

ACCESS/ONE™ NETWORK

PRODUCT DESCRIPTION



 **StrixSYSTEMS**
NETWORKS WITHOUT WIRES™

310 N. Westlake Boulevard, Suite 150
Westlake Village, CA 91362
Phone (805) 777-7911
www.strixsystems.com

Access/One™ Network Product Description

Overview

Access/One Network is a complete wireless local area network system, providing all of the management and security features that enterprise network managers expect. It includes multiple radio frequency technologies – 802.11a, 802.11b/g, and Bluetooth – all in one intelligent, secure, scalable and self-tuning network. Network Nodes are small – a 3.65 inch by 5 inch footprint, with heights ranging from about 3 inches to 5 inches. They may be mounted on walls, cubicles, desktops, or on or above the ceiling.



Access/One Network reduces and even eliminates costly Ethernet cables, making initial deployment and future upgrades extremely easy and cost effective. Yet Access/One Network provides a single secure and manageable network. Information Technology departments gain control of the wireless environment; Enterprises gain business advantages from improved workforce productivity, faster response to customers, and rapid network deployments to meet business needs.

An Access/One Network Node is about the size of a PDA.

Just as grid computing has evolved to maximize the advantages of distributed processing, so mesh topology is emerging as the best architecture for wireless networks. Strix Systems deploys a mesh network that frees the network administrator from the cost of detailed planning and wiring. Strix overcomes the two most costly hurdles in deploying a wireless LAN today by using a wireless uplink and a mesh topology.

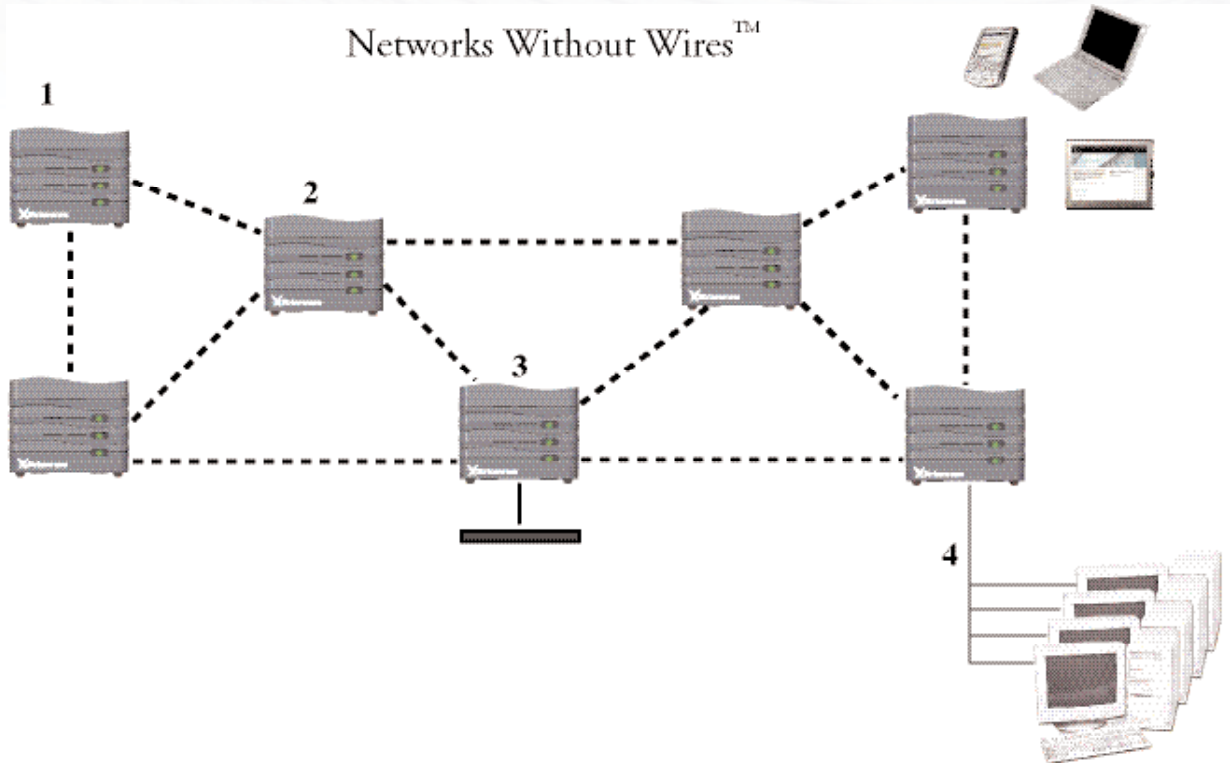
No expensive Ethernet cabling is needed with Access/One Network. Network Nodes can be installed using 802.11a/g uplinks to the wired network instead of the typical wired Ethernet method. This option is especially useful in very new or very old buildings, where it is impractical and expensive to install Ethernet cabling. This also provides enough flexibility that Nodes can be installed without a lengthy planning process.

