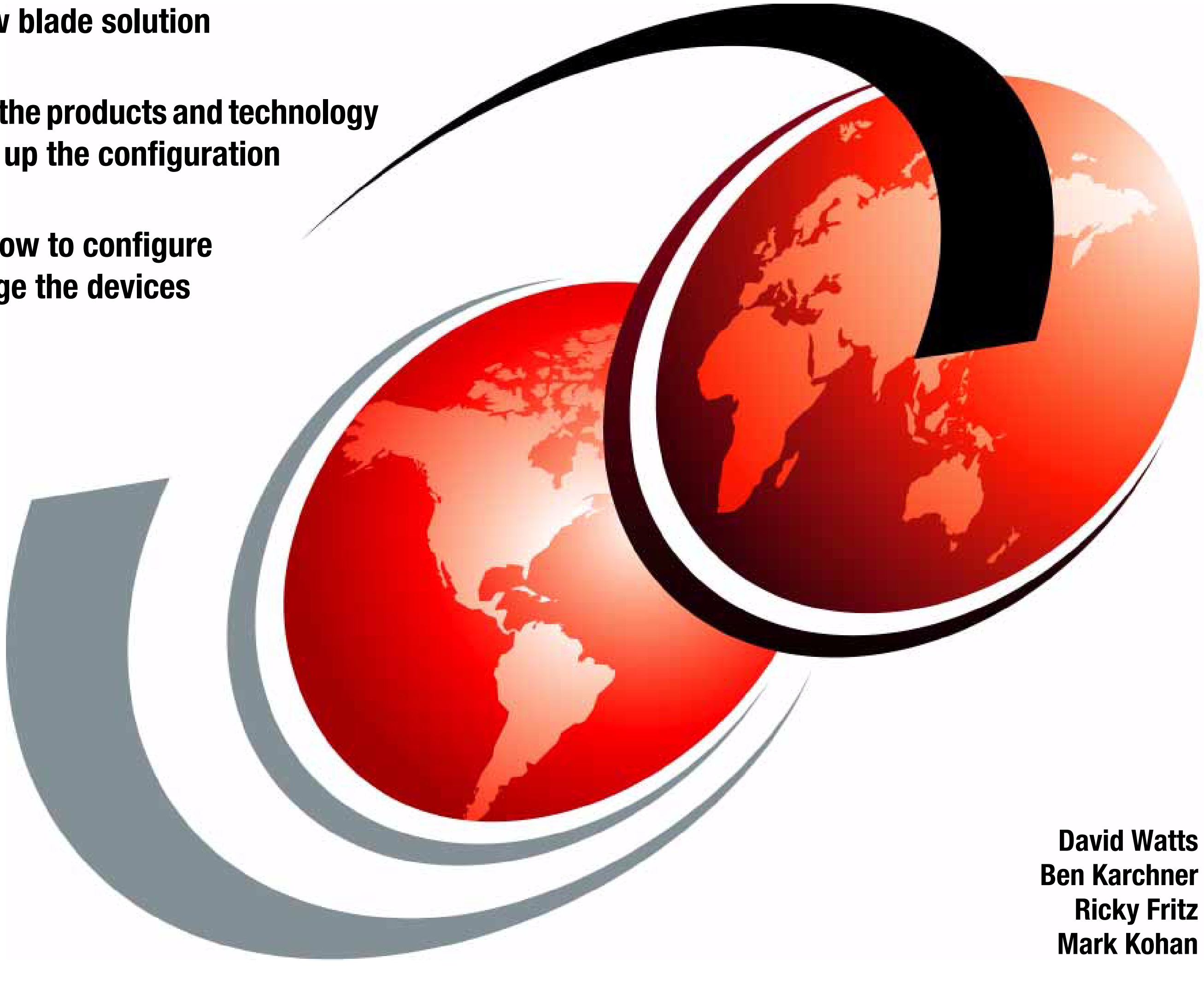
Implementing the IBM BladeCenter HC10 Workstation Blade

Introduces the concepts and benefits of this new blade solution

Describes the products and technology that make up the configuration

Explains how to configure and manage the devices



David Watts
Ben Karchner
Ricky Fritz
Mark Kohan

Redpaper

ibm.com/redbooks

International Technical Support Organization

Implementing the IBM BladeCenter HC10 Workstation Blade

March 2008

REDP-4331-00

Note: Before using this information and the product it supports, read the information in "Notices" on page vii.

First Edition (March 2008)

This edition applies to the IBM BladeCenter HC10, machine type 7996, based on Version 17 of the CP20 and HC10 compression card firmware.

This document created or updated on March 19, 2008.

Note: This book is based on a pre-GA version of a product and may not apply when the product becomes generally available. We recommend that you consult the product documentation or follow-on versions of this book for more current information.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Redbooks (logo) ®
BladeCenter®
Calibrated Vectored Cooling™
IntelliStation®
IBM®
PowerExecutive™
Predictive Failure Analysis®
Redbooks®
RETAIN®
System x™
Tivoli®
Wake on LAN®

The following terms are trademarks of other companies:

PCoIP, PC-over-IP, Teradici, and the Teradici logo are trademarks or registered trademarks of Teradici Corporation in the United States, other countries, or both.

QLogic, and the QLogic logo are registered trademarks of QLogic Corporation. SANblade is a registered trademark in the United States.

InfiniBand, and the InfiniBand design marks are trademarks and/or service marks of the InfiniBand Trade Association.

Brocade, and the Brocade logo are trademarks or registered trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries.

Active Directory, ESP, Internet Explorer, Microsoft, Windows Vista, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel Core, Pentium, Pentium 4, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

The IBM® BladeCenter® HC10 is a new blade offering for the BladeCenter family. The HC10 is a way to implement high-performance user computing without the noise, heat, and space issues that are associated with running a powerful workstation under your desk.

The HC10 provides server-based computing technology for workstation applications by offering high security and manageability, while delivering outstanding graphics performance and full USB capability. Built-in features are ideal for engineering design applications, trading floor and other financial applications, Geographic Information Systems applications, distance collaboration, and more.

The HC10s architecture is based on the Intel® Core 2 Duo desktop platform rather than a server chipset, ensuring performance characteristics suited to a power user. The system is certified with the Microsoft® Windows® Logo Program, ensuring maximum compatibility with Microsoft Windows applications.

This paper describes the technology and design of the IBM BladeCenter, the IBM BladeCenter HC10 workstation blade, and the IBM CP20 Workstation Connection Device that is placed on each user's desk where the monitors and USB devices are attached. The paper describes the planning steps needed to implement an HC10 solution and includes chapters on how to implement a connection broker to manage how the CP20s connect to the HC10s. It also includes a complete description of the configuration options and management interfaces.

This paper is for customers, IBM Business Partners, and IBM employees who want to understand how the HC10 solution is designed and implemented.

The team that wrote this paper

This paper was produced by a team of specialists from around the world working at the IBM International Technical Support Organization (ITSO), Raleigh Center.

David Watts is a Consulting IT Specialist at the IBM ITSO Center in Raleigh. He manages residencies and produces IBM Redbooks® publications on hardware and software topics related to IBM System x™ and BladeCenter servers and associated client platforms. He has authored over 80 books, papers, and technotes. He holds a Bachelor of Engineering degree from the University of Queensland (Australia) and has worked for IBM both in the U. S. and Australia since 1989. He is an IBM Certified IT Specialist.

Ricky Fritz is an IBM System x and IBM BladeCenter subject matter expert working for the IBM Sales and Distribution Techline organization in Atlanta, Georgia. He has more than 20 years of IT industry experience beginning with the U. S. Air Force Electronic Security Command and then stints in sales with Microsoft and Ingram Micro, and sales management with Compaq. He has more than 10 years with IBM supporting System x and BladeCenter sales and solutions. His areas of expertise include digital media solution design and virtual client infrastructure (desktop) solutions. He is an IBM Accredited IT Specialist and IBM Certified System x and BladeCenter Technical Sales Specialist.

Ben Karchner is an undergraduate student at Pennsylvania State University. He is currently working towards a BS degree in Information Sciences and Technology. His main focus is on the integration and application of information technology. He joined the IBM ITSO as a Co-op Pre-professional IT Specialist.

Mark Kohan is Field Technical Support Specialist working for IBM in Hungary.

The team (left to right): David, Ben, Ricky, and Mark

Thanks to the following people for their help with this project:

From the IBM ITSO:

- Carolyn Briscoe
- Linda Robinson
- Margaret Ticknor
- Jeanne Tucker
- Erica Wazewski
- Debbie Willmschen

From IBM Corporation:

- Richard Brothers
- Markesha Farmer
- Jordan Hibbits
- Makoto Ono
- Charles Perkins
- Stephen Poe
- Junjiro Sumikawa
- Ed Suffern
- Shawn Walsh

From Devon IT, Inc:

- Bill Horrocks
- Ian Geiser
- J. Adam Knudsen
- Paul Mancini
- Stephane Verdy

From Leostream:

- David Crosbie

From Teradici™ Corporation:

- Kurt Fennig
- Ziad Lammam
- Chris Michael
- Andrew Preston
- Ken Unger
- Brian Zingle

Other people who have graciously helped us:

- Nick Pellegrene, Pennsylvania State University

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

1

Introduction to BladeCenter

This chapter provides an introduction to the IBM BladeCenter. We discuss features of the BladeCenter chassis and of the blade servers, workstations, and networking options. We also discuss how the BladeCenter's flexible, adaptable, modular design has revolutionized the blade market since its announcement in 2002.

Topics that we cover in this chapter include:

- 1.1, "BladeCenter chassis" on page 2
- 1.2, "System management" on page 9
- 1.3, "Overview of blade servers and blade workstations" on page 13
- 1.4, "Networking options" on page 15

1.1 BladeCenter chassis

A blade server is an independent server with its own processors, memory, storage, network controllers, operating system, and applications. These blades are housed vertically in a *chassis*, called IBM BladeCenter, like books on a bookshelf.

Blade servers are the fastest growing server market segment due to the following major benefits:

- Density

  The physical orientation of blades and modules within the enclosure (chassis) results in very efficient use of space, generally yielding server densities greater than traditional-form-factor servers. Blade servers can provide rack densities several times greater than those obtained using traditional-form-factor servers.

- Cable management

  As the number of traditional-form-factor servers increases, the numbers of cables that are required for power, management, networking, keyboard, video, mouse, and so forth increase linearly. A typical full industry-standard rack of standard 1U servers can require as many as several hundred cables. A full rack of server blades can require as few as a couple of dozen cables, resulting in increased reliability, reduced complexity, and reduced cost.

- Setup and configuration cost

  Fewer chassis and less mounting hardware reduce several undesirable dimensions of server management. These include the time that is required to build and configure a rack of servers, the opportunity for error, and the skill level that is required to perform setup and configuration. This translates to savings for the supplier on preconfigured racks and for custom configuring within data centers.

- Infrastructure integration

  Traditional data center infrastructures have been characterized by physically separate boxes for servers and for networking and storage area network (SAN) gear. Server blade architectures can embed networking and SAN switches into the chassis. After *physical integration* is achieved, a platform for operational and administrative integration is established for seamless quality of service throughout the network and server and for a single systems management view of server, network, and storage.

- Reliability, availability, and serviceability

  In contrast to traditional rack-mounted servers, a server blade node can be replaced without the use of tools to manipulate mounting hardware and with no need to remove cables. A server blade can be removed by simply opening the chassis bezel and releasing a locking mechanism. In addition, server blades have accessibility to *hot-swap* components, which are not easily accessible for many rack-mounted 1U-form-factor servers. The server blade design also allows for simpler network and disk I/O component access and easier servicing and upgrades of switches within the chassis.

- Cost

  The contents and structure of the server blade chassis can result in lower effective cost of additional server nodes as node density increases. This lower cost is due to *node amortization*, which means that the costs of chassis frames, backplane, power supplies, fans, CD, diskette drive, and other I/O are shared and amortized. In addition, substantial electrical power savings are realized over traditional rack mount servers.

- Flexible function and technologies

  Replaceable processor blades and other modules, such as network routers, SAN switches, and power suppliers, provide customers with the opportunity to easily benefit from new and alternative technologies without replacing the entire server system. This flexibility keeps the chassis useful, providing protection against obsolescence.

The BladeCenter chassis allows individual blades to share resources, such as power supplies, fans, and switches, as well as an optical drive, USB, serial ports, and management interfaces. These resources are shared by the blades that are housed in the chassis. Up to 14 blade servers or workstations can be installed in the blade bays on the front of the chassis (see Figure 1-1). This sharing of resources allows for easy blade management and improved performance by increasing the rack density. The BladeCenter provides complete redundancy in a chassis and enables network and storage integration.

