User's Guide

Access/One® Network

Including Manager/One®

Indoor and Outdoor Wireless System

February 8th, 2007

210-0007-02 Rev. E

Strix Systems
Networks Without Wires®

Access/One® Network

Including Manager/One®

Part Number: 210-0007-02

Revision E

26610 Agoura Road
Calabasas, CA 91302
USA

www.strixsystems.com

Strix SYSTEMS
Networks Without Wires®

Copyright Notice

FCC Notice

Strix wireless network devices comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. The device may not cause harmful interference.
2. The device must accept any interference received, including interference that may cause undesired operation.

Strix wireless network devices have been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. Strix wireless network devices generate, use, and radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the wireless network device does cause harmful interference to radio or television reception, which can be determined by turning the wireless network device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the wireless network device and the affected receiver.
- Connect the wireless network device into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Other Notices

Industry Canada Notice

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

VCCI Notice

The Strix IWS and OWS products are Class B wireless network devices based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If the wireless network device is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the wireless network device according to the instruction manual.

European Community (EC) Directives and Conformity

Strix wireless network devices are in conformity with the Essential Requirements of R&TTE Directive 1999/5/EC of the European Union.

Non-Modification Statement

Unauthorized changes or modifications to Strix devices are not permitted. Modifications to Strix devices will void the warranty and may violate FCC regulations.

RF Exposure Requirements

To ensure compliance with FCC RF exposure requirements, the antenna used for Strix wireless network devices must be installed to provide a separation distance of a minimum of 2 meters (6.56 feet) or more from all persons, and must not be co-located or operated in conjunction with any other antenna or radio transmitter. Installers must follow these installation instructions.

Safety Warnings (OWS only)

The OWS (Outdoor Wireless System) product must be installed by a trained professional installer only. Read all safety warning before commencing an OWS installation.

General Safety Warning

ALWAYS BE AWARE OF ELECTRICAL POWER LINES!

You can be killed if any antennas come near electrical power lines. Carefully read and follow all instructions in this manual.

By performing these installation instructions, you may be exposed to hazardous environments and high voltage. Use caution when installing the Strix OWS product.

Electrical Power Warning

The OWS product must be installed by a trained professional installer only. Read the installation instructions before you connect the wireless network device to its power source.

Lightning Activity Warning

Do not connect or disconnect cables during periods of lightning activity.

For each antenna, a surge protective device meeting IEC 61000-4-5, Level 4 or IEEE C 62.41 A3/B3 requirements must be used to prevent potential damage from very high surges (for example, surges caused by lightning).

Explosive Device Proximity Warning

Do not operate your wireless network device near unshielded blasting caps or in an explosive environment.

Antenna Placement Warning

Do not locate any antenna near overhead power lines or other electric light or power circuits, or where the antenna can come into contact with such circuits. When installing antennas, take extreme care not to come into contact with such electrical circuits, as they can cause serious injury or death.

For the correct installation and grounding of antennas, please refer to national and local codes (for example, US:NFPA 70, National Electrical Code, Article 810; in Canada: Canadian Electrical Code, Section 54).

Ground Warning

You must ALWAYS install an external grounding wire on the OWS product. The ground connection must be complete before connecting power to the OWS enclosure—a simple continuity check between the enclosure and the ground termination point can confirm this. Grounding of the OWS must comply with National Electrical Code (NEC) requirements, unless local codes in your area take precedence over the NEC code.

Power Cord Assembly Caution

An assembled power cord is not supplied with the OWS. The power cord must be assembled by a professional installer, and the final assembly must comply with National Electrical Code (NEC) requirements, unless local codes in your area take precedence over the NEC code.

Battery Caution

The OWS product contains a non-rechargeable, non-user-serviceable lithium ion battery. Exercise caution to avoid shorting the terminals of this device.

Consult local laws and regulations for the proper disposal of batteries in your area.

Access/One® Indoor and Outdoor Wireless System Limited Warranty

Limited Warranty: Strix Systems, Inc. ("Strix") warrants the Access/One Indoor Wireless System ("IWS") and Outdoor Wireless System ("OWS"): (i) the hardware ("Hardware") will be free of defects in materials and workmanship from the date of shipment as set forth below and (ii) the embedded software ("Firmware") to the Hardware and any separately provided software product ("Software") are provided "AS-IS" and such items will substantially conform to their respective published product documentation (collectively the "Product") for the periods indicated below, commencing (as applicable) on the date of shipment.

Covered Product	Warranty Period
IWS products (Including but not limited to the BMEx, WM11x, NWSV-x, Antennas, AMECs, MTKIT, PSWW, SLCDT and SLCKIT)	12 months
OWS2400/OWS3600	12 months
OWS11xx (Radio Board)/OWS-NSxx (Network Servers)	12 months
Repaired or Replacement Items	90 days, or the balance of the original item warranty, whichever is the greater

This limited warranty extends only to the original user of the Product and such user's sole and exclusive remedy and the entire liability of Strix, at its option, will be to repair or replace the Hardware or component thereof and in the case of Firmware or Software Strix will make available the then available updated version of the Firmware or Software. Notwithstanding the foregoing, in no event does Strix warrant that the Product will operate with any software or hardware other than that provided by Strix or specified in the applicable Product documentation, that the Product is error free or will operate without problems or interruptions, or that the, Product will be free of vulnerability to intrusion or attack, or that the Product will satisfy any party's own specific requirements.

The repair or replacement of the Product does not include any labor or other costs related to the subsequent installation thereof. The obligations of Strix hereunder are conditioned upon the return of the Hardware in accordance with the Strix then-current Return Material Authorization (RMA) procedures (please contact your authorized Strix Systems reseller for return instructions). Repair or replacement of the defective Product or parts thereof shall neither extend nor decrease the warranty period.

Exceptions: The foregoing limited warranties of the Product do not apply if the Product (i) has been altered or modified, except by Strix or its duly trained and authorized service provider, (ii) has not been installed, operated, repaired, or maintained in accordance with written instructions of Strix, (iii) has been subjected to abnormal physical or electrical stress, misuse, negligence or accident, (iv) has been operated outside of the environmental specifications for the Product or (v) is related to configuration of customer's network beyond that necessary to the use or installation of the Strix Products. The Strix limited Firmware or Software warranty does not apply to Firmware or Software corrections or upgrades. Repair of Products or the supply of updated Firmware or Software requested after the expiration of the warranty period shall be at then current Strix repair or update charges.

DISCLAIMER; LIMITATION OF LIABILITY: EXCEPT FOR THE WARRANTIES SPECIFICALLY DESCRIBED HEREIN, STRIX DISCLAIMS ANY AND ALL WARRANTIES AND GUARANTEES, EXPRESS, IMPLIED OR OTHERWISE, ARISING, WITH RESPECT TO THE PRODUCTS OR SERVICES DELIVERED HEREUNDER, INCLUDING BUT NOT LIMITED TO THE WARRANTY OF MERCHANTABILITY, THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF NON-INFRINGEMENT OF THE INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY. LIABILITY OF STRIX FOR LOSS UNDER THIS CONTRACT IS LIMITED TO THE TOTAL AMOUNT PAID TO STRIX BY CUSTOMER DURING THE PREVIOUS CALENDAR YEAR. STRIX WILL HAVE NO OBLIGATION OR LIABILITY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) OR OTHERWISE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES INCLUDING BUT NOT LIMITED TO LOSS OF USE, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF REVENUE, LOSS OF BUSINESS OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH ANY OF THE PRODUCTS OR OTHER GOODS OR SERVICES FURNISHED BY STRIX UNDER THIS AGREEMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Software License Agreement

PLEASE READ THIS SOFTWARE LICENSE CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING THE STRIX SYSTEMS MANAGER/ONE® UTILITY SOFTWARE.

BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM STRIX OR AN AUTHORIZED STRIX RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL PURCHASER. “You” and “Customer” refer to the party lawfully in possession of the Software and entitled to use in accordance with terms and conditions set forth herein. “Strix” means Strix Systems, Inc.

The following terms govern your use of the Software except to the extent a particular program (a) is the subject of a separate written agreement with Strix or (b) includes a separate “click-on” license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, and (3) this Software License.

GRANT OF LICENSE. Subject to the terms and conditions of this License Agreement, Strix grants to you the limited, non-exclusive, non-transferable right to use the Software in object code from only and solely for use on Strix products which you have purchased. A license key may be required to enable the Software for use. A license key may be obtained by contacting Strix or its authorized Reseller.

OWNERSHIP. The Software is owned by Strix and/or its licensors and is protected by United States and foreign copyright laws and international treaty. You acquire only the right to use the Software in accordance with the terms of this Agreement and do not acquire any rights of ownership. You agree not to remove any product identification, trademark, copyright or other proprietary notices, legends or restrictions appearing in or upon any of the Software or any media containing the Software.

UPGRADES AND ADDITIONAL COPIES. For purposes of this Agreement, "Software" shall include (and the terms and conditions of this Agreement shall apply to) any upgrades, updates, bug fixes or modified versions (collectively, "Upgrades") or backup copies of the Software licensed or provided to Customer by Strix or an authorized distributor for which Customer has paid the applicable license fees.

NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY SUCH ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE; (2) USE OF UPGRADES IS LIMITED TO THE STRIX PRODUCT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) USE OF ADDITIONAL COPIES IS LIMITED TO BACKUP PURPOSES ONLY.

CONFIDENTIALITY. You agree that you will not duplicate, copy or otherwise reproduce the Software or any portion thereof, nor distribute, disseminate or otherwise disclose the Software in any form, in whole or in part, to any third party, nor use any knowledge derived from the use of the Software for any commercial purpose whatsoever, without the prior, express written consent of an officer of Strix. Further, you acknowledge that the Software is the confidential, proprietary and trade secret property of Strix and/or its licensors and agree to take all reasonable steps to protect the confidentiality of the Software and to prevent its unauthorized use or disclosure.

OTHER RESTRICTIONS. You may not rent, lease, transfer, modify, adapt, translate, reverse engineer, decompile, disassemble, or create derivative works based on the Software or any written materials distributed in connection with the Software, without the prior written consent of Strix (except as permitted by applicable law, but only to the extent that Strix is not permitted by such applicable law to exclude or limit such rights). Information relating to such Software that is necessary to enable the production of other software that is interoperable or compatible with the Software may be available from Strix upon written request.

CUSTOMER RECORDS. Customer grants to Strix and its independent accountants the right to examine Customer's books, records, and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Strix the appropriate licensee fees.

EXPORT. Software, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software.

LIMITATION AND EXCLUSIONS. THE SOFTWARE PROVIDED HEREUNDER IS PROVIDES ON AN "AS IS" AND "WITH ALL FAULTS" BASIS. STRIX AND ITS SUPPLIERS OR LICENSORS EXPRESSLY DISCLAIM ALL WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. WITHOUT IN ANY WAY LIMITING THE GENERALITY OF THE FOREGOING, NEITHER STRIX NOR ITS SUPPLIERS OR LICENSORS MAKE ANY WARRANTY OR REPRESENTATION THAT THE SOFTWARE OR USER DOCUMENTATION IS ERROR FREE OR THAT THE SOFTWARE WILL OPERATE WITHOUT INTERRUPTION OR SATISFY YOUR NEEDS OR REQUIREMENTS.

GOVERNMENT RESTRICTED RIGHTS. If this Software and accompanying documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in the Software shall be only as set forth in this license; this is in accordance with 48 C.F.R. 227.7201 through 227.7202-4 (for Department of Defense (DoD) acquisitions) and with 48 C.F.R. 2.101 and 12.212 (for non-DoD acquisitions).

TERMINATION. This License is effective until terminated. You may terminate it at any time by destroying the Software together with all copies and documentation in any form. Your rights under this License will terminate automatically without notice from Strix if You fail to comply with any material term or condition of this License. Upon termination, You must either return or destroy the written materials and all copies of the Software.

GENERAL. Governing Law: This Agreement is governed by the laws of the State of California, USA without regard to its choice of law provisions. Both parties expressly agree that the provisions of the United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transaction Act shall not apply to this Agreement (including any attachments) or any part hereof. Export: In the event that you export or re-export the Software, you shall have full responsibility for obtaining all necessary approvals, licenses, permits and the like which may be required by any regulatory or governmental body. You agree to abide by the rules and regulations of the U.S. Department of Commerce, Office of Export Administration and U.S. Anti-Boycott laws and regulations, as well as all applicable U.S. federal, state and municipal statutes, rules and regulations and all import and export regulations and of the Software's destination country, when exporting or re-exporting the Software. Severability: If any provision of this Agreement shall be held to be illegal or unenforceable for any reason, such provision shall, to the extent of such illegality or unenforceability, be severed, but without affect to the remainder of such or any other provision contained herein and shall remain in full force and effect. Entire Agreement: This Agreement constitutes the entire agreement between you and Strix concerning the subject hereof. Any terms and conditions appearing on your purchase order or in any other writing received from you which are different from or in addition to the terms and conditions contained herein are null and void and of no force or effect. This Agreement may only be modified by a writing signed by authorized representatives of both parties.

IN NO EVENT SHALL STRIX OR ITS SUPPLIERS OR LICENSORS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION ANY LOSS OF DATA OR LOSS OF USE OR LOSS OF REVENUES OR PROFITS (WHETHER OR NOT SO ADVISED OF THE POSSIBILITY THEREOF) ARISING OUT OF OR CONNECTED IN ANY WAY WITH THIS AGREEMENT OR THE SOFTWARE, DOCUMENTATION, SERVICES OR OTHER ITEMS PROVIDED HEREUNDER OR IN CONNECTION HEREWITH, REGARDLESS OF THE TYPE OF CLAIM OR FORM OF ACTION AND HOWSOEVER ARISING. IN NO EVENT SHALL THE MAXIMUM LIABILITY OF STRIX OR ANY OF ITS SUPPLIERS OR LICENSORS EXCEED THE LICENSE FEES ACTUALLY PAID BY YOU UNDER THIS AGREEMENT.

Table of Contents

The bulleted items before the main listing appear in the front matter (prior to the Table of Contents).

- Copyright Notice
- FCC Notice
- Other Notices
- Safety Warnings (OWS only)
- Access/One® Indoor and Outdoor Wireless System Limited Warranty
- Software License Agreement

List of Figures ix

Introduction 1

About this User's Guide 1

Organization 1

Notes, Cautions, and Warnings 3

Common Terms and Usage 3

Important Note About Rebooting 4

The Network Used in this Guide 4

Product Images 4

Chapter 1: Welcome to Access/One Network 5

Indoor and Outdoor Solutions 6

Why Choose Access/One Network? 8

Mesh Topology 9

An Intelligent Network 11

Self-Discovery (or Physical Inventory) 12

Self-Tuning and Self-Healing 12

Background Scanning 13

Detecting Rogue Devices 13
Network Servers 14
Master Network Server 15
Communicating Across Remote Subnets 16
Client Connect 16
Network Connect 17
Wireless Workgroups (IWS only) 17
Offering a Rich Technology Base 18
IWS and OWS Hardware 18
Manager/One 18
System and Security 19
Wireless 22
Hardware Specifications 22