Each Network Node has the ability to self-discover its neighbors, and to form a mesh network, regardless of whether it has a wired or wireless connection to the LAN. Mesh topology is the next step in network evolution, beyond centralized switching and lightweight access points. Mesh topology enables self-configuring, self-healing, and highly scalable networks. Distributed intelligence routes traffic on optimal paths, limits broadcasts and bottlenecks, simplifies installation requirements, and grows proportionately to provide connections for thousands of wireless devices. Intelligence is distributed in the wireless network – not centralized in a wiring closet or held in isolated islands of equipment.

Access/One™ Network Product Description

An IT Manager specifies only a few simple parameters:

- The type of wireless client devices to use (any combination of 802.11a/b/g and/or Bluetooth)
- The way the Network Nodes will be connected to the network (wireless, Ethernet, or a mix)
- The number of wireless users to serve and desired bandwidth per user



Network Nodes can then be deployed to perform many functions:

1. At the perimeter of the network, this Network Node serves wireless devices within the enterprise. This Node can be equipped with single or dual technologies (choose from 802.11b, 802.11a, 802.11g and/or Bluetooth) to serve clients. It uplinks to the network via a wireless connection rather than an Ethernet connection.
2. This Network Node provides a relay of the wireless uplink from Node #1 to Node #3. The IT Manager can augment this Node's wireless relay function by adding the ability to serve wireless clients within its range (802.11a/b/g and/or Bluetooth).
3. This Node connects via Ethernet to the wired LAN. It is typically where the Network Server is located. For redundancy purposes there can be more than one of these types of Nodes in the mesh.
4. The Wireless Workgroup Node serves a remote group of four users who are stationary and plug into the Ethernet connections on this Node. The Node connects wirelessly, even at a long distance, back to the LAN.

Access/One™ Network Product Description

Access/One Network Features and Benefits Summary

Feature	Benefits
Mesh Topology	Reduces costs and simplifies network operation. Next step in network evolution – no bottleneck or single point of failure. Scales proportionately with user growth – up to thousands of connected devices.
Networks Without Wires™	Reduces or avoids cabling costs. Provides rapid installation and moves for fixed and mobile type devices/computers. Reduces network administrator effort.
Strong Security (Strong authentication and encryption)	Reduces cost. Reduces administrator workload by using installed systems. Leverages existing RADIUS and certificate servers; standards-based so no special NIC cards required. Includes full range of security tools from WEP to EAP-TLS and AES.
Modularity	Reduces cost of ownership. Flexible, configurable to individual needs, including multiple RF technologies in a single network, with one management and security system. Linear scalability of nodes and technologies to meet enterprises' growing data networking needs.
Automatic Operation (Self-discovery, Self-healing)	Improves network uptime, reduces administrator workload. Automatically configures network paths. Add, move, change nodes without any changes in the wiring closet or server room. Automatically adjusts as nodes are removed or relocated.
Self-tuning	Improves network performance. Automatically selects highest performance path through the network, with lowest latency & best throughput.
Wireless Routing	Improves network throughput. Routes traffic to specific nodes, avoiding traffic congestion in shared wireless medium. Uses multicast to limit discovery broadcast traffic. No need to route all traffic through a central controller or switch.
Mobility for any Wireless Device	Improves worker productivity. Whether users carry a notebook, tablet, PDA, or other Bluetooth or WLAN device, they stay continually connected to the network as they move about the building. No special software is needed on the device.
Bluetooth Roaming and increased device density	Turns handheld devices into productive business tools. Adds roaming for Bluetooth devices and eliminates need for frequent re-logins. Handles almost 3 times the number of devices (20) compared to standard Bluetooth access points (7).
Architect/One	Reduces costs by eliminating need for detailed planning and surveys. Using easy-to-obtain site data, Architect/One defines equipment needs and places equipment for optimum coverage.

