WS 2000 Wireless Switch

symbol®
The Enterprise Mobility Company™

Wireless Switch System

INTEGRATED WIRED AND WIRELESS LAN

Integrated Wired and Wireless Networking for

Branch Office and Small/Medium Enterprises

The WS 2000 Wireless Switch from Symbol Technologies is an integrated wired and wireless networking solution, priced and designed to meet the needs of healthcare clinics, schools and colleges to warehouses, branch offices of government agencies, retail stores, manufacturing plants and more. Built on the same centralized packet switching architecture as Symbol's award-winning WS 5000 Wireless Switch, the WS 2000 offers enterprise class security (802.11i, site-to-site IPSec VPN), public/private network segmentation and 802.11abg standards support and provides:

- Extensive wireless LAN functionality and high performance
- Power and simplicity of centralized remote management
- Ability to scale to support future growth

…Investment protection and network simplicity.

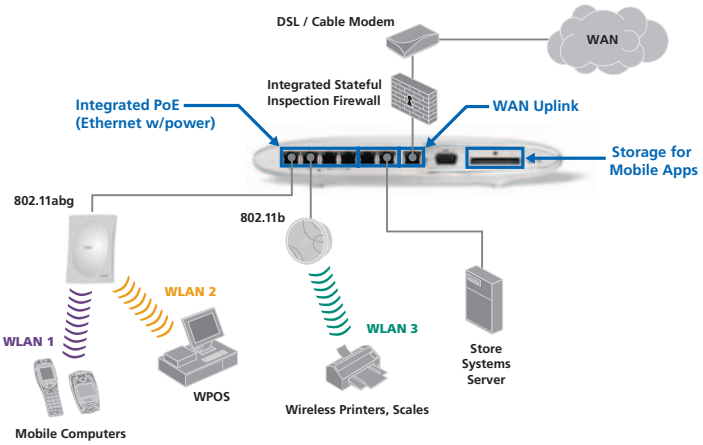
All-in-One Integrated Wired and Wireless Networking

The need to purchase and manage additional network equipment is eliminated with the elegant all-in-one design of the WS 2000. Support for multiple wireless LAN protocols (Wi-Fi® IEEE 802.11b, 802.11a, 802.11g), as well as integrated Ethernet switching (6 LAN ports), routing (RIP, Static Routes), Gateway and Power-over-Ethernet (PoE) simplifies network deployment and management, and reduces capital expense. Functionality includes an integrated Stateful Packet Inspection Firewall, Network Address Translation (NAT), DHCP server (on multiple subnets), and WAN connectivity support for flexible low cost installation.

Second-Generation Wireless LAN: the Power of Centralized Intelligence

The WS 2000 offers the power and cost-efficiencies of second-generation wireless networking. Intelligence previously distributed and duplicated throughout first-generation access point-based wireless LANs is centralized and aggregated in the WS 2000 Wireless Switch, delivering unprecedented power and control, and reduced deployment and management costs. Instead of traditional access points, the WS 2000 works in conjunction with low-cost Access Ports, which are essentially 'zero configuration' devices, operational right out of the box, and can be mounted almost anywhere—even inside ceiling tiles.

Integrated Wired-Wireless Networking: WS 2000 in a Retail Wireless Store



End-to-end layered security

WS 2000 supports a comprehensive suite of security mechanisms—including access-control, IPSec VPN (site-to-site), 802.1X based authentication, and strong encryption. In addition, the WS 2000 also integrates a Stateful Packet Inspection Firewall for protection against various types of Denial-of-Service attacks and filtering network traffic within the Local Area Network (LAN) and between the LAN and the Wide Area Network (WAN). The result is a layered security model that delivers robust end-to-end security. The WS 2000 supports the best-in-class wireless security standards of today (including 802.11i), and is easily upgradeable to tomorrow's standards.

Centralized management

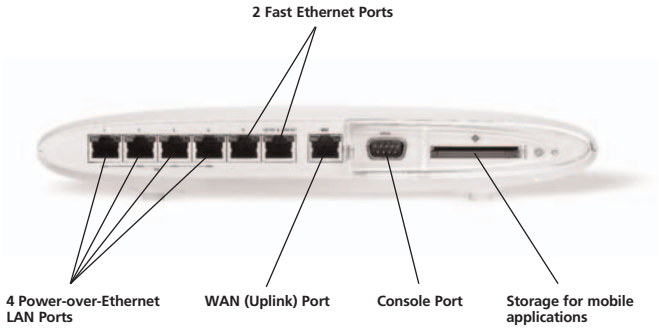
The WS 2000 simplifies day-to-day operations with unified management of hardware, software configuration, and network policies. Centralized management also enables the automatic distribution of configurations to all Access Ports—eliminating the need and the associated costs to configure and manage each access point. The WS 2000 also simplifies wireless network deployment across multiple locations (for example, multiple retail stores, restaurants or branch offices), delivering network design consistency and simplicity, as well as the ability to centrally manage from a regional Network Operations Center (NOC) or a data center.

