Spectrum24
CB2000 Client Bridge

Product Reference Guide

72E-59814-01
Revision A
October 2002

www.symbol.com

Copyright

Patents

This product is covered by one or more of the following U.S. and foreign Patents:

4,593,186; 4,603,262; 4,607,156; 4,652,750; 4,673,805; 4,736,095; 4,758,717; 4,760,248; 4,806,742; 4,816,660; 4,845,350;
4,896,026; 4,897,532; 4,923,281; 4,933,538; 4,992,717; 5,015,833; 5,017,765; 5,021,641; 5,029,183; 5,047,617; 5,103,461;
5,113,445; 5,130,520; 5,140,144; 5,142,550; 5,149,950; 5,157,687; 5,168,148; 5,168,149; 5,180,904; 5,216,232; 5,229,591;
5,230,088; 5,235,167; 5,243,655; 5,247,162; 5,250,791; 5,250,792; 5,260,553; 5,262,627; 5,262,628; 5,266,787; 5,278,398;
5,280,162; 5,280,163; 5,280,164; 5,280,498; 5,304,786; 5,304,788; 5,306,900; 5,324,924; 5,337,361; 5,367,151; 5,373,148;
5,378,882; 5,396,053; 5,396,055; 5,399,846; 5,408,081; 5,410,139; 5,410,140; 5,412,198; 5,418,812; 5,420,411; 5,436,440;
5,444,231; 5,449,891; 5,449,893; 5,468,949; 5,471,042; 5,478,998; 5,479,000; 5,479,002; 5,479,441; 5,504,322; 5,519,577;
5,528,621; 5,532,469; 5,543,610; 5,545,889; 5,552,592; 5,557,093; 5,578,810; 5,581,070; 5,589,679; 5,589,680; 5,608,202;
5,612,531; 5,619,028; 5,627,359; 5,637,852; 5,664,229; 5,668,803; 5,675,139; 5,693,929; 5,698,835; 5,705,800; 5,714,746;
5,723,851; 5,734,152; 5,734,153; 5,742,043; 5,745,794; 5,754,587; 5,762,516; 5,763,863; 5,767,500; 5,789,728; 5,789,731;
5,808,287; 5,811,785; 5,811,787; 5,815,811; 5,821,519; 5,821,520; 5,823,812; 5,828,050; 5,848,064; 5,850,078; 5,861,615;
5,874,720; 5,875,415; 5,900,617; 5,902,989; 5,907,146; 5,912,450; 5,914,478; 5,917,173; 5,920,059; 5,923,025; 5,929,420;
5,945,658; 5,945,659; 5,946,194; 5,959,285; 6,002,918; 6,021,947; 6,029,894: 6,031,830; 6,036,098; 6,047,892; 6,050,491;
6,053,413; 6,056,200; 6,065,678; 6,067,297; 6,082,621; 6,084,528; 6,088,482; 6,092,725; 6,101,483; 6,102,293; 6,104,620;
6,114,712; 6,115,678; 6,119,944; 6,123,265; 6,131,814; 6,138,180; 6,142,379; 6,172,478; 6,176,428; 6,178,426; 6,186,400;
6,188,681; 6,209,788; 6,209,789; 6,216,951; 6,220,514; 6,243,447; 6,244,513; 6,247,647; 6,308,061; 6,250,551; 6,295,031;
6,308,061; 6,308,892; 6,321,990; 6,328,213; 6,330,244; 6,336,587; 6,340,114; 6,340,115; 6,340,119; 6,348,773; D305,885;
D341,584; D344,501; D359,483; D362,453; D363,700; D363,918; D370,478; D383,124; D391,250; D405,077; D406,581;
D414,171; D414,172; D418,500; D419,548; D423,468; D424,035; D430,158; D430,159; D431,562; D436,104.

Invention No. 55,358; 62,539; 69,060; 69,187 (Taiwan); No. 1,601,796; 1,907,875; 1,955,269 (Japan); European Patent 367,299; 414,281; 367,300; 367,298; UK 2,072,832; France 81/03938; Italy 1,138,713

3/02

Symbol Technologies, Inc.
One Symbol Plaza
Holtsville, N.Y. 11742-1300
Telephone:(800)SCAN234, (631)738-2400, TLX:6711519
www.symbol.com

About This Document

Reference Documents

This reference guide refers to the following documents:

Part Number	Document Title
72E-56316-01	Spectrum24 AP-4131 Access Point Product Reference Guide

Conventions

Keystrokes are indicated as follows:

ENTER	identifies a key.
FUNC, CTRL, C	identifies a key sequence. Press and release each key in turn.
Press A+B	press the indicated keys simultaneously.
Hold A+B	press and hold the indicated keys while performing or waiting for another function. Used in combination with another keystroke.

Typeface conventions used include.

<angles>	indicates mandatory parameters in syntax.
[brackets]	for command line, indicates available parameters; in configuration files, brackets act as separators for options.
GUI Screen text	indicates the name of a control in a GUI-based application.
Italics	indicates the first use of a term, book title, variable or menu title.
`Screen`	indicates monitor screen dialog. Also indicates user input. A screen is the hardware device on which data appears. A display is data arranged on a screen.
`Terminal`	indicates text shown on a radio terminal screen.
URL	indicates Uniform Resource Locator.

This document uses the following for certain conditions or information:

Indicates tips or special requirements.

Indicates conditions that can cause equipment damage or data loss.

Indicates a potentially dangerous condition or procedure that only Symbol-trained personnel should attempt to correct or perform.

Contents

Chapter 1 Introduction

1.1 Spectrum24 CB2000 Client Bridge

Spectrum24 is a spread spectrum cellular network that operates between 2.4 and 2.5 GHz (gigahertz). This technology provides a high-capacity (up to 11Mbps) network using multiple access points within any environment.

The Spectrum24 High Rate CB2000 Client Bridge is a wireless network bridge allowing up to four devices to connect to a Wi-Fi IEEE 802.11b wireless local area network (LAN), or communicate directly with other mobile devices enabled for wireless LAN connectivity.

Features include:

- Wi-Fi certified for multi-vendor compatibility
- Compatible with NBX® communication systems to deploy fully managed voice and data networks
- Hub connections for up to four users per bridge provide affordable wireless connections
- Client tools for open networks with DHCP
- Remote manageability using a standard web browser or SNMP management tool
- Auto Network Connect keeps roaming users connected with a choice of ad hoc or infrastructure networks
- Support for 40-bit wired equivalent privacy (WEP), 128-bit, and Kerberos encryption.

1.2 Radio Basics

Spectrum24 devices use both *electromagnetic waves* to transmit and receive electric signals without wires. Users communicate with the network by establishing radio links between Mobile Units (MUs) and Access Points (APs).

Spectrum24 uses *FM (frequency modulation)* to transmit digital data from one device to another. Using FM, a radio signal begins with a carrier signal that provides the base or center frequency. The digital data signal is superimposed on the *carrier signal (modulation)*. The radio signal propagates into the air as electromagnetic waves. A receiving antenna in the path of the waves absorbs the waves as electrical signals. The receiving device demodulates the signal by removing the carrier signal. This demodulation results in the original digital data.

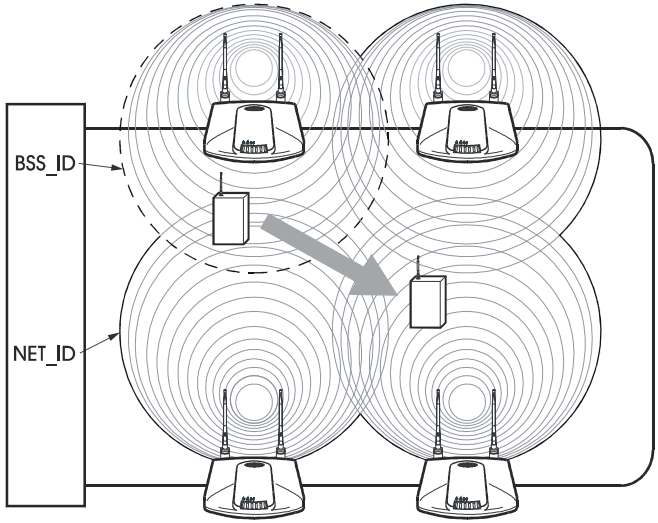
Spectrum24 uses the *environment* (the air and certain objects) as the transmission medium. Spectrum24 radio devices transmit in the 2.4 to 2.5-GHz frequency range, a license-free range throughout most of the world. The actual range is country-dependent.

