ACCESS/ONE® NETWORK

Product Description

StrixSYSTEMS
NETWORKS WITHOUT WIRES®
26610 Agoura Road, Suite 110
Calabasas, California 91302
1.877.STRIXSYS (1.877.787.4979)
www.strixsystems.com

Unlike traditional access point products that individually attach to a wired network, the Access/One® Network is a fully integrated, coherent wireless LAN system that offers all of the management and security features that enterprise and service provider network managers expect. It supports multiple radio frequency technologies within an intelligent, secure and highly scalable network.

Unlike switched wireless LAN products that rely upon a wired infrastructure, Access/One Network can be installed using wireless 802.11a/g uplinks instead of the typical wired Ethernet method. This capability is especially useful where it is impractical or expensive to install cabling – indoors or outdoors. This capability is not only cost-effective, but enables you to install a network without the need for a lengthy and often complex site planning process.

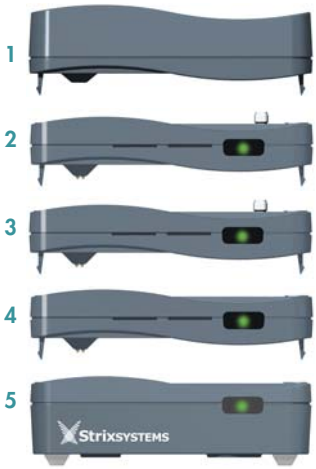
Access/One Network employs several types of hardware modules which are individually assembled to form scalable network nodes. The specific role of each node within the system is determined by its module mix. This approach ensures the flexibility to design wireless networks tailored to specific needs, eliminating redundant equipment and the unnecessary expenditure that comes with it. By reducing the need for expensive and inflexible cabling, and by providing the freedom to quickly deploy an operational system, Access/One Network offers a truly unique and versatile wireless solution.

Access/One Network provides freedom and flexibility and is operational and secure right out of the box. But it has far more to offer than mere convenience and cost savings...

Access/One Network nodes consist of compact modules with a 5.0 "x 3.65" footprint

MODULARITY AND NODE FUNCTIONS

Access/One Network nodes consist of compact modules (5.0 inches x 3.65 inches footprint) that stack atop one another with an interlocking mechanism that holds them securely together. Integrated connectors provide power and signal transfer between modules.



1 Antenna Module
2 Client Connect Wireless Module
3 Network Connect Wireless Module
4 Network Server Module
5 Base Module

Base Module

Each network nodes uses a base module that provides power via an external AC adapter and includes up to four 10/100 Ethernet ports for wired network connectivity. When present, one of the Ethernet ports supports Power-over-Ethernet (802.3af or Cisco proprietary).

Client Connect

These wireless modules provide access to client devices using 802.11a/b/g. Any mix of these modules can be supported within a single node or across the entire network. They support normal rates, Super-G and Turbo Mode.

Network Connect

These modules replace Ethernet cabling and provide the system infrastructure for node interconnectivity. By default, the wireless link utilizes AES encryption for both management and user traffic. Network nodes can support up to three client and network connect wireless modules.

Antenna Module

This module contains two 802.11a or one 802.11a and one 802.11b/g omni directional 3dBi gain antennas. Detachable external antennas can be used for increased RF gain and/or directional focus.

Network Server Module

Network server modules can be installed on any node within the network, and enable the distribution of network control logic and internal protocols. There are three network server module options; supporting two, four, and eight nodes respectively. Master/slave operation among multiple network servers reduces the amount of traffic between subnets and lowers overhead. The master network server transmits time-date packets enabling all nodes and modules to be synchronized. System software running on the server facilitates many of Access/One Network's unique features.