Chapter 2: Getting Started 23
Host Network Requirements 23
DHCP Server 23
Non-DHCP Server Environment 25
FTP Server 25
Internet Browser 26
Screen Resolution 26
About Manager/One 27
Installing the Manager/One Plug-In 27
Launching the Manager/One Utility Pane 29
Your New Manager/One Utility Pane 29
Accessing Manager/One for the First Time 31
Starting a New Network 32
Enabling Windows 2000 Servers for NTP Requests 33

Chapter 3: Updating the Firmware 35
Prerequisite Steps 35
Updating Firmware Across the Network 37

Updating Firmware on Individual Modules 41

Chapter 4: The Manager/One Interface 43

The Manager/One Plug-In 43
The General Layout 44
A Choice of Layouts 45
Switching Between Layouts 46
Features of the Logical Mesh Topology View 47
The Segment View 48
Switching from Segment View List to Segment View Icons 49
Tools 50
Logical View Legend 52
Panning and Zooming 53
Node Status Registers 54
Management Tools and Features (Any Layout) 55
The Details Pane 56
Node Operational Status Indicators 57
The Toolbar 58
Tabbed Pages 58
Commands 60
Legends 61
Refresh 62
Factory Default 62
Exporting Your Inventory File to an Excel Spreadsheet 63
Inventory or Auto Discovered 63
Intuitive Mouse Over 64
Inputting Data 64

Chapter 5: Managing the Network 65

The Manage Function 65
View Action Status 66
Action Status Results 67

Commands 68
Load Firmware on Network 68
Reboot Network 68
Update Node Names 68
Update Network Membership 69
Transfer System Files 69
Remote Network Server 70
The Configure Function 71
System 71
User Login 72
Network Management 73
TCP/IP Settings 78
Network Topology 79
Priority/One - Class of Service 81
Radius Accounting 84
Syslog 85
Date and Time 88
Operating Environment 91
Firmware Updates 91
Wi-Fi 92
General 92
Radio Parameters 95
Client Connect 101
Network Connect 109
Rogue Scan 114
The Inventory Function 116
Print Friendly Format 117
Export to CSV 118
Importing the CSV File to an Excel Spreadsheet 118
The Monitor Function 119
Tools 119
AP Monitor 119

Network Connect Monitor 121
Wireless Client Query 122
Rogue Monitor 123
The Apply Configuration Function 124
Important Notes About Apply Configuration 124
Enabling Communication Between Remote Subnets 125
Example 125
Procedure 126
Removing the NS to NS Feature 126
Managing Remote Subnets from Manager/One 126

Chapter 6: Managing Subnets and Nodes 127
Interface Features in the Subnet View 128
The Manage Function 128
Commands (at the Subnet Level) 129
Load Firmware... 129
Reboot... 129
Commands (at the Node Level) 130
Update Node Names 130
Update Network Membership 131

Chapter 7: Managing Modules 133
Manger/One at the Module Level 133
The Manage Function 134
Actions 135
Factory Defaults 135
Load Firmware/Configuration 136
Page Device 137
Reboot 137
The Configure Function 138
System 138
User Login 139

Network Management 141
TCP/IP Settings 143
Priority/One - Class of Service 144
Radius Accounting 144
Syslog 144
Date and Time 145
Operating Environment 145
Firmware Updates 145
Wi-Fi 146
Radio Parameters 147
Client Connect 155
Network Connect 156
Rogue Scan 157
The Monitor Function 158
Reports 159
Radio Statistics 160
Wireless Neighbors 161
Wireless Client Monitor 162
SSIDs / VLANs List 163
Device Information 164
The Rogue Devices Function 165
Commands 165
Scan 165

Appendix A: Power Settings for Antennas 167
Channels for IEEE 802.11b/g 167
Channels for IEEE 802.11a 169
Channels for Public Safety (4.9 GHz) 170

Appendix B: Technical Support 171
Warranty 171
Priority Assignment 171

Partner Training 172
Partner Tools 172
Integration 172
Goal 172
Syslog Messages 173
Format 173
Subsystems 173
Severity Levels 174
Message Listing 174
Security Subsystem 174
Wireless Subsystem 175
Management Subsystem 179
Supported MIBs 181
Strix Private MIBs 181
Standard MIBs 182
Contact Information 182

Glossary of Terms 183

Index 199

List of Figures

Figure 1. Strix Mesh Architecture (OWS Metro Scenario) 5
Figure 2. Indoor Wireless System (IWS) 6
Figure 3. Outdoor Wireless System (OWS) 7
Figure 4. Strix Mesh Architecture (OWS Transportation Scenario) 10
Figure 5. Manager/One Interface (Network Level) 11
Figure 6. Self-Tuning and Self-Healing 12
Figure 7. Windows Task Manager 26
Figure 8. Manager/One Interface (Subnet Level) 27
Figure 9. Access/One Network Setup Wizard 28
Figure 10. Manager/One Icon 28
Figure 11. Manager/One Utility Pane 29
Figure 12. Expanded Utility Pane Tree 30
Figure 13. Manager/One Session Login Prompt 31
Figure 14. Defining Your Network Name 31
Figure 15. Network (Cloud) View 32
Figure 16. Run Dialog (Editing the Registry) 33
Figure 17. Registry Editor 33
Figure 18. Partner Login 36
Figure 19. Firmware Updates Command (Network Level) 37
Figure 20. Warning and Confirmation Request 38
Figure 21. Command Progress (Firmware) 38
Figure 22. View Action Status Window 39
Figure 23. Inventory Window 40
Figure 24. Firmware Updates Command (Module Level) 41
Figure 25. Action Configuration Window 42
Figure 26. Firmware Update Completed Successfully 42
Figure 27. Manager/One Icon 43
Figure 28. The Manager/One Interface (Default Flat View) 44
Figure 29. The Manager/One Interface (Logical View) 45
Figure 30. Switching Between Layouts 46

Figure 31. Logical Mesh Topology View 47
Figure 32. Segment View (List Format) 48
Figure 33. Segment View (Icon Format) 49
Figure 34. Accessing the Tools Pane 50
Figure 35. Show Names 51
Figure 36. Show Link Strengths 51
Figure 37. Logical View Legend 52
Figure 38. Panning and Zooming 53
Figure 39. Node Status Registers 54
Figure 40. Management Tools and Features 55
Figure 41. Details Pane 56
Figure 42. Operational Status of Nodes 57
Figure 43. Function Tabs 58
Figure 44. Commands 60
Figure 45. Legends 61
Figure 46. Refresh Button 62
Figure 47. Factory Default Button 62
Figure 48. Inventory or Auto Discovered 63
Figure 49. Intuitive Mouse-Over 64
Figure 50. Network (Cloud) View 65
Figure 51. View Action Status Window 66
Figure 52. Transferring System Files 69
Figure 53. Including Remote Servers 70
Figure 54. Excluding Remote Servers 70
Figure 55. Managing User Logins 72
Figure 56. General Management Interface Security 73
Figure 57. Configuring Access/One Network for SNMP 75
Figure 58. Managing Traps 76
Figure 59. Assigning Trusted IP Addresses 77
Figure 60. TCP/IP Settings 78
Figure 61. Network Topology 79
Figure 62. Priority/One 81

