Wireless Switch WS 5000

Second Generation Wireless Networking

Wireless Switch System

W I R E L E S S   L A N s

The Power of Centralized Intelligence

The WS 5000 Wireless Switch from Symbol Technologies redefines the standard for enterprise class wireless networks, delivering extensive functionality, security, scalability and management at a much lower total cost of ownership than first-generation access point-based networks. By centralizing intelligence that was previously distributed throughout a wireless network via access points, this 2nd generation wireless switch architecture delivers an unparalleled level of wireless LAN control, performance and management simplicity.

Combined with Symbol's Access Ports, the WS 5000 creates the heart of the Symbol's Wireless Switch System. The WS 5000 moves beyond access point wireless networking by utilizing an extensible, expandable media independent Access Port architecture that supports 802.11a, 802.11b, and 802.11g, as well as supporting legacy access points. Symbol Access Ports represent the evolution of the access point from a network node that is difficult to scale to a simple RF media access device for the wireless switch. True plug-and-play with 'zero configuration', Access Ports are operational right out of the box, and can be mounted almost anywhere—even inside ceiling tiles. The power of the WS 5000 combined with the flexibility of Access Ports, results in a wireless LAN—Symbol's Wireless Switch System—with unsurpassed functionality.

End-to-end layered security

Our comprehensive suite of security mechanisms—including access-control, authentication, and encryption—can be deployed at various locations in the enterprise network: the perimeter, the network, the servers, and client devices. The result is a layered security model that delivers robust end-to-end security. With support for the wireless security standards of today, and the ability to easily upgrade to tomorrow's standards, the WS 5000 is the wireless gatekeeper for your enterprise network.

Centralized management

The WS 5000 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.

Scales and grows easily

Adding capacity and new functionality is easier and less expensive than an access point-based wireless LAN. The WS 5000 enables your wireless network to scale easily as your company grows, with a slim 1RU form factor that fits easily into any standard network equipment rack. Each WS 5000 supports up to 30 Access Ports and 32 WLANs.

Lower Total Cost of Ownership—Outstanding Investment Protection

The WS 5000 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 with the flexibility to support the standards of today and tomorrow, as well as the legacy wireless networks of yesterday, the WS 5000 provides outstanding investment protection.

Next Generation Wireless Switch Network Architecture with Access Ports

LAN

Centralized Management and Intelligence (Wireless Switch)

Ethernet PoE Switch

Ethernet Switch

2.4GHz DSSS & 5.2 GHz OFDM 802.11a/b AP

Access Ports

2.4GHz DSSS 802.11a/b AP
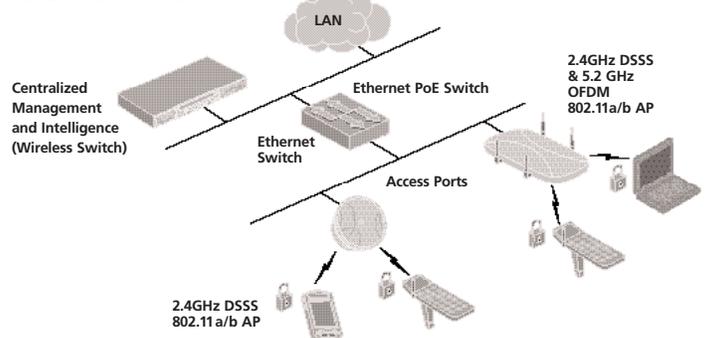
Extensive WLAN Functionality

The comprehensive feature set of the WS 5000 provides full control over wireless LAN traffic to provide peak performance. Extensive wireless LAN functionality enables you to maximize bandwidth and throughput, prioritize critical traffic, conserve power on mobile devices, and provide dependable connection speeds for users in challenging wireless environments.

Scalable Radio Architecture

Each WS 5000 supports up to 30 single or dual-band Access Port radios, easily accommodates new coverage, radio types, channels, and spectrum—offering the broadest radio technology support in the industry. The WS 5000 provides support across the 900 MHz, 2.4 GHz and 5 GHz frequencies with frequency hopping, direct sequence, and OFDM encoding techniques, as well as 802.11a/b/g, FH, and DS radio operations.

Access Ports: Next-Generation Access Points

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 5000, 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.