Access/One™ Network Product Description

Self-Discovery & Self-Tuning Provide Automatic Operation, Simplified Administration

Access/One Network Configures Itself

When a Network Node is turned on, the individual modules within the Node automatically discover each other and determine their physical position and role within the Node, including whether the interface to the network is wired or wireless.



The Network Node then automatically discovers the rest of the Nodes in the Access/One Network via the wired or wireless Network Connect module. The Node automatically associates with one Network Server using an algorithm based on several decision factors. The Network Server (which oversees the management and control of the network), Client Connect Modules (which enable wireless attachment of users to the network), and Network Connect Modules (which provide wired or wireless connectivity to the LAN) automatically request and establish IP addresses from the DHCP server on the enterprise network.

On-going Discovery Makes Access/One Network Self-healing and Self-tuning

After the network connections have been established, forming the mesh topology, each Network Node continues to process the decision algorithm at a user-defined time interval. This guarantees that any change in network topology due to Access/One Network elements being added or removed is immediately recognized and acted upon, ensuring the network is always tuned for optimal performance and operation.

Low Overhead Means More Bandwidth for Traffic

The discovery process utilizes a lightweight client and an ingenious combination of unicast and multicast messages. Only 1-2% of the available bandwidth is used for management and control messages with this scheme, as messages are usually routed to specific Network Nodes and discovery broadcasts are sent via a multicast technique to save bandwidth.

The Discovery Process Provides Other Benefits

In addition to this process, as Network Servers become aware of each other, they communicate and synchronize known element tables to provide failure redundancy. This not only tracks users, but also provides connection persistency as users move around the building.

The Network Server maintains a registry of Network Nodes and their modules, along with self-discovered routing information and routes in use. The Network Server also maintains the management database for SNMP monitoring, internal alarm and fault logging, configuration and performance tuning, usage metering, and topology mapping. Multiple Network Servers automatically discover each other and maintain synchronized registries for redundancy. A single Network Server is usually sufficient for a network with up to eight Network Nodes. The ratio is based on the management signaling required to support mobility and is not a function of the amount of data traffic.



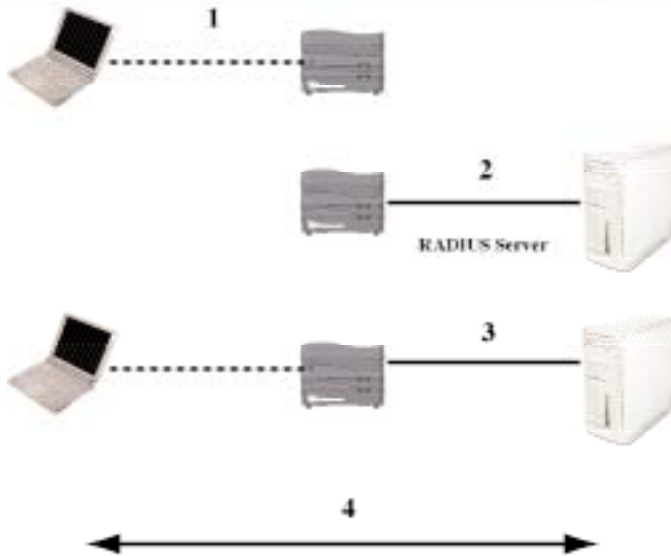
The Payoff is Clear

These features enable an IT administrator to install and manage an Access/One Network with minimal effort because Access/One Network performs all these functions automatically, with no human intervention required.

Access/One™ Network Product Description

Strong Security Protects the Network and its Users

Access/One Network provides a full array of standards-based tools to secure the wireless network. Securing a network means authenticating potential users and encrypting information exchanges to prevent outsiders from eavesdropping. On a wired network, IT managers routinely use login names and passwords and rely upon physical security to hide the transactions from snoopers. Secure wireless networks use certificates to authenticate identity, and dynamic encryption to protect information flow.



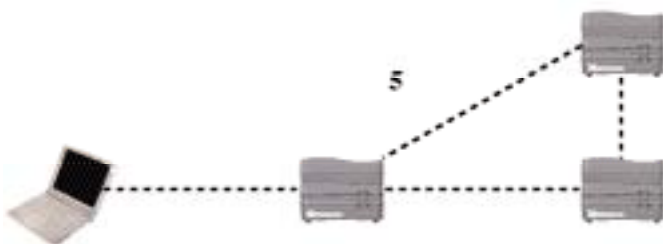
1. A wireless device connects to a Network Node and uses its public key certificate and the EAP-TLS protocol to request authentication.