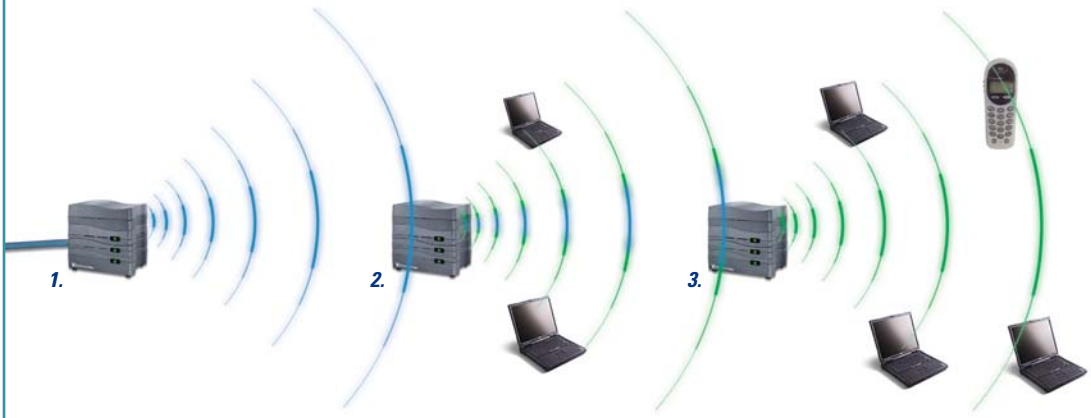
Flexible Node Functions

Node function is determined by the mix of modules within the node and its location in the network. For example, nodes at the network edge serve wireless clients and uplink traffic over wireless network connections. Other nodes act as relays of the wireless network connection, extending the reach of the wireless network beyond a single hop. These nodes can also provide client connectivity. Radio modules serve specific roles on a node, either to serve clients or to create the wireless mesh. At least one node provides conversion of the network from wireless to wired, connecting the Access/One Network to a wired LAN or Internet access device such as a DSL modem. Access/One Network can span multiple LAN segments and can include multiple wired and wireless network connections.

At least one node (1) provides conversion of the network from wireless to wired LAN or other access device.

Other nodes (2) act as relays of the wireless network connection, extending the reach of the wireless network beyond a single hop.

Nodes at the network edge (3) serve wireless clients and uplink traffic over wireless network connections, including VoIP traffic.



Future-ready

New technologies can be incorporated by design. Each module includes a 266MHz processor, with RAM and flash memory sized to accommodate present and future needs. Thus, as new radio chipsets become available, such as WiMAX or Ultra Wideband, they can be incorporated into new modules and placed into Access/One Network systems. The system software design with its multiple, linked state machines enables new technologies to benefit from the system features such as management and security.

MESH AND ADVANCED FEATURES

Access/One Network forms a mesh topology using wireless links between the nodes, creating "Networks without Wires". Each node has the ability to self-discover its neighbors. 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 as conditions change. And, because each node is constantly monitoring the system's health and inventory, Access/One Network can immediately detect the presence of rogue wireless devices operating within its range.

Although intelligence is distributed across the network, network security parameters, monitoring rules, and system upgrades can be conveniently controlled from one location. The combination of distributed intelligence and central governance fully harnesses the power of computing and networking into a single, managed system.

Self-Discovery

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.

Self-Tuning and Self-Healing

Each node automatically establishes the optimal path to its closest and least-congested Network Server (an Access/One Network module used for control signaling and data registry) and a path to the wired network via mesh links. As the wireless environment changes, such as the addition of a new node or congestion on a given link, data paths are automatically reevaluated to ensure that Access/One Network is self-tuned for peak performance, based on latency, throughput, and other measurements. If a data path is lost, or if RF interference impacts data

As the wireless environment changes, data paths are automatically reevaluated.

If a data path is lost, or if RF interference impacts data path and performance, the network self-heals by rerouting traffic so that nodes stay connected and data paths remain optimized.

path and performance, the network self-heals by rerouting traffic so that nodes stay connected and data paths remain optimized. These processes are dynamic – they occur in the background in real time and without human intervention.

Background Scanning

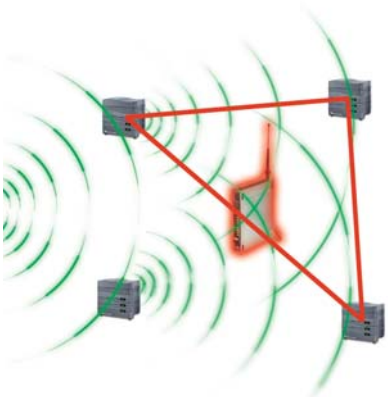
When a network module first connects, it scans all available channels and generates a list of potential client modules that are reachable. The module continuously scans in background to maintain the list and enable the system to make decisions on path selection and optimal channel selection to identify rogue access points.

Rogue Access Point Detection

A rogue access point can be a third party device that does not belong to the network, or an Access/One Network node that has yet to be admitted to the network. Network modules perform an active scan for rogues during every boot sequence and periodically thereafter. Client modules perform an active scan on command. Scans generally take between 10 and 20 seconds to complete. Detected rogue devices are immediately reported and the manager is alerted with triangulation information to locate the device.

Data Path Switching

Similar to standard Layer 3 switching, each network node learns IP information on the fly and maintains a dynamic table of known Wi-Fi clients. Each node provides a table to its associated network server, and because network servers are synchronized, data can be easily switched through the network.