Figure 63. Adding COS Filters 82
Figure 64. Editing or Deleting COS Filters 83
Figure 65. Setting Up RADIUS Accounting Servers 84
Figure 66. Configuring Access/One Network for Syslog 86
Figure 67. Establishing the Correct Date and Time for Your Environment 88
Figure 68. Time Zones 88
Figure 69. Configuring Daylight Saving Time 89
Figure 70. Setting Manual Time 90
Figure 71. Setting the Cooling Fan Speed 91
Figure 72. Setting Up General Radio Parameters 92
Figure 73. 802.11a Radio Parameters (5.745 GHz to 5.825 GHz) 95
Figure 74. 802.11g Radio Parameters (2.400 GHz to 2.4835 GHz) 96
Figure 75. Public Safety Radio Parameters (4.940 GHz to 4.990 GHz) 97
Figure 76. Client Connect (Virtual/Strix) 101
Figure 77. Adding an SSID 102
Figure 78. Deleting an SSID 103
Figure 79. Configuring RADIUS Servers 105
Figure 80. WPA Pass Phrase 105
Figure 81. Assigning Client Connect Security Keys 105
Figure 82. Encrypted Security Key 106
Figure 83. Configuring an Access Control List 106
Figure 84. Adding a New Station 107
Figure 85. Network Connect 110
Figure 86. Network Connect Security Key 113
Figure 87. Rogue AP Scanning 114
Figure 88. Defining the Refresh Period for the Rogue List 115
Figure 89. Inventory List 116
Figure 90. Deleting a Node from the Inventory List 117
Figure 91. Printing the Inventory List 117
Figure 92. CSV File 118
Figure 93. AP Monitor (Default View) 119
Figure 94. An Overview of Monitor Tables (AP Monitor) 120

Figure 95. Network Connect Monitor 121
Figure 96. RSSI Legend 121
Figure 97. Wireless Client Query Monitor 122
Figure 98. MAC Address Prompt 122
Figure 99. Rogue Monitor 123
Figure 100. Apply Configuration 124
Figure 101. Subnet (Subcloud) View 127
Figure 102. Command Progress Pane 129
Figure 103. Node Name (Flat View) 130
Figure 104. Network Membership 131
Figure 105. Device Configuration Window 135
Figure 106. Loading a New Firmware Image or Configuration File 136
Figure 107. Paging a Device 137
Figure 108. Rebooting a Module 137
Figure 109. Module Identity and User Management (Login) Parameters 139
Figure 110. Client Connect Privacy Tags 141
Figure 111. Module Description and Name 142
Figure 112. TCP/IP Settings (Module Level) 143
Figure 113. Setting Up the FTP Server (Module Level) 145
Figure 114. Single and Dual Band Wi-Fi Menu Structure 146
Figure 115. 802.11a Radio Parameters (5.745 GHz to 5.825 GHz) 147
Figure 116. 802.11g Radio Parameters (2.400 GHz to 2.4835 GHz) 148
Figure 117. Public Safety Radio Parameters (4.940 GHz to 4.990 GHz) 149
Figure 118. Client Connect Configuration Window 155
Figure 119. Network Connect Configuration Window 156
Figure 120. Single and Dual Band Reports Menu Structure 159
Figure 121. Radio Statistics 160
Figure 122. Wireless Neighbors 161
Figure 123. Wireless Client Monitor 162
Figure 124. SSID / VLANs List 163
Figure 125. Device Information (802.11a Module) 164
Figure 126. Device Information (Network Server) 164

Figure 127. Rogue Monitor Table 165
Figure 128. BSSID Information for Rogue Device..... 166
Figure 129. Partner Login Page 171

Introduction

About this User's Guide

This User's Guide provides detailed information and procedures that will enable you to install, configure, manage, and use our Access/One Network product and its components successfully and efficiently. Use this guide to take full advantage of the system's functionality and features.

Organization

This User's Guide is organized as follows:

Chapter 1: Welcome to Access/One Network

Provides an overview of Access/One Network, its deployment and application options, and the benefits of our structured mesh topology. This chapter also provides a summary of the product's main features.

Chapter 2: Getting Started

Defines the prerequisites for deploying your Access/One Network, and provides instructions for installing the Manager/One interface. This chapter also shows you how to upgrade the Access/One Network firmware and how to enable Windows 2000 servers for NTP requests.

Chapter 3: Updating the Firmware

Shows you the correct method to use when updating the Access/One Network firmware, with some important notes and cautions that will ensure your network and its components are upgraded to the latest version without problems.

Chapter 4: The Manager/One Interface

Describes the Manager/One graphical management interface, with some useful examples to help with navigation.

Chapter 5: Managing the Network

Provides instructions for managing and configuring your Access/One Network at the network level following a successful installation.

Chapter 6: Managing Subnets and Nodes

Provides instructions for managing a subnet within your Access/One Network.

Chapter 7: Managing Modules

Provides instructions for managing individual modules within your Access/One Network (for example, wireless modules and network servers).

Appendix A: Power Settings for Antennas

Shows the maximum power settings based on the type of antenna being used and the wireless band.

Appendix B: Technical Support

Offers partner information, includes the most Frequently Asked Questions, and provides contact information for Strix Systems, Inc.

Glossary of Terms

Provides an explanation of terms directly related to Strix product technology, organized alphabetically.

Index

The index is a valuable information search tool. Use the index to locate specific topics and categories discussed in this User's Guide.

Notes, Cautions, and Warnings

Although installing and managing your Access/One Network is relatively simple, please exercise care and take the time to read all notes, cautions and warnings where the following symbols and text styles appear.

This symbol and ITALICIZED text are used for general notes and additional information that may be useful to you.

This symbol and italicized ORANGE text are used to indicate that care needs to be taken when performing a task. Cautions provide critical information. If in doubt, contact Technical Support for assistance.

This symbol and BOLD text are used to warn you about the risk of serious damage to the system or the potential for personal injury if the warning is ignored.

Common Terms and Usage

The following terms are frequently used throughout this User's Guide and within the Manager/One management interface:

Term	Usage
Cloud	Refers to the network as a whole.
Subcloud	This is a subnet residing within the network.
Node	A combination of Access/One Network modules residing at the same physical location.
Network Server	Serves intelligence, management and security to connected network nodes and modules.
Client Connect	Connects client devices to Access/One Network.
Network Connect	Associates to a Client Connect to complete a wireless node-to-node link.

Important Note About Rebooting

Your Access/One Network can be configured and managed at the network, subnet or individual module levels. As a consequence, the Manager/One management interface has different reboot commands for each level. These are:

- **Reboot Network**
  When logged in at the network level, this command is accessed from the Manage tab under Commands.
- **Reboot ... Subnet or Network**
  When logged in at the subnet level, this command (with options for subnet or network) is accessed from the Manage tab under Commands.
- **Reboot**
  When logged in to an individual module, this command is accessed from the Manage tab under Actions.

Before rebooting, always ensure that you are logged in at the correct management level within Manager/One.

The Network Used in this Guide

For simplicity, the sample Access/One Network used in this User's Guide is small, consisting of just 3 IWS nodes and 2 OWS nodes. The designated master network server is an IWS module attached to a router via a standard CAT5 Ethernet cable. All other nodes are connected to the network wirelessly.

Product Images

Some of the images used in this document have been modified for clarity.

Welcome to Access/One Network

1

Unlike traditional access points that offer limited coverage within predefined local hot spots, or inadequate single radio/single RF mesh solutions that won't scale, Access/One Network enables you to create small or large wireless networks for indoor and/or outdoor deployments—drawing on the parallels of the successful wired Enterprise network and providing all of the management and security that network managers demand.

Access/One Network provides multiple RF technologies built into a secure, fully scalable and self-tuning system, with the flexibility to easily add new and emerging wireless technologies, applications and services. And with the Strix structured mesh architecture, Access/One Network defines the standard for intelligent self-governing wireless systems that offer unparalleled user mobility in a reliable and secure managed network.

