IWS

DATA SHEET

Why Choose the Access/One Network IWS?

Mesh Topology

- Mesh topology is the next evolutionary step in networking, moving beyond Wireless LAN switches and access points.
- Self-configuring, self-healing, self-tuning for automatic operation.
- Drops seamlessly into Cisco and Microsoft environments.

Differentiates Itself

- Manager/One® Web interface provides a full suite of intuitive management tools at the network, node, and radio levels.
- Supports all industry standard security protocols.
- Virtual/Strix and Priority/One support deployments of mixed use networks where varying security schemes are implemented based on user type.

Grows Proportionately

- Not dependent on a central control point, and scales much more effectively than typical solutions.
- Provides a reliable redundant system, extendable over thousands of square feet.
- Modular design makes Access/One Network IWS highly scalable.

Simplifies Installation

- Installs in hours, not weeks.
- Achieves reliable communications without complicated planning and site mapping.
- Weak or dead zones are easily corrected by simply moving a network node or dropping another node into place.

www.strixsystems.com

Network Server

Adds system-level protection against attackers and rogue access points

AES encrypts all wireless mesh links and network management and control data. Once a user is authenticated, the Network Server maintains user security while they roam the network.

Overseeing management and control of the wireless environment, the Network Server provides distributed functionality that enables the Access/One® Network IWS (Indoor Wireless System) to function as a secure system that scales as the Enterprise network grows. The Network Server offers the following key features:

- Advanced Security—standards-based and enhanced (system-wide).
- Dynamic Operation—self-configuring, self-tuning and self-healing.
- Network Management—configuring, monitoring and diagnostics.
- Traffic Prioritization and Control—switching and routing, for enhanced user mobility and tracking.

The Network Server enables Access/One Network IWS to provide a full array of standards-based tools to secure the wireless network. Using the same security servers and virtual private network (VPN) software that is used on the wired network, Access/One Network IWS adds system-level security for increased protection against attackers and rogue access points.

During the self-configuration process, each network node is automatically associated to one Network Server on the network. This association establishes the path used by management and control data as it moves through the network. Other traffic is routed to its destination based on the best available path. With any changes in the wireless environment (for example, adding a node), data paths are automatically re-evaluated to ensure that the network is always tuned for optimal performance. Similarly, if a connection is lost the Network Server automatically finds the best alternative path, keeping the Access/One Network IWS up and running—a fully self-healing system.

The Network Server and the Manager/One Web management interface work together to build node-level and module-level maps of the network, enabling nodes to be configured individually or as a group. In fact, every node in the Access/One Network IWS can be configured concurrently with a single click of the mouse from the Manager/One screen.

Strix Systems, Inc.
26610 Agoura Road,
Calabasas, CA 91302
USA

1-877-STRIXSYS (787-4979) Toll Free

StrixSYSTEMS
Networks Without Wires®

Access/One Network IWS user traffic is managed locally at the network node and system-wide by the Network Server. The Network Server generates internal tables that contain a list of users who are attached to each node. This list facilitates the prioritization and routing of user traffic through the network. By managing all user data this way, including broadcast and multicast traffic, the overhead on the network is reduced significantly.

Technical Specifications

Network Server Unit

- Network Architecture Type:
  Infrastructure, mesh, auto-discovery, self-healing
- Remote Configuration Support:
  BOOTP, DHCP, Telnet, HTTP, FTP, TFTP and SNMP
- SNMP Compliance:
  MIB I, MIB II, 802.11 MIB, Strix MIB
- Status LEDs:
  Single multi-state LED: green, orange, red
- Network Connect:
  Auto sensing 802.3 10/100 Ethernet via the Base Module or IEEE 802.11a / 802.11g
- Integrated Power over Ethernet Support:
  802.3af and Cisco proprietary (Base Module); 13 Watts maximum
- Input Power Requirements:
  Base Module - 90 to 265 VAC 47 to 63 KHz (power supply); 18 Watts maximum
- Dimensions: 5.0 x 3.65 x 0.60 in
- Environmental:
  32° to 104° F (0° to 40° C)10 to 90% humidity (non-condensing)
- MTBF: 150,000 hours

Security

- Authentication: 802.1x support, including RADIUS client, EAP-MD5, EAP-TLS, and PEAP-TTLS, WPA
- Encryption: IEEE 802.11i (WPA2) with AES, and WEP

Compliance (802.11a/b/g)

- Emissions:
  EN 55022:1998 + A1:2000, FCC Part 15, ICES-003, VCCI, AS/NZS, CNS 13438, CE Mark
- Immunity:
  EN 55024:1998 + A1:2001, CE Mark
- Product Safety:
  IEC 60950:1999 / EN 60950:2000, UL 60950, CSA 22.2 No. 60950-00, CE Mark
- Health (Radiation Hazard):
  RSS-102, FCC Bulletin OET-65C

The Network Server is a critical component in the Access/One Network IWS. It consists of a hardware platform and base software, plus additional optional software modules. The hardware is an Access/One Network IWS module and can be installed into any network node within the system. The software running on this module provides much of the intelligence within the system and facilitates most of the unique features and functions of the Access/One Network IWS.

The Network Server enables you to install, manage and maintain an Enterprise-class wireless network with minimal effort, while maintaining corporate LAN security that cannot be compromised. Multiple Network Servers can be distributed throughout the network to protect against a single point-of-failure and improve network performance.

Module Configurations

Dual Function Network Node with System Server

To add server functionality anywhere in the network, place a Network Server Module into any of the permissible network node configurations.

Module Placement Rule

The Network Server Module is always placed immediately above the Base Module.

Base Modules

The Network Server Module may be used with any of the following Base Modules:

BME0 – No Ethernet ports; used with 802.11a wireless network connect configurations.

BME1 – One Ethernet port; used for wired network connect or to attach to the wired LAN.

BME4 – Four switched Ethernet ports for added flexibility.

Access/One® Network IWS increases mobile worker productivity by providing a continuous and secure connection to company networks in Ethernet-free environments.

Networks Without Wires®