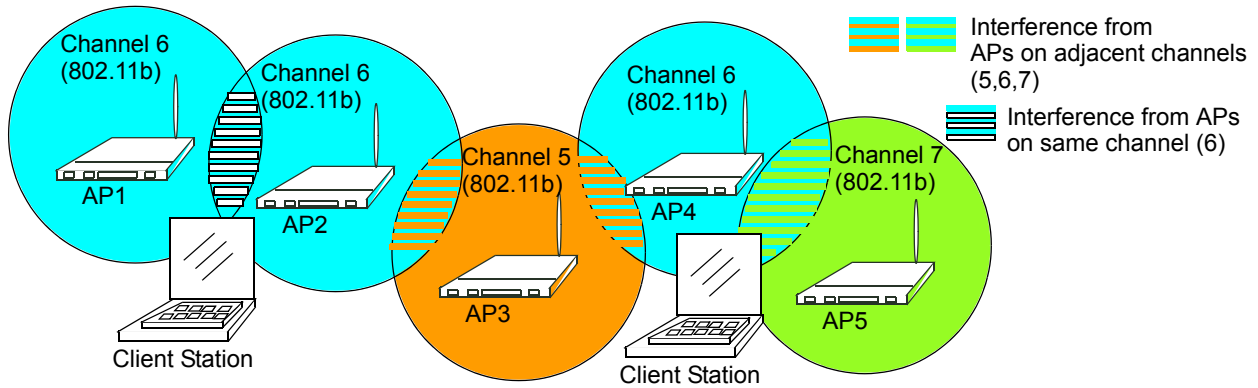


Figure 25. Without Automatic Channel Management: Access Points Can Broadcast on Overlapping Channels

With automated channel management, access points in the cluster are automatically reassigned to noninterfering channels as shown in Figure 26.

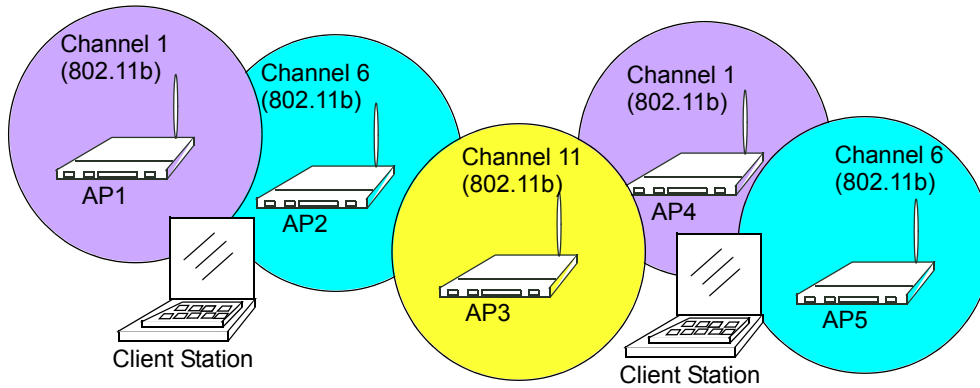


Figure 26. With Channel Management Enabled: Access Points are Re-Assigned to Non-Interfering Channels

Displaying the Channel Management Settings

To view channel management information, perform the following procedure:

1. From the main menu, select **Cluster > Channel Management**.

The Channel Management page is displayed, as shown in Figure 27.

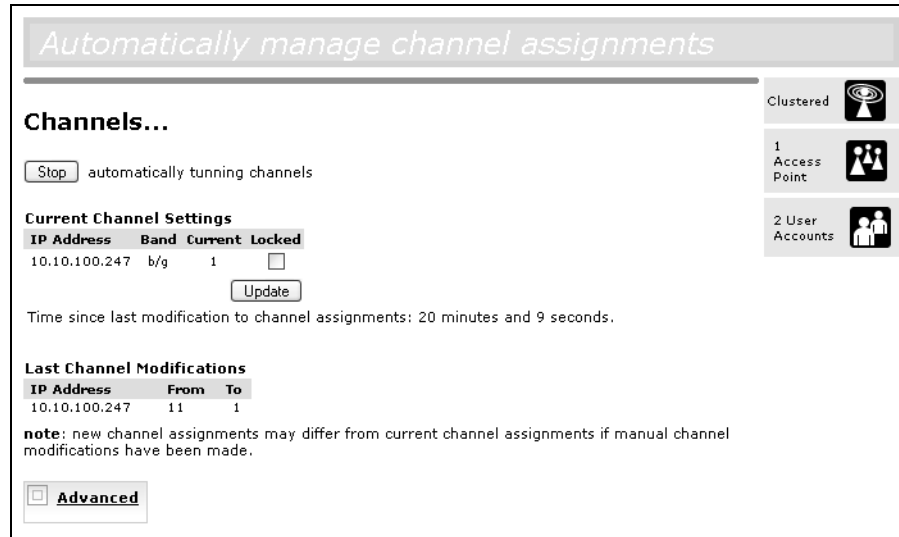


Figure 27. Channel Management Page

The Channel Management page shows previous, current, and planned channel assignments for clustered access points. By default, automatic channel assignment is disabled. You can start channel management to optimize channel usage across the cluster on a scheduled interval.

From this page, you can view channel assignments for all access points in the cluster, stop/start automatic channel management, and manually update the current channel map (access points to channels). When you do a manual update, the Channel Manager assesses channel usage and, if necessary, reassigns access points to new channels to reduce interference based on the current Advanced settings.

Using the Advanced settings you can modify the interference reduction potential that triggers channel reassignment, change the schedule for automatic updates, and reconfigure the channel set used for assignments.

Configuring the Channel Management Settings

This section contains the following procedures:

- “Stopping or Starting Automatic Channel Assignment,” next
- “Viewing Current Channel Assignments and Setting Locks” on page 73
- “Updating the Current Channel Settings Manually” on page 74
- “Viewing the Last Proposed Set of Changes” on page 74
- “Configuring Advanced Settings (Customizing and Scheduling Channel Plans)” on page 75

Stopping or Starting Automatic Channel Assignment

By default, automatic channel assignment is disabled (off).

To start or stop channel management, perform the following procedure:

1. From the main menu, select **Cluster > Channel Management**.

The Channels page is displayed, as shown in Figure 27 on page 72.

2. Click **Start** to resume automatic channel assignment.

When automatic channel assignment is enabled, the Channel Manager periodically maps radio channels used by clustered access points and, if necessary, reassigns channels on clustered access points to reduce interference (with cluster members or other access points outside the cluster).

Note

Channel Management overrides the default cluster behavior, which is to synchronize radio channels of all access points across a cluster. When Channel Management is enabled, the radio Channel is not synchronized across the cluster to other access points. See the note under Radio Settings in “Settings Shared in the Cluster Configuration” on page 45.

3. Click **Stop** to stop automatic channel assignment. (No channel usage maps or channel reassignments are made. Only manual updates affect the channel assignment.)

Viewing Current Channel Assignments and Setting Locks

The Current Channel Assignments section displays a list of all access points in the cluster by IP address. The display provides the following information:

IP Address

Specifies the IP address for the access point.

Band

Indicates the band (b/g or a) on which the access point is broadcasting.

Current

Indicates the radio channel on which this access point is currently broadcasting.

Locked

Click Locked if you want to this access point to remain on the current channel.

When the Locked checkbox is checked (enabled) for an access point, automated channel management plans will not re-assign the access point to a different channel as a part of the optimization strategy. Instead, access points with locked channels are factored in as requirements for the plan.

If you click Update, you will see that locked access points show the same channel for Current Channel and Proposed Channel. Locked access points keep their current channels.

Updating the Current Channel Settings Manually

To run a manual channel management update at any time, click **Update** in the Advanced section.

Viewing the Last Proposed Set of Changes

The Last Proposed Set of Channel Assignments section shows the last channel plan. The plan lists all access points in the cluster by IP Address, and shows the current and proposed channels for each access point. Locked channels are not reassigned and the optimization of channel distribution among access points takes into account the fact that locked access points must remain on their current channels. Access points that are not Locked may be assigned to different channels than they were previously using, depending on the results of the plan. The following information is displayed:

IP Address

Specifies the IP address for the access point.

Current

Indicates the radio channel on which this access point is currently broadcasting.

Proposed

Indicates the radio channel to which this access point would be re-assigned if the Channel Plan is executed.

Configuring Advanced Settings (Customizing and Scheduling Channel Plans)

If you use channel management as provided (without updating the Advanced settings), channels are automatically fine-tuned once every hour if interference can be reduced by 25 percent or more. Channels are reassigned even if the network is busy. The appropriate channel sets are used (b/g for access points using IEEE 802.11b/g and a for access points using IEEE 802.11a).

These defaults are designed to satisfy most scenarios where you would need to implement channel management.

You can use the Advanced settings to modify the interference reduction potential that triggers channel reassignment, change the schedule for automatic updates, and reconfigure the channel set used for assignments.

To configure the advanced settings, perform the following procedure:

1. From the main menu, select **Cluster > Channel Management**.

The Channel Management page is displayed, as shown in Figure 27 on page 72.

2. Click **Advanced** to show the advanced settings.

The advanced settings are shown at the bottom of

Automatically manage channel assignments

Channels...

automatically re-assigning channels

Current Channel Assignments

| IP Address | Band | Current | Locked |
|---------------|------|---------|--------------------------|
| 10.10.103.214 | b/g | 1 | <input type="checkbox"/> |

Time since last modification to channel assignments: 34 minutes and 52 seconds .

There is a set of channel combinations that would produce less interference but not by enough. You may redefine this threshold in the [advanced](#) settings panel.

Last proposed set of channel assignments.

| IP Address | Current | Proposed |
|---------------|---------|----------|
| 10.10.103.214 | 1 | 1 |

Advanced

Change channels if interference is reduced by at least %

Determine if there is better set of channel settings every Minutes

Use these channels when applying channel assignments:

Apply channel modifications even when network is busy.

3. Configure the following settings as necessary:

Change channels if interference is reduced by at least

Specify the minimum percentage of interference reduction a proposed plan must achieve in order to be applied. The default is 25 percent.

Choose percentages ranging from 25 percent to 75 percent from the list.

This setting lets you set a gating factor for channel reassignment so that the network is not continually disrupted for minimal gains in efficiency.

For example, if channel interference must be reduced by 75 percent and the proposed channel assignments will only reduce interference by 30 percent, then channels are not reassigned. However; if you re-set the minimal channel interference benefit to 25 percent and click Update, the proposed channel plan will be implemented and channels reassigned as needed.

Determine if there is better set of channels every

Select the schedule from the list. The range of intervals is from 1 Minute to 6 Months, and the default is 1 Hour (channel usage reassessed and the resulting channel plan applied every hour).

Use these channels when applying channel assignments

Choose a set of noninterfering channels on a particular band (b/g or a). The choices are:

- b/g channels 1-6-11
- b/g channels 1-4-8-11
- A

IEEE 802.11b/802.11g modes (802.11 b/g) support use of channels 1 through 11. For the b/g radio band, the classical set of non-interfering channels is 1, 6, 11. Channels 1, 4, 8, 11 produce minimal overlap.

IEEE 802.11a mode supports a larger set of non-consecutive channels (36,40,44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165). All "a" band channels are non-interfering.

Apply channel modifications even when the network is busy

Click to enable or disable this setting.

A checkmark indicates it is enabled and channel modifications are applied even when the network is busy.

If this is not checked, channel modifications are not applied on a busy network.

This setting (along with the interference reduction setting) is designed to help weigh the cost/benefit impact on network performance of re-assigning channels against the inherent disruption it can cause to clients during a busy time.

4. Click **Update** to apply these settings.

Advanced settings take effect when they are applied, and influence how automatic channel management is performed. (The new interference reduction minimum, scheduled tuning interval, channel set, and network busy settings are taken into account for automated and manual updates.)

Chapter 7

Wireless Neighborhoods

The wireless neighborhood view shows those access points within range of any access point in the cluster. This page provides a detailed view of neighboring access points including identifying information (SSIDs and MAC addresses) for each, cluster status (which are members and non-members), and statistical information such as the channel each access point is broadcasting on, signal strength, and so forth.

This chapter contains the following sections:

- “Understanding Wireless Neighborhood Information” on page 80
- “Displaying the Wireless Neighborhood Information” on page 81
- “Viewing Details of a Cluster Member” on page 84

Understanding Wireless Neighborhood Information

The wireless neighborhood shows all access points within range of every member of the cluster, shows which access points are within range of which cluster members, and distinguishes between cluster members and nonmembers.

For each neighbor access point, the Wireless Neighborhood view shows identifying information (SSID or Network Name, IP address, MAC address) along with radio statistics (signal strength, channel, beacon interval). You can click on an access point to get additional statistics about the access points in radio range of the currently selected access point.

The Wireless Neighborhood view can help you:

- ❑ Detect and locate unexpected (or *rogue*) access points in a wireless domain so that you can take action to limit associated risks
- ❑ Verify coverage expectations. By assessing which access points are visible at what signal strength from other access points, you can verify that the deployment meets your planning goals.
- ❑ Detect faults. Unexpected changes in the coverage pattern are evident at a glance in the color coded table.

Displaying the Wireless Neighborhood Information

To view the Wireless Neighborhood page, perform the following procedure:

1. From the main menu, select **Cluster > Wireless Neighborhood**.

The Wireless Neighborhood page is shown in Figure 28.

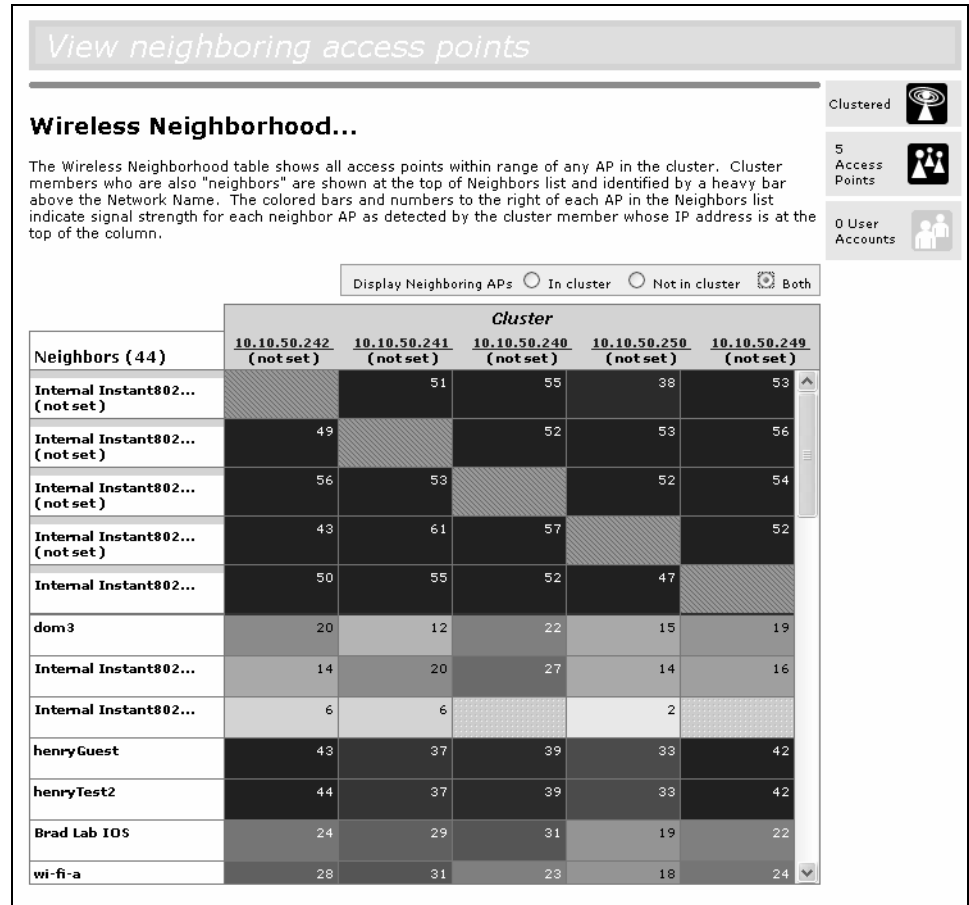


Figure 28. Wireless Neighborhood Page

The Wireless Neighborhood page displays the following information:

Display neighboring APs

Click one of the following radio buttons to change the view:

In cluster - Shows only neighbor access points that are members of the cluster

Not in cluster - Shows only neighbor access points that are not cluster members

Both - Shows all neighbor access points (cluster members and nonmembers)

Cluster

The Cluster list at the top of the table shows IP addresses for all access points in the cluster. (This is the same list of cluster members shown in the Cluster > Access Points page described in “Understanding and Changing Access Point Settings” on page 48.)

If there is only one access point in the cluster, only a single IP address column is displayed here, indicating that the access point is clustered with itself.

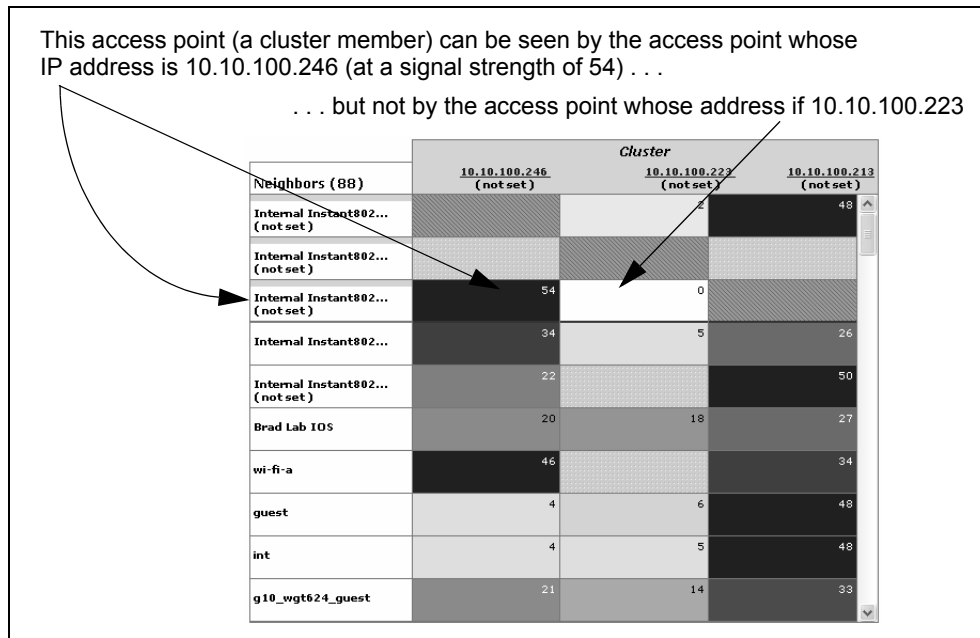
You can click on an IP address to view more details on a particular access point as shown in Figure 28 on page 81.

Neighbors

Access points which are neighbors of one or more of the clustered access points are listed in the left column by SSID (Network Name).

An access point which is detected as a neighbor of a cluster member can also be a cluster member itself. Neighbors who are also cluster members are always shown at the top of the list with a heavy bar above and include a location indicator.

The colored bars to the right of each access point in the Neighbors list shows the signal strength for each of the neighbor access points as detected by the cluster member whose IP address is shown at the top of the column



- ❑ **Dark Blue Bar** - A dark blue bar and a high signal strength number (for example 50) indicates good signal strength detected from the

Neighbor seen by the access point whose IP address is listed above that column.

- ❑ **Lighter Blue Bar** - A lighter blue bar and a lower signal strength number (for example 20 or lower) indicates medium or weak signal strength from the Neighbor seen by the access point whose IP address is listed above that column
- ❑ **White Bar** - A white bar and the number 0 indicates that a neighboring access point that was detected by one of the cluster members cannot be detected by the access point whose IP address is listed above that column.
- ❑ **Light Gray Bar** - A light gray bar and no signal strength number indicates a Neighbor that is detected by other cluster members but not by the access point whose IP address is listed above that column.
- ❑ **Dark Gray Bar** - A dark gray bar and no signal strength number indicates this *is* the access point whose IP address is listed above that column (since it is not applicable to show how well the access point can detect itself).

Viewing Details of a Cluster Member

To view details on a cluster member access point, perform the following procedure:

1. From the main menu, select **Cluster > Wireless Neighborhood**.

The Wireless Neighborhood page is displayed, as shown in Figure 28 on page 81.

2. Click the IP address of a cluster member at the top of the page.

The Neighbor Details section is displayed at the bottom of the page, as shown in Figure 29.

| Neighbor Details | | | | | | |
|--------------------------|-------------------|---------|------|--------|-----------------|------------|
| 10.10.100.246 - Sessions | | | | | | |
| SSID | MAC Address | Channel | Rate | Signal | Beacon Interval | Beacon Age |
| Internal Instant802... | 02:0c:41:00:02:e0 | 1 | 10 | 34 | 1098063136 | 100 |
| Internal Instant802... | 00:0c:41:16:a1:e4 | 6 | 10 | 22 | 1098063132 | 100 |
| wi-fi-a | 00:e0:b8:76:28:44 | 7 | 10 | 46 | 1098057207 | 100 |
| Brad Lab IDS | 00:0e:38:62:62:20 | 8 | 10 | 20 | 1098061627 | 2000 |
| guest | 00:e0:b8:76:25:f3 | 6 | 10 | 4 | 1098063103 | 100 |
| int | 00:e0:b8:76:25:f2 | 6 | 10 | 4 | 1098063112 | 100 |
| g10_wgt624_guest | 00:0e:81:01:01:97 | 5 | 10 | 21 | 1098062886 | 100 |
| g10_wgt624 | 00:0e:81:01:01:96 | 5 | 10 | 43 | 1098060060 | 100 |
| Purina | 00:e0:b8:76:28:e0 | 6 | 10 | 11 | 1098050710 | 100 |
| demoap-guest | 00:0c:41:16:df:95 | 11 | 10 | 8 | 1098063100 | 100 |
| BradLabNetwork | 00:40:96:58:7c:fd | 10 | 10 | 13 | 1098063117 | 100 |
| demoap | 00:0c:41:16:df:94 | 11 | 10 | 11 | 1098063120 | 100 |
| guest | 00:e0:b8:76:28:cf | 6 | 10 | 9 | 1098062834 | 100 |

Figure 29. Neighbor Details Information

The table displays the following information about the access point:

SSID

The *Service Set Identifier* (SSID) for the access point. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*.

To set the SSID, refer to “Configuring the Basic Settings and Starting the Wireless Network” on page 37, “Configuring Internal Wireless LAN Settings” on page 102, or “Configuring the Guest Network Wireless Settings” on page 103.

A guest network and an internal network running on the same access point must always have two different network names.

MAC Address

Shows the MAC address of the neighboring access point. A MAC address is a hardware address that uniquely identifies each node of a network.

Channel

Shows the channel on which the access point is currently broadcasting. The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving.

The channel is set on the Advanced > Radio Settings page. (See Chapter 13, "Configuring Radio Settings" on page 145.)

Rate

Shows the rate (in megabits per second) at which this access point is currently transmitting. The current rate will always be one of the rates shown in Supported Rates.

Signal

Indicates the strength of the radio signal emitting from this access point as measured in decibels (Db).

Beacon Interval

Shows the beacon interval being used by this access point. Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).

You set the Beacon Interval is set on the Advanced > Radio Settings page. (See Chapter 13, "Configuring Radio Settings" on page 145.)

Capability

A hexadecimal number which, when converted to binary, indicates each IEEE 802.11 feature or functionality and whether it is on or off on this access point.

Last Beacon

Shows the date and time of the most recent beacon was transmitted from the access point.

Chapter 8

Configuring Ethernet (Wired) Settings

Ethernet (wired) settings describe the configuration of your Ethernet local area network (LAN).

Note

The Ethernet settings, including guest access, are not shared across the cluster. You must configure these settings on the web pages for each access point. To get to the web pages for an access point that is a member of the current cluster, click on its IP Address link on the Cluster > Access Points page of the current access point. For more information about which settings are shared by the cluster and which are not, see “Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?” on page 45.

This chapter contains the following sections:

- ❑ “Setting the DNS Name” on page 88
- ❑ “Enabling or Disabling Guest Access” on page 90
- ❑ “Enabling or Disabling Spanning Tree” on page 92
- ❑ “Configuring the Internal Interface Ethernet Settings” on page 93
- ❑ “Configuring the Guest Interface Settings” on page 96

Setting the DNS Name

To set the DNS name, perform the following procedure:

1. From the main menu, select **Advanced > Ethernet (Wired) Settings**.

The Ethernet (Wired) Settings page is shown in Figure 30

Modify Ethernet (Wired) settings

DNS Name

Spanning Tree Protocol Enabled Disabled

Guest Access Enabled Disabled

For Guest access, use ▼

Virtual Wireless Networks Enabled Disabled
Using VLANs on Ethernet Port 1

Internal Interface Settings

MAC Address 00:0C:46:F2:D7:64

VLAN ID

PHY Type ▼

Secure Management Enabled Disabled

Management IP Address . . .

Deny Management via WLAN Enabled Disabled

Connection Type ▼

Static IP Address . . .

Subnet Mask . . .

Default Gateway . . .

DNS Nameservers Dynamic Manual

. . .

. . .

Guest Interface Settings

MAC Address 00:0C:46:F2:D7:64

VLAN ID

Subnet

Figure 30. Ethernet (Wired) Settings Page

2. In the Ethernet (Wired) Settings page, enter the DNS name.

The DNS name is the host name. It may be provided by your ISP or network administrator, or you can provide your own. The rules for DNS names are:

- The name can be up to 20 characters long.
- Only letters, numbers and dashes are allowed.
- The name must start with a letter and end with either a letter or a number.

Enabling or Disabling Guest Access

You can provide controlled guest access over a secure internal LAN on the AT-WA7400 Wireless Access Point.

Configuring an Internal LAN and a Guest Network

A local area network (LAN) is a communications network covering a limited area, for example, one floor of a building. A LAN connects multiple computers and other network devices like storage and printers.

Ethernet is the most common technology implementing a LAN. Wi-Fi (IEEE) is another very popular LAN technology.

The AT-WA7400 Management Software allows you to configure two different LANs on the same access point: one for a secure internal LAN and another for a public guest network with no security and little or no access to internal resources. To configure these networks, you need to provide both wireless and Ethernet (wired) settings.

Information on how to configure the Ethernet (wired) settings is provided in the sections below.

Enabling or Disabling Guest Access

The AT-WA7400 Management Software is shipped with the guest access feature disabled by default.

To provide guest access on your access point, perform the following procedure:

1. From the main menu, select **Advanced > Ethernet (Wired) Settings**.

The Ethernet (Wired) Settings page is shown in Figure 30 on page 88.

2. For the Guest Access setting, choose one of the following:

- Click **Enabled** to enable guest access.
- Click **Disabled** to disable guest access.

3. Click **Update** to save your changes.

Enabling or Disabling Virtual Wireless Networks on the Access Point

If you want to configure the internal network as a VLAN (whether or not you have a guest network configured), you must enable virtual wireless networks on the AT-WA7400 Wireless Access Point.

To enable or disable virtual wireless networks on the access point, perform the following procedure:

1. From the main menu, select **Advanced > Ethernet (Wired) Settings**.

The Ethernet (Wired) Settings page is shown in Figure 30 on page 88.

2. For the Virtual Wireless Networks setting, select one of the following:
 - Select **Enabled** to enable VLANs for the internal network and for additional networks. If you choose this option, you can run the internal network on a VLAN whether or not you have guest access configured and you can set up additional networks on VLANs using the Advanced > Virtual Wireless Networks page as described in Chapter 12, "VLANs" on page 139.
 - Select **Disabled** to disable the VLAN for the internal network, and for any additional virtual networks on this access point.
3. Click **Update** to save your changes.

Enabling or Disabling Spanning Tree

The AT-WA7400 Management Software allows you to enable or disable spanning tree through both the wired and wireless interfaces.

To enable or disable spanning tree, perform the following procedure:

1. From the main menu, select **Advanced > Ethernet (Wired) Settings**.

The Ethernet (Wired) Settings page is shown in Figure 30 on page 88.

2. For the Spanning Tree Protocol setting, choose one of the following:
 - Click **Enabled** to enable spanning tree.
 - Click **Disabled** to disable spanning tree.

Configuring the Internal Interface Ethernet Settings

To configure Ethernet (wired) settings for the internal LAN, perform the following procedure:

1. From the main menu, select **Advanced > Ethernet (Wired) Settings**.

The Ethernet (Wired) Settings page is shown in Figure 30 on page 88.

2. In the Internal Interface Settings section, configure the following settings:

MAC Address

Shows the MAC address for the internal interface for the Ethernet port on this access point. This is a read-only field that you cannot change.

VLAN ID

If you choose to configure internal and guest networks by VLANs, this field is enabled. Enter a number between 1 and 4094 for the internal VLAN.

This causes the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support VLAN IEEE 802.1Q frames. The access point must be able to reach the DHCP server.

Check with the Administrator regarding the VLAN and DHCP configurations.

PHY Type

The speed and duplex settings for the LAN (Ethernet) port. The options are:

Auto -The speed and duplex are automatically selected.
(recommended)

10Mbps Full - 10Mbps and full duplex.

10Mbps Half - 10Mbps and half duplex.

100Mbps Full - 100Mbps and full duplex.

100Mbps Half - 100Mbps and half duplex.

Secure Management

This selection enables or disables the Management IP Address field:
Enabled - Only the client with the IP address specified in the next selection can manage the access point.

Disabled - Even if an IP address for a wireless client is specified, no client can manage the AP.

Management IP Address

The IP address of a wireless client that can manage the access point.

Deny Management via WLAN

If checked, disables management access to the access point by a

wireless client associated with the AP, even if its IP address is defined in the Management IP Address field.

Connection Type

Select one of the following:

DHCP - The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows a centralized server to provide network configuration information to devices on the network. This information includes the IP address and netmask plus the address of its DNS servers and gateway.

Static IP - Static IP indicates that all network settings are provided manually. You must provide the IP address for the AT-WA7400 Wireless Access Point, its subnet mask, the IP address of the default gateway, and the IP address of at least one DNS nameserver.

If you select DHCP, the AT-WA7400 Wireless Access Point acquires its IP address, subnet mask, and DNS and gateway information from the DHCP Servers.



Caution

If you do not have a DHCP server on the internal network and do not plan to use one, the first thing you must do after you deploy the first access point is to verify that the connection type is set to Static IP. When you change the connection type to Static IP, you can either assign a new static IP address to the AT-WA7400 Wireless Access Point or continue using the default address. Allied Telesyn recommends assigning a new address so that if later you bring up another AT-WA7400 Access Point on the same network, the IP addresses for the two access points will be unique.

If you need to recover the default Static IP address, you can do so by resetting the access point to the factory defaults as described in “Resetting the Configuration to Factory Defaults” on page 206.

If you selected Static IP, configure the following settings:

Static IP Address

The static IP address.

Subnet Mask

The subnet mask. Obtain this information from your ISP or network administrator.

Default Gateway

The default gateway.

DNS Nameservers

The Domain Name Service (DNS) is a system that resolves the descriptive name (domainname) of a network resource (for example,

www.alliedtelesyn.com) to its numeric IP address (for example, 66.93.138.219). A DNS server is called a Nameserver.

There are usually two Nameservers; a Primary Nameserver and a Secondary Nameserver.

3. Choose **Dynamic** or **Manual** mode.

If you choose Manual, you should assign static IP addresses manually.

If you choose Dynamic, the IP addresses for the DNS servers is assigned automatically through DHCP. (This option is only available if you specified DHCP for the Connection Type.)

4. Click **Update** to save your changes.

Configuring the Guest Interface Settings

The guest interface settings allows a wireless client limited access to the network, for instance, to the Internet.

To configure the guest interface settings, perform the following procedure:

1. From the main menu, select **Advanced > Ethernet (Wired) Settings**.

The Ethernet (Wired) Settings page is shown in Figure 30 on page 88.

2. In the Guest Interface Settings section, configure the following settings:

MAC Address

Shows the MAC address for the internal interface for the Ethernet port on this access point. This is a read-only field that you cannot change.

VLAN ID

The ID number of the VLAN associated with the guest.

Subnet

The subnet mask of the subnetwork of which the guest is a member.

3. Click **Update** to save your changes.

Chapter 9

Configuring the Wireless Settings

Wireless settings describe aspects of the local area network (LAN) related specifically to the radio device in the access point (802.11 mode and channel) and to the network interface to the access point (MAC address for access point and wireless network name, also known as SSID).

The following sections describe how to configure the wireless address and related settings on the AT-WA7400 Wireless Access Point:

- “Configuring 802.11d Regulatory Domain Support” on page 98
- “Configuring the Radio Interface” on page 100
- “Configuring Internal Wireless LAN Settings” on page 102
- “Configuring the Guest Network Wireless Settings” on page 103

Configuring 802.11d Regulatory Domain Support

You can enable or disable IEEE 802.11d regulatory domain support to broadcast the access point country code information.

To configure the IEEE 802.11d regulatory domain support, perform the following procedure:

1. From the main menu, select **Advanced > Wireless Settings**.

The Wireless Settings page is shown in Figure 31.

The screenshot shows a web interface titled "Modify wireless settings". It contains several sections for configuration:

- 802.11d Regulatory Domain Support:** Includes radio buttons for "Enabled" (selected) and "Disabled". Below it is a dropdown menu for "Regulatory Domain (CountryCode)" set to "United States".
- Radio Interface One:** Includes a dropdown for "Mode" set to "IEEE 802.11a", a text field for "Wireless Network Name (SSID)" set to "allied", and a dropdown for "Channel" set to "52".
- Radar Detection:** Includes radio buttons for "Enabled" and "Disabled" (selected).
- Radio Interface Two:** Includes a dropdown for "Mode" set to "IEEE 802.11g", a text field for "Wireless Network Name (SSID)" set to "allied", and a dropdown for "Channel" set to "6".
- Guest Settings:** Includes a text field for "MAC Addresses" set to "n/a / n/a" and a text field for "Wireless Network Name (SSID)" set to "Guest AT-WA7400".

An "Update" button is located at the bottom right of the form.

Figure 31. Wireless Settings Page

2. Enable or disable the regulatory domain support setting:

Enabling support for IEEE 802.11d on the access point causes the access point to broadcast which country it is operating in as a part of its beacons:

- To enable 802.11d regulatory domain support click **Enabled**.
- To disable 802.11d regulatory domain support click **Disabled**.

3. Choose the regulatory domain from the **Regulatory Domain (Country Code)** list.
4. Click **Update** to save your settings

Configuring the Radio Interface

The radio interface allows you to set the radio channel and 802.11 mode for each radio.

To configure the radio interface, perform the following procedure:

1. From the main menu, select **Advanced > Wireless Settings**.

The Wireless Settings page is shown in Figure 31 on page 98.

2. In the Radio Interface sections one and two, configure the following settings:

Mode

The *Mode* defines the Physical Layer (PHY) standard being used by the radio.

The AT-WA7400 Wireless Access Point is available as a single or dual band access point with one or two radios. The configuration options for Mode differ depending on which product you have.

Single-Band Access Point - For the single-band access point, select one of these modes:

- IEEE 802.11b
- IEEE 802.11g
- Atheros Turbo 2.4 GHz
- Atheros Dynamic Turbo 2.4 GHz

Dual-Band Access Point - For the dual band access point, select one of these modes for each Radio Interface.

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11a
- Atheros Turbo 5 GHz (IEEE 802.11a Turbo)

Wireless Network Name (SSID)

The name for all wireless access points on this network. You cannot change this name on this page. To change this name, refer to “Configuring the Basic Settings and Starting the Wireless Network” on page 37.

Channel

Select the Channel. The range of channels and the default is determined by the Mode of the radio interface.

The channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).

The default is Auto, which picks the least busy channel at startup time.

Radar detection

When this option is enabled, if the access point detects military radar on the same frequency as the 802.11a channel to which the access point is set, the access point changes to a different channel.

3. Click **Update** to save your settings

Configuring Internal Wireless LAN Settings

The Internal Settings describe the MAC address (read-only) and Network Name (also known as the SSID) for the internal wireless LAN (WLAN).

To configure the internal settings, perform the following procedure:

1. From the main menu, select **Advanced > Wireless Settings**.

The Wireless Settings page opens, as shown in Figure 31 on page 98.

2. Configure the following settings:

MAC Address

Shows the MAC address(es) for internal interface for this access point. This is a read-only field that you cannot change.

Although this access point is physically a single device, it can be represented on the network as two or more nodes each with a unique MAC Address. You can do this by using multiple *Basic Service Set Identifiers* (BSSIDs) for a single access point.

The MAC address(es) shown for the internal access point is the BSSID(s) for the internal interface.

For the two-radio access point, two MAC addresses are shown: one for each radio on the internal interface.

Wireless Network Name (SSID)

Enter the **SSID** for the internal WLAN.

The *Service Set Identifier* (SSID) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

3. Click **Update** to save your settings

Configuring the Guest Network Wireless Settings

The guest settings describe the MAC address (read-only) and wireless network name (SSID) for the guest network. Configuring an access point with two different network names (SSIDs) allows you to leverage the guest interface feature on the AT-WA7400 Wireless Access Point.

To configure the guest network wireless settings, perform the following procedure:

1. From the main menu, select **Advanced > Wireless Settings**.

The Wireless Settings page is shown in Figure 31 on page 98.

2. In the Guest Settings section, configure the following settings:

MAC Address

Shows the MAC address for the guest interface for this access point. This is a read-only field that you cannot change.

Although this access point is physically a single device, it can be represented on the network as two or more nodes each with a unique MAC Address. This is accomplished by using multiple *Basic Service Set Identifiers* (BSSID) for a single access point.

The MAC address(es) shown for the guest access point is the BSSID(s) for the guest interface.

For the two-radio access point, two MAC addresses are shown: one for each radio on the guest interface.

Wireless Network Name (SSID)

Enter the SSID for the *guest network*.

The *Service Set Identifier* (SSID) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

For the guest network, provide an SSID that is different from the internal SSID and easily identifiable as the guest network.

3. Click **Update** to save your settings

Chapter 10

Configuring Security

The AT-WA7400 Management Software provides a number of authentication and encryption schemes to ensure that your wireless infrastructure is accessed only by the intended users. This chapter contains the following sections:

- ❑ “Understanding Security Issues on Wireless Networks” on page 106
- ❑ “Configuring Security Settings” on page 114
- ❑ “Configuring the IAPP Mapping Table” on page 129
- ❑ “Configuring SNMP” on page 131

Understanding Security Issues on Wireless Networks

Wireless mediums are inherently less secure than wired mediums. For example, an Ethernet NIC transmits its packets over a physical medium such as coaxial cable or twisted pair. A wireless NIC broadcasts radio signals allowing a wireless LAN to be easily tapped without physical access or sophisticated equipment. A hacker equipped with a laptop, a wireless NIC, and a bit of knowledge can easily attempt to compromise your wireless network. One does not even need to be within normal range of the access point. By using a sophisticated antenna on the client, a hacker may be able to connect to the network from many miles away.

For a more detailed explanation of security concepts, including a comparison of the advantages and disadvantages of using different security modes and suggestions on which mode to use, see Appendix B, “Configuring Security on Wireless Clients” on page 217.

How Do I Know Which Security Mode to Use?

In general, Allied Telesyn recommends that you use the most robust security mode that is feasible in your environment on your internal network. When you configure security on the access point, you first must choose the security mode, then in some modes an authentication algorithm, and whether to allow clients not using the specified security mode to associate.

Wi-Fi Protected Access (WPA) with Remote Authentication Dial-In User Service (RADIUS) using the CCMP (AES) encryption algorithm provides the best data protection available and is clearly the best choice if all client stations are equipped with WPA supplicants. However, backward compatibility or interoperability issues with clients or even with other access points may require that you configure WPA with RADIUS with a different encryption algorithm or choose one of the other security modes.

Security may not be as much of a priority on some types of networks. If you are only providing Internet and printer access, as on a guest network, plain text mode (no security) may be the appropriate choice. To prevent clients from accidentally discovering and connecting to your network, you can disable the broadcast SSID so that your network name is not advertised. If the network is sufficiently isolated from access to sensitive information, this may offer enough protection in some situations. This level of protection is the only one offered for guest networks, and also may be the right trade-off for other scenarios where the priority is making it as easy as possible for clients to connect. (See “Does Prohibiting the Broadcast SSID Enhance Security?” on page 113.)

Following is a brief discussion of what factors make one mode more secure than another, a description of each mode offered, and when to use each mode.

Comparison of Security Modes for Key Management, Authentication and Encryption Algorithms

Three major factors that determine the effectiveness of a security protocol are:

- How the protocol manages keys
- Presence or absence of integrated user authentication in the protocol
- Encryption algorithm or formula the protocol uses to encode/decode the data

Following are the security modes available in the AT-WA7400 Wireless Access Point along with a description of the key management, authentication, and encryption algorithms used in each mode and include some suggestions as to when one mode is more appropriate than another.

- Plain text
- Static WEP
- IEEE 802.1x
- WPA/WPA2 (Personal) PSK
- WPA/WPA2 Enterprise (RADIUS)

When to Use Plain Text

Plain text mode by definition provides no security. In this mode, the data is not encrypted but rather sent as “plain text” across the network. No key management, data encryption, or user authentication is used.

Plain text mode is **not recommended** for regular use on the internal network because it is not secure.

Plain text mode is the only mode in which you can run the guest network, which is by definition an unsecure LAN always virtually or physically separated from any sensitive information on the internal LAN.

Therefore, use plain text mode on the guest network and on the internal network for initial setup, testing, or problem solving only.

For information on how to configure plain text mode, see “Plain Text” on page 115.

When to Use Static WEP

Static Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared

Key for data encryption, as described in Table 1.

Table 1. Static WEP Configuration

| Key Management | Encryption Algorithm | User Authentication |
|--|---|--|
| <p>Static WEP uses a fixed key that is provided by the administrator. WEP keys are indexed in different slots (up to four on the AT-WA7400 Wireless Access Point). The client stations must have the same key indexed in the same slot to access data on the access point.</p> | <p>An RC4 stream cipher is used to encrypt the frame body and <i>cyclic redundancy checking</i> (CRC) of each 802.11 frame.</p> | <p>If you set the Authentication Algorithm to Shared Key, this protocol provides a rudimentary form of user authentication. However, if the Authentication Algorithm is set to Open System, no authentication is performed. If the algorithm is set to Both, only WEP clients are authenticated.</p> |

Static WEP was designed to provide security equivalent of sending unencrypted data through an Ethernet connection. However it contains major flaws and it does not provide even this intended level of security.

Therefore, **Static WEP is not recommended** as a security mode. The only time to use Static WEP is when interoperability issues make it the only option available to you and you are not concerned with the potential of exposing the data on your network.

For information on how to configure Static WEP security mode, see “Static WEP” on page 116.

When to Use IEEE 802.1x

IEEE 802.1x is the standard for passing the Extensible Authentication Protocol (EAP) over an 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). This is a newer, more secure standard than Static WEP, as described in Table 2.

Table 2. IEEE 802.1x Configuration

| Key Management | Encryption Algorithm | User Authentication |
|---|--|---|
| IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. There are different Unicast keys for each station. | An RC4 stream cipher is used to encrypt the frame body and <i>cyclic redundancy checking</i> (CRC) of each 802.11 frame. | IEEE 802.1x mode supports a variety of authentication methods, like certificates, Kerberos, and public key authentication with a RADIUS server. You have a choice of using the embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2. |

IEEE 802.1x mode is a better choice than Static WEP because keys are dynamically generated and changed periodically. However, the encryption algorithm used is the same as that of Static WEP and is therefore not as reliable as the more advanced encryption methods such as TKIP and SCMP (AES) used in Wi-Fi Protected Access (WPA) or WPA2.

Additionally, compatibility issues may be cumbersome because of the variety of authentication methods supported and the lack of a standard implementation method.

Therefore, IEEE 802.1x mode is not as secure a solution as Wi-Fi Protected Access (WPA) or WPA2. If, you cannot use WPA because some of your client stations do not have WPA, then a better solution than using IEEE 802.1x mode is to use WPA/WPA2 Enterprise (RADIUS) mode instead and check the Allow non-WPA IEEE 802.1x clients checkbox to allow non-WPA clients. This provides the benefit of IEEE 802.1x key management for non-WPA clients along with even better data protection of TKIP and CCMP (AES) key management and encryption algorithms for your WPA and WPA2 clients.

If you have an external RADIUS server on your network, Allied Telesyn recommends that you use it rather than the using the embedded RADIUS server on the access point. An external RADIUS server provides better security than the local authentication server.

For information on how to configure IEEE 802.1x security mode, see "IEEE 802.1x" on page 121.

When to Use WPA/WPA2 Personal (PSK)

Wi-Fi Protected Access 2 (WPA2) Personal Pre-Shared Key (PSK) is an implementation of the Wi-Fi Alliance IEEE 802.11 standard, which includes *Advanced Encryption Algorithm (AES)*, *Counter mode/CBC-MAC Protocol (CCMP)*, and *Temporal Key Integrity Protocol (TKIP)* mechanisms. This mode offers the same encryption algorithms as WPA 2 with RADIUS but without the ability to integrate a RADIUS server for user authentication.

This security mode is backwards-compatible for wireless clients that support only the original WPA. IEEE 802.1x mode supports a variety of authentication methods, like certificates, Kerberos, and public key authentication with a RADIUS server.

You have a choice of using the RADIUS server embedded in the AT-WA7400 Wireless Access Point or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2 WPA/WPA2 configuration is described in Table 3.

Table 3. WPA/WPA2 Configuration

| Key Management | Encryption Algorithm | User Authentication |
|---|--|---|
| WPA/WPA2 Personal (PSK) provides dynamically-generated keys that are periodically refreshed. There are different Unicast keys for each station. | - Temporal Key Integrity Protocol (TKIP) - Counter mode/CBC-MAC Protocol (CCMP) Advanced Encryption Standard (AES) | The use of a Pre-Shared (PSK) key provides user authentication similar to that of shared keys in WEP. |

WPA/WPA2 Personal (PSK) is not recommended for use with the AT-WA7400 Wireless Access Point when WPA/WPA2 Enterprise (RADIUS) is an option.

Allied Telesyn recommends that you use WPA/WPA2 Enterprise (RADIUS) mode instead, unless you have interoperability issues that prevent you from using this mode.

For example, some devices on your network may not support WPA or WPA2 with EAP talking to a RADIUS server. Embedded printer servers or other small client devices with very limited space for implementation may not support RADIUS. For such cases, we recommend that you use WPA/WPA2 Personal (PSK).

For information on how to configure this security mode, see “WPA/WPA2 Personal (PSK)” on page 123 under “Configuring Security Settings” on page 114.

When to Use WPA/WPA2 Enterprise (RADIUS)

Wi-Fi Protected Access 2 (WPA2) with Remote Authentication Dial-In User Service (RADIUS) is an implementation of the Wi-Fi Alliance IEEE 802.11i standard, which includes Advanced Encryption Standard (AES), Counter mode/CBC-MAC Protocol (CCMP), and Temporal Key Integrity Protocol (TKIP) mechanisms. This mode requires the use of a RADIUS server to authenticate users. WPA/WPA2 Enterprise (RADIUS) provides the best security available for wireless networks.

This security mode also provides backwards-compatibility for wireless clients that support only the original WPA, as described in Table 4.

Table 4. RADIUS Security

| Key Management | Encryption Algorithm | User Authentication |
|---|--|--|
| WPA/WPA2 Enterprise (RADIUS) mode provides dynamically-generated keys that are periodically refreshed. There are different unicast keys for each station. | <ul style="list-style-type: none"> - Temporal Key Integrity Protocol (TKIP) - Counter mode/CBC-MAC Protocol (CCMP) Advanced Encryption Standard (AES) | Remote Authentication Dial-In User Service (RADIUS) You have a choice of using the AT-WA7400 Management Software embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2. |

WPA/WPA2 Enterprise (RADIUS) mode is the **recommended mode**. The CCMP (AES) and TKIP encryption algorithms used with WPA modes are far superior to the RC4 algorithm used for Static WEP or IEEE 802.1x modes. Therefore, CCMP (AES) or TKIP should be used whenever possible. All WPA modes allow you to use these encryption schemes, so WPA security modes are recommended above the others when using WPA is an option.

Additionally, this mode incorporates a RADIUS server for user authentication which gives it an edge over WPA/WPA2 Personal (PSK) mode.

If you have an external RADIUS server on your network, Allied Telesyn recommends using it rather than the using the embedded RADIUS server on the access point. An external RADIUS server will provide better security than the local authentication server.