2. The Access/One Network Node uses its shared secret to authenticate with the RADIUS server. This makes the Network Node a trusted network element.

3. The Network Node then forwards the device's authentication request. The Network Node blocks all traffic to and from the device except the authentication request.

4. When the RADIUS server signals a successful authentication, an encrypted AES link to the wireless device is established using dynamic keys. The Network Node unblocks the traffic for this particular client device. All members of the network are now properly authenticated and encrypted.

**All of these steps take place automatically.
No user action is required.**



5. Access/One Network uses AES to encrypt all of the mesh links as well as all of the network management and control data, making it impossible for attackers to intercept this information and hijack the network. Finally, once a user is authenticated, the user security is maintained while the user roams about the network.

Access/One™ Network Product Description

Strix Systems Recommendations for Security

At least minimum security should be established on any wireless connection, using access control lists and static WEP (wired equivalent privacy). This minimum level can be achieved with any common NIC card and client software connected to an Access/One Network.

With the addition of a RADIUS server, the wireless connection can be made much more secure by using 802.1x Extensible Authentication Protocol (EAP) and some form of key rotation. The full Wi-Fi Alliance WPA standard (Wi-Fi Protected Access) calls for the Temporal Key Interchange Protocol (TKIP); if the client does not support TKIP, then a client-controlled key exchange can be established to provide dynamic WEP and improved protection against hackers.

The best implementation uses both a RADIUS server, with EAP authentication (either transport layer TLS or a tunneled TTLS), and encryption with the Advanced Encryption Standard (AES).

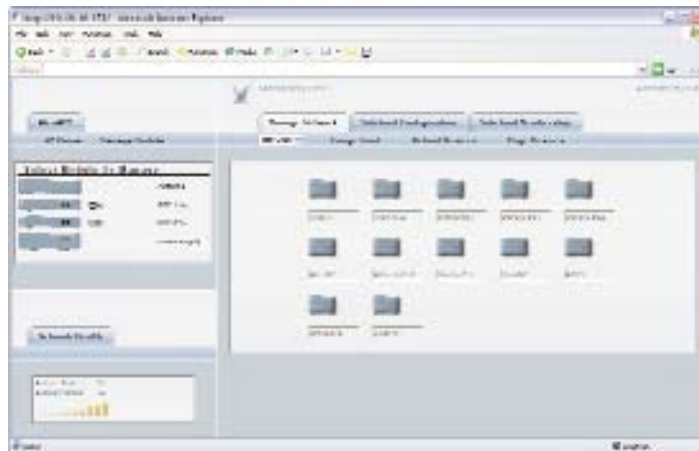
	Minimum	Better (WPA)	Best
Authentication	MAC address control list	802.1x EAP	802.1x EAP (TLS or TTLS)
Encryption	Static WEP	Dynamic WEP or 128-bit WEP with TKIP	Dynamic AES
Requirements	No RADIUS server	RADIUS Server, No AES hardware support or NICs	RADIUS Server, AES hardware support and AES NICs

Access/One™ Network Product Description

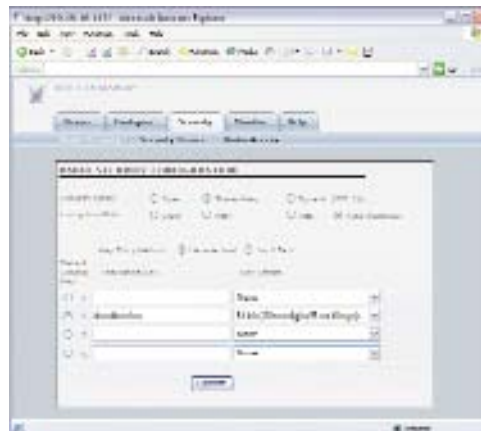
Manager/One Provides a Window into the Automatic Operation

Access/One Network has been designed to self-configure, self-tune, self-diagnose and heal without any user intervention. Access/One Network also offers the tools to maintain full manual control.

Access/One Network can be configured and monitored with a web browser via a built-in web server interface or from a terminal or PC connected via Telnet using the system's Command Line Interface (CLI).



Manager/One provides a map (via auto-discovery) of all Network Nodes within the Access/One Network. From this screen the IT Manager can define settings such as security on a network-wide, group-level or individual Node basis. This screen will also provide quick glance details of the Nodes such as health status. The IT Manager can also click on any Node and drill-down for element manager-type functionality, such as Node-level configuration and statistics.