Scalable and easy to upgrade

The WS 2000 Wireless Switch System is designed to grow and adapt to changing network and organizational needs. Adding capacity and new functionality is easier and less expensive than an access point-based wireless LAN. Each WS 2000 supports up to six Access Ports and four wireless LANs, each with its own security and network policies. The plug-and-play Access Ports are ready to install right out of the box. Just attach directly to the WS 2000 or to your layer 2 LAN with Power-over-Ethernet and the network is immediately operational—LAN network integration is transparent. And upgrading to support newer standards in the future is fast and easy.

Lower total cost of ownership—outstanding investment protection

The WS 2000 removes the overhead and complexity of first-generation access point-based wireless LANs, delivering a wireless network that is less expensive to implement and manage. The extensive functionality, expandability, and centralized management eliminate the time and management costs associated with access point-based solutions, providing a lower total cost of ownership. And the flexibility to support the standards of today and tomorrow, as well as the legacy wireless networks of yesterday, protects this valuable investment.



The WS 2000 offers integrated functionality including PoE and a CF Card Slot for additional application support.

Flexible mounting options: The WS 2000 can be mounted on the desk, wall or rack. The standard 1RU form factor enables easy mounting in any standard network rack for co-location with other network equipment.

Extensive WLAN Functionality

The comprehensive feature set of the WS 2000 provides full control over wireless LAN traffic to provide peak performance. Extensive wireless LAN functionality enables you to maximize bandwidth and throughput, secure network traffic, prioritize voice traffic, conserve power on mobile devices, and provide dependable connection speeds for users in challenging wireless environments.

Scalable Radio Architecture

Each WS 2000 supports up to six single or dual-band Access Port radios (802.11b and 802.11abg) in the 2.4 and 5 GHz frequencies—offering the broadest radio technology support in the industry. The WS 2000 supports a total of four wireless LANs.

Access Ports: Next-Generation Wireless Access Devices

Access Ports bring a new level of simplicity to wireless network implementation and management, as well as an unprecedented upgrade capability. Access Ports are easily upgraded with new features and functionality via the WS 2000, providing excellent investment protection. A wide range of 802.11a, 802.11b and 802.11g external antenna options enables the design of coverage patterns for the most challenging environments. Each Access Port/radio supports up to four wireless LANs.

The Access Port AP300 supports simultaneous 802.11bg and 802.11a operations and aids in high bandwidth applications. Support for Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) is included with the AP300 for regulatory compliance and radar detection and avoidance. Both the 802.11bg and 802.11a radios support four BSSIDs (which are mapped to four ESSIDs).

Voice Prioritization

The WS 2000 provides voice prioritization capabilities for devices such as VoIP phones, guaranteeing priority for voice traffic during periods of network congestion.

Power Saving for Client Devices

The Power Save Protocol (PSP) polling feature enables devices to maximize battery life and maintain application performance. The implementation allows devices to conserve power between wireless transmissions and also ensures that packets are stored and reliably delivered when the device awakens.

Virtual AP Enables True Virtual Wireless LANS

Virtual AP enables the wireless LAN to be segmented into true multiple broadcast domains—the wireless equivalent of Ethernet VLANs—providing the ability to map multiple ESSIDs (Extended Service Set Identifiers) to multiple BSSIDs (Basic Service Set Identifiers).

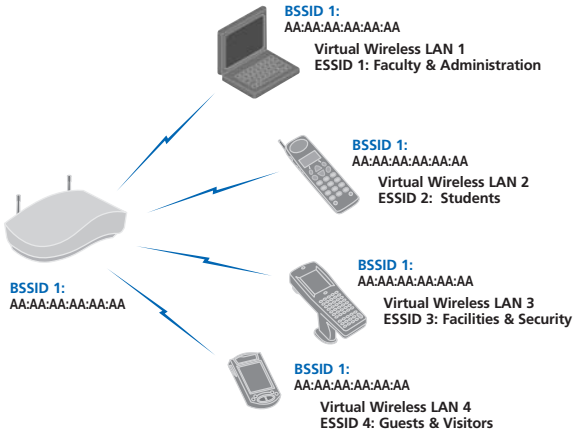
Virtual AP provides complete control over broadcast traffic. Control of broadcast traffic, including network level messages, is extremely important because of its potential negative effect on performance. Intelligent control of broadcast forwarding through proxy ARP and other mechanisms ensures that only the intended recipients receive broadcast traffic. The resulting reduction in traffic maximizes bandwidth and network throughput; device battery life and overall performance are improved with the elimination of the processing of messages intended for other recipients; and the possible compromise in confidentiality and security of messages is eliminated since broadcast messages can no longer reach the wrong recipients.