Per Device QoS with Bandwidth-Weighted Fair Queuing

The WS5000 controls Quality of Service (QoS) for each mobile device by guaranteeing bandwidth for specific traffic classes during periods of network congestion. With support for layer 2/3/4 classification, DiffServ, and 802.1p, packets are assigned into a bandwidth-weighted fair queuing scheduler that allocates a percentage of available bandwidth to each class queue. In addition, the Power Save Protocol (PSP) provides per device sleep-stage queues that maintain application performance for devices in sleep mode.

Power Saving for Client Devices

The Power Save Protocol (PSP) polling feature provides two modes (doze and sleep) that enable devices to maximize battery life and maintain application performance. Doze mode enables devices to conserve power between wireless transmissions, while sleep mode ensures that packets are stored and reliably delivered when the device awakens.

Virtual AP: The functionality of Four Access Points in One Access Port

Access Points with no Virtual AP
Requires Four Devices to Support Four Virtual LANs

Without Virtual AP, an access point can only support one wireless LAN. Separate access points must be deployed for each wireless LAN required, significantly increasing expense and maintenance costs.
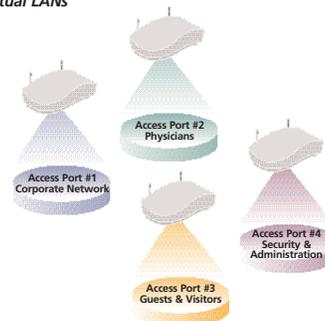
Access Ports with Virtual AP
One Access Port Supports Four Virtual LANs
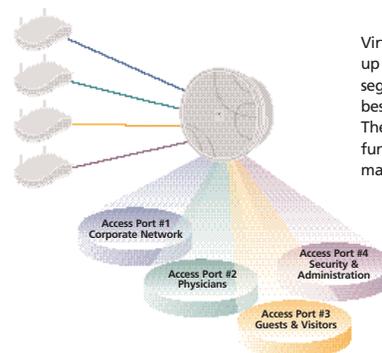
Virtual AP enables Access Ports to support up to four virtual LANs, enabling granular segmentation of the wireless network to best meet the needs of the enterprise. The result is more control, more functionality—with less capital and management expense.

Virtual AP Enables True Virtual LANS (VLANs)

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). Wireless traffic engineering capabilities control client to-client visibility, broadcast/multicast/unicast packet forwarding behavior, and security policies.

Virtual AP provides complete control over broadcast traffic, which is associated with a BSSID. 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.

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

BSSID 1:
AA:AA:AA:AA:AA:AA
Virtual Wireless Lan 4
ESSID 4: Guests & Visitors
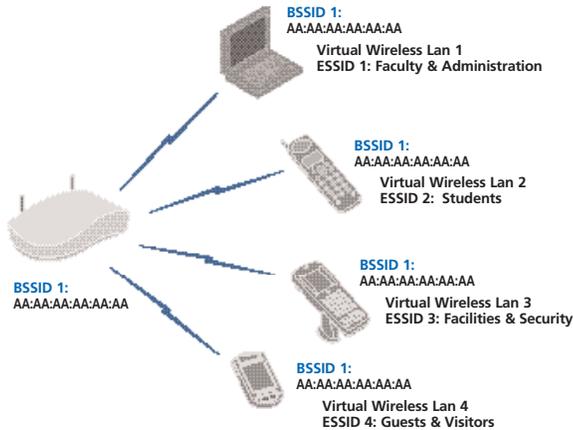
In a typical access point architecture, VLANs are defined using multiple ESSIDs. Since access points support only one BSSID, broadcast traffic intended only for Faculty and Administration (ESSID1) will be sent to all VLANs—Students (ESSID2), Facilities and Security (ESSID3) and Guests and Visitors (ESSID4). 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 1
BSSID 2
BSSID 3
BSSID 4

BSSID 4:
DD:DD:DD:DD:DD:DD
**Virtual Wireless Lan 4**
ESSID 4: Guests & Visitors
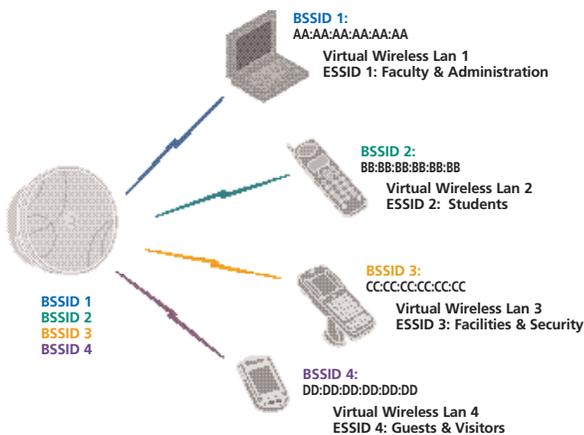
Virtual AP provides support for multiple BSSIDs, enabling the creation of true wireless VLANs. Broadcast traffic is sent only to recipients within a specific wireless VLAN (ESSID), improving overall battery life of client devices and network throughput, and ensuring security and confidentiality for broadcast traffic.