Network modules perform an active scan for rogue access points during every boot sequence and periodically thereafter.

Detected rogue devices are immediately reported and the manager is alerted with triangulation information to locate the device.

"We think that this could be the wave of the future for wireless networking"

CNET Reviews

Virtual Node Capability

Access/One Network nodes support up to 32 simultaneous service set identifiers (SSIDs). Nodes can be configured to enable or suppress broadcasting the primary and/or alternate information on a per-SSID basis. Nodes also support 802.1q virtual LAN (VLAN) tagging of wireless frames based on SSID or station MAC address by assigning a specific number (0-4095) to each frame generated by a particular station. The VLAN tagging format includes a priority lever (0-7) to be assigned to the frame for processing by a VLAN-aware switch. With these features, a single node may serve multiple classes of users (tenants) and carry multiple classes of traffic (services) – each with its own configuration and level of security.

Each node may serve multiple classes of users (tenants) and carry multiple classes of traffic (services) – each with its own configuration and level of security.

Voice over WLAN

Access/One Network supports SpectraLink Voice Priority (SVP) protocol, giving a controlled preference to voice packets over data packets on an 802.11b wireless LAN. Access/One Network prioritizes SpectraLink voice traffic over user data traffic, and it selects paths based on the lowest latency, to achieve voice over WLAN performance.

High Performance Mesh

Access/One Network nodes can be deployed wirelessly using mesh, routing traffic amongst each other using an 802.11 technology. The mesh backbone can be built using any variety of 802.11, including 802.11a, b, and g, though Strix recommends using 802.11a or 802.11g in order to take advantage of the higher available throughputs. Strix builds a high performance mesh, dedicating radios for particular functionality (either send or receive), eliminating the need for a single radio to perform both functions. Strix also uses all available channels to build a mesh, selecting the least congested channel at any given time. The impact of these decisions means that the Strix mesh can achieve multiple hops from node to node without an appreciable loss in performance.

SECURITY

Wired networks depend on physical boundaries – doors, walls, conduit – while wireless networks depend on technical means to secure the network. Securing a network requires that users authenticate to the network node to validate that they are allowed access to the network. The data must then be encrypted to prevent other users from eavesdropping. Access/One Network supports IEEE 802.11i, the Wi-Fi Alliance WPA, and subordinate standards.

Authentication

Access/One Network supports both local and remote authentication. In the local mode, Access/One Network is responsible for determining whether the user device has network privileges, using mechanisms such as an access control list. With remote authentication, Access/One Network becomes a gatekeeper, blocking user access until an external RADIUS server determines the user's authorization. Access/One Network supports EAP encapsulated RADIUS exchanges, including the MD5, TLS, TTLS, and PEAP mechanisms. Access/One Network is compatible with common RADIUS servers, such as Microsoft Server 200X/IAS, Funk Odyssey, or Cisco ACS.

Encryption

Access/One Network supports WEP, including TKIP/MIC enhancements, and AES cipher suites, with either static or dynamic keys. Access/One Network nodes perform encryption in hardware to assure high performance.

Advanced System Features

Once the mesh is formed by admitting the appropriate network nodes, an access control list is created on the network server and distributed to all the participating network nodes and modules. This access control list is used for bi-directional authentication of the modules whenever they communicate with each other. Devices that are not part of the access control list are not allowed to participate in network topology building, exchanging configuration information, or managing devices. This prevents network and/or node hijacking by unauthorized users. It also prevents neighboring Access/One Network users from accidentally cross-attaching to each other's nodes.

Network-level security, on the paths between the network nodes, is an integral part of Access/One Network and requires no external resources. By default, the network connect modules utilize Advanced Encryption Standard ciphers to secure both management and user traffic over the wireless paths.

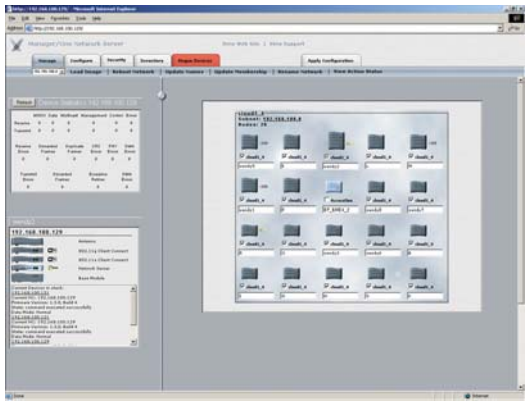
When multiple SSIDs and VLAN definitions are in use, security parameters can be configured on a per-SSID basis. The authentication types supported with the feature include Open, 802.1x (WEP), and WPA. Encryption methods include Clear, WEP, TKIP, and AES. During 802.1x authorization, VLAN information is retrieved from the RADIUS server and applied on a per-station basis.

