

Cisco Building Broadband Service Manager Technical Overview



Abstract

Cisco Building Broadband Service Manager (BBSM) is a service management gateway that helps service providers deploy, market, and operate broadband services for building network deployments. It is a proven server-software solution that provides plug-and-play access, authentication, end-user self provisioning, billing, tiered services, and Web-based reporting for buildings such as hotels and multi-dwelling units (MDUs).

Cisco BBSM enables end users to access broadband services. Many service providers now deploy broadband network connections to multiple users in buildings such as hotels, apartments, office facilities, and airports.

Broadband networks that meet the demands of mobile computer users require a solution that can control access, support mobile-user connections, collect connection fees, display user-specific content, and report on system use. Service providers must have the ability to deliver these services in a variety of public locations with a variety of access rules, costs, and content based on where the user is within the property.

Cisco BBSM meets service provider and building owner requirements for in-building network control. It controls user access to broadband services and provides a wide range of payment options, including charging to a hotel guest room folio, providing access for subscribers using remote access dial-in user service (RADIUS) authentication, or charging access fees to a credit card. Cisco BBSM can deliver different speed connections for specific revenue models and deliver content that is relevant to users when they connect to a high-speed network. Cisco BBSM can be deployed with a wide range of Cisco networking products to create a complete solution for building service delivery.

The Cisco BBSM system is similar to Cisco Service Selection Gateway (SSG), which is deployed at a central office to manage thousands of individual broadband access accounts. It is available on the Cisco 6400 platform and offers Web-based authentication, multiple service provider selection, and a rich set of physical interfaces and protocols. Cisco BBSM is a Windows 2000 software-based software platform for building broadband applications. It offers plug-and-play Internet access, self-service provisioning, authentication, local Web portals, tiered bandwidth/pricing, and it interfaces to all major hotel billing systems.

Cisco BBSM, however, is more focused on providing an easy-to-use end-user experience that can be easily customized with different portals/branding, billing options, pricing, tiered service levels. It also has many features designed to assist in the deployment and operation of building broadband networks SSG is a more industrial-strength product that supports service selection from multiple providers.

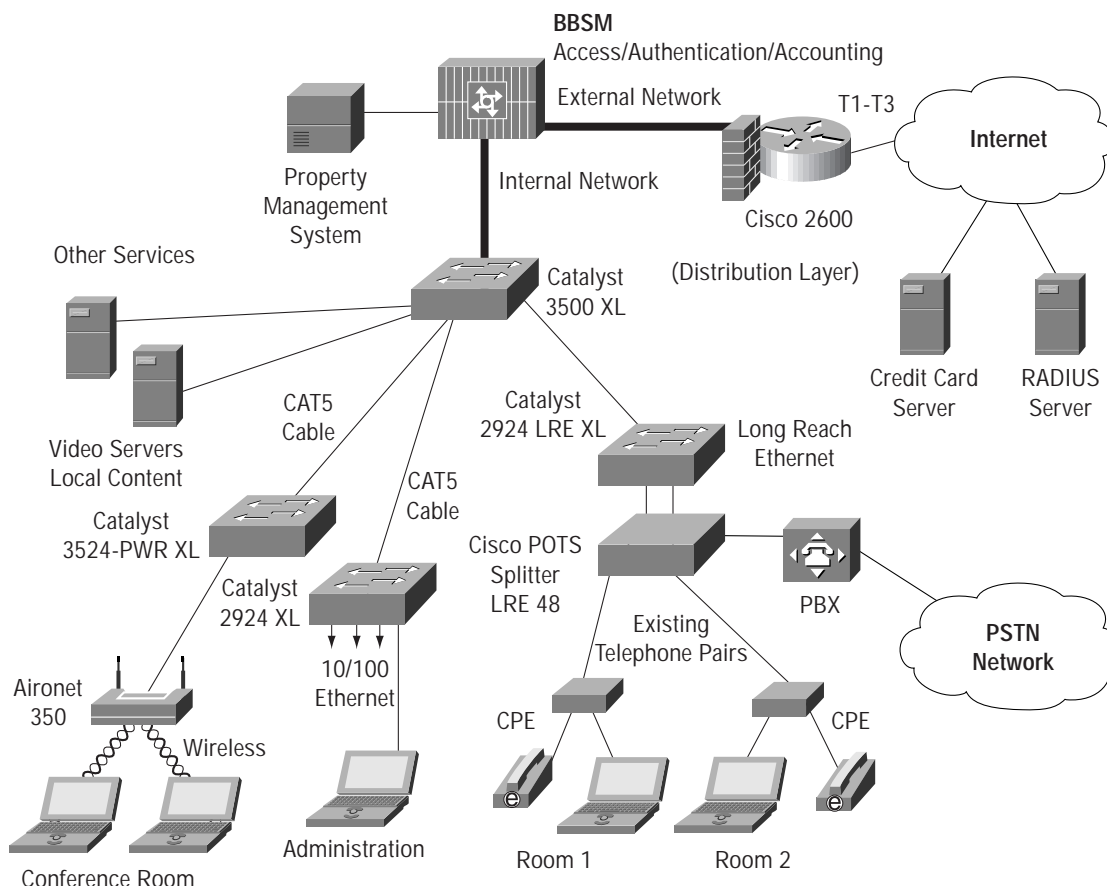
This paper describes a typical broadband building network and how Cisco BBSM effectively manages the complete solution.



