WS 2000 Wireless Switch

symbol®
The Enterprise Mobility Company™

Wireless Switch System

INTEGRATED WIRED AND WIRELESS LAN

Branch Office and Small/Medium Enterprises

The WS 2000 Wireless Switch from Symbol Technologies is the first integrated wired and wireless networking solution, priced and designed to meet the needs of small to medium enterprises and branch offices—from retail stores, warehouses, coffee shops and restaurants to libraries, satellite offices and more. Built on the same platform as Symbol's award-winning WS 5000 enterprise-class Wireless Switch, the WS 2000 offers:

► Extensive wireless LAN functionality and high performance

► The power and simplicity of centralized remote management

► Enterprise-class security

► The ability to scale to support future growth

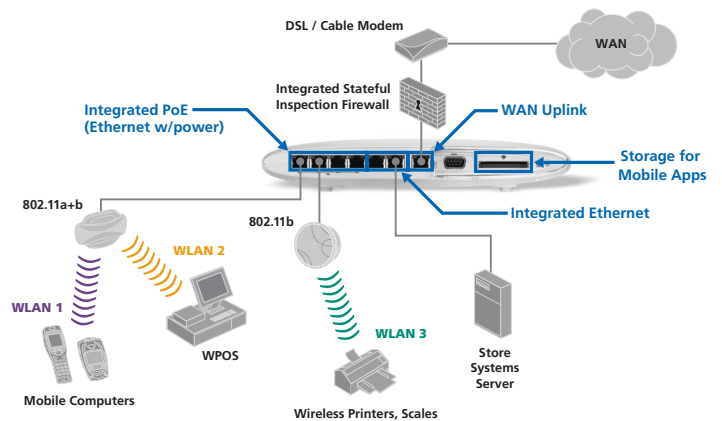…all combining to deliver outstanding investment protection and network simplicity.

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 capable), as well as an integrated router, 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, 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**

DSL / Cable Modem

WAN

Integrated Stateful Inspection Firewall

Integrated PoE (Ethernet w/power)

WAN Uplink

Storage for Mobile Apps

Integrated Ethernet

802.11a+b

802.11b

WLAN 2

WLAN 1

WLAN 3

WPOS

Mobile Computers

Wireless Printers, Scales

Store Systems Server

End-to-end layered security

WS 2000 supports a comprehensive suite of security mechanisms—including access-control, 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, and is easily upgradeable to tomorrow's standards.
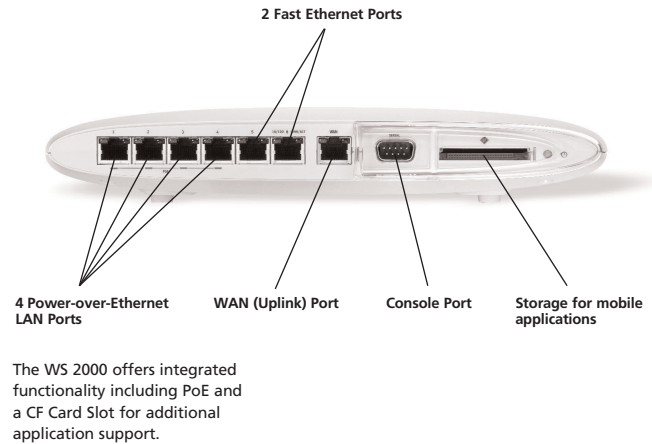
Centralized management

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.

Scaleable and easy to upgrade

Adding capacity and new functionality is easier and less expensive than an access point-based wireless LAN. The WS 2000 enables your wireless network to scale easily as your company grows. Each WS 2000 supports up to 6 Access Ports and 3 wireless LANs each with its own security and network policies. And with the centralized architecture of the WS 2000, upgrading to support newer standards, such as the new 802.11i security standard, 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.

2 Fast Ethernet Ports

4 Power-over-Ethernet LAN Ports   **WAN (Uplink) Port**   **Console Port**   **Storage for mobile applications**

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 6 single or dual-band Access Port radios (802.11b and 802.11a currently with 802.11g to follow) in the 2.4 as well as 5 GHz frequencies—offering the broadest radio technology support in the industry.