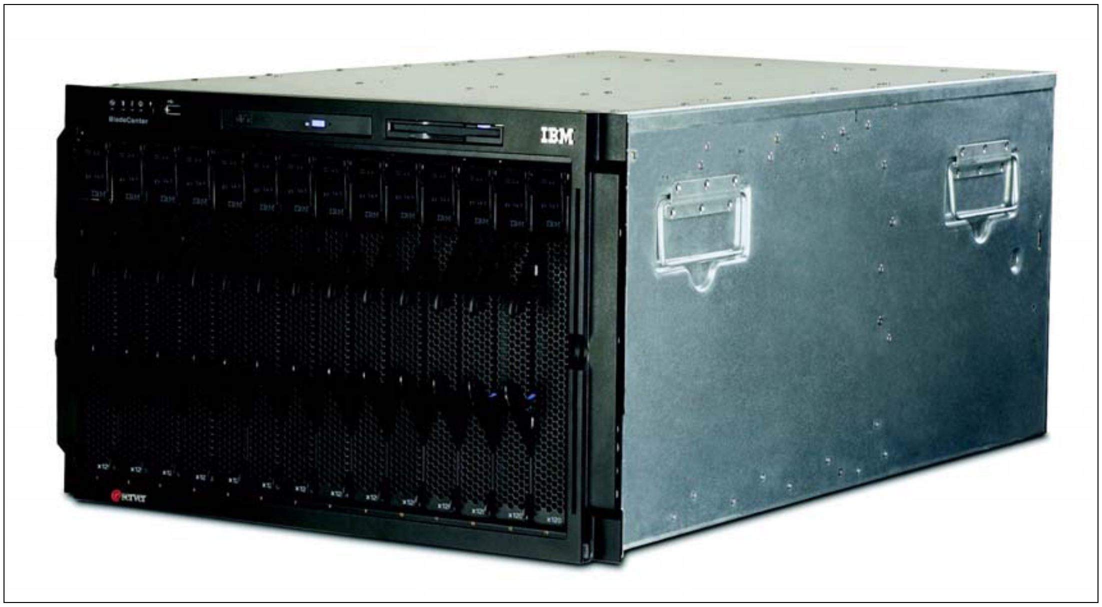


Figure 1-1 The BladeCenter E with up to 14 blade servers or workstations installed

Each BladeCenter chassis comes standard with an *advanced management module*. The advanced management module is a hot-swap device that you use to configure and manage all installed BladeCenter components. It provides system management functions and keyboard-video-mouse (KVM) multiplexing for all the blades in the BladeCenter chassis. It controls Ethernet and serial port connections for remote management access. A second advanced management module can also be installed for redundancy.

A wide variety of IBM and third-party switches are available for the BladeCenter chassis, providing connectivity for Ethernet, Fibre Channel, and InfiniBand® networks.

There are five chassis in the BladeCenter family:

- IBM BladeCenter E, which provide the greatest density and common fabric support.
- IBM BladeCenter S, which are ideal for small- and medium-sized businesses and larger enterprises that are looking for a branch office solution.
- IBM BladeCenter H, which deliver high performance, extreme reliability, and ultimate flexibility for the most demanding IT environments.
- IBM BladeCenter T, which are designed specifically for telecommunications network infrastructures and other rugged environments.
- IBM BladeCenter HT, which are designed for high-performance flexible telecommunications environments, support high-speed internetworking technologies such as 10G Ethernet, and provide robust platform for next-generation networks (NGNs).

All five chassis share a common set of blades and standard switch modules, and additionally, BladeCenter H and HT offer high-speed I/O bays for high-speed switches, such as the Nortel 10 Gb Ethernet High Speed Switch Module.

In this paper, we focus on the IBM BladeCenter E and BladeCenter S.

1.1.1 IBM BladeCenter E

IBM designed the IBM BladeCenter E to be a highly modular chassis to accommodate a range of diverse business requirements. BladeCenter E supports blade servers and blade workstations as well as a wide range of networking modules, including Gigabit Ethernet, Fibre Channel, and InfiniBand for high-speed connectivity to the client's existing network environment. BladeCenter E also supports a redundant pair of Management Modules for comprehensive systems management.

The superior density and feature set of BladeCenter E is made possible by the innovative chassis architecture. Because BladeCenter E uses energy-efficient components and shared infrastructure architecture, clients can realize lower power consumption when compared to their most likely alternative, non-blade server designs. BladeCenter E's lower power consumption and Calibrated Vectored Cooling™ allow more servers or workstations to fit in a tight power or cooling environment.

Figure 1-2 displays the front view of the BladeCenter E and its major components.

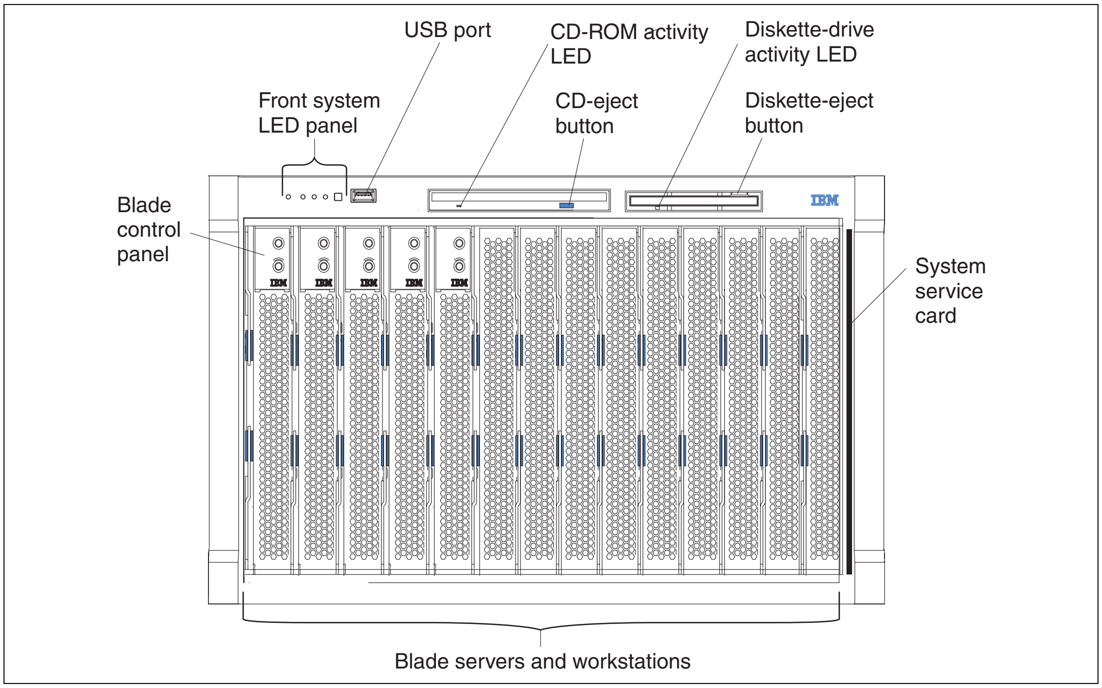


Figure 1-2 BladeCenter E front view and the key features of the chassis

Figure 1-3 and Figure 1-4 display the rear view of the BladeCenter E.

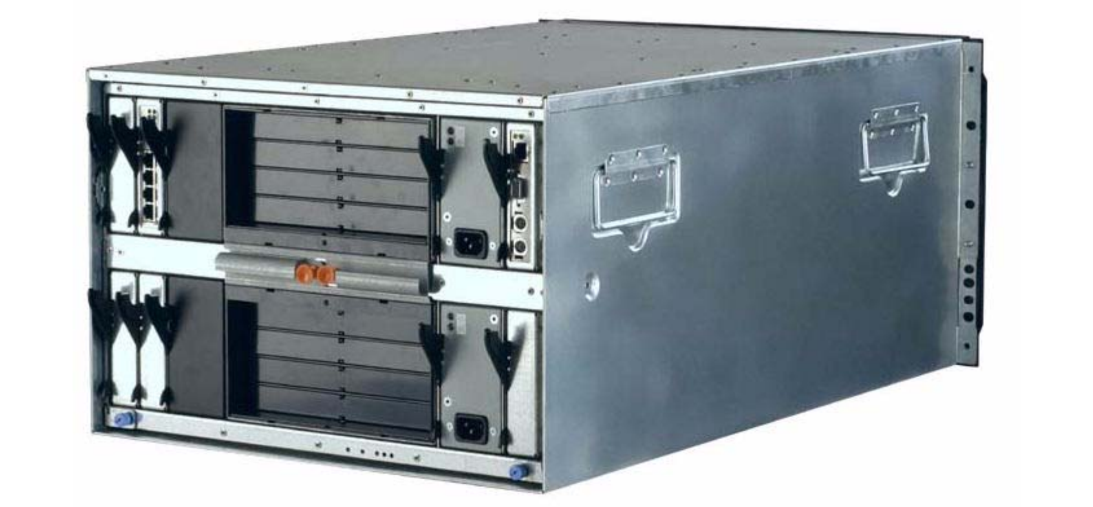


Figure 1-3 BladeCenter E rear view

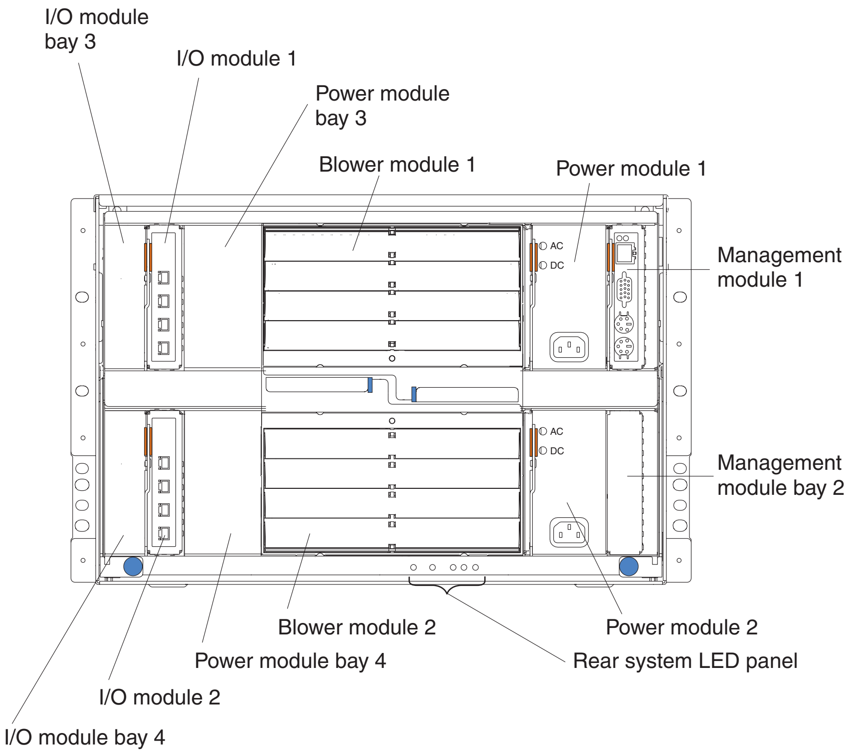


Figure 1-4 BladeCenter E rear view and the key features of the chassis

Key features on the rear of BladeCenter E include:

- Four hot swap I/O module bays
- Two hot swap Management Module bays - with one Management Module as standard
- Four hot swap power module bays - with two power modules as standard
- Two hot swap blowers

The BladeCenter E chassis allows for 14 single-slot blade servers or workstations. You can mix different blade server or workstation models in one chassis to meet your requirements, subject to power and cooling requirements.

The BladeCenter E does not ship standard with any I/O modules. You need to choose these I/O modules depending on your connectivity needs. For the BladeCenter HC10, you need an Ethernet Switch Module (ESM) in I/O module bays 1 and 2.

The I/O modules that are required in I/O module bays 3 and 4 depend on the I/O expansion card that you install in the server blades. The I/O modules installed in bays 3 and 4 are not connected to any installed HC10 workstation blades, because the HC10 does not support the use of expansion cards.

Table 1-1 lists the major features of the BladeCenter E chassis.

Table 1-1 BladeCenter E features at a glance

Feature	Specification
Machine type	8677-3RU, 3RX
Rack form factor (H x D)	7U x 711 mm (28 inches)
DVD/CD drives standard	1x DVD-ROM (in Media Tray)
Diskette drives standard	1x 1.44 MB diskette drive (in Media Tray)
Number of blade slots	14 (30 mm blade servers or workstations)
Number of switch module slots	4 hot-swap
Switch modules standard	None
Power supply size standard	2000 Watts AC
Number of power supplies (standard / maximum)	2 / 4
Number of blowers (standard / maximum)	2 / 2
Dimensions	Height: 305 mm (12.0 in.) Width: 4429 mm (17.5 in.) Depth: 711 mm (28.0 in.)

1.1.2 IBM BladeCenter S

The IBM BladeCenter S (machine type 8886) is the newest addition to the BladeCenter family. It is unique in the BladeCenter family in that it is designed specifically to be used outside of the data center. Acting on feedback from the small- to medium-sized marketplace, IBM created a chassis that has similar features to other models but that is more flexible and customizable.

The chassis brings with it years of rigorously tested and data center proven blade technology, highly energy efficient power supplies capable of running on 110V or 220V power, integrated SAS or SATA storage, and an Advanced Management Module that has the most sophisticated systems management capabilities available.

The BladeCenter S is the perfect complement to the BladeCenter family and is the ideal solution for offices where the controlled environmentals of a formal data center might not be possible.

Figure 1-5 shows the front of the BladeCenter S chassis, where the blade servers and drives are accessible.