Use the following guidelines for choosing options within the WPA/WPA2 Enterprise (RADIUS) mode security mode:

- ❑ The best security you can have on a wireless network is WPA/WPA2 Enterprise (RADIUS) mode using CCMP (AES) encryption algorithm. AES is a symmetric 128-bit block data encryption technique that works on multiple layers of the network. It is the most effective encryption system currently available for wireless networks. If all clients or other access points on the network are WPA/CCMP compatible, use this encryption algorithm. (If all clients are WPA2 compatible, choose to support only WPA2 clients.)
- ❑ The second best choice is WPA/WPA2 Enterprise (RADIUS) with the encryption algorithm set to Both (that is, both TKIP and CCMP). This lets WPA client stations without CCMP associate, uses TKIP for encrypting multicast and broadcast frames, and allows clients to select whether to use CCMP or TKIP for unicast (access point-to-single-station) frames. This WPA configuration allows more interoperability, at the expense of some security. Client stations that support CCMP can use it for their unicast frames. If you encounter access point-to-station interoperability problems with the Both encryption algorithm setting, then you will need to select TKIP instead. (See next bullet.)
- ❑ The third best choice is WPA/WPA2 Enterprise (RADIUS) with the encryption algorithm set to TKIP. Some clients have interoperability issues with CCMP and TKIP enabled at same time. If you encounter this problem, then choose TKIP as the encryption algorithm. This is the standard WPA mode, and most interoperable mode with client wireless software security features. TKIP is the only encryption algorithm that is being tested in Wi-Fi WPA certification.

Note

If there are older client stations on your network that do not support WPA or WPA2, you can configure WPA/WPA2 Enterprise (RADIUS) with Both, CCMP, or TKIP and check the “Allow non-WPA IEEE 802.1x clients” checkbox to allow non-WPA clients. This provides IEEE 802.1x key management for non-WPA clients with even better data protection of TKIP and CCMP (AES) key management and encryption algorithms for your WPA clients.

A typical scenario is when you are upgrading a current 802.1x network to use WPA. You might have a mix of clients, some new clients that support WPA or WPA2 and some older ones that do not support any flavors of WPA. You might even have other access points on the network that support only 802.1x and some that support WPA with RADIUS or WPA2 Enterprise (RADIUS). For as long as this mix persists, use the “Allow non-WPA IEEE 802.1x clients” option

When all the stations have been upgraded to use WPA or better yet WPA2, you should disable the “Allow non-WPA IEEE 802.1x clients” option, and set the WPA Versions option appropriately (WPA, WPA2, or Both).

For information on how to configure this security mode, see “WPA/WPA2 Enterprise (RADIUS)” on page 125.

Does Prohibiting the Broadcast SSID Enhance Security?

You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the access point's broadcast SSID is suppressed, the network name is not displayed in the List of Available Networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it can connect.

Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect, or monitor plain text traffic.

This offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.

(See also “Guest Network” on page 116.)

How Does Station Isolation Protect the Network?

When station isolation is enabled, the access point blocks communication between wireless clients. The access point still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients.

The traffic blocking extends to wireless clients connected to the network via WDS links; these clients cannot communicate with each other when Station Isolation is on. See Chapter 16, “Configuring the Wireless Distribution System (WDS)” on page 173 for more information about WDS.

Configuring Security Settings

The following section explains how to configure security modes on the access point. Keep in mind that each wireless client that wants to exchange data with the access point must be configured with the same security mode and encryption key settings consistent with access point security.

On a two-radio access point, these Security Settings apply to both radios.

Note

Security modes other than plain text apply only to configuration of the internal network. On the guest network, you can use only plain text mode. (For more information about guest networks, see Chapter 11, “Setting Up Guest Access” on page 133.)

Broadcast SSID, Station Isolation, and Security Mode

To configure the broadcast SSID, station isolation, and security Mode, perform the following procedure:

1. From the main menu, select **Advanced > Security**.

The Security page is shown in Figure 32.

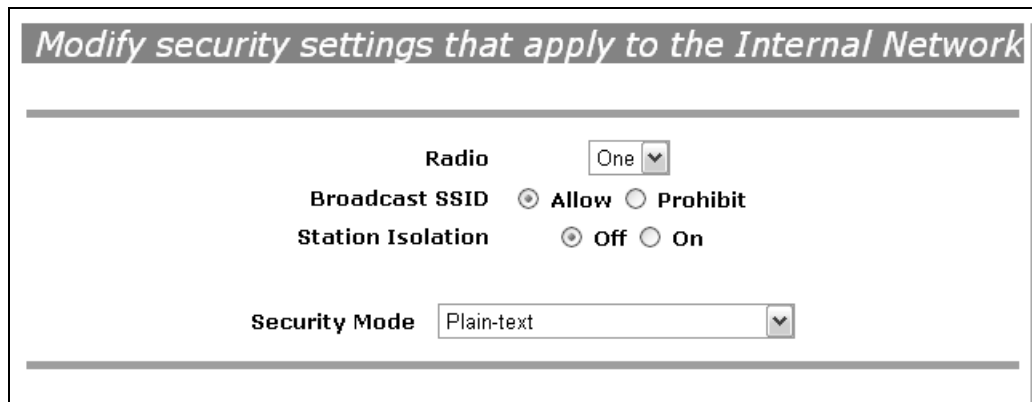


Figure 32. Security Page

2. Configure the following settings.

Note

Note you can also allow or prohibit the Broadcast SSID and enable/disable Station Isolation as extra precautions as mentioned below.

Broadcast SSID

Select the Broadcast SSID setting by clicking **Allow** or **Prohibit**.

By default, the access point broadcasts (allows) the Service Set Identifier (SSID) in its beacon frames.

You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the access point's broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it will be able to connect.

Station Isolation

Select Off to disable Station Isolation or On to enable it.

When Station Isolation is Off, wireless clients can communicate with one another normally by sending traffic through the access point.

When Station Isolation is On, the access point blocks communication between wireless clients. The access point still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients. The traffic blocking extends to wireless clients connected to the network via WDS links; these clients cannot communicate with each other when Station Isolation is on. See Chapter 16, "Configuring the Wireless Distribution System (WDS)" on page 173 for more information about WDS.

Security Mode

Select the Security Mode, one of the following:

- Plain Text
- Static WEP
- IEEE 802.1x
- WPA/WPA2 Enterprise (RADIUS)
- WPA/WPA2 Personal (PSK)

For a guest network, you can only use the plain text setting. (For more information, see Chapter 11, "Setting Up Guest Access" on page 133.)

3. Click **Update** to save your settings

Plain Text Plain text means any data transferred to and from the AT-WA7400

Wireless Access Point is not encrypted.

There are no further options for plain text mode.

Plain text mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the internal network because it is not secure.

Guest Network

Plain text mode is the only mode in which you can run the guest network, which is by definition an easily accessible, unsecure LAN always virtually or physically separated from any sensitive information on the internal LAN. For example, the guest network might provide Internet and printer access for day visitors.

The absence of security on the guest access point is designed to make it as easy as possible for guests to get a connection without having to program any security settings in their clients.

For a minimum level of protection on a guest network, you can choose to suppress (prohibit) the broadcast of the SSID (network name) to discourage client stations from automatically discovering your access point. (See also “Does Prohibiting the Broadcast SSID Enhance Security?” on page 113.)

For more about the guest network, see Chapter 11, “Setting Up Guest Access” on page 133.

Static WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

You cannot mix 64-bit and 128-bit WEP keys between the access point and its client stations.

Static WEP is not the most secure mode available, but it offers more protection than plain text mode as it does prevent an outsider from easily sniffing out unencrypted wireless traffic. (For more secure modes, see the sections on “IEEE 802.1x” on page 121, “WPA/WPA2 Enterprise (RADIUS)” on page 125, or “WPA/WPA2 Personal (PSK)” on page 123.)

WEP encrypts data moving across the wireless network based on a static key. (The encryption algorithm is a stream cipher called RC4.)

The access point uses a key to transmit data to the client stations. Each client station must use that same key to decrypt data it receives from the access point.

Client stations can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

If you selected Static WEP Security Mode, the settings in Figure 33 are displayed at the bottom of the page.

The screenshot shows a configuration window for Static WEP Security Mode. At the top, 'Security Mode' is set to 'Static WEP'. Below this, 'Transfer Key Index' is a dropdown menu set to '1'. 'Key Length' has two radio buttons: '64 bits' (unselected) and '128 bits' (selected). 'Key Type' has two radio buttons: 'ASCII' (unselected) and 'Hex' (selected). 'Characters Required' is a text input field containing '26'. Below this are four text input fields for 'WEP Keys', labeled '1:', '2:', '3:', and '4:'. At the bottom, 'Authentication Algorithms' is a dropdown menu set to 'Open System'.

Figure 33. Static WEP Security Mode Settings

1. Configure the following settings:

Transfer Key Index

Select a key index from the list. Key indexes 1 through 4 are available. The default is 1.

The Transfer Key Index indicates which WEP key the access point will use to encrypt the data it transmits.

Key Length

Specify the length of the key by clicking one of the buttons:

- 64 bits
- 128 bits

Key Type

Select the key type by clicking one of the buttons:

- ASCII
- Hex

Characters Required

Indicates the number of characters required in the WEP key.

The number of characters required updates automatically based on how you set Key Length and Key Type.

WEP Keys

You can specify up to four WEP keys. In each text box, enter a string of characters for each key.

If you selected ASCII, enter any combination of integers and letters 0–9, a–z, and A–Z. If you selected HEX, enter hexadecimal digits (any combination of 0–9 and a–f or A–F).

Use the same number of characters for each key as specified in the Characters Required field. These are the RC4 WEP keys shared with the stations using the access point.

Each client station must be configured to use one of these same WEP keys in the same slot as specified here on the access point. (See “Rules to Remember for Static WEP” on page 119.)

Authentication Algorithm

The authentication algorithm defines the method used to determine whether a client station is allowed to associate with an access point when static WEP is the security mode.

Specify the authentication algorithm you want to use by choosing one of the following from the list:

Open System

Open System authentication allows any client station to associate with the access point whether that client station has the correct WEP key or not. This algorithm is also used in plain text, IEEE 802.1x, and WPA modes. When the authentication algorithm is set to Open System, any client can associate with the access point.

Note that just because a client station is allowed to *associate* does not ensure it can exchange traffic with an access point. A station must have the correct WEP key to be able to successfully access and decrypt data from an access point, and to transmit readable data to the access point.

Shared Key

Shared Key authentication requires the client station to have the correct WEP key in order to associate with the access point. When the authentication algorithm is set to Shared Key, a station with an incorrect WEP key will not be able to associate with the access point.

Both

This is the default. When the authentication algorithm is set to Both:

- Client stations configured to use WEP in shared key mode must have a valid WEP key in order to associate with the access point.
- Client stations configured to use WEP as an open system (shared key mode not enabled) will be able to associate with the access point even if they do not have the correct WEP key.

Rules to Remember for Static WEP

- ❑ All client stations must have the wireless LAN (WLAN) security set to WEP and all clients must have one of the WEP keys specified on the access point in order to de-code access point-to-station data transmissions.
- ❑ The access point must have all keys used by clients for station-to-access point transmit so that it can de-code the station transmissions.
- ❑ The same key must occupy the same slot on all nodes (access point and clients). For example if the access point defines abc123 key as WEP key 3, then the client stations must define that same string as WEP key 3.
- ❑ On some wireless client software (like Funk Odyssey), you can configure multiple WEP keys and define a client station transfer key index, and then set the stations to encrypt the data they transmit using different keys. This ensures that neighboring access points cannot decode each other's transmissions.

Example of Using Static WEP

For a simple example, suppose you configure three WEP keys on the access point. In the following example, the Transfer Key Index for the access point is set to "3". This means that the WEP key in slot "3" is the key the access point will use to encrypt the data it sends.

The screenshot shows a configuration window for Static WEP. At the top, 'Security Mode' is set to 'Static WEP'. Below this, the 'Transfer Key Index' is set to '3'. The 'Key Length' is set to '64 bits' (selected with a radio button), and 'Key Type' is set to 'ASCII' (selected with a radio button). 'Characters Required' is set to '5'. There are four input fields for 'WEP Keys': key 1 is 'abcde', key 2 is 'fghij', key 3 is 'klmno', and key 4 is empty. At the bottom, 'Authentication Algorithms' is set to 'Both'.

Figure 34. Setting the AP Transfer Key on the Access Point

You must then set all client stations to use WEP and provide each client with one of the slot/key combinations you defined on the access point.

Figure 35 illustrates setting the WEP key 1 on a Windows client.

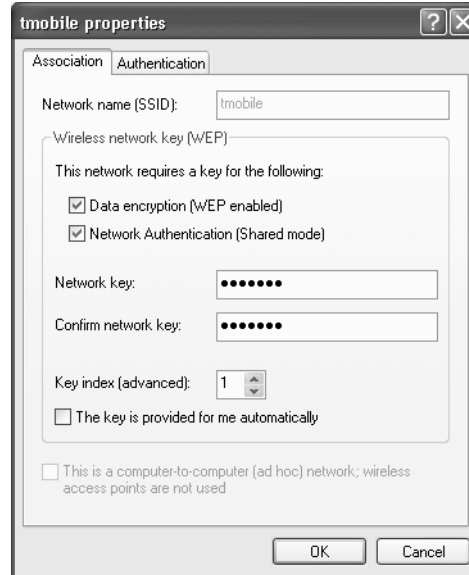


Figure 35. Providing a Wireless Client with a WEP Key

If you have a second client station, that station also needs to have one of the WEP keys defined on the access point. You could give it the same WEP key you gave to the first station. Or for a more secure solution, you could give the second station a different WEP key (key 2, for example) so that the two stations cannot decrypt each other's transmissions.

Static WEP with Transfer Key Indexes on Client Stations

Some wireless client software (like Funk Odyssey) lets you configure multiple WEP keys and set a transfer index on the client station, then you can specify different keys to be used for station-to-access point transmissions. (The standard Windows wireless client software does not allow you to do this.)

To build on the example, using Funk Odyssey client software you could give each of the clients WEP key 3 so that they can decode the access point transmissions with that key and also give client 1 WEP key 1 and set this as its transfer key. You could then give client 2 WEP key 2 and set this as its transfer key index.

The following figure illustrates the dynamics of the access point and two client stations using multiple WEP keys and a transfer key index.

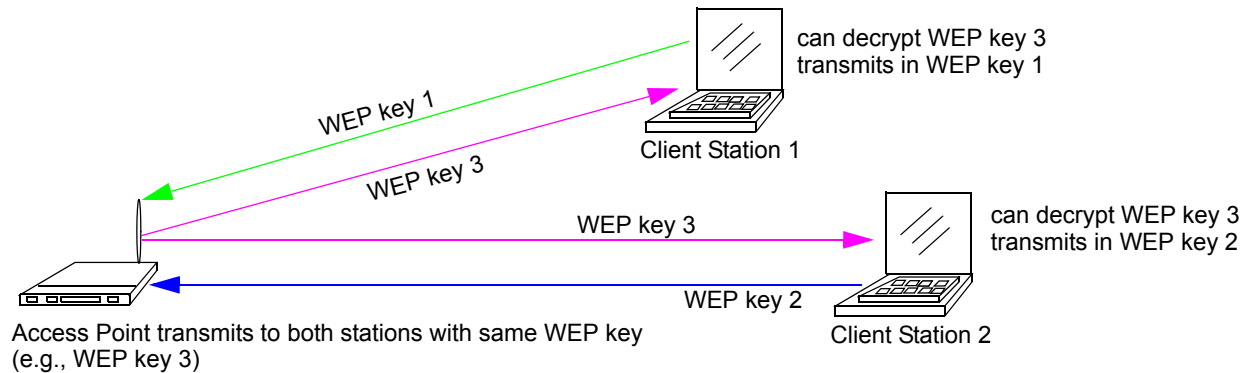


Figure 36. Example of Using Multiple WEP Keys and Transfer Key Index on Client Stations

IEEE 802.1x

IEEE 802.1x is the standard defining port-based authentication and infrastructure for doing key management. Extensible Authentication Protocol (EAP) messages sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

This mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts on the Cluster > User Management page.

The access point requires a RADIUS server capable of EAP, such as the Microsoft Internet Authentication Server or the AT-WA7400 Wireless Access Point's internal authentication server. To work with Windows clients, the authentication server must support Protected EAP (PEAP) and MSCHAP V2.

When configuring IEEE 802.1x mode, you have a choice of whether to use the embedded RADIUS server or an external RADIUS server that you provide. The AT-WA7400 Wireless Access Point's embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

If you use your own RADIUS server, you have the option of using any of a variety of authentication methods that the IEEE 802.1x mode supports, including certificates, Kerberos, and public key authentication. Keep in mind, however, that the client stations must be configured to use the same authentication method being used by the access point.

When you select IEEE 802.1x Security Mode, the settings shown in Figure 37 are displayed at the bottom of the page.

Security Mode IEEE 802.1x ▼

Authentication Server Built-in ▼

Radius IP 127 . 0 . 0 . 1

Radius Port 1812 (Range: 0-65535)

Radius Key ●●●●●●

WPA Group Rekey Interval 1800 (Range: 30-1800)

Enable radius accounting

Figure 37. IEEE 802.1x Security Mode Settings

1. Configure the following settings:

Authentication Server

Select one of the following from the list:

Built-in - To use the authentication server provided with the AT-WA7400 Wireless Access Point. If you choose this option, you do not need to provide the Radius IP and Radius Key; they are automatically provided.

External - To use an external authentication server. If you choose this option you must supply a Radius IP and Radius Key of the server you want to use.

Note

The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. With firmware version 1.0 and greater, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are configurable. (The AT-WA7400 Management Software defaults to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)

RADIUS IP

The Radius IP is the IP address of the RADIUS server.

(The IP address of the AT-WA7400 Wireless Access Point's internal authentication server is 127.0.0.1.)

If you have an external RADIUS server on your network, Allied Telesyn recommends that you use it rather than the using the embedded RADIUS server on the access point. An external RADIUS server will provide better security than the local authentication server.

For information on setting up user accounts, see Chapter 4, “Managing User Accounts” on page 57.

RADIUS Port

The default port number is 1812. You can change this if your application requires it.

RADIUS Key

The Radius Key is the shared secret key for the RADIUS server. The text you enter is displayed as “*” characters to prevent others from seeing the RADIUS key as you type.

(The AT-WA7400 Management Software internal authentication server key is secret.)

This value is never sent over the network.

WPA Group Rekey Interval

The interval after which the WPA encryption key is automatically changed and authenticated between devices. The shorter the interval is, the stronger that the encryption is. Allied Telesyn recommends that you use the default interval.

Enable RADIUS Accounting

Click Enable RADIUS Accounting if you want to track and measure the resources a particular user has consumed such system time, amount of data transmitted and received, and so on.

2. Click **Update** to save your settings.

WPA/WPA2 Personal (PSK)

Wi-Fi Protected Access 2 (WPA2) with Pre-Shared Key (PSK) is a Wi-Fi Alliance IEEE 802.11 standard, which includes Advanced Encryption Algorithm (AES), Counter mode/CBC-MAC Protocol (CCMP), and Temporal Key Integrity Protocol (TKIP) mechanisms. The Personal version of WPA2 employs a pre-shared key (instead of using IEEE 802.1x and EAP as is used in the Enterprise WPA2 security mode). The PSK is used for an initial check of credentials only.

This security mode is backwards-compatible for wireless clients that support the original WPA.

When you select the WPA/WPA2 Personal (PSK) security mode, the settings in Figure 38 are displayed.

The screenshot shows a configuration window for WPA/WPA2 Personal (PSK) Security Mode. At the top, the 'Security Mode' is set to 'WPA/WPA2 Personal (PSK)'. Below this, there are three sections: 'WPA Versions' with a dropdown menu set to 'Both', 'Cipher Suites' with a dropdown menu set to 'TKIP', and a 'Key' field which is currently empty.

Figure 38. WPA/WPA2 Personal (PSK) Security Mode Settings

1. Configure the following settings:

WPA Versions

Select the types of client stations you want to support:

WPA - If all client stations on the network support the original WPA but none support the newer WPA2, then select WPA.

WPA2 - If all client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.

Both - If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select Both. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.

Cipher Suites

Select the cipher you want to use:

Temporal Key Integrity Protocol (TKIP) - This is the default. TKIP provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be re-used to encrypt data (a weakness of WEP). TKIP uses a 128-bit temporal key shared by clients and access points. The temporal key is combined with the client's MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client station uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network.

Counter mode/CBC-MAC Protocol (CCMP) - CCMP is an encryption method for IEEE 802.11 that uses the Advanced Encryption Algorithm (AES). It uses a CCM combined with Cipher Block Chaining Counter

mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

Both - When the authentication algorithm is set to Both, both TKIP and AES clients can associate with the access point. WPA clients must have one of the following to be able to associate with the access point:

- A valid TKIP key
- A valid CCMP (AES) key

Clients not configured to use a WPA-PSK cannot associate with the access point.

Key

The Pre-shared Key is the shared secret key for WPA-PSK. Enter a string of at least 8 characters to a maximum of 63 characters.

2. Click **Update** to save your settings.

WPA/WPA2 Enterprise (RADIUS)

Wi-Fi Protected Access 2 (WPA2) with Remote Authentication Dial-In User Service (RADIUS) is an implementation of the Wi-Fi Alliance IEEE 802.11i standard, which includes Advanced Encryption Standard (AES), Counter mode/CBC-MAC Protocol (CCMP), and Temporal Key Integrity Protocol (TKIP) mechanisms. The Enterprise mode requires the use of a RADIUS server to authenticate users, and the configuration of user accounts using the Cluster > User Management page.

This security mode is backwards-compatible with wireless clients that support the original WPA.

When you configure WPA2 Enterprise (RADIUS) mode, you have a choice of whether to use the built-in RADIUS server or an external RADIUS server that you provide. The AT-WA7400 Management Software built-in RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

If you select the WPA/WPA2 Enterprise (RADIUS) security mode, the settings in Table 39 are displayed:

The screenshot shows a configuration window for WPA/WPA2 Enterprise (RADIUS) Security Mode. The settings are as follows:

- Security Mode:** WPA/WPA2 Enterprise (RADIUS) (dropdown)
- WPA Versions:** Both (dropdown)
- Enable pre-authentication:**
- Cipher Suites:** TKIP (dropdown)
- Authentication Server:** Built-in (dropdown)
- Radius IP:** 127 . 0 . 0 . 1 (text input)
- Radius Port:** 1812 (Range: 0-65535) (text input)
- Radius Key:** [Masked with 6 dots] (text input)
- WPA Group Rekey Interval:** 1800 (Range: 30-1800) (text input)
- Enable radius accounting:**

Figure 39. WPA/WPA2 Enterprise (RADIUS) Security Mode Settings

1. Configure the following settings:

WPA Versions

Select the types of client stations you want to support:

WPA - If all client stations on the network support the original WPA but none support the newer WPA2, then select WPA.

WPA2 - If all client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.

Both - If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select Both. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.

Enable pre-authentication

If for WPA Versions you select WPA2 or Both, you can enable pre-authentication for WPA2 clients.

Click Enable pre-authentication if you want WPA2 wireless clients to send pre-authentication packet. The pre-authentication information will be relayed from the access point the client is currently using to the target access point. Enabling this feature can help speed up authentication for roaming clients who connect to multiple access points.

This option does not apply if you selected WPA for WPA Versions because the original WPA does not support this feature.

Cipher Suites

Select the cipher you want to use:

Temporal Key Integrity Protocol (TKIP) - This is the default. TKIP provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be re-used to encrypt data (a weakness of WEP). TKIP uses a 128-bit temporal key shared by clients and access points. The temporal key is combined with the client's MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client station uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network.

Counter mode/CBC-MAC Protocol (CCMP) - CCMP is an encryption method for IEEE 802.11 that uses the Advanced Encryption Algorithm (AES). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

Both - When the authentication algorithm is set to Both, both TKIP and AES clients can associate with the access point. Client stations configured to use WPA with RADIUS must have one of the following to be able to associate with the access point:

- A valid TKIP RADIUS IP address and valid shared Key
- A valid CCMP (AES) IP address and valid shared Key

Clients not configured to use a WPA-PSK will not be able to associate with the access point. Both is the default.

Authentication Server

Select one of the following:

Built-in - To use the authentication server provided with the AT-WA7400 Management Software. If you choose this option, you do not have to provide the Radius IP and Radius Key; they are automatically provided.

External - To use an external authentication server. If you choose this option you must supply a Radius IP and Radius Key of the server you want to use.

Note

The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. With firmware version 1.0 and greater, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are configurable. (The AT-WA7400 Wireless Access Point defaults to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)

RADIUS IP

The IP address of the RADIUS server.

(The IP address of the AT-WA7400 Wireless Access Point's internal authentication server is 127.0.0.1.)

If you have an external RADIUS server on your network, we recommend using it rather than the using the embedded RADIUS server on the access point. An external RADIUS server will provide better security than the local authentication server.

For information on setting up user accounts, see Chapter 4, "Managing User Accounts" on page 57.

RADIUS Port

The default port number is 1812. You can change this if your application requires it.

RADIUS Key

The RADIUS Key, the shared secret key for the RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type.

(The IP address of the AT-WA7400 Wireless Access Point's internal authentication server key is secret.)

This value is never sent over the network.

WPA Group Rekey Interval

The interval after which the WPA encryption key is automatically changed and authenticated between devices. The shorter the interval is, the stronger that the encryption is. Allied Telesyn recommends that you use the default interval.

Enable RADIUS Accounting

Click Enable RADIUS Accounting if you want to enforce authentication for WPA client stations with user names and passwords for each station.

See also Chapter 4, "Managing User Accounts" on page 57.

2. Click **Update** to save your settings.

Configuring the IAPP Mapping Table

The Inter-Access-Point Protocol (IAPP) enforces a unique association through an extended service set (ESS) for the secure exchange of the station's security information between access points.

To configure the IAPP map table, perform the following procedure:

1. From the main menu, select **Advanced > IAPP Table**.

The Configure IAPP map table page is shown in Figure 40.

The screenshot shows the 'Configure IAPP Map Table' interface. At the top, the title 'Configure IAPP Map Table' is displayed. Below the title, the 'Inter-Access-Point Protocol (IAPP)' is set to 'Enabled'. A large empty box labeled 'IAPP Map Table' is present, with a 'Remove' button below it. At the bottom, there are input fields for 'IP Address' (four boxes separated by dots) and 'MAC Address' (six boxes separated by colons), with an 'Add' button between them. An 'Update' button is located at the bottom right.

Figure 40. IAPP Map Table

2. For the Inter-Access-Point-Protocol setting, click **Enable**.
3. To add a station to the map table:
 - a. In the fields below the map table, enter the IP and MAC addresses of the station you want to add.
 - b. Click **Add**.
 - c. Click **Update**.

4. To remove a station from the map table:
 - a. In map table, select the station you want to remove.
 - b. Click **Remove**.
 - c. Click **Update**.

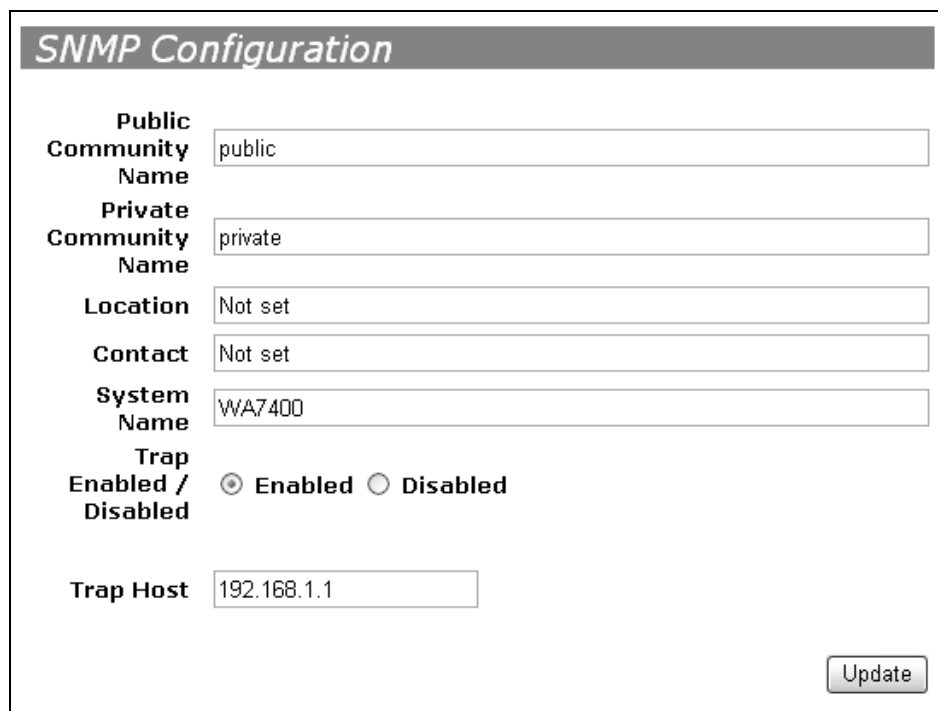
Configuring SNMP

Simple Network Management Protocol (SNMP) is another way for you to manage the access point. This type of management involves viewing and changing the management information base (MIB) objects on the device using an SNMP application program.

To configure SNMP, perform the following procedure:

1. From the main menu, select **Advanced > SNMP Configuration**.

The SNMP Configuration page is shown in Figure 41.



The screenshot shows the 'SNMP Configuration' page with the following fields and options:

- Public Community Name:** public
- Private Community Name:** private
- Location:** Not set
- Contact:** Not set
- System Name:** WA7400
- Trap Enabled / Disabled:** Enabled Disabled
- Trap Host:** 192.168.1.1
- Update:** Button

Figure 41. SNMP Configuration Page

2. Configure the following parameters:

Public Community Name

This community name has read privileges only. Enter a name for the public community name.

Private Community Name

The private community name has an access mode of read/write. If you enable SNMP management, Allied Telesyn recommends that you remove the private community name to prevent others from making unauthorized changes to the access point.

Location

The physical location of the access point.

Contact

The contact person for the access point.

System Name

A unique name given to this access point.

Trap Enabled/Disabled

A trap is a signal sent to one or more management workstations by the access point to indicate the occurrence of a particular operating event on the access point. Choose **Enabled** or **Disabled**.

Trap Host

The IP address of the workstation where trap messages are sent.

3. Click **Update**.

Chapter 11

Setting Up Guest Access

The guest interface features allow you to configure the AT-WA7400 Wireless Access Point for controlled guest access to an isolated network. You can configure the same access point to broadcast and function as two different wireless networks: a secure internal LAN and a public guest network.

Guest clients can access the guest network without a username or password. When guests log in, they see a guest Welcome screen (also known as a captive portal).

This chapter contains the following sections:

- “Understanding the Guest Interface” on page 134
- “Configuring the Guest Interface” on page 135
- “Using the Guest Network as a Client” on page 137

Understanding the Guest Interface

You can define unique parameters for guest connectivity and isolate guest clients from other more sensitive areas of the network. No security is provided on the guest network; only plain text security mode is allowed.

Simultaneously, you can configure a secure internal network (using the same access point as your guest interface) that provides full access to protected information behind a firewall and requires secure logins or certificates for access.

You configure an AT-WA7400 Wireless Access Point using a single network with VLANs by setting up the guest interface configuration options on the web pages for the AT-WA7400 Wireless Access Point. (For details on how to set up this type of guest interface, see “Configuring a Guest Network on a Virtual LAN” on page 135.)

This method leverages multiple BSSID and Virtual LAN (VLAN) technologies that are built in to the AT-WA7400 Wireless Access Point. The guest network is implemented as multiple BSSIDs on the same access point, each with different network names (SSIDs) on the wireless interface and different VLAN IDs on the Wired interface.

On a two-radio access point, the guest management and login settings apply to both radio one and radio two.

Configuring the Guest Interface

To configure the guest interface on the AT-WA7400 Wireless Access Point, perform these configuration steps:

1. Configure the access point to represent two *virtually* separate networks as described in “Configuring a Guest Network on a Virtual LAN” on page 135.
2. Set up the guest Welcome screen for the guest captive portal as described in “Configuring the Welcome Screen (Captive Portal)” on page 136.

Configuring a Guest Network on a Virtual LAN

Note

If you want to configure the guest and internal networks on Virtual LAN (VLANs), the switch and DHCP server you are using must support VLANs.

As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE 802.1Q standard.

Guest Welcome Screen settings are shared among access points across the cluster. When you update these settings for one access point, the configuration is shared with the other access points in the cluster. For more information about which settings are shared by the cluster and which are not, see “Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?” on page 45.

To configure internal and guest networks on virtual LANs, perform the following procedure:

1. Use only one wired connection from the network port on the access point to the LAN. (Make sure this port is configured to handle VLAN tagged packets.)
2. Configure Ethernet (wired) Settings for internal and guest networks on VLANs as described in Chapter 8, “Configuring Ethernet (Wired) Settings” on page 87.
3. Start by enabling guest access as described in “Enabling or Disabling Guest Access” on page 90.
4. Provide the radio interface settings and network names (SSIDs) for both internal and guest networks as described in Chapter 9, “Configuring the Wireless Settings” on page 97.

5. Configure the guest splash screen as described in “Configuring the Welcome Screen (Captive Portal),” next.

Configuring the Welcome Screen (Captive Portal)

You can set up or modify the Welcome screen (captive portal) guest clients see when they open a web browser or try to browse the web.

To set up the captive portal, perform the following procedure:

1. From the main menu, select **Advanced > Guest Login**.

The Guest Login configuration page is shown in Figure 42.

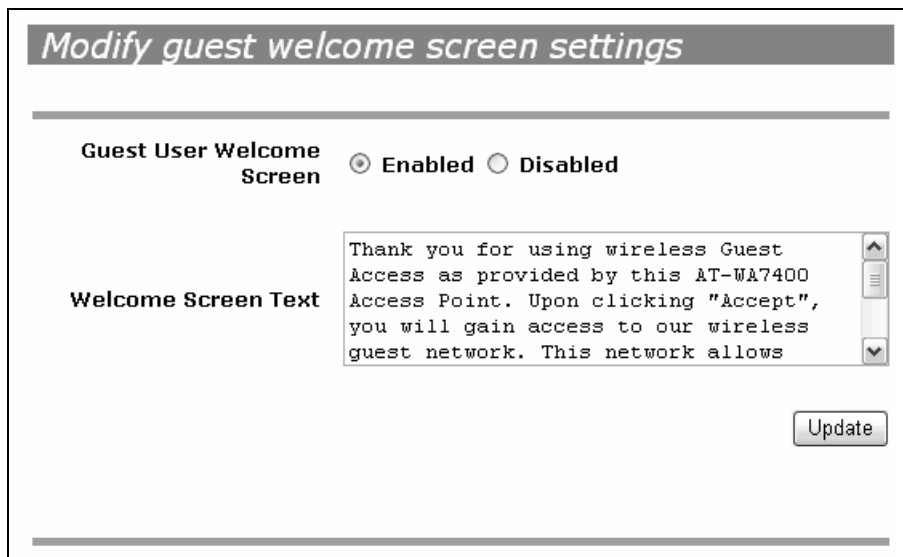


Figure 42. Guest Login Configuration Page

2. Choose **Enabled** to activate the Welcome screen.
3. In the Welcome Screen Text field, type the text message you would like guest clients to see on the captive portal.
4. Click **Update** to save your changes.

Using the Guest Network as a Client

After the guest network is configured, a client can access the guest network as follows:

- ❑ A guest client enters an area of coverage and scans for wireless networks.
- ❑ The guest network advertises itself via a guest AT-WA7400 Wireless Access Point SSID or some similar name, depending on how the guest SSID is specified in the web pages for the guest interface.
- ❑ The guest client chooses guest AT-WA7400 Wireless Access Point SSID.
- ❑ The guest client starts a web browser and receives a Guest Welcome screen.
- ❑ The guest Welcome Screen provides a button for the client to click to continue.
- ❑ The guest client is now enabled to use the guest network.

Chapter 12

VLANs

This chapter describes how to configure Virtual LANs (VLANs) for multiple wireless networks and management and includes the following sections:

- ❑ “Configuring VLANs” on page 140
- ❑ “Configuring the Management VLAN” on page 143

Configuring VLANs

Note

To configure additional networks on VLANs, you must first enable virtual wireless networks on the Ethernet (wired) interface. See “Enabling or Disabling Virtual Wireless Networks on the Access Point” on page 90.



Caution

If you configure VLANs, you may lose connectivity to the access point. First, be sure to verify that the switch and DHCP server you are using can support VLANs per the IEEE 802.1Q standard. After configuring VLANs, physically reconnect the Ethernet cable on the switch to the tagged packet (VLAN) port. Then, reconnect using the web pages to the new IP address. (If necessary, check with the infrastructure support administrator regarding the VLAN and DHCP configurations.)

To configure a VLAN, perform the following procedure:

1. From the main menu, select **Advanced > Virtual Wireless Networks**.

The Virtual Wireless Networks page is shown in Figure 43.

Modify Virtual Wireless Network settings

Virtual Wireless Network One ▾

Status On Off

Wireless Network Name (SSID)

VLAN ID

Broadcast SSID Allow Prohibit

Security Mode

Figure 43. Virtual Wireless Networks Page

2. Configure the following settings as necessary:

Virtual Wireless Network

Choose one of the following from the list to identify an additional network to configure:

- One
- Two

Status

To enable the specified network, click **On**. To disable the specified network, click **Off**.

Wireless Network Name (SSID)

Enter a name for the wireless network as a character string. This name applies to all access points on this network. As you add more access points, they will use this SSID.

The Service Set Identifier (SSID) is an alphanumeric string of up to 32 characters

Note

If you are connected as a wireless client to the same access point that you are administering, resetting the SSID will cause you to lose connectivity to the access point. You will need to reconnect to the new SSID after you save this new setting.

VLAN ID

Provide a number between 1 and 4094 for the internal VLAN.

This will cause the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support VLAN IEEE 802.1Q frames. The access point must be able to reach the DHCP server.

Check with the Administrator regarding the VLAN and DHCP configurations.

Broadcast SSID

Select the Broadcast SSID setting by clicking **Allow** or **Prohibit**.

By default, the access point broadcasts (allows) the Service Set Identifier (SSID) in its beacon frames.

You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the access point's broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it will be able to connect.

Note

The Broadcast SSID you set here is specifically for this Virtual Network (One or Two). Other networks continue to use the security modes already configured:

Your original internal network (configured on the Advanced > Ethernet [Wired] page) uses the Broadcast SSID set on the Advanced > Security page.

If a Guest network is configured, the Broadcast SSID is always allowed.

Security Mode

Select the Security Mode for this VLAN, one of the following:

- Plain text
- Static WEP
- IEEE 802.1x
- WPA/WPA2 Personal (PSK)
- WPA/WPA2 Enterprise (RADIUS)

Note

The Security mode you set here is specifically for this Virtual Network (One or Two). Other networks continue to use the security modes already configured.

Your original internal network (configured on the Advanced > Ethernet [Wired] page) uses the Security mode set on the Advanced > Security page.

If a Guest network is configured, it always using plain text security mode.

3. Click **Update** to save your changes.

Configuring the Management VLAN

When you configure a management VLAN, only those users who have the required IP address and subnet mask of the management AP can make any management changes.

To configure the management VLAN, perform the following procedure:

1. From the main menu, select **Advanced > VLAN Management**.

The VLAN Management page is shown in Figure 44.

Modify Management VLAN settings

Separated VLAN Management Enabled Disabled

VLAN ID

Management IP Address . . .

Management IP Subnet Mask . . .

Figure 44. VLAN Management Page

To set up the management VLAN, you must first enable it.

2. For the Separated VLAN Management setting, click **Enabled**.
The rest of the fields on the page become available.
3. For the VLAN ID, setting, enter a number for the VLAN ID.
4. For the Management IP address, enter the AT-WA7400 management IP address associated with this VLAN.
5. For the Management IP Subnet Mask, enter the subnet mask associated with the VLAN.
6. Click **Update**.

Chapter 13

Configuring Radio Settings

This chapter describes how to configure radio settings on the AT-WA7400 Wireless Access Point, and includes the following sections:

- “Understanding Radio Settings” on page 146
- “Configuring Radio Settings” on page 147

Note

If you are using the two-radio version of the AT-WA7400 Access Point, keep in mind that both radio one and radio two are configured on this page. The displayed settings apply to either radio one or radio two, depending on which radio you choose in the Radio field (first field on the page). When you have configured settings for one of the radios, click Update and then select and configure the other radio. Be sure to click Update to apply the second set of configuration settings for the other radio.

Understanding Radio Settings

Radio settings directly control the behavior of the radio device in the access point and its interaction with the physical medium; that is, how/ what type of electromagnetic waves the access point emits. You can specify whether the radio is on or off, radio frequency (RF), broadcast channel, beacon interval (amount of time between access point beacon transmissions), transmit power, IEEE 802.11 mode in which the radio operates, and so on.

The AT-WA7400 Wireless Access Point is capable of broadcasting in the following modes:

- IEEE 802.11b mode
- IEEE 802.11g mode
- IEEE 802.11a mode
- Atheros Turbo 5 GHz
- Atheros Dynamic Turbo 5 GHz
- Atheros Turbo 2.4 GHz
- Atheros Dynamic Turbo 2.4 GHz

For more information about Atheros Turbo modes see 802.11a Turbo.

You configure the IEEE mode along with other radio settings as described in “Configuring Radio Settings” on page 147.

Configuring Radio Settings

To configure the radio settings, perform the following procedure:

1. From the main menu, select **Advanced > Radio**.

The Radio page for radio one is shown in Figure 45.

Modify radio settings

Radio

Status On Off

Mode

Super AG Enabled Disabled

Channel

Beacon Interval (Msec, Range: 20 - 2000)

DTIM Period (Range: 1-255)

Fragmentation Threshold (Range: 256-2346, even numbers only)

RTS Threshold (Range: 0-2347)

Maximum Stations (Range: 0-2007)

Transmit Power (Percent)

| | Rate | Supported | Basic |
|-----------|---------|-------------------------------------|-------------------------------------|
| | 54 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 48 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 36 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Rate Sets | 24 Mbps | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| | 18 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 12 Mbps | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| | 9 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 6 Mbps | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Figure 45. Radio One Page

2. Configure the following settings as necessary:

Radio

Choose radio one or radio two. Be sure to configure settings for both radios.

Status (On/Off)

Specify whether you want the radio on or off by clicking **On** or **Off**.

Mode

The Mode defines the Physical Layer (PHY) standard being used by the radio.

Note

With a two-radio access point, different modes may be available depending on whether radio one or radio two is selected in the Radio field above.

Atheros Turbo 5 GHz is IEEE 802.11a Turbo mode.

Atheros Turbo 2.4 GHz is IEEE 802.11g Turbo mode.

Super AG

Enabling Super AG provides better performance by increasing radio throughput for a radio mode (IEEE 802.11b, g, a, and so on). Keep in mind that, with Super AG enabled, the access point transmissions will consume more bandwidth. To enable Super AG click **Enabled**. To disable Super AG click **Disabled**.

Channel

The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface.

For most Modes, the default is Auto. Auto is the recommended mode because it automatically detects the best channel choices based on signal strength, traffic loads, and so on.

Channels operate in a specific frequency range. The available frequencies depend upon the country, as shown in Table 5.

Table 5. Worldwide Frequencies for 802.11g and 802.11b Radios

| Channel | FCC | ETSI | France | Japan | Israel |
|---------|----------------|----------------|--------|----------------|----------------|
| 1 | 2412 | 2412 | | 2412 | |
| 2 | 2417 | 2417 | | 2417 | |
| 3 | 2422 (default) | 2422 (default) | | 2422 (default) | 2422 (default) |
| 4 | 2427 | 2427 | | 2427 | |
| 5 | 2432 | 2432 | | 2432 | |
| 6 | 2437 | 2437 | | 2437 | |
| 7 | 2442 | 2442 | | 2442 | |
| 8 | 2447 | 2447 | | 2447 | |

Table 5. Worldwide Frequencies for 802.11g and 802.11b Radios

| Channel | FCC | ETSI | France | Japan | Israel |
|---------|------|------|----------------|-------|--------|
| 9 | 2452 | 2452 | | 2452 | |
| 10 | 2457 | 2457 | 2457 | 2457 | |
| 11 | 2462 | 2462 | 2462 (default) | 2462 | |
| 12 | | 2467 | 2467 | 2467 | |
| 13 | | 2472 | 2472 | 2472 | |
| 14 | | | | 2484 | |

The 802.11g and 802.11b channels that are allowed in a given country may change without notice. Be sure you use only those frequencies that are permissible in the given country. Note the following:

- FCC countries include the United States, Canada, China, Taiwan, India, Thailand, Indonesia, Malaysia, Hong Kong, and most South American countries.
- ETSI countries include all European Union countries except France. It also includes Switzerland, Iceland, Norway, Czech Republic, Slovenia, Slovakia, Turkey, Russia, and the United Arab Emirates.
- France, Mexico, and Singapore use the same channels.

Beacon Interval

Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).

The Beacon Interval value is set in milliseconds. Enter a value from 20 to 2000.

DTIM Period

The Delivery Traffic Information Map (DTIM) message is an element included in some beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pick-up.

The DTIM period you specify here indicates how often the clients served by this access point should check for buffered data still on the access point awaiting pickup.

Specify a DTIM period within the range (1 - 255).

The measurement is in beacons. For example, if you set this to 1, clients check for buffered data on the access point at every beacon. If

you set this to 2, clients check on every other beacon. If you set this to 10, clients check on every 10th beacon.

Fragmentation Threshold

Specify a number between 256 and 2,346 to set the frame size threshold in bytes.

The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function is activated and the packet is sent as multiple 802.11 frames.

If the packet being transmitted is equal to or less than the threshold, fragmentation is not used.

Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation.

Fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help improve network performance and reliability if properly configured.

Sending smaller frames (by using lower fragmentation threshold) may help with some interference problems; for example, with microwave ovens.

By default, fragmentation is off. Allied Telesyn recommends not using fragmentation unless you suspect radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput.

RTS Threshold

Specify an RTS threshold value between 0 and 2347.

The RTS threshold specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, especially one with a lot of clients.

If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet.

On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.

Maximum Stations

Specify the maximum number of stations allowed to access this access point at any one time.

You can enter a value between 0 and 2007.

Transmit Power

Provide a percentage value to set the transmit power for this access point.

The default is to have the access point transmit using 100 percent of its power.

- ❑ In most situations, Allied Telesyn recommends keeping the default and having the transmit power set to 100 percent. This is more cost-efficient because it gives the access point a maximum broadcast range and reduces the number of access points needed.
- ❑ To increase capacity of the network, place access points closer together and reduce the value of the transmit power. This setup helps reduce overlap and interference among access points. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.

Preamble (This setting applies only to radio two)

Rate Sets

Radio one and radio two have different rate sets. See “Configuring the Rate Sets” on page 152 for information.

3. Click **Update** to save your settings.

Configuring the Rate Sets

Why do the different radios have different rate sets???

Rate sets specify the transmission rate sets you want the access point to support and the basic rate sets you want the access point to advertise.

Rates are expressed in megabits per second.

- ❑ Supported Rate Sets indicate rates that the access point supports. You can check multiple rates (click a checkbox to select or de-select a rate). The access point will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the access point.
- ❑ Basic Rate Sets indicate rates that the access point will advertise to the network for the purposes of setting up communication with other access points and client stations on the network. It is generally more efficient to have an access point broadcast a subset of its supported rate sets.

Figure 46 shows the rate sets for radio one.

| | <u>Rate</u> | <u>Supported</u> | <u>Basic</u> |
|------------------|-------------|-------------------------------------|-------------------------------------|
| | 54 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 48 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 36 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Rate Sets | 24 Mbps | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| | 18 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 12 Mbps | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| | 9 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 6 Mbps | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Figure 46. Radio One Rate Sets

Figure 47 shows the rate sets for radio two.

| | <u>Rate</u> | <u>Supported</u> | <u>Basic</u> |
|------------------|-------------|-------------------------------------|-------------------------------------|
| | 54 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 48 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 36 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 24 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 18 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Rate Sets | 12 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 11 Mbps | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| | 9 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 6 Mbps | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| | 5.5 Mbps | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| | 2 Mbps | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| | 1 Mbps | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Figure 47. Radio Two Rate Sets

To configure the rate sets, perform the following procedure:

1. From the main menu, select **Advanced > Radio**.

The Radio page for radio one is shown in Figure 45 on page 147. Figure 46 on page 152 shows the rate sets for radio one, and Figure 47 on page 152 shows the rate sets for radio two.

2. Make your radio rate set choices
3. Click **Update** to save your settings.

Chapter 14

Load Balancing

The AT-WA7400 Management Software allows you to balance the distribution of wireless client connections across multiple access points. Using load balancing, you can prevent scenarios where a single access point in your network shows performance degradation because it is handling a disproportionate share of the wireless traffic.

The following sections describe how to configure Load Balancing on your wireless network:

- “Understanding Load Balancing” on page 156
- “Configuring Load Balancing” on page 157

Understanding Load Balancing

Like most configuration settings on the AT-WA7400 Wireless Access Point, load balancing settings are shared among clustered access points.

Note

In some cases you might want to set limits for only one access point that is consistently over-utilized. You can apply unique settings to a particular access point if it is operating in standalone mode. (See “Understanding Clustering” on page 44 and “Understanding and Changing Access Point Settings” on page 48.)