Load Balancing and Pre-emptive Roaming

Normal roaming does not occur until the device connection has reached a minimum connection speed of 1 Mbps—normally well beyond the boundaries of a cell and approximately halfway through an adjacent cell. Two features, client load balancing and pre-emptive roaming, work hand-in-hand to ensure that devices roam before the connection quality erodes, providing users with more consistent connection speeds for smooth application performance. The WS 2000 provides the information needed for roaming decisions, ensuring that critical wireless connections—such as real-time voice and data connections—are maintained.

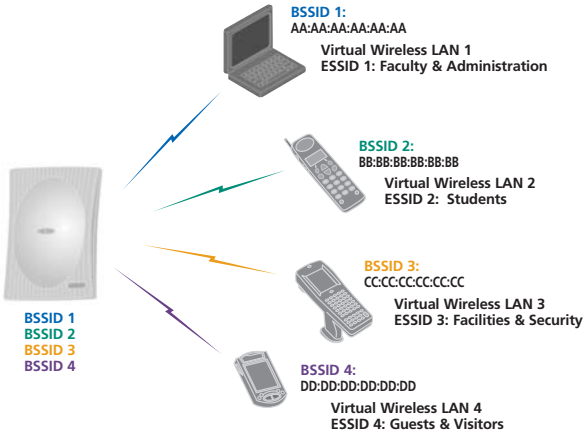
Virtual AP Enables True Virtual LANs

Access Point VLAN Architecture: Single BSSID VLAN
Performance and Security Issues



In a typical access point architecture, VLANs are defined using multiple ESSIDs. Since access points support only one BSSID, broadcast traffic intended only for Faculty and Administration (ESSID1) will be sent to all VLANs—Students (ESSID2), Facilities and Security (ESSID3) and Guests and Visitors (ESSID4). The resulting processing of unnecessary messages reduces battery life and network throughput, and delivery of messages to unintended recipients presents security and confidentiality issues.

Access Port VLAN Architecture: Multiple BSSID VLAN
Improved Performance and Security



Virtual AP provides support for multiple BSSIDs, enabling the creation of true wireless VLANs. Broadcast traffic is sent only to recipients within a specific wireless VLAN (ESSID), improving overall battery life of client devices and network throughput, and ensuring security and confidentiality for broadcast traffic.

Transmit Power Control

Transmit Power Control minimizes radio interference for sites that require a very dense population of radios (Access Ports) to support bandwidth requirements. The transmit power along with antenna gain can be set on all supported Access Ports.

Multicast Masking

This feature enables multicast traffic to be sent to intended clients without any queuing, providing essential support for push-to-talk and other multimedia applications.

Proxy ARP

Proxy ARP enables the WS 2000 to respond to ARP requests on behalf of a mobile client, acting as the client's agent or Proxy. No longer burdened with the processing of ARP requests, the mobile client can temporarily suspend the WLAN adapter. The result is substantial savings of battery power on the client device, while preserving the integrity of the IP connection.

Storage of Software Update Packages for Client Devices

With the WS 2000 and AirBEAM Smart, managing and updating software on Symbol mobile devices is fast, easy—and automatic. The WS 2000 acts as an FTP server, storing software updates via a CompactFlash™ card. AirBEAM® Smart, Symbol's software management program resident on Symbol mobile devices, accesses the WS 2000 to automatically download and install everything from new or updated wireless applications and drivers to operating systems on boot up.

End-to-End Layered Security

There is no element of networking—wired or wireless—more important than security. The WS 2000 offers an integrated firewall as well as a complete end-to-end layered security model that supports all of today's wireless security standards, and is easily upgradeable to support the standards of tomorrow. Users can configure security policies that specify the correct level of control for users, applications, and devices within those groups.

Network Access Control

Access Control Lists (ACLs)

Layer 2 Access Control Lists provide filtering for advanced network traffic control, enabling administrators to forward or drop packets based on protocol type or MAC Addresses.

Stateful Packet Inspection Firewall

Firewalls prevent unauthorized access to and from a private network by inspecting data packets that leave and enter the network, blocking data packets that do not meet certain criteria. In addition, firewalls prevent various types of Denial-of-Service attacks initiated both internally and externally.

The integrated firewall in the WS 2000 is always enabled on the WAN interface by default, providing instant protection against intruders and a wide variety of attacks. The Stateful Packet Inspection Firewall offers advanced packet inspection and filtering—much stronger protection than standard simple packet inspection engines. "Stateful inspection" keeps track of information in the packet header, such as Sequence numbers, source/destination IP address, source/destination port numbers, as well as the state of all TCP sessions passing through the firewall. The firewall checks for compatibility between the header of the responding packets (TCP Acks) and the associated session information in the inspection table. If the information does not match, the packet is dropped.