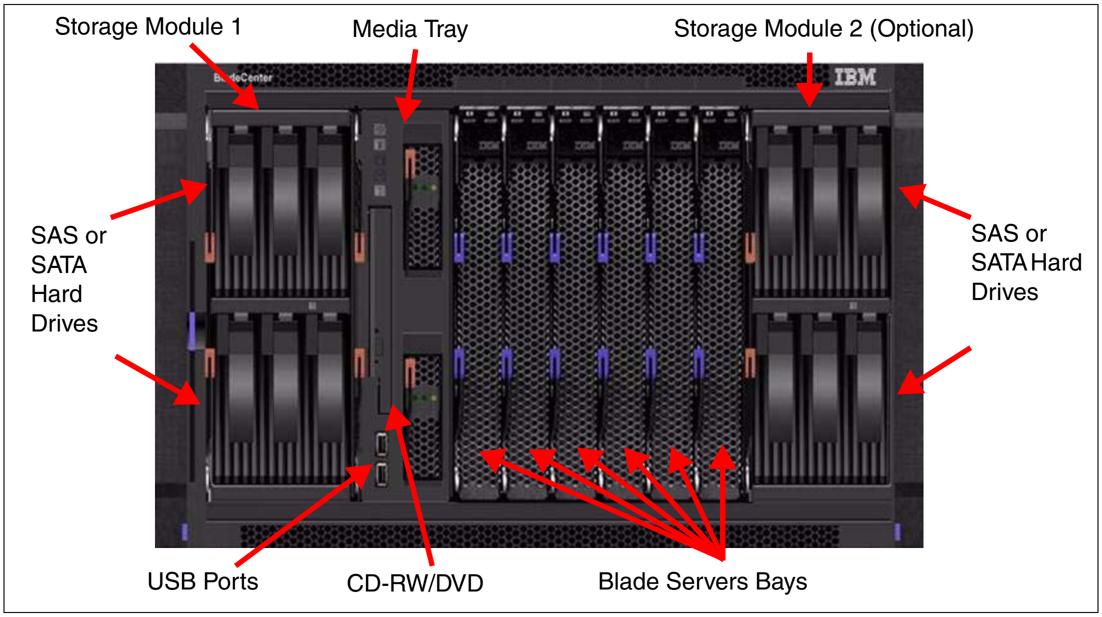


Figure 1-5 The front of the BladeCenter S chassis

Figure 1-6 shows the rear of the BladeCenter S chassis with access to hot-swap fans, power supplies, and I/O modules.

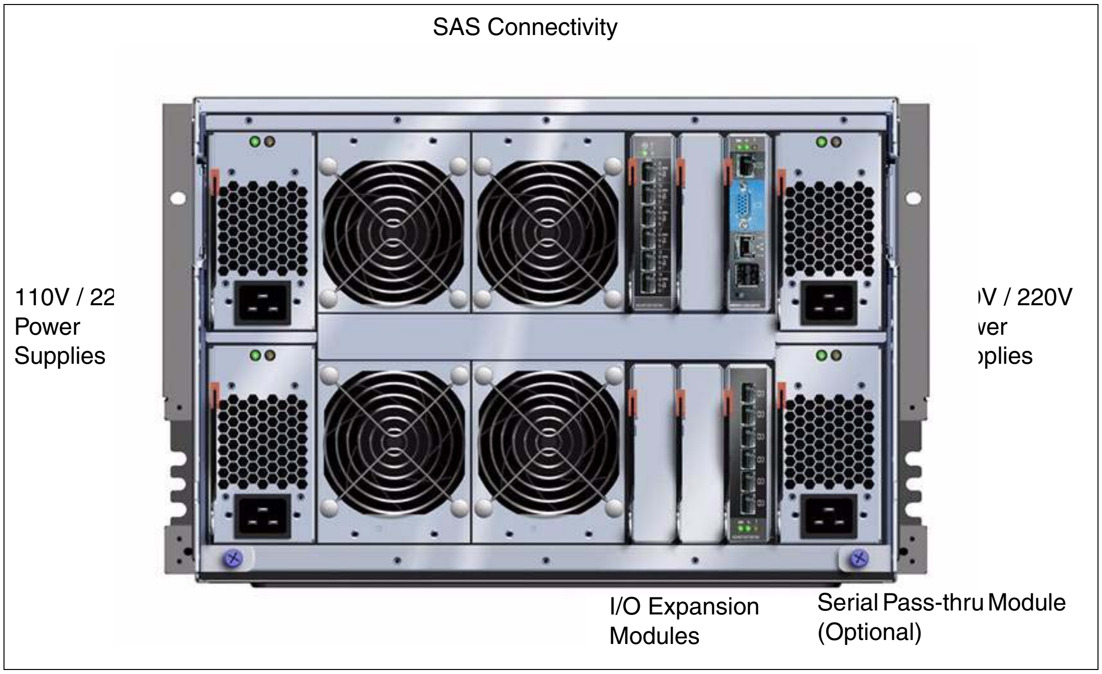


Figure 1-6 The rear of the BladeCenter S chassis

The BladeCenter S chassis allows for either six single-slot blade servers, or three double-slot blade servers. However, you can mix several different blade server models and widths in one chassis simultaneously to support virtually any requirement, subject to power and cooling requirements.

Table 1-2 highlights the major features of the BladeCenter S.

Table 1-2 BladeCenter S features at a glance

Feature	Specification
Machine type	8886-1MX, E1Y
Rack form factor (H x D)	7U x 733.4 mm (28.9 inches)
Disk Storage Modules (standard / maximum)	1 / 2
DVD/CD drives standard	1x CD-RW / DVD-ROM (in media tray)
USB Ports standard	2x USB 2.0 ports (in media tray)
Serial pass-through capability	Yes
Number of blade server slots	6 (30 mm blade servers)
Number of I/O switch module bays	4 hot-swap (1 reserved)
Switch modules standard	None
Power supply size standard	950 Watts AC (110V) or 1450 Watts AC (220V)
Number of power supplies (standard / maximum)	2 / 4
Number of blowers (standard / maximum)	4 / 4
Dimensions	Height: 12.0" (306.3 mm) Width: 17.5" (444 mm) Depth: 28.9" (733.4 mm)

1.2 System management

Effective systems management is more important than ever as IT administrators are faced with the task of managing complex, heterogeneous IT environments. Reducing the complexity with intuitive, automated tools that simplify critical IT tasks and require less training is key to helping customers face this challenge. The systems management component for the IBM BladeCenter is the combination of the IBM Director, Advanced Management Module, and IBM Remote Deployment Manager (RDM). With these tools you can reduce system outages, increase IT personnel productivity, and reduce support costs.

1.2.1 IBM Director

IBM Director consists of a suite of systems management tools that deliver strong hardware manageability. IBM Director's industry-standard foundation enables heterogeneous hardware support and works with a variety of operating systems and network protocols.

As the sole systems management application in an environment, IBM Director can provide a complete management solution for inventorying hardware features and settings, obtaining general system information, invoking proactive systems management functions, and providing a direct link to IBM service and support Web pages. Using industry standards allows for easy integration with other systems management tools and applications.

The list of capabilities that IBM Director provides is long, with a range of features including easy installation and setup, self-managing smart tools, and seamless integration into leading workgroup and enterprise systems management environments. IBM Director is based on industry standards, so you can use many of the tools that it provides to manage non-IBM hardware.

The capabilities of IBM Director can be divided into the following categories:

- Inventory

  A critical first step in any systems management strategy is to understand exactly what hardware exists in the environment and how it is configured. IBM Director performs a thorough inventory scan of each managed system it discovers. Hundreds of hardware and software data points are collected and stored in the IBM Director database. Inventory collection can be repeated both manually and through multiple automated processes.

- Hardware status

  The moment you install IBM Director, it starts working to let you know about hardware problems that occur on managed IBM System x servers. If there is a problem with a power supply, fan, voltage regulator module (VRM), network interface card (NIC), or other hardware, IBM Director lets you know what the problem is and which system is affected.

- Event management

  At the heart of any systems management solution is the ability to alert IT staff in the event of a system problem. IBM Director provides a unique and very powerful method of alerting called *Event Action Plans*. This method enables you to define event triggers independently from actions that might be taken. Then, you can simply combine these two types of items into customized plans for action and assign them to individual or groups of managed systems.

- Process management

  Using the Process Management task in IBM Director, you can keep track of all important processes running in your environment. IBM Director can alert you if any monitored process starts, stops, or fails to start. On managed systems running a supported Windows operating system, you can also get status from every service and device driver installed.

- Resource management

  Resource management is an important aspect of keeping an IT environment running at peak efficiency. It is important to know whether any given system is overloaded and not able to keep up with the workload demand. IBM Director provides the ability to monitor hundreds of system resources, set individual or group thresholds for these resources, and alert you in the event that a resource threshold has been exceeded.

- Remote management

  IBM Director was built to perform remote management. Any management task that can be performed on a local system can also be performed on a system thousands of miles away, provided network connectivity is available. In addition, the Remote Control task in IBM Director allows you to take control of any managed system in your managed environment.

- Update management

  The new Update Manager, introduced in IBM Director 5.20, provides update management through a native IBM Director task. Update functions include tasks for creating profiles, downloading updates, comparing updates defined in profiles against systems, and generating reports.

- Mass configuration

  One of the advantages of managing systems using IBM Director is in its ability to make certain configuration changes on multiple managed systems at once. Even in a dynamic host control protocol (DHCP)-enabled environment, many critical servers tend to use static addresses. Using Mass configuration profiles, you can, for example, change the IP address that these managed systems use to locate their primary DNS server without having to visit each system physically.

- SNMP management

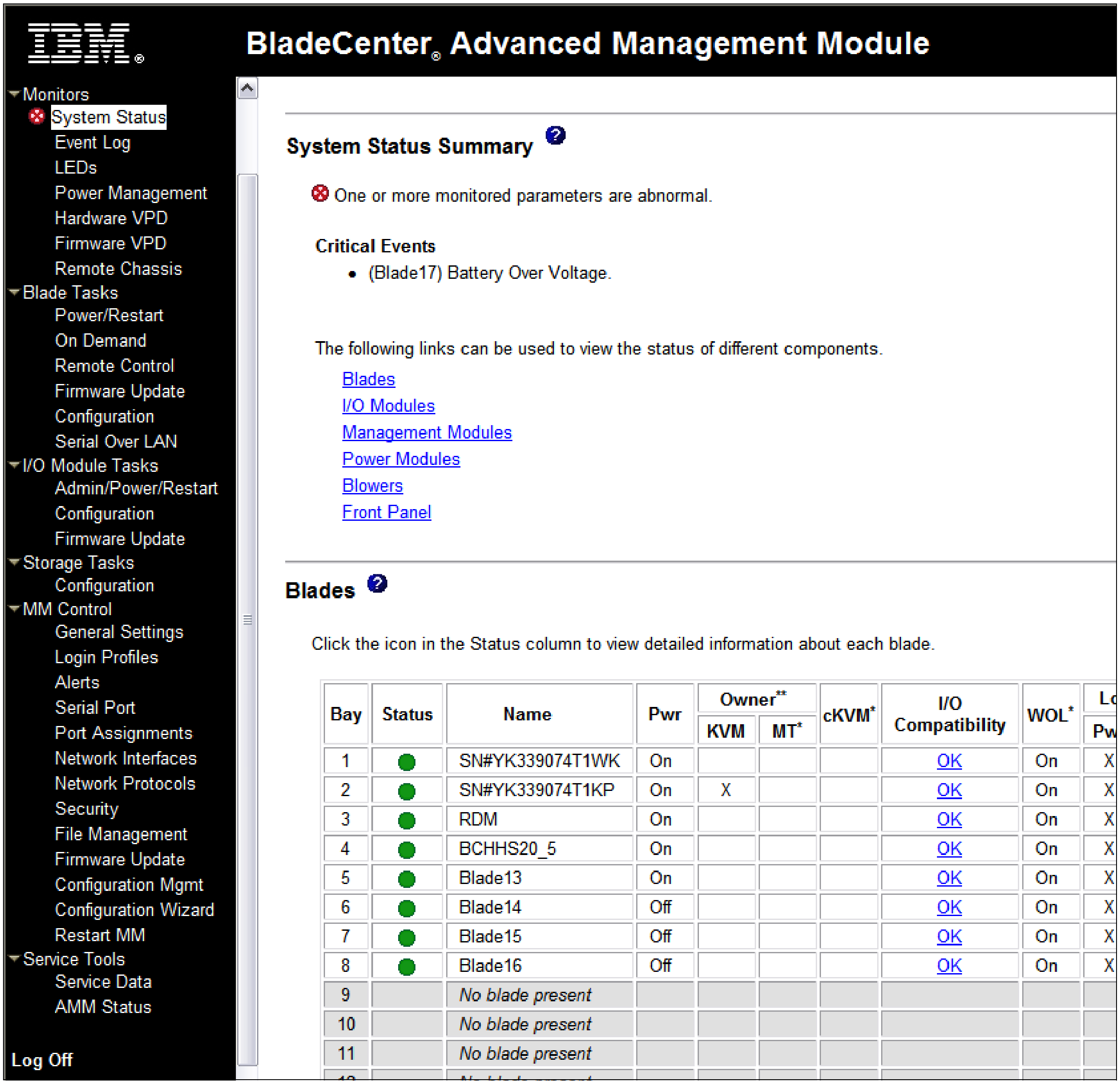
  In addition to the sophisticated management capabilities that IBM Director enables for systems running the IBM Director Agent, any SNMP device can be discovered and managed as well. IBM Director can send and receive SNMP traps and convert these traps into native IBM Director alerts, delivering more helpful information than a raw SNMP trap normally can provide.

1.2.2 Advanced Management Module

The Advanced Management Module manages the BladeCenter chassis itself, the installed networking modules, and all installed blades.

The Advanced Management Module has an integrated KVM switch and an integrated network switch for internal IP connections to all the modules such as Ethernet switch modules (ESMs), Fibre Channel switch modules, and so forth to manage the blades. The Advanced Management Module communicates with the service processor that is integrated into every blade.

The Advanced Management Module has a built-it Web interface that allows you to manage and check the status of each of the modules and blades, remotely control a blade, restart a blade, and many other options. Figure 1-7 on page 12 shows an example of the interface. The menu on the left indicates the key tasks that you can perform.



System Status Summary

One or more monitored parameters are abnormal.

Critical Events

- (Blade17) Battery Over Voltage.

The following links can be used to view the status of different components.

Blades
I/O Modules
Management Modules
Power Modules
Blowers
Front Panel

Blades

Click the icon in the Status column to view detailed information about each blade.