Identifying the Imbalance: Overworked or Under-utilized Access Points

A comparison of session monitoring data for multiple access points allows you to identify an access point that is consistently handling a disproportionately large percentage of wireless traffic. This can happen when location placement or other factors causes one access point to transmit the strongest signal to a majority of clients on a network. By default, that access point will receive most of client requests while the other access points stay idle much of the time.

Imbalances in distribution of wireless traffic across access points will be evident in session monitoring statistics, which will show higher utilization rates on overworked access points and conversely, higher idle times on under-utilized access points. An access point that is handling more than its fair share of traffic might also show slower data rates or lower transmit/receive rates due to the overload.

Specifying Limits for Utilization and Client Associations

You can correct for imbalances in network access point utilization by enabling load balancing and setting limits on utilization rates and number of client associations allowed per access point.

Load Balancing and QoS

Load balancing also plays a part in contributing to Quality of Service (QoS) for *Voice Over IP* (VoIP) and other such time-sensitive applications competing for bandwidth and timely access to the air waves on a wireless network. For more information about configuring your network for QoS, see Chapter 15, “Configuring Quality of Service (QoS)” on page 161.

Configuring Load Balancing

To configure load balancing, you enable load balancing and set limits and behavior to be triggered by a specified utilization rate of the access point.

Note

To view the current Utilization Rates for access points, click Cluster > Sessions on the web pages. (See Chapter 5, "Session Monitoring" on page 65.)

Even when clients are disassociated from an access point, the network still provides continuous service to client stations if another access point is within range so that clients can re-connect to the network. Clients should automatically retry the access point they were originally connected to and other access points on the subnet. Clients who are disassociated from one access point should experience a seamless transition to another access point on the same subnet.

Load Balancing settings apply to the access point load as a whole. When guest access is enabled, the settings apply to both internal and guest networks together.

On a two-radio access point, Load Balancing settings apply to both radios but the load of each radio is calculated independently and includes both the internal and guest network (when guest access is enabled).

To configure load balancing, perform the following procedure:

1. From the main menu, select **Advanced > Load Balancing**.

The Load Balancing page is shown in Figure 48.

Modify load balancing settings

Load Balancing Enabled Disabled

Utilization for No New Associations (Percent, 0 disables)

Utilization for Disassociation (Percent, 0 disables)

Station Threshold for Disassociation (Range: 1-2007, 0 disables)

Update

Figure 48. Load Balancing Page

- Configure the following settings as required:

Load Balancing

To enable load balancing on this access point, click **Enable**. To disable load balancing on this access point, click **Disable**.

Utilization for No New Associations

Utilization rate limits relate to wireless bandwidth utilization.

Provide a bandwidth utilization rate percentage limit for this access point to indicate when to stop accepting new client associations.

When the utilization rate for this access point exceeds the specified limit, no new client associations are allowed on this access point.

If you specify 0 in this field, all new associations are allowed regardless of the utilization rate.

Utilization for Disassociation

Utilization rate limits relate to wireless bandwidth utilization.

Provide a bandwidth utilization rate percentage limit for this access point to indicate when to disassociate current clients.

When the utilization rate exceeds the specified limit, a client currently associated with this access point is disconnected.

If you specify 0 in this field, current clients are never disconnected regardless of the utilization rate.

Stations Threshold for Disassociation

Specify the number of client stations you want as a stations threshold

for disassociation. If the number of client stations associated with the access point at any one time is equal to or less than the number you specify here, no stations will be disassociated regardless of the "Utilization for Disassociation" value.

Theoretically, the maximum number of client stations allowed is 2007.

Allied Telesyn recommends setting the maximum to between 30 and 50 client stations. This allows for a workable load on the access point, given that bandwidth is shared among the access point clients.

Chapter 15

Configuring Quality of Service (QoS)

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like Voice-over-IP (VoIP), other types of audio, video, and streaming media as well as traditional IP data over the AT-WA7400 Wireless Access Point.

The following sections describe how to configure Quality of Service queues using the AT-WA7400 Management Software:

- “Understanding QoS” on page 162
- “Configuring QoS Queues” on page 167

Understanding QoS

A primary factor that affects QoS is network congestion due to an increased number of clients attempting to access the air waves and higher traffic volume competing for bandwidth during a busy time of day. The most noticeable degradation in service on a busy, overloaded network will be evident in time-sensitive applications such as video, Voice-over-IP (VoIP), and streaming media.

Unlike typical data files which are less affected by variability in QoS, video, VoIP and streaming media must be sent in a specific order at a consistent rate and with minimum delay between packet transmission. If the quality of service is compromised, the audio or video will be distorted.

QoS and Load Balancing

By using a combination of load balancing (see Chapter 14, “Load Balancing” on page 155) and QoS techniques, you can provide a high quality of service for time-sensitive applications even on a busy network. Load balancing is a way of better distributing the traffic volume across access points. QoS is a means of allocating bandwidth and network access based on transmission priorities for different types of wireless traffic within a single access point.

802.11e and WMM Standards Support

QoS describes a range of technologies for controlling data streams on shared network connections. The IEEE 802.11e task group is in the process of defining a QoS standard for transmission quality and availability of service on wireless networks. QoS is designed to provide better network service by minimizing network congestion; limiting jitter, latency, and packet loss; supporting dedicated bandwidth for time-sensitive or mission critical applications, and prioritizing wireless traffic for channel access.

As with all IEEE 802.11 working group standards, the goal is to provide a standard way of implementing QoS features so that components from different companies are interoperable.

The AT-WA7400 Management Software provides QoS based on the wireless multimedia (WMM) specification and wireless multimedia (WMM) standards, which are implementations of a subset of 802.11e features.

Both access points and wireless clients (laptops, consumer electronics products, and so forth) can be WMM-enabled.

QoS Queues and Parameters to Coordinate Traffic Flow

Configuring QoS options on the AT-WA7400 Wireless Access Point consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for voice, video, multimedia, and mission

critical applications, and rely on best-effort parameters for traditional IP data.

For example, time-sensitive voice, video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

The AT-WA7400 Management Software implements QoS based on the IEEE wireless multimedia (WMM) standard. A Linux-based queuing class is used to tag packets and establish multiple queues. The queues provided offer built-in prioritization and routing based on the type of data being transmitted.

AT-WA7400 Management Software provides a way for you to configure parameters on the queues.

QoS Queues and Type of Service (ToS) on Packets

QoS on the AT-WA7400 Wireless Access Point leverages WMM information in the IP packet header related to Type of Service (ToS). Every IP packet sent over the network includes a ToS field in the header that indicates how the data should be prioritized and transmitted over the network. The ToS field consists of a 3 to 7 bit value with each bit representing a different aspect or degree of priority for this data as well as other meta-information (low delay, high throughput, high reliability, low cost, and so on).

For example, the ToS for FTP data packets is likely to be set for maximum throughput because the critical consideration for FTP is the ability to transmit relatively large amounts of data in one go. Interactive feedback is nice to have in this situation but certainly less critical. VoIP data packets are set for minimum delay because that is a critical factor in quality and performance for that type of data.

The access point examines the ToS field in the headers of all packets that pass through the access point. Based on the value in a packet's ToS field, the access point prioritizes the packet for transmission by assigning it to one of the queues. This process occurs automatically, regardless of whether you deliberately configure QoS or not.

A different type of data is associated with each queue. The queue and associated priorities and parameters for transmission are as follows:

- ❑ Data 0 (Voice). Highest priority queue, minimum delay. Time-sensitive data such as Voice over IP (VoIP) is automatically sent to this queue.
- ❑ Data 1 (Video). High priority queue, minimum delay. Time-sensitive data such as Video and other streaming media are automatically sent to this queue.

- ❑ Data 2 (Best Effort). Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- ❑ Data 3 (Background). Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

Packets in a higher priority queue will be transmitted before packets in a lower priority queue. Interactive data in the queues labeled Data 0 and Data 1 is always sent first, best effort data in Data 2 is sent next, and Background (bulk) data in Data 3 is sent last. Each lower priority queue (class of traffic) gets bandwidth that is left over after the higher classes of traffic have been sent. At an extreme end if you have enough interactive data to keep the access point busy all the time, low priority traffic would never get sent.

Using the QoS settings on the web UI, you can configure *Enhanced Distributed Channel Access* (EDCA) parameters that determine how each queue is treated when it is sent by the access point to the client or by the client to the access point.

Note

Wireless traffic travels:

- Downstream from the access point to the client station
- Upstream from client station to access point
- Upstream from access point to network
- Downstream from network to access point

With WMM enabled, QoS settings on the AT-WA7400 Wireless Access Point affect the first two of these; *downstream* traffic flowing from the access point to client station (AP EDCA parameters) and the *upstream* traffic flowing from the station to the access point (station EDCA parameters).

With WMM disabled, you can still set some parameters on the downstream traffic flowing from the access point to the client station (AP EDCA parameters).

The other phases of the traffic flow (to and from the network) are not under control of the QoS settings on the access point.

EDCF Control of Data Frames and Arbitration Interframe Spaces

Data is transmitted over 802.11 wireless networks in frames. A frame consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network.

Note

A frame is similar in concept to a *packet*. The difference is that a packet operates on the network layer (layer 3 in the OSI model) whereas a frame operates on the data-link layer (layer 2 in the OSI model).

Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection.

The 802.11 standard defines various frame types for management and control of the wireless infrastructure, and for data transmission. The 802.11 frame types are (1) management frames, (2) control frames, and (3) data frames. Management and control frames (which manage and control the availability of the wireless infrastructure) automatically have higher priority for transmission.

802.11e uses interframe spaces to regulate which frames get access to available channels and to coordinate wait times for transmission of different types of data.

Management and control frames wait a minimum amount of time for transmission; they wait a short interframe space (SIF). These wait times are built-in to 802.11 as infrastructure support and are not configurable.

The AT-WA7400 Management Software supports the Enhanced Distribution Coordination Function (EDCF) as defined by the 802.11e standard. EDCF, which is an enhancement to the DCF standard and is based on CSMA/CA protocol, defines the interframe space (IFS) between data frames. Data frames wait for an amount of time defined as the arbitration interframe space (AIFs) before transmitting.

This parameter is configurable.

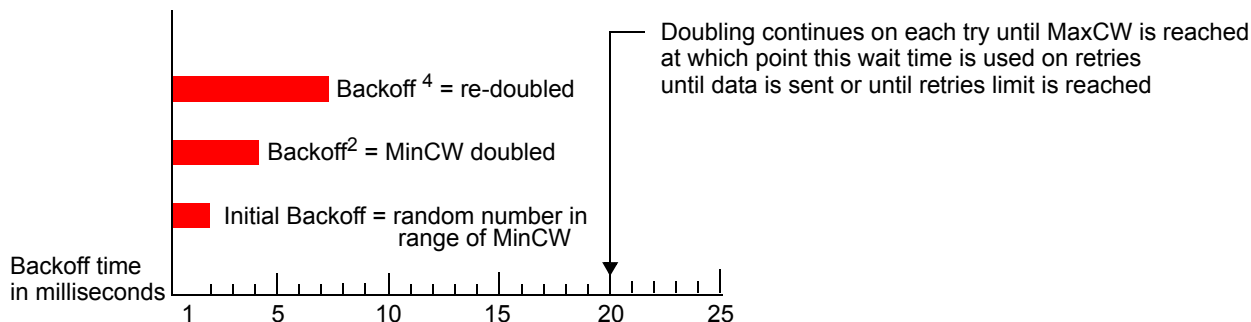
(Note that sending data frames in AIFs allows higher priority management and control frames to be sent in SIFs first.)

The AIFs ensures that multiple access points do not try sending data at the same time but instead wait until a channel is free.

Random Backoff and Minimum / Maximum Contention Windows

If an access point detects that the medium is in use (busy), it uses the DCF *random backoff* timer to determine the amount of time to wait before attempting to access a given channel again. Each access point waits some random period of time between retries. The wait time (initially a random value within a range specified as the Minimum Contention Window) increases exponentially up to a specified limit (Maximum Contention Window). The random delay avoids most of the collisions that

would occur if multiple access points got access to the medium at the same time and tried to transmit data simultaneously. The more active users you have on a network, the more significant the performance gains of the backoff timer will be in reducing the number of collisions and retransmissions.



The random backoff used by the access point is a configurable parameter. To describe the random delay, a Minimum Contention Window (MinCW) and a Maximum Contention Window (MaxCW) is defined.

- ❑ The value specified for the Minimum Contention Window is the upper limit of a range for the initial random backoff wait time. The number used in the random backoff is initially a random number between 0 and the number defined for the Minimum Contention Window.
- ❑ If the first random backoff time ends before successful transmission of the data frame, the access point increments a retry counter, and doubles the value of the random backoff window. The value specified in the Maximum Contention Window is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

Packet Bursting for Better Performance

The AT-WA7400 Management Software includes 802.11e based packet bursting technology that increases data throughput and speed of transmission over the wireless network. Packet bursting enables the transmission of multiple packets without the extra overhead of header information. The effect of this is to increase network speed and data throughput. The size of packet bursts allowed (maximum burst length) is a configurable parameter.

Transmission Opportunity (TXOP) Interval for Client Stations

The Transmission Opportunity (TXOP) is an interval of time when a Wi-Fi Multimedia (WMM) client station has the right to initiate transmissions onto the wireless medium (WM).

Configuring QoS Queues

Configuring Quality of Service (QoS) on the AT-WA7400 Wireless Access Point consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (via Contention Windows) for transmission. The settings described here apply to data transmission behavior on the access point only, not to that of the client stations.

Note

For the guest interface, QoS queue settings apply to the access point load as a whole (both BSSes together).

On a two-radio access point these settings apply to both radios but the traffic for each radio is queued independently. (The exception to this is guest traffic as noted below.)

Internal and guest network traffic is always queued together within each radio. This is the case on both one-radio and two-radio access points.

QoS on the access point leverages existing information in the IP packet header related to Type of Service (ToS). The access point examines the ToS field in the headers of all packets that pass through the access point. Based on the value in a packet's ToS field, the access point prioritizes the packet for transmission by assigning it to one of the queues. A different type of data is associated with each queue. You can configure parameters that determine how each queue is treated when it is sent by the access point.

To configure QoS, perform the following procedure:

1. From the main menu, select **Advanced > Quality of Service**.

The Quality of Service page is shown in Figure 49.

Modify QoS queue parameters

| Queue | AIFS | cwMin | cwMax | Max. Burst |
|--------------------------------|------|-------|-------|------------|
| Data 0 (Voice) | 1 | 3 | 7 | 1.5 |
| Data 1 (Video) | 1 | 7 | 15 | 3.0 |
| Data 2 (Best Effort) | 3 | 15 | 63 | 0 |
| Data 3 (Background) | 7 | 15 | 1023 | 0 |

AP EDCA parameters

Wi-Fi Multimedia (WMM) Enabled Disabled

| Queue | AIFS | cwMin | cwMax | TXOP Limit |
|--------------------------------|------|-------|-------|------------|
| Data 0 (Voice) | 2 | 3 | 7 | 47 |
| Data 1 (Video) | 2 | 7 | 15 | 94 |
| Data 2 (Best Effort) | 3 | 15 | 1023 | 0 |
| Data 3 (Background) | 7 | 15 | 1023 | 0 |

Station EDCA parameters

Figure 49. Quality of Service Page

The Quality of Service page has three sections:

- AP EDCA parameters
- Wi-Fi Multimedia (WMM)
- Station EDCA Parameters

The following procedures describe how to configure the parameters in these sections.

Configuring AP EDCA Parameters

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station. To configure these parameters, perform the following procedure:

1. In the AP EDCA parameters section of the Quality of Service page, configure the following parameters:

Queue

Queues are defined for different types of data transmitted from access point-to-station:

Data 0 (Voice) - High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.

Data 1 (Video) - High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.

Data 2 (best effort) - Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.

Data 3 (Background) - Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

For more information, see “QoS Queues and Parameters to Coordinate Traffic Flow” on page 162.

AIFs

(Inter-Frame Space)

The Arbitration Inter-Frame Spacing (AIFs) specifies a wait time (in milliseconds) for *data frames*.

Valid values for AIFs are 1 through 255.

For more information, see “EDCF Control of Data Frames and Arbitration Interframe Spaces” on page 164.

cwMin

(Minimum Contention Window)

This parameter is input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.

The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.

The first random number generated will be a number between 0 and the number specified here.

If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window.

Valid values for the `cwmin` are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for `cwmin` must be lower than the value for `cwmax`.

For more information, see “Random Backoff and Minimum / Maximum Contention Windows” on page 165.

cwMax

(Maximum Contention Window)

The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

When the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached.

Valid values for the `cwmax` are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for `cwmax` must be higher than the value for `cwmín`.

For more information, see “Random Backoff and Minimum / Maximum Contention Windows” on page 165.

Max. Burst Length

AP EDCA Parameter Only (The Max. Burst Length applies only to traffic flowing from the access point to the client station.)

This value specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A *packet burst* is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.

Valid values for maximum burst length are 0.0 through 999.9.

For more information, see “Packet Bursting for Better Performance” on page 166.

2. Click **Update** to save the settings.

Enabling/ Disabling Wi-Fi Multimedia

By default, Wi-Fi MultiMedia (WMM) is enabled on the access point. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the AT-WA7400 Wireless Access Point control downstream traffic flowing from the access point to client station (AP EDCA parameters) and the upstream traffic flowing from the station to the access point (station EDCA parameters).

Disabling WMM deactivates QoS control of station EDCA parameters on upstream traffic flowing from the station to the access point

With WMM disabled, you can still set some parameters on the downstream traffic flowing from the access point to the client station (AP EDCA parameters).

- To disable WMM extensions, click **Disabled**.
- To enable WMM extensions, click **Enabled**.

Configuring Station EDCA Parameters

Station Enhanced Distributed Channel Access (EDCA) parameters affect traffic flowing from the client station to the access point. To configure the EDCA parameters, perform the following procedure:

1. In the Station EDCA parameters section of the Quality of Service page, configure the following parameters:

Queue

Queues are defined for different types of data transmitted from station-to-access point:

Data 0 (Voice) - Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.

Data 1 (Video) - Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.

Data 2 (best effort) - Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.

Data 3 (Background) - Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

For more information, see “QoS Queues and Parameters to Coordinate Traffic Flow” on page 162.

AIFs

(Inter-Frame Space)

The Arbitration Inter-Frame Spacing (AIFs) specifies a wait time (in milliseconds) for *data frames*.

For more information, see “EDCF Control of Data Frames and Arbitration Interframe Spaces” on page 164.

cwMin

(Minimum Contention Window)

This parameter is input to the algorithm that determines the initial random backoff wait time (“window”) for retry of a transmission.

The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.

The first random number generated will be a number between 0 and the number specified here.

If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling continues until the size of the random

backoff value reaches the number defined in the Maximum Contention Window.

For more information, see “Random Backoff and Minimum / Maximum Contention Windows” on page 165.

cwMax

(Maximum Contention Window)

The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached.

For more information, see “Random Backoff and Minimum / Maximum Contention Windows” on page 165.

TXOP Limit

Station EDCA Parameter Only (The TXOP Limit applies only to traffic flowing from the client station to the access point.)

The Transmission Opportunity (TXOP) is an interval of time when a WME client station has the right to initiate transmissions onto the wireless medium (WM).

This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.

2. Click **Update** to save the settings.

Chapter 16

Configuring the Wireless Distribution System (WDS)

The AT-WA7400 Management Software lets you connect multiple access points using a wireless distribution system (WDS). WDS allows access points to communicate with one another wirelessly in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required.

The following sections describe how to configure the WDS using the AT-WA7400 Management Software:

- “Understanding the Wireless Distribution System” on page 174
- “Configuring WDS Settings” on page 178

Understanding the Wireless Distribution System

A wireless distribution system (WDS) is an 802.11f technology that wirelessly connects access points, known as Basic Service Sets (BSS), to form what is known as an Extended Service Set (ESS).

Note

A BSS generally equates to an access point (deployed as a single-access point wireless “network”), except in cases where multi-BSSID features make a single access point look like two or more access points to the network. In such cases, the access point has multiple unique BSSIDs.

Using WDS to Bridge Distant Wired LANs

In an ESS, a network of multiple access points, each access point serves part of an area which is too large for a single access point to cover. You can use WDS to bridge distant Ethernets to create a single LAN. For example, suppose you have one access point which is connected to the network by Ethernet and serving multiple client stations in the Conference Room (LAN Segment 1), and another Ethernet-wired access point serving stations in the West Wing offices (LAN Segment 2). You can bridge the Conference Room and West Wing access points with a WDS link to create a single network for clients in both areas, as shown in Figure 50.

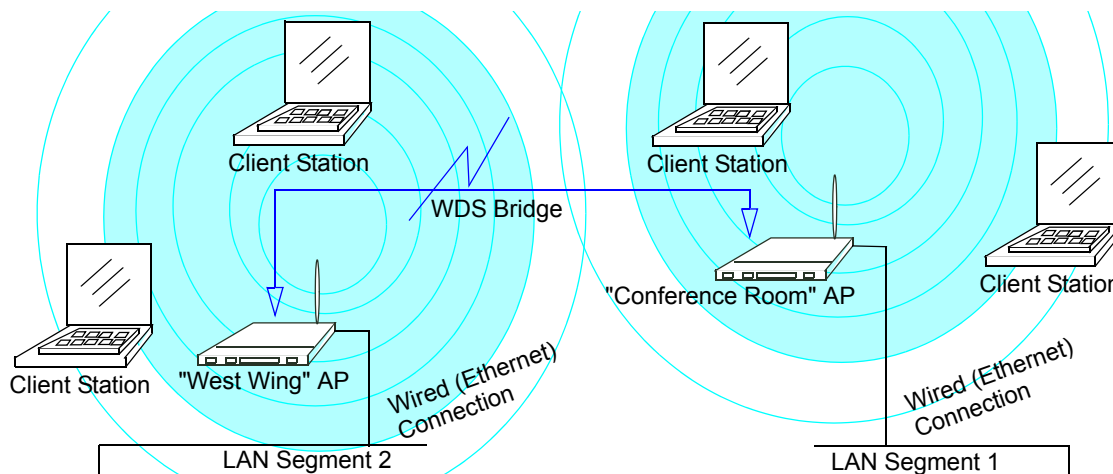


Figure 50. Example Wireless Network

Using WDS to Extend the Network Beyond the Wired Coverage Area

An ESS can extend the reach of the network into areas where cabling would be difficult, costly, or inefficient.

For example, suppose you have an access point which is connected to the network by Ethernet and serving multiple client stations in one area (East Wing in the example) but cannot reach others which are out of range. Suppose also that it is too difficult or too costly to wire the distant area with

Ethernet cabling. You can solve this problem by placing a second access point closer to second group of stations (Poolside in the example) and bridge the two access points with a WDS link. This *extends* your network wirelessly by providing an extra hop to get to distant stations, as shown in Figure 51.

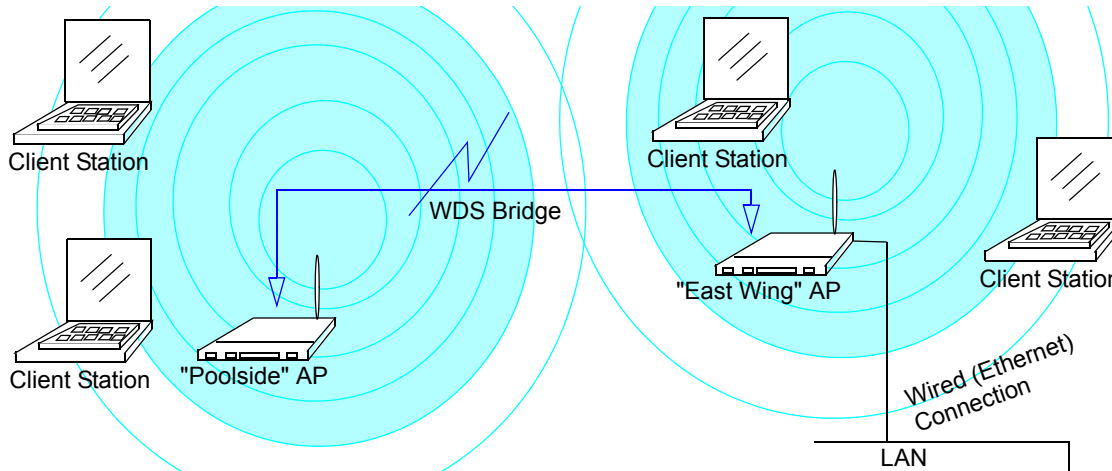


Figure 51. WDS Bridge

Backup Links and Unwanted Loops in WDS Bridges

Another use for WDS bridging, the creation of backup links, is not supported in this release of the AT-WA7400 Management Software. The topic is included here to emphasize that you should not try to use WDS in this way; backup links will result in unwanted, endless loops of data traffic

If an access point provides Spanning Tree Protocol (STP), WDS can be used to configure backup paths between access points across the network. For example, between two access points you could have both a primary path via Ethernet and a secondary (backup) wireless path via a WDS link. If the Ethernet connection goes down, STP would reconfigure its map of the network and effectively fix the down network segment by activating the backup wireless path.

In this release, the AT-WA7400 Management Software does not provide STP. Without STP, it is possible that both connections (paths) may be active at the same time, and result in an endless loop of traffic on the LAN.

Therefore, be sure not create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges.

For more information, see "WDS Guidelines" on page 176.

Security Considerations Related to WDS Bridges

Static Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. Both access points in a given WDS link must be configured with the same security settings. For static WEP, either a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key is specified for data encryption.

You can enable Static WEP on the WDS link (bridge). When WEP is enabled, all data exchanged between the two access points in a WDS link is encrypted using a fixed WEP key that you provide.

Static WEP is the only security mode available for the WDS link, and it does not provide effective data protection to the level of other security modes available for service to client stations. If you use WDS on a LAN intended for secure wireless traffic you are putting your network at risk. Therefore, Allied Telesyn recommends using WDS to bridge the guest network only for this release. Do not use WDS to bridge access points on the internal network unless you are not concerned about the security risk for data traffic on that network.

For more information about the effectiveness of different security modes, see Appendix B, “Configuring Security on Wireless Clients” on page 217. This topic also covers use of plain text security mode for access point-to-station traffic on the guest network, which is intended for less sensitive data traffic.

WDS Guidelines

The following list summarizes some critical guidelines regarding WDS configuration:

- ❑ The only security mode available on the WDS link is Static WEP, which is not very secure. Therefore, Allied Telesyn recommends that you use WDS to bridge the guest network only for this release. Do not use WDS to bridge access points on the internal network unless you are not concerned about the security risk for data traffic on that network.
- ❑ When using WDS, be sure to configure WDS settings on *both* access points participating in the WDS link.
- ❑ You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.
- ❑ Both access points participating in a WDS link must be on the same radio channel and using the same IEEE 802.11 mode. (See “Configuring Radio Settings” on page 147 for information on configuring the Radio mode and channel.)
- ❑ **Do not create loops** with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. Spanning Tree Protocol (STP), which manages path redundancy and prevent unwanted loops, is not enabled for this release.

Keep these rules in mind when working with WDS in this release of the AT-WA7400 Management Software:

- ❑ Any two access points can be connected by only a single path; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both.
- ❑ Do not create backup links.

- ❑ If you can trace more than one path between any pair of access points going through any combination of Ethernet or WDS links, you have a loop.
- ❑ You can only extend or bridge either the internal or guest network but not both.

Configuring WDS Settings

You must configure the WDS settings for each access point intended to receive hands-off and send information from the sending access point.

To configure WDS on an AT-WA7400 Access Point, perform the following procedure:

1. From the main menu, select **Advanced > Wireless Distribution System**.

The Wireless Distribution System page is shown in Figure 52 on page 179.

Note

Figure 52 shows the WDS settings page for the two-radio access point. The web page for the one-radio access point will look slightly different.

Configure WDS bridges to other access points

Radio

Local Address

Remote Address

Bridge with

WEP Enabled Disabled

Key Length 64 bits 128 bits 152 bits

Key Type ASCII Hex

Characters Required

WEP Key

Radio

Local Address

Remote Address

Bridge with

WEP Enabled Disabled

Key Length 64 bits 128 bits 152 bits

Key Type ASCII Hex

Characters Required

WEP Key

Radio

Local Address

Remote Address

Bridge with

WEP Enabled Disabled

Key Length 64 bits 128 bits 152 bits

Key Type ASCII Hex

Characters Required

WEP Key

Radio

Local Address

Remote Address

Bridge with

WEP Enabled Disabled

Key Length 64 bits 128 bits 152 bits

Key Type ASCII Hex

Characters Required

WEP Key

Figure 52. Wireless Distribution System Page

2. Configure the following settings as necessary:

Radio

For each WDS link, select Radio One or Radio Two. The rest of the settings for the link apply to the radio selected in this field. The read-only “Local Address” changes depending on which radio you select here.

Local Address

Indicates the media access control (MAC) addresses for this access point.

A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point or interface.

For each WDS link, the Local Address reflects the MAC address for the internal interface on the selected radio (Radio one on WLAN0 or radio two WLAN1).

Remote Address

Specify the MAC address of the destination access point; that is, the access point to which data will be sent or “handed-off” and from which data will be received.

Bridge with

The AT-WA7400 Management Software provides the capability of setting up guest and internal networks on the same access point. (See Chapter 11, “Setting Up Guest Access” on page 133.)

The guest network typically provides Internet access but isolates guest clients from more sensitive areas of your internal network. It is common to have security disabled on the guest network to provide open access.

Alternatively, the internal network provides full access to protected information behind a firewall and requires secure logins or certificates for access.

When you use WDS to link up one access point to another, you need to identify within which of these networks you want the data exchange to occur.

Specify the network to which you want to bridge this access point:

- Internal Network
- Guest Network

WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. Both access points on the WDS link must be configured with the same security settings. For static WEP, a static

64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

Specify whether you want Wired Equivalent Privacy (WEP) encryption enabled for the WDS link.

- Enabled
- Disabled

Key Length

If WEP is enabled, specify the length of the WEP key:

- 64 bits
- 128 bits

Key Type

If WEP is enabled, specify the WEP key type:

- ASCII
- Hex

Characters Required

Indicates the number of characters required in the WEP key.

The number of characters required updates automatically based on how you set Key Length and Key Type.

WEP Key

Enter a string of characters. If you selected ASCII, enter any combination of 0–9, a–z, and A–Z. If you selected HEX, enter hexadecimal digits (any combination of 0–9 and a–f or A–F). These are the RC4 encryption keys shared with the stations using the access point.

3. Click **Update** to save your settings.

Example of Configuring a WDS Link

When you use WDS, be sure to configure WDS settings on both access points on the WDS link.

For example, to create a WDS link between a pair of access points named **MyAP1** and **MyAP2** do the following:

1. Open the web pages for MyAP1, by entering the IP address for MyAP1 as a URL in the web browser address bar in the following form:

`http://IPAddressOfAccessPoint`

where *IPAddressOfAccessPoint* is the address of MyAP1.

2. Go to the Wireless Distribution System page on the MyAP1 web pages.

The MAC address for MyAP1 (the access point you are currently viewing) are displayed as the Local Address at the top of the page.

3. Configure a WDS interface for data exchange with MyAP2.

Start by entering the MAC address for MyAP2 as the Remote Address and fill in the rest of the fields to specify the network (guest or internal), security, and so on. Save the settings (click Update).

4. Navigate to the radio settings on the web pages (Advanced > Radio) to verify or set the mode and the radio channel on which you want MyAP1 to broadcast.

Remember that the two access points participating in the link, MyAP1 and MyAP2, must be set to the same Mode and be transmitting on the same channel.

For our example, if you use IEEE 802.11b Mode and broadcasting on Channel 6, you would choose Mode and Channel from the lists on the Radio page.)

5. Now repeat the same steps for MyAP2:

- Open the web pages for MyAP2 by using MyAP2's IP address in a URL.
- Navigate to the WDS page in the MyAP2 web pages. (MyAP2's MAC address will show as the Local Address.)
- Configure a WDS interface for data exchange with MyAP1, starting with the MAC address for MyAP1.
- Navigate to the radio settings for MyAP2 to verify that it is using the same mode and broadcasting on the same channel as MyAP1. (For our example Mode is 802.11b and the channel is 6.)

6. Be sure to save the settings by clicking **Update**.

Chapter 17

Maintenance and Monitoring

The maintenance and monitoring tasks described here all pertain to viewing and modifying settings on specific access points; *not* on a cluster configuration that is automatically shared by multiple access points. Therefore, it is important to ensure that you are accessing the management software web pages for the particular access point you want to configure. For information on this, see Chapter 3, “Managing Access Points and Clusters” on page 43.

This chapter contains the following sections:

- ❑ “Monitoring Wired and Wireless LAN Settings” on page 184
- ❑ “Viewing the Event Logs” on page 186
- ❑ “Viewing the Transmit/Receive Statistics” on page 190
- ❑ “Viewing the Associated Wireless Clients” on page 192
- ❑ “Viewing the Status of Neighboring Access Points” on page 193
- ❑ “Viewing System Information” on page 197
- ❑ “Setting the Administrator Password” on page 199
- ❑ “Enabling the Network Time Protocol (NTP) Server” on page 202
- ❑ “Setting the HTTP Timeout” on page 204
- ❑ “Rebooting the Access Point” on page 205
- ❑ “Resetting the Configuration to Factory Defaults” on page 206
- ❑ “Upgrading the Firmware” on page 207
- ❑ “SNMP Firmware Upgrade” on page 209

Monitoring Wired and Wireless LAN Settings

To monitor wired LAN and wireless LAN (WLAN) settings, perform the following procedure:

1. From the main menu, select **Status > Interfaces**.

The Interfaces page is shown in Figure 53.

Note

On a two-radio access point, current wireless settings for both radio one and radio two are shown. On a one-radio access point, settings are shown for one radio. The Interfaces page for a two-radio access point is shown in Figure 53.

View settings for network interfaces

Wired Settings (Configure)

Internal Interface

MAC Address 00:0C:46:F2:D7:64

VLAN ID 20

IP Address 10.10.20.230

Subnet Mask 255.255.255.0

Guest Interface

MAC Address 00:0C:46:F2:D7:64

VLAN ID 30

Subnet 10.10.30.0

Wireless Settings (Configure)

Radio One

MAC Addresses 00:0C:46:F2:D7:64 / 00:0C:46:F2:D7:65

Mode IEEE 802.11a

Wireless Network Name (SSID) 10_1_1_2a

Channel 60 (5300 MHz)

Radio Two

MAC Addresses 00:0C:46:F2:D7:68 / 00:0C:46:F2:D7:69

Mode IEEE 802.11g

Wireless Network Name (SSID) 10_1_1_2g

Channel 11 (2462 MHz)

Figure 53. Interfaces Page

This page displays the current settings of the AT-WA7400 Wireless Access Point.

The wired settings show the Ethernet MAC address, IP address, subnet mask, and Associated Network Wireless Name (SSID) for the internal interface.

The guest Interface includes the MAC address, VLAN ID, and Associated Network Wireless Name (SSID).

2. To change these settings, click **Configure**, and the Advanced > Ethernet (Wired) Settings page is displayed.

The wireless settings for the Radio Interface settings include the radio mode and channel. Also shown here are MAC addresses (read-only) for internal and guest interfaces. (See Chapter 9, "Configuring the Wireless Settings" on page 97 and Chapter 13, "Configuring Radio Settings" on page 145 for more information.)

3. To change these settings, click **Configure**, and the Advanced > Wireless Settings page is displayed.

Viewing the Event Logs

To view system events and the kernel log for a particular access point, perform the following procedure:

1. From the main menu, select **Status > Events**.

The Events page is shown in Figure 54.

View events generated by this access point

Log Relay Host Enabled Disabled

Relay Host

Relay Port

Events Log

| Time | Severity | Service | Description |
|-----------------|----------|------------------|--|
| Jan 30 18:34:33 | info | mini_httpd [662] | (manager) login web server from:(149.35.8.54) success. |
| Jan 30 18:25:20 | info | mini_httpd [658] | (manager) logout web server from:(149.35.8.54) done. |
| Jan 30 18:14:21 | info | mini_httpd [554] | (manager) login web server from:(149.35.8.54) success. |
| Jan 30 18:13:00 | info | mini_httpd [550] | (manager) logout web server from:(149.35.8.54) done. |
| Jan 30 17:47:14 | info | mini_httpd [285] | (manager) login web server from:(149.35.8.54) success. |
| Jan 30 17:44:54 | debug | udhcpc | Sending select for 149.35.8.81... |
| Jan 30 17:44:54 | debug | udhcpc | Sending discover... |
| Jan 30 17:44:32 | info | udhcpc | udhcp client (v0.9.8-pre) started |

Figure 54. Events Page

This page lists the most recent events generated by this access point (see “Events Log” on page 188).

This page also gives you the option of enabling a remote log relay host to capture all system events and errors in a Kernel Log. (This requires setting up a remote relay host first. See “Log Relay Host for Kernel Messages” on page 187).

Note

The AT-WA7400 Wireless Access Point acquires its date and time information using the network time protocol (NTP). This data is reported in UTC format (also known as *Greenwich Mean Time*). You need to convert the reported time to your local time.

For information on setting the network time protocol, see Chapter 18, “Enabling the Network Time Protocol (NTP) Server” on page 202.

Log Relay Host for Kernel Messages

The kernel log is a comprehensive list of system events (shown in the system log) and kernel messages such as error conditions like dropping frames.

You cannot view kernel Log messages directly from the web pages for an access point. You must first set up a remote server running a syslog process and acting as a syslog log relay host on your network. Then, you can configure the AT-WA7400 Wireless Access Point to send its syslog messages to the remote server.

Using a remote server to collect access point syslog messages provides several benefits. You can:

- Aggregate syslog messages from multiple access points
- Store a longer history of messages than kept on a single access point
- Trigger scripted management operations and alerts

Setting Up the Log Relay Host

To use kernel log relaying, you must configure a remote server to receive the syslog messages. This procedure varies, depending on the type of machine you use as the remote log host. Following is an example of how to configure a remote Linux server using the syslog daemon.

The following steps activate the syslog daemon on a Linux server. Make sure you have root user identity for these tasks:

1. Log on as root to the machine you want to use as your syslog relay host.

The following operations require root user permissions. If you are not already logged on as root, type `su` at the command line prompt to become root (“super user”).

2. Edit `/etc/init.d/syslogd` and add “-r” to the variable `SYSLOGD` near the top of the file. The line you edit will look like this:

```
SYSLOGD="-r"
```

Consult the man pages to get more information on `syslogd` command options. (Type `man syslogd` at the command line.)

3. If you want to send all the messages to a file, edit `/etc/syslog.conf`.

For example you can add this line to send all messages to a log file called “AP_syslog”:

```
*.* -/tmp/AP_syslog
```

Consult the man pages to get more information on `syslog.conf` command options. (Type `man syslog.conf` at the command line.)

4. Restart the syslog server by typing the following at the command line prompt:

```
/etc/init.d/syslogd restart
```

Note

The syslog process will default to use port 514. Allied Telesyn recommends keeping this default port.

However; If you choose to reconfigure the log port, make sure that the port number you assign to syslog is not being used by another process.

Enabling or Disabling the Log Relay Host

To enable and configure the log relay host, perform the following procedure:

1. In the upper section of the **Status > Events** page, configure the following parameters:

Log Relay Host Enabled

To enable the Log Relay Host, click **Enable**. To disable it, click **Disabled**.

If you select Enabled, the Relay Host and Relay Port fields are editable.

Relay Host

Specify the IP address or DNS name of the Relay Host.

Relay Port

Specify the Port number for the syslog process on the Relay Host. The default port is 514.

2. To apply your changes, click **Update**.

If you enabled the Log Relay Host, clicking Update activates remote logging. The access point sends its kernel messages real-time for display to the remote log server monitor, a specified kernel log file, or other storage, depending on how you configured the Log Relay Host.

If you disabled the Log Relay Host, clicking Update disables remote logging.

Events Log

The events log shows system events on the access point such as stations associating, being authenticated, and other occurrences. The real-time

events log is always shown on the Status > Events page for the access point you are monitoring.

Viewing the Transmit/Receive Statistics

To view transmit/receive statistics for a particular access point, perform the following procedure:

1. From the main menu of the access point you want to monitor, select **Status > Transmit/Receive Statistics**.

Note

The following figure shows the Transmit / Receive page for a two-radio access point. The page for the one-radio access point will look slightly different.

The Transmit/Receive Statistics page is shown in Figure 55.

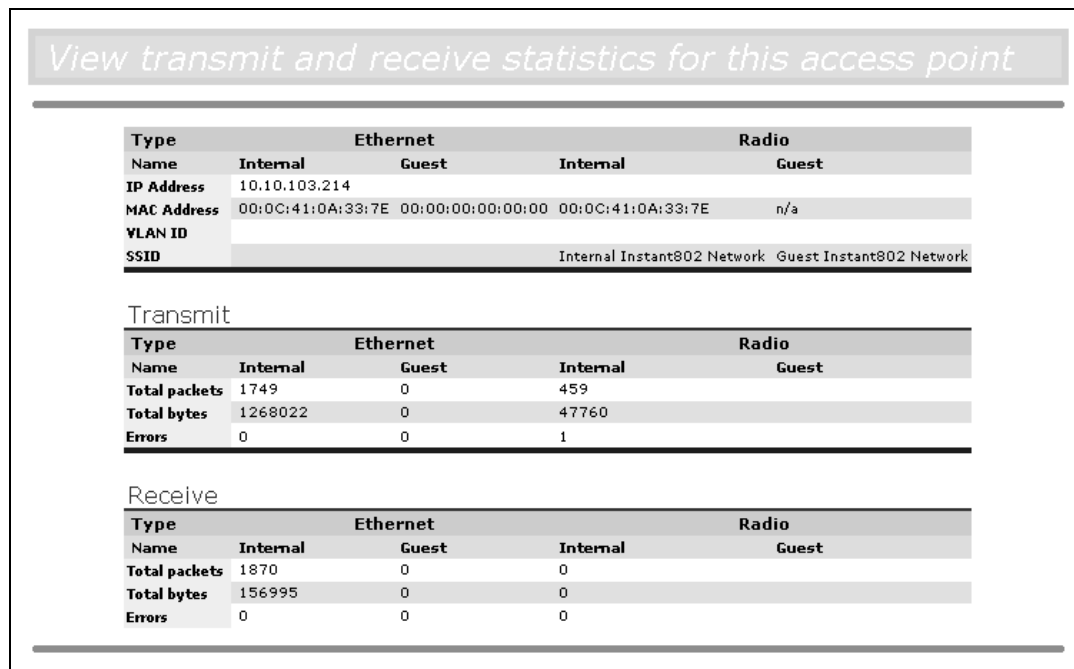


Figure 55. Transmit/Receive Statistics Page

This page provides some basic information about the current access point and a real-time display of the transmit and receive statistics for this access point as described in the following table. All transmit and receive statistics shown are totals because the access point was last started. If the access point is rebooted, these figures indicate transmit/receive totals since the reboot.

IP Address

IP address for the access point.

MAC Address

Media access control (MAC) address for the specified interface.

A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer.

The AT-WA7400 Wireless Access Point has a unique MAC address for each interface. A two-radio access point has a different MAC address for each interface on each of its two radios.

VLAN ID

Virtual LAN (VLAN) ID.

A VLAN is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be.

VLANs can be used to establish internal and guest networks on the same access point.

SSID

Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network.

The SSID is set on the Basic Settings page.

The Transmit and Receive sections provide the following information:

Total Packets

Indicates total packets sent (in Transmit table) or received (in Received table) by this access point.

Total Bytes

Indicates total bytes sent (in Transmit table) or received (in Received table) by this access point.

Errors

Indicates total errors related to sending and receiving data on this access point.

Viewing the Associated Wireless Clients

To view the client stations associated with a particular access point, perform the following procedure:

1. From the main menu, select **Status > Client Associations**.

The Client Associations page is shown in Figure 56.

The screenshot shows a table titled "View list of currently associated client stations". The table has columns for Radio, Network, Station, Status, and traffic statistics. Two rows are visible, representing different client stations.

| Radio | Network | Station | Status | | From Station | | To Station | |
|-------|----------|-------------------|---------------|------------|--------------|--------|------------|--------|
| | | | Authenticated | Associated | Packets | Bytes | Packets | Bytes |
| Two | Internal | 00:0a:79:89:66:3d | Yes | Yes | 39 | 1134 | 26 | 2749 |
| Two | Guest | 00:0a:79:89:66:42 | Yes | Yes | 12906 | 402859 | 6616 | 676428 |

Figure 56. Client Associations Page

The associated stations are displayed along with information about packet traffic transmitted and received for each station.

Link Integrity Monitoring

The AT-WA7400 Wireless Access Point provides link integrity monitoring to continually verify its connection to each associated client (even when there is no data exchange occurring). To do this, the access point sends data packets to clients every few seconds when no other traffic is passing. This allows the access point to detect when a client goes out of range, even during periods when no normal traffic is exchanged. The client connection drops off the list of associated clients within 300 seconds of a client disappearing, even if they do not disassociate (but went out of range).

What is the Difference Between an Association and a Session?

An association describes a client connection to a particular access point. A session describes a client connection to the network. A client network connection can shift from one clustered access point to another within the context of the same session. A client station can roam between access points and still maintain the session.

For information on monitoring sessions, see Chapter 5, "Session Monitoring" on page 65.

Viewing the Status of Neighboring Access Points

The status page for neighboring access points provides real-time statistics for all access points within range of the access point on which you are viewing the web pages.

To view information about other access points on the wireless network, perform the following procedure:

1. From the main menu, select **Status > Neighboring Access Points**.

The Neighboring Access Points page is shown in Figure 57.

| MAC Addr. | Radio | Beacon Int. | Type | SSID | Privacy | WPA | Band | Channel | Rate | Signal | # of Beacons | Last Beacon | Rates |
|-------------------|-------|-------------|------|--------|---------|-----|------|---------|------|--------|--------------|--------------------------------|---------------------------------------|
| 00:0c:46:f2:e2:fc | wlan0 | 100 | AP | ATNET | On | On | 5 | 52 | 60 | 2 | 305 | Fri Mar 10 10:01:33 2006 | 6, 9, 12, 18, 24, 36, 48, 54 |
| 00:0c:46:cf:2c:f4 | wlan0 | 100 | AP | allied | Off | Off | 5 | 52 | 60 | 10 | 5598 | Fri Mar 10 10:01:33 2006 | 6, 9, 12, 18, 24, 36, 48, 54 |
| 00:0c:46:cf:46:64 | wlan0 | 100 | AP | allied | Off | Off | 5 | 52 | 60 | 16 | 5599 | Fri Mar 10 10:01:33 2006 | 6, 9, 12, 18, 24, 36, 48, 54 |
| 00:0c:46:f2:dd:7c | wlan0 | 100 | AP | allied | Off | Off | 5 | 52 | 60 | 42 | 5601 | Fri Mar 10 10:01:33 2006 | 6, 9, 12, 18, 24, 36, 48, 54 |
| 00:0c:46:cf:32:84 | wlan0 | 100 | AP | allied | Off | Off | 5 | 52 | 60 | 46 | 15256 | Fri Mar 10 10:01:33 2006 | 6, 9, 12, 18, 24, 36, 48, 54 |

Figure 57. Neighboring Access Points Page

2. Click **Enabled** to allow the software to detect the neighboring access points.

The Neighboring Access Points page displays a table that provides the following items of information:

MAC Address

Shows the MAC address of the neighboring access point.

A MAC address is a hardware address that uniquely identifies each node of a network.

Radio

Two-Radio Access Points - If the access point that detecting the neighboring access points is a two-radio access point, the Radio field is included.

The Radio field indicates which radio the neighboring access point was detected on:

- wlan0 (radio one)
- wlan1 (radio two)

One-Radio Access Points - This field is not included on the Neighboring Access Points pages of one-radio access points.

Beacon Interval

Shows the beacon interval being used by this access point.

Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).

See Chapter 13, “Configuring Radio Settings” on page 145 for information on setting the beacon interval.

Type

Indicates the type of device:

- AP indicates the neighboring device is an access point that supports the IEEE 802.11 wireless networking framework in infrastructure mode.
- Ad hoc indicates a neighboring station running in ad hoc mode. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional access point. Ad-hoc mode is an IEEE 802.11 wireless networking framework also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS).

SSID

The Service Set Identifier (SSID) for the access point.

The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the Network Name.

To set the SSID, refer to “Configuring the Basic Settings and Starting the Wireless Network” on page 37, “Configuring Internal Wireless LAN Settings” on page 102, or “Configuring the Guest Network Wireless Settings” on page 103.

A guest network and an internal network running on the same access point must always have two different network names.

Privacy

Indicates whether there is any security on the neighboring device.

- Off** indicates that the Security mode on the neighboring device is set to “plain text” mode (no security).
- On** indicates that the neighboring device has some security in place.

For more information on security settings, see Appendix B, “Configuring Security on Wireless Clients” on page 217.

WPA

Indicates whether WPA security is “on” or “off” for this access point.

Band

This indicates the IEEE 802.11 mode being used on this access point. (For example, IEEE 802.11a, IEEE 8-2.11b, IEEE 802.11g.)