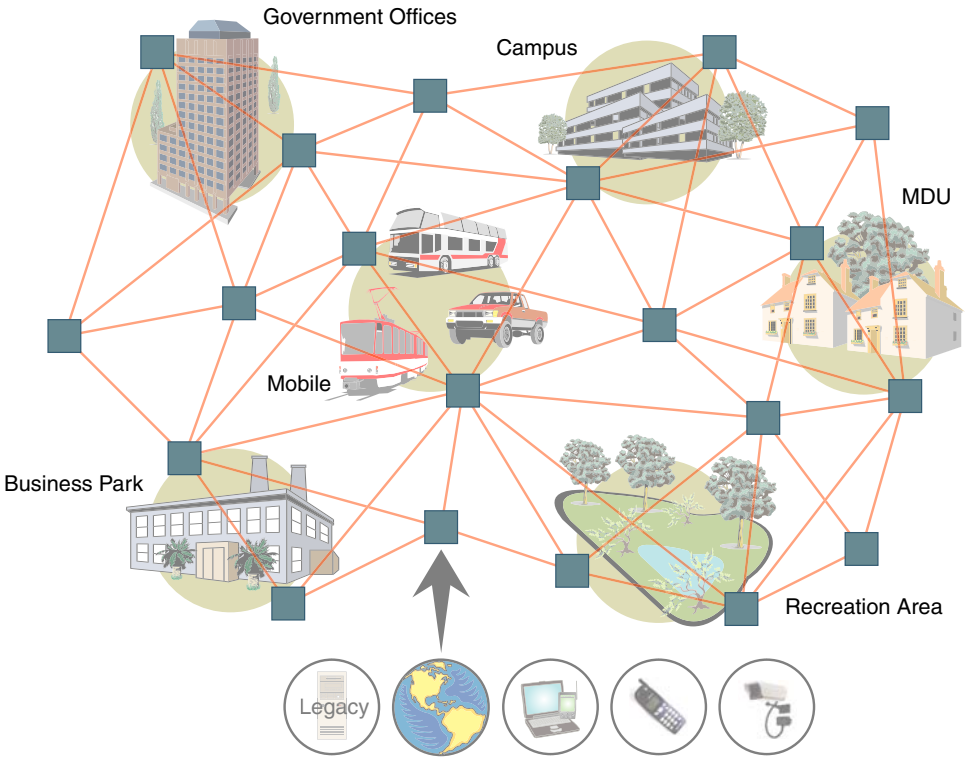

Figure 1. Strix Mesh Architecture (OWS Metro Scenario)

1

Indoor and Outdoor Solutions

Access/One Network has been designed for both indoor and outdoor wireless applications. Strix offers hardware solutions for both indoor and outdoor applications.

- **Indoor Wireless System (IWS)**

  Access/One Network IWS is designed for indoor deployments, with nodes being deployed using conventional Ethernet, or wirelessly via the Strix structured mesh architecture. State-of-the-art management and security features built into the IWS allow IT managers to deploy networks that can be secured using the latest authentication and encryption schemes, and managed entirely from a single point.

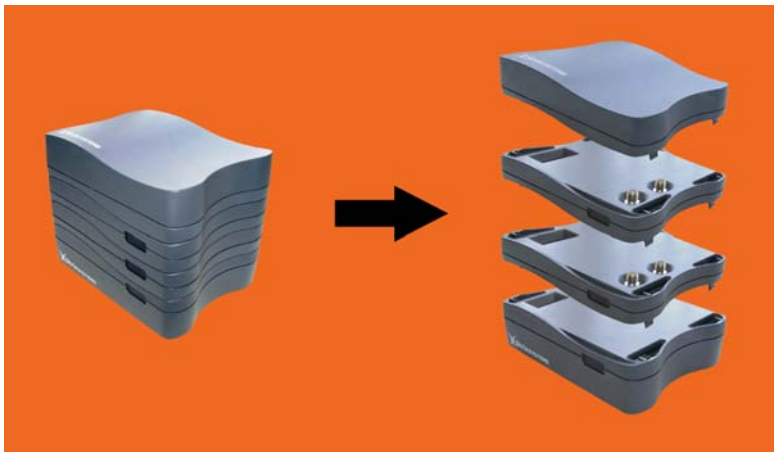

Figure 2. Indoor Wireless System (IWS)

The IWS is modular and flexible, with each network node capable of supporting up to three wireless modules of any type and mix. This flexibility provides the configuration options needed to meet the most demanding user connectivity requirements. Support for future wireless technologies, such as 802.16, Ultrawideband (802.15.3a), or 802.20, is as simple as adding the appropriate module to the network nodes wherever they are needed. With the IWS, 802.11a and 802.11g Client Connect modules can be configured to achieve speeds up to 108 Mbps, significantly improving the performance of your wireless network.

- **Outdoor Wireless System (OWS)**

  Access/One Network OWS is designed for outdoor deployments where network performance, reliability and scalability are a must. A single OWS node supports up to 6 radios, each of which can be dedicated to a unique function, such as mesh backbone ingress, egress, or client connectivity. High throughput and low latency across the Strix mesh backbone allows for the deployment of hundreds of nodes while utilizing only limited wired drops or termination points, making the OWS a highly scalable wireless networking solution for outdoor deployments.

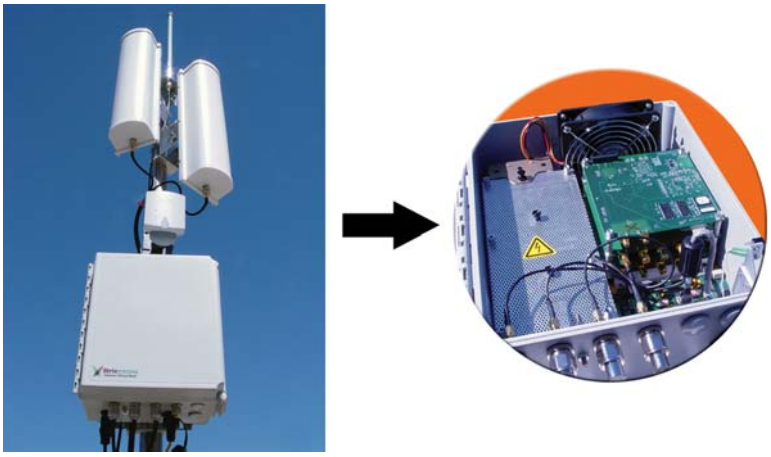

Figure 3. Outdoor Wireless System (OWS)

The OWS architecture makes 802.11 a full duplex technology, moving traffic more efficiently through the network and utilizing different RF frequencies and channels for network connectivity and client access. In addition, channels are selected dynamically, making the network more tolerant of interference than standard mesh networks. Working closely together, these features deliver higher throughput and lower latency across multiple hops, supporting real time voice, video, and data applications.

The OWS product is available in multiple configurations (2400 and 3600 series) that are fully upgradeable, driven by a 110/220 VAC auto-sensing power supply, with a DC power option and an optional heater for extreme environments.

1 Why Choose Access/One Network?

Access/One Network employs several categories of wireless modules which are individually assembled to form scalable network nodes. The specific role of each node within your network is determined by the mix of modules within the node itself. This approach ensures that our customers are given the flexibility to design wireless networks that are tailored to meet their specific needs, eliminating redundancy and the unnecessary expenditure that comes with it. And by reducing the need for expensive Ethernet cabling, effectively removing the restrictions of additional wired components within your network, Access/One Network offers a truly unique and versatile wireless solution.

Our network nodes can be installed using wireless 802.11a/g uplinks to corporate, regional or metro-wide networks instead of the typical wired 10/100 Ethernet method, an option that is highly convenient in established Enterprise environments where it is impractical and expensive to install new Ethernet cabling (especially in old buildings where cable routing can mean substantial modifications to existing structures). This capability is not only cost-effective, but also allows you to install nodes without the need for a lengthy and often complex site planning process.

With Access/One Network, IT administrators need only answer four simple questions when planning their network deployment criteria:

- What types of wireless client connections do I need?
- Do I want to use a wired or wireless network connection?
- How many potential users do I have?
- What throughput do I want to offer my users?