Access/One™ Network Product Description

The configuration function consists of general and advanced parameters, such as security settings, privacy settings, firmware updates, and SNMP configuration. As you would expect, from these screens all of the standard networking and wireless parameters can be defined and set. Examples include SSID, Turbo on/off, DHCP/static IP, Encryption on/off, WEP/TKIP/AES, Encryption key and length, 802.1x enable, and RADIUS setup.

The reported statistics are separated by Network Node versus attached stations. The Network Node statistics reported include total authentication and association attempts, number of packets sent & received, various types of transmit/receive errors, and CRC errors. The per-station statistics monitored and reported include association state, signal strength, data rate (Mbps), various types of packet errors, authentication type, encryption, number of associations / disassociations / reassociations, and number of packets sent and received.

Additionally, for quick visual reference, each Access/One Network module (with the exception of the Antenna Module) contains a single multi-state LED on the front panel. This LED maintains the following states:

- Not lit – the module has no power or has failed
- Solid Green – the module is functioning normally
- Flashing Green – the module is initializing
- Solid Orange – fault condition; the module is not functional
- Flashing Orange – the module is functioning but it is overloaded or the radio signal is too weak
- Flashing Red/Green/Orange sequence – the unit is being 'paged' by the administrator (to aid in locating a particular device)

Access/One™ Network Product Description

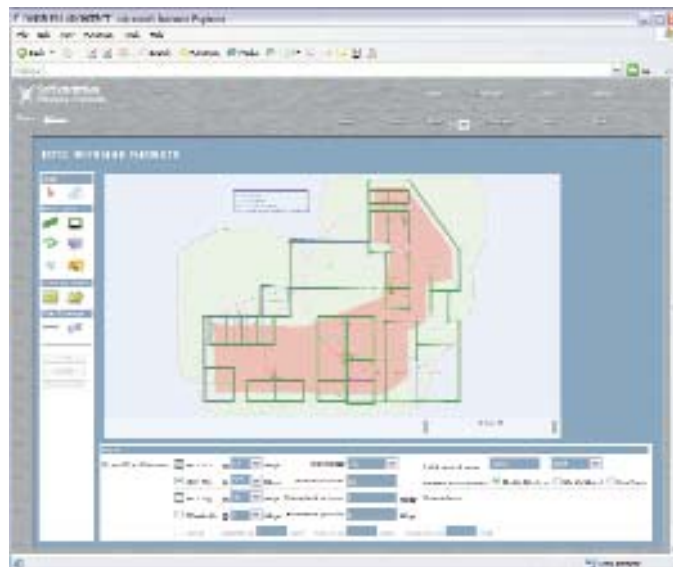
Architect/One Simplifies Network Planning

A customer needs to make only a few simple decisions:

- the type and combination of client connect (802.11b, 802.11g, etc),
- the type of network connect (wireless or wired), and
- the number of users to be supported, and the desired bandwidth for each

The Architect/One software determines the necessary equipment and optimal placement to meet the customer's stated needs. It also allows for manual placement and changes as desired.

Access/One Network Architect/One combines the advantages of both empirical and deterministic models to accommodate wideband signals, high site-specific accuracy, short computation time, and easy-to-obtain input data. All of the electromagnetic effects, including diffuse scattering, are taken into account. Signal strength and angle of arrival are predicted in each element of the bitmap background for high accuracy of results. The web-based software can be run from an ordinary PC, with predictions obtained within a few seconds.



New projects are simply defined using a set of general information, which includes the building area, number of floors, type of construction, ceiling heights, mounting preference (wall, ceiling, desktop), RF technology, desired bandwidth per user, desired throughput per user, number of users per floor, and infrastructure type (wired, wireless, or mix).

Floor plans may be loaded as AutoCAD, PDF, GIF, or JPEG files, providing a background for more detailed input. A user may set the scale and then add details such as offices, cubicles, walls, power locations, Ethernet outlets, and building obstructions such as elevators, columns, and stairwells. Various wall types may be selected as well. With a single click, Architect/One then optimizes coverage for the selected RF type using its sophisticated algorithm.

Network Node placement may be manually modified if desired, and the software automatically generates new coverage predictions based on the physical placement selected. When finished, a network designer prints out the map and module configuration as the guide to product placement during installation. An output report automatically generates the equipment-ordering list.