Bay	Status	Name	Pwr	Owner**		cKVM*	I/O Compatibility	WOL*	Lo
				KVM	MT*				Pw
1	●	SN#YK339074T1WK	On				OK	On	X
2	●	SN#YK339074T1KP	On	X			OK	On	X
3	●	RDM	On				OK	On	X
4	●	BCHHS20_5	On				OK	On	X
5	●	Blade13	On				OK	On	X
6	●	Blade14	Off				OK	On	X
7	●	Blade15	Off				OK	On	X
8	●	Blade16	Off				OK	On	X
9		*No blade present*							
10		*No blade present*							
11		*No blade present*							
12		*No blade present*							

Figure 1-7 Web interface of the Advanced Management Module

1.2.3 Remote Deployment Manager

The Remote Deployment Manager (RDM) is a powerful tool that allows you to deploy system images to blade serves and workstations. Remote Deployment Manager is an IBM Director-based tool used for deploying, updating, and configuring servers and workstations. RDM reduces server deployment time and TCO while deploying across multiple platforms and multiple hardware vendors. Thus, the cost and complexity of deploying new systems and hardware and operating systems migration is lowered.

RDM V4.40 offers the following types of deployment:

- Deploys servers and clients
- Deploys Windows and Linux®

> **Note:** The HC10 Workstation Blade does not currently support Linux.

- Runs on Windows and Linux
- Configures deployment tasks and images from IBM Director

1.3 Overview of blade servers and blade workstations

Although blade servers and blade workstations look very similar, they are quite different. This section gives an overview of blade servers and blade workstations and the benefits that they provide.

1.3.1 Blade servers

IBM BladeCenter servers support a wide selection of processor technologies and operating systems to allow clients to run all of their diverse work loads inside a single architecture. The slim, hot-swappable blade servers fit in a single chassis similar to books in a bookshelf, and each is an independent server, with its own processors, memory, storage, network controllers, operating system, and applications. The blade server simply slides into a bay in the chassis and plugs into a midplane or backplane, sharing power, fans, diskette drives, switches, and ports with other blade servers. Figure 1-8 shows the HS21 XM blade server.

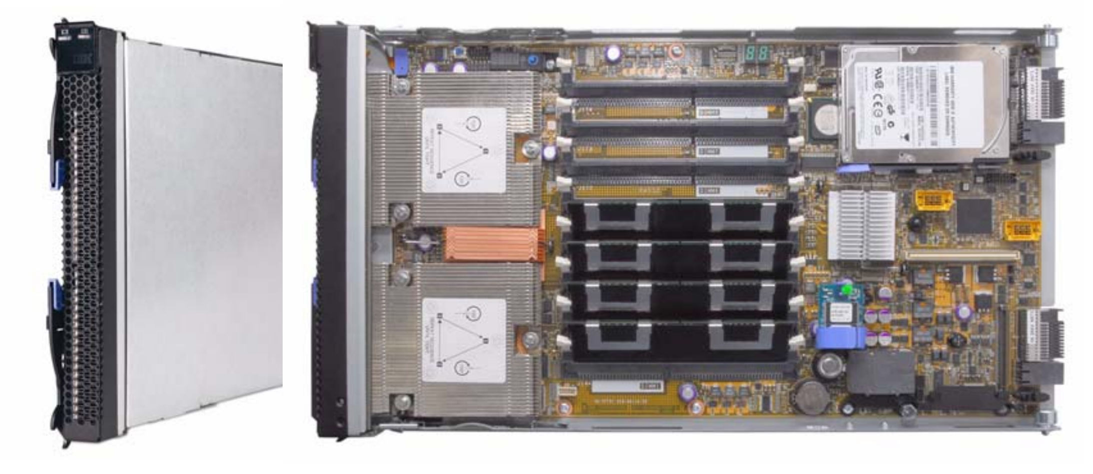


Figure 1-8 The HS21 XM server

The benefits of the blade approach will be obvious to anyone tasked with running down hundreds of cables strung through racks just to add and remove servers. With switches and power units shared, precious space is freed, and blade servers enable higher density with far greater ease.

1.3.2 Blade workstations

Similar to the blade servers, the IBM BladeCenter workstations fit into a single chassis by sliding into a bay and plugging in to a midplane or backplane. They share power, fans, diskette and optical drive, switches, and ports. Each workstation is an independent system, with its own processors, memory, storage, network controllers, operating system, and applications.

The blade workstation concept combines desktop workstation computing resources with server-based computing solutions. The blade is housed in the chassis in the data center and communicates with a user workstation connection device. This device consists of a communications module, USB keyboard, monitor, mouse, and other USB user devices, such as a printer. Figure 1-9 shows the HC10 blade workstation.

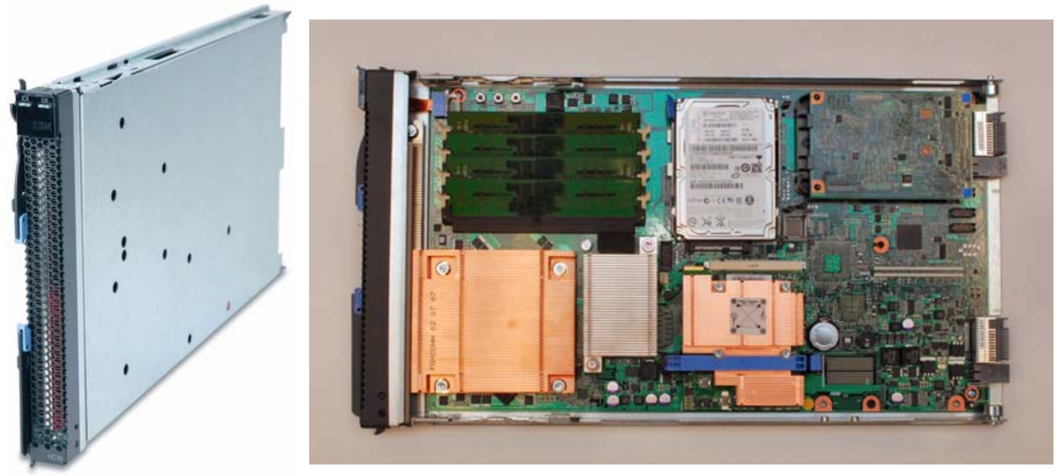


Figure 1-9 The HC10 blade workstation

Blade workstations provide a greater amount of security and privacy because the valuable assets and data are secured and managed inside the data center rather than on the vulnerable user's workstation. The desktop TCO is lowered dramatically by consolidating PCs and user data and by providing a centralized way to manage support and repair. Users are able to access the blade workstation from many locations without closing applications or re-establishing working environment. Blade workstations also provide a more ideal workplace environment, lowering the amount of clutter in an office and reducing the amount of heat and noise produced in the workplace.

1.4 Networking options

This section discusses a few of the networking options. It provides an overview of compatible Ethernet switch modules and specifically the IBM Server Connectivity Module.

The HC10 supports the following types of I/O modules in bay 1 and bay 2 of the BladeCenter chassis (bay 2 on all supported BladeCenter chassis except BladeCenter S):

- Ethernet switch modules as described in the next section
- Copper Pass-thru Module as described in 1.4.3, “IBM BladeCenter Copper Pass-thru Module” on page 16
- Optical Pass-thru Module as described in 1.4.4, “IBM BladeCenter Optical Pass-thru Module” on page 18

1.4.1 Ethernet switch modules

Various types of Ethernet switch modules are available for BladeCenter that support different network layers and services. The Ethernet switch module (as shown in Figure 1-10 on page 16) has several purposes. It provides network connectivity for the BladeCenter unit and blades and also provides interconnectivity between the blades and Management Modules. The Ethernet switch module does not come standard with the BladeCenter chassis; however, two are required for the HC10 implementation.

> **Note:** Other switch modules include InfiniBand switch modules and Fibre Channel switch modules. In this document, we do not focus on these modules because they cannot be used with the HC10. For more information about these modules, see the IBM Redbooks publication, *IBM BladeCenter Products and Technology*, SG24-7523.

Various types of Ethernet switch modules are available for BladeCenter that support different network layers and services, as shown in Table 1-3.

Table 1-3 Ethernet switch modules

Park number	Name	External ports	Network layers
39Y9324	IBM Server Connectivity Module	6	Layer 2
32R1888	Cisco Systems Fiber Intelligent Gigabit ESM	4	Layer 2 Layer 3 QoS[a]
32R1892	Cisco Systems Intelligent Gigabit ESM	4	Layer 2 Layer 3 QoS[a]
32R1860	Nortel Networks L2/3 Copper Gigabit ESM	6	Layer 2 Layer 3
32R1861	Nortel Networks L2/3 Fiber Gigabit ESM	6	Layer 2 Layer 3
32R1859	Nortel Networks Layer 2-7 Gigabit ESM	4	Layer 2 to 7
32R1783	Nortel 10 Gb Uplink Ethernet Switch Module	4[b]	Layer 2 Layer 3
39Y9267	Nortel 10 Gb Ethernet Switch Module	6	Layer 2 Layer 3

[a] Only QoS (Quality of Service) is supported by this switch for Layer 3
[b] This switch has three 10 Gb ports and one 1 Gb port

Layer 2 support means that Ethernet switch is capable of processing frame headers that contain physical addresses such as MAC addresses. Layer 3 processing means that the switch is capable of inspecting packet headers that contain logical addresses such as IP addresses.

If switch supports Layers above 3, it is able to inspect packet content (such as TCP ports or even application protocols such as FTP, HTTP and so one) and not only header.

1.4.2 IBM Server Connectivity Module

The IBM Server Connectivity Module is an example of an Ethernet switch module that can be used with the HC10. The Server Connectivity Module, part number 39T9324, is a switch that provides basic Layer 2 functionality. This device is configurable by a non-networking system administrator through a graphical user interface (GUI) or a command-line interface (CLI). Figure 1-10 shows the IBM Server Connectivity Module.

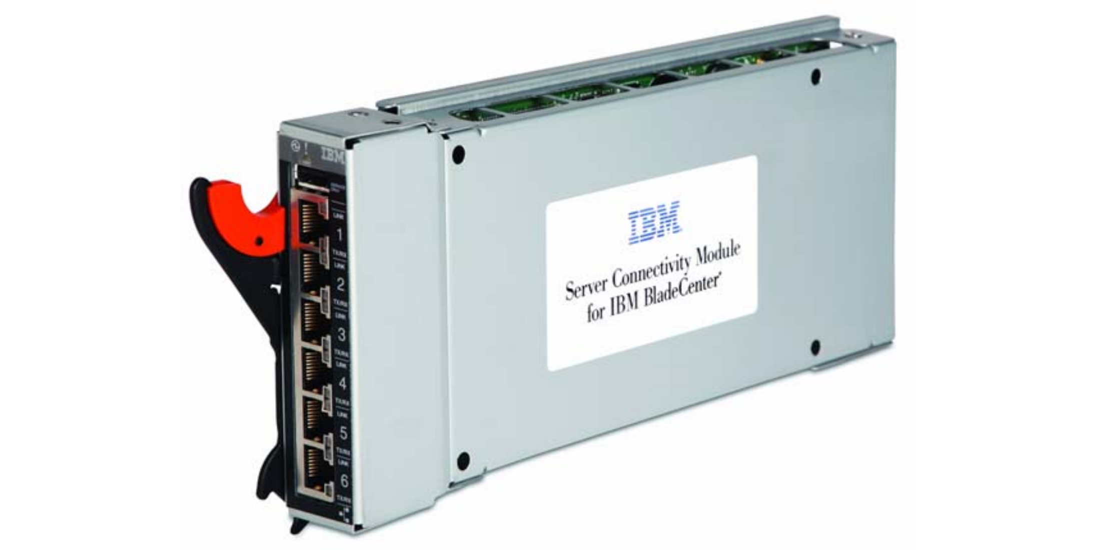


Figure 1-10 IBM Server Connectivity Module

The IBM Server Connectivity Module contains 14 internal full-duplex Gigabit ports that each connect to the blades in the BladeCenter chassis. There are two additional internal full-duplex 100 Mbps ports connected to the management module in slots 1 and 2. Six external ports are provided using standard Category 5 enhanced (5e) copper cable connectors. The external ports connect at 10 Mbps Full Duplex, 100 Mbps Full Duplex, or 1 Gbps Full Duplex. The copper connections provide a way for making connections to a backbone, end stations, and servers.

1.4.3 IBM BladeCenter Copper Pass-thru Module

The IBM BladeCenter Copper Pass-thru Module (CPM), part number 39Y9320 provides an unconfigured network connection that enables the blade in the BladeCenter chassis to connect to an existing network infrastructure. No configuration of the Copper Pass-thru Module is required.