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.

Normal vs Pre-emptive Roaming

Normal Roaming
Frequently Results in Uneven Load Balancing and Poor Connection

Cell 1:
11 devices

Normal Roaming Point

Cell 2:
3 devices
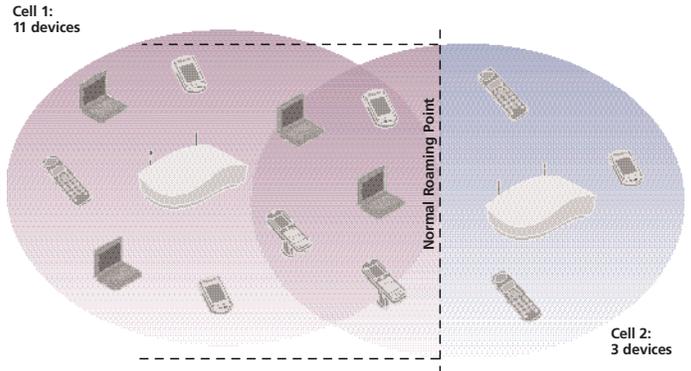
Mobile devices communicate over the wireless network at 11, 5.5, 2 or 1 Mbps. Since normal roaming does not occur until device reaches 1 Mbps, many devices are well into another cell before the connection erodes to 1 Mbps, and actual roaming to the next access point occurs. The result is uneven load balancing—too many devices supported by the Cell 1 access point result in a lack of connection quality, while only a few devices are supported by the Cell 2 access point—even though the devices have technically roamed into Cell 2.

Pre-emptive Roaming
Results in Even Load Balancing and Higher Connection Speeds

Cell 1:
8 devices

Pre-emptive Roaming Point

Cell 2:
6 devices
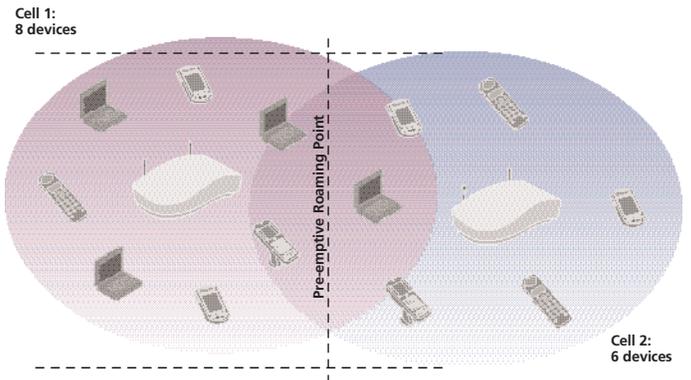
Pre-emptive roaming occurs close to the cell 'edges', ensuring that the load on any given access point is limited to those devices within the actual cell. Users experience higher and more consistent connection speeds, resulting in smoother running of applications.

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. A complete set of configuration controls provides time, mode of operation and Access Port exclusion lists.

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 5000, this can also be part of a group policy.

End-to-End Layered Security

There is no element of networking—wired or wireless—more important than security. As a pioneer and leader in wireless LANs, Symbol has implemented a complete end-to-end layered security model that includes support for all of today's wireless security standards, and is easily upgradeable to support the standards of tomorrow. Policy-based classes enable the organization of security requirements in groups—public, low, medium, and high. Policies are then configured to specify the correct level of control for users, applications, and devices within those groups.

Network Access Control

Access Control Lists (ACLs)

Layer 2/3/4 Access Control Lists provide filtering for advanced network traffic control, enabling administrators to forward, drop or redirect packets based on application type, protocol, IP Address, MAC Address and more.

Authentication

Authentication ensures that only authorized users and devices can access your network. The WS 5000 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 5000 supports a variety of EAP methods, including Microsoft®—TLS, Funk Software® —TTLS, and WPA—PEAP.