Access/One™ Network Product Description

Feature	System Requirement
IEEE 802.1x Authentication	<p>Industry standard RADIUS server, such as:</p> <ul style="list-style-type: none"> • Microsoft IAS • Cisco Access Control Server • Funk Odyssey or Funk Steel-Belted RADIUS • Meetinghouse Data AEGIS <p>Industry standard certificate server, such as Microsoft CertSrv</p> <p>Industry standard software clients, such as:</p> <ul style="list-style-type: none"> • Microsoft Windows 2000 Service Pack 3 • Microsoft Windows XP • Funk Odyssey <p>No special NIC cards required. No special Strix Systems software is required.</p>
AES Encryption	<p>PC card with AES hardware and software support, such as:</p> <ul style="list-style-type: none"> • Accton WN6301, Accton WN4301 • ActionTec 802.11a PC Card • D-Link DWLAB-650, DWLAG-650 • Gemtek WL-611 • Linksys WPC55AG • Wistron CB-100AB, CB-500AG
IP Address Assignment	Any enterprise DHCP server
Power over Ethernet (PoE)	Any 802.3af-compliant injector, such as PowerDsine, or PoE infrastructure (LAN switch or hub); Access/One Network modules are also compatible with Cisco proprietary version of PoE provided by their injectors and LAN switches.
SNMP Management	Any MIB I, MIB II –compliant management console, such as CiscoWorks or HP OpenView. Telnet or web access from any PC workstation
Multiple Ethernet Segments	Operates across existing switches and wired Ethernet segments: no special switches or VLAN tagging required.
Bluetooth roaming and increased device density	Any Bluetooth-equipped device with version 1.1 or higher and LAN Access Protocol; no special client software is required.
General	Access/One Network is designed to be fully compatible in Microsoft Windows and Cisco switching/routing environments with no special software, servers, or power injectors required.

Access/One™ Network Product Description

Modular Design Meets Specific Customer Requirements

Access/One Network modules are designed to stack on top of each other with an interlocking mechanism to hold them securely together. Integrated connectors provide power and signal transfer between modules. No special tools are required for assembly or disassembly. A product label on the bottom of each module indicates the specific model name, model number, MAC address, and serial number. A stack of modules becomes a Network Node. Each Network Node provides localized connectivity and intelligence. Multiple Network Nodes connect in a mesh to form the Access/One Network. The role of a Network Node is determined by the selection of modules:

Client Connect

- 802.11b Client Connect
 - o 802.11b Wireless Module (WM11B)
 - o 802.11b Antenna Module (AM11ABG)
- 802.11g Client Connect
 - o 802.11g Wireless Module (WM11G)
 - o 802.11g Antenna Module (AM11ABG)
- 802.11a Client Connect
 - o 802.11a Wireless Module (WM11A)
 - o 802.11a Antenna Module (AM11AA)
- Bluetooth Client Connect
 - o Bluetooth Wireless Module (WMBT)

Network Connect

- Wired Ethernet Network Connect
 - o Base Module with 1-port Ethernet (BME1)
- Wireless 802.11a Network Connect
 - o 802.11a Wireless Module (WM11A)
 - o Wireless Base Module (BME0)

Wireless Workgroup

- 4-port Wireless Workgroup
 - o 802.11a Wireless Module (WM11A)
 - o 802.11a Antenna Module (AM11AA)
 - o Base Module with 4-port Ethernet (BME4)

Network Server

- Network Server (NWSV)
 - o Network Server Module
 - o System Software
- Bluetooth Mobility Software (SWBT)

Example Access/One Network Node Combinations



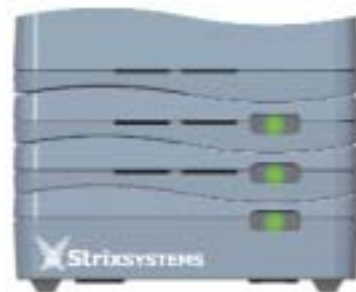
Antenna Module
(AM11ABG)

Client Connect Wireless Module
(WM11B)

Network Connect Wireless Module
(WM11A)

Network Server Module
(NWSV)

Base Module (BME0)



Strix Systems, Access/One, Manager/One, Architect/One, Networks Without Wires, among others, are trademarks of Strix Systems, Inc. and all applicable affiliated companies, Reg. U.S. Pat. & Tm. Off. and in many other countries. All other marks are the properties of their respective owners.

Strix Systems

310 N. Westlake Boulevard, Suite 150

Westlake Village

California 91362

Phone: 805.777.7911

www.strixsystems.com