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. The innovative design removes duplicate computing components and management requirements associated with using access points throughout a wireless LAN. Access Ports are easily upgraded with new features and functionality via the WS 2000, providing excellent investment protection. A wide range of 802.11a and 802.11b external antenna options enables the design of coverage patterns for the most challenging environments.

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).
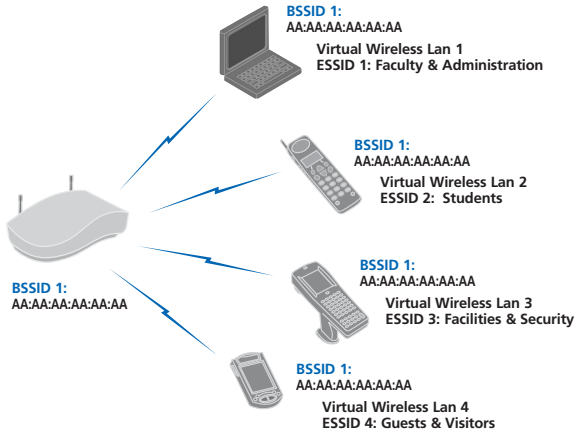
Virtual AP provides complete control over broadcast traffic. Control of broadcast traffic, including network level messages, is extremely important because of its potential negative effect on performance. Intelligent control of broadcast forwarding through proxy ARP and other mechanisms ensures that broadcast traffic is received only by the intended recipients. 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.
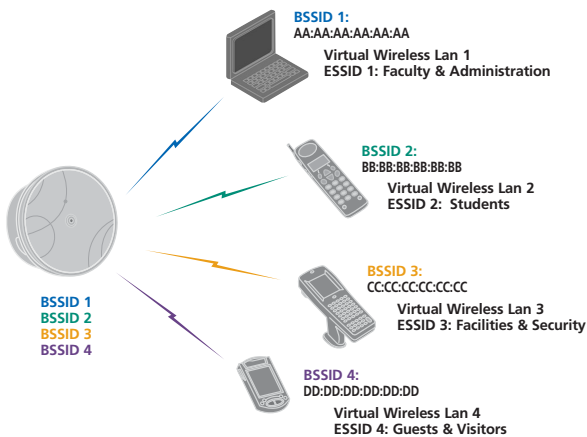
Virtual AP Enables True Virtual LANs

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

BSSID 1:
AA:AA:AA:AA:AA:AA

Virtual Wireless Lan 1
ESSID 1: Faculty & Administration

BSSID 1:
AA:AA:AA:AA:AA:AA

Virtual Wireless Lan 2
ESSID 2: Students

BSSID 1:
AA:AA:AA:AA:AA:AA

Virtual Wireless Lan 3
ESSID 3: Facilities & Security

BSSID 1:
AA:AA:AA:AA:AA:AA

Virtual Wireless Lan 4
ESSID 4: Guests & Visitors

BSSID 1:
AA:AA:AA:AA:AA:AA

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

BSSID 1:
AA:AA:AA:AA:AA:AA

Virtual Wireless Lan 1
ESSID 1: Faculty & Administration

BSSID 2:
BB:BB:BB:BB:BB:BB

Virtual Wireless Lan 2
ESSID 2: Students

BSSID 3:
CC:CC:CC:CC:CC:CC

Virtual Wireless Lan 3
ESSID 3: Facilities & Security

BSSID 4:
DD:DD:DD:DD:DD:DD

Virtual Wireless Lan 4
ESSID 4: Guests & Visitors

BSSID 1
BSSID 2
BSSID 3
BSSID 4

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.

Automatic Channel Selection

The degradation of RF performance due to environmental factors is eliminated with Automatic Channel Select (ACS). ACS optimizes radio channel planning and installation, scanning and selecting the best channel for each Access Port based on noise and signal properties.

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. Configured from within the WS 2000, this can also be part of a group policy.

Multicast Masking

This features 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 wireless applications and drivers to operating systems.

The WS 2000 extends the power of Symbol's award-winning WS 5000 Wireless Switch to the small and medium enterprise, offering the first integrated wired and wireless networking solution, priced and designed to meet the needs of small to medium enterprises—from retail stores, warehouses, coffee shops and restaurants to libraries, small offices and more.