The number shown indicates the mode according to the following list:

- 2.4 indicates IEEE 802.11b mode or IEEE 802.11g mode
- 5 indicates IEEE 802.11a mode
- 5 Turbo indicates Atheros Turbo 5 GHz mode

Channel

Shows the channel on which the access point is currently broadcasting.

The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving.

See Chapter 13, “Configuring Radio Settings” on page 145 for information on the radio settings.

Rate

Shows the rate (in megabits per second) at which this access point is currently transmitting.

The current rate will always be one of the rates shown in Supported Rates.

Signal

Indicates the strength of the radio signal emitting from this access point as measured in decibels (Db).

of Beacons

Shows the total number of beacons transmitted by this access point since it was last booted.

Last Beacon

Shows the date and time of the most recent beacon was transmitted from the access point.

Rates

Shows supported and basic (advertised) rate sets for the neighboring access point. Rates are shown in megabits per second (Mbps).

All Supported Rates are listed, with Basic Rates shown in bold.

For information about setting the rates, refer to Chapter 13, “Configuring Radio Settings” on page 145. The rates shown for an

access point will always be the rates currently specified for that access point in its Radio Settings.

Viewing System Information

You can view information about a particular access point, such as its hardware version and current firmware version, by viewing the System Information page.

To view system information, perform the following procedure:

1. From the main menu, select **Status > Information**.

The System Information page is shown in Figure 58.

| <i>System information</i> | |
|---------------------------|--|
| Hardware Version | 1.00.00 |
| Serial No. | A02956B050900288A |
| MAC Addresses | 00:0C:46:F2:E2:BC / 00:0C:46:F2:E2:C0 |
| Boot Code Version | 1.00 |
| Firmware Version | wa7400 ver 1.12c_DUAL (Nov 3 2006 23:17:00) |
| System Up Time | 0 Days 00 : 25 : 18 (hh:mm:ss) |
| Telnet timeout | Times out after idling for 3 minutes |
| HTTP timeout | Times out after idling for 5 minutes |
| System name | WA7400 |

Figure 58. System Information Page

The System Information page provides the following information about the access point:

Hardware Version

The hardware version number.

Serial No.

The access point's serial number.

MAC Address

The access point's MAC address.

Boot Code Version

The version of the boot code currently loaded on the access point.

Firmware Version

The version of the firmware that is currently installed on the access point.

System Up Time

The length of time that the access point has been running since it was installed or last booted. This is shown in days, hours, minutes, and seconds.

Telnet Timeout

Displays the length of time that a Telnet session is available before it times out. You cannot change this parameter.

HTTP Timeout

The length of time that an HTTP session is available before it times out from inactivity. To change this parameter, refer to “Setting the HTTP Timeout” on page 204.

System Name

The name for the system that you assigned on the SNMP Configuration page. To change this setting, refer to “Configuring SNMP” on page 131.

Setting the Administrator Password

The administrator password controls access to the AT-WA7400 Management Software web pages for the AT-WA7400 Wireless Access Point. This setting is also available on the Basic Settings administration page. When you set the administration password in either place and apply the change, the new password is updated and shared by all access points in the cluster.

To set the administrator password, perform the following procedure:

1. From the main menu, select **Basic Settings**.

The Basic Settings page is shown in Figure 59.

Provide basic settings

1 Review Description of this Access Point ...


These fields show information specific to this access point.


IP Address: 10.10.20.230


MAC Address: 00:0c:46:f2:d7:64

Firmware Version: wa7400 ver 1.11.06c_DUAL (Jan 24 2006 10:45:53)

Location

Clustered 

0 Access Points 

0 User Accounts 

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster if the policy for adding new access points is set to "configure automatically".

Current Password

New Password

Confirm New Password

Wireless Network Name (SSID)

3 Set Configuration Policy for New Access Points ...

If you choose "configure automatically" as the policy for adding new access points, new access points will join the cluster when they are powered up and inherit the settings specified on this page. (If you choose to ignore new access points, you must configure them manually.)

New Access Points

This access point is in standalone mode. If you need to change these settings, click the "Access Points" tab.

4 Settings ...

Click "update" to save the new settings.

Figure 59. Basic Settings Page

2. In the Provide Network Settings section, enter the current administrator password. (The default is "manager.")

The text you enter is displayed as "*" characters to prevent others from seeing your password as you type.

3. In the **New Password** field, enter the new password. (The default is "friend.")

The Administrator password must be an alphanumeric string of up to 8 characters. Do not use special characters or spaces.

4. Re-enter the new administrator password to confirm that you typed it as intended.
5. Click **Update** to save the changes.

Enabling the Network Time Protocol (NTP) Server

The Network Time Protocol (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

The timestamp is used to indicate the date and time of each event in log messages.

See <http://www.ntp.org> for more general information on NTP.

To configure your access point to use a network time protocol (NTP) server, perform the following procedure:

1. From the main menu, select **Advanced > Time Protocol**.

The Time Protocol page is shown in Figure 60.

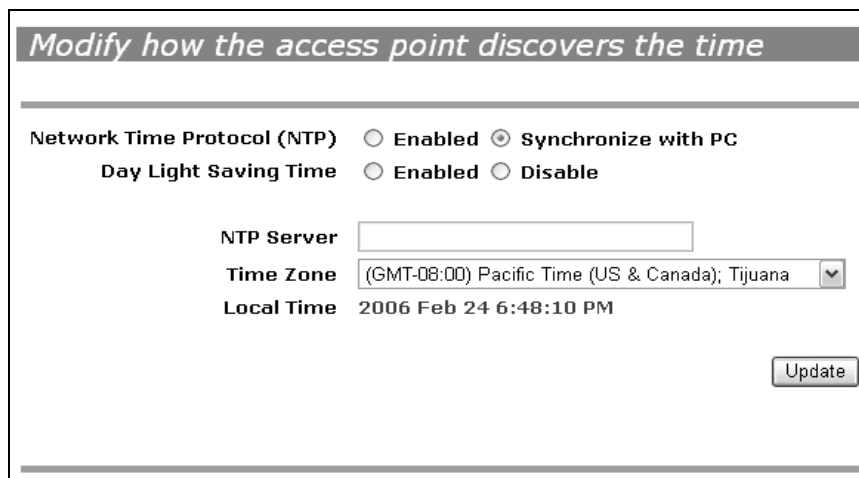


Figure 60. Time Protocol Page

2. For the Network Time Protocol (NTP) setting, select one of the following:

Enabled

The access point sets its time by contacting the NTP server.

Synchronize with PC

The access point synchronizes its clock with the PC from which you are managing the access point.

3. For the Daylight Saving Time setting, select one of the following:

Enabled

Daylight saving time is automatically adjusted.

Diabled

No adjustment is made for daylight saving time.

Note

If the time zone you select in the next setting is not one that participates in daylight saving time, then this selection is unavailable.

4. For the NTP Server setting, specify the NTP server by host name or IP address.
5. For the Time Zone, select your time zone from the list.
6. Click **Update** to apply your changes and the time shown as the Local Time reflects the correct local time.

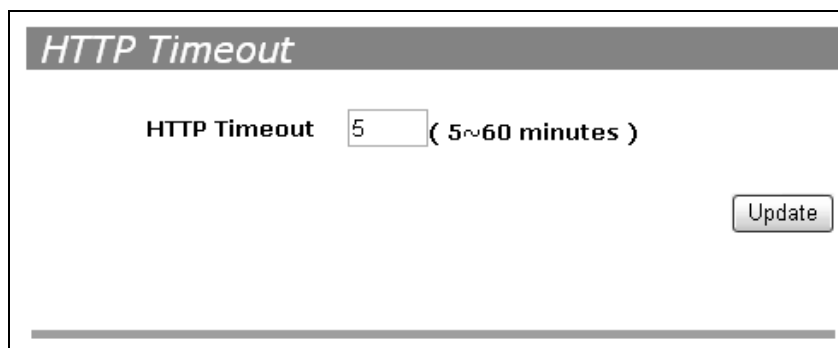
Setting the HTTP Timeout

You can set the length of time that an HTTP session is available before it times out from inactivity. The default is 5 minutes.

To set the HTTP timeout, perform the following procedure:

1. From the main menu, select **Advanced > HTTP timeout**.

The HTTP timeout page is shown in Figure 61.



The screenshot shows a web interface for configuring the HTTP timeout. At the top, there is a dark grey header with the text "HTTP Timeout" in white. Below the header, the text "HTTP Timeout" is displayed in a standard font. To its right is a text input field containing the number "5". Further to the right, the text "(5~60 minutes)" is shown in a smaller font. At the bottom right of the page, there is a button with the text "Update".

Figure 61. HTTP Timeout

2. Change the timeout time and click **Update**.

Rebooting the Access Point

For maintenance purposes or as a troubleshooting measure, you can reboot the AT-WA7400 Wireless Access Point.

To reboot the access point, perform the following procedure:

1. From the main menu, select **Advanced > Reboot**.

The Reboot page is shown in Figure 62.

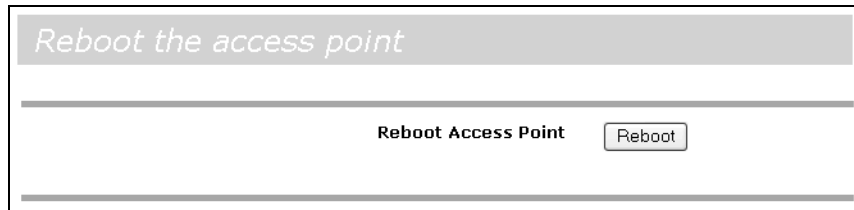


Figure 62. Reboot Page

2. Click **Reboot**.

The access point reboots.

Note

Another option is to press and release the Reset button on the back of the AT-WA7400 Wireless Access Point.

Resetting the Configuration to Factory Defaults

If the AT-WA7400 Wireless Access Point is not functioning correctly and if you have tried all other troubleshooting measures, use the Reset Configuration function. This feature restores the factory defaults and clears all settings, including settings such as a new password or wireless settings.

To reboot the access point, perform the following procedure:

1. From the main menu, select **Advanced > Reset Configuration**.

The Reset Configuration page is shown in Figure 63.

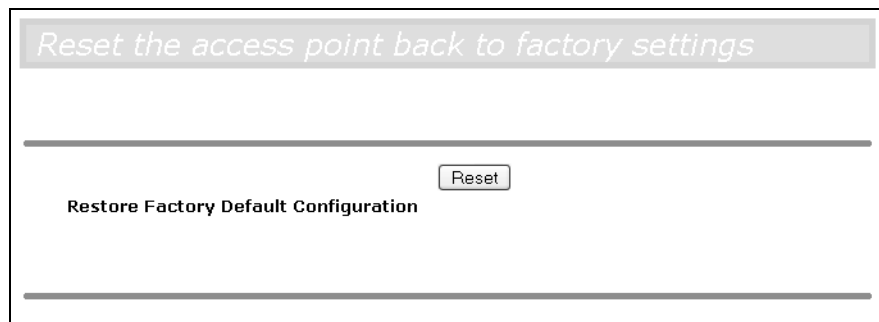


Figure 63. Reset Configuration Page

2. Click **Reset**.

The factory defaults are restored.

Note

Another option is to press the Reset button on the back of the AT-WA7400 Wireless Access Point for at least 10 seconds when the power is on.

Note

If you do reset the configuration from this page, you are doing so for this access point only; not for other access points in the cluster.

For information about the factory default settings, see Appendix A, “Management Software Default Settings” on page 215.

Upgrading the Firmware

As new versions of the AT-WA7400 Wireless Access Point firmware become available, you can upgrade the firmware on your devices to take advantages of new features and enhancements.



Caution

Do not upgrade the firmware from a wireless client that is associated with the access point you are upgrading. Doing so causes the upgrade to fail. Furthermore, all wireless clients are disassociated and no new associations are allowed.

If you encounter this scenario, the solution is to use a wired client to gain access to the access point:

- Create a wired Ethernet connection from a PC to the access point.
 - Start the AT-WA7400 Management Software.
 - Repeat the upgrade process using the wired client.
-

Note

You must upgrade each access point; you cannot upgrade firmware automatically across the cluster.

Keep in mind that a successful firmware upgrade restores the access point configuration to the factory defaults. (See Appendix A, "Management Software Default Settings" on page 215.)

To upgrade the firmware on a particular access point, perform the following procedure:

1. From the main menu of the access point you want to upgrade, select **Advanced > Upgrade**.

The Upgrade Firmware page is shown in Figure 64.

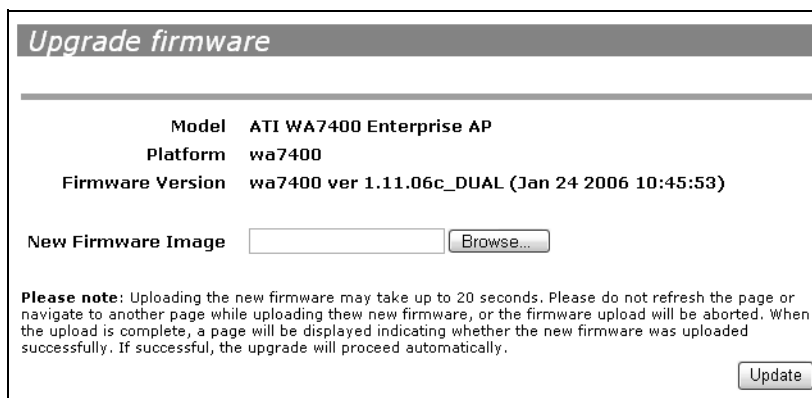


Figure 64. Upgrade Firmware Page

Information about the current firmware version is displayed and an option to upgrade to a new firmware image is provided.

2. If you know the path to the New Firmware Image file, enter it in the text box. Otherwise, click **Browse** and locate the firmware image file.
3. Click **Update** to apply the new firmware image.

A confirmation window is displayed that describes the upgrade process.

4. Click **OK** to confirm the upgrade and start the process.



Caution

The firmware upgrade process begins after you click Update and then OK in the confirmation window.

The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point restarts and resumes normal operation using the factory default configuration settings.

**Verifying the
Firmware
Upgrade**

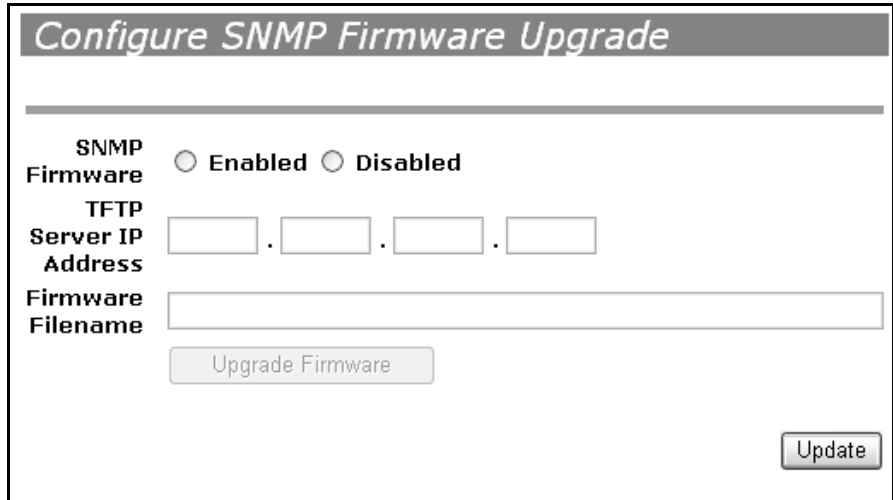
To verify that the firmware upgrade completed successfully, check the firmware version shown on the Advanced > Upgrade page (and also on the Basic Settings page). If the upgrade was successful, the updated version name or number is displayed.

SNMP Firmware Upgrade

To upgrade the firmware using SNMP, perform the following procedure:

1. From the main menu, select **Advanced > SNMP Firmware Upgrade**.

The Configure SNMP Firmware Upgrade page is shown in Figure 65.



Configure SNMP Firmware Upgrade

SNMP Firmware Enabled Disabled

TFTP Server IP Address . . .

Firmware Filename

Upgrade Firmware

Update

Figure 65. Configure SNMP Firmware Upgrade Page

2. For the **SNMP Firmware** option, click **Enabled**.
3. In the **TFTP Server IP Address** field, enter the IP address of the server where the software is located.
4. In the **Firmware Filename** field, enter the path and file name of the file you want to download.
5. Click **Upgrade Firmware**.

Wait about five minutes for the upgrade to complete.

Chapter 18

Backing Up and Restoring a Configuration

You can save a copy of the current settings on the AT-WA7400 Wireless Access Point to a backup configuration file. You can use the backup file at a later date to restore the access point to the previously saved configuration.

The following topics describe how to back up and restore access point configurations:

- “Backing up the Configuration Settings for an Access Point” on page 212
- “Restoring Access Point Settings to a Previous Configuration” on page 213

Backing up the Configuration Settings for an Access Point

To save a copy of the current settings on an access point to a backup configuration file (.cbk format), perform the following procedure:

1. From the main menu, select **Advanced > Backup/Restore**.

The Backup/Restore page is shown in Figure 66.

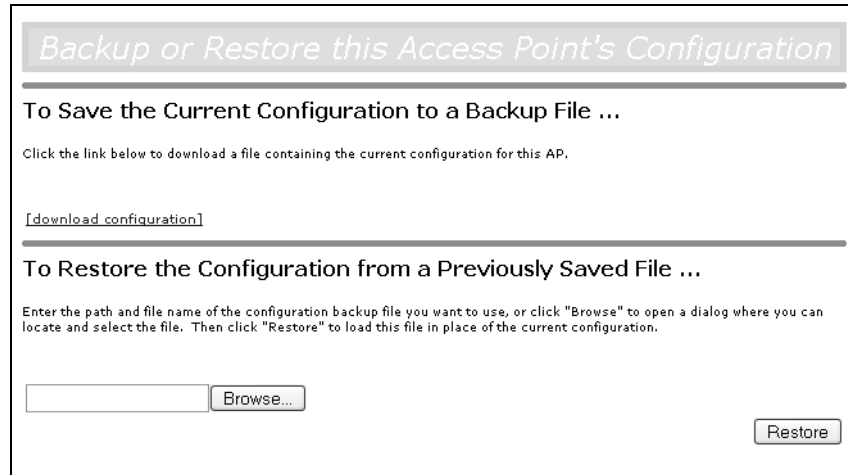


Figure 66. Backup/Restore Page

2. In the top section of the page, click **download configuration**.

A File Download or Open dialog box is displayed

3. Choose the **Save** option in this first dialog box.

The file browser window opens.

4. Navigate to the directory where you want to save the file, and click **OK** to save the file.

You can keep the default file name (apconfig.cbk) or rename the backup file, but be sure to save the file with a .cbk extension.

Restoring Access Point Settings to a Previous Configuration

To restore the configuration on an access point to previously saved settings, perform the following procedure:

1. From the main menu, select **Advanced > Backup/Restore**.

The Backup/Restore page opens, as shown in Figure 66 on page 212.

2. Select the backup configuration file you want to use, either by typing the full path and file name in the Restore field or clicking **Browse** and selecting the file.

Note

Only those files that were created with the Backup function and saved as .cbk backup configuration files are valid to use with Restore; for example, apconfig.cbk.

3. Click **Restore**.

The access point reboots.

Note

When you click Restore, the access point reboots. A reboot confirmation dialog box and follow-on rebooting status message are displayed. Wait for the reboot process to complete (a minute or two). After a moment, try accessing the web pages as described in the next step; they are not accessible until the access point has rebooted.

4. When the access point has rebooted, access the web pages either by clicking again on one of the pages (if the UI is still displayed) or by typing the IP address of the AT-WA7400 Wireless Access Point as a URL in the address field of the web browser. The URL for the access point should be entered as `http://IPAddressOfAccessPoint`.

Now you should see the configuration settings restored to the saved configuration from the Backup file you selected.

Appendix A

Management Software Default Settings

Table 1 lists the management software default settings.

Table 1. Management Software Default Settings

| Setting | Default |
|-----------------------------|----------------|
| System Name | WA7400 |
| User Name | manager |
| Password | friend |
| Network Name (SSID) | Allied |
| Network Time Protocol (NTP) | None |
| IP Address | 192.168.1.230 |
| Connection Type | DHCP |
| Subnet Mask | None |
| Radio | On |
| IEEE 802.11 Mode | 802.11g |
| 802.11g Channel | Auto |
| Beacon Interval | 100 |
| DTIM Period | 2 |
| Fragmentation Threshold | 2346 |
| Regulatory Domain | FCC |
| RTS Threshold | 2347 |
| MAX Stations | 2007 |
| Transmit Power | 100 percent |

Table 1. Management Software Default Settings (Continued)

| Setting | Default |
|-------------------------------------|--|
| Rate Sets Supported (Mbps) | IEEE 802.1a: 54, 48, 36, 24, 18, 12, 9, 6 (Upgrade required) IEEE 802.1g: 54, 48, 36, 24, 18, 12, 11, 9, 5.5, 2, 1 IEEE 802.1b: 11, 5.5, 2, 1 Atheros Turbo 5 Ghz: 108, 96, 72, 48, 36, 24, 18, 12 (Upgrade required) |
| Rate Sets (Mbps) (Basic/Advertised) | IEEE 802.1a: 24, 12, 6 (Upgrade required) IEEE 802.1g: 11, 5.5, 2, 1 IEEE 802.1b: 2, 1 Atheros Turbo 5 Ghz: 48, 214, 12 (Upgrade required) |
| Broadcast SSID | Allow |
| Security Mode | None (plain text) |
| Authentication Type | None |
| MAC Address Filtering | Allow any station unless in list |
| Guest Login and Management | Disabled |
| Load Balancing | Disabled |
| WDS Settings | None |

Appendix B

Configuring Security on Wireless Clients

Users will typically configure security on their wireless clients for access to many different networks (access points). The list of Available Networks changes depending on the location of the client and which access points are online and detectable in that location.

The exception to this setup is if the access point is set to prohibit the broadcast of its network name. In this case the SSID will not show up in the list of Available Networks on the client. Instead, the client must have the exact network name configured in the network connection properties before it will be able to connect.

After an access point has been detected by the client and security is configured for it, the access point remains in the client's list of networks but shows as either reachable or unreachable depending on the situation. For each network (access point) you want to connect to, configure security settings on the client to match the security mode being used by that network.

This appendix describes the security setup on a client that uses Microsoft Windows client software for wireless connectivity. The Windows client software is used as the example because of its widespread availability on Windows computers and laptops. These procedures will vary slightly if you use different software on the client (such as Funk Odyssey), but the configuration information you need to provide is the same.

The recommended sequence for security configuration is (1) set up security on the access point, and (2) configure security on each of the wireless clients.

Initially, you will connect to an access point that has no security set (plain text mode) from an unsecure wireless client. With this initial connection, you can go to the access point's web pages and configure a security mode (Advanced > Security).

When you reconfigure the access point with a security setting and click Update, your wireless client is disassociated and you lose connectivity to the AT-WA7400 Wireless Access Point. In some cases, you may need to make additional changes to the access point security settings before configuring the client. Therefore, you must have a backup Ethernet (wired) connection.

The following sections describe how to set up each of the supported

security modes on wireless clients of a network served by the AT-WA7400 Wireless Access Point.

- ❑ “Network Infrastructure and Choosing Between the Built-in or External Authentication Server” on page 219
- ❑ “Make Sure the Wireless Client Software is Up to Date” on page 220
- ❑ “Accessing the Microsoft Windows Wireless Client Security Settings” on page 221
- ❑ “Configuring a Client to Access an Unsecure Network (Plain Text mode)” on page 223
- ❑ “Configuring Static WEP Security on a Client” on page 224
- ❑ “Configuring IEEE 802.1x Security on a Client” on page 227
- ❑ “Configuring WPA/WPA2 Enterprise (RADIUS) Security on a Client” on page 236
- ❑ “Configuring WPA/WPA2 Personal (PSK) Security on a Client” on page 245
- ❑ “Configuring an External RADIUS Server to Recognize the AT-WA7400 Wireless Access Point” on page 248
- ❑ “Obtaining a TLS-EAP Certificate for a Client” on page 253

Network Infrastructure and Choosing Between the Built-in or External Authentication Server

Network security configurations including Public Key Infrastructures (PKI), Remote Authentication Dial-in User Server (RADIUS) servers, and Certificate Authority (CA) can vary a great deal from one organization to the next in terms of how they provide Authentication, Authorization, and Accounting (AAA). Ultimately, the particulars of your infrastructure will determine how clients should configure security to access the wireless network. Rather than try to predict and address the details of every possible scenario, this section provides general guidelines about each type of client configuration supported by the AT-WA7400 Wireless Access Point.

I Want to Use the Built-in Authentication Server (EAP-PEAP)

If you do not have a RADIUS server or PKI infrastructure in place and/or are unfamiliar with many of these concepts, Allied Telesyn strongly recommends setting up the AT-WA7400 Wireless Access Points with security that uses the Built-in Authentication Server on the access point. This will mean setting up the access point to use either IEEE 802.1x or WPA/WPA2 Enterprise (RADIUS) security mode. (The built-in authentication server uses the EAP-PEAP authentication protocol.)

- ❑ If the AT-WA7400 Wireless Access Point is set up to use IEEE 802.1x mode and the Built-in Authentication Server, then configure wireless clients as described in “IEEE 802.1x Client Using EAP/PEAP” on page 227.
- ❑ If the AT-WA7400 Wireless Access Point is configured to use WPA/WPA2 Enterprise (RADIUS) mode and the Built-in Authentication Server, then configure wireless clients as described in “WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP” on page 236.

I Want to Use an External RADIUS Server with EAP-TLS Certificates or EAP-PEAP

The following sections assume that if you have an external RADIUS server and PKI/CA setup, you will know how to configure client security options appropriate to your security infrastructure beyond the fundamental suggestions given here. Topics covered here that particularly relate to client security configuration in a RADIUS - PKI environment are:

- ❑ “IEEE 802.1x Client Using EAP/TLS Certificate” on page 231
- ❑ “WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate” on page 241
- ❑ “Configuring an External RADIUS Server to Recognize the AT-WA7400 Wireless Access Point” on page 248
- ❑ “Obtaining a TLS-EAP Certificate for a Client” on page 253

Details about how to configure an EAP-PEAP client with an external RADIUS server are not covered in this document.

Make Sure the Wireless Client Software is Up to Date

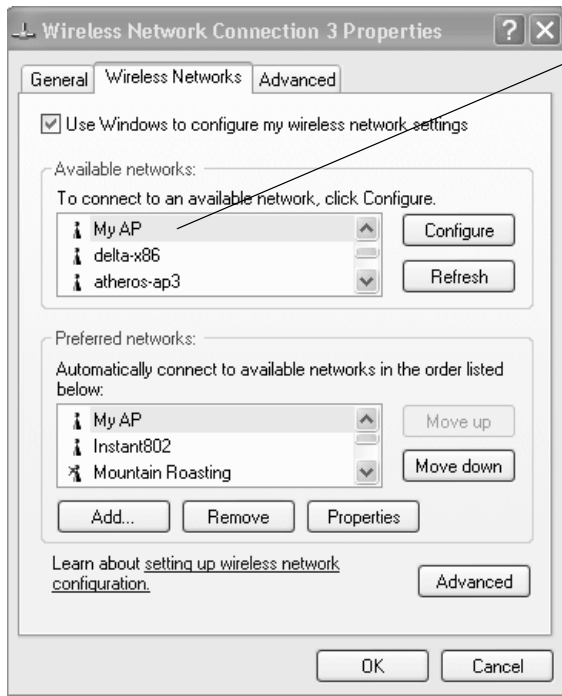
Before starting out, please keep in mind that service packs, patches, and new releases of drivers and other supporting technologies for wireless clients are being generated at a fast pace. A common problem encountered in client security setup is not having the right driver or updates to it on the client. For example, if you are setting up WPA on the client, make sure you have a driver installed that supports WPA, which is a relatively new technology. Even many client cards currently available do not ship from the factory with the latest drivers.

Accessing the Microsoft Windows Wireless Client Security Settings

To access the Microsoft Windows wireless client settings, perform the following procedure:

1. Use one of the following two ways to access the security properties for a wireless client:
 - a. From the wireless connection icon on the Windows task bar:
 - Right-click on the wireless connection icon in your Windows task bar and select **View available wireless networks**.
 - Select the SSID of the network to which you want to connect and click **Advanced** to open the Wireless Network Connection Properties dialog box.
 - b. From the Windows Start menu at the left end of the task bar:
 - Choose **Start > My Network Places** to open the Network Connections window.
 - From the Network Tasks menu on the left, select **View Network Connections** to open the Network Connections window.
 - Select the wireless network connection you want to configure, right-click and choose **View available wireless networks**.
 - Select the SSID of the network to which you want to connect and click **Advanced** to open the Wireless Network Connection Properties dialog box.

The Wireless Networks page (which should be automatically displayed) lists Available networks and Preferred networks, as shown in Figure 1.



List of available networks changes depending on client location. Each network (or access point) that that is detected by the client shows up in this list. ("Refresh" updates the list with current information.)

For each network you want to connect to, configure security settings on the client to match the security mode being used by that network.

Note: The exception to this is if the access point is configured to prohibit broadcast of its network name, the name is not shown on this list. In that case you would need to type in the exact network name to be able to connect to it.

Figure 1. Wireless Network Connections Properties Dialog Box

2. From the list of Available networks, select the SSID of the network to which you want to connect and click **Configure**.

The Wireless Network Connection Properties dialog box (Figure 2) opens with the Association and Authentication tabs for the selected network.

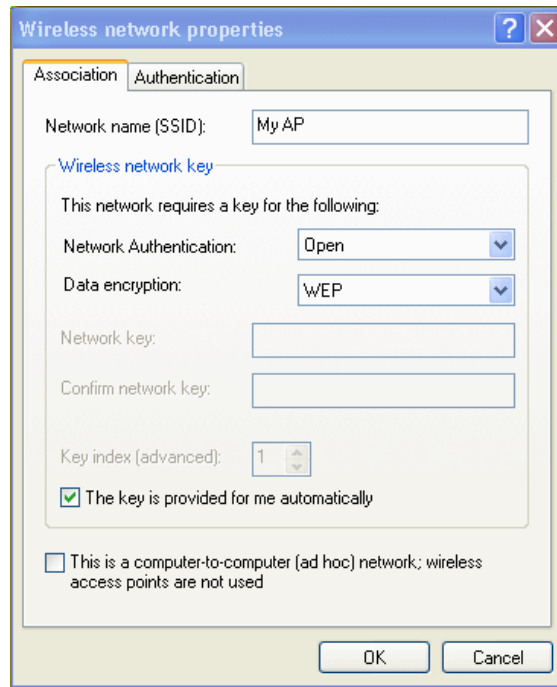


Figure 2. Wireless Network Properties Dialog Box

Use this dialog box to configure the types of client security described in the following sections. Make sure that the Wireless Network Properties dialog box you are working in pertains to the Network Name (SSID) for the network you want to reach on the wireless client you are configuring.

Configuring a Client to Access an Unsecure Network (Plain Text mode)

If the access point or wireless network to which you want to connect is configured as plain text security mode (no security), you need to configure the client accordingly. A client using no security to connect is configured with Network Authentication Open to that network and Data Encryption Disabled as described below.

If you do have security configured on a client for properties of an unsecure network, the security settings actually can prevent successful access to the network because of the mismatch between client and access point security configurations.

To configure the client to not use any security, perform the following procedure:

1. Open the client's Network Properties dialog box.
2. Configure the following settings as shown in Figure 5:

- a. For Network Authentication, choose Open.
- b. For Data encryption, choose Disabled.

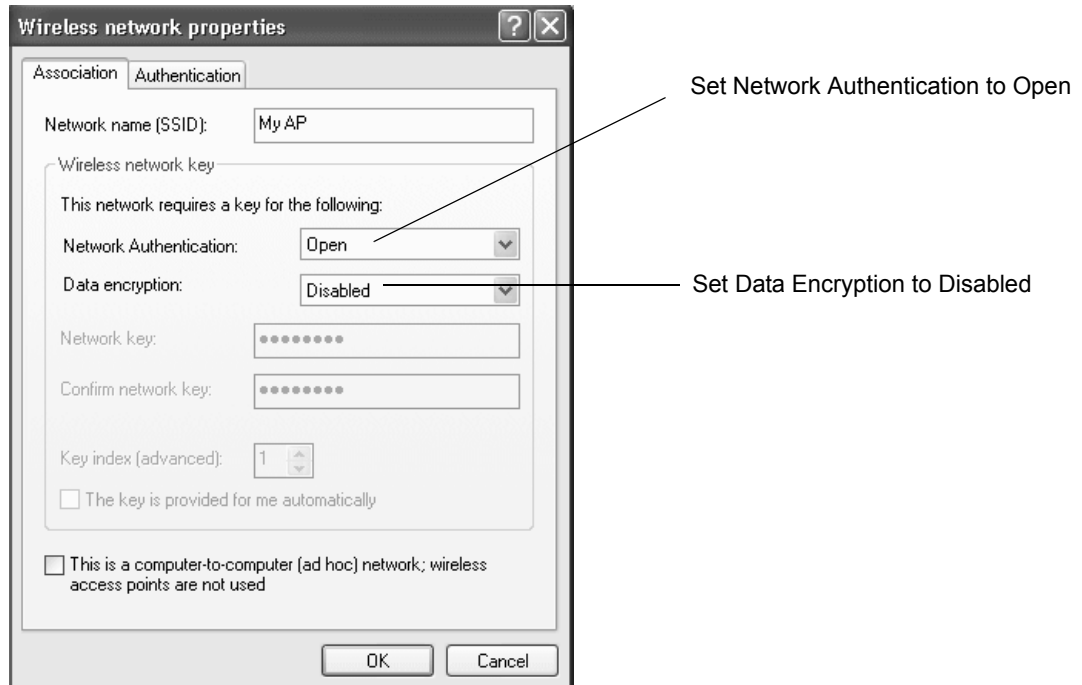


Figure 3. Wireless Network Properties Dialog Box

Configuring Static WEP Security on a Client

Static Wired Equivalent Privacy (WEP) encrypts data moving across a wireless network based on a static (non-changing) key. The encryption algorithm is a stream cipher called RC4. The access point uses a key to transmit data to the client stations. Each client must use that same key to decrypt data it receives from the access point. Different clients can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

To configure Static WEP security on a client, perform the following procedure:

1. Confirm the Security mode setting on the Security Settings page, as

shown in Figure 4.

Figure 4. Security Settings Page

2. Configure WEP security on each client as shown in Figure 5.

Figure 5. Wireless Network Properties Dialog Box

Network Authentication

Choose Open or Shared, depending on how you configured this option on the access point.

Note

When the Authentication Algorithm on the access point is set to Both, clients set to either Shared or Open can associate with the access point. Clients configured to use WEP in Shared mode must have a valid WEP key in order to associate with the access point. Clients configured to use WEP as an Open system can associate with the access point even without a valid WEP key (but a valid key will be required to actually view and exchange data).

Data Encryption

Choose WEP.

Network Key

Provide the WEP key you entered on the access point Security settings in the Transfer Key Index position.

For example, if the Transfer Key Index on the access point is set to “1”, then for the client Network Key specify the WEP Key you entered as WEP Key 1 on the access point.

Key Index

Set key index to indicate which of the WEP keys specified on the access point Security page will be used to transfer data from the client back to the access point.

For example, you can set this to 1, 2, 3, or 4 if you have all four WEP keys configured on the access point.

The key is provided for me automatically

Disable this option (click to uncheck the box).

3. On the Authentication tab, configure the following parameter:

Enable IEEE 802.1x authentication for this network

Make sure that IEEE 802.1x authentication is disabled (box should be unchecked).

(Setting the encryption mode to WEP should automatically disable authentication.)

4. Click **OK** on the Wireless Network Properties dialog box to close it and save your changes.

Connecting to the Wireless Network with a Static WEP Client

Static WEP clients should now be able to associate and authenticate with the access point. As a client, you will not be prompted for a WEP key. The WEP key configured on the client security settings is automatically used when you connect.

Configuring IEEE 802.1x Security on a Client

IEEE 802.1x is the standard defining port-based authentication and infrastructure for doing key management. Extensible Authentication Protocol (EAP) messages sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

IEEE 802.1x Client Using EAP/PEAP

The built-in authentication server on the AT-WA7400 Wireless Access Point uses Protected Extensible Authentication Protocol (EAP) referred to here as EAP/PEAP.

- ❑ If you are using the built-in authentication server with IEEE 802.1x security mode on the AT-WA7400 Wireless Access Point, then you will need to set up wireless clients to use PEAP.
- ❑ Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to (1) add the AT-WA7400 Wireless Access Point to the list of RADIUS server clients, and (2) configure your IEEE 802.1x wireless clients to use PEAP.

Note

The following example assumes that you are using the built-in authentication server that is shipped with the AT-WA7400 Wireless Access Point. If you are setting up EAP/PEAP on a client of an access point that is using an external RADIUS server, the client configuration process will differ somewhat from this example especially with regard to certificate validation.

To configure IEEE 802.1x security on a client, perform the following procedure:

1. If you configured the AT-WA7400 Wireless Access Point to use IEEE

802.1x security mode as shown in Figure 6,

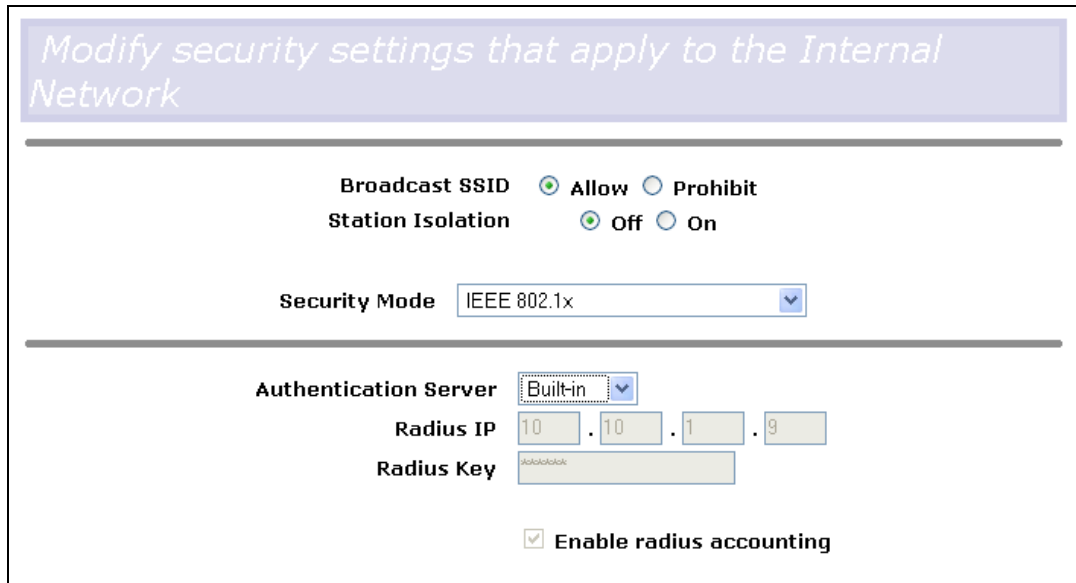


Figure 6. Security Settings Page

633Then configure IEEE 802.1x security with PEAP authentication on each client as follows.

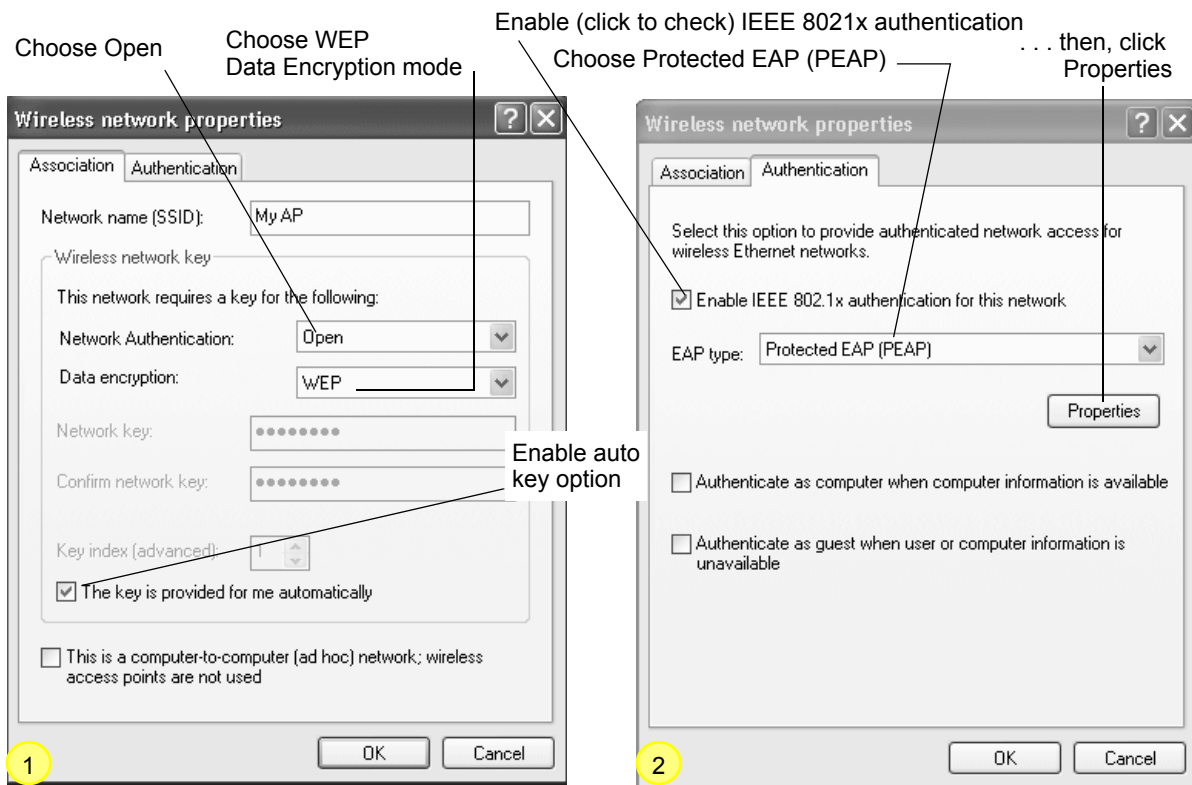


Figure 7. Association and Authentication Tabs

2. Configure the following settings on the Association tab in the Network Properties dialog box:

Network Authentication

Open

Data Encryption

WEP

Note

An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.

This key is provided for me automatically

Enable (click to check) this option.

3. Configure this setting on the Authentication tab.

EAP Type

Choose Protected EAP (PEAP).

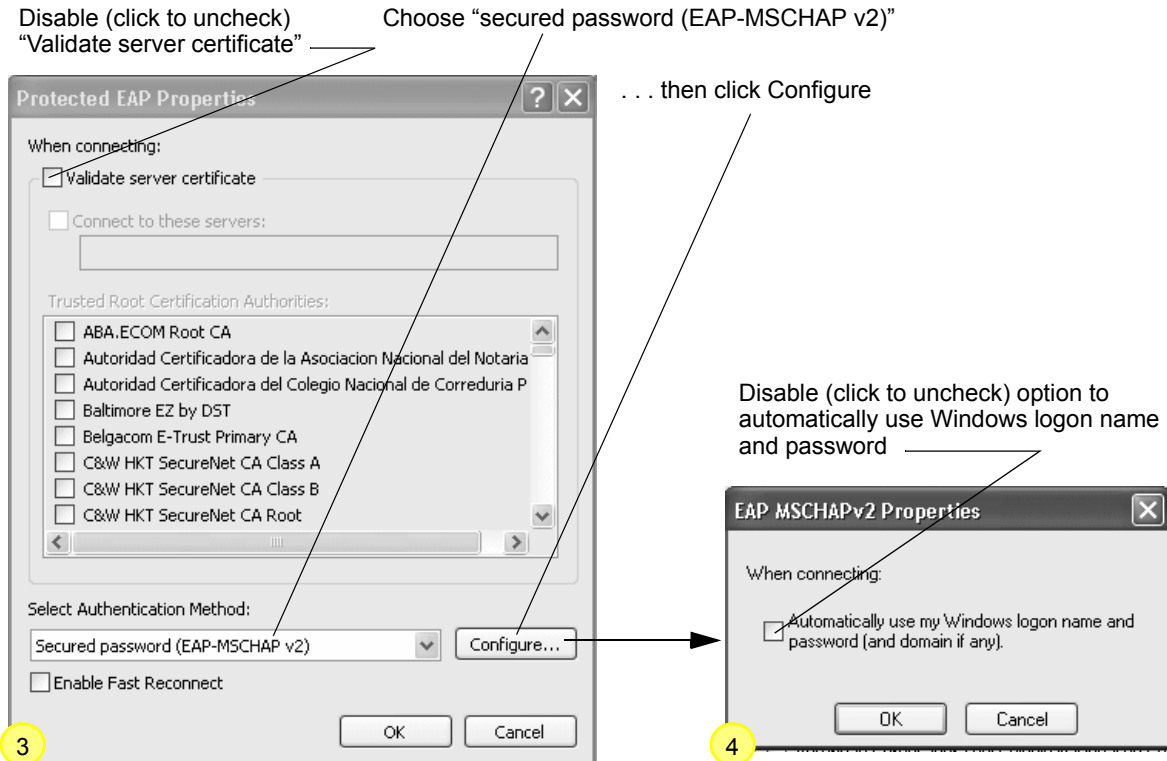


Figure 8. Protected EAP Properties Dialog Box and EAP Properties Dialog Box

4. Click **Properties** to open the Protected EAP Properties dialog box and configure the following settings:

Validate Server Certificate

Disable this option (click to uncheck the box).

Note

This example assumes that you are using the built-in authentication server on the access point. If you are setting up EAP/PEAP on a client of an access point that is using an external RADIUS server, you might see a certificate validation dialog box and need to choose a certificate, depending on your infrastructure.

Select Authentication Method

Choose Secured password (EAP-MSCHAP v2).

5. Click **Configure** to open the EAP MSCHAP v2 Properties dialog box.
6. Disable (click to uncheck) the option to “Automatically use my Windows login name etc.”

7. Click **OK** on all dialog boxes (starting with the EAP MSCHAP v2 Properties dialog box) to close and save your changes.

IEEE 802.1x PEAP clients should now be able to associate with the access point. Client users will be prompted for a user name and password to authenticate with the network.

IEEE 802.1x Client Using EAP/TLS Certificate

Extensible Authentication Protocol (EAP) Transport Layer Security (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA/WPA2 Enterprise (RADIUS) and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.

Note

If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), including a Certificate Authority (CA), server configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

Some good starting points available on the web for the Microsoft Windows PKI software are: "How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881> and How to Configure a Certificate Server at <http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3>.

To use this type of security, you must do the following:

1. Add the AT-WA7400 Wireless Access Point to the list of RADIUS server clients. (See "Configuring an External RADIUS Server to Recognize the AT-WA7400 Wireless Access Point" on page 248.)
2. Configure the AT-WA7400 Wireless Access Point to use your RADIUS server (by providing the RADIUS server IP address as part of the IEEE 802.1x security mode settings).
3. Configure wireless clients to use IEEE 802.1x security and "Smart Card or other Certificate" as described in this section.
4. Obtain a certificate for this client as described in "Obtaining a TLS-EAP Certificate for a Client" on page 253.

5. Verify that you configured the AT-WA7400 Wireless Access Point to use IEEE 802.1x security mode with an external RADIUS server, as shown in Figure 9.