With the freedom and flexibility that Access/One Network provides, implementation becomes a rapid and painless experience, ensuring that your network is up and running on time and at minimal cost (compared with a wired solution, or a wireless solution that does not offer scalability and/or the power and intelligence of a structured mesh). But deploying Access/One Network is just the beginning of the story—once your network is established, you very quickly discover that Access/One Network has so much more to offer than mere convenience.

Mesh Topology

"mesh: The space or interstice between the threads of a net."
New English Dictionary, March 1932

In the current WLAN market, the trend is to strip the intelligence from the access point and put the workload on the switch. Although this approach may reduce the initial cost of the AP, it introduces serious problems, like single-point-of-failure, bottlenecks, and an obvious lack of scalability and flexibility. For example, whenever you add just a few APs and exceed the port limitation of the existing WLAN switch, the only solution is to add a new switch. This is not only expensive, but does nothing to solve the root cause of the problem.

Strix Systems believes that the power of computing and networks can only be fully harnessed when the intelligence of the system is distributed between its component parts and used locally. But to function effectively and reliably, this type of "distributed intelligence" must be governed by a centrally managed source.

Access/One Network's structured mesh topology enables nodes within the network to communicate with each other and perform intelligent tasks and analysis, ensuring that the network's performance is always at its peak. But if problems do arise, the system has the remarkable ability to **tune** and **heal** itself instead of failing. Quite simply, there is no single point of failure or any loss in the network's performance and its ability to deliver the services its customers demand.

Each network node is fully aware of its neighbor and, in the event of an adjacent node's failure or overload, will redirect the affected user traffic. Although the intelligence of the network is distributed, network security parameters, monitoring rules, and system upgrades can be conveniently controlled from one central location via our Manager/One graphical management interface.

Mesh is inherently reliable and can be extended easily to include thousands of nodes. As a result, Access/One Network can be installed in hours instead of days or weeks, meaning a successful wireless mesh network deployment doesn't require elaborate planning and site mapping to achieve its goal. When installed, the network is self-governing—simply moving a network node, or dropping another node into place, can fix a weak signal or dead zone.

1

Any wireless network can now benefit from a Strix structured mesh solution that satisfies the multiple conflicting demands of redundancy, distributed communications, flexibility and scalability, security and management, cost, and overall reliability.

Sold globally by a dedicated network of qualified and approved distributors and integrators, Access/One Networks have been deployed in hundreds of indoor and outdoor locations worldwide. These deployments cover the broadest range of markets, such as Metro, Public Safety, Government, Energy, Transportation, Hospitality, Education, Enterprise, Residential and Carrier Accesss.

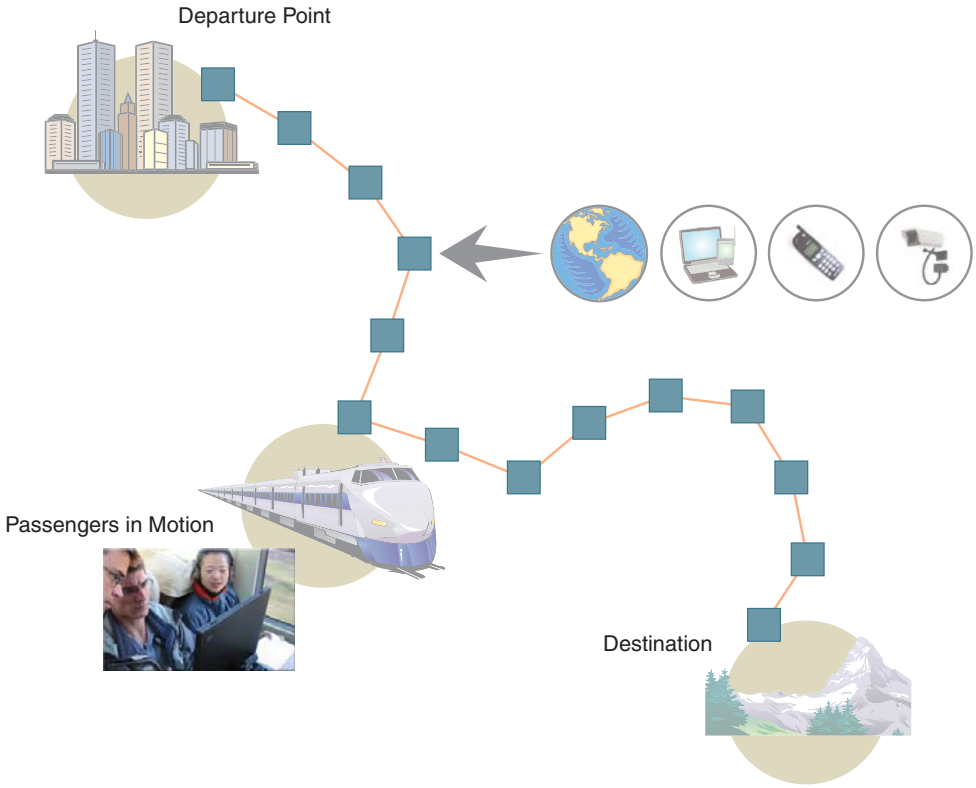

Figure 4. Strix Mesh Architecture (OWS Transportation Scenario)

To find out why Strix Systems is the leader in wireless mesh deployments, and to learn more about our family of INDOOR products and OUTDOOR products that have been installed around the world, visit us at http:// www.strixsystems.com.

An Intelligent Network

Every node in your Access/One Network has the ability to self-discover its neighbors and form a highly versatile mesh network, regardless of whether its connection to the LAN is wired or wireless. As nodes communicate with each other, the entire system becomes one intelligent network where traffic is routed on optimal paths as the system automatically **self-tunes** and **self-heals** in real time.

In addition, because each network node is constantly monitoring the system's health and inventory, Access/One Network has the ability to immediately detect the presence of any rogue wireless devices on multiple frequencies operating within its range.

Statistical data is periodically sent to all network servers and can be viewed at the network, subnet, node or individual module level from our Manager/One intuitive management interface.

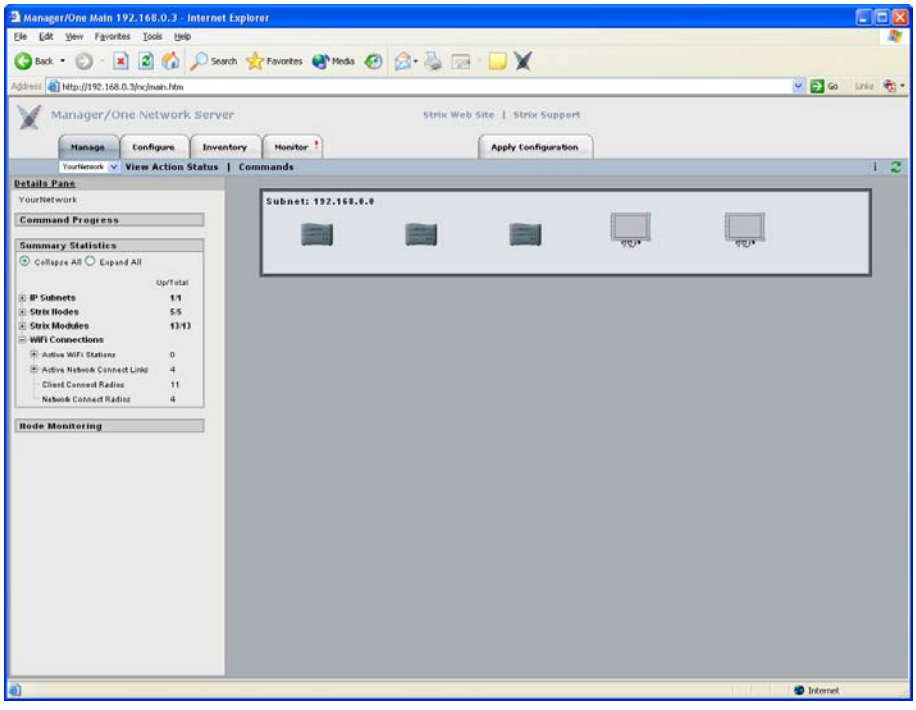

Figure 5. Manager/One Interface (Network Level)

1

Self-Discovery (or Physical Inventory)

All network nodes automatically identify themselves to the network, and as a consequence each node discovers the identities and configurations of its neighbors, as well as their current active state. In short, they know who they are, what they are, and what they're doing. Access/One Network's self-tuning, self-healing and rogue detection features depend heavily on this functionality. Alternatively, you can configure and manage the network based on an inventory list of physical components. The inventory list is generated by Manager/One automatically, but you can add and/or delete items from the list, as needed.