Cisco BBSM Manages the Broadband Building Network

Today's building networks require a complex combination of multiple technologies to deliver broadband services to end users. Service providers are pushing higher-and higher-speed bandwidth to the network edge. Many types of buildings; hotels, apartments, office buildings, airport concourses, even cruise ships benefit from the availability of T1, T3, and higher-speed network connections. As high-speed connections become universally available, service providers need to provide an effective solution for managing the provisioning and delivery of broadband services to building occupants.

Figure 1 Typical Cisco BBSM Building Network



Cisco BBSM manages the delivery of broadband services and all network components required for broadband services delivery. Cisco BBSM is a software application that works with a general-purpose operating system and database platform that interact with policy servers as well as intelligent network devices to manage service delivery. Cisco BBSM allows service providers to deliver specific policies to each network access port where users connect. These policies, available on a per-port, per building, or per-user basis, include:

- Multiple access methods; Ethernet, wireless, Long Reach Ethernet (LRE), DSL, cable
- Multiple authentication methods; port based, RADIUS, prepaid accounts
- Multiple payment methods; charge to property management system, credit card, RADIUS account, access codes
- Multiple portal options; forced portal, "walled-garden," free access, custom connect screens
- Multiple bandwidth options; multiple limited bandwidth options



Cisco BBSM essentially combines all network access control and management functions normally contained in multiple servers into one compact management device sized for deployment in the building network environment.

The Cisco BBSM server in Figure 1 is the unifying agent that integrates the multiple in-building technologies into a complete solution. The Cisco BBSM server manages several key functions:

- **Access**—Cisco BBSM enables user access regardless of their network interface configurations. Computer users in conference or guest rooms can connect to the network using Ethernet or wireless interfaces configured for Dynamic Host Configuration Protocol (DHCP or static IP addressing methods. This plug-and-play capability enables access to the greatest number of mobile users.
- **Authentication**—Cisco BBSM supports multiple authentication methods. These methods include automated authentication and granting access to users in hotel guest rooms based on identifying the room the guest connects from. Other methods include RADIUS authentication to either local or remote RADIUS servers for prepaid users or service subscribers.
- **Accounting**—Cisco BBSM accounts for usage and collects payment using multiple methods, including:
 - Direct posting of charges to a hotel property management system (PMS) for users connecting from guest rooms
 - Charge processing by a remote credit card processing service; this enables payment from any location on a property
 - Subscribers or prepaid users can authenticate via RADIUS and pay through offline methods
 - Meeting room attendees can use broadband access paid for via access codes

PMS interface and credit card billing also enable “impulse” charges for additional bandwidth or future value-added services. Billing can be based on full-day or time-block increments.

- **Portal**—Cisco BBSM redirects all users through two steps during connection. First, they are directed to a Connect Screen, which explains the services available to them, including potentially multiple bandwidth and price options; Walled Garden free access areas, such as local sites, advertising, or weather; and a link to the hotel or property owners’ home page. Once users select and purchase service, they are directed to a portal page as their first location on the Internet. This provides a second branding and marketing opportunity. With the Walled Garden feature a property could allow free browsing (pre-authentication) of a single network of Web servers. The Cisco BBSM server includes a “transparent proxy” feature, which allows the service provider to force all Web requests to the Internet to go through the Microsoft Proxy Server installed with Cisco BBSM—without requiring the client computers to configure a proxy in their Web browsers. This feature is useful when logging is turned on in the Microsoft Proxy Server application, which allows the software to capture a list of Web sites. Marketing staff can later mine this information to determine popular Web sites frequented by hotel guests or apartment tenants.
- **Network Buildout and Configuration**—Cisco BBSM includes multiple features designed to support network installation, configuration, and testing. These features are important to ensure effective deployment of broadband building networks. Features include switch discovery; enforced line testing to ensure ports can not be mapped until the connection meets quality standards; and a limited set of local network performance monitoring tests to enable proactive quality assurance.