The best security can be achieved by using remote authentication running TTLS or PEAP, combined with AES using dynamic keys and combined with the system level security features. Access/One Network can be deployed as a highly secure system, with varying levels of security applied on a per-node, per-SSID, or per-station basis as required to meet user needs.

	Minimum	Better	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		RADIUS Server	RADIUS Server, AES hardware support and AES NICs

MANAGEMENT

Manager/One is an easy-to-use graphical interface to the Access/One Network, residing on all modules within the network, and it provides the tools to configure the network to suit individual needs and to assure the network is functioning efficiently and effectively.



Functions, with their associated commands, enable the administrator to monitor and configure the Access/One Network.

Manager/One uses tabbed page design with supporting frames that contain detailed information. The frames and their content change as the administrator makes selections and drills down into the system. Icons represent elements within the network, and various color schemes denote the type, function, and active state of the component. A mouse-over feature activates color changes and pop-up windows to visually depict module-server associations and connection paths through the network.

Manage Function

This function provides tools to manage at the network, subnet, node, or module level. An administrator can view the current status of the network components, load new firmware, initiate a reboot, update node names, update network membership, or rename the network.

Configure Function

This function provides tools to configure all or any subset of the network nodes simultaneously. An administrator can establish System and Wi-Fi parameters:

System Parameters

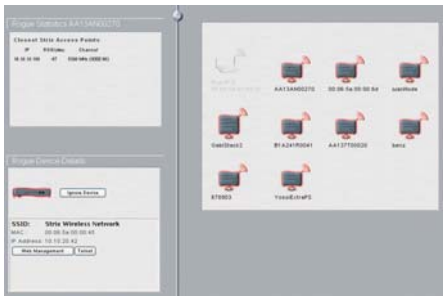
- Password
- TCP/IP
- Topology
- Date-time
- Operating environment
- Syslog
- SNMP, etc

Wi-Fi parameters

- Radio settings
- Country code
- 11a/b/g wireless mode
- SSIDs and VLAN tags
- Background scans
- Authorization
- Encryption settings

Inventory Function

This function provides a list of node names and serial numbers, device types and serial numbers, device status and IP addresses, and the current firmware version.



Rogue Device Function

This function enables on-demand rogue detection scans at the network or module level.

Apply Configuration Function

This function is used to apply configuration changes that have been made at the network or subnet level, including communication across remote subnets.

Syslog Support

Access/One Network offers comprehensive system logging functionality, including the ability to monitor Syslog events from the command line interface (CLI) via Telnet. Syslog events include end user events (add, drop, authenticate, etc.) and system events (role changes, antennas found, rogue devices, etc.). Logged events can be sent to multiple Syslog servers. Access/One Network also supports Syslog via an SNMP manager where Syslog text information is encoded in an SNMP trap message and presented to the administrator.

Access/One Network also supports Syslog via an SNMP manager where Syslog text information is encoded in an SNMP trap message and presented to the administrator.

FEATURES, FUNCTIONS, & BENEFITS SUMMARY

Mesh Networking

Function: Reduces need to run wire and simplifies network operation

Benefit: Deploys faster than traditional wired networks. Reduces costs and hassles of deployment in hard-to-wire environments. No single point of failure. Scales better and can handle thousands of connected devices.

Networks Without Wires

Function: Building networks without the need for Ethernet cable or other wire.

Benefit: All the performance, reliability, scalability and security of a wired network, with the freedom and flexibility of wireless. Reduces or avoids cabling costs. Provides rapid installation and moves. Reduces administrator efforts.

Modular Design

Function: "Snap together" modules allow for customization at the node level.

Benefit: Configure nodes to suit individual needs, including programming of multiple RF technologies, all in a single network with one management and security system. Reduces cost of ownership and provides maximum flexibility.

Standards Based Security

Function: Full range of security tools ranging including 802.1x authentication and encryption schemes up to and including AES for easy configuration.

Benefit: Reduces costs and administrative workload by using installed systems. Leverages existing RADIUS and certificate servers. No special NIC cards required. Includes full range of security tools up to and including AES.

Self-Discovery

Function: Modules automatically discover their role to serve as either client connect modules serving user traffic or network connect modules connecting the node to the network.

Benefit: Minimizes network set up time and system management. Add, move or change nodes without any changes in wiring closet, physical infrastructure or server room.

Self-Configuration

Function: Nodes configure themselves as part of the overall network.