Spectrum24 devices, like other Ethernet devices, have unique, hardware-encoded *Media Access Control (MAC)* or *IEEE addresses*. MAC addresses determine the device sending or receiving data. A MAC address is a 48-bit number written as six hexadecimal bytes separated by colons.

For example:
`00:A0:F8:24:9A:C8`

1.2.1 Cellular Coverage

An Access Point (AP) establishes an average communication range with Mobile Units (MUs) called a *Basic Service Set (BSS*) or *cell*. The CB2000 and any Ethernet devices connected to it appear as a single MU to the AP. When in a particular cell, the MU associates and communicates with the AP of that cell. Each cell has a *Basic Service Set Identifier (BSS_ID)*. In IEEE 802.11, the AP MAC address represents the BSS_ID. The MU recognizes the AP it associates with using the BSS_ID. Adding APs to a LAN establishes more cells in an environment, making it an RF Network using the same *Extended Service Set Identifier (ESSID)*.



APs with the same ESSID define a coverage area. The MU searches for APs with a matching ESSID and synchronizes with an AP to establish communications. Device association allows MUs within the coverage area to move about or roam. As the MU roams from cell to cell, it switches APs. The switch occurs when the MU analyzes the reception quality and determines that a different AP can provide better service based on the best signal strength and lowest load distribution.

If the CB2000 does not find an AP with a usable signal, it performs a scan to find any AP. As MUs switch APs, the AP updates the association table.

1.2.2 Network Topology

The variations possible in Spectrum24 network topologies depend on the following factors:

- Operating mode, either Ad Hoc (Peer-to-Peer) or Access Point (Infrastructure)
- The location and number of APs present in the network
- client bridge function in the network
- type of network security, i.e. open network with DHCP, 40-bit wired equivalent privacy (WEP), 128-bit, or Kerberos encryption.

1.2.3 Site Topology

For optimal performance, place the bridge in a dry, clean location near the hub, telephone, computer, or printer connected to the bridge. The location must have a power source and be within 300 feet (100 meters) of a Wi-Fi compliant wireless LAN access point. The location should be away from transformers, heavy-duty motors, fluorescent lights, micro-wave ovens, refrigerators, or other equipment that could cause radio signal interference.

1.3 CB2000 Client Bridge Functional Theory

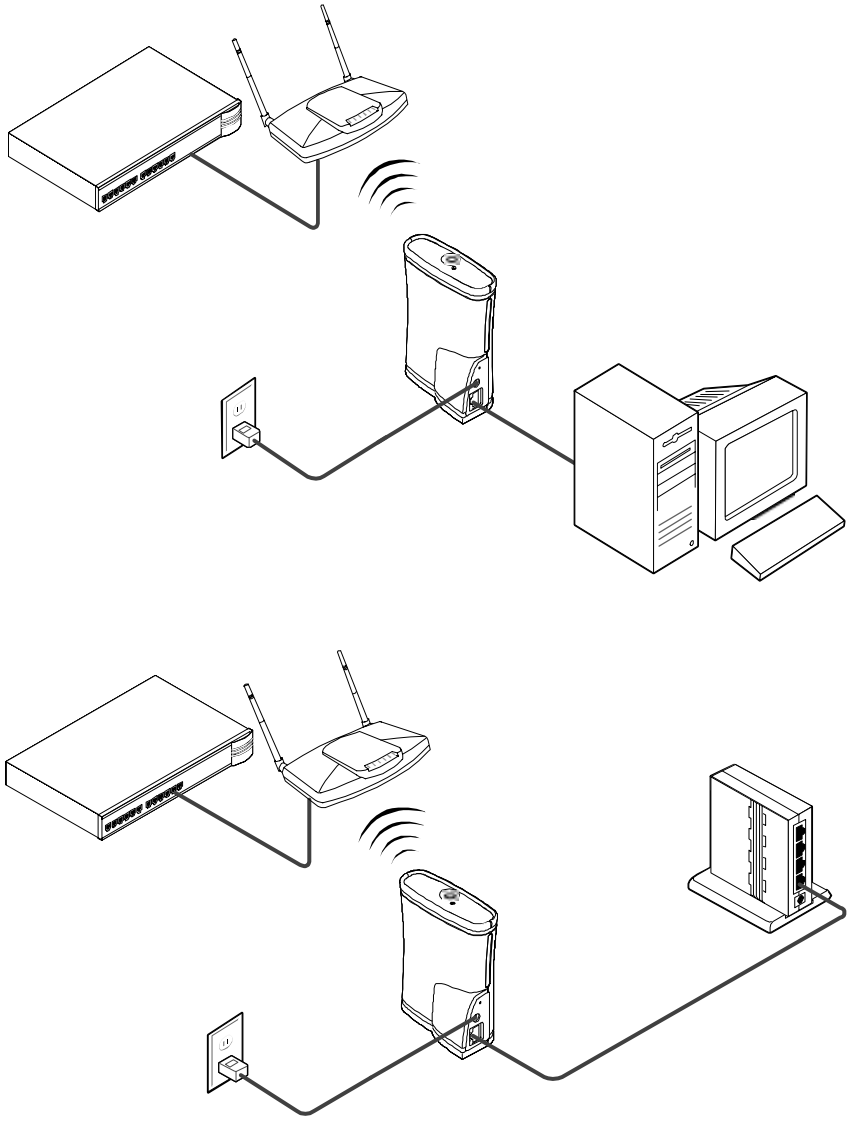
To improve CB2000 management and performance, users need to understand basic client bridge operating modes, functionality, and configuration options.

1.3.1 Operating Modes

Access Point (Infrastructure) Mode

In infrastructure mode, the CB2000 operates as an infrastructure device that connects with the LAN through a wireless Access Point (AP). Ethernet client devices, such as PCs, printers, and ethernet-enabled appliances connect to the CB2000, either directly, or up to four devices through a hub connection.

Typical infrastructure mode computer connections:



The CB2000 associates with an AP located nearby. The AP sees the client bridge/network device combination as a standard Mobile Unit (MU). The AP forms a wireless bridge between the wired LAN and the wireless clients through the CB2000.

The AP is a dedicated device that is wired into the LAN back bone while the CB2000 units can be physically moved throughout the LAN. Because each unit can support up to four Ethernet client devices, the CB2000 is designed to be placed in a single location for optimal use.

Ethernet clients connected to the CB2000 communicate with the network by routing data through the associated AP. The 802.11 standard enables the CB2000 and its clients to be moved from one location to another. Reassociation occurs instantly on an open network with DHCP, but IP configuration is necessary for the CB2000 to communicate with an AP for networks with any form of security. See “Configuring System Parameters” on page 23 for additional information.

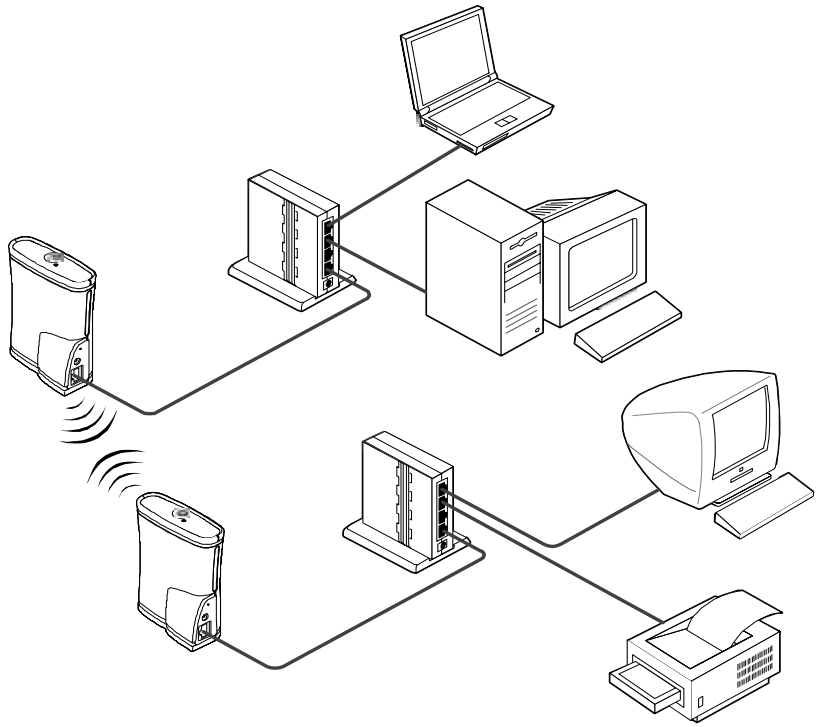
Ad Hoc (Peer-to-Peer) Mode

Peer-to-Peer mode allows two or more CB2000 units to communicate exclusively with one another without the use of an AP. Use this mode to bridge two or more Ethernet devices.