Self-Tuning and Self-Healing

If the wireless environment changes for any reason, such as the addition of a new network node, data paths are automatically re-evaluated to ensure that the network is self-tuned for peak performance.

The same process occurs if there's a loss of a data path, ensuring that the network can heal (repair) itself and that nodes stay connected. With our mesh topology, there is never a single point of failure that can affect the entire system. The following graphic offers a simple illustration of how a node finds an alternative path to its neighbor when one data path is temporarily lost.

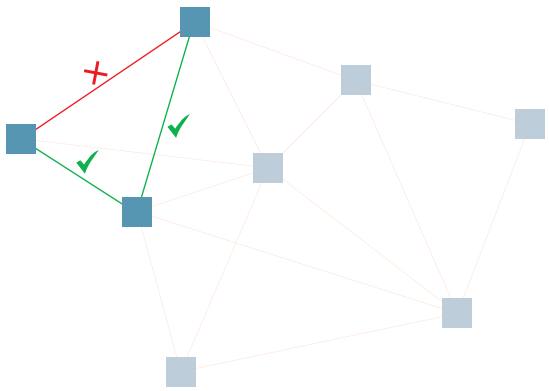

Figure 6. Self-Tuning and Self-Healing

The self-tuning and self-healing processes are dynamic, meaning they occur in the background in real time and without human intervention.

Background Scanning

When a Network Connect first connects to the network, it performs an initial scan of available Wi-Fi channels and generates a list of potential alternative Client Connects that are reachable. Following the initial scan, the Network Connect continually scans in the background to maintain the inventory list and enable the system to make the following intelligent decisions:

- When to drop the current path and select a better path, then connect to the appropriate node (self-tuning).
- When to select the best path (or detect the loss of a path) and select the next best path, then connect to the appropriate node (self-healing).
- Which APs are rogues.

Detecting Rogue Devices

A rogue device is any access point that the network doesn't recognize. This can be a third party AP that is not part of your Access/One Network or a valid network node that has yet to be assigned.

Network Connects perform an active scan for rogue devices during every boot sequence, and periodically thereafter. Alternatively, you can initiate a client scan from Manager/One. When a rogue scan is started from Manager/One, all Client Connects are placed in active scan mode, while Network Connects continue to perform the background scan. Scans generally take between 10 and 20 seconds to complete. Detected rogue devices are immediately reported to the network server and the operator is alerted immediately. Rogue detection distinguishes between:

- Wired devices
- Wireless devices
- Wired and wireless devices (the most common culprit)

Rogue detection is achieved by triangulation, with Wi-Fi scanning performed by selected Access/One Network elements. Rogue detection can affect the network service because the system needs to scan all the available WiFi frequencies.

1

Network Servers

The network server is a critical component in your Access/One Network. It consists of a hardware platform and base software. The network server can be installed into any node within the network—wired nodes are preferred, and at least one network server should be installed in a wired node.

The software running on the network server provides much of the intelligence within the system and facilitates most of Access/One Network's unique features and functions. Overseeing the overall management and control of the system, the network server provides distributed functionality that enables your Access/One Network to function effectively as a secure wireless system that easily scales as your Enterprise network grows.

Some of the key features provided by the network server include advanced security, dynamic operation, network management, traffic prioritization and control, and enhanced user mobility and tracking.

- **Advanced Security**
  The network server enables your Access/One Network to provide a full array of standards-based tools to secure the network. In addition to using the same security servers and virtual private network (VPN) software that is used on wired networks, Access/One Network offers enhanced system-level security against attackers and rogue access points. All of the wireless mesh links, as well as network management and control data, are encrypted using the Advanced Encryption Standard (AES), making it nearly impossible for attackers to intrude into the network. In addition, whenever a user is authenticated, the network server ensures that user security is maintained while they roam the network.

- **Dynamic Operation**
  Each network node automatically associates itself with the best available network server (least congested and closest). If the wireless environment changes for any reason, associations are automatically re-evaluated to ensure that the network remains at its peak performance.

- **Network Management**
  The network server maintains internal tables for each network node that it communicates with, as well as any other network servers within Access/One Network. The network server works in conjunction with Manager/One to build detailed system/node/module level mapping of the network, enabling you to monitor and configure the network at any level.

- **Traffic Prioritization and Control**
  User traffic on the network is managed locally at the network node. Network traffic is managed at the system-level by the network server. Knowing the users that are attached to each node allows the network server to determine how user traffic should be prioritized and routed through the network. All types of user data are managed in this way (including broadcast and multicast traffic) which significantly reduces any overhead on the network.

- **Enhanced User Mobility and Tracking**
  Network servers make roaming possible for users of devices, such as PDAs, who previously had to re-login every time they entered a conventional access point coverage area. But thanks to the availability of 24/7 connectivity through Access/One Network, even the smallest, most mobile and most battery-sensitive of the handheld devices can now serve as productive business tools.

Master Network Server

Establishing a master/slave relationship between network servers facilitates efficient Wide Area Network management by reducing the amount of traffic between two subnets on the same network. It also provides a single network server responsible for all Strix devices within its subnet, which Manager/One users are redirected to if they try to log into a non-master network server.

The master network server transmits time/date packets periodically to all Strix devices using the Strix Time Distribution protocol, enabling all Strix network nodes and wireless modules to be synchronized.

1

Communicating Across Remote Subnets

Access/One Network can be configured to enable communication between network servers on remote subnets (for example, remote subnets in New York and Los Angeles can be managed from the same Manager/One session). When network servers are configured to communicate with each other across remote subnets, you should expect the following behaviors from the system.

- If you decide to remove the NS to NS communication feature and just one network server does not register the updated configuration during the reboot, the network servers will continue to exchange information.

  See also, "Starting a New Network" on page 32.

- In Manager/One, using the intuitive mouse-over feature on Network Connects does not reveal their corresponding Client Connects. You can access this information by connecting to remote network servers directly from the Web.

Client Connect

Client Connect is the system topology that enables your Access/One Network to support and provide access to client devices using 4.9 GHz Public Safety, 802.11a or 802.11g wireless technologies. With Client Connect you can customize each network node to support the wireless technologies you need in the locations you need them. Any mix of these technologies can be supported within a single node or across the entire Access/One Network.

Whether users carry a notebook, PDA, barcode reader, or other WLAN device, they are able to stay continually connected to the network as they roam. No special software is needed on the device, and no special configuration is required to remain connected.

Each network node is capable of supporting multiple Client Connect modules of any type and technology mix. This versatility of design provides you with a wide variety of configuration options to meet all your user connectivity needs. And support of future wireless technologies is as simple as adding a new Client Connect module.

Network Connect

Network Connect is the system infrastructure used by your Access/One Network for wired or wireless connection to an existing wired network (small or large). Each node within the Access/One Network can utilize a wired Ethernet or wireless module (802.11a or 802.11g) for node interconnectivity or connection to a wired legacy network.