The CPM provides a single connection from each blade—one RJ-45 connector goes directly from each of the 14 blades in the chassis to an RJ-45 plus for connection into an external switch or patch panel. The CPM comes with one cable, which is only five blade servers in the chassis. If you have 14 blades in the chassis, then you need two extra cables, which gives you

15 RJ-45 connectors (1 is left unused). Figure 1-11 shows the IBM BladeCenter Copper pass-thru Module and cable.

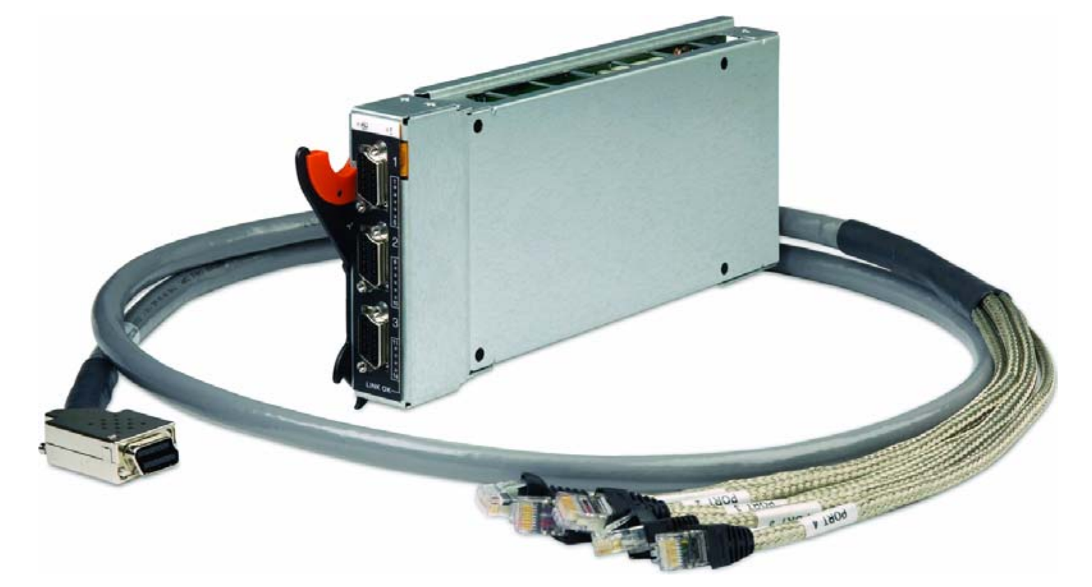


Figure 1-11 IBM BladeCenter Copper pass-thru Module and cable

Up to three copper pass-thru module cables can be connected to the copper pass-thru module (one copper pass-thru module cable is provided). The copper pass-thru module cables are terminated with industry-standard bi-directional connectors.

Table 1-4 shows Copper pass-thru Module options.

Table 1-4 Copper pass-thru Module options

Part number	Description
39Y9320	IBM BladeCenter Copper Pass-thru Module (includes one cable)
39Y9170	IBM BladeCenter Copper Pass-thru Module Cable

The cable for the Copper pass-thru Module has a multi-port copper connector on one end and fanout to five RJ45 Ethernet connectors at the other. One copper pass-thru cable comes with the Copper pass-thru module, and you can purchase two additional cables separately if you require them.

Note: The Copper pass-thru Module is a Gb Ethernet that only supports a 1000 Mbps connection and requires no configuration. Ensure that the external switch devices to which the Copper pass-thru Module connects provide 1000base-T ports.

1.4.4 IBM BladeCenter Optical Pass-thru Module

The Optical Pass-thru Module, part number 39Y9316, provides an unconfigured network connection that enables the blade servers in the BladeCenter unit to connect to an existing network infrastructure. No configuration of the Optical Pass-thru Module is required. Figure 1-12 shows the IBM BladeCenter Optical Pass-thru Module and SC cable.

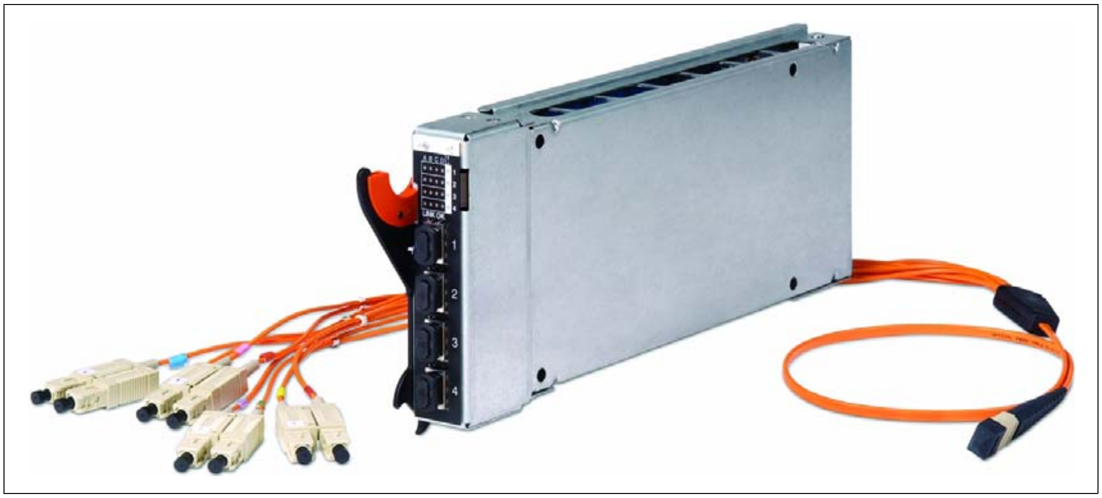


Figure 1-12 IBM BladeCenter Optical Pass-thru Module and SC cable

Up to four Optical Pass-thru Module cables (not included) can be connected to the Optical Pass-thru Module. The Optical Pass-thru Module cable are terminated with industry-standard duplex connectors.

Table 1-5 shows Optical Pass-thru Module options.

Table 1-5 Optical Pass-thru Module options

Option number	Description
39Y9316	IBM BladeCenter Optical Pass-thru Module (does *not* include any cables)
39Y9171	IBM BladeCenter Optical Pass-thru Module SC Cable
39Y9172	IBM BladeCenter Optical Pass-thru Module LC Cable

The Optical Pass-thru Module cable does not come with the Optical Pass-thru Module, and you must purchase it as a separate item. The cable provides four connections between the optical pass-thru module and an external Ethernet or Fibre environment. The Optical Pass-thru Module Cable is 1.5 meters in length, and optical couplers are supplied with the cables so that their length can be extended to 150 meters.

The Multi-Port Optical connector on the optical pass-thru cable is attached to the Optical Pass-thru Module fiber optic port and the other end of the cable has 4 SC or LC duplex optical connectors, that are attached to networking device beyond the Optical Pass-thru Module.

Note: Optical Pass-thru Module supports speeds of up to 2 Gb Fibre Channel. If you use external 4 Gb FC switches and internal 4 Gb FC expansion cards together with Optical Pass-thru Module, the FC fabric operates at 2 Gb.

2

The case for workstation blades

In this chapter, we introduce the concepts of the *workstation blade* and the benefits of such a solution compared to traditional workstations such as the IBM IntelliStation® workstation and other server-based computing options that are available currently. We also discuss the types of customers that would benefit from such a solution and the general benefits of the IBM BladeCenter HC10 workstation blade.

Topics that we cover in this chapter include:

2.1 The use of IBM IntelliStation workstations

Workstation PCs, such as the IBM IntelliStation, are client system that are used by users who require high amounts of local compute power, sophisticated graphics processing, and typically large memory configurations and I/O capability. They are used in a number of industries, such as:

- Engineers and designers in the automotive, aerospace, defense, energy, and transportation industries
- Traders of securities, bonds, and commodities
- Geographic Information Systems professions
- Visual artists
- Medical imaging and scientific visualization

Workstations reside at each professional's work space and present many of the same IT issues as did *server sprawl* in the past.

The key issues with workstation PCs include:

- Security

  Safeguarding the intellectual property created and stored on the workstations, particularly with the availability of removable storage devices such as USB memory keys.

- Environment and operation

  Power, cooling, and space issues due to having high-powered workstations on or under each professional's desk. With professional designers in tight work spaces, power and heat are especially problematic.

- Support

  The expense of desk-side support and the loss of productivity when a user's workstation is down.

- Change management

  When systems are kept in users' workspaces, it can be more difficult to roll out new applications or to move workstations from office to office when required. Some customers require frequent layout change to improve productivity and rolling leases lead to frequent system replacement and significant IT support personnel needs.

To address these issues, the server-based workstation blade solutions such as the HC10 provide the following features:

- Security

  Desktop assets and data are located in the data center where they can be better safeguarded. USB device access is controlled to only allow certain devices (such as printers, mice, and keyboards).

- Environment and operation

  The use of more efficient server technologies found in BladeCenter leads to lower overall costs. Each professional's workspace is improved by moving high-power workstation hardware to the data center, thereby lowering the power requirements as well as heating and space issues.

- Support

  Support is now handled in the data center by IT staff rather than desk-side or using remote control tools.

- Change management

  Workstation deployment can now occur within the data center. Work space moves involve user devices, but not the bulky workstation itself. A new capability called *Free-seating* where a user can connect to the PC from any workstation connection device offers greater flexibility.

A compelling reason for large enterprises to move to workstation blades is the situation where employees work in shifts and only a portion of the workforce is online at any one time. In this case, instead of maintaining unique systems for every single user, a company can use a shared pool of workstation blades that is only slightly larger than the maximum number of concurrent users online at peak periods. This strategy provides better utilization of resources, and the company might need to purchase, for example, only 750 workstation blades for a staff of 1000. This is one example of the cost savings possible when deploying workstation blades.

2.2 Server-based computing for clients

There are three approaches to implementing server-based computing, as shown in Figure 2-1:

- Terminal server and Citrix-type solutions host applications within the same operating system image. Application interoperability and compatibility is essential but makes most efficient use of server resources at the expense of individual client performance characteristics.
- Virtualized and independent operating system images take away the issues of application compatibility while still maximizing server resources within the confines of sharing server resources amongst multiple users.
- The Workstation blade solution is characterized by specialized hardware both on the user's desktop as well as in the blade, ensuring compression and security of data to the user desktop. Dedicated server hardware (in the form of workstation blades housed in a BladeCenter chassis) ensures maximum user performance.

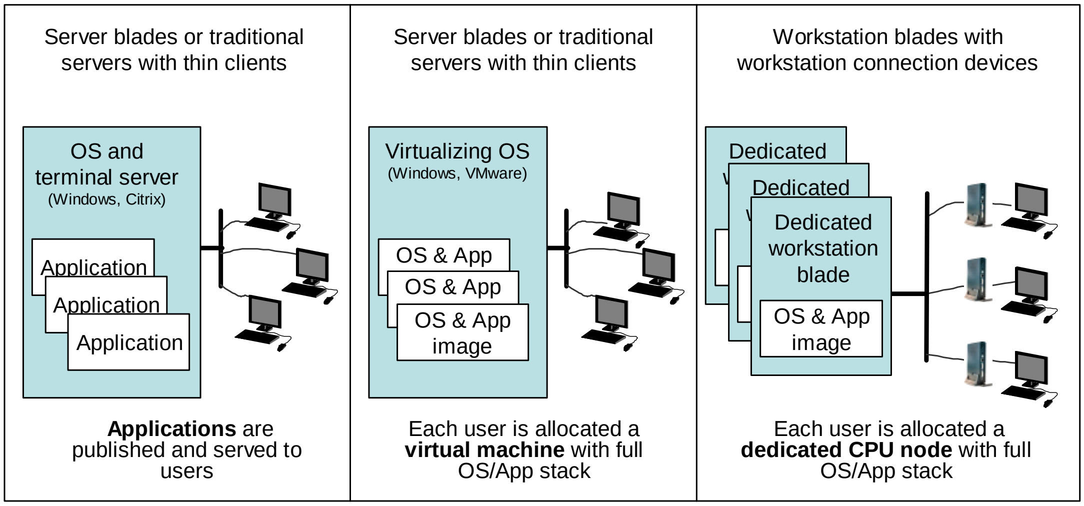

Server blades or traditional servers with thin clients
OS and terminal server
(Windows, Citrix)
Application
Application
Application
Applications are published and served to users
Server blades or traditional servers with thin clients
Virtualizing OS
(Windows, VMware)
OS & App
OS & App
OS & App image
Each user is allocated a virtual machine with full OS/App stack
Workstation blades with workstation connection devices
Dedicated
Dedicated
Dedicated workstation blade
OS & App image
Each user is allocated a dedicated CPU node with full OS/App stack

Figure 2-1 Three approaches to server-based computing for clients

The key differences with the workstation blade solution is its high performance characteristics in terms of CPU, memory, and graphics capacity. This performance is made available to the user due to dedicated hardware to compress the data prior to transmission to the workstation connection device.

Security is also a key feature. The workstation connection device contains no user data and requires access to the corporate network and a valid user login credential to establish a connection with a workstation blade. The user's data remains securely on the workstation blade in the data center and there is no chance for a user to access sensitive data without authentication.

The workstation connection device also supports a wide variety of USB devices connected locally. In addition to a mouse and keyboard, the device supports printers, storage devices, and specialized user interface devices. To ensure data security, an administrator can restrict connectivity to only certain devices (for example, just keyboards, mice, and printers).

Workstation blades are most beneficial for professionals who require more computing power than virtual solutions, such as terminal services or virtualizations. These professionals include financial traders who require huge amounts of processing power to cope with vast amounts of graphical data and spreadsheets. Other potential users are entry to mid-range CAD and CAE application users in the industrial sector.

2.3 Target customers

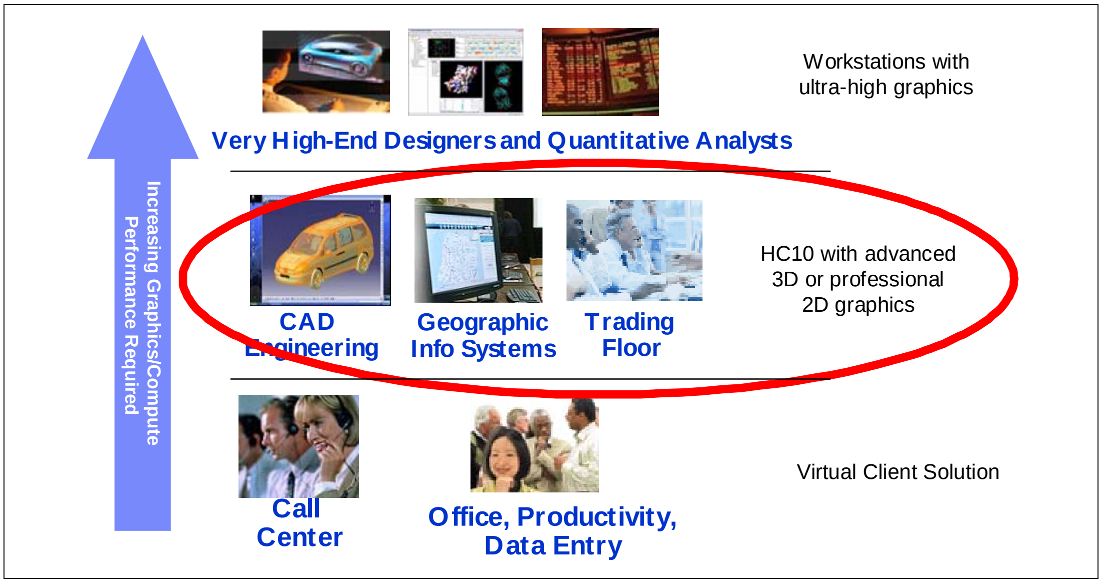
For many years, proponents of server-based computing have insisted that the time is ripe for this architecture. They declare the PC is no longer the best option and cite efficiency of managing computing centrally, rather than at many individual endpoints. Other benefits include better security and higher availability (less downtime).