Kerberos

The industry-standard Kerberos v5 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. The Kerberos ticket-based security mechanism enables fast roaming, even with the highest levels of security.

Certificate Based Public Key Infrastructure (PKI)

PKI, used in conjunction with the AES-based VPN transport, uses secure digital certificates to provide robust authentication capabilities including verification of identity as well as integrity of data (ensuring that tampering or corruption has not occurred), and authorization for network access.

Layered Security Architecture

	Compound Security Layers	Device/User Class

HIGH	Two-stage Mutual Authentication
	    1st Stage: Device level w/PKI
	    2nd Stage: User Auth. w/Radius
	Multilayer Transport Security
	    1st WEP 128
	    2nd WTLS-AES -VPN Tunneling
	Access Scope from FW/ACLs
		Core App's
		POS
		CRM/ERP
		Mobile Worker
		User Access to corporate network

MEDIUM	User Authentication
	    EAP: TLS/TTLS/PEAP
	    Kerberos
	Transport Security
	    WEP w/TKIP
	    Keyguard -MCM
	    802.11i (when ratified)
	Access Scope from FW/ACLs
		VOIP
		Kiosks
		Controlled local access for PCs
		Client Bridge with Kerberos

LOW	NOS Based User Authentication
	Basic transport Security
	    WEP 128 Encryption
	Access Scope
	    Firewall Rules
	    ACLS
		Scales
		Price Checker
		Wireless Video Security
		Client Bridge Attached

OPEN	Open System Access	Public Access Hot Spot

A layered security approach achieves the most robust and cost-effective security, deploying multiple mechanisms throughout the various layers of your wireless network—the perimeter, the network, the servers, and client devices (also known as the link, network and session layers). User rights, network access, application types, content classes and location dependencies can all be grouped into layers, creating aggregate security policies that are simpler and less expensive to deploy and manage.

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 WS5000 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-TKIP is an early version of the forthcoming IEEE 802.11i security standards.

KeyGuard™—MCM

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

WTLS Advanced Encryption Standard (AES) Virtual Private Networking (VPN)

Symbol's AirBEAM® Safe VPN server provides a complete end-to-end VPN, ensuring the privacy, integrity and authentication of your wireless communications. The AES encryption algorithm (the standard encryption used by the U.S. government) provides a very high-level of security between clients and the VPN server. Support for session persistence and resume ensures continuous communications, protecting against interrupted transactions and preventing the need for repeated logins. Extensive client support for DOS, WIN CE, Pocket PC/Window Mobile 2003 and Windows PC platforms provides integration and security for all of your mobile devices.

As a pioneer and leader in wireless LANs, Symbol has implemented a complete
end-to-end layered security model that includes support for all of today's
wireless security standards, and is easily upgradeable to support the standards of tomorrow.

Security Elements

Features	Description	Benefit
Network Access Control	Network based packet filtering or ACLs that limit access based on MAC and IP addresses, and more	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
Accounting	Creates audit logs of who/when/how	Allows tracking of activity and network status

Security Mechanism

Control Mechanism	Best Used for Securing...	Auth. Support	Mobility Support	Layer of Security
L2-4 Access Control Lists	Device Access, Application	No	Moderate	Low
Firewall	Device Access, Application	No	Moderate	Low
WEP 10/128	Transport	No	Moderate	Low
KeyGuard-MCM	Transport	No	Excellent	Medium
WPA-PSK	Transport	No	Poor	Medium
WPA-802.1x	Transport, User	Yes	Poor	Medium
IEEE 802.11i	Transport, User	Yes	Poor	Medium
Kerberos	Transport, User	Yes	Excellent	Medium
WTLS VPN	Device, Transport, User	Yes	Excellent	High

Ease of Management

Management is intuitive and secure, and can be accessed via our command line interfaces (telnet, serial), embedded web-based java applet, and standard Simple Network Management Protocol (SNMP).

Policy-Based Management
Policy-based management enables the creation of user, application, and device groups with specific resource and network access configurations, including physical layer attributes, WLAN topologies, forwarding rules, and security components. A wide variety of parameters can be configured for each group for up to 32 WLANs, either manually or via easy-to-use wizards, such as radio settings, service definitions, Quality of Service (QoS), virtual LANs, ESS/BSSID domains, Layer 2/3 filtering, DHCP, NAT, and more.