In Ad Hoc mode, both CB2000 units share the same subnet and have identical configurations to work properly. Specifically, the Wireless LAN Service Area, channel selections, data preamble setting and security settings are required to be the same for both units to communicate. Refer to *Configuring System Parameters* on page 23 for additional information.

Ad Hoc mode supports no security (open network) and 40-bit Shared Key security. 128-bit encryption and Kerberos are not supported in Ad Hoc mode.

Typical Ad Hoc mode connection:



1.3.2 MAC Layer Bridging

The CB2000 communicates with an AP via *MAC layer bridging*. The AP monitors traffic from the CB2000 and other interfaces and, based on frame address, forwards the frames to the proper destination. The AP tracks the frames sources and destinations to provide intelligent bridging as MUs roam or network topologies change. The AP also handles broadcast and multicast messages and responds to MU association requests. The MU in turn passes this information to the client to complete the network communication process.

The CB2000 maintains a client list of MAC addresses to keep track of specific devices connected to the device. Each time a new device is connected to the bridge, either directly or through a hub, that device's MAC address is added to the client list. After connecting four different devices, the client list is full. To connect another new device, clear the device to be replaced from the client list before the next new device can associate with the network through the CB2000. To clear a device from the list, access the bridge's configuration management system. See “Ethernet Client List” on page 33 for additional information.

To aid in managing the CB2000, the MAC address for each unit is located on the bottom of the unit.

1.3.3 DHCP Support

The CB2000 uses Dynamic Host Configuration Protocol (DHCP) to obtain a leased IP address and configuration information from a remote DHCP server on an open network.

1.3.4 Media Types

The CB2000 supports bridging between Ethernet and radio media.

The Ethernet interface fully complies with Ethernet Rev. 2 and IEEE 802.3 specifications. The access point supports a 10/100Base-T wired connection. The data transfer rate is 11 Mbps.

The radio interface conforms to IEEE 802.11 specifications. The interface operates at 11 Mbps using direct-sequence radio technology.

1.3.5 Direct Sequence Spread Spectrum

Spread spectrum (broadband) uses a narrowband signal to spread the transmission over a segment of the radio frequency band or spectrum. Direct-sequence is a spread spectrum technique where the transmitted signal is spread over a particular frequency range. The CB2000 client bridge uses Direct-Sequence Spread Spectrum (DSSS) for radio communication. Direct-sequence systems communicate by continuously transmitting a redundant pattern of bits called a chipping sequence. Each

bit of transmitted data is mapped into chips by the access point and rearranged into a pseudorandom spreading code to form the chipping sequence. The chipping sequence is combined with a transmitted data stream to produce the AP output signal.

Mobile Units receiving a direct-sequence transmission use the spreading code to map the chips within the chipping sequence back into bits to recreate the original data transmitted by the access point. Intercepting and decoding a direct-sequence transmission requires a predefined algorithm to associate the spreading code used by the transmitting access point to the receiving MU. This algorithm is established by IEEE 802.11b specifications. The bit redundancy within the chipping sequence enables the receiving MU to recreate the original data pattern, even if bits in the chipping sequence are corrupted by interference.

The ratio of chips per bit is called the spreading ratio. A high spreading ratio increases the resistance of the signal to interference. A low spreading ratio increases the bandwidth available to the user. The access point uses a constant chip rate of 11Mchips/s for all data rates, but uses different modulation schemes to encode more bits per chip at the higher data rates. The access point is capable of an 11 Mbps data transmission rate, but the coverage area is less than a 1 or 2 Mbps access point since coverage area decreases as bandwidth increases.

1.3.6 AP to MU Association Process

APs recognize MUs as they associate with the AP. The AP keeps a list of the MUs it services. MUs associate with an AP based on the following conditions:

- the signal strength between the AP and MU
- MUs currently associated with the AP
- the MUs encryption and authentication capabilities and the type enabled
- the MUs supported data rates (1 Mbps, 2 Mbps, 5.5 Mbps or 11 Mbps for the CB2000).

1.3.7 Data Encryption

Mobile nodes and other hosts can be a target of information theft. This occurs when unauthorized users eavesdrop on a network to glean proprietary information. The absence of a physical connection makes wireless links particularly vulnerable to eavesdropping.

Encryption is the most efficient method in preventing information theft and improving data security. Encryption requires scrambling and coding of information, typically with mathematical formulas called algorithms, before the information is transmitted over a communications link or network. An algorithm is a set of instructions or formula describing how to scramble and encode the data. A *key* is the unique code used by the algorithm to encrypt or decrypt the data. Decryption is decoding and unscrambling the received encrypted data.

The same device, host computer or front-end processor, usually performs both encryption and decryption. The data direction determines which function, encryption or decryption, the device performs. The device takes plain text, encrypts and scrambles the text by mathematically combining the key with the plain text as instructed by the algorithm, then transmits the data over the network. At the receiving end, another device unscrambles and decodes the encrypted text revealing the original message.

A user can know the algorithm, but cannot interpret the data without the key. Only the sender and receiver of the transmitted data know the secret key.

Symbol uses the Wired Equivalent Privacy (WEP) algorithm, specified in IEEE 802.11 section 8, for encryption and decryption. WEP uses the same secret key for both encrypting and decrypting plain text. An external key management service distributes the secret key. Symbol recommends that users regularly change keys for added security.

IEEE 802.11 defines two types of authentication, Open System and Shared Key. Open System authentication is a null authentication algorithm. Shared Key authentication is an algorithm where both the AP and the MU share an *authentication key* to perform a checksum, an error-checking operation, on the original message.

By default, IEEE 802.11 devices operate in an *open system network* where any wireless device can associate with an AP without authorization. A wireless device with a valid shared key is allowed to associate with the AP. Authentication management messages, also called packets, are unicast, meaning authentication messages transmit between only one AP and one MU, not broadcast or multicast.

1.3.8 Kerberos Authentication

Authentication is critical for the security of any wireless LAN device, including a Spectrum24 device operating on a wireless network. Traditional authentication methods are not suitable for use in wireless networks where an unauthorized user can monitor network traffic and intercept passwords. The use of strong authentication methods that do not disclose passwords is necessary.

Symbol uses the Kerberos authentication service protocol (specified in RFC 1510), to authenticate users/clients in a wireless network environment and to securely distribute the encryption keys used for both encrypting and decrypting plain text.

For a detailed description of the Kerberos authentication service protocol refer to RFC 1510: Kerberos Network Authentication Service (V5).

A basic understanding of RFC 1510 Kerberos Network Authentication Service (V5) is helpful in understanding how Kerberos functions.
By default, Spectrum24 devices operate in an open system network where any wireless device can associate with an AP without authorization. Kerberos requires Spectrum24 device authentication before access to the wired network is permitted. Kerberos cannot operate when the AP is in wireless (WLAP) mode.

If DHCP is disabled or a DHCP server is not available, use the Kerberos Network Parameters screen to manually configure Kerberos. See “Security Settings” on page 28 for additional information.

Kerberos is enabled in the Security Settings page of the Configuration Management System UI for the CB2000, and can be enabled automatically in an AP physically attached to an Ethernet network from a DHCP server on the same network. Consult the *Spectrum24 Access Point Product Reference Guide* for information on configuring Kerberos for a wireless network. When the AP boots, it automatically requests the KSS for Kerberos parameters. If a DHCP server is not present, a user manually enables Kerberos in the AP. A Key Distribution Center (KDC) contains a database of authorized users and passwords within its realm (a realm is the Kerberos equivalent of a Windows domain). The KDC is responsible for user authentication, the distribution of session/service keys (tickets).

The optional KSS requires restarting whenever the KDC is rebooted.