Server-based computing has not taken off yet, despite all of the benefits that are associated with it. Most organizations still use PCs over server-based computing. Although the growth rate of server-based computing sales has outpaced that of PCs for years, the total market remains two orders of magnitude smaller. Thus, while worldwide shipments of PCs were expected to hit 250 million units in 2007, workstation connection devices and thin clients were expected to ship only 4 million units.

In the past, remote computing has been relegated to office tasks, such as call center, data entry, and productivity applications. Although workstation blades can handle most workstation-class workloads, IBM recommends that users who perform high-end workstation tasks, such as digital mockup and video rendering, use traditional workstations.

However, many workloads that were formerly impossible for server-based computing—such as mainstream CAD, geographic information systems (GIS), trading floor, and distance collaboration—are well within the BladeCenter HC10 capabilities. Workstation blades are built with a large amount of reliability to safeguard the huge investment that is represented by the typical workloads of its target market. Complex designs and financial models, for example, are extremely costly to rebuild if lost.

Figure 2-2 shows the customer types most suited to the IBM workstation blade solution.



Increasing Graphics/Compute Performance Required
Workstations with ultra-high graphics
Very High-End Designers and Quantitative Analysts
CAD Engineering
Geographic Info Systems
Trading Floor
HC10 with advanced 3D or professional 2D graphics
Call Center
Office, Productivity, Data Entry
Virtual Client Solution

Figure 2-2 Target uses of the IBM BladeCenter HC10

2.4 Benefits of using workstation blades

Figure 2-3 shows the IBM BladeCenter HC10 solution.

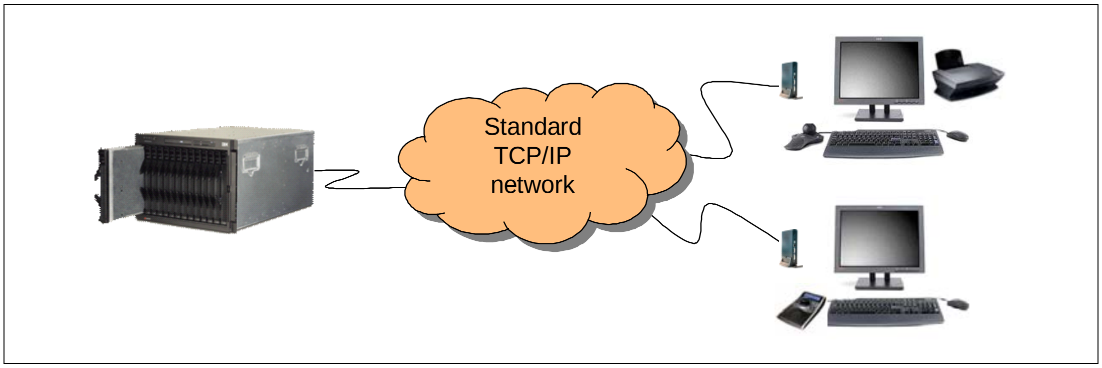


Figure 2-3 The HC10 in the BladeCenter chassis and two CP20 workstation connection devices

The benefits of the IBM BladeCenter HC10 include:

- Data security

  With the HC10, the data is stored physically on the HC10 workstation blade in the data center, away from unauthorized users. Users can be restricted to data access only as it appears on screen, because there is no storage in the IBM CP20 Workstation Connection Device and USB connectivity can be configured to disallow the use of portable storage media such as memory keys. In addition, data transmissions between the HC10 and CP20 is encrypted with 128-bit ciphers to ensure data confidentiality.

- Flexible access

  Depending on the way that the HC10 is configured, users can access applications and data from any location where there is a CP20 connected to the network. Depending on the network's bandwidth and latency, the CP20 can be as far away as 2500 miles from the data center where the HC10s are located.

You can configure the solution such that a specific user always connects to the same HC10 with each connection, or you can configure it to select any available HC10 and rely on Windows roaming profiles to load the user's Windows desktop. With the appropriate connection broker management software installed to manage CP20-HC10 connections, you can also implement pooling where a user gets assigned one of a subset of available HC10s based on logon credentials.

- Improved working environment

  The CP20 workstation connection device consumes as little as 15 watts of power and has no disk drive, fan, or any other moving parts. Thus, the CP20 has lower power consumption when compared to a regular workstation PC plus lower cooling costs in the office environment. In addition, the CP20 is a small device not much larger than the average computing reference book, so there is less clutter in the professional's work space.

- Facilitates centralized management

  The HC10 solution locates assets in the data center for centralized provisioning, maintenance and support. In addition, the HC10 is designed to allow customers to leverage middleware from IBM such as IBM Director and IBM Tivoli® Provisioning Manager for efficient management.

- Workstation-class performance

  The HC10 includes a number of features that are on par with many professional workstations, including NVIDIA high-performance 2D and 3D graphics controllers, Intel Core™ 2 Duo processor, and Gigabit Ethernet controller with support for TCP/IP Offload Engine (TOE) for higher performance data transport.

- Local device support

  The HC10 and the CP20 workstation connection device support USB devices attached locally. This support includes most USB devices, including printers, thumb drives, Web cams, and specialized user-input devices. The types of devices that are supported can be customized by the administrator to prevent (for example) memory thumb drives from being used.

- Application compatibility

  The HC10 is certified by the Microsoft Windows Logo Program, which means a high level of application and device compatibility.

3

HC10 architecture and design

The IBM BladeCenter HC10 is a new blade offering for the BladeCenter family. The HC10 provides server-based computing technology for workstation applications by offering high security and manageability, while delivering outstanding graphics performance and full USB capability. Built-in features are ideal for engineering design applications, trading floor and other financial applications, Geographic Information Systems applications, distance collaboration, and more. The architecture of the HC10 is based on the Intel Core 2 Duo desktop platform rather than a server chipset.

This chapter describes how the HC10 workstation blade solution is designed and gives technical details about its major components. We also describe the protocol that is used for communication between the HC10 workstation blade and the IBM CP20 Workstation Connection Device.

Topics that we cover in this chapter include:

- 3.1, “HC10 networking” on page 26
- 3.2, “HC10 specification” on page 30
- 3.3, “IBM CP20 Workstation Connection Device” on page 34

3.1 HC10 networking

The HC10 solution has two main components, as shown in Figure 3-1:

- The HC10 workstation blade, which is housed in a BladeCenter chassis in the data center
- The CP20 workstation connection device, which is placed on the user's desk

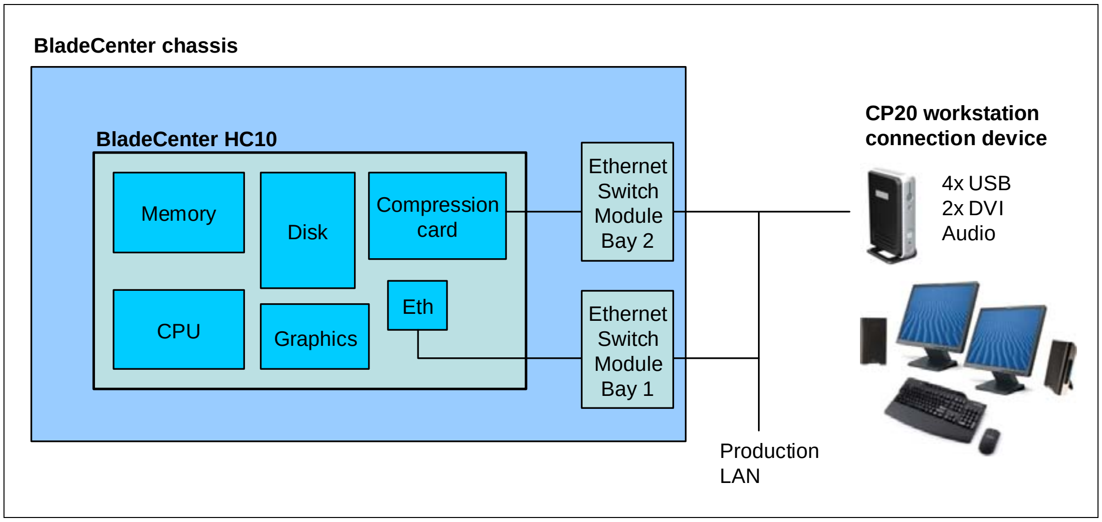


Figure 3-1 Layout and connectivity of the HC10 (default settings in the HC10 BIOS)

The HC10 has two Ethernet connections using a Broadcom 5708S dual-port Gigabit Ethernet controller. Each connection is routed through an Ethernet switch module in the BladeCenter chassis:

- The Ethernet connection that Windows running on the HC10 uses is, by default, the one provided through the Ethernet switch module in bay 1 of the BladeCenter chassis.
- The compression card in the HC10 (also known as the *I/O Graphics Transmission Adapter*) is connected to the CP20, by default, through the Ethernet switch module in Bay 2 of the BladeCenter chassis.

  The network between the compression card and the CP20 can be a private network (or VLAN) if you so desire, or you can simply add these connections to your production LAN. Either way, data is secure because the traffic is encrypted.

The default networking settings are as shown in Figure 3-1. You can change which Ethernet switch modules are used in the Advanced Settings of the HC10 BIOS, as described in 6.2, "Specifying how the Ethernet switch modules are used" on page 100.

3.1.1 The PC-over-IP protocol

The key to the performance of the link between the HC10 and the CP20 is the implementation of the PC-over-IP™ (also known as *PCoIP™*) protocol. A PC-over-IP processor is the basis of both the CP20 and the compression card in the HC10.

The PC-over-IP processor in the HC10 encodes and encrypts the complete user interface of the HC10 (video, USB signals, and audio) in real time, then transmits the secure signals over a standard TCP/IP network to the PC-over-IP processor in the paired CP20, where it is decoded real-time and delivered to the user.

As shown in Figure 3-2, this process results in a low-latency connection between the graphics processor and the monitor on the user's desktop.

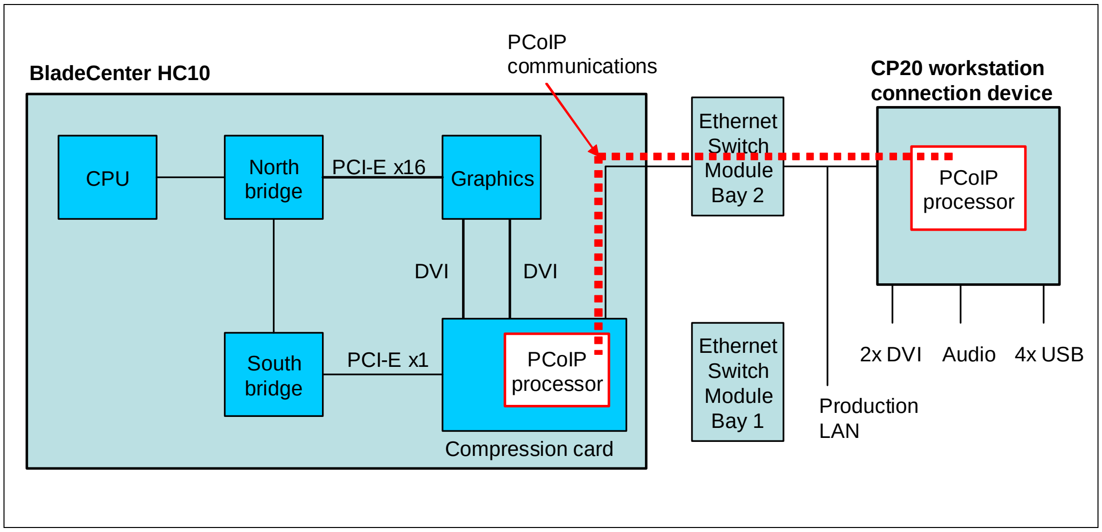


Figure 3-2 PC-over-IP communications between the HC10 and CP20

The PC-over-IP processor in the HC10 is connected to the graphics processor digital video interface and a PCI Express link for transparent bridging of the PC peripherals such as the USB and HD Audio devices.

Prior to network transmission, the PC-over-IP processor in the HC10 compresses the video stream and combines the USB and audio traffic from the south bridge. At the CP20, the PC-over-IP processor decrypts and decompresses the data stream for distribution to the video, audio, and USB devices.

In the return path, the audio and peripheral input data—such as microphone, keyboard, and mouse—is packaged for transmission back to the HC10. This process of compression, transmission, and rebuilding of the user's desktop occur in a very short time, typically less than 10 milliseconds, so as to have little impact on latency.

A 128-bit SSL tunnel is used for all non-media communications with the PC-over-IP processor in the CP20. Mutual device authentication based on certificates is performed as part of the SSL handshake protocol. Media traffic is encrypted through an 128-bit IPsec ESP™ tunnel. The keying information for the IPsec tunnel is established securely over the 128-bit SSL tunnel.