Management Interfaces
Four interfaces provide flexibility for managing the WS 5000:

▶ The Command Line Interface (CLI) is designed with well-known industry semantics and provides complete baseline management through Telnet or Serial interfaces.
▶ Web-based management provides secure, anytime-anywhere management with an intuitive, web-based GUI that supports step-by-step software-based wizards that enable easy configuration of a wide variety features.
▶ SNMP, combined with our extensive Management Information Base (MIB) support, allows you to manage wireless functionality with common Network Management Station (NMS) tool sets, including Symbol's Enterprise Mobility Manager (SEMM) and Wavelink's Mobile Manager.
▶ Trivial File Transfer Protocol (TFTP) is provided to support image and configuration downloads.

Automatic Access Port Management
The WS 5000 automatically provides the latest firmware to Access Ports upon installation, ensuring all components in the wireless LAN are always up-to-date. Management is simplified because there is no longer a need to configure and load firmware on each access point.

Features	Benefits
Switch-based architecture	Delivers unparalleled functionality, performance and simplicity of implementation and management via centralization of intelligence
Overlay network architecture	Simplifies network integration tasks by fitting in the distribution layer of an existing and trusted network
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 generation access ports, due to the centralization of processing power in the WS 5000
Supports up to 30 Access Ports	Enables fast, easy and cost-effective expansion to meet growing company needs
Centralized management of Access Ports	Eliminates the need to configure and manage each device, dramatically reducing the time and costs previously associated with wireless LAN management
Supports 2.4 GHz and 5 GHz frequencies with frequency hopping, direct sequence, and OFDM encoding techniques, as well as 802.11a/b/g, FH, and DS radio operations	Offers the broadest and most flexible radio technology support in the industry, with the ability to 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
Per Device, Bandwidth Allocation-Weighted Fair Queuing	Enables multiple mobile and wireless applications with quality of service during periods of network congestion
Power Save Protocol	Maximizes battery life of devices and ensures continual application performance for users
True virtual 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	Ensuring that devices roam before connection speed degrades; loads are always balanced between Access Ports, ensuring quality of application performance
Automatic Channel Selection	Reduces cost of installation by eliminating the need for manual configuration of Access Port channels
Transmit Power Control	Minimizes interference between wireless devices in networks where a dense population of Access Ports are required to meet bandwidth needs
Support for Access Control Lists (ACLs), 802.1X, Kerberos and Certificate Based Public Key Infrastructure (PKI)	Provides the flexibility to select from a complete security suite of authentication mechanisms to validate user identify and authorize network access
Support for WEP, WPA-TKIP, KeyGuard™ MCM and WTLS AES Virtual Private Networking (VPN)	Provides the flexibility to select from a complete security suite of encryption mechanisms to ensure privacy of data during transmission
Support for Command Line Interface (CLI), web-based interface and Simple Network Management Protocol (SNMP)	Support for multiple management protocols provides flexible anytime anywhere management; supports Symbol's Enterprise Mobility Manager (SEMM) and Wavelink's Mobile Manager
Policy-based management	Simplifies management by enabling a pre-defined set of policies to be assigned to a selected group of users, applications and device groups
Extensive management wizards	Greatly simplifies management tasks, such as adding new features
Standard 1U form factor chassis	Mounts into any standard 19" rack mount for co-location with other network equipment
Support for 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

The WS 5000 redefines the standard for
enterprise class wireless networks,
delivering extensive functionality, security,
scalability and management at
a much lower total cost of ownership
than first-generation access
point-based wireless networks.

Scalability

The WS 5000 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 5000
enables the addition of up to 30 Access Ports and 32 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 scalable wireless network architecture that
eliminates the complexities associated with the management
of a traditional access point-based infrastructure.

System Redundancy
The WS 5000 supports redundant warm-standby switch
configuration. Designed for parallel use with an active
WS 5000, the WS 5000-RS unit provides complete
redundancy. Less expensive than the WS 5000, this
secondary device exchanges the system configuration
and a simple heartbeat message with the primary WS 5000
switch. In the event of a hardware or software failure, the
redundant switch takes control of the wireless infrastructure
ensuring consistency of operations and continuity of service.

Power over Ethernet Accessories
To lower your cost of installation, Symbol's Wireless Switch
System family includes a complete line of components to
meet all your wireless networking needs, including a complete
line of Power-over-Ethernet (POE) devices. POE devices
eliminate the need to run costly power lines and install
outlets to provide power for Access Ports, simplifying
installation and reducing costs.