The default Firewall settings also protect against the following types of attacks:

- IP Spoofing
- Ping of Death
- Land Attacks
- IP Reassembly attacks

Configurable filters guard against other types of attacks including Syn Flooding, Source Routing, Winnuke, FTP Bounce, Sequence Number Prediction, IP Unaligned Timestamp, and Mime Flood Attack. Defense against a total of more than 50 types of attacks is provided by WS 2000.

Between each of the available subnets, the WS 2000 also provides filtering capabilities based on protocol, port and IP source and destination addresses.

802.1x/Extensible Authentication Protocol (EAP)

802.1x and Extensible Authentication Protocol (EAP) work hand-in-hand, providing the infrastructure for robust authentication and dynamic key rotation and distribution. EAP provides a means for mutual authentication. Authorized users identify themselves to the wireless network, and the wireless network identifies itself to the user—ensuring that unauthorized users cannot access your network, and authorized users do not inadvertently join a rogue network. A wide variety of authentication types can be used—from user name and password to voice signatures, public keys, and biometrics, with the ability to upgrade to support future authentication types. And dynamic key rotation and distribution provides a new encryption key per user per session, greatly increasing the strength of the chosen encryption algorithm (WEP, AES or TKIP) used to encode data. The WS 2000 supports a variety of EAP methods, including TLS, TTLS, PEAP and SIM.

Kerberos

The industry-standard Kerberos protocol meets all of the requirements for scalable, effective security in a mobile environment. Kerberos features mutual authentication and end-to-end encryption. All traffic is encrypted and security keys are generated on a per-client basis, keys are never shared or reused, and are automatically distributed in a secure manner. WS 2000 requires an external Key Distribution Center (KDC), such as a Windows® 2000 server.

Encryption

Encryption ensures that data privacy is maintained while in transmission. As a common rule, the stronger the encryption, the more complex and expensive it is to implement and manage. The WS 2000 supports a range of encryption options (including AES and 3DES that support wireless networking, SNMP access and site-to-site VPN) that provide basic to strong encryption techniques, providing the flexibility to select the right level for your data.

Wired Equivalent Privacy (WEP)
The 802.11 Wired Equivalent Privacy (WEP) provides static key encryption—a single key is distributed to all users for encryption and decryption of data. WEP generates either a 40- or 128-bit key using the widely used RC-4 encryption algorithm. WEP allows full interoperability with legacy clients and provides basic over-the-air security in less-critical environments, such as an open public-access application.

WPA—Temporal Key Integrity Protocol (TKIP)
WPA-TKIP addresses well-known vulnerabilities in WEP encryption. TKIP provides key rotation on a per-packet basis along with Michael message integrity check (MIC), which determines if data has been tampered or corrupted while in transit. This robust method of encryption provides a higher level of protection for your data and protects your network from a variety of types of attacks.

WPA2 (AES/CCMP)
WPA relies on RC4 and TKIP. In order to completely eliminate the WEP related flaws, IEEE recently ratified a new security standard, 802.11i (termed WPA2 by the Wi-Fi Alliance). WPA2 specifies the use of stronger cipher systems such as AES (Advanced Encryption Standard) and a security protocol called CCMP (Counter Mode CBC MAC Protocol). CCMP uses AES for encryption and a well-proven method called CBC-MAC (Cipher Block Chaining Message Authentication Code) to compute the message integrity check (MIC) (for data integrity checks). CCMP in a sense is the equivalent of TKIP used in the original WPA but much stronger.