The PC-over-IP processor in the HC10 also optimizes the compression algorithms and quality in real time to achieve the best possible image quality for the available network bandwidth. This optimization allows the PC-over-IP devices to operate in various types of networks and data rates. When more network bandwidth becomes available or when the display image is not changing too frequently, the image processor continues to enhance the compressed image quality until it becomes a lossless replica of the original image.

Although it is possible that, due to the nature of the Ethernet networks, some of the compressed image information might be lost or corrupted, the image processor implements an error detection and recovery algorithms to guarantee high image quality.

The effect of the PC-over-IP technology is that the user devices that are attached to the CP20 are effectively connected locally to the HC10, as shown in Figure 3-3.

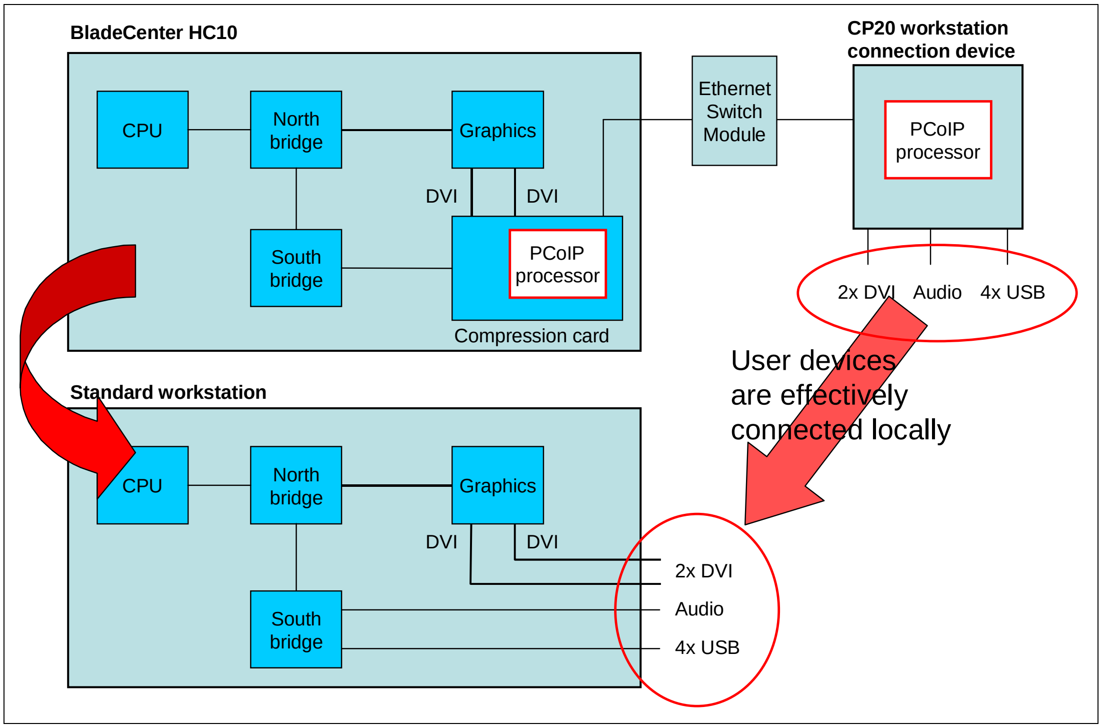


Figure 3-3 User devices are effectively connected locally

3.1.2 USB

The PC-over-IP processors bridge the USB controller from the HC10 to the CP20. The HC10 presents industry-standard USB interfaces to the operating system, which means that no special device drivers are required. Bulk, Interrupt, and Isochronous USB transfers are supported, allowing for compatibility with the full suite of USB 1.1.

Note: The current implementation runs USB 2.0 devices at USB 1.1 speeds.

3.1.3 High Definition Audio support

The audio system implements the Intel High Definition Audio (HD Audio) Specification. HD Audio is a new specification for integrated audio that is capable of delivering the features and high-end performance of an add-in audio card. For details about this specification and its uses, see:

http://www.intel.com/design/chipsets/hdaudio.htm
http://www.intel.com/standards/hdaudio/

The audio controller is compatible with standard device drivers and adheres to the Universal Audio Architecture draft from Microsoft, which is available at:

http://www.microsoft.com/whdc/device/audio

The audio controller supports four output audio streams and three input audio streams for a single client codec. With the exception of performing silence suppression, the PC-over-IP processor is agnostic to the configuration of each audio stream. A full eight audio channels per stream is supported. The sampling rates supported are multiples (up to 192 K sample per second) and sub-multiples of 48 k Hz and 44.1 k Hz.

3.1.4 Network bandwidth recommendations

While network bandwidth is consumed during screen changes or continuous screen updates (that is, high resolution video), most office applications are characterized by long periods without screen changes, resulting in virtually no network traffic. Bandwidth requirements are, therefore, based on applications and usage scenarios, becoming a function of the changing display content rather than being solely a function of display resolution and refresh rate.

In addition to display graphics and video, the PC-over-IP processor also bridges USB peripherals and audio transparently between the host and user desktop. These types of media typically have lower bandwidth requirements.

Regardless of the network bandwidth provisioning, if for any reason the network does not have sufficient resources, the HC10 and the CP20 continues to work by adjusting the display compression dynamically to fit within the available network bandwidth. This adjustment is done in such a way to avoid any short-term degradation in the user experience. As a rule of thumb, the bandwidth for a given user to maintain an acceptable level of performance in a fully loaded scenario can be calculated by multiplying 12.5 bits per second per pixel by the total number of pixels.

For high-end visual applications, such as 3D CAD rendering, video editing, or animation, a minimum of 25 bits/pixel/second should be used in the network bandwidth calculation. To determine the total per-user network bandwidth requirement, USB and audio bandwidth should be considered as well. For most users, 2-3 Mbps bandwidth allocation is sufficient with occasional peak USB/audio loads momentarily using some display bandwidth resources. However, if the users are expected to use demanding USB applications such as burning DVDs or DVD playback, extra bandwidth should be provisioned.

Table 3-1 shows the network bandwidth allocations on the evidence of application usage.

Table 3-1 Network bandwidth allocations based on application usage

Display resolution	1024x768	1280x1024	1680x1050	1600x1200	1920x1200
Typical bandwidth allocation	10 Mbps	16 Mbps	22 Mbps	24 Mbps	29 Mbps
Extreme bandwidth allocation	-	-	44 Mbps	48 Mbps	58 Mbps

3.2 HC10 specification

The HC10 is designed to provide hardware-based graphics compression and encryption that delivers performance and security. Encrypted USB signals are transmitted transparently over the TCP/IP network to a workstation device. No additional software or device drivers are required by customers for encryption and transmission of graphics and USB information over the network. This workstation solution is designed for Microsoft Windows XP and Vista.

Topics in this section include:

- 3.2.1, “Features” on page 30
- 3.2.2, “Processor” on page 31
- 3.2.3, “Memory” on page 32
- 3.2.4, “Network controllers” on page 32
- 3.2.5, “Graphics adapters” on page 32
- 3.2.6, “Compression Card” on page 33
- 3.2.7, “Integrated systems management processor” on page 33
- 3.2.8, “Local storage” on page 34
- 3.2.9, “I/O expansion options” on page 34

3.2.1 Features

The HC10 has the following features:

- One dual-core Intel Core 2 Duo, up to 2.66 GHz
- 1066 MHz front-side bus
- 2 MB or 4 MB L2 cache
- Up to 8 GB of DDR2 SDRAM (PC2-5300 667 MHz)
- 1 SATA disk bay with a 60 GB drive standard
- NVIDIA graphics adapter standard; choice of:
  - Quadro NVS 120M Professional 2D Graphics adapter
  - Quadro FX 1600M Advanced 3D Graphics adapter
- Integrated baseboard management controller (BMC)
- Preloaded Microsoft Windows Vista® Business Blade PC Edition (64-bit)
- Supported operating systems:
  - Microsoft Windows XP Professional (32-bit and x64)
  - Microsoft Windows Vista Business (32-bit/64-bit)
  - Microsoft Windows Vista Enterprise (32-bit/64-bit)
  - Microsoft Windows Vista Ultimate (32-bit/64-bit)
- 1-year customer replaceable unit and onsite limited warranty

Table 3-2 lists the available models. The character *x* in the model numbers varies from country to country.

Table 3-2 BladeCenter HC10 models

Model	Intel Core 2 Duo	Speed	L2 cache	Mem (std/max)	Graphics	Disk
7996-21x	E6300	1.86 GHz	2 MB	1 GB / 8 GB	Quadro NVS 120M 2D	60 GB SATA
7996-51x	E6700	2.66 GHz	4 MB	2 GB / 8 GB	Quadro NVS 120M 2D	60 GB SATA
7996-5Ax	E6700	2.66 GHz	4 MB	2 GB / 8 GB	Quadro FX 1600M 3D	60 GB SATA
7996-5Bx	E6700	2.66 GHz	4 MB	4 GB / 8 GB	Quadro FX 1600M 3D	60 GB SATA

Figure 3-4 shows the HC10 layout.

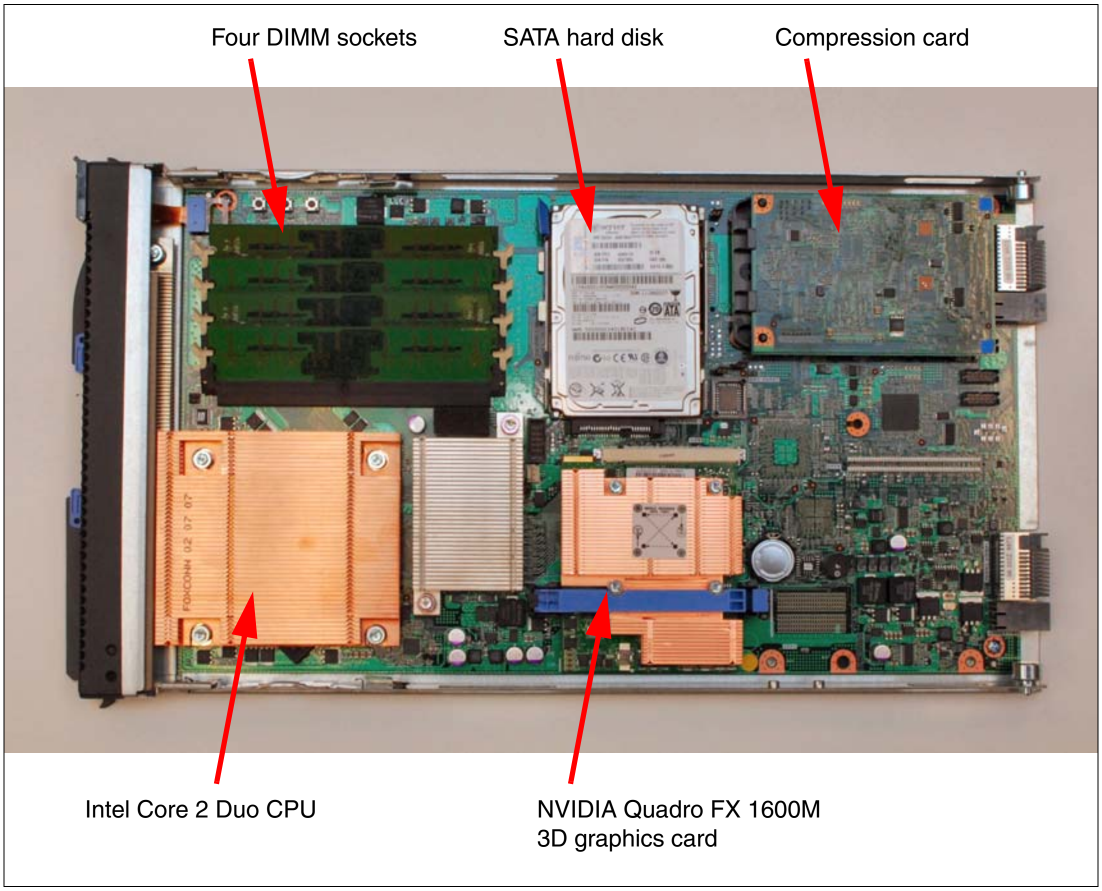


Figure 3-4 The BladeCenter HC10

3.2.2 Processor

The HC10 has one processor standard and maximum. No upgrades are available. There are two processors available, depending on the model. The only differences between the two are the internal clock speed and the size of the L2 cache, as shown in Table 3-3.

Table 3-3 Differences between the Intel Core 2 Duo processors

Processor	Clock speed	Front-side bus	L2 cache size	CPU power consumption
Intel Core 2 Duo E6300	1.86 GHz	1066 MHz	2 MB	65 W
Intel Core 2 Duo E6700	2.66 GHz	1066 MHz	4 MB	65 W

Both processors have the following features:

- Dual core architecture with shared L2 cache
- Intel 64 Architecture (EM64T)
- 1066 MHz front-side bus
- Support for Intel Virtualization Technology
- 65 nm technology

3.2.3 Memory

The memory used in the HC10 is unbuffered DDR2 SDRAM running at 667 MHz (PC2-5300). DIMMs are non-ECC and must be installed in matched pairs (sockets 1 and 3, and sockets 2 and 4). Table 3-4 lists the available memory DIMM options.