The Cisco BBSM is a dual-homed server. The Internal Network (see Figure 1) connects to all network devices within the property. In most installations, the Cisco BBSM Internal Network connects to an aggregation switch that is part of the building distribution network. In Figure 1, this function is provided by the Cisco Catalyst® 3500 Series XL Switch. The External Network connects to the broadband Internet connection used to deliver services to the property.



Works with All Form of Building Area Networks

The Catalyst 3500 switch connects to a range of different networking solutions in the property. The link to the lower left connects to a Catalyst 3524-PWR XL switch. This switch connects to Cisco Aironet® 350 wireless access points that deliver wireless network connections to end users in a conference room. The Cisco BBSM server, as part of the network installation process, “discovers” the wireless access capabilities of the building network and configures the Cisco BBSM network for management of wireless connections from these access locations. Wireless connection users in the conference room can connect to local content available on the property, to the Internet, or to their corporate offices using a virtual private network (VPN).

The second CAT 5 branch from the Catalyst 3500 switch connects to a Catalyst 2900 Series XL switch. This switch delivers Ethernet connections to other building locations such as meeting spaces, public areas, or administrative areas. Each switch port can provide different policies for user connection. For example, computers in the administrative area can be granted free access and upon connection can be redirected to corporate intranet portal. Users connecting in meeting rooms could be challenged to enter a pass code for a prepaid connection authorized by the Cisco BBSM meeting room management feature.

The right branch from the Catalyst 3500 switch connects to the Catalyst 2924 LRE XL switch. The Cisco LRE switch delivers up to 15 Mbps of symmetrical Ethernet bandwidth to a distance of up to 5,000 feet over existing telephone wiring in the building. The Plain Old Telephone Service (POTS) splitter illustrated under the LRE switch combines analog telephone signals from the private branch exchange (PBX) system with the LRE data and sends the combined signal to the guest room. The guest room connection is terminated with the Cisco 575 LRE customer premises equipment (CPE), which provides an Ethernet connection for the user's computer in the room and a connection for the room telephone. The Cisco BBSM server manages the user connection in the guest room and applies all per-port policies described above, allowing the service provider to deliver different levels of service and connection experiences, even on a room-by-room basis. When an end user connects in the guest room, the Cisco BBSM server automatically detects the user connection, detects which port (room) the user is connected to, and uses this information to select, from the Cisco BBSM database, the policies that will be applied to this connection session.

The distribution layer network (Catalyst 3500 in the diagram) should be sized to support nonblocking delivery of the full-bandwidth capacity of the access-layer networking devices. This supports the delivery of additional services over the existing network. The “Other Services” illustrated on the left side of Figure 1 include examples for delivering video services or other local content. The bandwidth and packets produced by the “Other Services” do not transit through the Cisco BBSM server. The only packets processed by the Cisco BBSM server are the Ethernet packets required for high-speed Internet access delivery to end users connected to network access ports.

The Cisco BBSM provides multiple services for network management, which are discussed in detail later in this paper. The most important function from a network design standpoint is Ethernet packet routing from the internal network to the external network. The Cisco BBSM acts as a gateway, allowing only authorized packets to transit from the internal to external networks. Cisco BBSM determines which end-users packets are allowed to reach the external network based on whether the user is authorized for connection to the Internet (normally this means they have paid for access). Before authorization, users are restricted to accessing local content or the portal pages provided by the Cisco BBSM, which include opportunities to pay for network access.

The external network illustrated in Figure 1 accesses the Internet through a low-end router, typically a Cisco 2600 or 3600 router. The building network solution will use the router's firewall services.

The standard Cisco BBSM is designed to manage network access distribution for up to T3 (45-Mb) connections. Most Cisco BBSM installations manage bandwidth ranging between T1 and T3 speeds.



Cisco BBSM may also interact with network components outside the building. These components include a credit card server for real-time processing of credit card payments for network access and RADIUS servers for authenticating users with subscription or prepaid service agreements.