When nodes in your Access/One Network are configured for wireless Network Connect, the system provides several distinct advantages over a typical wireless network that uses wired connections. These advantages include:

- Secure networking
- Self tuning, rapid self-healing, and rogue device detection
- Scalability
- Simple installation
- Lowest cost of deployment

Unlike traditional wired Ethernet LAN/WAN connections used by access points and WLAN switches, Access/One Network's wireless Network Connect option provides an advanced level of security between the network node and the LAN/WAN. By default, the wireless Network Connect link utilizes AES encryption with a secret key and cannot be compromised.

Wireless Workgroups (IWS only)

Wireless Workgroups enable wired Ethernet users to take full advantage of the wireless capabilities of Access/One Network. By connecting stationary users to the wired Ethernet ports within a network node, wired users can have access to all of the benefits that Access/One Network offers. The advantages of this option include:

- Connecting stationary users throughout the network without incurring the time and expense associated with providing individual wiring drops.
- Enables user workgroups in remote locations to connect to your Access/One Network where wired connectivity may not be feasible.

1

Offering a Rich Technology Base

Access/One Network provides many technology features, most of which are transparent to the user but nonetheless instrumental to the smooth and efficient operation of the network. In addition to some of the key features and functionality already mentioned, here are just a few more, organized alphabetically and by functional area:

IWS and OWS Hardware

- **Dual Band Radio Modules**
  The OWS supports dual band radio module configurations, where a single module offers 4.9 GHz Public Safety/802.11a and 802.11g wireless technologies. IWS modules operate as either 802.11a or 802.11g radios (not both).

- **Integrated Base Module and Lightning Protection (OWS only)**
  By integrating the Base Module and lightning protection circuitry, power distribution within the OWS enclosure is more efficient and the expansion capability of the module stack has been broadened.

- **Minimal Mechanical Components**
  Both the IWS and OWS have been designed with minimal mechanical components to reduce the risk of mechanical failure, while maintaining the highest standards of construction and durability.

Manager/One

- **Configurable Tools**
  Users can configure tools within Manager/One to help them personalize their use of the interface and use it more efficiently and effectively.

- **Intuitive Mouse-Over**
  An intuitive mouse-over feature assists you with navigation and provides detailed information at your fingertips. For example, when you roll over an icon, the color of the icon changes and a pop-up window appears that contains important information about the device associated with the icon.

- **Monitors**
  A comprehensive choice of monitors is included within the Manager/One interface, including AP monitoring, Network Connect monitoring, wireless client monitoring, and rogue device monitoring.

- **Multi-View Management Interface**
  The Manager/One interface offers a standard graphical view of the network and its components, or a logical mesh view that allows you to see a graphical representation of the relationship between the wired and wireless segments of the network.

- **Segment View**
  This feature provides a window into each Ethernet connection segment within the network, with a choice of views (list or icon). Simply choose the view you prefer with a click of the mouse.

System and Security

- **Easy Rollback to Factory Defaults**
  Allows network administrators to re-establish factory default configuration settings via the simple click of a button.

- **GPS Positioning**
  Allows you to enter a GPS location (in degrees) and vertical elevation for a specific node. This information is displayed in Manager/One, the Command Line Interface, and SNMP.

- **Inventory Control**
  Once the mesh network is formed an inventory list is created on the network server and distributed to all Strix devices participating in the network. The inventory list is used for bi-directional authentication of network devices whenever they communicate with each other. For obvious security reasons, any devices that are not part of the inventory list cannot participate in network topology building, exchanging configuration information, or managing Strix devices.

1

- **MIBs and Secure Remote Management**
  Access/One Network supports the 802.11 MIB (Management Information Base), as well as various Strix proprietary MIBs. Any MIB I or MIB II compliant SNMP management console (such as CiscoWorks or HP OpenView) can be used to manage your network remotely and securely. Network management sessions running through SSH (Secure SHell) or HTTPs (secure HTTP) ensures that the session is fully encrypted and cannot be compromised by unauthorized users.

- **Multiple Ethernet Segments**
  Network servers operate across existing Ethernet switches, routers, hubs and other wired Ethernet segments without the need for special equipment or VLAN tagging.

- **Network Server Security**
  Management traffic on the Ethernet between the network server and module is automatically encrypted to prevent "listening" on the LAN/WAN. When set to the automatic mode, the network server will communicate with wireless modules over an unencrypted connection while maintaining a secure connection throughout the rest of the wired network.

- **Power-over-Ethernet (IWS only)**
  Each network node uses a Base Module that provides power via an external AC adapter, and includes up to four 10/100 Fast Ethernet ports for wired network connectivity. When present, one of the Ethernet ports supports Power-over-Ethernet (PoE) technology. PoE eliminates the need for a power cord by delivering the necessary power to a device via a standard CAT5 Ethernet cable.

- **Priority/One**
  User-definable Class of Service (CoS) filters enforce end-to-end Quality of Service characteristics throughout the Strix network, including VLAN priorities, IP TOS and IP Protocol. CoS classifies packets by examining their parameters or CoS markings, then placing packets in queues of different priorities based on predefined criteria.

- **RADIUS Accounting**

  Through a wireless interface, Access/One Network supports RFC 2866 standard RADIUS (Remote Authentication Dial-In User Service) accounting, allowing customers with existing RAS Radius-parsing scripts/tools to leverage their investment as well as customize their tools to extract all available statistical information.

- **Syslog Support**

  Access/One Network offers comprehensive Syslog (system logging) functionality, including the ability to monitor Syslog events. Logged events can be sent to multiple Syslog servers, though using more than one server can impact the system's performance.

- **VirtualStrix**

  Access/One Network nodes support the 802.1Q VLAN tagging of wireless frames based on SSID or station MAC address. This is achieved by assigning a specific VLAN number and priority level to each frame generated by a particular station. Nodes support up to 16 simultaneous SSIDs and users can enable or suppress the broadcasting of SSID information. Security parameters can be applied for each SSID tied to a VLAN definition, including Open, 802.1x (WEP) and WPA for authentication, and Clear, WEP, TKIP and AES for encryption. During 802.1x authentication, VLAN information is retrieved from the RADIUS server and applied on a per-station basis.

- **Zero Configuration Networking**

  In the absence of a DHCP server, Strix modules will automatically select unique IP addresses, enabling users to statically configure the modules and manage the Strix network (IP gateway, DNS server or DHCP server IP addresses must be properly configured).

1

Wireless

- **Public Safety Support (4.9 GHz)**
  Access/One Network now allocates 50 MegaHertz (MHz) of spectrum in the 4940-4990 MHz (4.9 GHz) band in support of Public Safety applications.
- **Active WLAN Associations**
  Each radio can support 128 WLAN associations, with the OWS dual radio able to support 256 WLAN associations (128 x 4.9 GHz Public Safety or 128 x 802.11a, and 128 x 802.11g).
- **Channel Coordination**
  To prevent conflicting channel assignments, each radio within an IWS or OWS product coordinates channel selection with any neighboring radios running the same technology (4.9 GHz Public Safety, 802.11a or 802.11g).
- **Super G™**
  Access/One Network supports Super G technology offering data rates up to 108Mbps, compatible with the 802.11g (54 Mbps) wireless technology.
- **Wi-Fi Channel List**
  Specific Wi-Fi channels (or a set of channels) can be defined that will be scanned for AP and backhaul operation.
- **Wi-Fi Client Query**
  This feature provides the option of querying the network in search of Wi-Fi clients, based on a matching MAC address or any client showing an RSSI value less than -85 dBm. Query results are displayed in a table that can be sorted by the user.

Hardware Specifications

Data sheets contain the most up-to-date specifications for the Strix family of Indoor Wireless System (IWS) and Outdoor Wireless System (OWS) products. These data sheets can be downloaded from our Web site at: http://www.strixsystems.com.