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.

Authentication
Authentication ensures that only authorized users and devices can access your network. The WS 2000 provides a comprehensive set of authentication mechanisms to support a variety of security requirements.

Pre-shared keys
Simple shared authentication through non-wireless distribution of authentication keys ensures secure key management.

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, 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 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 rule of thumb, the stronger the encryption, the more complex and expensive it is to implement and manage. The WS 2000 supports a range of encryption options 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. Released by the WECA industry consortium, WPA is an early version of the forthcoming IEEE 802.11i security standard.

KeyGuard™—MCM

This implementation of TKIP is based on the IEEE 802.11i draft security standard. Like 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.

Security Elements

| Features	Description	Benefit
Network Access	Network based packet filtering or ACLs that limit access based on MAC addresses	Restricts authorized users and devices to specific resources
Application Access Control	Authenticates users based on application or network-based packet filtering using TCP/UDP ports	Restricts authorized users and devices to specific applications
Device and User Authentication	Provides one-way or mutual authentication between the network and associated mobile clients	Allows control of who and what attaches to your network
Transport Encryption	Transforms or scrambles data into a form that is unreadable without the key	Enables privacy of data to be maintained when sending data across an insecure network
Encryption Key Management	Provides automatic distribution and maintenance of encryption keys	Reduces management overhead by automating key distribution and increases security by constantly changing base keys

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 Ethernet ports on WS 2000.

Virtual LANs

Up to 3 independent subnets (broadcast domains) can be configured in the WS 2000. The 6 physical ports and 3 wireless LANs are mapped to one of the three subnets. Separate IP addressing and outbound network policies (filtering traffic based on Protocol type and Port ranges 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

WS 2000 also 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 3 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.
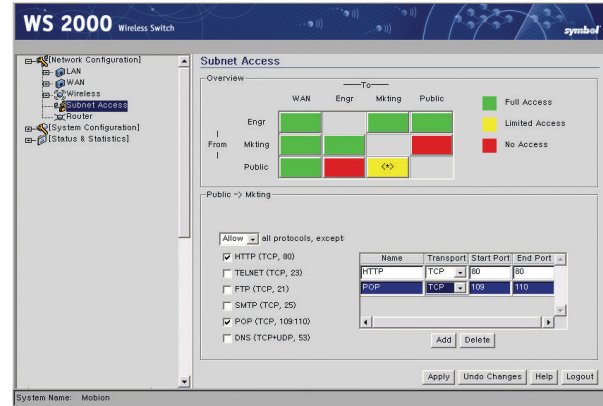
With WS 2000, it is easy to segment the network based on user profiles. Subnet access rules define what type of traffic can or cannot flow through between the subnets and between the subnet and WAN.

Integrated Gateway

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

DHCP Client and Server

The WS 2000 offers integrated DHCP services for all three 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 3 private interfaces (Subnets 1-3) 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.

8

The advanced DHCP configuration allows for specification of lease time 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 3 different NAT configurations:

▶ *One-to-One*—A pool of available public IP address can be used to map to 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 3 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 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.

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 all interfaces 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 type 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.

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 not only easy to configure, it is 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 (via cut and paste) into the WS 2000, or published to a remote FTP server which is accessible to your WS 2000 Wireless Switches. Firmware can be easily updated as well, either via FTP or TFTP servers.

Support for 4 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 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)

Key system traps are also supported. The traps can beforwarded to any enterprise management system and provide early notification of network problems related to Access Port adoption, Mobile Unit association and system resets.

Scalability

The WS 2000 Wireless Switch System is designed to grow and adapt to changing network and organizational needs. Adding additional network capacity is much easier and less expensive than traditional WLAN solutions: each WS 2000 enables the addition of up to 6 Access Ports and 3 WLANs. The plug-and-play Access Ports are ready to install right out of the box—just attach to your layer 2 LAN with Power-over-Ethernet and the network is immediately operational. LAN network integration is transparent. The result is a highly scaleable wireless network architecture that eliminates the complexities associated with the management of a traditional access point-based infrastructure servers.