Cisco BBSM posts charges to the property management system for user access ports configured to charge payment for access directly to the guest folio. The Cisco BBSM billing application tracks session connections and reports usage to the one-way property management system (PMS) through a direct serial cable connection. Cisco BBSM supports the following PMS systems:

- Bell HOBIC PMS protocol
- Protocol Technologies (Bell HOBIC)
- MSI (Bell HOBIC)
- Promus 21 (Bell HOBIC)
- Encore (Bell HOBIC)
- Logistics (Bell HOBIC)
- XIOX, Fidelio 6.0
- Hilton H1, Hilton H2

If a hotel uses a nonsupported PMS system, it can either develop an interface to the Cisco BBSM PMS application programming interface (API) or print the charge to a local printer located at the front desk and manually enter the charges into a PMS.

Cisco BBSM Architecture

Cisco BBSM is a software application built on the Windows 2000 Server platform with the Microsoft Proxy Server installed. Cisco BBSM uses a data engine as a repository for configuration and policy information. The combination of Windows 2000, Proxy Server, and the data engine give Cisco BBSM the flexibility required to deliver a rich, customized connection experience to each network user.

Cisco BBSM is a flexible platform for advanced service management. The standard Cisco BBSM product manages a wide range of in-building networking equipment to enable service delivery to customers. Cisco BBSM includes APIs that can be extended by the service provider to support new network hardware solutions, as well as create new accounting and billing methods. It also allows buildings to interface with different payment processing systems and to create customized graphical user interfaces to control customer interaction with a broadband network.

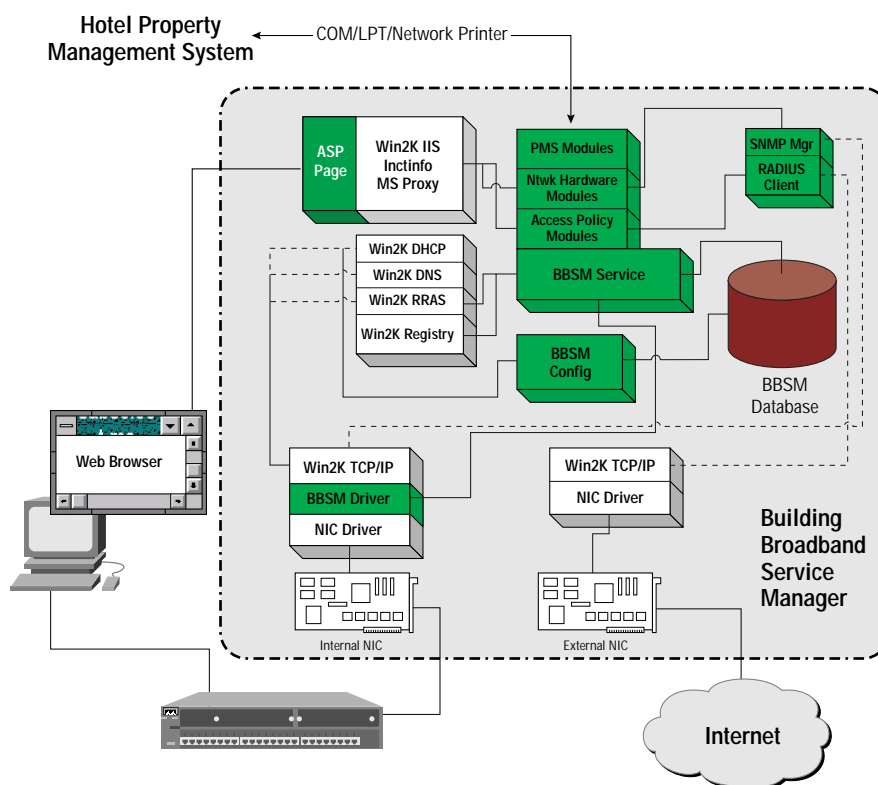
When users boot their computers, if the computers are configured for DHCP, the DHCP server provides a DHCP lease (Figure 2).

The Cisco BBSM software inspects network traffic on the Cisco BBSM Internal Network (Figure 2). If the user's computer is configured for static IP addressing, the Cisco BBSM software analyzes the user's packets and performs network address translation (NAT) and other low-level network translations. These translations allow the user to connect to the network using the intelligent network devices.

Cisco BBSM has an internal Web server that interacts with the user during the connection process through the user's Web browser. In effect, the user's Web browser is the "dialer" for connecting to the broadband building network. The user's browser is redirected to a Web page generated by the J-script/ASP function. The content, appearance, and options presented to the user during the connection process are controlled by data managed by the Cisco BBSM Core and the data engine.