The KDC contains two components:

- Authentication Service (AS)
  - Provides the authentication ticket containing information about the client and the session key used with the KDC.
- Ticket Granting Ticket Service (TGS)
  - Permits devices to communicate with a service (this could be any application or service such as the AP RF services).

The default expiration time of a ticket is 12 hours (for the AP) and is not user configurable. If the lifetime of a ticket in the KDC's security policy is different than what is requested, the KDC selects the shortest expiration time between the two. Each time a ticket is generated a new session and WEP encryption key is generated.

The KDC resides on the Kerberos server (the Kerberos server can also be the DNS server). In addition to the KDC, an optional *Kerberos Setup Service (KSS)* can be installed on the Kerberos server. The KSS runs as a client on the KDC server when initially launched. The KSS can be used to administer Spectrum24 devices authorized on the network. For example, an AP on the Access Control List (ACL) is lost or stolen. The KSS marks the AP (using the MAC address of the AP) as not authorized and notifies the administrator if the missing AP appears elsewhere on the network attempting authentication. All clients (MUs), KDC and services (APs) participating in the Kerberos authentication system are required to have their internal clocks synchronized within a specified maximum amount of time (known as clock skew). The KSS uses Network Time Protocol (NTP) or the system clock on the Kerberos server to provide clock synchronization (timestamp) between the KDC and APs as part of the authentication process. Clock synchronization is essential since the expiration time is associated with each ticket. If the clock skew is exceeded between any of the participating hosts, requests are rejected.

Additionally, the KSS provides a list of authorized APs and other security setup information that the KDC uses to authenticate clients. Refer to the *Spectrum24 Access Point Product Reference Guide* available from the Symbol Website (http://www.symbol.com) for information on configuring KSS parameters for a wireless network.

When the AP boots up it contacts the KSS to obtain KDC information. The AP sends an Authentication Service Request (AS_REQ) to the KDC. The KDC looks up the username (ESSID in the case of APs), the associated password, and other authentication information including the current time stamp. If the AP has provided the correct information the KDC responds

with an Authentication Service Response (AS_REP). These initial Kerberos messages are used to obtain the client credentials and session key known as the Ticket Granting Ticket. The AP verifies the information and is authenticated with the KDC. After the AP validates the message, it turns on its RF services but does not bridge data packets until the MU has been authenticated.

An MU is required to authenticate with the KDC before the AP allows any RF bridging. The MU appears to associate but because it has not been authenticated, the AP does not bridge any non-Kerberos authentication type packets to the network. The AP acts as a conduit (the AP will proxy the MU requests/replies to and from the KDC) passing AS_REQ, AS_REP, Ticket Granting Service Request (TGS_REQ) and Ticket Granting Service Reply (TGS_REP) between the clients and the KDC until authentication is successful.

Once a ticket is issued and the authentication process is completed, the AP continues to bridge data with the MU even if the KDC/KSS are unavailable. Once the ticket expires, the AP/MU stop passing Kerberos data if the KDC/KSS are still unavailable to issue tickets.

The authentication process for an MU is similar to an AP authentication. The difference being that the MU/client sends all requests through the AP with one additional step. The additional step is sending the KDC a TGS_REQ for RF services. The TGS_REQ message is encrypted with the encryption key that the MU received during the first part of the authentication process. The ticket the MU received in the AS_REP includes: the ESSID of the AP whose RF services it wishes to access. The AP proxies (forwards) the MU request to the KDC. The KDC verifies the request and responds with a TGS_REP sent to the MU through the AP which proxies the reply to the MU. The AP proxy does not read the MU TGS_REQ but replaces the header information with an IP header (the AP IP address). Conversely, the AP replaces the TGS_REP header with a WNMP header and forwards the response to the MU. Once the MU has verified the message it prepares an Application Request (AP_REQ) for the AP. This AP_REQ

contains the ticket the KDC has sent to the MU. The AP decrypts the ticket. If the ticket is valid the AP responds with an AP_REP (the AP generates and includes128 bit WEP encryption key in the reply) and permits the MU to bridge data.

The KDC cannot authenticate an MU with administrator as the username.

The optional KSS runs only on a Windows 2000 server with Active Directory enabled. Consult the *Spectrum24 Access Point Product Reference Guide* for additional information on KSS.

Roaming and Authentication

When an MU authenticates through the KDC it specifies that it wants access to the AP that it has associated with. When the MU completes the full ASREQ/AS-REP, TGT-REQ/TGT-REP, and AP-REQ/AP-REP hand-shake sequence, it possesses a ticket and a session key (WEP encryption key) for use in communicating with that AP. However, since the password and the username are the same for all APs, that ticket decrypts and validates with any AP. When a MU roams, after it has associated with the new AP it sends to that AP the same AP-REQ that it sent to the AP that it first authenticated with. The new AP decrypts the ticket and validates the authenticator in the AP-REQ message. It then sends back an AP-REP with a new session key to the MU and normal communication through the new AP can continue.

1.3.9 Web Management Support

A Symbol CB2000 Client Bridge includes an HTTP Web server to allow the user to access and manage the bridge with a standard Java-compatible browser. This capability provides the user with a Web-based interface for configuration and firmware download.

Using either Netscape Navigator 4.5 or greater or Microsoft Internet Explorer 4.0 or greater, point the browser at either the IP address of the bridge or use the CB2000 Device Manager to access the User Interface (UI). See “Gaining Access to the UI” on page 20. Once accessed, a user can view configuration, setup and performance information for the bridge and make changes as necessary.

Chapter 2 Configuring the CB2000

2.1 Configuration Requirements

CB2000 configuration requires a direct or LAN connection to the bridge and access to the UI (User Interface). To access the UI through a Web browser or SNMP management tool, refer to “Gaining Access to the UI” on page 20.

The type of network and level of security used with the CB2000 dictates the steps necessary to configure the device.

- *Open system, DHCP server, no special security requirements.* Use the CB2000 as it ships from the factory.

  After connecting the device, the CB2000 establishes a wireless connection with an AP, automatically receives IP and subnet addresses via DHCP and is ready for use.

  Once operational, use the Spectrum24 CB2000 Management Tool to obtain specific information, such as IP and MAC addresses, which are necessary for relocating the device within the network.

  The CB2000 factory default configuration is:

Property	Default Setting
Device Name	Symbol_CB2000
Device Location	None
Help File Location	Embedded in device
IP Address	Default is 10.1.1.3
Subnet Mask	255.255.0.0
Gateway IP Address	Obtained automatically
Channel Selection	Automatically select the best channel; uses access point setting.
Channel	Uses access point channel.
Wireless LAN Service Area	Attach to any WLAN Service Area automatically
Network Mode	Access Point (infrastructure)

Access Point Privacy Mode	Off
Antenna Selection	Diversity
Network Traffic Accelerator	Off (Wi-Fi interoperable)
Data Preamble	N/A (Not applicable)
Security Setting	No Security (Open System)
Administration Password	None
TFTP Server IP Address	None (Uses TFTP port 69)

- *Closed network with security requirements.* For first-time installations, connect the CB2000 directly to a workstation. For device relocation, use the CB2000 Device Manager to locate and configure the CB2000 prior to moving the unit.

2.2 Gaining Access to the UI

The two primary methods for establishing access to the UI include:

- Using the management tool to locate the device and launch the Configuration Management System
- Accessing the device directly through a Web browser.

The type of method used depends on whether the workstation used to access the CB2000 has the Device Manager installed and the type of connection used. Select the access that best fits the network environment.

2.2.1 Using the CB2000 Device Manager

The Spectrum24 CB2000 Device Manager simplifies the process of accessing the CB2000 to view or change system parameters.

Using the Device Manager to gain access to the UI requires the tool be installed and the computer accessing the bridge be on the same subnet.

If the computer accessing the CB2000 is on a different subnet, the Pre-IP Configuration Wizard activates automatically. If the subnet settings are changed with the Wizard, users or devices connected to the bridge may lose contact with the LAN.

To launch the Device Manager and access the UI:

1. Select Start, Programs, Symbol Wireless, and CB2000 Device Manager.

   If more than one network adapter is installed on the computer, the user could be prompted to choose a network adapter. Choose the appropriate adapter and click OK.

   The Wireless Network Tree appears in the Spectrum24 CB2000 Device Manager window. The tree lists all WLAN service areas on the network and expands to show the Spectrum24 CB2000 devices associated with each service area. Devices in a different subnet are

identified with exclamation points (!). To refresh this display, click Refresh.