Modify security settings that apply to the Internal Network

Broadcast SSID Allow Prohibit
Station Isolation Off On

Security Mode IEEE 802.1x

Authentication Server External

Radius IP 10 . 10 . 1 . 9

Radius Key [Masked]

Enable radius accounting

Figure 9. Security Settings Page

6. Then configure IEEE 802.1x security with certificate authentication on each client as follows (Figure 10).

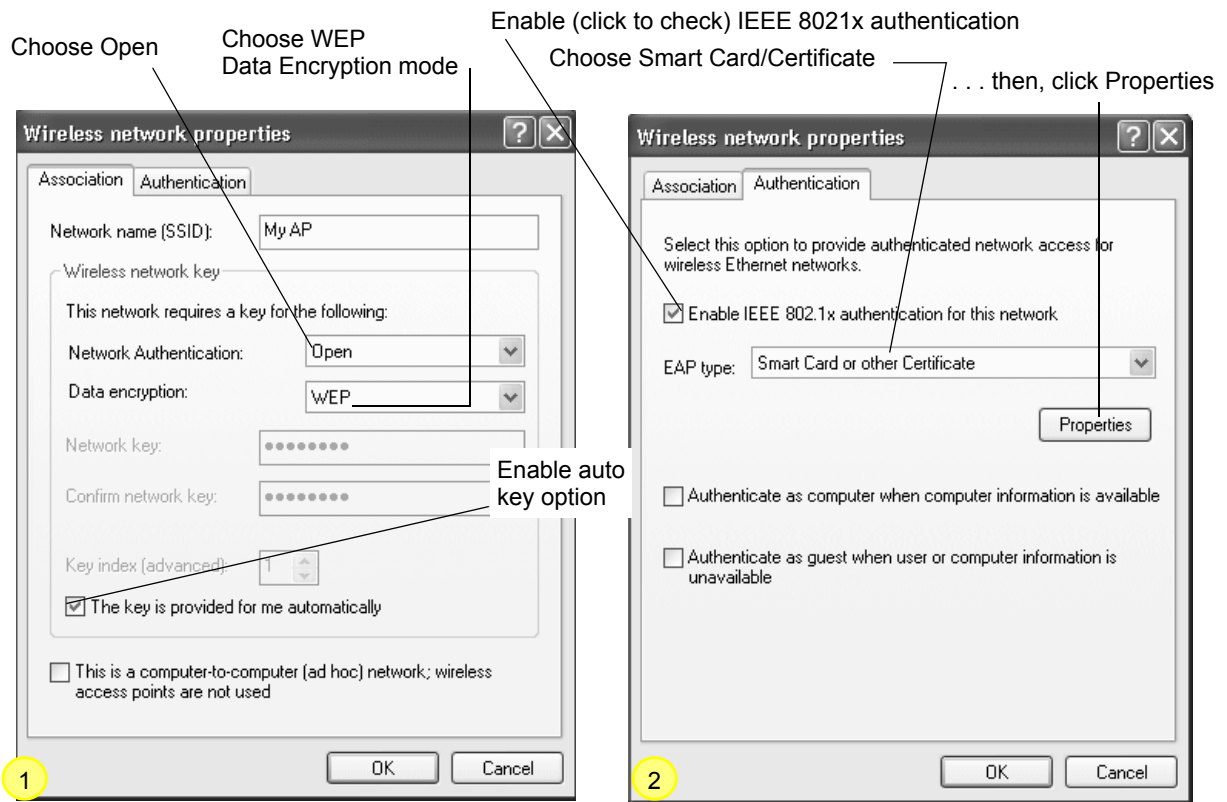


Figure 10. Association and Authentication Tabs

- Configure the following settings on the Association tab in the Network Properties dialog box.

Network Authentication

Open

Data Encryption

WEP

Note

An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.

This key is provided for me automatically

Enable (click to check) this option.

- Configure these settings on the Authentication tab.

Enable IEEE 802.1x authentication for this network

Enable (click to check) this option.

EAP Type

Choose Smart Card or other Certificate.

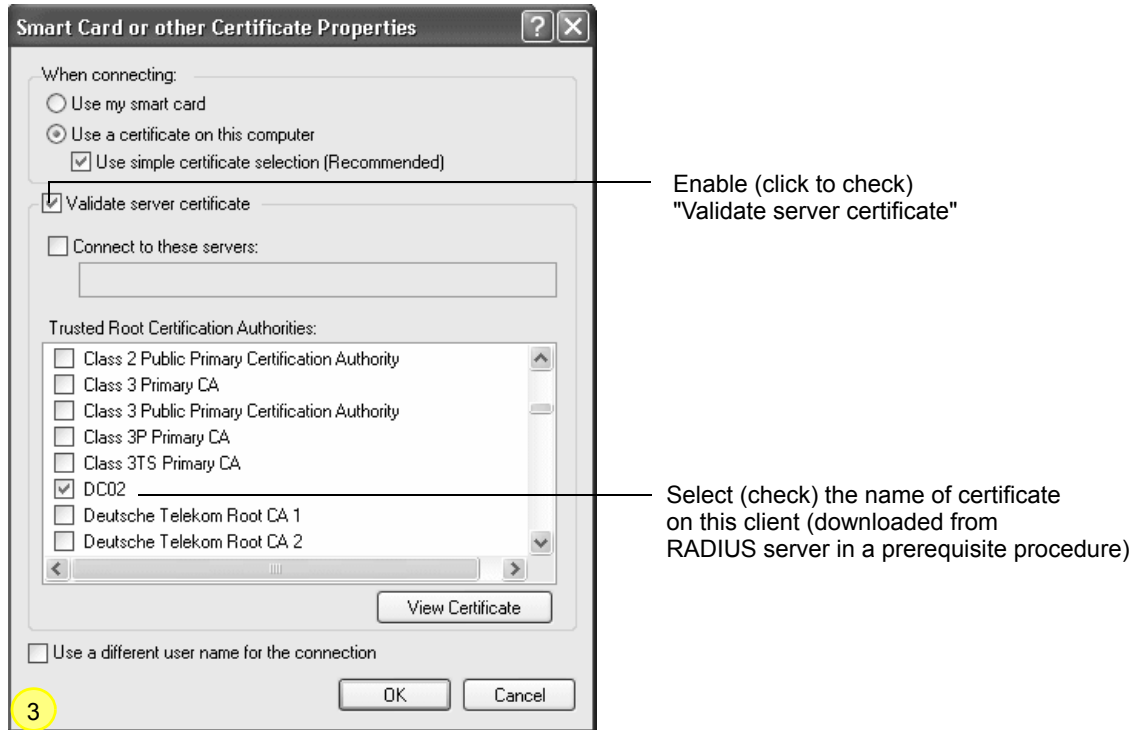


Figure 11. Smart Card or other Certificate Properties Dialog Box

9. Click **Properties** to open the Smart Card or other Certificate Properties dialog box and enable the “Validate server certificate” option.

Validate Server Certificate

Enable this option (click to check the box).

Certificates

In the certificate list shown, select the certificate for this client.

10. Click **OK** on all dialog boxes to close them and save your changes.
11. To complete the client configuration you must now obtain a certificate from the RADIUS server and install it on this client. For information on how to do this see “Obtaining a TLS-EAP Certificate for a Client” on page 253.

IEEE 802.1x clients should now be able to connect to the access point using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for login information. The

certificate is automatically sent to the RADIUS server for authentication and authorization.

Configuring WPA/WPA2 Enterprise (RADIUS) Security on a Client

Wi-Fi Protected Access 2 (WPA2) with Remote Authentication Dial-In User Service (RADIUS) is an implementation of the Wi-Fi Alliance IEEE 802.11 standard, which includes Advanced Encryption Standard (AES), Counter mode/CBC-MAC Protocol (CCMP), and Temporal Key Integrity Protocol (TKIP) mechanisms. This mode requires the use of a RADIUS server to authenticate users.

This security mode also provides backwards-compatibility for wireless clients that support only the original WPA.

When you configure WPA/WPA2 Enterprise (RADIUS) security mode on the access point, you have a choice of whether to use the built-in authentication server or an external RADIUS server that you provide.

The AT-WA7400 Wireless Access Point's built-in authentication server supports Protected Extensible Authentication Protocol (EAP) known as EAP/PEAP and Microsoft Challenge Handshake Authentication Protocol *Version 2* (MSCHAP V2), which provides authentication for point-to-point (PPP) connections between a Windows-based computer and network devices such as access points.

If you configure the network (access point) to use security mode and choose the built-in authentication server, you must configure client stations to use WPA/WPA2 Enterprise (RADIUS) and EAP/PEAP.

If you configure the network (access point) to use this security mode with an external RADIUS server, you must configure the client stations to use WPA/WPA2 Enterprise (RADIUS) and whichever security protocol your RADIUS server is configured to use.

WPA/WPA2 Enterprise (RADIUS) Client Using EAP/PEAP

The built-in authentication server on the AT-WA7400 Wireless Access Point uses Protected Extensible Authentication Protocol (EAP) known as EAP/PEAP.

- ❑ If you are using the Built-in Authentication server with WPA/WPA2 Enterprise (RADIUS) security mode on the AT-WA7400 Wireless Access Point, then you will need to set up wireless clients to use PEAP.
- ❑ Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to (1) add the AT-WA7400 Wireless Access Point to the list of RADIUS server clients, and (2) configure your WPA/WPA2 Enterprise (RADIUS) wireless clients to use PEAP.

Note

The following example assumes that you are using the built-in authentication server that is shipped with the AT-WA7400 Wireless Access Point. If you are setting up EAP/PEAP on a client of an access point that is using an external RADIUS server, the client configuration process will differ somewhat from this example especially with regard to certificate validation.

If you configured the AT-WA7400 Wireless Access Point to use WPA/WPA2 Enterprise (RADIUS) security mode and to use either the built-in authentication server or an external RADIUS server that uses EAP/PEAP, perform the following procedure:

1. On the Security Settings page (Figure 12), verify that the Security Mode is set to WPA/WPA2.

Modify security settings that apply to the Internal Network

Broadcast SSID Allow Prohibit

Station Isolation Off On

Security Mode WPA/WPA2 Enterprise (RADIUS) ▼

Supported Client Stations

WPA ▼
 Enable pre-authentication

Cipher Suites

TKIP ▼

Authentication Server

Built-in ▼

Radius IP

127 . 0 . 0 . 1

Radius Key

XXXXXXXXXX

Enable radius accounting
 Allow non-WPA IEEE 802.1x clients

Figure 12. Security Settings Page

2. Set up user accounts on the access point (Cluster > User Management) as shown in Figure 13.

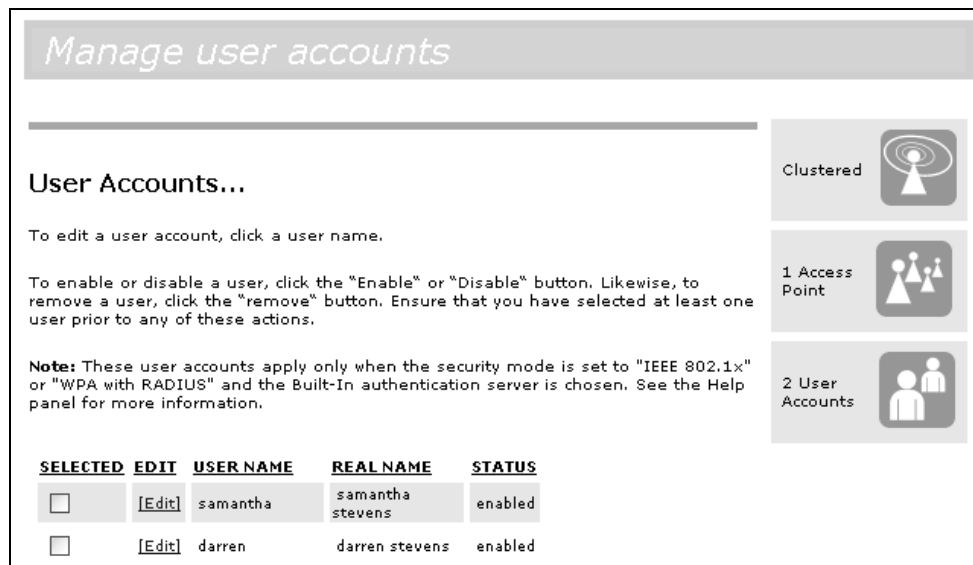


Figure 13. User Management Accounts Page

3. Then configure WPA security with PEAP authentication on each client as shown in Figure 14.

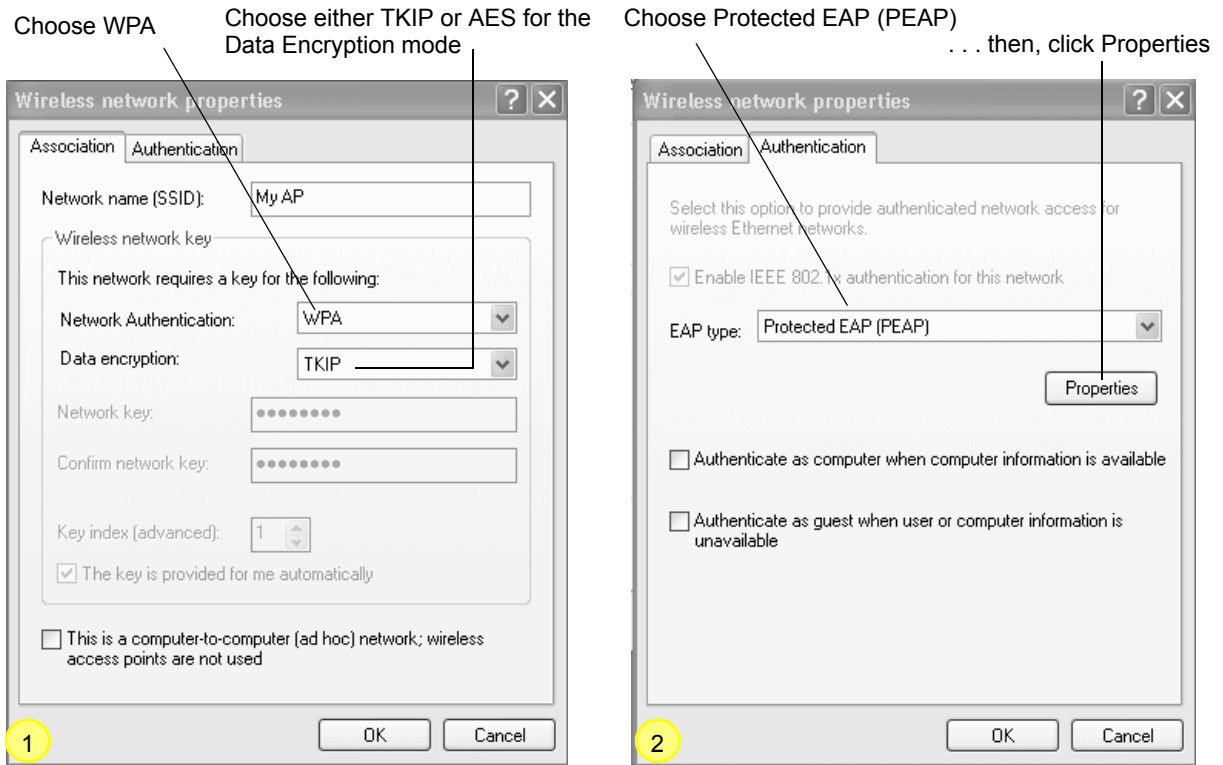


Figure 14. Wireless Network Properties Dialog Box

- Configure the following settings on the Association and Authentication tabs in the Network Properties dialog box.

Network Authentication

WPA

Data Encryption

TKIP or AES depending on how this option is configured on the access point.

Note

When the Cipher Suite on the access point is set to Both, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point.

- Configure this setting on the Authentication tab.

EAP Type

Choose Protected EAP (PEAP).

Click **Properties** to open the Protected EAP Properties dialog box as shown in Figure 15.

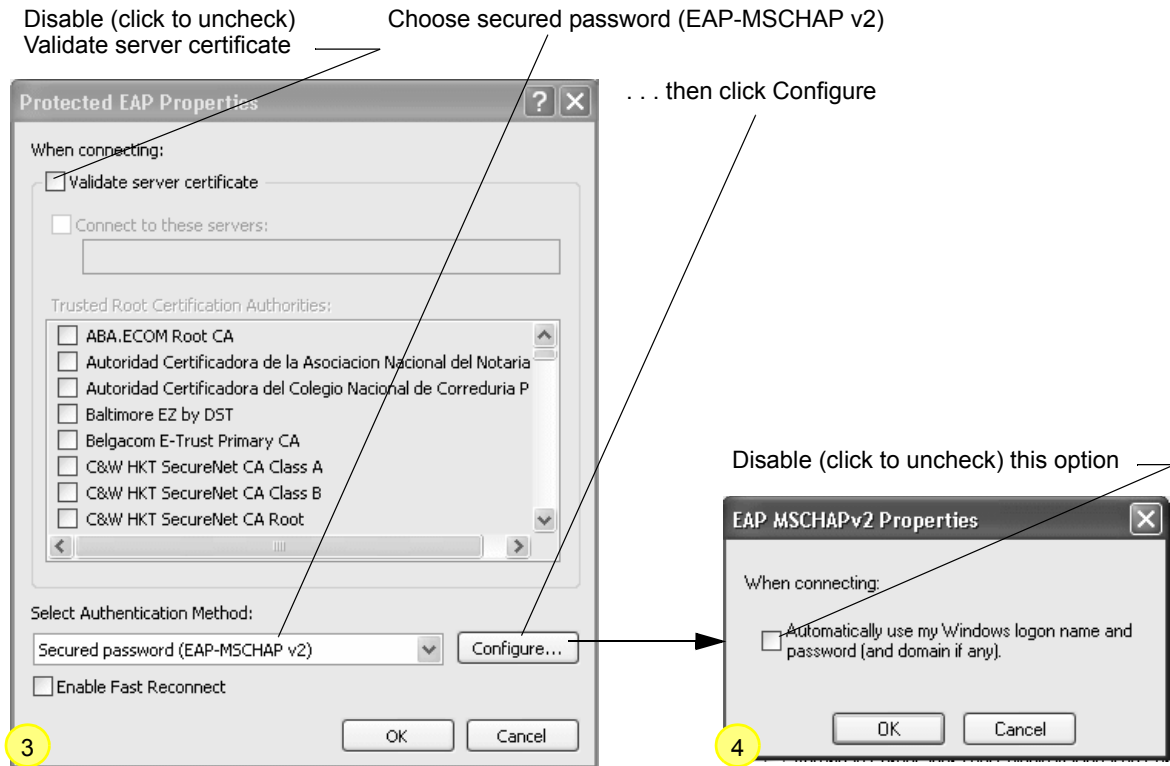


Figure 15. Protected AP Properties Dialog Box

6. Configure the following settings.

Validate Server Certificate

Disable this option (click to uncheck the box).

Note

This example assumes you are using the Built-in Authentication server on the access point. If you are setting up EAP/PEAP on a client of an access point that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.

Select Authentication Method

Choose “Secured password (EAP-MSCHAP v2)”

7. Click **Configure** to open the EAP MSCHAP v2 Properties dialog box.
8. Disable (click to uncheck) the option to “Automatically use my Windows login name etc.” so that upon login you will be prompted for user name and password.

- Click **OK** in all dialog boxes (starting with the EAP MSCHAP v2 Properties dialog) to close and save your changes.

WPA/WPA2 Enterprise (RADIUS) PEAP clients should now be able to associate with the access point. Client users will be prompted for a user name and password to authenticate with the network.

WPA/WPA2 Enterprise (RADIUS) Client Using EAP-TLS Certificate

Extensible Authentication Protocol (EAP) Transport Layer Security (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA/WPA2 Enterprise (RADIUS) and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.

Note

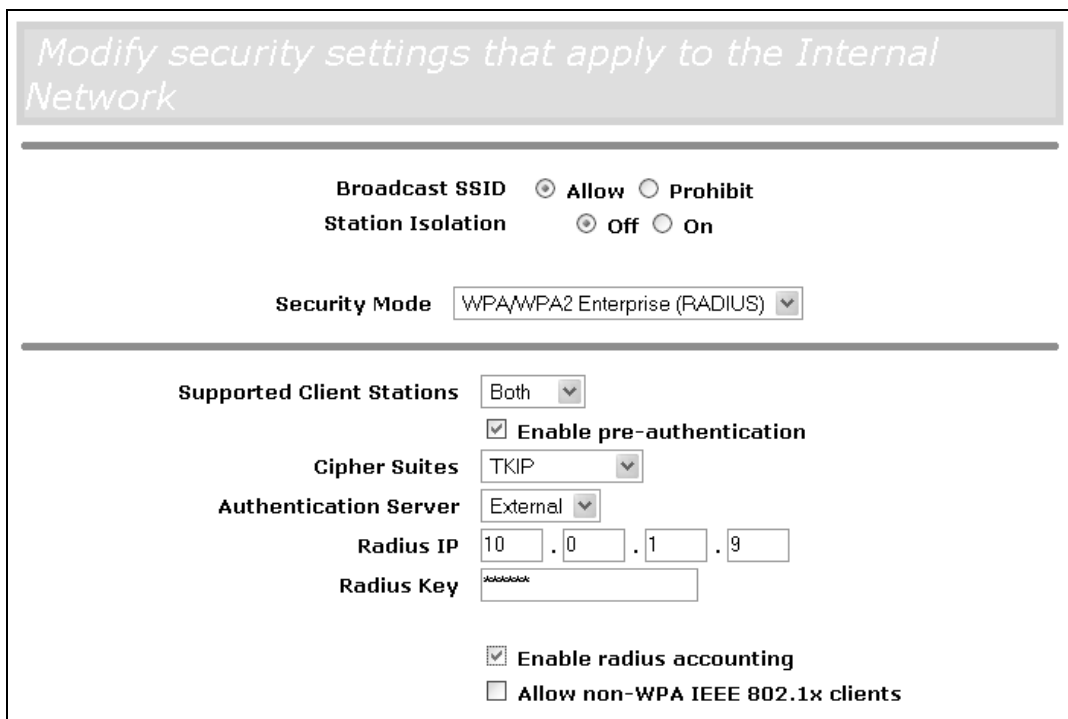
If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a Public Key Authority Infrastructure (PKI), including a Certificate Authority (CA), server configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

Some good starting points available on the web for the Microsoft Windows PKI software are: "How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881> and "How to Configure a Certificate Server" at <http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3>.

To use this type of security, you must do the following:

- Add the AT-WA7400 Wireless Access Point to the list of RADIUS server clients. (See "Configuring an External RADIUS Server to Recognize the AT-WA7400 Wireless Access Point" on page 248.)
- Configure the AT-WA7400 Wireless Access Point to use your RADIUS server by providing the RADIUS server IP address as part of the WPA/WPA2 Enterprise [RADIUS] security mode settings.
- Configure wireless clients to use WPA security and Smart Card or other Certificate as described in this section.
- Obtain a certificate for this client as described in "Obtaining a TLS-EAP Certificate for a Client" on page 253.

5. Verify that you configured the AT-WA7400 Wireless Access Point to use WPA/WPA2 Enterprise (RADIUS) security mode with an external RADIUS server, as shown in Figure 16.



Modify security settings that apply to the Internal Network

Broadcast SSID Allow Prohibit
Station Isolation Off On

Security Mode WPA/WPA2 Enterprise (RADIUS) ▼

Supported Client Stations Both ▼
 Enable pre-authentication

Cipher Suites TKIP ▼

Authentication Server External ▼

Radius IP 10 . 0 . 1 . 9

Radius Key *~*~*~*~*~*~*

Enable radius accounting
 Allow non-WPA IEEE 802.1x clients

Figure 16. Security Settings Page

6. Configure WPA security with certificate authentication on each client as shown in Figure 17.

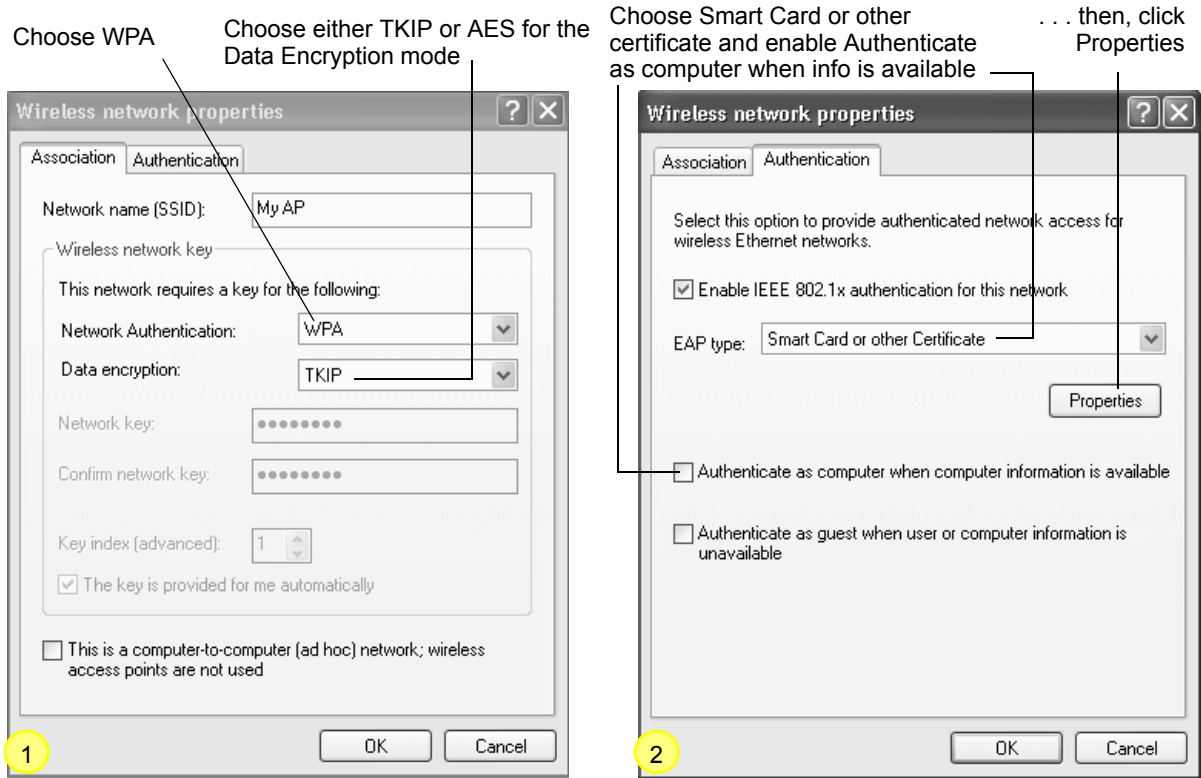


Figure 17. Association and Authentication Tabs

- Configure the following settings on the Association tab on the Network Properties dialog.

Network Authentication

WPA

Data Encryption

TKIP or AES depending on how this option is configured on the access point.

Note

When the Cipher Suite on the access point is set to Both, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point.

- Configure these settings on the Authentication tab.

Enable IEEE 802.1x authentication for this network

Enable (click to check) this option.

EAP Type

Choose Smart Card or other Certificate.

9. Click **Properties** to open the Smart Card or other Certificate Properties dialog and enable the “Validate server certificate” option, as shown in Figure 18.

Validate Server Certificate

Enable this option (click to check the box).

Certificates

In the certificate list shown, select the certificate for this client.

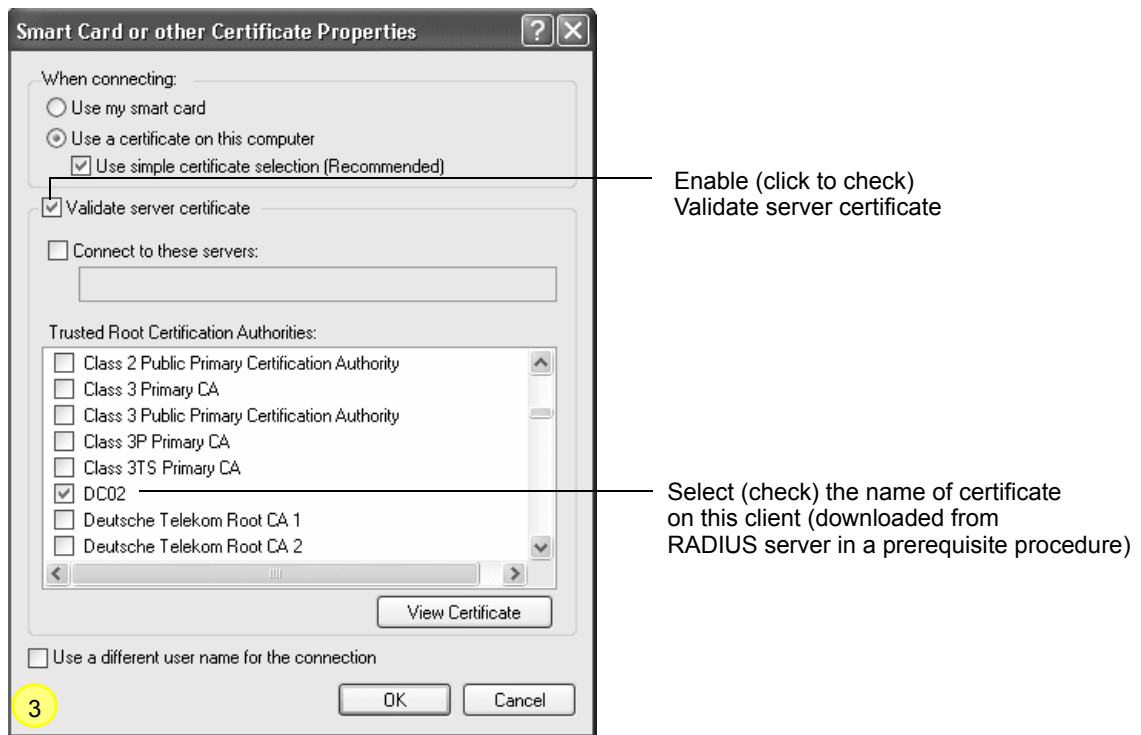


Figure 18. Smart Card or other Certificate Properties Dialog Box

10. Click **OK** in all dialog boxes to close and save your changes.
11. To complete the client configuration you must now obtain a certificate from the RADIUS server and install it on this client. For information on how to do this see “Obtaining a TLS-EAP Certificate for a Client” on page 253.

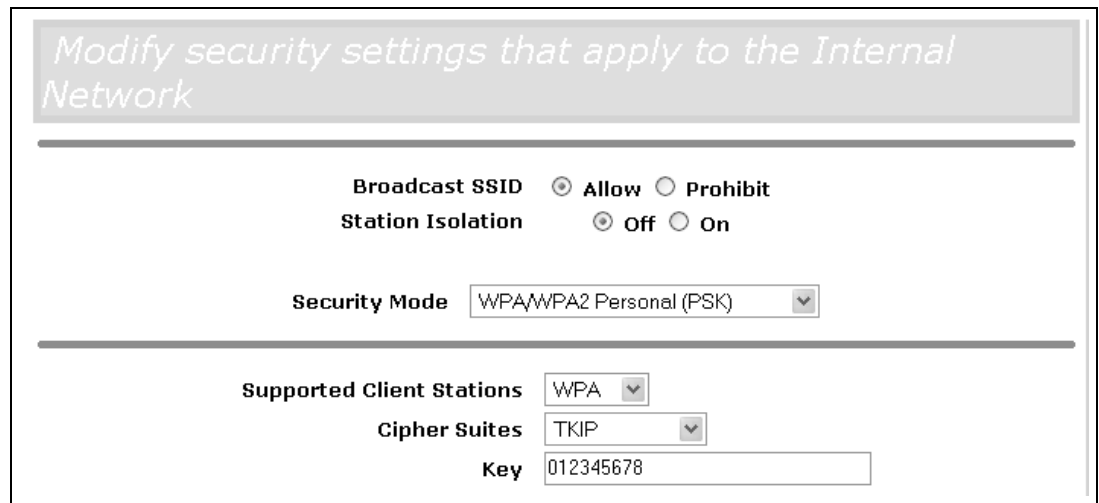
WPA clients should now be able to connect to the access point using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for login information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

Configuring WPA/WPA2 Personal (PSK) Security on a Client

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes Temporal Key Integrity Protocol (TKIP), Advanced Encryption Algorithm (AES), and Counter mode/CBC-MAC Protocol (CCMP) mechanisms. PSK employs a pre-shared key for an initial check of client credentials.

To configure WPA/WPA2 security on a client, perform the following procedure:

1. Verify that you configured the AT-WA7400 Wireless Access Point to use WPA/WPA2 Personal (PSK) security mode, as shown Figure 19.



Modify security settings that apply to the Internal Network

Broadcast SSID Allow Prohibit
Station Isolation Off On

Security Mode WPA/WPA2 Personal (PSK) ▼

Supported Client Stations WPA ▼
Cipher Suites TKIP ▼
Key 012345678

Figure 19. Security Settings Page

2. Configure WPA/WPA2 Personal (PSK) security on each client as shown in Figure 20.

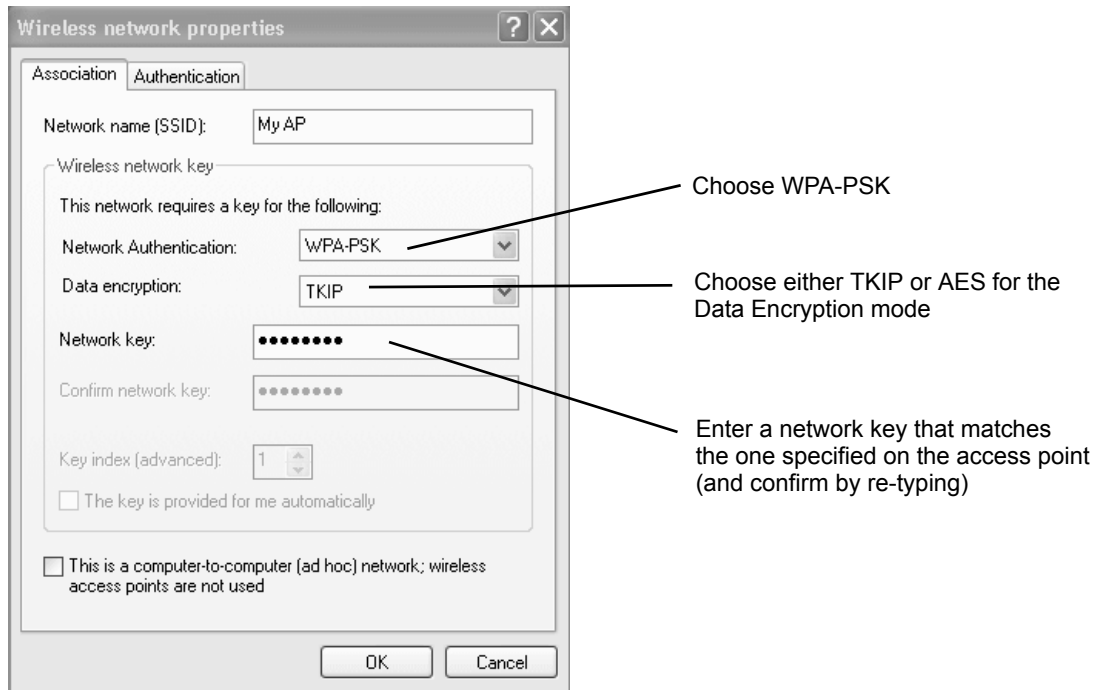


Figure 20. Association Tab

3. Configure the following settings on the Association tab:

Network Authentication

WPA-PSK

Data Encryption

TKIP or AES depending on how this option is configured on the access point.

Note

When the Cipher Suite on the access point is set to Both, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point.

Network Key

Provide the key you entered on the access point Security settings for the cipher suite you are using.

For example, if the key on the access point is set to use a TKIP key of "012345678," then a TKIP client specifies this same string as the network key.

The key is provided for me automatically

This box should be disabled automatically based on other settings.

4. Configure the following settings on the Authentication tab:

Enable IEEE 802.1x authentication for this network

Make sure that IEEE 802.1x authentication is disabled (unchecked).

(Setting the encryption mode to WEP should automatically disable authentication.)

5. Click **OK** in the Wireless Network Properties dialog box to close it and save your changes.

WPA-PSK clients should now be able to associate and authenticate with the access point. As a client, you are not prompted for a key. The TKIP or AES key you configured on the client security settings is automatically used when you connect.

Configuring an External RADIUS Server to Recognize the AT-WA7400 Wireless Access Point

An external Remote Authentication Dial-in User Server (RADIUS) server running on the network can support of EAP-TLS smart card/certificate distribution to clients in a Public Key Infrastructure (PKI) as well as EAP-PEAP user account setup and authentication. By external RADIUS server, we mean an authentication server external to the access point itself. This is to distinguish between the scenario in which you use a network RADIUS server versus one in which you use the built-in authentication server on the AT-WA7400 Wireless Access Point.

This section provides an example of configuring an external RADIUS server for the purposes of authenticating and authorizing TLS-EAP certificates from wireless clients of a particular AT-WA7400 Wireless Access Point configured for either WPA/WPA2 Enterprise (RADIUS) or IEEE 802.1x security modes. The intention of this section is to provide some idea of what this process will look like; procedures will vary depending on the RADIUS server you use and how you configure it. For this example, the Internet Authentication Service that is shipped with Microsoft Windows 2003 server is used.

Note

This document does not describe how to set up Administrative users on the RADIUS server. In this example, Allied Telesyn assumes that you already have RADIUS server user accounts configured. You will need a RADIUS server user name and password for both this procedure and the following one that describes how to obtain and install a certificate on the wireless client. Please consult the documentation for your RADIUS server for information on setting up user accounts.

The purpose of this procedure is to identify your AT-WA7400 Wireless Access Point as a client to the RADIUS server. The RADIUS server can then handle authentication and authorization of wireless clients for the access point. This procedure is required *per access point*. If you have more than one access point with which you plan to use an external RADIUS server, you need to follow these steps for each of those access points.

Keep in mind that the information you need to provide to the RADIUS server about the access point corresponds to settings on the access point (Advanced > Security) and vice versa. You should have already provided the RADIUS server IP Address to the access point. In the steps that follow, you provide the access point IP address to the RADIUS server. The RADIUS Key provided on the access point is the shared secret you will provide to the RADIUS server.

To configure an external RADIUS server, perform the following procedure:

1. On the Security Settings page, verify that the Authentication Server field is set to "External," as shown in Figure 21.

Modify security settings that apply to the Internal Network

Broadcast SSID Allow Prohibit
 Station Isolation Off On

Security Mode IEEE 802.1x

Authentication Server External

Radius IP 127 . 0 . 0 . 1

Radius Port 1812 (Range: 0-65535)

Radius Key ••••••

WPA Group Rekey Interval 1800 (Range: 30-1800)

Enable radius accounting

Figure 21. Security Settings Page

Note

The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. With firmware version 1.0 and greater, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are configurable. (The AT-WA7400 Management Software defaults to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)

2. Log on to the system hosting your RADIUS server and open the Internet Authentication Service window (Figure 22).

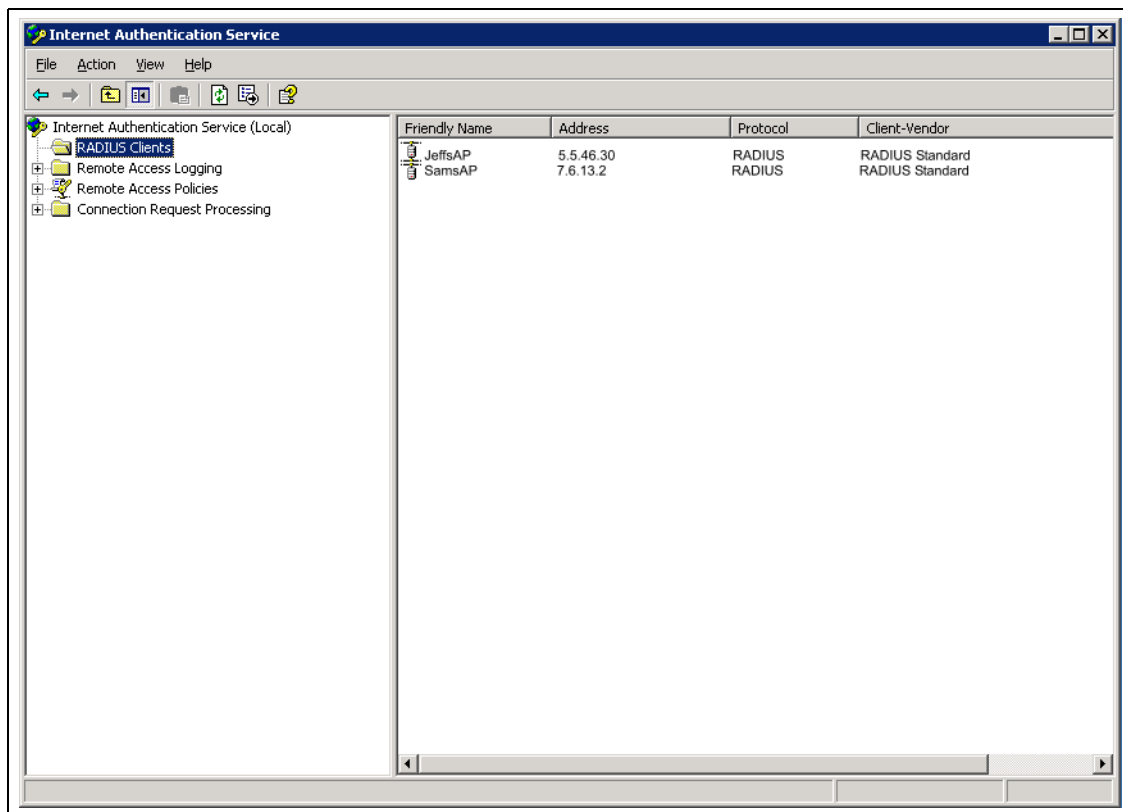
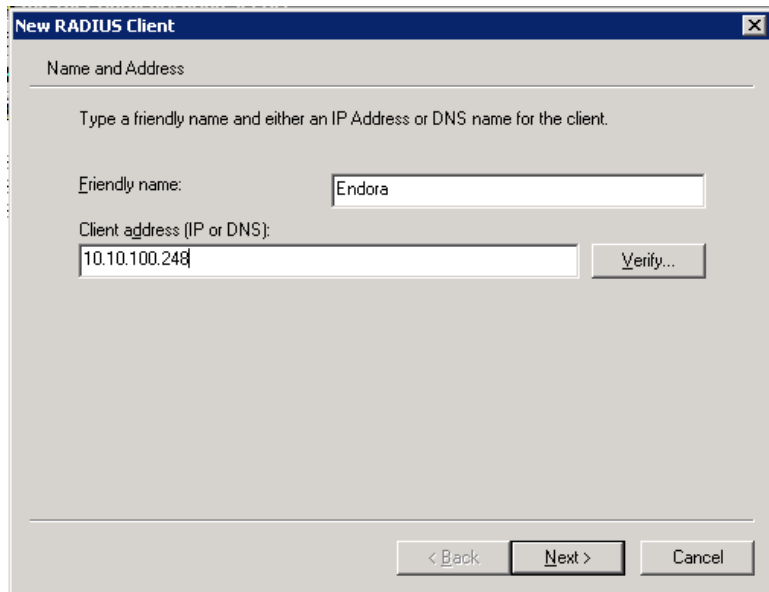


Figure 22. Internet Authentication Service Window

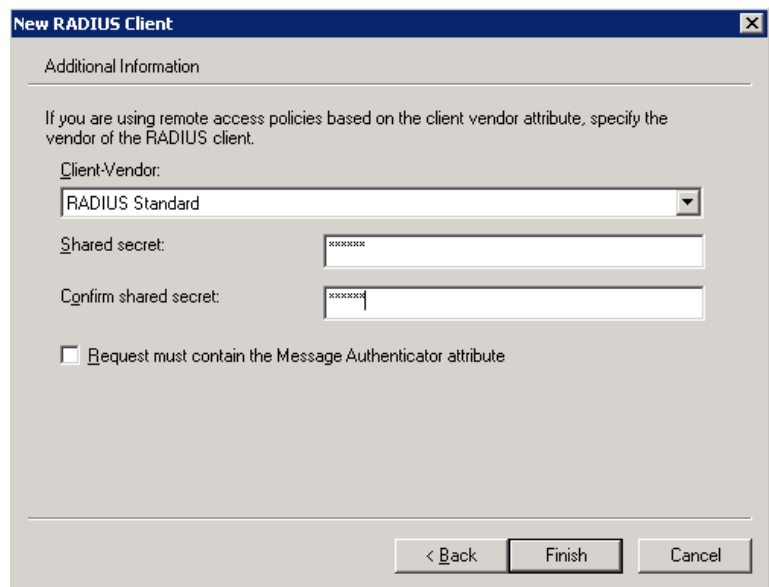
3. In the left panel, right click on the RADIUS Clients node and choose New > Radius Client from the menu.
4. On the first dialog box of the New RADIUS Client wizard (Figure 23) provide information about the AT-WA7400 Wireless Access Point to which you want your clients to connect:
 - A logical (friendly) name for the access point. (You might want to use DNS name or location.)
 - IP address for the access point.



The dialog box is titled "New RADIUS Client" and has a tab labeled "Name and Address". Below the tab, there is a section titled "Name and Address" with the instruction: "Type a friendly name and either an IP Address or DNS name for the client." There are two input fields: "Friendly name:" with the text "Endora" and "Client address (IP or DNS):" with the text "10.10.100.248". A "Verify..." button is located to the right of the client address field. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Figure 23. New RADIUS Client Dialog Box, Name and Address Dialog Box

5. Click **Next**.
6. For the Shared secret, enter the RADIUS Key you provided to the access point (on the Advanced > Security page) as shown in Figure 24.



The dialog box is titled "New RADIUS Client" and has a tab labeled "Additional Information". Below the tab, there is a section titled "Additional Information" with the instruction: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client." There is a "Client-Vendor:" dropdown menu with "RADIUS Standard" selected. Below this are two input fields for "Shared secret:" and "Confirm shared secret:", both containing masked text (asterisks). At the bottom, there is a checkbox labeled "Request must contain the Message Authenticator attribute" which is currently unchecked. At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".

Figure 24. New RADIUS Client Wizard Additional Information Dialog Box

7. Re-type the key to confirm.
8. Click **Finish**.

The access point is now displayed as a client of the Authentication Server (Figure 25).

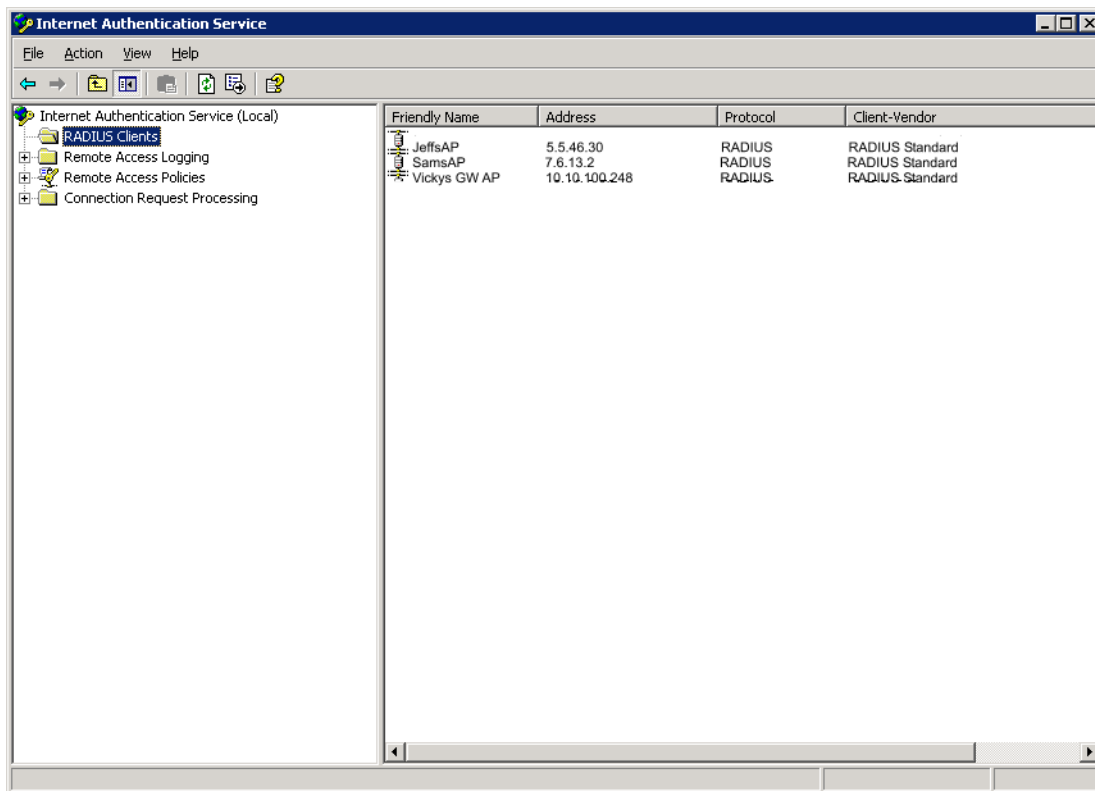


Figure 25. Internet Authentication Service Window Showing Access Point

Obtaining a TLS-EAP Certificate for a Client

Note

If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a *Public Key Authority Infrastructure* (PKI), including a *Certificate Authority* (CA), server configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

Some good starting points available on the web for the Microsoft Windows PKI software are: "How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881> and "How to Configure a Certificate Server" at <http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3>.

Wireless clients configured to use either WPA/WPA2 Enterprise (RADIUS) or IEEE 802.1x security modes with an external RADIUS server that supports TLS-EAP certificates must obtain a TLS certificate from the RADIUS server.

This is an initial one-time step that must be completed on each client that uses either of these modes with certificates. In this procedure, we use the Microsoft Certificate Server as an example.

To obtain a certificate for a client, perform the following procedure:

1. Go to the following URL in a web browser:

`https://IPAddressOfServer/certsrv/`

Where *IPAddressOfServer* is the IP address of your external RADIUS server, or of the Certificate Authority (CA), depending on the configuration of your infrastructure, as shown in Figure 26.



Figure 26. Security Alert Window

2. Click **Yes** to open the secure web page for the server.

The Welcome page for the Certificate Server is displayed in the browser, as shown in Figure 27.