Figure 2 Cisco BBSM Architecture



When the user first attempts to connect through a browser, the Cisco BBSM software detects the network traffic. Cisco BBSM uses simple network management protocol (SNMP) to query the intelligent network devices to detect the network access port the user is connected to, for example, an Ethernet switch port, a wireless access point, and so on. The Cisco BBSM core uses the port identification information returned by the SNMP query to select the port-specific connection parameters from the data engine for the set of policy parameters to be applied to the user's session. This includes the parameter that defines the Active Server Page (ASP Web page) used to drive the users forced portal Web page. Every access port to the network can have different connection parameters and a different connection experience (the ASP Web page defines the session initialization experience). These connection parameters are the input to the COM objects and J-script/ASP functions that are executed on the server and display the welcome information on the user's Web browser.

The user interacts with the Web pages delivered by Cisco BBSM to initiate a connection to broadband services. This interaction can include agreeing to pay for service in a hotel room and pay for the services on the room bill. In this case, the PMS module (Figure 2) posts a charge to the property management system. In a public area of the property, the user may initiate a wireless connection to the network may be asked to pay using a credit card. In this case, the credit card module accepts credit card information from the Web page generated for the user and processes the transaction. In other cases, the user may have a subscription for broadband services and would use RADIUS to authenticate using a centralized RADIUS database.



The user may select different service levels; such as 128k or 512k maximum connect speeds. In some cases, the service level may be specified in data (RADIUS attribute) returned from the RADIUS database. In all cases, a service provider has a large amount of flexibility in creating customized services for each user and each network access port. This flexibility is provided by the Cisco BBSM data engine, the use of Web pages to interact with the user, and the flexibility of the Cisco BBSM architecture.

After the user has agreed to pay or has been authenticated as a subscriber to the broadband service, the Cisco BBSM software causes the Windows 2000 Routing and Remote Access Service (RRAS) to open a filter from the Cisco BBSM Internal Network (see Figure 1). This filter allows access to the Cisco BBSM external network to enable the user's broadband connection. From this point, the user may use any protocol or network application enabled by the property firewall to connect to the Internet. This includes VPN connections, voice over IP (VoIP), streaming audio and video content, file transfer protocol (FTP), simple mail transfer protocol (SMTP) mail, hypertext transfer protocol (HTTP), and so on.

Cisco BBSM provides continuing services for users for the duration of their connections. These services include a very specialized version of Network Address Translation (NAT) for users whose computers were configured for static IP addresses, DNS services, bandwidth throttling (to limit bandwidth for users to their subscribed maximum service level), and Web proxy services.

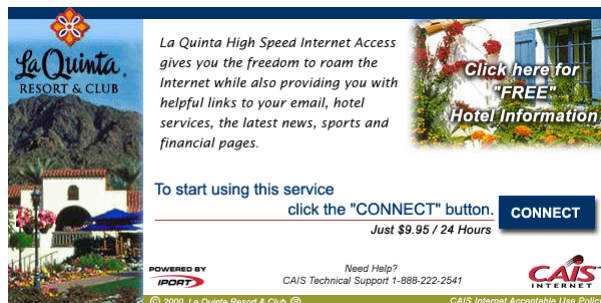
When the network user disconnects from the network, Cisco BBSM detects the disconnection and terminates the connection.

Cisco BBSM Web Page Construction

The Cisco BBSM's ASP Web pages drive the session authentication and accounting policy implemented for each user. The Cisco BBSM system was designed to allow service providers to customize the Web pages and design a unique user experience according to the target business model. For example, the Cisco BBSM meeting room feature is just a set of Web pages designed using the access code authentication model for Cisco BBSM. It allows a hotel event manager, for example, to sell access codes at a throttled bandwidth from one set of admin Web pages. The end user in the meeting rooms is asked to authenticate from another set of Web pages. All the Web pages use the Cisco BBSM library of COM objects to drive the meeting room functionality. Other possible applications that service providers can design in a Web-based environment include Internet cafes, university dormitory rooms, even time-share condominiums. With a variety of accounting and billing models available, the Cisco BBSM system becomes a powerful Web-based platform from which to drive more services.



Figure 3 Sample ASP Page for various MxU Properties



Sample BBSM Connect pages created for Hotels or

Cisco BBSM Administration

The Cisco BBSM server is managed remotely using Web-based user interfaces. These interfaces give remote administrators complete control over operation and allow the collection of detailed statistics on system use. Transaction reports and other information are presented in a Web-based format to allow for remote management of the Cisco BBSM system.