Refresh the display, for example, after changing a device IP address.

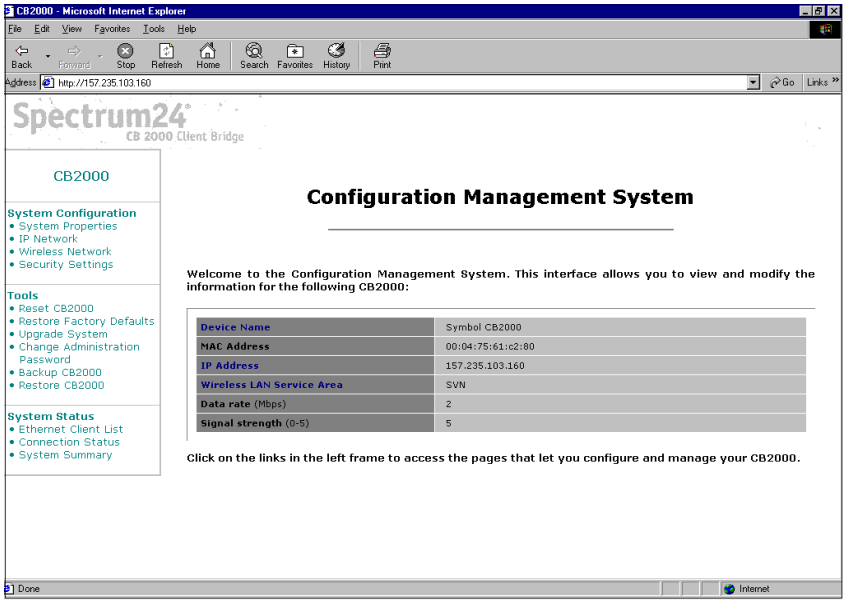
2. In the Wireless Network Tree, select the device to configure.

   If more than one wireless LAN device appear in the tree, determine the right one by clicking Properties and checking the MAC address (serial number, located on the bottom of the device) to verify that it is correct.

3. Click Configure.
   If the selected device is on the same subnet as the computer, the Configuration Management System main page appears in the Web browser. (If a password is set on the device, enter it when prompted.)

   If the selected device is on a different subnet, the Pre-IP Configuration Wizard is activated automatically. For more information, Refer to “Pre-IP Configuration Wizard” on page 42.

4. The next window prompts for an administrative password to allow the new IP address to be set. When the units are shipped from the factory, there is no administration password. Enter a password and click Next. The Configuration Management System main page appears in the Web browser.



5. View or change configuration parameters as necessary. See online help and *Configuring System Parameters* on page 23 for additional information on setting and changing configuration settings.

2.2.2 Using a Browser

Using a Web browser to gain access to the UI requires the workstation to have a TCP/IP stack and a Web browser. The remote station can be on the wired or wireless LAN.

Note

The workstation accessing the UI must be on the same subnet as the device. The Web browser (Internet Explorer 4.0 or greater or Netscape) requires JavaScript to gain access to the UI.

To access the CB2000 UI using a Web browser from a workstation:

1. From the NCPA properties window set the IP address of the workstation and the subnet mask. The system prompts the user to reboot for the changes to take effect.
2. To verify the connection, ping the CB2000. At the default DOS prompt, type:

   ```
   ping -t xxxx.xxxx.xxxx.xxxx
   ```

   – If the ping receives no response, verify the hardware connections, IP address, gateway address and subnet mask are correct. If correct, contact the site System Administrator for network assistance.
3. Start a Web browser such as Internet Explorer 4.0 or greater, or Netscape 3.0 or greater. Type the IP Address for the associated AP to access the AP using a Web browser:

   ```
   http://xxx.xxx.xxx.xxxaccess
   ```

Once accessed, the main page of the Configuration Management System displays an overview of the CB2000 settings, including the Device Name, MAC Address, IP Address, Wireless LAN Service Area, Data Rate, and Signal Strength.

Use the mouse to navigate the menus requiring modification.

2.3 Configuring System Parameters

CB2000 system parameters configuration requires setting the default parameters to enable the device to communicate with an AP on a specified wireless network (Infrastructure Mode) or another CB2000 (Peer-to-Peer Mode). These settings include: System Properties, IP Network, Wireless Network, and Security Settings.

Entering, Clearing, and Applying Configuration Settings

Some configuration pages have three buttons: Enter, Clear All Changes, and Apply All Changes. Use these buttons in the following manner:

- Enter stores settings temporarily in the device cache memory, but does not apply them permanently in the device nonvolatile memory. Use Enter to save changes while still configuring the bridge. The changes do not appear on the System Summary page until the user clicks Apply All Changes. Use Enter if making changes on multiple configuration pages, but do not want the changes to take effect until after all have been set.
- Clear All Changes returns the settings in the device cache memory to the values they had when Apply All Changes was last clicked.
- Apply All Changes stores the settings permanently in the device nonvolatile memory. After clicking Apply All Changes, the new configuration settings take effect and the changes appear on the System Summary page.

If a user does not click Enter or Apply All Changes before moving to a new configuration page, the changes to the current page are lost.

If a user does not click Apply All Changes before resetting the device, the changes are lost.

If a user does not click Apply All Changes before closing the browser, the changes remain in the device cache memory, but do not appear in the System Summary until the user starts a new session and clicks Apply All Changes.

2.3.1 System Properties

Under System Configuration, click System Properties. The System Properties page displays the properties of the selected device. Change properties by entering values in the fields and clicking the radio buttons. When finished, click Enter or Apply All Changes.

- *Device Name.* Appears in the System Summary window. Change the default name if desired. The default value is Symbol_CB2000.
- *Device Location.* Optionally, enter a location to identify where the device is installed. (For example, Building 4, Cubicle 7.)

2.3.2 IP Network

Under System Configuration, click IP Network. The IP Network Properties page appears, where changes to the configuration can be made.

Changes made to the IP network settings will disrupt the configuration session when the new settings are applied. To continue a configuration session after applying new IP settings, close the browser and start a new configuration session.

When IP Settings Change

1. Close the browser.
2. Return to the Spectrum24 CB2000 Device Manager and click Refresh. Select the device and click Configure to start a new configuration session.

   If accessing the UI through a browser, change the workstation IP settings to match the new CB2000 settings and reconnect. Refer to “Using a Browser” on page 22.

IP Network Configuration Settings

View or change the following settings:

- *IP Network Setting*. Use to change the device IP address.

  To obtain an IP address automatically from a DHCP server, click Obtain an IP Address automatically and click Enter. Please note that this setting is for open networks without security restrictions.

  To specify an IP address, click Specify an IP address, enter the IP address parameters, and click Enter.

- *IP Address, Subnet Mask, and Gateway IP Address*. Enter the parameters in the spaces provided and click *Enter*.

2.3.3 Wireless Network

In the Wireless Network Properties page, select radio channel settings, antenna selection, and advanced performance settings. When finished, click Enter or Apply All Changes.

- *Network Mode.* Click Access Point (Infrastructure) to associate with an access point. Click Ad-hoc (Peer-to-Peer) to associate to a networked peer.
- *Wireless LAN Service Area.* Click Attach to any WLAN Service Area (ESSID) to allow the bridge to associate with any access point without specifying the ESSID. In this mode, the bridge uses the ESSID of the access point with the best signal strength. This mode is not available when the network mode is Ad-hoc (Peer-to-Peer).

  Click Specify the Wireless LAN Service Area to allow the bridge to associate only with access points with the same service area. Enter the WLAN service area name or select it from the list. Specify the WLAN service area when the network mode is Ad-hoc (Peer-to-Peer).

To maintain device association, the WLAN service area on a bridge and the access point are required to match. If the bridge is set to specify the WLAN service area and the user changes the access point WLAN service area, make sure to change the bridge WLAN service area.

- *Access Point Privacy Mode.* This mode only applies when the network mode is Access Point (Infrastructure) and should only be used when access points have privacy enabled. Click On to associate with access points set with privacy mode enabled. Click Off to associate with access points set with privacy mode disabled. When privacy mode is on, specify a Wireless LAN Service Area matching the access point service area.
- *Channel Selection.* When the network mode is Access Point (Infrastructure), this option is set to *Automatically select the best channel*, and cannot be changed. The bridge uses the channel the access point is using.