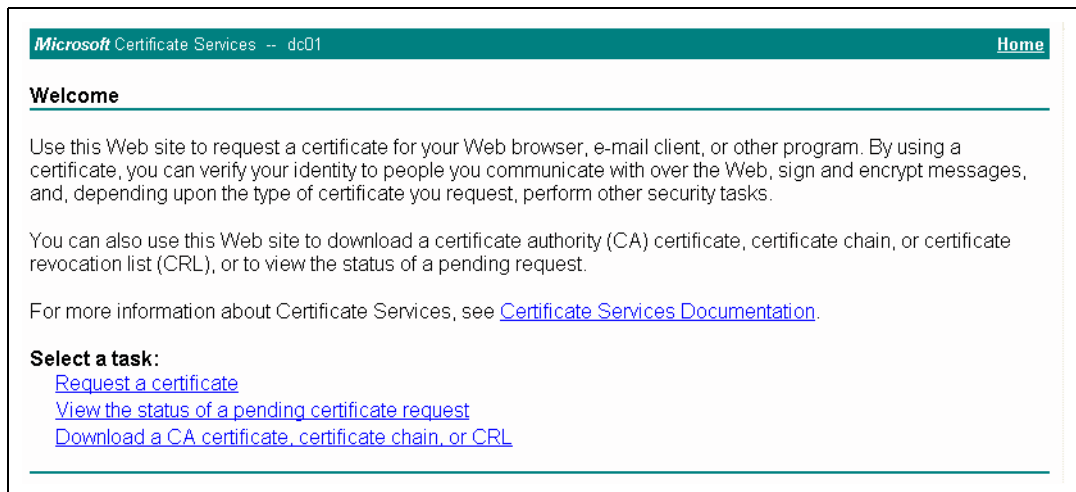


Figure 27. Certificate Server Welcome Page

3. Click **Request a certificate**.

The login window for the RADIUS server opens, as shown in Figure 28.



Figure 28. RADIUS Server Login Window

4. Provide a valid user name and password to access the RADIUS server.

Note

The user name and password you need to provide here is for access to the RADIUS server, for which you will already have user accounts configured at this point. This document does not describe how to set up Administrative user accounts on the RADIUS server. Please consult the documentation for your RADIUS server for these procedures.

The Request a Certificate page opens, as shown in Figure 29.

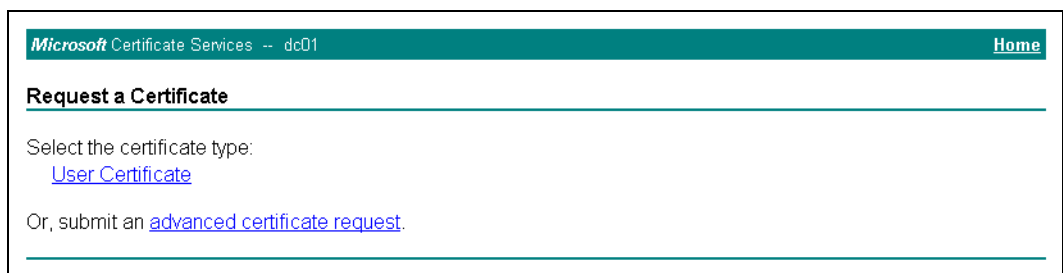


Figure 29. Request a Certificate Page

5. Click **User Certificate**.

The Security Warning dialog box opens, as shown in Figure 30.

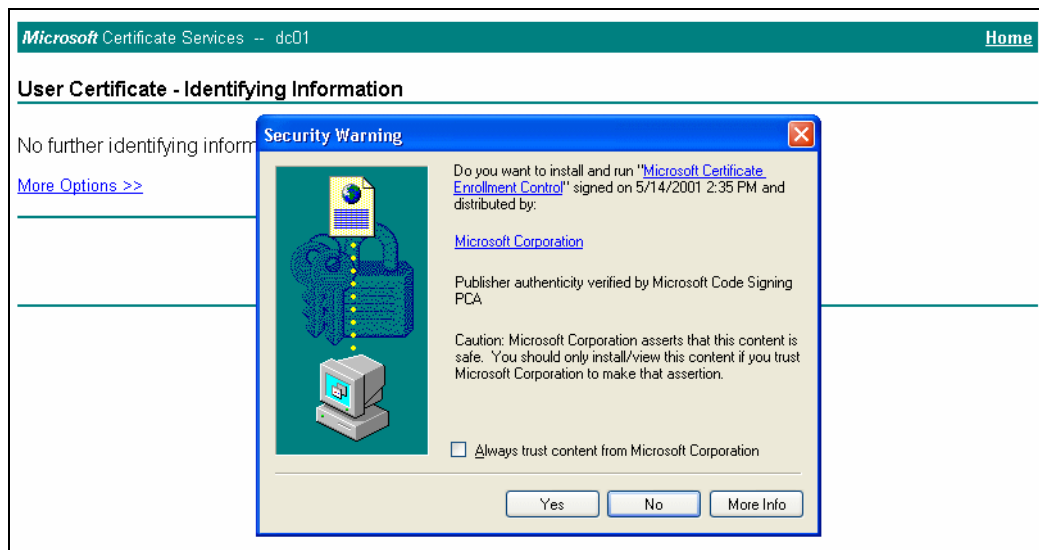


Figure 30. Security Warning Dialog Box

6. Click **Yes**.

The User Certificate dialog box opens, as shown in Figure 31.

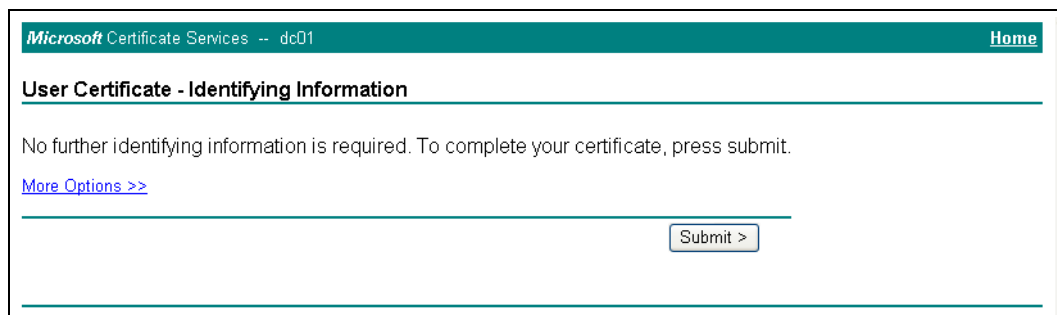


Figure 31. User Certificate Dialog Box

7. Click **Submit** to complete.

The Potential Scripting Violation dialog box opens, as shown in Figure 32.

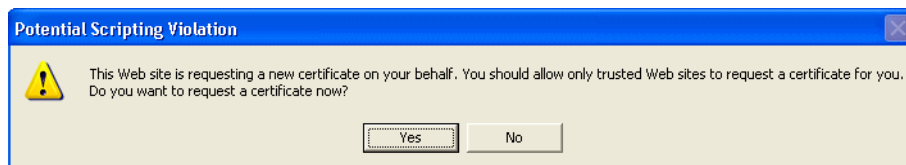


Figure 32. Potential Scripting Violation Dialog Box

8. Click **Yes**.

The Certificate Issued dialog box opens, as shown in Figure 33.

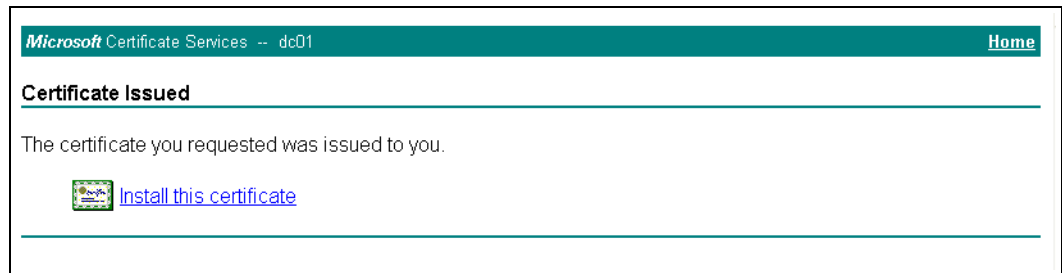


Figure 33. Certificate Issued Dialog Box

9. Click **Install this certificate** to install the newly issued certificate on your client station.

The Potential Scripting Violation dialog box opens, as shown in Figure 34.

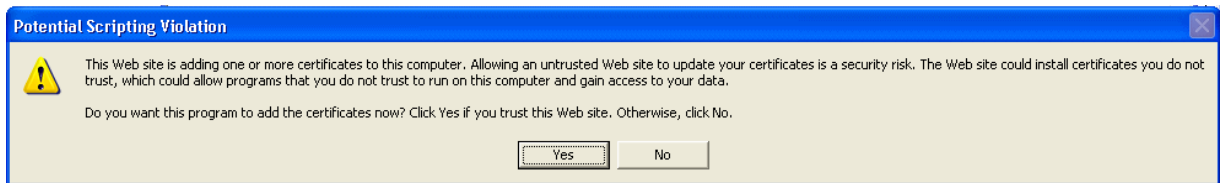


Figure 34. Potential Scripting Error Dialog Box

10. Click **Yes**.

The Root Certificate Store dialog box is displayed, as shown in Figure 35.

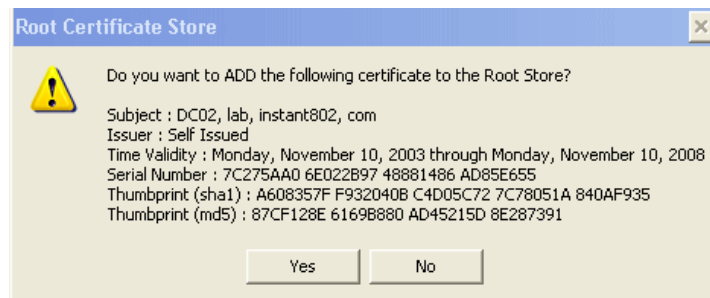


Figure 35. Root Certificate Store Dialog Box

11. Click **Yes**.

A success message (Figure 36) is displayed indicating the certificate is now installed on the client.

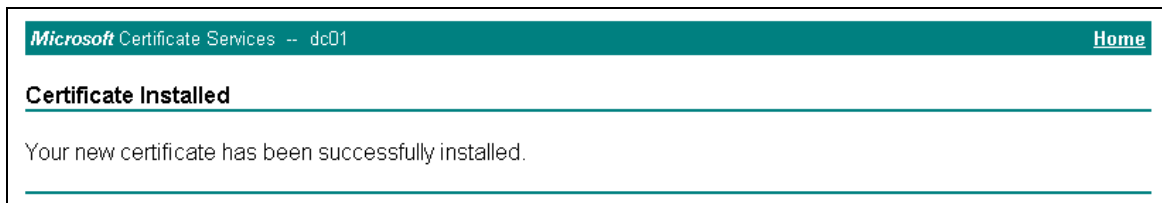


Figure 36. Certificate Installed Confirmation Window

Appendix C

Troubleshooting

This appendix provides information about how to solve common problems you might encounter in the course of updating network configurations on networks served by multiple, clustered access points. This appendix includes the following sections:

- ❑ “Wireless Distribution System (WDS) Problems and Solutions” on page 260
- ❑ “Cluster Recovery” on page 261

Wireless Distribution System (WDS) Problems and Solutions

If you are having trouble configuring a WDS link, read the following list of guidelines for configuring WDS. The most common problem Administrators encounter with WDS setups is forgetting to set both access points in the link to the same radio channel and IEEE 802.11 mode.

The following list summarizes some critical guidelines regarding WDS configuration:

- ❑ The only security mode available on the WDS link is Static WEP, which is not particularly secure. Therefore, Allied Telesyn recommends that you use WDS to bridge the guest network only for this release. Do not use WDS to bridge access points on the internal network unless you are not concerned about the security risk for data traffic on that network.
- ❑ When you use WDS, be sure to configure WDS settings on *both* access points participating in the WDS link.
- ❑ You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.
- ❑ Both access points participating in a WDS link must be on the same radio channel and using the same IEEE 802.11 mode. (See “Configuring Radio Settings” on page 147 for information on configuring the Radio mode and channel.)
- ❑ **Do not create loops** with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. *Spanning Tree Protocol* (STP), which manages path redundancy and prevent unwanted loops, is not enabled for this release. Keep these rules in mind when working with WDS on this release of the AT-WA7400 Management Software:
 - ❑ Any two access points can be connected by only a single path; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both.
 - ❑ Do not create backup links.
 - ❑ If you can trace more than one path between any pair of access points going through any combination of Ethernet or WDS links, you have a loop.
 - ❑ You can only extend or bridge either the internal or guest network but not both.

Cluster Recovery

In cases where the access points in a cluster become out of sync or an access point cannot join or be removed from a cluster, the following methods for cluster recovery are recommended.

Reboot or Reset the Access Point

These recovery methods are given in the order you should try them. In all but the last case (stop clustering), you only need to reset or reboot the particular access point whose configuration is out of sync with other cluster members or cannot remove/join the cluster.

- ❑ Reboot the access point from its web UI. To do this, go to `http://IPAddressOfAccessPoint`, navigate to **Advanced > Reboot** and click **Reboot**. (IP addresses for access points are on the Cluster > Access Points page for cluster members.)
- ❑ Physically reboot the access point by pressing the Reset button on the AT-WA7400 Wireless Access Point.
- ❑ Reset the access point from its web UI. To do this, go to `http://IPAddressOfAccessPoint`, navigate to **Advanced > Reset Configuration**, and click **Reset**. (IP addresses for access points are on the Cluster > Access Points page for any cluster member.)
- ❑ Physically reset the access point by pressing the Reset button on the device.
- ❑ In some extreme cases, reboot or reset may not solve the problem. In these cases, follow the procedure described next in “Stop Clustering and Reset Each Access Point in the Cluster” to recover every access point on the subnet.

Stop Clustering and Reset Each Access Point in the Cluster

If the previous reboot or reset methods do not solve the problem, do the following to stop clustering and reset all access points:

1. Enter the Stop Clustering command as part of the URL in the address bar of your web browser as follows:

```
http://IPAddressOfAccessPoint/stop_clustering.cgi
```

Where *IPAddressOfAccessPoint* is the IP address of the access point you want to stop clustering. You can find the IP addresses for the cluster members on the Cluster > Access Points page for any of the clustered access points. Allied Telesyn recommends making a note of all IP addresses at this point.

The Stop Clustering page for this access point is displayed, as shown in Figure 37.

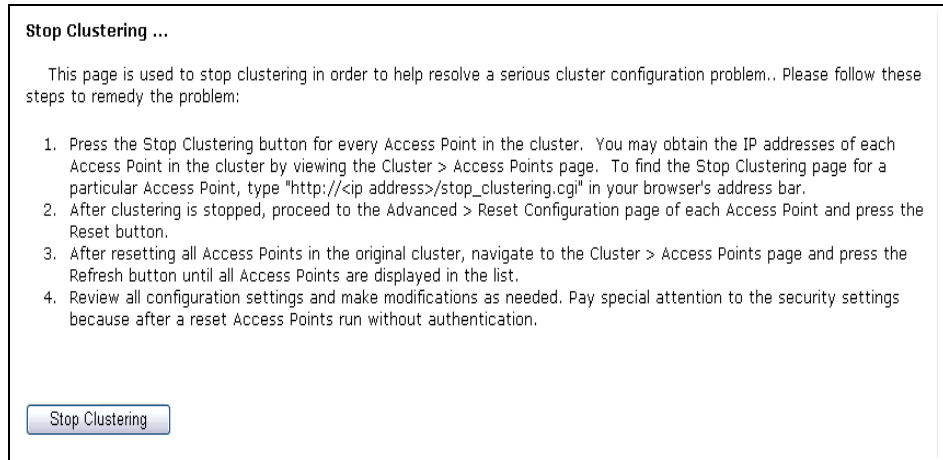


Figure 37. Stop Clustering Page

2. Click **Stop Clustering**.

Repeat this stop clustering step for every access point in the cluster.



Caution

Do not proceed to the next step of resetting any access points until you have stopped clustering on all of them. Make sure that you first stopping clustering on every access point on the subnet, and only then perform the next part of the process of resetting each one to the factory defaults.

3. Go to the web pages of the access point you want to reset by entering its URL into the address bar of your web browser:

`http://IPAddressOfAccessPoint/`

Where *IPAddressOfAccessPoint* is the IP address of the access point you want to reset.

4. From the main menu, choose **Advanced > Reset Configuration**.

The Reset Configuration page is shown in Figure 38.

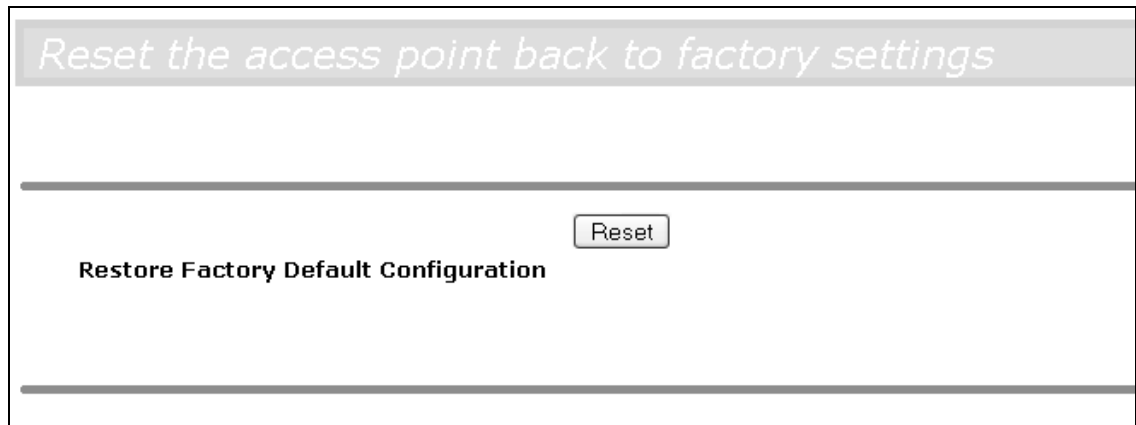


Figure 38. Reset Configuration Page

5. Click **Reset** to restore the factory defaults on the access point. (This will clear all of your previous settings, including updated passwords.)
6. Repeat this reset step for every access point in the cluster.



Caution

Do not proceed to the next step until you have stopped clustering on all of access points in the pre-existing cluster.

7. From the main menu of any access point, select **Cluster > Access Points**.

The Cluster Management page is shown in Figure 39.

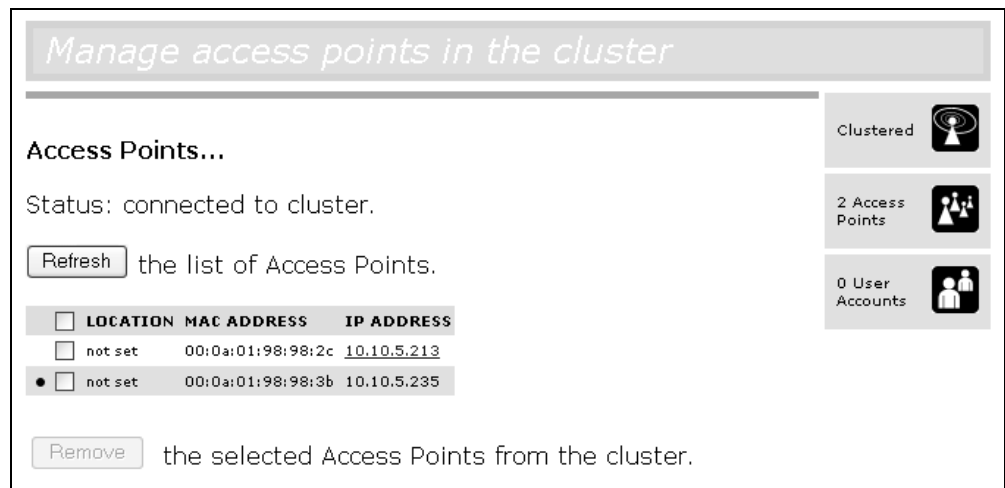


Figure 39. Cluster Management Page

8. Click **Refresh**.

All previous cluster members are displayed in the list.

Before proceeding to the last step, verify that the cluster has reformed by making sure all access points are listed.

9. Review all configuration settings and make modifications as needed.

Pay special attention to the security settings because after a reset, access points run without any security in place.

Appendix D

Command Line Interface (CLI) for Access Point Configuration

In addition to the web-based user interface, the AT-WA7400 Wireless Access Point includes a command line interface (CLI) for administering the access point. The CLI lets you view and modify status and configuration information.

From the client station perspective, even a single deployed AT-WA7400 Wireless Access Point broadcasting its network name to clients constitutes a wireless network. Keep in mind that CLI configuration commands, like web UI settings, can affect a single access point running in standalone mode or automatically propagate to a network of clustered access points that share the same settings. (For more information on clustering, see “Understanding Clustering” on page 44. For information on how to set an access point to standalone or cluster mode from the web interface, see “Cluster Mode” on page 46 and “Standalone Mode” on page 46.)

The following topics provide an introduction to the class structure upon which the CLI is based, CLI commands, and examples of using the CLI to get or set configuration information on an access point or cluster of access points:

- ❑ “Comparison of Settings Configurable with the CLI and Web UI” on page 266
- ❑ “Accessing the CLI for an Access Point” on page 269
- ❑ “Quick View of Commands and How to Get Help” on page 272
- ❑ “Command Usage and Configuration Examples” on page 278
- ❑ “Keyboard Shortcuts and Tab Completion Help” on page 349
- ❑ “CLI Classes and Fields Reference” on page 354

Comparison of Settings Configurable with the CLI and Web UI

The command line interface (CLI) and the web user interface (UI) to the AT-WA7400 Wireless Access Point are designed to suit the preferences and requirements of different types of users and scenarios. Most administrators will probably use both UIs in different contexts. Some features (such as clustering) can only be configured through the web UI and, conversely, some details and more complex configurations are only available through the CLI.

The CLI is particularly useful because it provides an interface to which you can write programmatic scripts for access point configurations. The CLI may also be less resource-intensive than a web interface.

Table 2 shows a feature-by-feature comparison of which settings can be configured through the CLI or the web UI, and which are configurable with either.

Table 2. Comparison of CLI to Web Browser Interface Settings

| Feature or Setting | Configurable from CLI | Configurable from Web |
|---|---|---|
| Basic Settings Getting/changing Administrator Password Getting/changing access point name and location Viewing information such as MAC, IP address, and firmware version | Yes | Yes |
| Access Point and Cluster Settings | Get existing settings only. You cannot set configuration <i>policy</i> or other cluster features from the CLI. Use for clustering settings. | Yes |
| User Accounts | Yes | Yes |
| User Database Backup and Restore | No | Yes, as described in “Backing Up and Restoring a User Database” on page 62. |
| Sessions | No | Yes |
| Channel Management | No | Yes, as described in Chapter 6, “Channel Management” on page 69 |

Table 2. Comparison of CLI to Web Browser Interface Settings (Continued)

| Feature or Setting | Configurable from CLI | Configurable from Web |
|--|--|--|
| Wireless Neighborhood | No | Yes, as described in Chapter 7, "Wireless Neighborhoods" on page 79. |
| Displaying Status | Yes | Yes |
| Ethernet (Wired) Interface | Yes You can configure all Ethernet (Wired) settings from the CLI except the Connection Type. To change the Connection Type from DHCP to Static IP addressing (or vice versa), you must use the web UI. | Yes |
| Setting Up the Wireless Interface | Yes | Yes |
| Setting Up Security | Yes | Yes |
| Enabling and Configuring the Guest Login Welcome Page | Yes | Yes |
| Configuring Multiple BSSIDs on Virtual Wireless Networks | Yes | Yes |
| Radio Settings | Yes You can configure all radio settings from the CLI except for turning on/off Super AG. | Yes |
| MAC Filtering | Yes | Yes |
| Load Balancing | Yes | Yes |
| Quality of Service | Yes | Yes |
| Wireless Distribution System | Yes | Yes |
| Time Protocol | Yes | Yes |
| Rebooting the Access Point | Yes | Yes |
| Resetting the Access Point to the Factory Defaults | Yes | Yes |
| Upgrade the Firmware | No | Yes, as described in "Upgrading the Firmware" on page 207. |

Table 2. Comparison of CLI to Web Browser Interface Settings (Continued)

| Feature or Setting | Configurable from CLI | Configurable from Web |
|---------------------------|------------------------------|--|
| Back Up and Restore | No | Yes, as described in Chapter 18, “Backing Up and Restoring a Configuration” on page 211. |

Accessing the CLI for an Access Point

You can use any of these methods to access the CLI for the access point or wireless network:

- “Telnet Connection to the Access Point,” next
- “SSH Connection to the Access Point” on page 270

Telnet Connection to the Access Point

If you know already have your network deployed and know the IP address of your access point, you can use a remote Telnet connection to the access point to view the system console over the network.

Note

The default Static IP address is 192.168.1.230. If there is no DHCP server on the network, the access point retains this static IP address at first-time startup. You can use KickStart to find the IP address of the access point. (For more about IP addressing, see “Understanding Dynamic and Static IP Addressing on the AT-WA7400 Management Software” on page 23.)

To make a Telnet connection to the AT-WA7400 Wireless Access Point, perform the following procedure:

1. Open a command window on your PC.

(For example, from the system tray on the desktop choose Start > Run to bring up the Run dialog, and type cmd in the Open field, and click **OK**.)

2. At the command prompt, type the following:

```
telnet IPAddressOfAccessPoint
```

where *IPAddressOfAccessPoint* is the address of the access point you want to monitor.

(If your Domain Name Server is configured to map domain names to IP addresses via DHCP, you can also telnet to the domain name of the access point.)

3. You will be prompted for an Administrator user name and password for the access point.

```
AT-WA7400 login:
```

```
Password:
```

Enter the default Administrator username and password for the AT-WA7400 Wireless Access Point (manager, friend), and press

Enter after each. (The password is masked, so it will not be displayed on the screen.)

When the user name and password is accepted, the screen displays the AT-WA7400 Wireless Access Point help command prompt.

AT-WA7400 login: **manager**

Password: **friend**

Enter 'help' for help.

You are now ready to enter CLI commands at the command line prompt.

SSH Connection to the Access Point

If you know already have your network deployed and know the IP address of your access point, you can use a remote SSH connection to the access point to view the system console over the network.

Note

The default Static IP address is 192.168.1.230. If there is no DHCP server on the network, the access point retains this static IP address at first-time startup. You can use KickStart to find the IP address of the access point. (For more about IP addressing, see “Understanding Dynamic and Static IP Addressing on the AT-WA7400 Management Software” on page 23.)

Using an SSH connection to the access point is similar to Telnet because it gives you remote access to the system console and CLI. SSH has the added advantage of being a secure connection traffic encrypted.

To use an SSH connection, you need to have SSH software installed on your PC (such as PuTTY, which is available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/>).

1. Start your SSH application. (PuTTY is used here as an example.)

The PuTTY settings are shown in Figure 40.

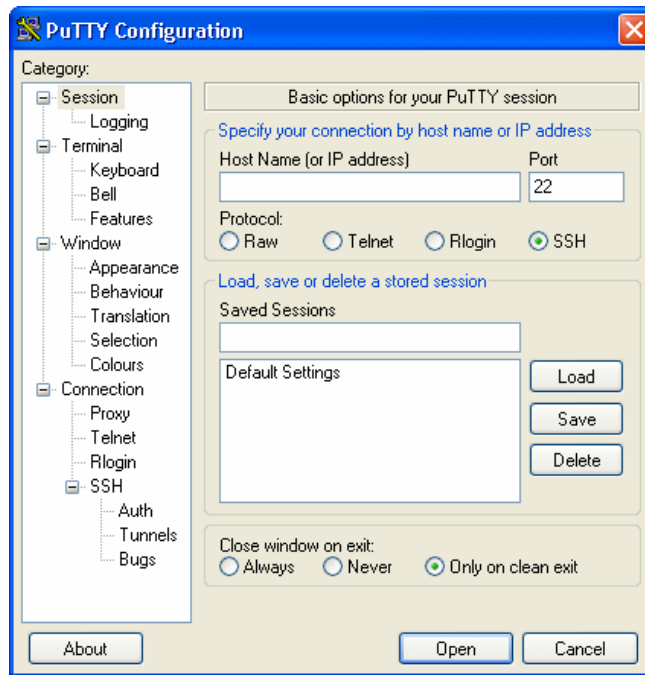


Figure 40. PuTTY Configuration Dialog Box

2. Enter the IP address of access point and click **Open**.

(If your Domain Name Server is configured to map domain names to IP addresses via DHCP, you can enter the domain name of the access point instead of an IP address.)

This brings up the SSH command window and establishes a connection to the access point. The login prompt is displayed.

login as:

3. Enter the default Administrator username and password for the AT-WA7400 Wireless Access Point (`manager`, `friend`), and press Enter after each. (The password is masked, so it will not be displayed on the screen.)

login as: **manager**

admin@10.10.100.110's password:

Enter 'help' for help.

When the user name and password is accepted, the screen displays the AT-WA7400 Wireless Access Point help command prompt.

AT-WA7400#

You are now ready to enter CLI commands at the command line prompt.

Quick View of Commands and How to Get Help



Caution

Settings you update from the CLI (with the **get**, **set**, **add**, and **remove** commands) are not saved to the startup configuration unless you explicitly save them using the **save-running** command. For a description of configurations maintained on the access point and details on how to save your updates, see “Saving Configuration Changes” on page 281.

Commands and Syntax

The CLI for the AT-WA7400 Wireless Access Point provides the commands shown in Table 3.

Note

- *named_class* is a class of an object from the configuration whose instances are individually named.

- *instance* is a name of an instance of class.

- field values cannot contain spaces unless the value is in quotes

For a detailed class and field reference, see “CLI Classes and Fields Reference” on page 354.

Table 3. Commands and Syntax

| Command | Description |
|---------|--|
| get | <p>The get command allows you to get the field values of existing instances of a class.</p> <p>Classes can be named or unnamed. The command syntax is: get unnamed-class [<i>field</i> ... detail] get named-class [<i>instance</i> all [<i>field</i> ... <i>name</i> detail]]</p> <p>The rest of the command line is optional. If provided, it is either a list of one or more <i>fields</i>, or the keyword detail.</p> <p>An example of using the get command on an unnamed class with a single instance is: get log (There is only one log on the access point. This command returns information on the log file.)</p> <p>An example of using the get command on an unnamed class with multiple instances is: get log-entry (There are multiple log entries but they are not named. This command returns all log entries.)</p> <p>An example of using the get command on a named class with multiple instances is: \get bss wlan0bssInternal (There are multiple bss's and they are named. This command returns information on the BSS named wlan0bssInternal.)</p> <p>An example of using the get command on a named class to get all instances: get radius-user all name get radius-user all</p> <p>Note: wlan0bssInternal is the name of the basic service set (BSS) on the internal network (wlan0 interface). For information on <i>interfaces</i>, see "Understanding Interfaces as Presented in the CLI" on page 278.</p> |

Table 3. Commands and Syntax (Continued)

| Command | Description |
|---------|--|
| set | <p>The set command allows you to set the field values of existing instances of a class, for example:</p> <pre>set <i>unnamed-class</i> [with <i>qualifier-field</i> <i>qualifier-value</i> ... to] <i>field value</i> . . .</pre> <p>The first argument is an unnamed class in the configuration. After this is an optional qualifier that restricts the set to only some instances. For singleton classes (with only one instance) no qualifier is needed. If there is a qualifier, it starts with the keyword with, then has a sequence of one or more <i>qualifier-field</i> <i>qualifier-value</i> pairs, and ends with the keyword to. If these are included, then only instances whose present value of <i>qualifier-field</i> is <i>qualifier-value</i> will be set. The <i>qualifier-value</i> arguments cannot contain spaces. Therefore, you cannot select instances whose desired <i>qualifier-value</i> has a space in it. The rest of the command line contains <i>field-value</i> pairs.</p> <pre>set <i>named-class instance</i> all [with <i>qualifier-field</i> <i>qualifier-value</i> ... to] <i>field value</i> . . .</pre> <p>The first argument is either a named class in the configuration. The next argument is the name of the <i>instance</i> to set, or the keyword all, which indicates that all instances should be set. Classes with multiple instances can be set consecutively in the same command line as shown in Example 4 below. The <i>qualifier-value</i> arguments cannot contain spaces.</p> <p>Here are some examples. (Bold text indicates class names, field names or keywords; the unbold text are values to which the fields are being set.)</p> <ol style="list-style-type: none"> 1. set interface wlan0 ssid "Vicky's AP" 2. set radio all beacon-interval 200 3. set tx-queue wlan0 with queue data0 to aifs 3 4. set tx-queue wlan0 with queue data0 to aifs 7 cwmin 15 cwmax 1024 burst 0 5. set bridge-port br0 with interface eth0 to path-cost 200 <p>Note: For information on <i>interfaces</i> used in this example (such as wlan0, br0, or eth0) see "Understanding Interfaces as Presented in the CLI" on page 278.</p> |
| add | <p>The add command allows you to add a new instance of a class.</p> <pre>add <i>named-class instance</i> [<i>field value</i> ...] add <i>anonymous-class</i> [<i>field value</i> ...]</pre> <p>For example:</p> <pre>add radius-user wally</pre> |

Table 3. Commands and Syntax (Continued)

| Command | Description |
|---------------|---|
| remove | <p>The remove command allows you to remove an existing instance of a class.</p> <pre>remove <i>unnamed-class</i> [<i>field value</i> . . .]</pre> <pre>remove <i>named-class instance</i> all [<i>field value</i> . . .]</pre> <p>For example: remove radius-user wally</p> |
| save-running | <p>The save-running command saves the running configuration as the startup configuration.</p> <p>For more information, see “Saving Configuration Changes” on page 281.</p> |
| reboot | <p>The reboot command restarts the access point (a soft reboot).</p> <p>For more information, see “Rebooting the Access Point” on page 348.</p> |
| factory-reset | <p>The factory-reset command resets the access point to factory defaults and reboots.</p> <p>For more information, see “Resetting the Access Point to the Factory Defaults” on page 348.</p> |

Getting Help on Commands at the CLI

To get help on commands, at the CLI prompt, use the TAB key. This is a quick way to see all valid completions for a class.

Press TAB once to complete the current command.

If multiple completions exist, a beep is sounded and no results are displayed. Press TAB again to display all available completions.

- **Example 1:** At a blank command line, press TAB twice to get a list of all commands.

```
AT-WA7400#
```

```
add                Add an instance to the running configuration
factory-reset      Reset the system to factory defaults
get                Get field values of the running configuration
reboot             Reboot the system
remove             Remove instances in the running configuration
save-running       Save the running configuration
set                Set field values of the running configuration
```

- **Example 2:** Type `get TAB TAB` (including a space after `get`) to see a list of all field options for the `get` command.

```
AT-WA7400# get
association      Associated station
basic-rate      Basic rates of radios
bridge-port     Bridge ports of bridge interfaces
bss             Basic Service Set of radios
cluster         Clustering-based configuration settings
cluster-member  Member of a cluster of like-configured access
                points
config         Configuration settings
detected-ap    Detected access point
dhcp-client    DHCP client settings
dot11          IEEE 802.11 (all radios)
host           Internet host settings
interface      Network interface
ip-route       IP route entry
klog-entry     Kernel log entry
log            Log settings
log-entry      Log entry
mac-acl        MAC address access list item
ntp            Network Time Protocol client
portal         Guest captive portal
radio          Radio
radius-user    RADIUS user
ssh            SSH access to the command line interface
supported-rate Supported rates of radios
system         System settings
telnet         Telnet access to the command line interface
tx-queue      Transmission queue parameters
wme-queue      Transmission queue parameters for stations
```

- **Example 3:** Type `get system v TAB`. This will result in completion with the only matching field, `get system version`. Press Enter to display the output results of the command.

For detailed examples on getting help, see “Keyboard Shortcuts and Tab Completion Help” on page 349.

Command Usage and Configuration Examples

The following sections provide examples of using the CLI to perform functions similar to those documented in the web browser interface chapters in this book:

- ❑ “Understanding Interfaces as Presented in the CLI,” next
- ❑ “Saving Configuration Changes” on page 281
- ❑ “Basic Settings” on page 282
- ❑ “Access Point and Cluster Settings” on page 285
- ❑ “User Accounts” on page 287
- ❑ “Displaying Status” on page 289
- ❑ “Ethernet (Wired) Interface” on page 301
- ❑ “Setting Up the Wireless Interface” on page 304
- ❑ “Setting Up Security” on page 304
- ❑ “Enabling and Configuring the Guest Login Welcome Page” on page 323
- ❑ “Configuring Multiple BSSIDs on Virtual Wireless Networks” on page 325
- ❑ “Radio Settings” on page 326
- ❑ “MAC Filtering” on page 333
- ❑ “Load Balancing” on page 335
- ❑ “Quality of Service” on page 336
- ❑ “Wireless Distribution System” on page 344
- ❑ “Time Protocol” on page 347
- ❑ “Rebooting the Access Point” on page 348
- ❑ “Resetting the Access Point to the Factory Defaults,” next
- ❑ “Keyboard Shortcuts” on page 349
- ❑ “Tab Completion and Help” on page 350

Understanding Interfaces as Presented in the CLI

The following summary of interface names is provided to help clarify the related CLI commands and output results. These names are not shown in the web UI, but are used throughout the CLI. You get and set many configuration values on the access point by referring to interfaces. In order to configure the access point through the CLI, you need to understand which interfaces are available on the access point, what role they play (corresponding setting on the web UI), and how to refer to them.

Table 4. Interfaces in the CLI

| Interface | Description |
|-----------|---|
| lo | Local loopback for data meant for the access point itself. |
| eth0 | The wired (Ethernet) interface for the internal network. |
| br0 | <p>The internal bridge represents the internal interface for the access point. To telnet or ssh into the access point, use the IP address for this interface.</p> <p>br0 consists of:</p> <ul style="list-style-type: none"> • eth0 (or <code>vlanSomeNumber</code> if you have VLANs configured) • wlan0 • wlan1 (if the access point is a two-radio access point) <p>The IP address of the access point is provided in the output detail for br0. So, a useful command is <code>get interface</code>. This gives you common information on all interfaces. From the output results, you can find the IP address for br0. Use this IP address to connect to the access point.</p> |
| brguest | The guest bridge, which consists of eth1 and wlan0guest. |
| brvwn1 | <p>The bridge interface for virtual wireless network (VWN) 1. On a one-radio access point, the bridge interface for VWN1 consists of:</p> <ul style="list-style-type: none"> • wlan0vwn1 • <code>vlanVLANID</code> where <i>VLANID</i> is a four-digit VLAN ID that you provided. (For example, if you provided a VLAN ID of 1234, the VLAN interface would be <code>vlan1234</code>.) <p>On a two-radio access point, the bridge interface for VWN1 consists of:</p> <ul style="list-style-type: none"> • wlan0vwn1 • wlan1vwn1 • <code>vlanVLANID</code> where <i>VLANID</i> is a four-digit VLAN ID that you provided. (For example, if you provided a VLAN ID of 1234, the VLAN interface would be <code>vlan1234</code>.) |

Table 4. Interfaces in the CLI

| Interface | Description |
|------------|---|
| brvwn2 | <p>This is for the second virtual wireless network (VWN) 2.</p> <p>On a one-radio access point, the bridge interface for VWN2 consists of: wlan0vwn1</p> <p>vlan <i>VLANID</i> where <i>VLANID</i> is a four-digit VLAN ID that you provided. (For example, if you provided a VLAN ID of 1234, the VLAN interface would be vlan1234.</p> <p>On a two-radio access point, the bridge interface for VWN2 consists of: wlan0vwn1 wlan1vwn1</p> <p>vlan <i>VLANID</i> where <i>VLANID</i> is a four-digit VLAN ID that you provided. (For example, if you provided a VLAN ID of 5678, the VLAN interface would be vlan5678.</p> |
| wlan0 | The wireless (radio) interface for the internal network. |
| wlan0guest | The wireless (radio) interface for the guest network. |
| wlan0vwn1 | The wireless interface for virtual wireless network (VWN) 1. |
| wlan0vwn2 | The wireless interface for virtual wireless network (VWN) 2. |
| wlan0wdsx | A wireless distribution system (WDS) interface where “x” indicates the number of the WDS link. (For example, wlan0wds1.) |
| wlan1 | On a two-radio access point, the wireless (radio) interface for the internal network on the second radio. |
| wlan1guest | On a two-radio access point, the wireless (radio) interface for the guest network on the second radio. |
| wlan1vwn1 | On a two-radio access point, the wireless interface for virtual wireless network (VWN) 1 on the second radio. |
| wlan1vwn2 | On a two-radio access point, the wireless interface for virtual wireless network (VWN) 2 on the second radio. |
| vlanxxxx | <p>A VLAN interface for VLAN ID xxxx. To find out what this VLAN interface is (Internal, guest, VWN1 or VWN2), use the following command to look at the role field:</p> <pre>get interface vlan<i>VLANID</i> role</pre> <p>For example:</p> <pre>get interface vlan1234 role</pre> |

Saving Configuration Changes

The AT-WA7400 Wireless Access Point maintains three different configurations.

- ❑ **Factory Default Configuration** - This configuration consists of the default settings shipped with the access point (as specified in Appendix A, "Management Software Default Settings" on page 215).

You can always return the access point to the factory defaults by using the `factory-reset` command, as described in "Resetting the Access Point to the Factory Defaults" on page 348.

- ❑ **Startup Configuration** - The startup configuration contains the settings with which the access point will use the next time it starts up (for example, upon reboot).

To save configuration updates made from the CLI to the *startup* configuration, you must execute the `save-running` or `set config startup running` command from the CLI after making changes.

- ❑ **Running Configuration** - The running configuration contains the settings with which the access point is currently running.

When you view or update configuration settings through the CLI using `get`, `set`, `add`, and `remove` commands, you are viewing and changing values on the *running* configuration only. If you do not save the configuration (by executing the `save-running` or `set config startup running` command in the CLI), you will lose any changes you submitted via the CLI upon reboot.

The `save-running` command saves the *running* configuration as the startup configuration. (The `save-running` command is a shortcut command for `set config startup running`, which accomplishes the same thing)

Settings updated from the CLI (with the `get`, `set`, `add`, and `remove` commands) are not saved to the startup configuration unless you explicitly save them via the `save-running` command. This gives you the option of maintaining the *startup* configuration and trying out values on the *running* configuration that you can discard (by not saving).

By contrast, configuration changes updated from the web UI are automatically saved to both the *running* and *startup* configurations. If you make changes from the web UI that you do not want to keep, your only option is to reset to factory defaults. The previous startup configuration will be lost.

Basic Settings

Note

Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 278. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface, the internal or guest network, or (on a two-radio access point) to radio one or radio two.

The following CLI command examples correspond to tasks you can accomplish on the Basic Settings page of the web UI for access points with clustering capabilities. In some cases, the CLI `get` command provides additional details not available through the web UI.

Table 5 provides a quick view of Basic Settings commands and provides links to detailed examples.

Table 5. Basic Settings Commands

| Function | Command |
|--|---|
| Get the IP Address for the Internal Interface on an Access Point | <pre>get interface br0 ip</pre> or <pre>get interface</pre> <p>get interface is a catch-all command that shows common information on all interfaces for the access point such as IP addresses, MAC addresses, and so on. The IP address for the internal interface (and the one used to access the access point) is that shown for <code>br0</code>. (See “Understanding Interfaces as Presented in the CLI” on page 278.)</p> |
| Get the MAC Address for an Access Point | <pre>get interface br0 mac</pre> |
| Get Both the IP Address and MAC Address | <pre>get interface br0 mac ip</pre> |
| Get Common Information on All Interfaces for an Access Point | <pre>get interface</pre> |
| Get the Firmware Version for the Access Point | <pre>get system version</pre> |
| Get the Location of the Access Point | <pre>get cluster location</pre> |

Table 5. Basic Settings Commands (Continued)

| Function | Command |
|--------------------------------------|---|
| Set the Location for an Access Point | <pre>set system location <i>NewLocation</i></pre> <p>For example: <pre>set system location hallway</pre> or <pre>set system location "Vicky's office"</pre></p> |
| Get the Current Password | <pre>get system encrypted-password</pre> |
| Set the Password | <pre>set system password <i>NewPassword</i></pre> <p>For example: <pre>set system password admin</pre></p> |
| Get the Wireless Network Name (SSID) | <pre>get interface wlan0 ssid</pre> |
| Set the Wireless Network Name (SSID) | <pre>set interface wlan0 ssid <i>NewSSID</i></pre> <p>For example: <pre>set interface wlan0 ssid vicky</pre> <pre>set interface wlan0 ssid "Vicky's AP"</pre></p> |

Get the IP Address for the Internal Interface on an Access Point

In the following example, the IP address for the access point is: 10.10.55.216. Use the **get** command as shown to obtain the IP address for the internal network.

```
AT-WA7400# get interface br0 ip
10.10.55.216
```

Get the MAC Address for an Access Point

In the following example, the MAC address for the access point is: 00:a0:c9:8c:c4:7e. Use the **get** command as shown to obtain the MAC address.

```
AT-WA7400# get interface br0 mac
00:a0:c9:8c:c4:7e
```

Get Both the IP Address and MAC Address

The following command returns both the IP address and the MAC address for an access point:

```
AT-WA7400# get interface br0 mac ip
```

```

Field Value
-----
ip      10.10.55.216
mac     00:a0:c9:8c:c4:7e

```

Get Common Information on All Interfaces for an Access Point

The following example shows common information (including IP addresses) for all interfaces:

```

AT-WA7400# get interface
name      type      status  mac                ip                mask
-----
lo                up      00:00:00:00:00:00  127.0.0.1        255.0.0.0
eth0                up      00:02:B3:01:01:01
eth1                down   00:02:B3:02:02:02
br0      bridge   up      00:02:B3:01:01:01  10.10.100.110    255.255.255.0
brguest  bridge   down   00:00:00:00:00:00
wlan0     service-set up      00:0C:41:16:DF:A6
wlan0guest service-set up
wlan0wds0 wds      down
wlan0wds1 wds      down
wlan0wds2 wds      down
wlan0wds3 wds      down
AT-WA7400#

```

Get the Firmware Version for the Access Point

In the following example, the access point is running Firmware Version: 1.0.0.9. Use the **get** command as shown to obtain the Firmware Version.

```

AT-WA7400# get system version
1.0.0.9

```

Get the Location of the Access Point

In the following example, the location of the access point has not been set. Use the **get** command as shown to obtain the location of the access point.

```
AT-WA7400# get cluster location
not set
```

Set the Location for an Access Point

To set the location for an access point, use the **set** command as follows:

```
AT-WA7400# set system location hallway
AT-WA7400# set system location "vicky's office"
```

To check to make sure that the location was set properly, use the **get** command again to find out the location

```
AT-WA7400# get system location
vicky's office
```

Get the Current Password

```
AT-WA7400# get system encrypted-password
2yn.4fvaTgedM
```

Set the Password

```
AT-WA7400# set system password admin
AT-WA7400# get system encrypted-password
/rYSvxS40kptc
```

Get the Wireless Network Name (SSID)

```
AT-WA7400# get interface wlan0 ssid
Internal AT-WA7400 Network
```

Set the Wireless Network Name (SSID)

```
AT-WA7400# set interface wlan0 ssid "vicky's AP"
AT-WA7400# get interface wlan0 ssid
vicky's AP
```

Access Point and Cluster Settings

The command examples in this section show how to get the configuration for a cluster of access points. These settings generally correspond to those on the Cluster > Access Points page in the web UI.

Table 6 provides a quick view of Access Point Cluster commands and

links to detailed examples.

Table 6. Cluster Functions and Commands

| Function | Command |
|---|---------------------------|
| Determine if the Access Point is a Cluster Member or in Standalone Mode | get cluster detail |
| Get MAC Addresses for all Access Points in the Cluster | get clustered-ap all name |
| Configure the Access Point as a Member of a Cluster | set cluster clusterable 1 |
| Configure the Access Point as a Standalone Device | set cluster clusterable 0 |

Determine if the Access Point is a Cluster Member or in Standalone Mode

This command shows whether the access point is clustered or not. If the command returns 0, the access point is in standalone mode (not clustered). If the command returns 1, the access point is a member of a cluster. In the following example, the access point is in standalone mode.

AT-WA7400# get cluster detail

```
Field      value
-----
clustered  0
clusterable 0
kickstarted 0
location   not set
formation
```

Get MAC Addresses for all Access Points in the Cluster

AT-WA7400# get cluster-member all

```
name          mac          ip          location removed
-----
00:e0:b8:76:23:b4  00:e0:b8:76:23:b4  10.10.10.248  not set  0
00:e0:b8:76:16:88  00:e0:b8:76:16:88  10.10.10.230  not set  0
```

Configure the Access Point as a Member of a Cluster

set cluster clusterable 1

Configure the Access Point as a Standalone Device

```
set cluster clusterable 0
```

User Accounts The following command examples show configuration tasks related to user accounts. These tasks correspond to the Cluster > User Management page in the web UI.