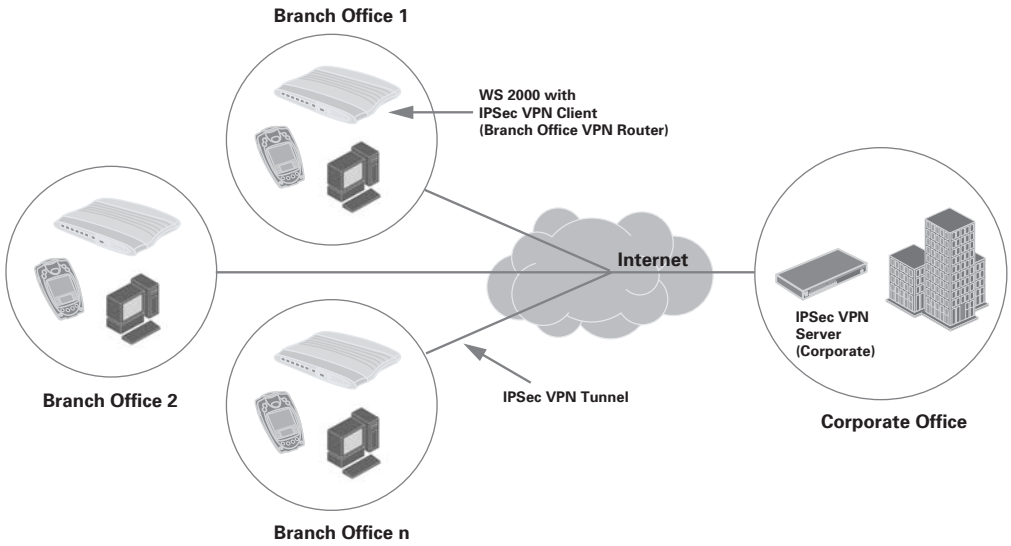
As part of the WPA2 implementation, support for PMK (Pairwise Master Key) Caching, Pre-Authentication, and "Opportunistic" PMK Caching is available, enabling fast roaming of mobile clients between Access Ports. These mechanisms basically act by foregoing either the 802.1X part of the authentication or the 4-way handshake associated with CCMP message exchanges between the client and the Access Port.

KeyGuard™—MCM
Similar to WECA's version of TKIP, KeyGuard provides a different key for every packet of data, but uses a different version of message integrity check (MIC) to determine if data has been tampered or corrupted during transmission. KeyGuard was developed by Symbol prior to WPA. It is supported on Symbol mobile clients and due to its small footprint, has the advantage of being supported even in older DOS based devices.

IPSec VPN (Site-to-Site)
Virtual Private Networking (VPN) provides a cost-effective, secure solution for businesses to take advantage of the public Internet instead of dedicated leased WAN links to transmit information between remote branch offices (Intranet) or with external customers/partners (Extranet).

The WS 2000 supports IPSec (Internet Protocol Security) based VPN for securing communication between a WS 2000 in a branch location and another VPN Gateway at the main office. The implementation in WS 2000 includes a complete IPSec engine, IKE engine, DES/3DES/AES encryption and NAT Traversal support.

Site-to-Site VPN Diagram



Wired Networking Services

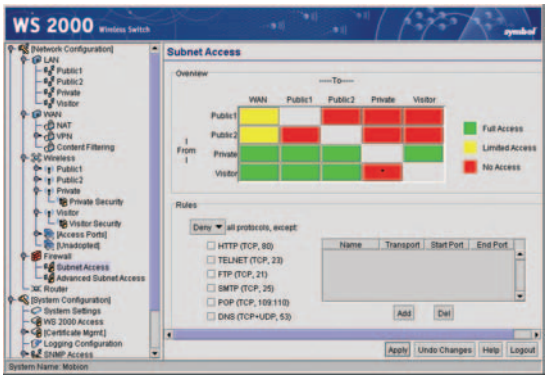
In addition to wireless network connectivity, data switching capabilities are also provided for wired devices (such as Store Servers, wired Point-of-Sales Systems, wired printers, etc.) that are connected to any of the six Ethernet ports on the WS 2000.

Virtual LANs

Up to four independent subnets (broadcast domains) can be configured in the WS 2000. The six physical ports and four wireless LANs are mapped to one of the four subnets. Separate IP addressing and outbound network policies (filtering traffic based on Protocol type and Port ranges, IP Source and Destination addresses or completely blocking traffic between subnets and the WAN) can be applied on a per subnet basis. This provides a great deal of flexibility in segmenting and securing the network.

Routing

The WS 2000 supports Layer 3 services. It supports Routing Information Protocol (RIP) v1 and v2. The primary benefits of RIP are ease of configuration and suitability for small networks (less than 15 hops). If RIP is enabled on any of the four private interfaces, RIP broadcasts are periodically sent over that interface, and the routing table is also updated based on the broadcast received on that interface from other connected routers. Static routes can be configured for each IP interface on the private side as well.



With the WS 2000, it is easy to segment the network based on user profiles. Subnet access rules define what type of traffic can or cannot flow through between the subnets and between the subnet and WAN.

Integrated Gateway

The WS 2000 integrates gateway functionality for ease of provisioning network services—Network Address Translation (NAT), DHCP Server, Firewall—for SMBs.

DHCP Client and Server

The WS 2000 offers integrated DHCP services for all four of its subnets. The need to purchase, manage and maintain additional network equipment to obtain this functionality is eliminated–saving capital as well as operational expenses.

Each of the four private interfaces (Subnets 1-4) can be configured as a static IP address or either as a DHCP (Dynamic Host Configuration Protocol) client or a DHCP server. The WAN interface can have a static IP address or be configured to be a DHCP client.