  When the network mode is Ad-hoc (Peer-to-Peer), specify the channel selection as follows:
  - *Automatically select the best channel.* When this option is enabled, the bridge scans the primary channels. If the bridge is establishing a new ad hoc network, it chooses the channel with the least number of packets. If the bridge is joining an existing ad hoc network, it selects the channel in use.
  - *Specify the channel to use.* When this option is enabled, choose a channel from the Channel list.
- *Antenna Selection.* The workgroup bridge contains two internal antennas, used by default (the diversity setting). Select from the following antenna options:

- *Internal.* Uses only one internal antenna (not recommended if an external antenna is connected). Select this option and place the workgroup bridge in a fixed location that provides a steady signal. This setting can be used to improve reception if the signal is not steady with the default Diversity setting.
- *External.* Uses only the external antenna. Select this option when the external antenna is connected.
- *Diversity.* The use of two internal antennas (not recommended if an external antenna is connected). The workgroup bridge switches between the internal antennas dynamically, choosing the antenna with the best signal.

2.3.4 Security Settings

In the Security Settings Properties page, view or change security settings necessary for the CB2000 to operate on the network.

To change security settings:

- Under System Configuration, click Security Settings. The Security Settings page appears. Use this page to select the type of security used on the bridge. The bridge can be configured to support only one type of security at a time. Change the settings by clicking the radio buttons and entering values in the fields. When finished, click Enter or Apply All Changes.

  If configuring through a wireless association (not on the wired LAN) and the user reconfigures both the WLAN service area and the security settings, click Enter to save changes temporarily until finished. After making all system changes, click Apply All Changes.

To maintain device association, the settings on clients and associated access points are required to match.

If applying one set of changes and not the other, the bridge could lose association with one access point before it is configured to associate with another. If this happens, it disrupts network operation for all clients associated with the bridge until resolved.

- *No Security (Open System).* No encryption is used. The network communications could be intercepted by unintended recipients.
- *40-bit Shared Key.* Encrypts the wireless transmissions, but still allows communication among compatible wireless LAN clients and access points from third-party manufacturers that are Wi-Fi certified. *40-bit Shared Key* requires encryption be set in one of the following ways:
  - *String.* Use only with other Symbol Technologies Spectrum24 High Rate Wireless LAN devices. An encryption string is a case-sensitive string of characters between 6 and 30 characters long. To enter the string, click Enter a string to generate shared keys. Then type any combination of letters and numbers in the space provided and click Enter or Apply All Changes.

  - *Shared keys.* Hexadecimal keys are sequences of digits arranged into four keys. A hexadecimal digit could be a letter from A to F or a number from 0 to 9. This type of encryption is compatible with equipment from other manufacturers that use Wi-Fi certified 40-bit encryption. Click Specify shared keys and enter the keys. Click the link *to* specify and select the shared keys. In the shared keys window, enter all the keys in the provided spaces, then click a radio button in the Selected Key column to specify which key to use and click Enter or Apply All Changes.

- *128-bit Shared Key.* This option can be used with other Symbol Technologies Spectrum24 High Rate Wireless LAN devices and with equipment from certain manufacturers supporting 128-bit shared key encryption. 128-bit Shared Key provides a higher level of security than the 40-bit Shared Key option and uses a more complicated encryption scheme.
- *Kerberos.* This option can only be used with other Symbol Technologies Spectrum24 Wireless LAN devices. Kerberos provides an extremely high level of security. See “Kerberos Authentication” on page 11.

  If using Kerberos security, specify Kerberos network parameters. In addition, the client is set for authentication on the Kerberos server. Click To specify the Kerberos login, click here to set Kerberos network parameters.

2.4 Using System Tools

CB2000 system tools provide tools for managing client bridge operation. Tools include: Reset CB2000, Restore Factory Defaults, Upgrade System, Change Administration Password and Backup and Restore CB2000 configurations.

2.4.1 Reset CB2000

If the bridge stops responding, it can be reset. Resetting disrupts the network association temporarily, but does not affect bridge configuration settings already applied with Apply All Changes. (Changes stored in cache memory with Enter are lost in a reset.) To reset the bridge, click Reset.

2.4.2 Restore Factory Defaults

Click Restore to reset the bridge back to factory default settings.

Restoring factory defaults can cause the CB2000 to lose network communication with the workstation. If this occurs, close the browser window and start a new configuration session. Refer to “Gaining Access to the UI” on page 20 for additional information.

2.4.3 Upgrade System

Download firmware and configuration management system upgrades from the Symbol Web site and install those upgrades on the CB2000.

The upgrade procedure requires a Trivial File Transfer Protocol (TFTP) server. The workgroup bridge acts as a TFTP client to receive the download.

To locate an upgrade file and download it to the computer:

1. Log on to the Symbol technologies Web site at http://www.symbol.com/services/downloads/dwnload_spec24_select.htm
2. Select the firmware or software update to match the operating system.
3. Follow the instructions to download the file into a directory on the computer.
4. Copy or move the file to the TFTP server upload/download directory.

To install an upgrade:

1. Use the Spectrum24 CB2000 Device Manager to select the device and launch its configuration or obtain the device IP address and http directly to it. Refer to “Gaining Access to the UI” on page 20.

2. Under Tools, click Upgrade System.
3. Enter the name of the upgrade file downloaded earlier.
4. Enter the IP address of the TFTP server where the upgrade file is located.
5. Click Upgrade. The upgrade file is copied from the TFTP server to the workgroup bridge. The bridge restarts using the new upgrade.

2.4.4 Change Administration Password

The first time the Configuration Management System is launched or after a reset to factory defaults, the user is prompted to set an administrative password. Although a password is not required, Symbol Technologies recommends setting a password to protect against unauthorized access.

After setting the password, enter it each time the configuration is launched for the device. A user name is not required.

To change the administration password:

- Select Tools, click Change Administration Password. The Change Administration Password page appears. Use the Change Administration Password page to change the administration password for the device. Enter the current password and new password in the spaces provided and click Save.

2.4.5 Backup CB2000

As a maintenance operation, save and back up the configurations of individual bridges to reload them in the future. The backup saves all the parameters of the selected bridge in a file. The file can be used later to restore the configuration on this or another bridge.

To backup a CB2000 configuration:

1. Set/verify CB2000 parameters in the System Configuration pages.
2. Under Tools, click Backup CB2000.
3. In the Backup CB2000 Configuration page, click Backup Now.
4. Specify a name and location for the backup. Click OK.

2.4.6 Restore CB2000

After performing system maintenance or after a network malfunction, it can be necessary to restore the CB2000 to a previous known working configuration.

To restore a backup configuration from a file:

1. Enter a file name and backup file location or click Browse and select the backup file to upload to the access point.
2. Click Restore.
   The configuration is restored and activated on the bridge.
   This operation could cause the bridge to reboot.

If the bridge was using an IP address different than the backup, restoring the configuration changes the IP address. To continue:

1. Close the browser.
2. Return to the Spectrum24 CB2000 Device Manager and click Refresh.
3. Select the device and click Configure to start a new configuration session.

2.5 Viewing System Status

CB2000 system status provides information on the Ethernet clients connected to the bridge, wireless communications to the AP, and a summary of system status.

2.5.1 Ethernet Client List

The CB2000 supports up to four clients (computers or printers) and keeps track of the clients with a list of MAC addresses. After the client limit is reached, a user removes an existing client and reset the client in the client list to allow a new client to associate with the network. For example, in a hub configuration with four clients connected, if the user disconnects a desktop computer and connects a new laptop in its place, clear the desktop from the client list to establish network association for the laptop.

To clear the Ethernet Client List:

1. Disconnect a client by unplugging its Ethernet cable from the hub or the bridge.

2. Use the Spectrum24 CB2000 Device Manager to select the CB2000 and launch its configuration manager, or locate the IP address and http directly to the device via a Web browser.
3. Under System Status, click Ethernet Client List.
4. In the Ethernet Client List page, select the radio button next to the client to be removed and click Clear Client List. The bridge erases the client list for the selected client.
5. Connect the new client by plugging its Ethernet cable into the hub or the bridge.
   New clients are added automatically to the list during the next network interaction.