Table 7 provides a quick view of User Management commands and provides links to detailed examples.

Table 7. User Account Commands

| Function | Command |
|--------------------------|--|
| Get All User Accounts | To view all usernames: get radius-user all name To view all user accounts: get radius-user all |
| Add Users | add radius-user <i>UserName</i> For example: add radius-user samantha |
| Set the user's real name | set radius-user <i>UserName RealName</i> For example: set radius-user samantha "Elizabeth Montgomery" (or set radius-user samantha Elizabeth) |
| Set user's password | set radius-user <i>UserName password Password</i> For example: set radius-user samantha password bewitched |
| Remove a User Account | remove radius-user <i>UserName</i> |

Get All User Accounts

To view all user names:

```
AT-WA7400# get radius-user all name
```

```
name
```

```
-----
```

```
larry
```

To view all user accounts:

```
AT-WA7400# get radius-user all
name      username  disabled  password  realname
-----
Larry                                David white
```

Add Users

In this example, four new users are added: (1) samantha, (2) endora, (3) darren, and (4) wally, and their user names, real names, and passwords are set up.

1. Add **username** "samantha":

```
AT-WA7400# add radius-user samantha
```

2. Provide a **real name** (Elizabeth Montgomery) for this user:

```
AT-WA7400# set radius-user samantha realname "Elizabeth
Montgomery"
```

3. Set the user **password** for samantha to "bewitched":

```
AT-WA7400# set radius-user samantha password bewitched
```

4. Repeat this process to add some other users (endora, darren, and wally):

```
AT-WA7400# add radius-user endora
```

```
AT-WA7400# set radius-user endora realname "Agnes Moorhead"
```

```
AT-WA7400# set radius-user endora password scotch
```

```
AT-WA7400# add radius-user darren
```

```
AT-WA7400# set radius-user darren realname "Dick York"
```

```
AT-WA7400# set radius-user darren password martini
```

```
AT-WA7400# add radius-user wally
```

```
AT-WA7400# set radius-user wally realname "Tony Dow"
```

```
AT-WA7400# set radius-user wally password sodapop
```

5. After configuring these new accounts, use the **get** command to view all users. (Passwords are always hidden.)

```
AT-WA7400# get radius-user all
```



```

name      username  disabled  password  realname
-----
larry                                David white
samantha                               Elizabeth Montgomery
endora                                  Agnes Moorhead
darren                                  Dick York
wally                                   Tony Dow

```

Remove a User Account

To remove a user account, type the following:

```
AT-WA7400# remove radius-user wally
```

Use the **get** command to view all user names. (You can see that “wally” has been removed.)

```
AT-WA7400# get radius-user all name
```

```

name
-----
larry
samantha
endora
darren

```

Displaying Status

The command tasks and examples in this section show status information on access points. These settings correspond to what is shown on the Status pages in the web UI. (See “Monitoring Wired and Wireless LAN Settings” on page 184, “Viewing the Event Logs” on page 186, “Viewing the Transmit/Receive Statistics” on page 190, “Viewing the Associated Wireless Clients” on page 192, and “Viewing the Status of Neighboring Access Points” on page 193.)

Note

Make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 278. The interface name you reference in a **get** command determines whether the command output shows a wired or wireless interface, the internal or guest network, or (on a two-radio access point) to radio one or radio two.

Table 8 provides a quick view of all Status commands and links to detailed

examples.

Table 8. Status Commands

| Function | Command |
|--|---|
| Understanding Interfaces as Presented in the CLI | Reference of interface names and purposes as described in “Understanding Interfaces as Presented in the CLI” on page 278. |
| Global command to get all detail on a Basic Service Set (BSS). This is a useful command to use to get a comprehensive picture of how the access point is currently configured. | get bss all detail |
| Get Common Information on the Internal Interface for the Access Point | get interface br0 |
| Get All Wired Settings for the Wired Internal Interface | get interface br0 |
| Get Current Settings for the Ethernet (Wired) Guest Interface | get interface brguest get interface brguest mac get interface brguest ssid |
| Get the MAC Address for the Wired Internal Interface | get interface wlan0 mac |
| Get the Network Name (SSID) for the Wired Internal Interface | get interface wlan0 ssid |
| Get the Current IEEE 802.11 Radio Mode | get radio wlan0 mode |
| Get the Channel the Access Point is Currently Using | get radio wlan0 channel |
| Get Basic Radio Settings for the Internal Interface | get radio wlan0 get radio wlan0 detail |
| Get Status on Events | get log-entry all |

Table 8. Status Commands (Continued)

| Function | Command |
|---|--|
| Enable Remote Logging and Specify the Log Relay Host for the Kernel Log | As a prerequisite to remote logging, the Log Relay Host must be configured first as described in "Setting Up the Log Relay Host" on page 187. See a complete explanation of CLI commands at "Enable Remote Logging and Specify the Log Relay Host for the Kernel Log" on page 295. Here are a few: set log relay-enabled 1 enables remote logging set log relay-enabled 0 disables remote logging get log set log TAB TAB shows values you can set on the log |
| Get Transmit / Receive Statistics | get interface all ip mac ssid tx-packets tx-bytes tx-errors rx-packets rx-bytes rx-errors |
| Get Client Associations | get association |
| Get Neighboring Access Points | get clustered-ap |

Get Common Information on the Internal Interface for the Access Point

The following command obtains all information on the internal interface for an access point:

```
AT-WA7400# get interface br0
```

```
Field          value
-----
type           bridge
status        up
hello         10
mac           00:a0:c9:8c:c4:7e
ip            192.168.1.1
mask          255.255.255.0
```

Get Current Settings for the Ethernet (Wired) Internal Interface

The following example shows how to use the CLI to get the Ethernet (Wired) settings for the internal interface for an access point. You can see by the output results of the command that the MAC address is 00:a0:c9:8c:c4:7e, the IP address is 192.168.1.1, and the subnet mask is 255.255.255.0.

Get All Wired Settings for the Wired Internal Interface

```
AT-WA7400# get interface br0
```

| Field | Value |
|-------|-------------------|
| ----- | |
| mac | 00:a0:c9:8c:c4:7e |
| ip | 192.168.1.1 |
| mask | 255.255.255.0 |

Get the MAC Address for the Wired Internal Interface

```
AT-WA7400# get interface wlan0 mac
```

```
02:0c:41:00:02:00
```

Get the Network Name (SSID) for the Wired Internal Interface

```
AT-WA7400# get interface wlan0 ssid
```

```
elliott_AP
```

Get Current Settings for the Ethernet (Wired) Guest Interface

The following example shows how to use the CLI to get the Ethernet (Wired) settings for the guest interface for an access point. You can see by the output results of the command that the MAC address is 00:50:04:6f:6f:90, the IP address is 10.10.56.248, and the subnet mask is 255.255.255.0.

```
AT-WA7400# get interface brguest
```

| Field | Value |
|--------|-------------------|
| ----- | |
| type | bridge |
| status | up |
| mac | 00:50:04:6f:6f:90 |
| ip | 10.10.56.248 |
| mask | 255.255.255.0 |

Note

You can get specifics on the guest interface by using the same types of commands as for the internal interface but substituting `brguest` for `wlan0`. For example, to get the MAC address for the guest interface: `get interface wlan0 ssid`

Get Current Wireless (Radio) Settings

The following examples show how to use the CLI to get wireless radio settings on an access point, such as mode, channel, and so on. You can see by the output results of the commands that the access point mode is set to IEEE 802.11g, the channel is set to 6, the beacon interval is 100, and so forth.

For information on how to configure radio settings through the CLI, see “Radio Settings” on page 326.

(Radio settings are fully described in the web UI topic on “Configuring Radio Settings” on page 147.)

Get the Current IEEE 802.11 Radio Mode

```
AT-WA7400# get radio wlan0 mode
```

```
g
```

Get the Channel the Access Point is Currently Using

```
AT-WA7400# get radio wlan0 channel
```

```
2
```

Get Basic Radio Settings for the Internal Interface

```
AT-WA7400# get radio wlan0
```

| Field | Value |
|-------------------------|-------|
| status | up |
| max-bsses | 2 |
| channel-policy | best |
| channel | 6 |
| static-channel | 9 |
| mode | g |
| fragmentation-threshold | 2346 |

```

rts-threshold      2347
ap-detection       on
beacon-interval    100
    
```

Get All Radio Settings on the Internal Interface

```
AT-WA7400# get radio wlan0 detail
```

| Field | Value |
|---|-------------|
| status | up |
| description | IEEE 802.11 |
| mac | |
| max-bss | 2 |
| channel-policy | best |
| mode | g |
| static-channel | 11 |
| channel | 2 |
| tx-power | 100 |
| tx-rx-status | up |
| beacon-interval | 100 |
| rts-threshold | 2347 |
| fragmentation-threshold | 2346 |
| load-balance-disassociation-utilization | 0 |
| load-balance-disassociation-stations | 0 |
| load-balance-no-association-utilization | 0 |
| ap-detection | on |
| station-isolation | off |
| frequency | 2417 |
| wme | on |

Get Status on Events

```
AT-WA7400# get log-entry all
```

```

Number  Time                Priority  Daemon
      Message
-----
1      Apr 20 21:39:55    debug    udhcpc
      Sending renew...
2      Apr 20 21:39:55    info     udhcpc
      Lease of 10.10.55.216 obtained, lease time 300
3      Apr 20 21:37:25    debug    udhcpc
      Sending renew...
4      Apr 20 21:37:25    info     udhcpc
      Lease of 10.10.55.216 obtained, lease time 300
5      Apr 20 21:34:55    debug    udhcpc
      Sending renew...
6      Apr 20 21:34:55    info     udhcpc
      Lease of 10.10.55.216 obtained, lease time 300

```

Enable Remote Logging and Specify the Log Relay Host for the Kernel Log

The Kernel Log is a comprehensive list of system even its and kernel messages such as error conditions like dropping frames. To capture Access Point Kernel Log messages you need access to a remote syslog server on the network.

Prerequisites for Remote Logging

To capture Kernel Log messages from the access point system, you must first set up a remote server running a syslog process and acting as a syslog log relay host on your network. (For information on how to set up the remote server, see “Setting Up the Log Relay Host” on page 187.)

Then, you can use the CLI to configure the AT-WA7400 Wireless Access Point to send its syslog messages to the remote server.

View Log Settings

To view the current log settings:

```
AT-WA7400# get log
```

```
Field          value
-----
depth          15
relay-enabled  0
relay-host
relay-port     514
```

When you start a new access point, the Log Relay Host is disabled. From the above output for the **get log** command, you can identify the following about the Log Relay Host (syslog server):

- The syslog server is *disabled* (because “relay-enabled” is set to “0”)
- No IP address or Host Name is specified for the syslog server.
- The access point is listening for syslog messages on the default port 514

Enable / Disable Log Relay Host

To enable the Log Relay Host:

```
AT-WA7400# set log relay-enabled 1
```

To disable the Log Relay Host:

```
AT-WA7400# set log relay-enabled 0
```

Specify the Relay Host

To specify the Relay Host, provide either the IP address or a DNS name for the Log Relay Host as parameters to the **set log relay-host** command as shown below.

- To specify an IP address for the syslog server:

```
set log relay-host IP_Address_of_LogRelayHost
```

Where *IP_Address_of_LogRelayHost* is the IP address of the Log Relay Host.

For example:

```
AT-WA7400# set log relay-host 10.10.5.220
```

- To specify a Host Name for the syslog server:


```
set log relay-host Host_Name_Of_LogRelayHost
```

Where *Host_Name_Of_LogRelayHost* is the a DNS name for the Log Relay Host.

For example:

```
AT-WA7400# set log relay-host myserver
```

Specify the Relay Port

To specify the Relay Port for the syslog server:

```
set log relay-port Number_Of_LogRelayPort
```

Where *Number_Of_LogRelayPort* is the port number for the Log Relay Host.

For example:

```
AT-WA7400# set log relay-port 514
```

Review Log Settings After Configuring Log Relay Host

To view the current log settings:

```
AT-WA7400# get log
```

| Field | Value |
|---------------|-------------|
| ----- | |
| depth | 15 |
| relay-enabled | 1 |
| relay-host | 10.10.5.220 |
| relay-port | 514 |

From the above output for the **get log** command, you can identify the following about the Log Relay Host (syslog server):

- The syslog server is *enabled* (because relay-enabled is set to 1)
- The syslog server is at the IP address 10.10.5.220
- The access point is listening for syslog messages on the default port 514

Get Transmit / Receive Statistics

AT-WA7400# **get interface all ip mac ssid tx-packets tx-bytes tx-errors rx-packets rx-bytes rx-errors**

| Name | Ip | Mac | Ssid | Tx-packets | |
|------------|--------------|-------------------|-------------------|------------|-----------|
| | Tx-bytes | Tx-errors | Rx-packets | Rx-bytes | Rx-errors |
| ----- | | | | | |
| lo | 127.0.0.1 | 00:00:00:00:00:00 | | 1319 | |
| | 151772 | 0 | 1319 | 151772 | 0 |
| eth0 | | 00:A0:C9:8C:C4:7E | | 4699 | |
| | 3025566 | 0 | 11323 | 1259824 | 0 |
| eth1 | 0.0.0.0 | 00:50:04:6F:6F:90 | | 152 | |
| | 49400 | 0 | 6632 | 664298 | 0 |
| br0 | 10.10.55.216 | 00:A0:C9:8C:C4:7E | | 4699 | |
| | 3025566 | 0 | 10467 | 885264 | 0 |
| brguest | 10.10.56.248 | 00:50:04:6F:6F:90 | | 152 | |
| | 48032 | 0 | 5909 | 293550 | 0 |
| wlan0 | 0.0.0.0 | 02:0C:41:00:02:00 | AAP1000 (Trusted) | 6483 | |
| | 710681 | 0 | 0 | 0 | 0 |
| wlan0guest | 0.0.0.0 | 02:0C:41:00:02:01 | AAP1000 (Guest) | 5963 | |
| | 471228 | 0 | 0 | 0 | 0 |
| wlan0wds0 | | | | | |
| wlan0wds1 | | | | | |
| wlan0wds2 | | | | | |
| wlan0wds3 | | | | | |

Get Client Associations

AT-WA7400# **get association**

| Interf | Station | Authen | Associ | Rx-pac | Tx-pac | Rx-byt | Tx-byt | Tx-rat |
|--------|-------------------|--------|--------|--------|--------|--------|--------|--------|
| wlan0 | 00:0c:41:8f:a7:72 | Yes | Yes | 126 | 29 | 9222 | 3055 | 540 |
| wlan0 | 00:09:5b:2f:a5:2f | Yes | Yes | 382 | 97 | 16620 | 10065 | 110 |

AT-WA7400# **get association detail**

| Inter | Station | Authe | Assoc | Rx-pa | Tx-pa | Rx-byt | Tx-byt | Tx-ra | Liste |
|-------|-------------------|-------|-------|-------|-------|--------|--------|-------|-------|
| wlan0 | 00:0c:41:8f:a7:72 | Yes | Yes | 126 | 29 | 9222 | 3055 | 540 | 1 |
| wlan0 | 00:09:5b:2f:a5:2f | Yes | Yes | 382 | 97 | 16620 | 10065 | 110 | 1 |

Get Neighboring Access Points

The Neighboring access point view shows wireless networks within range of the access point. These commands provides a detailed view of neighboring access points including identifying information (SSIDs and MAC addresses) for each, and statistical information such as the channel each access point is broadcasting on, signal strength, and so forth.

To see the kinds of information about access point neighbors you can search on, type **get detected-ap TAB TAB**.

AT-WA7400# **get detected-ap**

```
[Enter]          * Get common fields *
band             Frequency band
beacon-interval Beacon interval in kus (1.024 ms)
capability       IEEE 802.11 capability value
channel          Channel
detail           * Get all fields *
erp              ERP
last-beacon      Time of last beacon
mac              MAC address
num_beacons      Number of beacons received
phy-type         PHY mode detected with
privacy          WEP or WPA enabled
```

```

rate           Rate
signal        Signal strength
ssid          Service Set Identifier (a.k.a., Network
Name)
supported-rates Supported rates list
type          Type (AP, Ad hoc, or Other)
wpa           WPA security enabled
    
```

To get the neighboring access points, type **get detected-ap**.

```
AT-WA7400# get detected-ap
```

```

Field  value
-----
mac    00:e0:b8:76:28:e0
type   AP
privacy On
ssid   Purina
channel 6
signal 2
    
```

```

Field  value
-----
mac    00:0e:81:01:01:62
type   AP
privacy Off
ssid   Internal AT-WA7400 Network
channel 6
signal 1
    
```

```

Field  value
-----
mac    00:e0:b8:76:1a:f6
    
```

```

type      AP
privacy   off
ssid      domani
channel   6
signal    3
    
```

```

Field     Value
-----
    
```

```

mac       00:e0:b8:76:28:c0
type      AP
privacy   off
ssid      domani
channel   6
signal    4
    
```

Ethernet (Wired) Interface

Note

Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 278. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface, the internal or guest network, or (on a two-radio access point) to radio one or radio two.

Table 9 provides a quick view of commands for getting and setting values for the Wired interface and links to detailed examples.

Table 9. Wired Interface Commands

| Function | Command |
|---|---|
| Get Summary View of Internal and Guest Interfaces | <code>get bss</code> |
| Get the DNS Name | <code>get host id</code> |
| Set the DNS Name | <code>set host id <i>HostName</i></code> For example: <code>set host id vicky-ap</code> |

Table 9. Wired Interface Commands (Continued)

| Function | Command |
|---|--|
| Get Current Settings for the Ethernet (Wired) Internal Interface | get interface br0 |
| Find out if guest access is enabled and configured.) | get interface brguest status (will be “up” or “down”) |
| Set DNS Nameservers to Use Static IP Addresses (Dynamic to Manual Mode) | See example below. |
| Set DNS Nameservers to Use DHCP IP Addressing (Manual to Dynamic Mode) | See example below. |

Get Summary View of Internal and Guest Interfaces

```
AT-WA7400# get bss
```

```
name                status  radio  beacon-interface  mac
```

```
-----
wlan0bssInternal  up      wlan0  wlan0
00:0C:41:16:DF:A6
```

Get the DNS Name

```
AT-WA7400# get host id
```

```
AT-WA7400-AP
```

Set the DNS Name

```
AT-WA7400# set host id vicky-ap
```

```
bob# get host name
```

```
vicky-ap
```

Get Wired Internal Interface Settings

See “Get Current Settings for the Ethernet (Wired) Internal Interface” on page 291 under Displaying Status.

Get Wired Guest Interface Settings

See “Get Current Settings for the Ethernet (Wired) Guest Interface” on page 292 under Displaying Status.

Set DNS Nameservers to Use Static IP Addresses (Dynamic to Manual Mode)

This example shows how to reconfigure DNS Nameservers from *Dynamic* mode (where name server IP addresses are assigned through DHCP) to *Manual* mode, and specify static IP addresses for them.

1. Check to see which mode the DNS Name Service is running in. (In our example, DNS naming is running in DHCP mode when we start because the following command returns up for the mode.)

```
AT-WA7400# get host dns-via-dhcp
up
```

2. Turn off Dynamic DNS Nameservers and re-check the settings:

```
AT-WA7400# set host dns-via-dhcp down
AT-WA7400# get host dns-via-dhcp
down
```

3. Get the current IP addresses for the DNS Nameservers:

```
AT-WA7400# get host static-dns-1
10.10.3.9
AT-WA7400# get host static-dns-2
10.10.3.11
```

4. Re-set the IP addresses for the DNS Nameservers as desired:

```
AT-WA7400# set host static-dns-1 10.10.3.10
AT-WA7400# get host static-dns-1
10.10.3.10
AT-WA7400# set host static-dns-2 10.10.3.12
AT-WA7400# get host static-dns-2
10.10.3.12
```

Set DNS Nameservers to Use DHCP IP Addressing (Manual to Dynamic Mode)

To switch DNS Nameservers from Manual (static IP addresses) to Dynamic mode (nameserver addresses assigned by DHCP), use the reverse command and check to see the new configuration:

```
AT-WA7400# set host dns-via-dhcp up
```

```
AT-WA7400# get host dns-via-dhcp
up
```

Setting Up the Wireless Interface

To set up a wireless (radio) interface, configure the following on each interface (Internal or guest) as described in other sections of this CLI document.

- ❑ Configure the Radio Mode and Radio Channel as described in “Configuring Radio Settings” on page 147.
- ❑ Configure the Network Name as described in “Configuring Internal Wireless LAN Settings” on page 102.

Setting Up Security

Note

Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 278. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface, the internal or guest network, or (on a two-radio access point) to radio one or radio two.

The following sections show examples of how to use the CLI to view and configure security settings on the access point. These settings correspond to those available from the web UI on the Advanced > Security page. For a detailed discussion of concepts and configuration options, see Chapter 10, “Configuring Security” on page 105.

This section focuses on configuring security on the *internal* network. (Security on the *guest* network defaults to plain text. See “Plain Text” on page 115.)

Table 10 shows a quick view of Security commands and links to detailed examples.

Table 10. Security Commands

| Function | Command |
|---|---|
| Get the Current Security Mode | get interface wlan0 security |
| Get Detailed Description of Current Security Settings | get bss wlan0bssInternal detail get interface wlan0 detail |
| Set the Broadcast SSID (Allow or Prohibit) | set radio wlan0 ignore-broadcast-ssid on set radio wlan0 ignore-broadcast-ssid off |

Table 10. Security Commands (Continued)

| Function | Command |
|--|--|
| Enable/Disable Station Isolation | get interface br0 port-isolation off set radio wlan0 station-isolation off |
| Set Security to Plain Text | set interface wlan0 security plain-text |
| Set Security to Static WEP | See detailed example in “Set Security to Static WEP” on page 307. |
| Set Security to IEEE 802.1x | See detailed example in “Set Security to IEEE 802.1x” on page 312. |
| Set Security to WPA/WPA2 Personal (PSK) | See detailed example in “Set Security to WPA/WPA2 Personal (PSK)” on page 315 |
| Set Security to WPA/WPA2 Enterprise (RADIUS) | See detailed example in “Set Security to WPA/WPA2 Enterprise (RADIUS)” on page 318 |

Get the Current Security Mode

```
AT-WA7400# get interface wlan0 security
plain text
```

Get Detailed Description of Current Security Settings

```
AT-WA7400# get bss wlan0bssInternal detail
```

```
Field                value
-----
status                up
description           Internal
radio                 wlan0
beacon-interface      wlan0
mac                   00:0C:41:16:DF:A6
dtim-period
max-stations
ignore-broadcast-ssid off
mac-acl-mode          deny-list
mac-acl-name          wlan0bssInternal
radius-accounting
```

```

radius-ip                127.0.0.1
radius-key               secret
open-system-authentication
shared-key-authentication
wpa-allow-non-wpa-stations
wpa-cipher-tkip
wpa-cipher-ccmp
wpa-allowed              off
wpa2-allowed             off
rsn-preauthentication
    
```

Set the Broadcast SSID (Allow or Prohibit)

To set the Broadcast SSID to on (allow):

```
AT-WA7400# set radio wlan0 ignore-broadcast-ssid on
```

To set the Broadcast SSID to off (prohibit):

```
AT-WA7400# set radio wlan0 ignore-broadcast-ssid off
```

Enable/Disable Station Isolation

```
AT-WA7400# get interface br0 port-isolation
off
```

```
AT-WA7400# set radio wlan0 station-isolation off
```

```
AT-WA7400# get radio wlan0 detail
```

| Field | value |
|----------------|------------------------|
| status | up |
| description | Radio 1 - IEEE 802.11g |
| mac | |
| max-bss | 4 |
| channel-policy | static |
| mode | g |
| static-channel | 6 |

| | |
|---|------|
| channel | 6 |
| tx-power | 100 |
| tx-rx-status | up |
| beacon-interval | 100 |
| rts-threshold | 2347 |
| fragmentation-threshold | 2346 |
| load-balance-disassociation-utilization | 0 |
| load-balance-disassociation-stations | 0 |
| load-balance-no-association-utilization | 0 |
| ap-detection | off |
| station-isolation | off |
| frequency | 2437 |
| wme | on |

Set Security to Plain Text

```
AT-WA7400# set interface wlan0 security plain-text
```

Set Security to Static WEP

Set the Security Mode

```
AT-WA7400# set interface wlan0 security static-wep
```

Set the Transfer Key Index

The following commands set the Transfer Key Index to 4.

```
AT-WA7400# set interface wlan0 wep-default-key 1
```

```
AT-WA7400# set interface wlan0 wep-default-key 2
```

```
AT-WA7400# set interface wlan0 wep-default-key 3
```

```
AT-WA7400# set interface wlan0 wep-default-key 4
```

Set the Key Length

For the CLI, valid values for Key Length are 40 bits or 104 bits.

Note

The Key Length values used by the CLI do not include the initialization vector in the length. On the web UI, longer Key Length values may be shown which include the 24-bit initialization vector. A Key Length of 40 bits (not including initialization vector) is equivalent to a Key Length of 64 bits (with initialization vector). A Key Length of 104 bits (not including initialization vector) is equivalent to a Key Length of 128 bits (which includes the initialization vector).

To set the WEP Key Length, type one of the commands in Table 11.

Table 11. WEP Key Length Commands

| Function | Command |
|------------------------------------|---|
| Set the WEP Key Length to 40 bits | <code>set interface wlan0 wep-key-length 40</code> |
| Set the WEP Key Length to 104 bits | <code>set interface wlan0 wep-key-length 128</code> |

The following example sets the WEP Key Length to 40.

```
AT-WA7400# set interface wlan0 wep-key-length 40
```

Set the Key Type

Valid values for Key Type are ASCII or Hex. The following commands set the Key Type.

Table 12. Key Type Commands

| Function | Command |
|---------------------------|--|
| Set the Key Type to ASCII | <code>set interface wlan0 wep-key-ascii yes</code> |
| Set the Key Type to Hex | <code>set interface wlan0 wep-key-ascii no</code> |

In the following example, the key type is set to ASCII:

```
AT-WA7400# set interface wlan0 wep-key-ascii yes
```

Set the WEP Keys

Note

The number of characters required for each WEP key depends on how you set Key Length and Key Type:

If Key Length is 40 bits and the Key Type is “ASCII,” then each WEP key be 5 characters long.

If Key Length is 40 bits and Key Type is “Hex,” then each WEP key must be 10 characters long.

If Key Length is 104 bits and Key Type is “ASCII,” then each WEP Key must be 13 characters long.

If Key Length is 104 bits and Key Type is “Hex,” then each WEP Key must be 26 characters long.

Although the CLI will allow you to enter WEP keys of any number of characters, you must use the correct number of characters for each key to ensure a valid security configuration.

```
AT-WA7400# set interface wlan0 wep-key-1 abcde
```

```
AT-WA7400# set interface wlan0 wep-key-2 fgghi
```

```
AT-WA7400# set interface wlan0 wep-key-3 klmno
```

```
AT-WA7400# set interface wlan0 wep-key-4
```

Set the Authentication Algorithm

The options for the authentication algorithm are Open System, Shared Key or Both and are shown in Table 13.

Table 13. Authentication Algorithm Commands

| Function | Command |
|--|--|
| Set Authentication Algorithm to Open System | set bss wlan0bssInternal open-system-authentication on set bss wlan0bssInternal shared-key-authentication off |
| Set Authentication Algorithm to Shared Key | set bss wlan0bssInternal open-system-authentication off set bss wlan0bssInternal shared-key-authentication on |
| Set Authentication Algorithm to Both | set bss wlan0bssInternal open-system-authentication on set bss wlan0bssInternal shared-key-authentication on |

In the following example, the authentication algorithm is set to Shared Key:

```
AT-WA7400# set bss wlan0bssInternal shared-key-authentication on
```

```
AT-WA7400# set bss wlan0bssInternal open-system-authentication off
```

Get Current Security Settings After Re-Configuring to Static WEP Security Mode

Now use the **get** command again to view the updated security configuration and see the results of the new settings. The following

command gets the security mode in use on the internal network:

```
AT-WA7400# get interface wlan0 security
static-wep
```

The following command gets details on how the internal network is configured, including details on Security.

```
AT-WA7400# get bss wlan0bssInternal detail
```

| Field | Value |
|----------------------------|-------------------|
| status | up |
| description | Internal |
| radio | wlan0 |
| beacon-interface | wlan0 |
| mac | 00:0C:41:16:DF:A6 |
| dtim-period | 2 |
| max-stations | 2007 |
| ignore-broadcast-ssid | off |
| mac-acl-mode | deny-list |
| mac-acl-name | wlan0bssInternal |
| radius-accounting | off |
| radius-ip | 127.0.0.1 |
| radius-key | secret |
| open-system-authentication | off |
| shared-key-authentication | on |
| wpa-allow-non-wpa-stations | off |
| wpa-cipher-tkip | off |
| wpa-cipher-ccmp | off |
| wpa-allowed | off |
| wpa2-allowed | off |
| rsn-preauthentication | off |

The following command gets details on the interface and shows the WEP

Key settings, specifically.

```
AT-WA7400# get interface wlan0 detail
```

| Field | value |
|---------------|---------------------|
| ----- | |
| type | service-set |
| status | up |
| description | wireless - Internal |
| mac | 00:0C:41:16:DF:A6 |
| ip | 0.0.0.0 |
| static-ip | 0.0.0.0 |
| static-mask | |
| nat | |
| rx-bytes | 0 |
| rx-packets | 0 |
| rx-errors | 0 |
| rx-drop | 0 |
| rx-fifo | 0 |
| rx-frame | 0 |
| rx-compressed | 0 |
| rx-multicast | 0 |
| tx-bytes | 259662 |
| tx-packets | 722 |
| tx-errors | 0 |
| tx-drop | 0 |
| tx-fifo | 0 |
| tx-colls | 0 |
| tx-carrier | 0 |
| tx-compressed | 0 |
| ssid | vicky's AP |

```

bss wlan0bssInternal
security static-wep
wpa-personal-key
wep-key-ascii yes
wep-key-length 104
wep-default-key 4
wep-key-1 abcde
wep-key-2 fghij
wep-key-3 klmno
wep-key-4
vlan-interface
vlan-id
radio
remote-mac
wep-key
    
```

Set Security to IEEE 802.1x

Set the Security Mode

```
AT-WA7400# set interface wlan0 security dot1x
```

Set the Authentication Server

You can use the built-in authentication server on the access point or an external RADIUS server. Table 14 lists the authentication server commands.

Note

To use the built in authentication server, set the RADIUS IP address to that used by the built-in server (127.0.0.1) and turn RADIUS accounting off because it is not supported by the built-in server.

Table 14. Authentication Server Commands

| Function | Command |
|--|---|
| Set the access point to use the built-in authentication server | set bss wlan0bss Internal radius-ip 127.0.0.1 |

Table 14. Authentication Server Commands (Continued)

| Function | Command |
|---|--|
| Set the access point to use an external RADIUS server | <pre>set bss wlan0bss Internal radius-ip radius_ip_address</pre> <p>where <i>radius_ip_address</i> is the IP address of an external RADIUS server.</p> |

The following example sets the access point to use the built-in server:

```
AT-WA7400# set bss wlan0bss Internal radius-ip 127.0.0.1
```

Set the RADIUS Key (For External RADIUS Server Only)

If you use an external RADIUS server, you must provide the RADIUS key. (If you use the built-in authentication server the RADIUS key is automatically provided.)

This command sets the RADIUS key to secret for an external RADIUS server.

```
AT-WA7400# set bss wlan0bss Internal radius-key secret
```

Enable RADIUS Accounting (External RADIUS Server Only)

You can enable RADIUS Accounting if you want to track and measure the resources a particular user has consumed such system time, amount of data transmitted and received, and so on. The RADIUS accounting commands are shown in Table 15.

Note

RADIUS accounting is not supported by the built-in server, so if you are using the built in server make sure that RADIUS accounting is off.

Table 15. RADIUS Accounting Commands

| Function | Command |
|---------------------------|--|
| Enable RADIUS accounting | <pre>set bss wlan0bss Internal radius-accounting on</pre> |
| Disable RADIUS accounting | <pre>set bss wlan0bss Internal radius-accounting off</pre> |

For our example, we'll disable RADIUS accounting since we're using the built-in server:

```
AT-WA7400# set bss wlan0bss Internal radius-accounting off
```

Get Current Security Settings After Re-Configuring to IEEE 802.1x Security Mode

Now use the **get** command again to view the updated security configuration and see the results of our new settings.

The following command gets the security mode in use on the internal network:

```
AT-WA7400# get interface wlan0 security
dot1x
```

The following command gets details on how the internal BSS is configured, including details on Security.

```
AT-WA7400# get bss wlan0bssInternal detail
```

| Field | Value |
|----------------------------|-------------------|
| status | up |
| description | Internal |
| radio | wlan0 |
| beacon-interface | wlan0 |
| mac | 00:0C:41:16:DF:A6 |
| dtim-period | 2 |
| max-stations | 2007 |
| ignore-broadcast-ssid | off |
| mac-acl-mode | deny-list |
| mac-acl-name | wlan0bssInternal |
| radius-accounting | off |
| radius-ip | 127.0.0.1 |
| radius-key | secret |
| open-system-authentication | off |
| shared-key-authentication | on |
| wpa-allow-non-wpa-stations | off |
| wpa-cipher-tkip | off |
| wpa-cipher-ccmp | off |

```
wpa-allowed          off
wpa2-allowed         off
rsn-preauthentication off
```

Set Security to WPA/WPA2 Personal (PSK)

1. Set the Security Mode

```
AT-WA7400# set interface wlan0 security wpa-personal
```

2. Set the WPA Versions

Select the WPA version based on what types of client stations you want to support, as shown in Table 16.

Table 16. WPA Version

| Function | Command |
|--|--|
| WPA: If all client stations on the network support the original WPA but none support the newer WPA2, then use WPA. | <pre>set bss wlan0bssInternal wpa-allowed on set bss wlan0bssInternal wpa2-allowed off</pre> |
| WPA2: If all client stations on the network support WPA2, use WPS2 which provides the best security based on the IEEE 802.11i standard. | <pre>set bss wlan0bssInternal wpa-allowed off set bss wlan0bssInternal wpa2-allowed on</pre> |
| Both: If you have a mix of clients, some of which support WPS2 and others which support only the original WPA, use Both. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients that support it. This WPA configuration allows more interoperability at the expense of some security. | <pre>set bss wlan0bssInternal wpa-allowed on set bss wlan0bssInternal wpa2-allowed on</pre> |

The following example sets the access point to support **Both** WPA and WPA2 client stations:

```
AT-WA7400# set bss wlan0bssInternal wpa-allowed on
AT-WA7400# set bss wlan0bssInternal wpa2-allowed on
```

3. Set the Cipher Suites

Set the cipher suite you want to use. The options are shown in Table 17.

Table 17. Cipher Commands

| Function | Commands |
|---|--|
| TKIP: Temporal Key Integrity Protocol (TKIP), which is the default. | <pre>set bss wlan0bssInternal wpa-cipher-tkip on set bss wlan0bssInternal wpa-cipher-ccmp off</pre> |
| CCMP (AES): Counter mode/ CBC-MAC protocol (CCMP) is an encryption method for IEEE 802.11i. that uses the Advanced Encryption Algorithm (AES). | <pre>set bss wlan0bssInternal wpa-cipher-tkip off set bss wlan0bssInternal wpa2-cipher-ccmp on</pre> |
| Both: When the authentication algorithm is set to Both, both TKIP and AES clients can associate with the access point. WPA clients must have either a valid TKIP key or a valid CCMP (AES) key to be able to associate with the access point. | <pre>set bss wlan0bssInternal wpa-cipher-tkip on set bss wlan0bssInternal wpa2-cipher-ccmp on</pre> |

The following example sets the cipher suite to **Both**:

```
AT-WA7400# set bss wlan0bssInternal wpa-cipher-tkip on
AT-WA7400# set bss wlan0bssInternal wpa-cipher-ccmp on
```

4. Set the Pre-shared Key

The *Pre-shared Key* is the shared secret key for WPA-PSK. Enter a string of at least 8 characters to a maximum of 63 characters. Following are two examples; the first sets the key to “secret!”, the second sets the key to “KeepSecret.”

Ex 1. AT-WA7400# **set interface wlan0 wpa-personal-key "secret !"**

or

Ex 2. AT-WA7400# **set interface wlan0 wpa-personal-key KeepSecret**

Note

Shared secret keys can include spaces and special characters if the key is placed inside quotation marks as in the first example above. If the key is a string of characters with no spaces or special characters in it, the quotation marks are not necessary as in the second example above.

5. Get Current Security Settings After Reconfiguring to WPA/WPA2 Personal (PSK)

Now use the **get** command again to view the updated security configuration and see the results of the new settings.

The following command gets the security mode in use on the internal network:

```
AT-WA7400# get interface wlan0 security
wpa-personal
```

The following command gets details on how the internal network is configured, including details on Security.

```
AT-WA7400# get bss wlan0bssInternal detail
```

| Field | Value |
|----------------------------|-------------------|
| status | up |
| description | Internal |
| radio | wlan0 |
| beacon-interface | wlan0 |
| mac | 00:0C:41:16:DF:A6 |
| dtim-period | |
| max-stations | |
| ignore-broadcast-ssid | off |
| mac-acl-mode | deny-list |
| mac-acl-name | wlan0bssInternal |
| radius-accounting | |
| radius-ip | 127.0.0.1 |
| radius-key | secret |
| open-system-authentication | |
| shared-key-authentication | |
| wpa-allow-non-wpa-stations | |
| wpa-cipher-tkip | on |
| wpa-cipher-ccmp | on |

```
wpa-allowed on
wpa2-allowed on
rsn-preauthentication
```

Set Security to WPA/WPA2 Enterprise (RADIUS)

Set the Security Mode

```
AT-WA7400# set interface wlan0 security wpa-enterprise
```

Set the WPA Versions

Select the WPA version based on what types of client stations you want to support, as shown in Table 18.

Table 18. WPA Version Command

| Function | Command |
|--|--|
| WPA: If all client stations on the network support the original WPA but none support the newer WPA2, then use WPA. | <pre>set bss wlan0bssInternal wpa-allowed on set bss wlan0bssInternal wpa2-allowed off</pre> |
| WPA2: If all client stations on the network support WPA2, use WPS2 which provides the best security based on the IEEE 802.11i standard. | <pre>set bss wlan0bssInternal wpa-allowed off set bss wlan0bssInternal wpa2-allowed on</pre> |
| Both: If you have a mix of clients, some of which support WPS2 and others which support only the original WPA, use Both. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients that support it. This WPA configuration allows more interoperability at the expense of some security. | <pre>set bss wlan0bssInternal wpa-allowed on set bss wlan0bssInternal wpa2-allowed on</pre> |

For this example, set the access point to support WPA client stations only:

```
AT-WA7400# set bss wlan0bssInternal wpa-allowed on
AT-WA7400# set bss wlan0bssInternal wpa2-allowed off
```

Enable Pre-Authentication

If you set WPA versions to “WPA2” or “Both,” you can enable *pre-*

authentication for WPA2 clients, as shown in Table 19..

Table 19. Preauthentication Commands

| Function | Command |
|---|--|
| Enable pre-authentication if you want WPA2 wireless clients to send pre-authentication packet. The pre-authentication information will be relayed from the access point the client is currently using to the target access point. Enabling this feature can help speed up authentication for roaming clients who connect to multiple access points. | <code>set bss wlan0bssInternal rsn-preauthentication on</code> |
| To disable pre-authentication for WPA2 clients: | <code>set bss wlan0bssInternal rsn-preauthentication on</code> |

This option does not apply if you set the WPA Version to support “WPA” clients only because the original WPA does not support this pre-authentication

For our example, we'll disable pre-authentication.

```
AT-WA7400# set bss wlan0bssInternal rsn-preauthentication off
```

Set the Cipher Suites

Set the cipher suite you want to use. The options are shown in Table 20.

Table 20. Cipher Commands

| Function | Commands |
|--|--|
| TKIP: Temporal Key Integrity Protocol (TKIP), which is the default. | <code>set bss wlan0bssInternal wpa-cipher-tkip on</code> <code>set bss wlan0bssInternal wpa-cipher-ccmp off</code> |
| CCMP (AES): Counter mode/ CBC-MAC protocol (CCMP) is an encryption method for IEEE 802.11i. that uses the Advanced Encryption Algorithm (AES). | <code>set bss wlan0bssInternal wpa-cipher-tkip off</code> <code>set bss wlan0bssInternal wpa2-cipher-ccmp on</code> |

Table 20. Cipher Commands (Continued)

| Function | Commands |
|---|---|
| Both: When the authentication algorithm is set to Both, both TKIP and AES clients can associate with the access point. WPA clients must have either a valid TKIP key or a valid CCMP (AES) key to be able to associate with the access point. | <pre>set bss wlan0bssInternal wpa-cipher-tkip on set bss wlan0bssInternal wpa2-cipher-ccmp on</pre> |

In this example, the cipher suite is set to **TKIP Only**:

```
AT-WA7400# set bss wlan0bssInternal wpa-cipher-tkip on
AT-WA7400# set bss wlan0bssInternal wpa-cipher-ccmp off
```

Set the Authentication Server

You can use the built-in authentication server on the access point or an external RADIUS server. The commands are shown in Table 21.

Note

To use the built-in authentication server, set the RADIUS IP address to that used by the built-in server (127.0.0.1) and turn RADIUS accounting off because it is not supported by the built-in server.

Table 21. Authentication Server Commands

| Function | Commands |
|--|--|
| Set the access point to use the built-in authentication server | <pre>set bss wlan0bssInternal radius-ip 127.0.0.1</pre> |
| Set the access point to use an external RADIUS server | <pre>set bss wlan0bssInternal radius-ip RADIUS_IP_Address</pre> <p>where <i>RADIUS_IP_Address</i> is the IP address of an external RADIUS server</p> |

In this example, an external RADIUS server with an IP address of 142.77.1.1 is used as the authentication server:

```
AT-WA7400# set bss wlan0bssInternal radius-ip 142.77.1.1
```

Set the RADIUS Key (For External RADIUS Server Only)

If you use an external RADIUS server, you must provide the RADIUS key. (If you use the built-in authentication server the RADIUS key is automatically provided.)

This command sets the RADIUS key to keepSecret for an external RADIUS server.

```
AT-WA7400# set bss wlan0bssInternal radius-key keepSecret
```

Enable RADIUS Accounting (External RADIUS Server Only)

You can enable RADIUS Accounting if you want to track and measure the resources a particular user has consumed such system time, amount of data transmitted and received, and so on. The commands to enable or disable RADIUS accounting are shown in Table 22.

Note

RADIUS accounting is not supported by the built-in server, so if you are using the built-in server make sure that RADIUS accounting is off.

Table 22. RADIUS Accounting Commands

| Function | Command |
|---------------------------|--|
| Enable RADIUS accounting | set bss wlan0bssInternal radius-accounting on |
| Disable RADIUS accounting | set bss wlan0bssInternal radius-accounting off |

For our example, we'll enable RADIUS accounting for our external RADIUS server:

```
AT-WA7400# set bss wlan0bssInternal radius-accounting on
```

Allow Non-WPA Clients

You can let non-WPA (802.11), unauthenticated client stations use this access point by setting the "wpa-allowed" option to "on." The commands are listed in Table 23.

Table 23. WPA Client Commands

| Function | Command |
|--------------------------|---|
| Allow non-WPA clients | set bss wlan0bssInternal wpa-allowed on |
| Disallow non WPA clients | set bss wlan0bssInternal wpa2-allowed off |

For this example, allow non-WPA clients:

```
AT-WA7400# set bss wlan0bssInternal wpa-allowed on
```

Get Current Security Settings After Reconfiguring to WPA/WPA2 Enterprise (RADIUS)

Use the **get** command again to view the updated security configuration

and see the results of our new settings.

The following command gets the security mode in use on the internal network:

```
AT-WA7400# get interface wlan0 security
wpa-enterprise
```

The following command gets details on how the internal network is configured, including details on Security.

```
AT-WA7400# get bss wlan0bssInternal detail
```

| Field | Value |
|----------------------------|-------------------|
| status | up |
| description | Internal |
| radio | wlan0 |
| beacon-interface | wlan0 |
| mac | 00:0C:41:16:DF:A6 |
| dtim-period | 2 |
| max-stations | 2007 |
| ignore-broadcast-ssid | off |
| mac-acl-mode | deny-list |
| mac-acl-name | wlan0bssInternal |
| radius-accounting | on |
| radius-ip | 142.77.1.1 |
| radius-key | KeepSecret |
| open-system-authentication | on |
| shared-key-authentication | off |
| wpa-allow-non-wpa-stations | off |
| wpa-cipher-tkip | on |
| wpa-cipher-ccmp | off |
| wpa-allowed | on |
| wpa2-allowed | off |

```
rsn-preauthentication      off
```

Enabling and Configuring the Guest Login Welcome Page

The guest login and welcome page commands are shown in Table 24.

Table 24. Guest Login and Welcome Page Commands

| Function | Command |
|--|---|
| View all guest login settings | <code>get portal</code> |
| Enable guest login and Welcome page | <code>set portal status up</code> |
| Disable guest login and Welcome page | <code>set portal status down</code> |
| Specify Guest Welcome page text for the captive portal | <code>set portal welcome-screen-text "welcome Screen Text"</code> Where " <i>welcome Screen Text</i> " is the content of the Welcome message you want displayed on the Guest Welcome page. The Welcome message must be in quotes if it contains spaces, punctuation, and special characters. |

Note

Guest login settings are only relevant if you have first configured a guest network. For information about configuring a guest network, see Chapter 11, "Setting Up Guest Access" on page 133.

You can set up a captive portal that guest clients will see when they log on to the guest network. or modify the Welcome screen guest clients see when they open a web browser or try to browse the web.

View Guest Login Settings

To view the current settings for guest login:

```
AT-WA7400# get portal
```

```
Field                value
```

```
-----
```

```
status                down
```

```
welcome-screen        on
```

welcome-screen-text Thank you for using wireless Guest Access as provided by this Allied Telesyn AT-WA7400 wireless access point. When you click "Accept", you will gain access to our wireless guest network. This network allows complete access to the Internet but is external to the corporate network. Please note that this network is not configured to provide any level of wireless security.

Enable/Disable the Guest Welcome Page

To enable the Guest Welcome page:

```
AT-WA7400# set portal status up
```

To disable the Guest Welcome page:

```
AT-WA7400# set portal status down
```

Set Guest Welcome Page Text

To specify the text for the Guest Welcome page:

```
AT-WA7400# set portal welcome-screen-text "welcome to the wireless Network"
```

Review Guest Login Settings

The following example shows the results of the set portal command after specifying some new settings:

```
AT-WA7400# get portal
```

| Field | Value |
|---------------------|---------------------------------|
| status | up |
| welcome-screen | on |
| welcome-screen-text | welcome to the wireless Network |

Configuring Multiple BSSIDs on Virtual Wireless Networks

Note

Before you configure this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 278. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface, the internal or guest network, or (on a two-radio access point) to radio one or radio two.

Configuring Virtual Wireless Network “One” on Radio One

Configure These Settings from the Web UI First

- ❑ On the Advanced > Ethernet (Wired) settings page in the web UI, enable virtual wireless networks as described in “Enabling or Disabling Virtual Wireless Networks on the Access Point” on page 90.
- ❑ On the Advanced > Virtual Wireless Networks page in the web UI, provide a VLAN ID as described in “Configuring VLANs” on page 140.

Use the CLI to Configure Security on the Interface

The following example shows commands for configuring WPA/WPA2 Enterprise (RADIUS) security mode, allowing Both WPA and WPA2 clients to authenticate and using a TKIP cipher suite:

```
AT-WA7400# set bss wlan0bssvwn1 open-system-authentication on
AT-WA7400# set bss wlan0bssvwn1 shared-key-authentication on
AT-WA7400# set bss wlan0bssvwn1 wpa-allowed on
AT-WA7400# set bss wlan0bssvwn1 wpa2-allowed on
AT-WA7400# set bss wlan0bssvwn1 wpa-cipher-tkip on
AT-WA7400# set bss wlan0bssvwn1 wpa-cipher-ccmp off
AT-WA7400# set bss wlan0bssvwn1 radius-ip 127.0.0.1
AT-WA7400# set bss wlan0bssvwn1 radius-ip 127.0.0.1
AT-WA7400# set bss wlan0bssvwn1 radius-key secret
AT-WA7400# set bss wlan0bssvwn1 status up
AT-WA7400# set interface wlan0vwn1 security wpa-enterprise
```

Use the CLI to set the Network Name (SSID) for the New Virtual Wireless Network

```
AT-WA7400# set interface wlan0vwn1 ssid my-vwn-one
```

Creating VWN “Two” on Radio One with WPA security

To configure the second virtual wireless network, repeat the previous procedures as with the following differences:

- ❑ Create a second VLAN ID from the web UI with a new SSID
- ❑ In the CLI commands, replace wlan0bssvwn1 with wlan0bssvwn2.

Radio Settings

Note

Before you configure this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 278. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface, the internal or guest network, or (on a two-radio access point) to radio one or radio two.