If the interface is configured to be a DHCP client, the IP address is obtained from an external DHCP server. If the interface is configured to be a DHCP server, the WS 2000 serves (leases) IP addresses to connected clients (wired or wireless). The scope of IP addresses (the range) is configurable per subnet. The clients also receive DNS configuration and default route information from the DHCP server on the WS 2000.

The advanced DHCP configuration allows for specification of lease time, WINS Server and static IP mappings (mapping individual MAC addresses to specific IP addresses).

Network Address Translation (NAT) with Application Layer Gateway (ALG)
With NAT, the IP addresses of client devices in the internal network are invisible to the external world. Identity is protected, while the client devices connect to the Internet through the WS 2000 as if directly on the Internet. The WS 2000 supports three different NAT configurations:

- *One-to-One*—A pool of available public IP address can be used to map to an individual (internal) client IP address. One-to-one NAT translates the IP address on behalf of the client.

- *Many-to-One*—The IP addresses for a group of mobile clients in the internal network can be mapped to a group with a single public IP address. The WS 2000 allows the range of IP addresses in each of the three subnets to be mapped to the same (or different) public IP address.

- *Port Forwarding*—This inbound network policy allows communication from the public network to a computer on the internal network via a specified port. Essentially, this allows the creation of a tunnel through the firewall, between the computer on the LAN and the Internet. This is useful, for example, to run a Web Server (Port 80) or FTP Server (Port 23) using a single IP address. The WS 2000 also allows the port translation and forwarding of all unspecified ports to a specific IP address on the internal network.

Application Layer Gateways (ALGs) enable applications that embed addressing information in the payload (such as FTP, Quicktime, Real Networks, Net2Phone and Netmeeting), and protocols (such as PPTP, L2TP, IKE and IPSec) to work when NAT is enabled. ALGs for over 40 different applications and protocols are supported.

WAN Connectivity
The integrated uplink 10/100 Ethernet Port enables the WS 2000 to connect to a WAN access device (such as a DSL or Cable modem, or Frame Relay Access Device), enabling client devices to share Internet connectivity.

In addition, the WS 2000 provides support for industry-standard PPP (Point-to-point) and PPPoE (PPP over Ethernet) protocols. The PPPoE protocol enables multiple LAN users to connect to the Internet through a single DSL modem.

Ease of Management

The WS 2000 is easy to configure, and even easier to manage. The configuration of any WS 2000 can be easily replicated for fast and simple deployment of additional WS 2000 Wireless Switches. The configuration file can be exported to a text file and directly imported into the WS 2000, or published to a remote FTP or TFTP server that is accessible to your WS 2000 Wireless Switches. Firmware can be easily updated as well, either via FTP or TFTP servers.

Support for different interfaces is provided to ensure a maximum flexibility in configuring and managing the WS 2000:

- *Command Line Interface (CLI)*—Designed with well-known industry semantics and provides complete baseline management through the Telnet or Serial interfaces.

- *Web-based Management*—Provides anytime-anywhere management with an intuitive, web-based (Java) GUI that supports step-by-step, easy configuration of all the system features.

- *Simple Network Management Protocol (SNMP)*—The SNMP implementation in the WS 2000 provides support for commands for updating configuration and firmware files and allows for remote monitoring of system health and key RF parameters. Supported MIBs include:

  - MIB II (RFC 1213)
  - Ping and Traceroute MIB (RFC 2925)
  - Symbol MIB (802.11 related)

The WS 2000 provides several key RF statistics that help in real-time monitoring of the network health. These statistics (such as throughput, percentage of retries, average signal strength and SNRs on per MU, Access Port, and Switch basis) are updated frequently and available via all supported interfaces (CLI, Web, SNMP). Key system traps are also supported. Traps can be configured when any of the key system performance parameters fall outside the user configured bounds. The traps can be forwarded to any enterprise management system and provide early notification of network problems related to Access Port adoption, Mobile Unit association and system resets.