Specification Highlights

Packet Forwarding

802.1D-1999 Ethernet Bridging
802.11-.802.3 Bridging
802.1Q VLAN Tagging & Trunking
Proxy ARP
IP packet steering-redirection

Wireless Networking

Wireless LAN
　　Supports 32 WLANs
　　Multi-ESS/BSSID traffic segmentation
　　VLAN to ESSID mapping
　　Power Save Protocol Polling
　　Pre-emptive Roaming
　　Congestion control with bandwidth allocation

Access Port Radios
　　Supports 1-30 Access Ports
　　Automatic Access Port Adoption with ACLs
　　Access Port Load Balancing
　　Frequency Hopping AP-to-APort Conversion
　　Direct Sequence AP-to-APort Conversion

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

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
　　PKI Certificates

Transport Encryption
　　WEP 40/128 (RC4)
　　KeyGuard
　　WPA—TKIP
　　AES

Key Exchange and Management
　　Extensible Authentication Protocol (EAP)
　　Kerberos

Optimized Wireless QoS

Per Device Weighted Fair Queuing
　　8 queues per device
　　Bandwidth management controls
　　Power Save Protocol (PSP) integration

Classification & Marking
　　Layer 1-4 Packet Classification
　　802.1p VLAN Priority
　　DiffServ/TOS

System Resiliency & Redundancy

Redundant Warm-Standby Switch
Access Port Load Balancing
Hardware based watchdog timer

Management

Command Line Interface (Serial, Telnet)
Secure Web Based GUI (SSL)
Telnet Server
SNMP v1/v2
SNMP Traps—40+ user configurable options
Syslog
TFTP Client
Simple Network Time Protocol (SNTP)
Text-Based Switch Configuration Files
DHCP
　　Client/Server/Relay
　　Switch Auto-Configuration with DHCP options
Authentication
　　Radius Client
　　Kerberos Authentication Server
MIBs
　　MIB-II
　　Etherstats
　　Wireless Switch specific monitoring and configuration

Physical Characteristics

Form Factor:	Standard 1RU
Dimensions:	1.71 in. H x 16.89 in. W x 15.75 in. D 43.5 mm H x 429 mm W x 400.2 mm D
Weight:	13.23 lbs./6 kg
Physical Interfaces:	RS232 serial console port; 10/100 Ethernet ports
MTBF:	>50,000 Hours

Power Requirements

AC Input Voltage:	100-240 VAC
Max AC Input Current:	6A@115 VAC, 3A@230 VAC
Max Power Consumption:	100-240 VAC, 50/60 Hz, 3A
Input Frequency:	47 Hz to 63 Hz

User Environment

Operating Temperature:	10°C to 35°C (50°F to 95°F)
Storage Temperature:	-40°C to 65°C (40°F to 149°F)
Operating Humidity:	8%-80% (w/o condensation)
Storage Humidity:	5%-95% (w/o condensation)
Operating Altitude:	16 m to 3,048 m (50 ft. to 10,000 ft.)
Storage Altitude:	16 m to 10,600 m (50 ft. to 35,000 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

CC-5000-SME-WW
CC-5000-RS-WW

Symbol—Your Complete Wireless Mobility Provider

Symbol Technologies is the industry leader in wireless solutions, providing everything you need to put wireless mobility to work in your business. In addition to the Wireless Switch System, Symbol Technologies offers a broad range of wireless LAN clients and technology. CompactFlash™, PC and PCI-format cards enable PDA, laptop and desktop connectivity. Design-in solutions enable integration of our award-winning technology into original designs. Voice-over-IP appliances bring the power of voice communications to your data network. Rugged and sealed mobile computers—from handhelds to tablets in a wide range of form factors with popular operating systems—integrate data capture and wireless LAN/WAN communications.

Our extensive partner network delivers application software strategic to your initiatives, allowing you to gain greater value and advantage from your wireless mobile technology. And Symbol Services provide you with expertise required to maximize system performance and realize the full potential of the Wireless System. Symbol's total solution approach ensures smooth implementation and ongoing 24/7 support.

Symbol Technologies. From wireless innovation and expertise to the most complete range of products, services and solutions, to value and ROI—no other company compares.

For more information, call any of our convenience locations or visit us at **www.symbol.com/wireless**

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

WS5BRO 12/03