2.5.2 Connection Status

Under System Status, click Connection Status to display information about the quality of the wireless association with the access point. Data rate values (1, 2, 5.5, or 11 Mbps) indicate the speed of data transfer. A data rate of 0 indicates no data transfer. Signal strength values range from 0 (no signal) to 5 (excellent signal quality).

Click Refresh to update the information.

2.5.3 System Summary

Select System Status and click System Summary to display information about the bridge. Navigate the configuration pages by clicking their names in the list, which brings the user to the configuration pages in this section.

Click Refresh to update the information.

Chapter 3 Hardware Installation

3.1 Precautions

Before installing the CB2000 verify the following:

- Do not install in wet or dusty areas without additional protection. Contact a Symbol representative for more information.
- Verify the environment temperature range is between -20° C to 55° C.

Do not connect a workgroup bridge set in Access Point (Infrastructure) mode directly to the LAN (for example, through a wall port). Such a connection could cause a transmission loop between the workgroup bridge and access point, disrupting network operation.

3.2 Package Contents

Before beginning the installation, verify the hardware package contains:

- Spectrum24 CB2000 Client Bridge
- Power adapter and power cord
- Standard Category 5 unshielded twisted pair (UTP) Ethernet cable.
- Spectrum24 CB2000 Software and Documentation CDROM.

Contact the Symbol Support Center to report missing or improperly functioning items.

3.3 Requirements

In addition to the package contents, The following items (which are not included) are also required:

- A workstation with network access to a Wi-Fi compliant wireless LAN access point
  The workstation requires Windows 98/ME/2000/XP and Netscape 4.7 (or later) or Internet Explorer 5.0 or higher.

Windows 95 and NT are not supported. If configuring the CB2000 using a non-Windows computer, see the readme file on the install CD.

- An Ethernet crossover cable to connect the CB2000 to a hub that does not have an uplink (MDIX) port.

3.4 Placing the CB2000

For optimal performance, place the bridge in a dry, clean location near the hub, telephone, computer or printer connected to the bridge. The location is required to have a power source and be within 300 feet (100 meters) of a Wi-Fi compliant wireless LAN access point. The location should be away from transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators or other equipment that could cause radio signal interference.

3.5 Connecting the Power Adapter

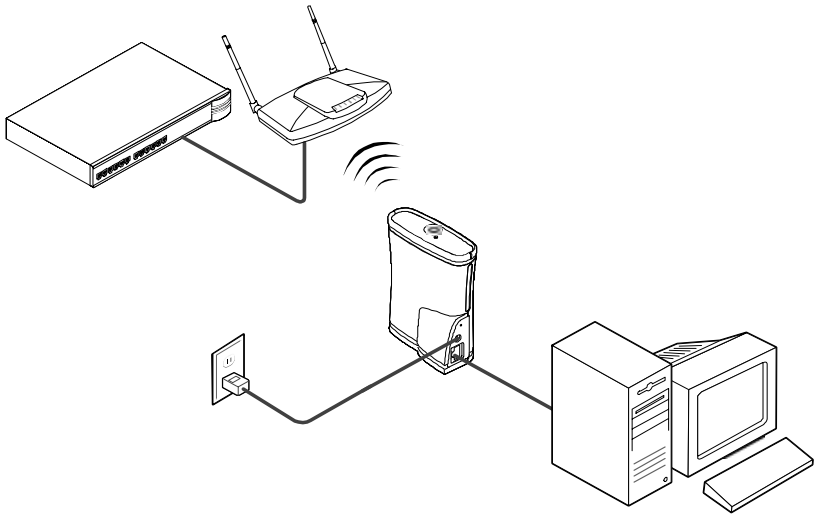
The CB2000 uses a 5 volt 1500mA power supply. Connect the supply to a 100-240 volt, 50-60 Hz power source.

3.6 Connecting the CB2000

The client bridge is designed to be connected to an Ethernet client device such as a hub, telephone, computer, or printer.

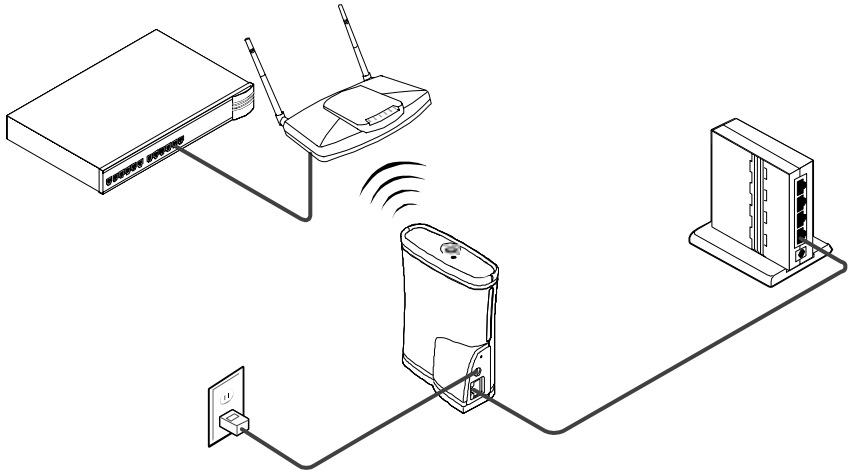
Workstation Connection

Use the workstation connection to initially configure the CB2000 for networks with security features. Connect the CB2000 to a workstation and change default network parameters to allow the bridge access to the network.



Hub Connection

Supply network connections for up to four devices, such as computers and network printers, by connecting the bridge to an Ethernet hub. Use a hub connection to configure the CB2000 in the location it will reside.



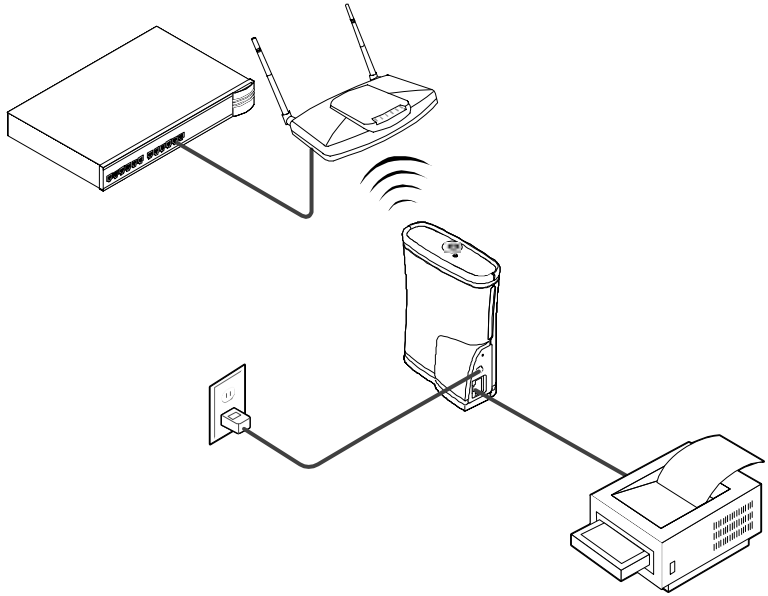
Note

Verify the CB2000 Ethernet cable is plugged into the hub uplink (MDIX) port. If the hub does not have an uplink port, use an Ethernet crossover cable (not provided) which can be connected in any port.

Network Printer Connection

Connect a network printer directly to the bridge or to a hub connected to the bridge. Used this way, network administrators can place network printers in areas that are not wired for Ethernet.

1. Configure the network printer as necessary for connection to the wired LAN. For details on configuring the printer, refer to the documentation shipped with the printer.
2. If necessary, configure the workgroup bridge to associate with the nearest access point. For details, see “Configuring System Parameters” on page 23. Connect the bridge to power in its permanent location.
3. Connect the network printer directly to the bridge or into a hub that is connected to the bridge as shown in Hub Connection.



NBX Telephone Set Connection

Provide converged voice and data services in an office cubicle that is not wired for Ethernet by connecting the bridge and a computer to a NBX telephone.

1. Configure the NBX telephone as necessary for connection to the wired LAN. For details on configuring the telephone, refer to the documentation shipped with the phone.
2. If necessary, configure the workgroup bridge to associate with the nearest access point. For details, refer to “Configuring System Parameters” on page 23.
3. Connect the NBX chassis to the same switch or router to which the access point is connected to.
4. Connect the bridge to power in its permanent location.