Benefit: Minimizes network set up time and system management. Eliminates need to manually configure system. Automatically adjusts as nodes are removed or relocated within system.

Self-Tuning

Function: The system continually scans to determine if the current data paths between and amongst nodes are optimal and if RF power output needs to be dynamically modified to minimize interference with other nodes.

Benefit: Network automatically optimizes for best performance with lowest latency and best throughput, ensuring a high performance network.

Virtual Node Capability

Function: Ability to broadcast up to 32 different service set identifiers (SSIDs) and apply different security schemes per SSID. Using VLAN tagging can assign priorities per SSIDs and classes of service or quality of service.

Benefit: Users can set up multi-purpose networks and segment users to particular parts of the network. The Access/One Network can also be used as a multi-purpose network, making it appear as if multiple WLANs were installed in a given coverage area.

Manage System from a Single Point

Function: Manager/One software allows distributed management of entire system from a single point, including management of system configuration, security, inventory and rogue access point detection.

Benefit: Reduces administrative headaches and costs by eliminating need to re-wire, re-configure and re-set status at the node level. Network IT administrator can easily control and apply security policies by authenticating and encrypting from a single point and rogue access point detection prevents unwanted devices from corrupting network.

Background Scanning

Function: Scanning of environment to search for other Strix nodes. This provides system information on the RF environment for optimal channel selection.

Benefit: Monitoring of airwaves ensures that system is optimally operating and routing data through the most effective node paths. It also enables the system to make dynamic decisions on channel selection to mitigate against RF interference issues.

Upgradeability

Function: Easy to reconfigure nodes allow for simple network changes (adding new RF technologies) or network expansion (expanding coverage areas).

Benefit: No need to run additional wires. New nodes can be integrated into the network by simply placing it and turning it on. All management and security is established centrally. Adding technologies to the network, such as adding 802.11a coverage, is as simple as snapping on a new node. New technologies such as WiMAX can also be added when available.

A SUMMARY OF KEY TECHNICAL FEATURES

Basic System Features

- 802.11 a/b/g radio modules
- Turbo mode and Super G support (data rate up to 108 Mbps)
- Simultaneous support for 108Mbps Super G, 54Mbps 802.11g, and 11Mbps 802.11b
- User configurable to select all approved FCC bands or by country
- Automatic channel selection
- Radio power management (dynamic and static)
- Dual mode, dual input antenna cross polarized omni 3dBi gain
- External antenna options (and 3rd party directional, fan beam, or omni for all wireless technologies)
- Ceiling mount, wall mount, desktop, and cubicle mount
- Power over Ethernet (Cisco and 802.3af)
- Modular architecture
- High performance modules (266MHz cpu, internal Ethernet switch, RAM, flash)

Software System Features

- Wireless uplink (backhaul)
- Auto-Configuration (Self-Discovery)
- Active Self-Tuning with configurable Background Scanning
- Self-Healing (automatic failover)
- Communication across subnets
- Load balancing
- Data path switching (client Layer 3 IP switching)
- Fast bring-up capability
- Multiple SSIDs per node with VLAN tagging
- Broadcast of alternate/multiple SSIDs per AP
- Configurable security levels per SSID
- Automated VLAN application on per-station basis upon authentication
- Rogue AP detection & signal triangulation
- Automated site planning

Security Features

- Access control
- Authentication – 802.1x EAP (MD-5, TLS, TTLS, PEAP), WPA
- Encryption – WEP, TKIP, AES
- AES encryption on internodal links
- Hardware-based TKIP and AES for performance

Voice Support Features

- Voice over WLAN support (low latency, priority on network paths)
- SpectraLink voice support

Network Management Features

- Secure browser-based management interface
- Telnet command line and scripting support; SNMP
- Firmware/software upgrades
- Software configuration & reboot facility
- Remote configuration support
- Rapid network discovery & automatic IP address identification
- Function tabs with associated commands and pull-down menus
- Graphic display of network, subnets, nodes, and active links
- Performance monitor frame
- Module monitor frame
- Intuitive mouse-overs with icon-based navigation
- Event Monitoring – end user events, system events
- Syslog with SNMP trap generation

To learn more about us, or to purchase the Access/One Network, contact your Strix Systems' reseller. You may also visit us at www.strixsystems.com or phone our toll free number: **1.877.STRIXSYS (1.877.787.4979)**.

NETWORKS WITHOUT WIRES®

Strix Systems
26610 Agoura Road, Suite 110
Calabasas, California 91302

1.877.STRIXSYS (1.877.787.4979)
1.818.251.1000 (outside the U.S.)

www.strixsystems.com