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**

Features	Benefits
Switch-based architecture	Delivers unparalleled functionality, performance and simplicity of implementation and management via centralization of intelligence
Works in conjunction with Symbol's family of next-generation Access Ports—AP 100 and AP 200	Much lower costs and more functionality than traditional access points, due to the centralization of processing power in the WS 5000
Easily scaleable—each WS 2000 supports up to 6 Access Ports	Enables fast, easy and cost-effective expansion to meet growing company needs
Supports 2.4 GHz and 5 GHz frequencies with direct sequence and OFDM encoding techniques	Offers the broadest and most flexible radio technology support in the industry, with the ability to accommodate new coverage, radio types, channels, and spectrum; ensures maximum flexibility in wireless network design, enables the use of the right protocols to support specific applications for maximum cost-efficiencies
Upgradeable to support future 802.11 standards	Delivers outstanding investment protection—no forklift upgrade required to implement new standards
Ability to upgrade Access Ports	Enables very cost-effective implementation of the latest features, ensuring that the wireless LAN can always take advantage of new features and functionality as they are developed
Secure Gateway	Provides a self contained, one box network solution for small to medium enterprises with integrated Routing (RIP v1, v2, Static Routes), DHCP (client and server) and NAT (1-1, 1-Many, Port Forwarding)
WAN Uplink	Provides connectivity to Cable/DSL Modem; supports industry standard WAN protocols (PPP and PPPoE)
Voice Prioritization	Ensures quality of service for voice traffic during periods of network congestion
Power Save Protocol	Maximizes battery life of devices and ensures continual application performance for users
Virtual AP: True virtual wireless LAN support with multiple BSSID support	Enables segmentation of the wireless LAN to meet company needs, ensures that broadcast traffic reaches only devices for which it is intended; protects against broadcast storms; maximizes battery life for mobile devices by eliminating processing of unnecessary messages; and increases security by eliminating the possibility that broadcast messages could reach unintended recipients
Load Balancing and Pre-emptive Roaming	Ensures that devices roam before connection speed degrades; balances loads between Access Ports for dependable application performance
Automatic Channel Selection	Eliminates degradation of RF performance due to environmental factors
Transmit Power Control	Minimizes interference between wireless devices in networks where a dense population of Access Ports are required to meet bandwidth needs
Stateful Inspection Firewall	Prevents various types of Denial of Service (DoS) attacks; provides traffic filtering capabilities (based on ports and protocols) for more secure data network management
Authentication Support: Access Control Lists (ACLs), 802.1X, Kerberos	Provides the flexibility to select from a complete security suite of authentication mechanisms to validate user identify and authorize network access
Encryption Support: WEP, WPA-TKIP, KeyGuard™-MCM	Provides the flexibility to select from a complete security suite of encryption mechanisms to ensure privacy of data during transmission
Support for secure http, Command Line Interface (CLI), and Simple Network Management Protocol (SNMP v2, v3)	Flexible anytime anywhere remote configuration and management
Support for integrated 802.3af Symbol or standard Power-over-Ethernet devices	Eliminates the need to run expensive power lines and install outlets to provide power to Access Ports

WS 2000 Specification Highlights

Packet Forwarding

802.1D-1999 Ethernet Bridging
802.11-.802.3 Bridging

Wireless Networking

Wireless LAN:	Supports 3 WLANs
	Virtual AP: Multi-ESS/BSSID traffic segmentation
	Pre-emptive Roaming
	Virtual AP support
	Access Port Load Balancing
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

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
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)
Web Based GUI
Telnet Server
SNMP v1/v2/v3
Syslog
TFTP Client/Server
FTP Client/Server
Text-Based Configuration Files
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
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:	0°C to 40°C (50°F to 95°F)
Storage Temperature:	-40°C to 70°C (40°F to 149°F)
Operating Humidity:	8% - 95% (w/o condensation)
Storage Humidity:	5% - 95% (w/o condensation)
Operating Altitude:	16 m to 3,048 m (50 ft to 8,000 ft)
Storage Altitude:	16 m to 10,600 m (50 ft to 12,000 ft)

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

WS2BR0 02/04

symbol®

The Enterprise Mobility Company™