5. Connect the telephone directly to the bridge and connect the computer to the telephone.

3.7 LED Indicators

When the bridge is powered, verify its operation through two LEDs:

LED Indicator	Location	Description
Wireless association	On the top of the bridge	*On.* Unit is receiving power. *Off.* Unit is not receiving power. *Blinking.* The unit is transmitting or receiving.
Ethernet connection	At the RJ45 Ethernet connector	*On.* Unit has an Ethernet connection. *Off.* Unit does not have an Ethernet connection. *Blinking.* Wired LAN traffic is detected. Faster blinking indicates heavier traffic.

Chapter 4 CB2000 Device Manager

4.1 Installing the Device Manager

Follow these steps to install the Device Manager on a workstation:

1. Insert the Software and Documentation CDROM in the CD-ROM drive. The setup menu appears. If it does not appear, start the setup menu from the Windows Start menu. For example: Start, Run, D:setup.exe.
2. In the menu, click Install the Tools and Documentation.
3. Follow the displayed instructions to complete the installation. If prompted, reboot the computer.

4.2 Device Manager Interface

The Spectrum24 CB2000 Device Manager provides a useful interface for accessing Spectrum24 wireless devices and launching their configurations in a standard Web browser.

Use the management tool to:

- View Spectrum24 CB2000 devices
- Change CB2000 IP and subnet mask settings
- Launch the Configuration Management System for a selected device.

The interface buttons perform the following functions:

Properties. Displays the following properties of the selected device: Device Name, Device Type, Wireless LAN Service Area (ESSID), IP Address, Subnet Mask, and MAC Address.

Configure. Launches the Configuration Management System for the selected device. If the selected device is on a different subnet, the Pre-IP Configuration Wizard prompts the user to assign an address on the same subnet as the workstation.

Refresh. Scans the network and displays the connected Spectrum24 CB2000 devices.

Choose NIC. If the workstation has more than one network interface card installed, select this button to choose which card to use.

Close. Closes the device manager window and ends the session.

Help. Launches the device manager help page in a browser.

4.3 Pre-IP Configuration Wizard

The Pre-IP Configuration Wizard allows a user to enter a preferred IP and subnet setting or accept a suggested setting for the CB2000. Use this wizard to temporarily access a CB2000 to view or change configuration parameters.

A user can only configure devices on the same subnet as their workstation. To configure a device on a different subnet, a user must first assign it an IP address on the same subnet as their workstation.

When a user selects Configure from the Device Manager and the IP address and subnet settings of their workstation and CB2000 are different, the Pre-IP Configuration Tool launches automatically to facilitate setting new IP and subnet values for the workstation to communicate with the CB2000.

Perform the following to use the wizard:

1. In the Wireless Infrastructure Device Pre-IP Configuration window, accept the suggested settings or change them as required.
   – You can assign a static IP address or specify that the device obtain its IP address from a DHCP server.
2. The next window prompts for an administrative password to allow the new IP address to be set. When the units are shipped from the factory, there is no administration password. Leave the password field blank. If an administration password has been set for the device, enter the password and click Next. The Configuration Management System main page appears in the Web browser.
3. Make changes to the configuration settings as usual.

4. After completing all other changes, do the following:
   - If configuring a new CB2000 for use on a network, click Apply All Changes.
   - If changing or viewing parameters from a workstation and the Pre-IP Configuration Wizard changed the IP and subnet settings for the sole porpose of communicating with the device, click IP Network. In the IP Network page, restore the IP address to its original setting and click Apply All Changes.
5. Close the browser window.

After changing the IP address, the configuration session is disrupted. To continue configuring, follow these steps after closing the browser:

1. Return to the Device Manager window.
2. Click Refresh.
3. Select the device and click Configure.
4. Repeat the procedure for using the Pre-IP configuration wizard.

Chapter 5 Troubleshooting

5.1 Diagnosing Problems

If the Spectrum24 CB2000 is experiencing difficulties, try the following:

Symptom	Solutions
After changing the IP address, restoring a backup configuration, or resetting the bridge to factory defaults, the Configuration Management System stops responding, keeping the user from making additional configuration changes.	Once the IP address is changed and a user clicks Apply All Changes, the CB2000 loses the network connection with the workstation, which is now on a different IP address. To keep this from happening, click Enter to continue configuring the device after changing the IP address. Similarly, restoring a backup configuration or resetting the bridge to factory defaults can change the IP address setting. To recover from this situation and continue configuring the bridge: 1. Close the browser. 2. Return to the Spectrum24 CB2000 Device Manager and click Refresh. 3. Select the device and click Configure to start a new configuration session.
The bridge cannot associate with an access point.	• Adjust the position of the bridge to improve reception. • Launch the bridge configuration and verify the security settings, advanced performance settings, and access point privacy mode settings on the bridge match those on the access point.

Two workgroup bridges cannot communicate in Ad Hoc (Peer-to-Peer) mode.	• Adjust the positions of the bridges to improve reception. • To ensure correct operation in ad hoc mode, the settings on the two bridges must match exactly. Launch the bridge configuration management system and verify the Wireless LAN Service Area, channel selections, Data Preamble setting, and security setting are the same on both bridges.
The wireless network tree does not appear in the Spectrum24 CB2000 Device Manager window.	Verify the correct network adapter is chosen and operating properly. In the device manager window, click Choose NIC. Select the network adapter and click OK.
After upgrading the system, custom configuration settings are lost.	Under some circumstances, upgrading the firmware and the configuration management system forces a return to configuration defaults. In this case, launch the bridge configuration and reconfigure the settings.

Appendix A Specifications

A.1 Physical Characteristics

Height: 109 mm (4.29 in)

Width: 82 mm (3.24 in)

Depth: 39 mm (1.52 in)

A.2 Environmental Operating Ranges

Temperature: 0 to 40°C (32 to 104°F)

Humidity: 10 to 95% non-condensing

A.3 Network Characteristics

Driver Support: NDIS v4.0 and v5.0

Ethernet Frame: DIX, Ethernet_II and IEEE 802.3

Filtering Packet Rate: 14,400 frames per second filtering and forwarding

Ethernet Connection: 10/100Base-T (AP-4131 model access point only)

SNMP s24dsap.mib, MIB-II and 802.1x.mib

A.3.1 Features

- Embedded HTTP Web management server in each access point works with any Web browser that supports HTML and Javascript
- Remote configuration capable.

A.3.2 Protocol Support

- TCP/IP
- IPX
- NetBEUI
- DHCP.

A.3.3 Security

- 40-bit WEP and 128-bit (shared and session key) encryption
- Kerberos

A.3.4 Standards Conformance

- IEEE 802.11b High Rate
- IEEE 802.11
- IEEE 802.3
- IEEE 802.1d
- HTTP

Appendix B Customer Support

Symbol Technologies provides its customers with prompt and accurate customer support. Use the Symbol Support Center as the primary contact for any technical problem, question or support issue involving Symbol products.

If the Symbol Customer Support specialists cannot solve a problem, access to all technical disciplines within Symbol becomes available for further assistance and support. Symbol Customer Support responds to calls by email, telephone or fax within the time limits set forth in individual contractual agreements.

When contacting Symbol Customer Support, please provide the following information:

- serial number of unit
- model number or product name
- software type and version number.

B.1 North American Contacts

Inside North America, contact Symbol by:

- Symbol Technologies, Inc.
  One Symbol Plaza Holtsville, New York 11742-1300
  Telephone: 1-631-738-2400/1-800-SCAN 234
  Fax: 1-631-738-5990
- Symbol Support Center (for warranty and service information):
  - telephone: 1-800-653-5350
  - fax: (631) 563-5410
  - Email: support@symbol.com

B.2 International Contacts

Outside North America, contact Symbol by:

- Symbol Technologies
  Symbol Place
  Winnersh Triangle, Berkshire, RG41 5TP
  United Kingdom
  0800-328-2424 (Inside UK)
  +44 118 945 7529 (Outside UK)

B.3 Web Support Sites

MySymbolCare

http://www.symbol.com/services/msc

Symbol Services Homepage

http://symbol.com/services

Symbol Software Updates

http://symbol.com/service/downloads

Symbol Developer Program

http://software.symbol.com/devzone

Symbol Knowledge Base

http://kb.symbol.com

B.4 Additional Information

Obtain additional information by contacting Symbol at:

- 1-800-722-6234, inside North America
- +1-631-738-5200, in/outside North America
- http://www.symbol.com/