Features	Benefits
Switch-based architecture	Delivers unparalleled functionality, performance, simplicity of implementation and management via centralized intelligence; lowers overall cost of ownership; provides investment protection.
802.11a+bg and dual mode support	Works with Symbol's next-generation thin Access Ports (AP 100/802.11b and AP 300/Dual mode 802.11a+bg), delivering more functionality at much lower costs; centralized management for all Access Ports includes automatic distribution of the latest firmware, eliminating the need to configure, load and manage first-generation access points.
Scalability	Supports up to six Access Ports (802.11b or dual mode 802.11a+bg); offers the broadest and most flexible radio technology support in the industry; ability to accommodate new coverage, radio types, channels and spectrum; ensures maximum flexibility in wireless network design; enables fast, easy and cost-effective expansion to meet growing company needs; delivers outstanding investment protection by eliminating costly rip-and-replace upgrades often required to implement new standards.
Power-over-Ethernet (PoE)	Simplifies and reduces total cost of installation; integrated 802.3af compliant Power-over-Ethernet (PoE) on 4 of the 6 LAN ports enables Access Ports (or any device supporting PoE such as a VoIP phone) to be directly connected to the WS 2000 without installing costly power lines and outlets.
Wired networking services	Eliminates need for additional equipment (i.e. Hubs or Switches) through integrated wired networking services including Switching and Routing (RIP v1, v2); supports up to 4 subnets (independent broadcast domains) with configurable access rules between subnets and between subnets and WAN.
Integrated gateway	Provides a self contained, one box network solution for SMBs and branch offices with NAT (1-1, 1-Many, Port Forwarding), DHCP (on all 4 subnets), Stateful Inspection Firewall, Support for WAN Protocol (PPPoE); eliminates need for separate DHCP server and NAT router/appliance – saving additional costs; offers better network protection at the edge by preventing various types of Denial of Service (DoS) attacks through the Stateful Inspection Firewall.
Mobility-centric Wireless LAN features	Provides core mobility features for reduced operational expenses; features such as Virtual APs, Power Save Polling Protocol, Load Balancing and Preemptive Roaming, Voice Prioritization, Automatic Channel Selection, and Transmit Power Control deliver tremendous cost benefits and productivity enhancements, including increased performance of mobile devices attached to the network (throughput, bandwidth management, minimized interference, increased battery life), better network security and easier deployment.
Enterprise class security	Provides the flexibility to select from a complete security suite of authentication and encryption mechanisms for a highly secure wireless network environment; switch architecture provides an easy upgrade path to integrate future security standards providing additional investment protection; authentication and Encryption on a per WLAN basis includes 802.1X/EAP, Kerberos, WPA-TKIP, WPA2 (802.11i) and KeyGuard™-MCM; AES-CCMP is available as an encryption option on a per WLAN basis; as part of 802.11i implementation, WS 2000 supports various mechanisms to enable fast roaming and handoff including: PMK ("Pairwise Master Key") Caching, Pre-Authentication, "Opportunistic PMK Caching".
IPSec VPN (for site-to-site security)	Low cost, secure, site-to-site communication through a secure tunnel between a WS 2000 installed in a branch office and a VPN Gateway at the Corporate office (or another WS 2000); precludes the need for installing costly, standalone VPN appliances; supports up to 25 simultaneous tunnels and provides industry standard encryption and authentication mechanisms including 3DES and Public Key Infrastructure (PKI).
Ease of configuration and management	Reduces deployment and maintenance costs; provides multiple management interfaces for configuration; mechanisms for fast, easy configuration replication across distributed locations; remote access to update and monitoring capabilities for system administrators and broad SNMP capabilities.
Enhanced RF statistics	More robust statistics improve the visibility, management and monitoring of the wireless system—including per Mobile Unit, Wireless LAN and individual Switch; statistics are available through the management console and SNMP, including Packets per second, Data Packets and bytes per second, Mgmt packets and bytes per second (both receive and transmit),% Retries and Retries per second, System packets per second and total Wired LAN packet per second.
Storage of mobile application (software management of mobile clients)	Allows for easier device software management at the local site; software update packages can be stored on a CF memory card which can be inserted into the WS 2000. mobile devices equipped with AirBeam Smart clients can then easily and automatically download the updates—from applications to Operating Systems—when the WS 2000 is booted.

WS 2000 Specification Highlights

Packet Forwarding

802.1D-1999 Ethernet Bridging
802.11-.802.3 Bridging

Wireless Networking

Wireless LAN:	Supports 4 WLANs Virtual AP: Multi-ESS/BSSID traffic segmentation (Virtual AP support) Pre-emptive Roaming Load Balancing Proxy ARP
Access Port Radios:	Supports 1-6 Access Ports Automatic Access Port Adoption with ACLs Access Port Load Balancing
Radio & Frequency Management:	Automatic Channel Select (ACS) Transmit Power Control (TPC) Country Code based RF Configuration 802.11b – 3 Non-overlapping channels 802.11a – 11 Non-overlapping channels 802.11g - 3 Non-overlapping channels

Network Security

Packet Filtering:	L2/3/4 Stateful Packet Analysis Network Address Translation (NAT)
Authentication Mechanisms:	Access Control Lists (ACLS) Pre-Shared Keys (PSK) 802.1x/EAP Transport Layer Security (TLS) Tunneled Transport Layer Security (TTLS) Protected EAP (PEAP) Kerberos
Transport Encryption:	WEP 40/128 (RC4), KeyGuard, WPA—TKIP, AES-CCMP
Key Exchange and Management:	Extensible Authentication Protocol (EAP) Kerberos