In addition to the Web-based interface, the Microsoft Windows 2000 Server operating system provides an optional Telnet service, which could be enabled by customers. The operating system provides a rich environment of command-line interface utilities to manage a server. The Cisco BBSM server is shipped with a version of PERL to allow service providers to create PERL scripts to help automate some of the management functions.

Cisco BBSM Installed in a Central Location

The Cisco BBSM server can be installed in a central location in a cluster of buildings and provide service for a group of buildings rather than a single building. Each building is configured as a “site” in the Cisco BBSM system, and separate policies and Web pages can be created for each site (building). Many service providers desire to configure Cisco BBSM in a redundant fashion to minimize network downtime in the event of a failure. Figure 4 represents a typical Cisco BBSM redundant configuration.

For hotel properties, the Cisco BBSM server’s “site controller” feature allows a remote PC installed in a hotel to connect to the serial port of the hotel property management system. This PC serves as an IP/serial gateway to allow the central Cisco BBSM server to post charges to the local hotel property management system.



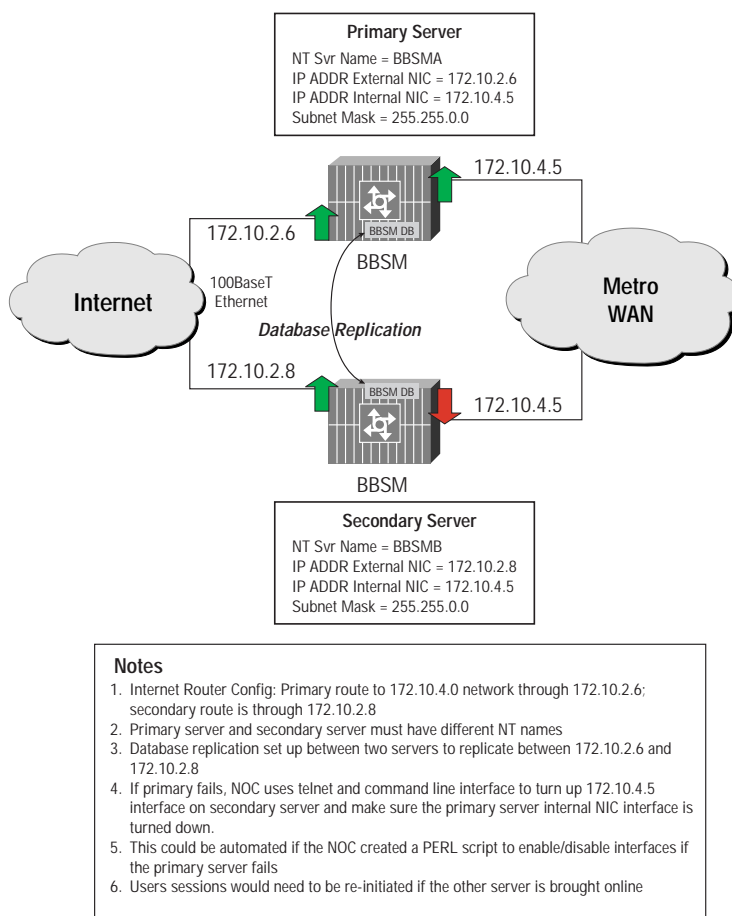
Cisco BBSM Security

The Cisco BBSM software operates on the Windows 2000 server operating system. The default configuration is shipped to customers with configured settings to ensure enhanced security of the server system. Microsoft Networking (File and Print Sharing, Local NetBIOS) is disabled on both interfaces of the Cisco BBSM server (to the WAN and LAN). This means that locally (from client to server), only a few ports available on the Cisco BBSM system are open to a client connection.

The internal building network equipment must be configured to prevent one hotel/apartment room from searching another room's packets. This also ensures attacks do not occur between client computers and the unauthorized searches of authentication information during session initiation. The port-to-port security should be implemented between client to switch and switch to network. The switches should also implement storm controls with rising and falling thresholds. VLANs are another secure way of implementing added security in a building area network.

The Cisco BBSM Server can also be configured with additional static routing filters to provide security for broadcasts, turning off services for applications not implemented (SMTP), and implementing a secure encrypted remote control application for remote management. The router installed on the property should also be configured with access control lists and broadcast thresholds.

Figure 4 Redundant Server Configuration for BBSM



Implementing many of these features requires a more detailed level of installation expertise and configuration management. A combination of optimal settings on all the network equipment provides both security and manageability for service providers.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia
Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru
Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa
Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems Logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0108R)