Table 25 provides a quick view of Radio Settings commands.

Table 25. Radio Settings Commands

| Function | Command |
|----------------------------|--|
| Get Radio Settings | get radio get radio wlan0 get radio wlan0 detail |
| Get IEEE 802.11 Radio Mode | get radio wlan0 mode |
| Get Radio Channel | get radio wlan0 channel |
| Get Basic Radio Settings | get radio wlan0 |
| Get All Radio Settings | get radio wlan0 detail |
| Get Supported Rate Set | get supported-rate |
| Get Basic Rate Set | get basic-rate |

Get IEEE 802.11 Radio Mode

To get the current setting for radio Mode:

```
AT-WA7400# get radio wlan0 mode
```

(The radio in the example is using IEEE 802.11g mode.)

Get Radio Channel

To get the current setting for radio Channel:

```
AT-WA7400# get radio wlan0 channel
6
```

(The radio in this example is on Channel 6.)

Get Basic Radio Settings

To get basic current radio settings:

```
AT-WA7400# get radio wlan0
```

| Field | Value |
|----------------|--------|
| status | up |
| mac | |
| channel-policy | static |
| mode | g |
| static-channel | 6 |
| channel | 6 |
| tx-rx-status | up |

Get All Radio Settings

To get all current radio settings: get radio wlan0 detail

```
AT-WA7400# get radio wlan0 detail
```

| Field | Value |
|----------------|-------------|
| status | up |
| description | IEEE 802.11 |
| mac | |
| max-bss | 2 |
| channel-policy | static |

```

mode g
static-channel 6
channel 6
tx-power 100
tx-rx-status up
beacon-interval 100
rts-threshold 2347
fragmentation-threshold 2346
load-balance-disassociation-utilization 0
load-balance-disassociation-stations 0
load-balance-no-association-utilization 0
ap-detection off
station-isolation off
frequency 2437
wme on
    
```

Get Supported Rate Set

The *Supported Rate Set* is what the access point supports. The access point will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the access point.

```
AT-WA7400# get supported-rate
```

```

name    rate
-----
wlan0   54
wlan0   48
wlan0   36
wlan0   24
wlan0   18
wlan0   12
wlan0   11
wlan0   9
    
```



```
wlan0 6
wlan0 5.5
wlan0 2
wlan0 1
```

Get Basic Rate Set

The *Basic Rate Set* is what the access point will advertise to the network for the purposes of setting up communication with other access points and client stations on the network. It is generally more efficient to have an access point broadcast a subset of its supported rate sets.

```
AT-WA7400# get basic-rate
```

```
name    rate
-----
wlan0  11
wlan0  5.5
wlan0  2
wlan0  1
```

Configure Radio Settings

Note

To get a list of all fields you can set on the access point radio, type the following at the CLI prompt: `set radio wlan0 [SpaceKey] [TAB] [TAB]`.

Turn the Radio On or Off

The commands to turn the radio on or off are listed in Table 26.

Table 26. Radio Operation Commands

| Function | Command |
|--------------------|---|
| Turn the radio on | <code>set radio wlan0 status on</code> |
| Turn the radio off | <code>set radio wlan0 status off</code> |

Set the Radio Mode

Valid values depend on the capabilities of the radio. Possible values and

how you would use the CLI to set each one are shown in Table 27.

Table 27. Radio Mode Commands

| Function | Command |
|-------------------------------|---|
| IEEE 802.11b | set radio wlan0 mode b |
| IEEE 802.11g | set radio wlan0 mode g |
| IEEE 802.11a | set radio wlan0 mode a |
| Atheros Turbo 5 GHz | set radio wlan0 mode turbo-a |
| Atheros Dynamic Turbo 5 GHz | set radio wlan0 mode dynamic-turbo-a |
| Atheros Turbo 2.4 GHz | set radio wlan0 mode turbo-g |
| Atheros Dynamic Turbo 2.4 GHz | set radio wlan0 mode dynamic-turbo-g |

The following command sets the wireless mode to IEEE 802.11g:

```
AT-WA7400# set radio wlan0 mode g
```

Enable or Disable Super AG

You cannot enable/disable Super AG from the CLI. You must set this from the web UI. For information on how to set this option, please see the field description for this option in “Configuring Radio Settings” on page 147.

Set the Radio Channel

The following command sets the Channel to 6:

```
AT-WA7400# set radio wlan0 channel 6
```

Set the Beacon Interval

The following command sets the beacon interval to 80.

```
AT-WA7400# set radio wlan0 beacon-interval 80
```

Set the DTIM Period

The Delivery Traffic Information Map (DTIM) period indicates how often wireless clients should check to see if they have buffered data on the access point awaiting pickup. The measurement is in beacons. Specify a DTIM period within a range of 1 - 255 beacons. For example, if you set this to “1,” clients will check for buffered data on the access point at every beacon. If you set this to “2,” clients will check on every other beacon.

The following command sets the DTIM interval to 3.

```
AT-WA7400# set bss wlan0bssInternal dtim-period 3
```

To get the updated value for DTIM interval after you have changed it:

```
AT-WA7400# get bss wlan0bssInternal dtim-period
```

```
3
```

Set the Fragmentation Threshold

You can specify a fragmentation threshold as a number between 256 and 2,346 to set the frame size threshold in bytes. The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function will be activated and the packet will be sent as multiple 802.11 frames. If the packet being transmitted is equal to or less than the threshold, fragmentation will not be used. Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation.

The following command sets the fragmentation threshold to 2000.

```
AT-WA7400# set radio wlan0 fragmentation-threshold 2000
```

Set the RTS Threshold

You can specify an RTS Threshold value between 0 and 2347. The RTS threshold specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, especially one with a lot of clients.

The following command sets the RTS threshold at

```
AT-WA7400# set radio wlan0 rts-threshold 2346
```

Configure Basic and Supported Rate Sets

The rate set commands are shown in Table 28.

Table 28. Rate Set Commands

| Function | Command |
|-------------------------|---|
| Add a basic rate set | add basic-rate <i>wirelessInterface</i> rate <i>SomeRate</i> For example: add basic-rate wlan0 rate 48 |
| Get current basic rates | get basic-rate |

Table 28. Rate Set Commands (Continued)

| Function | Command |
|-----------------------------|---|
| Add supported rate | add supported-rate <i>wirelessInterfaceName</i> rate <i>SomeRate</i> For example: add supported-rate wlan0 rate 9 |
| Get current supported rates | get supported-rate wlan0 |

The following command adds “48” as a basic rate to wlan0 (the internal, wireless interface):

```
AT-WA7400# add basic-rate wlan0 rate 48
```

To get the basic rates currently configured for this access point:

```
AT-WA7400# get basic-rate
```

```
name    rate
-----
wlan0   11
wlan0   5.5
wlan0   2
wlan0   1
wlan1   24
wlan1   12
wlan1   6
wlan0   48
```

The following command adds “9” as a supported rate to wlan0 (the internal, wireless interface):

```
AT-WA7400# add supported-rate wlan0 rate 9
```

To get the supported rates currently configured for this access point (using wlan0 as the interface for this example):

```
AT-WA7400# get supported-rate wlan0
```

```
rate
----
```

1
2
5.5
6
11
12
18
24
36
48
54
9

Note

You can use the `get` command to view current rate sets from the CLI as described in “Get Supported Rate Set” on page 328 and “Get Basic Rate Set” on page 329. However, you cannot reconfigure Supported Rate Sets or Basic Rate Sets from the CLI. You must use the Advanced > Radio page on the web UI to configure this feature.

MAC Filtering**Note**

Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 278. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface, the internal or guest network, or (on a two-radio access point) to radio one or radio two.

You can control access to AT-WA7400 Wireless Access Point based on media access control (MAC) addresses. Based on how you set the filter, you can *allow* only client stations with a listed MAC address or *prevent* access to the stations listed.

Specify an Accept or Deny List

To set up MAC filtering you first need to specify which type of list you want

to configure. The commands are shown in Table 29.

Table 29. Accept and Deny List Commands

| Function | Command |
|---|--|
| Set up an Accept list: (With this type of list, client stations whose MAC addresses are listed will be allowed access to the access point.) | <code>set bss wlan0bssInternal mac-acl-mode accept-list</code> |
| Set up a Deny list: (With this type of list, the access point will prevent access to client stations whose MAC addresses are listed.) | <code>set bss wlan0bssInternal mac-acl-mode deny-list</code> |

Add MAC Addresses of Client Stations to the Filtering List

To add a MAC address to the list:

```
add mac-acl wlan0bssInternal mac MAC_Address_of_Client
```

Where *MAC_Address_of_Client* is the MAC address of a wireless client you want to add to the MAC filtering list.

For example, to add 4 new clients to the list with the following MAC addresses:

```
AT-WA7400# add mac-acl wlan0bssInternal mac 00:01:02:03:04:05
```

```
AT-WA7400# add mac-acl wlan0bssInternal mac 00:01:02:03:04:06
```

```
AT-WA7400# add mac-acl wlan0bssInternal mac 00:01:02:03:04:07
```

```
AT-WA7400# add mac-acl wlan0bssInternal mac 00:01:02:03:04:08
```

Remove a Client Station's MAC Address from the Filtering List

To remove a MAC address from the list:

```
remove mac-acl wlan0bssInternal mac MAC_Address_of_Client
```

Where *MAC_Address_of_Client* is the MAC address of a wireless client you want to remove from the MAC filtering list.

For example:

```
AT-WA7400# remove mac-acl wlan0bssInternal mac 00:01:02:03:04:04
```

Getting Current MAC Filtering Settings

Get the Type of MAC Filtering List Currently Set (Accept or Deny)

The following command shows which type of MAC filtering list is currently configured:

```
AT-WA7400# get bss wlan0bssInternal mac-acl-mode
accept-list
```

Get MAC Filtering List

The following command shows the clients on the MAC filtering list:

```
AT-WA7400# get mac-acl
name                mac
-----
wlan0bssInternal    00:01:02:03:04:05
wlan0bssInternal    00:01:02:03:04:06
wlan0bssInternal    00:01:02:03:04:07
wlan0bssInternal    00:01:02:03:04:08
```

Load Balancing

Note

Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 278. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface, the internal or guest network, or (on a two-radio access point) to radio one or radio two.

Load balancing parameters affect the distribution of wireless client connections across multiple access points. Using load balancing, you can prevent scenarios where a single access point in your network shows performance degradation because it is handling a disproportionate share of the wireless traffic. (For a detailed conceptual overview of Load Balancing, see Chapter 14, “Load Balancing” on page 155.)

The access point provides default settings for load balancing.

The following command examples reconfigure some load balancing settings and get details on the configuration:

```
AT-WA7400# set radio wlan0 load-balance-disassociation-stations 2
```

```
AT-WA7400# get radio wlan0 load-balance-disassociation-stations
2
AT-WA7400# set radio wlan0 load-balance-disassociation-
utilization 25
AT-WA7400#
AT-WA7400# get radio wlan0 load-balance-disassociation-
utilization
25
AT-WA7400# set radio wlan0 load-balance-no-association-
utilization 50
AT-WA7400#
AT-WA7400# get radio wlan0 load-balance-no-association-
utilization
50
```

Quality of Service

Note

Before configuring this feature from the CLI, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 278. The interface name referenced in a command determines if a setting applies to a wired or wireless interface, the internal or guest network, or (on a two-radio access point) to radio one or radio two.

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like *Voice-over-IP* (VoIP), other types of audio, video, and streaming media as well as traditional IP data over the AT-WA7400 Wireless Access Point.

For a complete conceptual overview of QoS, see “Understanding QoS” on page 162.

Table 30 provides a quick view of QoS commands.

Table 30. QoS Commands

| Function | Command |
|--|--|
| Enable/Disable Wi-Fi Multimedia | <pre>set radio wlan0 wme off set radio wlan0 wme on get radio wlan0 wme</pre> |
| About Access Point and Station EDCA Parameters | See “About Access Point and Station EDCA Parameters” on page 338. |
| Understanding the Queues for Access Point and Station | See “Understanding the Queues for Access Point and Station” on page 339. |
| Distinguishing between Access Point and Station Settings in QoS Commands | See “Distinguishing between Access Point and Station Settings in QoS Commands” on page 339 |
| Get QoS Settings on the Access Point | get tx-queue |
| Get QoS Settings on the Client Station | get wme-queue |
| Set Arbitration Interframe Spaces (aifs) | <p>On the access point:</p> <pre>set wme-queue wlan0 with queue <i>Queue_Name</i> to aifs <i>AIFs_Value</i></pre> <p>On a client station:</p> <pre>set wme-queue wlan0 with queue <i>Queue_Name</i> to aifs <i>AIFs_Value</i></pre> <p>See examples in “Set Arbitration Interframe Spaces (aifs)” on page 340.</p> |
| Set Minimum and Maximum Contention Windows (cwmin, cwmax) | <p>On the access point:</p> <pre>set tx-queue wlan0 with queue <i>Queue_Name</i> to cwmin <i>cwmin_Value</i> cwmax <i>cwmax_Value</i></pre> <p>On a client station:</p> <pre>set wme-queue wlan0 with queue <i>Queue_Name</i> to cwmin <i>cwmin_Value</i> cwmax <i>cwmax_Value</i></pre> <p>See examples in “Set Minimum and Maximum Contention Windows (cwmin, cwmax)” on page 341.</p> |
| Set the Maximum Burst Length (burst) on the Access Point | <pre>set tx-queue wlan0 with queue <i>Queue_Name</i> to burst <i>burst_Value</i></pre> <p>See examples in “Set the Maximum Burst Length (burst) on the Access Point” on page 343.</p> |

Table 30. QoS Commands (Continued)

| Function | Command |
|---|---|
| Set Transmission Opportunity Limit (txop-limit) for WMM client stations | <pre>set wme-queue wlan0 with queue <i>Queue_Name</i> to txop-limit <i>txop-limit_value</i></pre> <p>See examples in “Set Transmission Opportunity Limit (txop-limit) for WMM client stations” on page 344.</p> |

Enable/Disable Wi-Fi Multimedia

By default, Wi-Fi MultiMedia (WMM) is enabled on the access point. With WMM enabled, QoS settings on the AT-WA7400 Wireless Access Point control both *downstream* traffic flowing from the access point to client station (access point EDCA parameters) and *upstream* traffic flowing from the station to the access point (station EDCA parameters). Enabling WMM essentially activates station-to-access point QoS control.

Disabling WMM will deactivate QoS control of station EDCA parameters on *upstream* traffic flowing from the station to the access point. With WMM disabled, you can still set downstream access point-to-station QoS parameters but no station-to-access point QoS parameters.

- ❑ To disable WMM:

```
AT-WA7400# set radio wlan0 wme off
AT-WA7400# get radio wlan0 wme
off
```

- ❑ To enable WMM:

```
AT-WA7400# set radio wlan0 wme on
AT-WA7400# get radio wlan0 wme
on
```

About Access Point and Station EDCA Parameters

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station (access point-to-station).

Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the access point (station-to-access point). Keep in mind that station-to-access point parameters apply only when WMM is enabled as described in “Enable/Disable Wi-Fi Multimedia” on page 338 above.

Understanding the Queues for Access Point and Station

The same types of queues are defined for different kinds of data transmitted from access point-to-station and station-to-access point but they are referenced by differently depending on whether you are configuring access point or station parameters. The commands are shown in Table 31.

Table 31. Queue Commands

| Data | Access Point | Station |
|---|--------------|---------|
| Voice - High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. | data0 | vo |
| Video - High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. | data1 | vi |
| Best Effort - Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. | data2 | be |
| Background - Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). | data3 | bk |

Distinguishing between Access Point and Station Settings in QoS Commands

Access Point - To get and set QoS settings on the access point (access point), use **tx-queue** class name in the command.

Station - To get and set QoS settings on the client station, use the **wme-queue** class name in the command.

Get QoS Settings on the Access Point

To view the current QoS settings and queue names for access point-to-station parameters:

```
AT-WA7400# get tx-queue
```

```
name   queue  aifs  cwmin  cwmax  burst
-----
wlan0  data0  1     3      7      1.5
wlan0  data1  1     7      15     3.0
wlan0  data2  3     15     63     0
```

```
wlan0 data3 7 15 1023 0
```

Get QoS Settings on the Client Station

To view the current QoS settings queue names for station-to-access point parameters:

```
AT-WA7400# get wme-queue
```

```
name queue aifs cwmin cwmmax txop-limit
```

```
-----
```

```
wlan0 vo 2 3 7 47
```

```
wlan0 vi 2 7 15 94
```

```
wlan0 be 3 15 1023 0
```

```
wlan0 bk 7 15 1023 0
```

Set Arbitration Interframe Spaces (aifs)

Arbitration Inter-Frame Spacing (AIFs) specifies a wait time (in milliseconds) for data frames.

Valid values for AIFs are 1-255.

Set AIFs on the Access Point

To set AIFs on access point-to-station traffic:

```
set tx-queue wlan0 with queue Queue_Name to aifs AIFs_Value
```

Where *Queue_Name* is the queue on the access point to which you want the setting to apply and *AIFs_Value* is the wait time value you want to specify for AIFs.

For example, this command sets the AIFs wait time on the access point Voice queue (data0) to 13 milliseconds.

```
AT-WA7400# set tx-queue wlan0 with queue data0 to aifs 13
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
AT-WA7400# get tx-queue
```

```
name queue aifs cwmin cwmmax burst
```

```
-----
```

```
wlan0 data0 13 3 7 1.5
```

```
wlan0 data1 1 7 15 3.0
wlan0 data2 3 15 63 0
wlan0 data3 7 15 1023 0
```

Set AIFs on the Client Station

To set the AIFs on station-to-access point traffic:

```
set wme-queue wlan0 with queue Queue_Name to aifs AIFs_Value
```

Where *Queue_Name* is the queue on the station to which you want the setting to apply and *AIFs_Value* is the wait time value you want to specify for AIFs.

For example, this command sets the AIFs wait time on the station Voice queue (vo) to 14 milliseconds.

```
AT-WA7400# set wme-queue wlan0 with queue vo to aifs 14
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
AT-WA7400# get wme-queue
```

```
name  queue  aifs  cwmin  cymax  txop-limit
-----
wlan0  vo      14   3      7      47
wlan0  vi      2      7      15     94
wlan0  be      3      15     1023   0
wlan0  bk      7      15     1023   0
```

Set Minimum and Maximum Contention Windows (cwmin, cymax)

The Minimum Contention Window (*cwmin*) sets the upper limit (in milliseconds) of the range from which the initial random backoff wait time is determined. For more details, see “Random Backoff and Minimum / Maximum Contention Windows” on page 165 and the more detailed field description for this value in that topic.)

Valid values for the *cwmin* are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for *cwmin* must be lower than the value for *cymax*.

The Maximum Contention Window (*cymax*) sets the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. For more details, see “Random Backoff and Minimum / Maximum Contention Windows” on page 165 and the more

detailed field description for this value in that topic.)

Valid values for the `cwmax` are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for `cwmax` must be higher than the value for `cwmin`.

Set `cwmin` and `cwmax` on the Access Point

To set the Minimum and Maximum Contention Windows (`cwmin`, `cwmax`) on access point-to-station traffic:

```
set tx-queue wlan0 with queue Queue_Name to cwmin cwmin_value
cwmax cwmax_value
```

Where *Queue_Name* is the queue on the access point to which you want the setting to apply and *cwmin_value* and *cwmax_value* are the values (in milliseconds) you want to specify for contention back-off windows.

For example, this command sets the access point Video queue (`data1`) `cwmin` value to 15 and `cwmax` value to 31.

```
AT-WA7400# set tx-queue wlan0 with queue data1 cwmin 15 cwmax 31
```

View the results of this configuration update (bold in the command output highlights the modified values):

```
AT-WA7400# get tx-queue
```

```
name  queue  aifs  cwmin  cwmax  burst
-----
wlan0  data0  13    3      7      1.5
wlan0  data1  1     15   31   3.0
wlan0  data2  3     15    63    0
wlan0  data3  7     15    1023  0
```

Set `cwmin` and `cwmax` on the Station

To set the Minimum and Maximum Contention Windows (`cwmin`, `cwmax`) on station-to-access point traffic:

```
set wme-queue wlan0 with queue Queue_Name to cwmin cwmin_value
cwmax cwmax_value
```

Where *Queue_Name* is the queue on the station to which you want the setting to apply and *cwmin_value* and *cwmax_value* are the values (in milliseconds) you want to specify for contention back-off windows.

For example, this command sets the client station Video queue (`vi`) `cwmin` value to 15 and `cwmax` value to 31.

```
AT-WA7400# set wme-queue wlan0 with queue vi cwmn 7 cwmx 15
```

View the results of this configuration update (bold in the command output highlights the modified values):

```
AT-WA7400# get wme-queue
```

```
name  queue  aifs  cwmn  cwmx  txop-limit
-----
wlan0  vo     14    3     7     47
wlan0  vi     2     7     15    94
wlan0  be     3     15    1023  0
wlan0  bk     7     15    1023  0
```

Set the Maximum Burst Length (burst) on the Access Point

The Maximum Burst Length (burst) specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The `burst` applies only to the access point (access point-to-station traffic).

Valid values for maximum burst length are 0.0 through 999.9.

To set the maximum burst length on access point-to-station traffic:

```
set tx-queue wlan0 with queue Queue_Name to burst burst_value
```

Where *Queue_Name* is the queue on the access point to which you want the setting to apply and *burst_value* is the wait time value you want to specify for maximum burst length.

For example, this command sets the maximum packet burst length on the access point Best Effort queue (data2) to 0.5.

```
AT-WA7400# set tx-queue wlan0 with queue data2 to burst 0.5
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
AT-WA7400# get tx-queue
```

```
name  queue  aifs  cwmn  cwmx  burst
-----
wlan0  data0  13    3     7     1.5
wlan0  data1  1     15    31    3.0
```

```
wlan0 data2 3 15 63 0.5
wlan0 data3 7 15 1023 0
```

Set Transmission Opportunity Limit (txop-limit) for WMM client stations

The Transmission Opportunity Limit (txop-limit) specifies an interval of time (in milliseconds) when a WMM client station has the right to initiate transmissions on the wireless network. The txop-limit applies only to the client stations (station-to-access point traffic).

To set the txop-limit on station-to-access point traffic:

```
set wme-queue wlan0 with queue Queue_Name to txop-limit txop-limit_value
```

Where *Queue_Name* is the queue on the station to which you want the setting to apply and *txop-limit_value* is the value you want to specify for the txop-limit.

For example, this command sets the txop-limit on the station Voice queue (vo) to 49.

```
AT-WA7400# set wme-queue wlan0 with queue vo to txop-limit 49
```

View the results of this configuration update (bold in the command output highlights the modified value):

```
AT-WA7400# get wme-queue

name  queue  aifs  cwmin  cwmax  txop-limit
-----
wlan0  vo     14    3      7      49
wlan0  vi     2     7      15     94
wlan0  be     3     15     1023   0
wlan0  bk     7     15     1023   0
```

Wireless Distribution System

Note

Before configuring this feature, make sure you are familiar with the names of the interfaces as described in “Understanding Interfaces as Presented in the CLI” on page 278. The interface name you reference in a command determines whether a setting applies to a wired or wireless interface, the internal or guest network, or (on a two-radio access point) to radio one or radio two.

Table 32 provides a list of the WDS commands.

Table 32. WDS Commands

| Function | Command |
|------------------------------------|---|
| Configure a WDS Link | See detailed command example below. |
| Get Details on a WDS Configuration | <code>get interface wlan0wds0 detail</code> |

Configure a WDS Link

To set up a wireless distribution system (WDS) link between two wireless networks:

Enable the WDS interface (`wlan0wds0`) on the current access point:

```
AT-WA7400# set interface wlan0wds0 status up
```

```
AT-WA7400# set interface wlan0wds0 radio wlan0
```

Provide the MAC address of the remote access point to which you want to link:

```
AT-WA7400# set interface wlan0wds0 remote-mac
MAC_Address_of_Remote_AP
```

For example:

```
AT-WA7400# set interface wlan0wds0 remote-mac 00:E0:B8:76:1B:14
```

Get Details on a WDS Configuration

Verify the configuration of the WDS link you just configured by getting details on the WDS interface:

```
AT-WA7400# get interface wlan0wds0 detail
```

```
Field                value
-----
type                 wds
status               up
description          wireless Distribution System - Link 1
mac                  00:E0:B8:76:26:08
ip
mask
```

```
static-ip
static-mask
nat
rx-bytes      0
rx-packets    0
rx-errors     0
rx-drop       0
rx-fifo       0
rx-frame      0
rx-compressed 0
rx-multicast  0
tx-bytes      0
tx-packets    0
tx-errors     0
tx-drop       0
tx-fifo       0
tx-colls      0
tx-carrier    0
tx-compressed 0
port-isolation
ssid
bss
security
wpa-personal-key
wep-key-ascii    no
wep-key-length   104
wep-default-key
wep-key-1
wep-key-2
```

```
wep-key-3
wep-key-4
vlan-interface
vlan-id
radio          wlan0
remote-mac     00:E0:B8:76:1B:14
```

Time Protocol

The *Network Time Protocol* (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock. The timestamp will be used to indicate the date and time of each event in log messages. See <http://www.ntp.org> for more general information on NTP.

To enable the Network Time Protocol (NTP) server on the access point do the following:

1. Enable the NTP Server.

```
ntp status up
```

2. Provide the Host Name or Address of an NTP Server.

```
ntp server NTP_Server
```

Where *NTP_Server* is the host name or IP address of the NTP server you want to use. (Allied Telesyn recommends using the host name rather than the IP address, because IP addresses change more frequently.)

For example, this command sets the NTP server by host name to "ntp.at-wa7400.com":

```
ntp server ntp.at-wa7400.com
```

3. Get the Current Time Protocol Settings.

```
AT-WA7400# get ntp detail
```

```
Field  value
```

```
-----
```

```
status  up
```

```
server  ntp.at-wa7400.com
```

Rebooting the Access Point

To reboot the access point, type `reboot` at the command line:

```
AT-WA7400# reboot
```

Resetting the Access Point to the Factory Defaults

If you are experiencing extreme problems with the AT-WA7400 Wireless Access Point and have tried all other troubleshooting measures, you can reset the access point. This will restore factory defaults and clear all settings, including settings such as a new password or wireless settings.

The following command resets the access point from the CLI:

```
AT-WA7400# factory-reset
```

Note

Keep in mind that the `factory-reset` command resets only the access point you are currently administering; not other access points in the cluster.

For information on the factory default settings, see Appendix A, “Management Software Default Settings” on page 215.

Keyboard Shortcuts and Tab Completion Help

The CLI provides keyboard shortcuts to help you navigate the command line and build valid commands, along with “tab completion” hints on available commands that match what you have typed so far. Using the CLI will be easier if you use the tab completion help and learn the keyboard shortcuts.

Keyboard Shortcuts Table 33 lists the keyboard shortcuts that are available when you use the CLI.

Table 33. Keyboard Shortcuts

| CLI Action | Keyboard Shortcut |
|---|---------------------------|
| Move cursor to the beginning of the current line | Ctrl-a Home |
| Move cursor to the end of the current line | Ctrl-e End |
| Move cursor back on the current line, one character at a time | Ctrl-b Left Arrow key |
| Move the cursor forward on the current line, one character at a time | Ctrl-f Right Arrow Key |
| Start over at a blank command prompt (abandons the input on the current line) | Ctrl-c |
| Remove one character on the current line. | Ctrl-h |
| Remove the last word in the current command. (Clears one word at a time from the current command line, always starting with the last word on the line.) | Ctrl-W |
| Remove characters starting from cursor location to end of the current line. (Clears the current line from the cursor forward.) | Ctrl-k |
| Remove all characters before the cursor. (Clears the current line from the cursor back to the CLI prompt.) | Ctrl-U |
| Clear screen but keep current CLI prompt and input in place. | Ctrl-l |
| Display previous command in history. (Ctrl-p and Ctrl-n let you cycle through a history of all executed commands like Up and Down arrow keys typically do. Up/Down arrow keys also work for this.) | Ctrl-p Up Arrow key |

Table 33. Keyboard Shortcuts (Continued)

| CLI Action | Keyboard Shortcut |
|---|--------------------------|
| Display next command in history. (Ctrl-p and Ctrl-n let you cycle through a history of all executed commands like Up and Down arrow keys typically do. Up/Down arrow keys also work for this.) | Ctrl-n Down Arrow key |
| Exit the CLI. (At a blank command prompt, typing Ctrl-d closes the CLI.) (Typing Ctrl-d within command text also removes characters, one at a time, at cursor location like Ctrl-h.) | Ctrl-d |

Tab Completion and Help

You can get help on commands in the command line interface (CLI) by using the TAB key. (See also “Basic Settings” on page 282.)

Hitting TAB once will attempt to complete the current command.

If multiple completions exist, a beep will sound and no results will be displayed. Enter TAB again to display all available completions.

- **Example 1:** At a blank command line, press TAB twice to get a list of all commands.

```
AT-WA7400#
add          Add an instance to the running
             configuration
factory-reset Reset the system to factory defaults
get          Get field values of the running
             configuration
reboot       Reboot the system
remove       Remove instances in the running
             configuration
save-running Save the running configuration
set          Set field values of the running
             configuration
```

- **Example 2:** Type `get` TAB TAB (including a space after `get`) to see a list of all field options for the `get` command.

```
AT-WA7400# get
association  Associated station
basic-rate   Basic rates of radios
```

| | |
|----------------|---|
| bridge-port | Bridge ports of bridge interfaces |
| bss | Basic Service Set of radios |
| cluster | Clustering-based configuration settings |
| cluster-member | Member of a cluster of like-configured accesspoints |
| config | Configuration settings |
| detected-ap | Detected access point |
| dhcp-client | DHCP client settings |
| dot11 | IEEE 802.11 (all radios) |
| host | Internet host settings |
| interface | Network interface |
| ip-route | IP route entry |
| klog-entry | Kernel log entry |
| log | Log settings |
| log-entry | Log entry |
| mac-acl | MAC address access list item |
| ntp | Network Time Protocol client |
| portal | Guest captive portal |
| radio | Radio |
| radius-user | RADIUS user |
| ssh | SSH access to the command line interface |
| supported-rate | Supported rates of radios |
| system | System settings |
| telnet | Telnet access to the command line interface |
| tx-queue | Transmission queue parameters |
| wme-queue | Transmission queue parameters for stations |

- **Example 3:** Type `get system v` TAB. This will result in completion with the only matching field, `get system version`. (Press ENTER to get the output results of the command.)

```
AT-WA7400# get system v
```

```
AT-WA7400# get system version
```

- **Example 4:** Type `set TAB TAB` (including a space after `set`) to get a list of all field options for the `set` command.

```
AT-WA7400# set
```

```
bss                Basic Service Set of radios
cluster            Clustering-based configuration settings
cluster-member    Member of a cluster of like-configured
                  access points
config            Configuration settings
dhcp-client       DHCP client settings
dot11             IEEE 802.11 (all radios)
host              Internet host settings
interface         Network interface
ip-route          IP route entry
log               Log settings
mac-acl           MAC address access list item
ntp               Network Time Protocol client
portal            Guest captive portal
radio             Radio
radius-user       RADIUS user
ssh               SSH access to the command line interface
system            System settings
telnet            Telnet access to the command line
                  interface
tx-queue          Transmission queue parameters
wme-queue         Transmission queue parameters for
                  stations
```

- **Example 5:** Type `set mac TAB`, and the command will complete with the only matching option:

```
AT-WA7400# set mac-acl
```

- **Example 6:** Type `set cluster TAB TAB`, and the two matching options are displayed:


```
AT-WA7400# set cluster
```

```
cluster          Clustering-based configuration settings
cluster-member  Member of a cluster of like-configured
access points
```

- **Example 7:** Type **add** TAB TAB (including a space after **add**) to get a list of all field options for the **add** command.

```
AT-WA7400# add
```

```
basic-rate      Basic rates of radios
bridge-port     Bridge ports of bridge interfaces
bss            Basic Service Set of radios
interface       Network interface
mac-acl        MAC address access list item
radius-user     RADIUS user
supported-rate  Supported rates of radios
```

- **Example 8:** Type **remove** TAB TAB (including a space after **remove**) to get a list of all field options for the **remove** command

```
AT-WA7400# remove
```

```
basic-rate      Basic rates of radios
bridge-port     Bridge ports of bridge interfaces
bss            Basic Service Set of radios
interface       Network interface
ip-route        IP route entry
mac-acl        MAC address access list item
radius-user     RADIUS user
supported-rate  Supported rates of radios
```

CLI Classes and Fields Reference

The following is an introduction to the CLI classes and fields.

Configuration information for the AT-WA7400 Wireless Access Point is represented as a set of classes and objects.

Different kinds of information uses different classes. For example, information about a network interface is represented by the interface class, while information about an NTP client is represented by the ntp class.

Depending on the type of class, there can be multiple instances of a class. For example, there is one instance of the interface class for each network interface the access point has (Ethernet, radio, and so on), while there is just a singleton instance of the ntp class, since an access point needs only a single NTP client. Some classes require their instances to have names to differentiate between them; these are called *named classes*. For example, one interface might have a name of eth0 to indicate that it is an Ethernet interface, while another interface could have a name of wlan0 to indicate it is a wireless LAN (WLAN) interface. Instances of singleton classes do not have names, since they only have a single instance. Classes that can have multiple instances but do not have a name are called anonymous classes. Together, singleton and anonymous classes are called unnamed classes. Some classes require their instances to have names, but the multiple instances can have the same name to indicate that they are part of the same group. These are called group classes.

| has name? \ # of instances? | one | multiple |
|-----------------------------|-----------|--------------|
| no | singleton | anonymous |
| yes - unique | n/a | unique named |
| yes - non-unique | n/a | group named |

Each class defines a set of fields that describe the actual information associated with a class. Each instance of a class will have a value for each field that contains the information. For example, the interface class has fields such as “ip” and “mask.” For one instance, the ip field might have a value of 192.168.1.1 while the mask field has a value of 255.255.0.0; another instance might have an ip field with a value of 10.0.0.1 and mask

field with a value of 255.0.0.0.

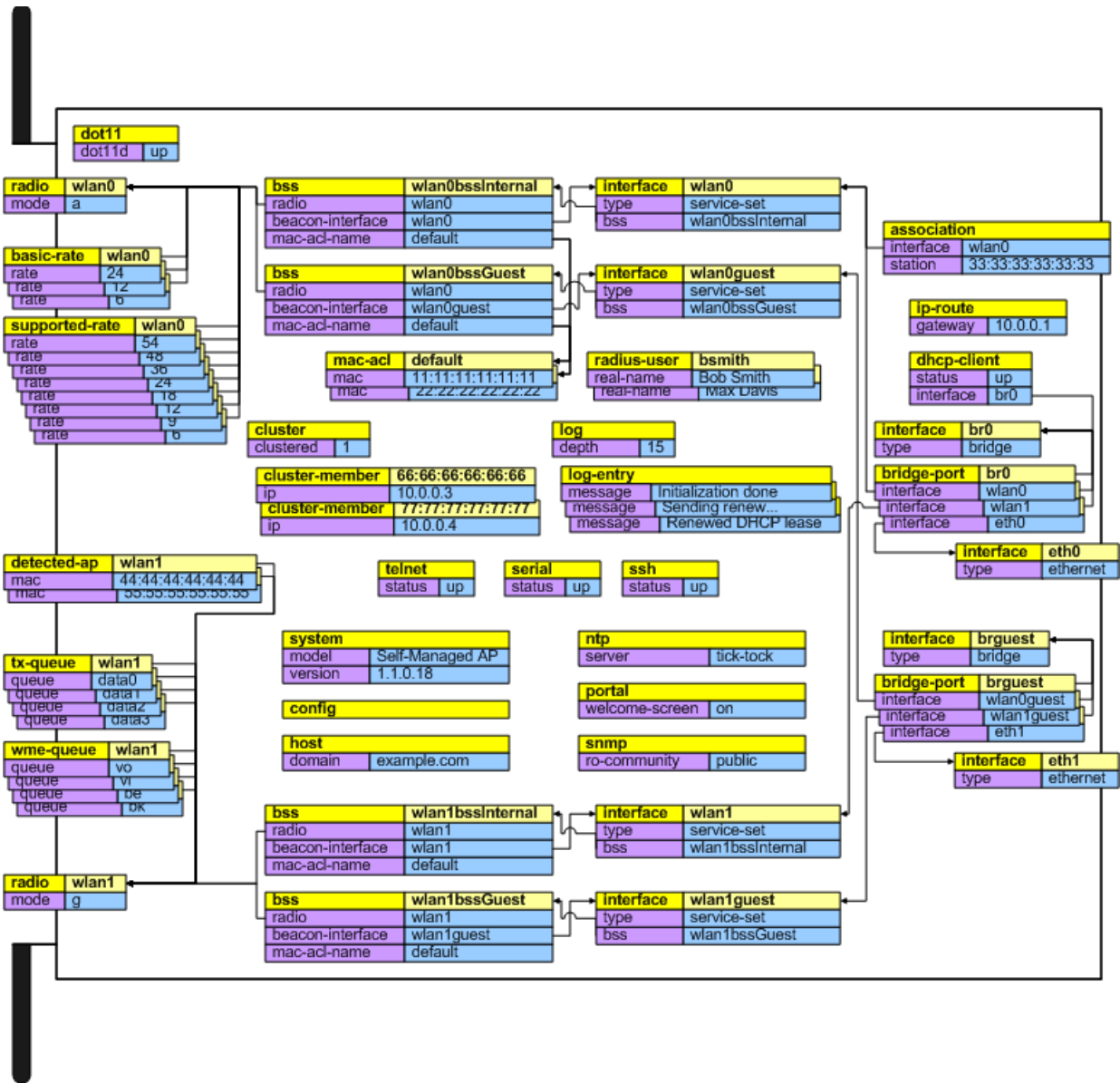


Figure 41. CLI Class Relationships

Appendix E

Radio Bands

Allied Telesyn's AT-WA7400 Wireless Access Point is capable of operating in the 2.4GHZ (IEEE 802.11g/b) AND in the 5GHZ band (IEEE 802.11a) simultaneously. The access point is shipped with the 802.11g/b radio enabled and is software upgradeable to operate in 802.11g/b and 802.11a. For further information about this upgrade, please contact your Allied Telesyn sales representative.

Some of the advantages of the 802.11a option are:

- ❑ Higher performance. 802.11a can deliver data rates up to 54Mbps and there is enough room in the 5GHz spectrum to support up to 12 access points operating in the same area without causing interference between access points. This equates to 432Mbps (12 X 54Mbps) total data rate performance. With 802.11g, you have three non-overlapping channels for setting access point frequencies, which can limit capacity.
- ❑ Less RF interference: The growing use of 2.4GHz cordless phones and Bluetooth devices is crowding the radio spectrum within many facilities. This significantly decreases the performance of 802.11g wireless LANs. The use of 802.11a operating in the relatively uncrowded 5GHz band avoids this interference.
- ❑ Ability to use the Wireless Distribution System (WDS) feature, using the 802.11a radio for bridging to another access point while servicing 802.11g customers without using user bandwidth for the bridging function.

Index

A

- access point
 - adding to cluster 50
 - clustering 44
 - factory default configuration 281
 - navigating to 52
 - removing from cluster 49
 - running configuration 281
 - startup configuration 281
- Access Points page 48
- administrator name, default setting 215
- administrator password
 - changing 38
 - configuring 199
 - default setting 215
- administrator's PC, setting up 20
- AP EDCA parameters, configuring 168
- associated wireless clients, displaying 192
- AT-WA7400 Wireless Access Point
 - rebooting 205
 - resetting to factory defaults 206
- authentication server
 - for IEEE 802.1x security mode 121
 - for WPA/WPA2 Enterprise (RADIUS) security mode 125
- authentication, in different security modes 107
- auto-synch of cluster configuration 47

B

- back up, user accounts database 62
- backup links, WDS 175
- basic settings, configuring 37
- basic setup, testing 41
- beacon interval, configuring 147
- bridges, WDS 174
- broadcast SSID
 - configuring 114
 - default setting 216
- built-in authentication server, described 219

C

- captive portal, configuring 136
- certificate
 - obtaining TLS-EAP certificate for client 253
 - security for IEEE 802.1x client 231
 - security for WPA/WPA2 Enterprise (RADIUS) client 241
- channel
 - automated management of clustered APs 72

- configuring 147
- channel assignment
 - starting or stopping 73
 - updating 74
 - viewing 73
- channel management
 - advanced settings 75
 - configuring 73
 - described 70
 - displaying 72
 - example 71
 - starting or stopping 73
 - updating assignments 74
- channel management of clustered APs
 - advanced settings 75
 - example 71
 - proposed channel assignments 74
 - understanding 70
 - viewing/setting locks 73
- channel plan, viewing last 74
- CLI
 - basic settings commands 282
 - class and field reference 354
 - cluster commands 285
 - commands and syntax quick view 272
 - comparison with Web UI 266
 - configuring time protocol 347
 - configuring WDS 345
 - getting help on 275
 - guest login configuration 323
 - how to access 269
 - how to save configuration changes 281
 - interface names used in 278
 - keyboard shortcuts 349
 - load balancing commands 335
 - MAC filtering configuration 333
 - multi-BSSIDs configuration 325
 - quality of service configuration 336
 - rebooting AP from 347
 - resetting AP from 348
 - security commands 304
 - status and monitoring commands 289
 - user accounts commands 287
 - virtual wireless networks configuration 325
 - wired interface commands 301
 - wireless interface commands 304
- client
 - link integrity monitoring 192
 - platform 22

- session, definition 65
 - See also *stations*
- client workstations, setting up 22
- cluster
 - adding access point 50
 - adding an access point to 50
 - auto-synch 47
 - configuration changes 47
 - configuration settings 45
 - definition 44
 - description 44
 - formation 47
 - mode 46
 - recovering 261
 - recovery 261
 - removing access point 49
 - removing an access point from 49
 - security 47
 - size 44, 47
 - size and membership 47
 - troubleshooting 261
 - types of access points supported 44
 - understanding 44
 - viewing 48
- cluster member, viewing 84
- cluster mode, described 46
- cluster neighbors 80
- cluster recovery 261
- commands
 - add 272
 - factory-reset 348
 - get 272
 - reboot 348
 - remove 272
 - save-running 281
 - set 272
- configuration file
 - backing up 212
 - factory default 281
 - restoring 213
 - running configuration 281
 - startup configuration 281
- connecting to AP
 - SSH 270
- country codes 98
- D**
- DCF, as related to QoS 164
- default settings
 - list 215
 - resetting to 206
- DNS name, setting 88
- DTIM period, configuring 147
- Dynamic Host Control Protocol (DHCP)
 - understanding in relation to self-managed APs 23
- E**
- EAP-PEAP
 - configuring on IEEE 802.1x client 227
 - configuring on WPA/WPA2 Enterprise (RADIUS) client 236
- EDCA parameters, configuring 171
- encryption in different security modes 107
- Ethernet (wired) settings 87
- event log, configuring 186
- events, monitoring 186
- extended service set, with WDS bridging 174
- external RADIUS server, configuring 248
- F**
- factory defaults 40
 - reverting to from CLI 281
 - reverting to from Web UI 206
- firmware, upgrading 207, 209
- fragmentation threshold, configuring 147
- frequency, radio 148
- G**
- guest access, enabling or disabling 90
- guest interface
 - configuring 135
 - described 134
 - explanation 134
 - VLANs 135
- guest network
 - accessing 137
 - wireless settings, configuring 103
- H**
- HTTP timeout 204
- I**
- IAPP map table 129
- IEEE 802.11a Turbo, configuring 147
- IEEE 802.11a, configuring 147
- IEEE 802.11b, configuring 147
- IEEE 802.11d regulatory domain, configuring 98
- IEEE 802.11g, configuring 147
- IEEE 802.1x radio mode, configuring 147
- IEEE 802.1x security for a client 227
- IEEE 802.1x security mode 108
 - client configuration 227
 - configuring 121
- IEEE rate set, configuring 147
- interframe spaces, as related to QoS 164
- internal and guest networks on virtual LANs, configuring 135
- internal LAN, configuring 93
- internal wireless LAN settings 102
- IP address, default setting 215
- IP addresses
 - configuring 37
 - dynamic 23
 - navigating to 52
 - recovering 24
 - static 23
 - viewing for access points 81

K

key management, security 107
 KickStart 26
 KickStart utility, running to find access points 26

L

link integrity monitoring 192
 load balancing
 configuring 157
 default setting 216
 described 156
 location description 49
 log relay host
 configuring 187
 enabling or disabling 188
 logon, administration Web pages 34
 logout 36
 loops, WDS 175

M

MAC address filtering
 configuring 53
 default setting 216
 MAC address, configuring 37
 master access point, described 44

N

neighboring access point, displaying status 193
 network name, configuring 38
 network time protocol (NTP) server, enabling or disabling 202
 Network Time Protocol (NTP), default setting 215

P

packet bursting, as related to QoS 166
 password, configuring 37
 PEAP
 configuring on IEEE 802.1x client 227
 configuring on WPA/WPA2 Enterprise (RADIUS) client 236
 plain text security mode
 client configuration 223
 compared 107
 configuring 115
 for wireless client 223
 progress bar for cluster auto-synch 47

Q

QoS (Quality of Service)
 configuring 167
 described 162
 queues, configuring for QoS 167

R

radar detection 101
 radio
 bands 357
 beacon interval 147

 configuring 147
 configuring one or two radio AP 147
 DTIM period 147
 fragmentation threshold 147
 IEEE 802.11 mode 147
 maximum stations 147
 rate sets 147
 RTS threshold 147
 SuperAG 147
 transmit power 147
 turning on or off 147
 radio frequencies 148
 radio interface, configuring 100
 radio settings
 configuring 147
 described 146
 RADIUS server
 configuring to acknowledge access points 248
 described 219
 See also authentication server
 rate sets 152
 regulatory domain 98
 reset access point to factory defaults 206
 RTS threshold, configuring 147
 running configuration 281

S

security
 authentication server 248
 certificates on client 253
 comparison of modes 107
 configuring on the access point 114
 default setting 216
 IEEE 802.1x 121
 plain text 115
 pros and cons of different modes 106
 static WEP 116
 WEP 116
 WPA/WPA2 Enterprise (RADIUS) 125
 WPA/WPA2 Personal (PSK) 123
 security modes
 configuring 114
 described 107
 session
 definition 65
 described 65
 monitoring 66
 specific information, viewing 67
 session information
 sorting 68
 SNMP firmware upgrade 209
 SNMP, configuring 131
 software defaults 215
 spanning tree, enabling or disabling 92
 SSH connection to AP 270
 standalone mode, described 46
 startup configuration 281
 static WEP security mode 107
 configuring 116

- on WDS bridge 175
 - station isolation
 - configuring 114
 - described 113
 - stations
 - configuring maximum allowed 147
 - See *also* client
 - Stop Clustering page 262
 - subnet mask, default setting 215
 - supported platforms
 - administrator 20
 - client 22
 - synchronization of cluster 47
 - system name, default setting 215
- T**
- Telnet connection to AP 269
 - TLS-EAP
 - configuring on IEEE 802.1x client 231
 - configuring on WPA/WPA2 Enterprise (RADIUS) client 241
 - obtaining certificate for client 253
 - TLS-EAP certificate for a client 253
 - ToS, as related to QoS 163
 - transmit power, configuring 147
 - transmit/receive statistics, displaying 190
 - troubleshooting 259
- U**
- user
 - adding 58
 - editing 60
 - user account
 - backing up and restoring 62
 - disabling 61
 - enabling 60
 - removing 61
 - user authentication
 - configuring on IEEE 802.1x client 227
 - configuring on WPA/WPA2 Enterprise (RADIUS) client 236
 - user database
 - backing up 62
 - restoring 63
 - user management, described 57
 - users, managing 57
- V**
- virtual wireless networks, enabling or disabling 90
 - VLANs
 - configuring 140
 - for internal and guest interface 135
- W**
- wait time for cluster auto-synch 47
 - WDS
 - configuring 178
 - default setting 216
 - example 181
 - explanation 174
 - Welcome screen, configuring 136
 - WEP security mode
 - client configuration 224
 - configuring 116
 - when to use 107
 - Wi-Fi MultiMedia, enabling or disabling 170
 - Wired Equivalent Privacy security mode for client 224
 - wired LAN settings, monitoring 184
 - wireless client settings 221
 - wireless distribution system (WDS)
 - configuration guidelines 260
 - configuring 178
 - described 174
 - guidelines 176
 - troubleshooting 260
 - wireless LAN settings, monitoring 184
 - wireless neighborhood
 - described 80
 - displaying 81
 - wireless network, security 106
 - WPA/WPA2 Enterprise (RADIUS) security mode 111
 - client configuration 236
 - configuring 125
 - WPA/WPA2 Enterprise client using EAP-TLS certificate 241
 - WPA/WPA2 Personal (PSK) Security client 245
 - WPA/WPA2 Personal (PSK) security mode
 - client configuration 245
 - configuring 123
 - when to use 110
 - WPA2 Enterprise security mode, configuring 125