Optimized Wireless QoS

Voice Prioritization
Power Save Protocol (PSP) integration

Management

Command Line Interface (Serial, Telnet)
Java Applet (HTTP, Secure HTTP)
Syslog
Text-Based Configuration Files
Remote configuration and firmware update (via TFTP, FTP)
SNMP v1/v2/v3
MIBs: MIB-II, Ping MIB, TraceRoute MIB, Symbol MIB

Physical Characteristics

Form Factor:	Standard 1RU
Dimensions:	1.75 in. H x 11.25 in. W x 8 in. D 44.5 mm H x 286 mm W x 203 mm D
Weight:	1.41 lb/0.64 kg
Physical Interfaces:	1 - RS232 serial console port 7 - 10/100 Ethernet ports (including 1 WAN uplink port), 4 Ports support 802.3af Power-over-Ethernet (PoE)
MTBF:	> 50,000 Hours

Power Requirements

AC Input Voltage:	100-250 VAC
Max AC Input Current:	3A@230 VAC
Max Power Consumption:	120 W
Input Frequency:	47 Hz to 63 Hz

User Environment

Operating Temperature:	32°F to 104°F/0°C to 40°C
Storage Temperature:	-40°F to 158°F/-40°C to 70°C
Operating Humidity:	5% - 95% (without condensation)
Storage Humidity:	5% - 95% (without condensation)
Operating Altitude:	50 ft. to 8,000 ft./16 m to 2,438 m
Storage Altitude:	50 ft. to 12,000 ft./16 m to 3,658 m

Regulatory

Safety Certifications:	FCC (Art.15, part B), Industry Canada, CE, VCCI, C-Tick, BSMI
EMI Compliance:	UL 1950, cUL (Canada), VDE GS, DENAN (Japan), CB Cert

Part Numbers

WS-2000-SME-WW
WS-2000-IC-ABG-WW (WS 2000 and 1 AP 300 Solution)
WS-2000-IC-WW (WS 2000 and 1 AP 100 Solution)

About Symbol Technologies

Symbol Technologies, Inc., The Enterprise Mobility Company™, delivers solutions that capture, move and manage information in real time, from the point of activity to the point of decision. Symbol solutions integrate advanced data capture technology, ruggedized mobile computers, wireless infrastructure, enabling software and high-ROI applications from our business partners and Symbol Enterprise Mobility Services. Symbol enterprise mobility solutions increase business productivity and velocity, reduce costs and realize competitive advantage for the world's leading retailers, transportation and logistics companies and manufacturers as well as government agencies and providers of healthcare, hospitality and security. More information is available at **www.symbol.com**

Symbol Enterprise Mobility Services

Symbol Enterprise Mobility Services provide comprehensive support and technical expertise for designing, deploying and maintaining successful mobility solutions. Our diverse service offerings enhance your business operations, so you receive the highest value and uptime across the entire lifecycle of your mobility solution.

Our **Mobility Services** give you access to Symbol's expertise in designing and deploying global mobility solutions. Our extensive knowledge base and experience of successful mobility implementations enables early adopters to gain competitive advantage. **SymbolCertified Professional Services** providers apply best practices that integrate established mobility systems, devices and applications into your business environment. As a seamless extension of Symbol, certified partners provide services ranging from design and implementation to training and project management to help ensure a smooth transition from implementation to operations. Symbol **Customer Services** deliver the experience, expertise and global repair capabilities for maximum uptime of your business operations. A flexible and comprehensive portfolio of support services ensures that your mobility infrastructure, systems and solutions operate at peak performance.

For system, product or services availability and specific information within your country, please contact your local Symbol Technologies office or Business Partner.

Corporate Headquarters
Symbol Technologies, Inc.
One Symbol Plaza
Holtsville, NY 11742-1300
TEL: +1.800.722-6234/+1.631.738.2400
FAX: +1.631.738.5990

For Asia Pacific Area
Symbol Technologies Asia, Inc.
(Singapore Branch)
Asia Pacific Division
230 Victoria Street #05-07/09
Bugis Junction Office Tower
Singapore 188024
TEL: +65.6796.9600
FAX: +65.6337.6488

For Europe, Middle East and Africa
Symbol Technologies
EMEA Division
Symbol Place, Winnersh Triangle
Berkshire, England RG41 5TP
TEL: +44.118.9457000
FAX: +44.118.9457500

For North America, Latin America and Canada
Symbol Technologies
The Americas
One Symbol Plaza
Holtsville, NY 11742-1300
TEL: +1.800.722.6234/+1.631.738.2400
FAX: +1.631.738.5990

Symbol Website
For a complete list of Symbol subsidiaries and business partners worldwide contact us at:
www.symbol.com
Or contact our pre-sales team at:
www.symbol.com/sales

Part No. WS2BRO Printed in USA 10/04

symbol®
The Enterprise Mobility Company™