Table 3-4 Blade server HS20 type 7981 memory options

Part number	Memory description
41Y2822	1 GB (2 x 512 MB kit) PC2-5300 CL5 DDR2 SDRAM RDIMM
41Y2825	2 GB (2 x 1 GB kit) PC2-5300 CL5 DDR2 SDRAM RDIMM
41Y2828	4 GB (2 x 2 GB kit) PC2-5300 CL5 DDR2 SDRAM RDIMM

3.2.4 Network controllers

The HC10 uses a Broadcom 5708S dual-port Gigabit Ethernet controller. This chip has the following features:

- PCI Express-based
- TCP/IP Offload Engine (TOE) support
- Wake on LAN®
- Serial over LAN (SOL)
- PXE 2.0 boot agent
- Alert Standard Format (ASF) 2.0

Note: The iSCSI initiator in the Broadcom 5708S is not enabled.

The two Ethernet ports are configured in BIOS as follows:

- Connectivity to the bay 1 of the chassis for use by the HC10 operating system
- Connectivity to the Compression Card and CP20 routing through bay 2 in the chassis

Both of these can be changed as described in 6.2, “Specifying how the Ethernet switch modules are used” on page 100.

3.2.5 Graphics adapters

One of two graphics adapters are installed as standard, depending on the HC10 model (see Table 3-2 on page 30). The adapters are installed in an MXM3 type connector on the planar. Both are PCI Express x16 adapters. The graphics adapters include:

- The NVIDIA Quadro NVS 120M graphics board is targeted as the professional 2D workstation graphics solution. It has 256 MB of onboard video memory and a 64-bit interface.
- The NVIDIA Quadro FX 1600M graphics is targeted at customers needing 3D graphics capabilities. It has 128 MB of onboard video memory, a 256-bit memory interface, and supports Shader Model 4.0.

Both graphics adapters support up to two displays as follows:

- One monitor attached: Maximum resolution is 1920 x 1200 at 75 Hz
- Two monitors attached: Maximum resolution is 1600 x 1200 at 60 Hz on each monitor

If you have one or two CRT displays attached to the workstation connection device, you might experience problems at high resolutions. See the following RETAIN® tip H191783 for details:

http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072597

3.2.6 Compression Card

The Compression Card, also known as the *I/O Graphics and Transmission Adapter* or *IGTA*, contains the PC-over-IP processor and a separate Ethernet connector.

The Compression Card provides the following functions:

- I^2C circuitry to provide vital product data (VPD) functions to and from the Advanced Management Module.
- PCI Express interface to provide data communication with the HC10 CPU.
- Route USB controller capability to the CP20 workstation connection device.
- Two DVI inputs from an industry-standard graphics card.
- Dual-monitor support.
- Microsoft WHQL support for plug and play of the CP20 monitor within the HC10.
- Lossless video compression.
- IPsec protocols for secure communications.
- Minimum number of roundtrips in display updates.
- Ability to tag IP packets with VLAN information.
- Ability to detect the monitor resolution of the CP20 using the EDID standard. This can be accomplished using the DDC interface from the compression chip to the graphics card.
- Support for enhanced security and authentication functions such as SSL, LDAP, and Kerberos.

3.2.7 Integrated systems management processor

The HC10 has an integrated Baseboard Management Controller (BMC) that provides:

- IPMI 1.5 (Intelligent Platform Management Interface) compliance
- Serial over LAN (SOL)
- Wake on LAN (WOL)
- Power management functions
- KVM and media tray ownership
- Light path diagnostics support
- Automatic BIOS recovery
- Automatic server restart
- Predictive failure analysis (PFA) on system components (processor, memory, and drives)
- Inventory
- Error logging
- Environmental monitoring (voltages and temperature on the system board)

The BMC is not directly accessible by the administrator. The BMC is only used as an interface to the management module in the BladeCenter chassis. The management module is a single point of control for hardware management of all server and switch components contained within the chassis.

3.2.8 Local storage

The HC10 has a 60 GB SATA drive as standard with the following features:

- 60 GB capacity
- 2.5” SFF form factor
- SATA interface, 300 MBps
- 5400 RPM rotation speed
- Non-hot swap

3.2.9 I/O expansion options

Unlike blade servers such as the BladeCenter HS21, there are no PCI-X or PCI Express connectors on the HC10 to support I/O expansion cards.

3.3 IBM CP20 Workstation Connection Device

The IBM CP20 Workstation Connection Device, 3096-CDX, shown in Figure 3-5, is the user device that has connections for the displays, mouse, keyboard, speakers, and other USB devices. It has no moving parts and has an external power adapter. The CP20 has the following dimensions:

- Height: 232 mm (9.13 in.)
- Width: 94 mm (3.7 in.)
- Depth: 174 mm (6.85 in.)
- Weight 1.1 Kg (2.43 lb)

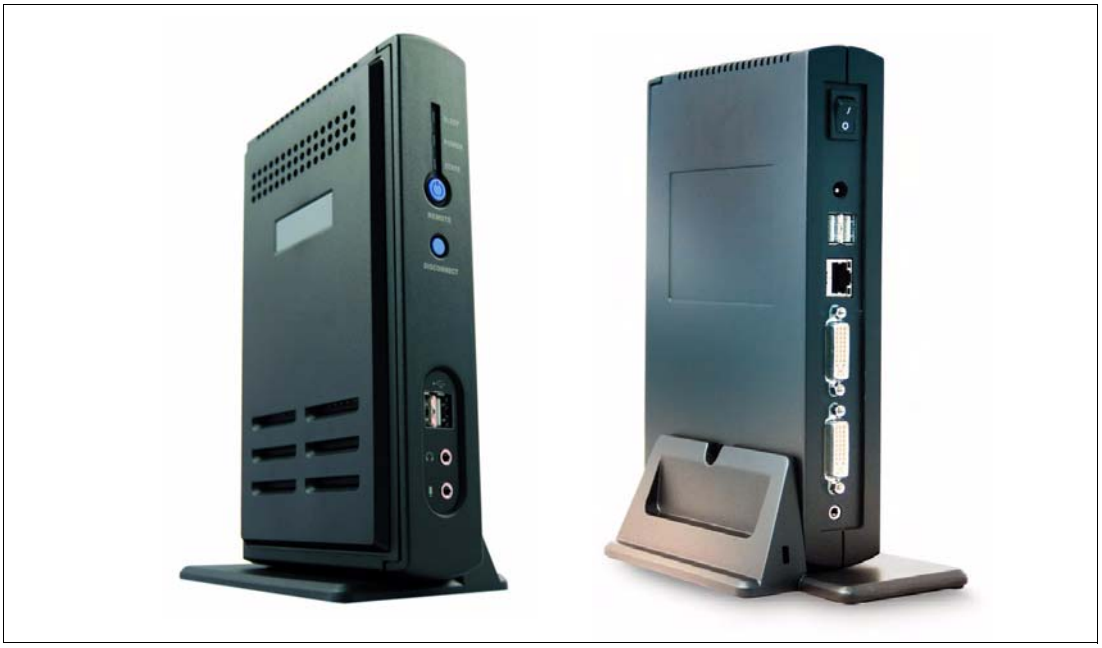


Figure 3-5 CP20 front (left photo) and rear (right photo)

The CP20 provides both increased security and lower support overhead for the enterprise while giving users complete remote display and I/O functionality for personal computer or workstation graphical user interface.

The CP20 has the following functionality:

- Display video information transmitted from the HC10.
- Dual monitor support. Supports both DVI connectors or VGA analog connectors with the addition of a converter.
- Quad monitor support with the addition of two DVI video splitters.
- USB device support (USB 1.1).
- Ability to detect the monitor resolution and transmit that to the HC10.
- Interpretation of the IPsec packets to properly separate compressed video from audio.
- EEPROM-based panels for local configuration.
- Integrated Web-server for browser-based configuration.
- Support for both peer-to-peer connections and connections through broker software.

Figure 3-6 shows a block diagram of the CP20.

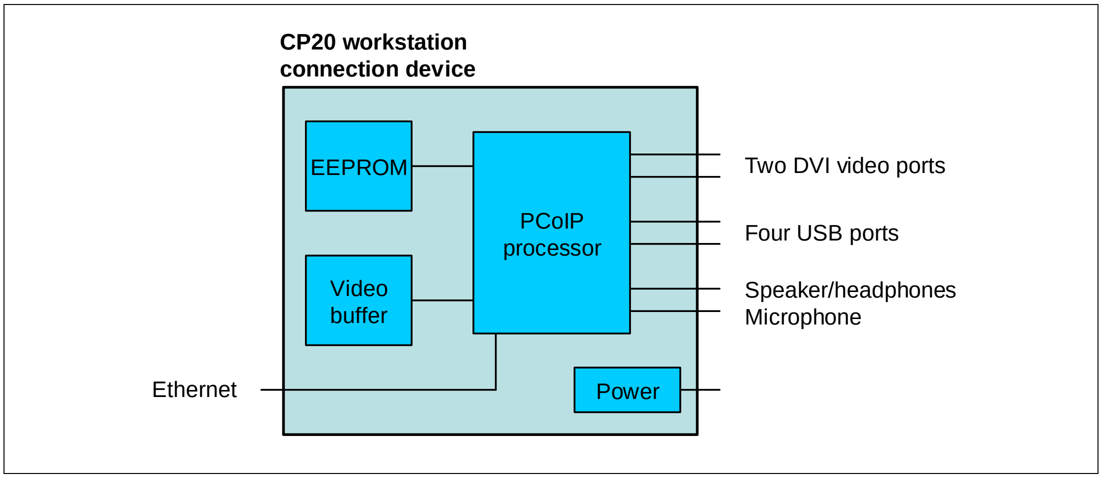


Figure 3-6 CP20 block diagram

3.3.1 Connectors and controls

Figure 3-7 shows the front side of the CP20 where there are two USB connectors, a disconnect button, a remote HC10 power on/off button, one microphone-in jack, one headphone jack, and the status LEDs that indicate the connection state, power, and HC10 power status.

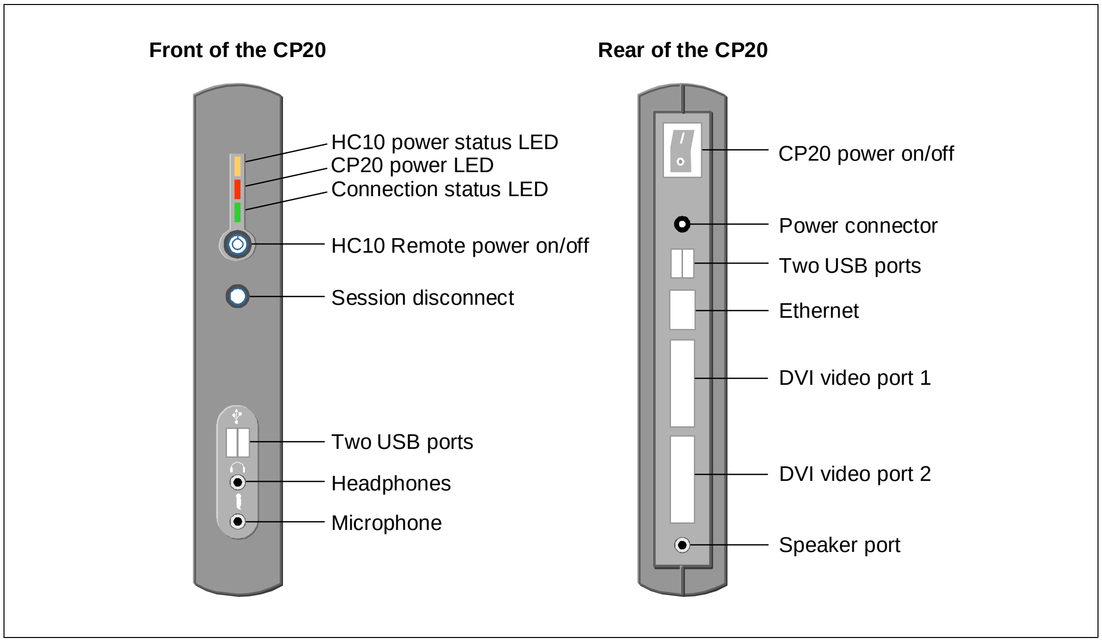


Figure 3-7 CP20 front and rear controls and connectors

The HC10 power status LED has the following meaning:

- *On*: A session is connected and the HC10 is powered on.
- *Off*: HC10 power is off, or there is no session (determine session state using the Connection status LED).
- *Blink*: A session is connected and the HC10 is in standby/hibernate mode.

On the rear of the CP20 there is one RJ-45 10/100/1000 Mbps Ethernet port, dual DVI video ports, two USB ports, a socket for speakers (duplicating the headphones socket on the front), power connector and the power switch.

4

Planning a HC10 installation

This chapter describes the critical areas to consider for planning and implementing the IBM BladeCenter HC10 workstation blade solution. The HC10 installs in the BladeCenter E chassis. It is important to understand that to implement a BladeCenter configuration includes networking, storage and power requirements.

This chapter also describes how to connect the CP20 workstation connection devices to the HC10 workstation blades using peer-to-peer connections and a connection broker. We then discuss the actual implementation of these methods in the next two chapters.

Topics that we cover in this chapter include:

- 4.1, “IBM BladeCenter E chassis” on page 38
- 4.2, “IBM BladeCenter S chassis” on page 43
- 4.3, “Network connectivity” on page 48
- 4.4, “Security” on page 53
- 4.5, “USB control” on page 53
- 4.6, “Video connectivity” on page 54
- 4.7, “Connection methods” on page 57
- 4.8, “Devon IT Connection Manager” on page 60
- 4.9, “Leostream Hosted Desktop Connection Broker” on page 62

4.1 IBM BladeCenter E chassis

As we describe in Chapter 1, "Introduction to BladeCenter" on page 1, the BladeCenter E chassis supports up to 14 blades, including the BladeCenter HC10. You can mix any supported blade servers with the HC10, but we expect that most customers will implement a large number of HC10 workstation blades so that the entire chassis will be full with HC10 blades.

Figure 4-1 displays the front view of the IBM BladeCenter E.

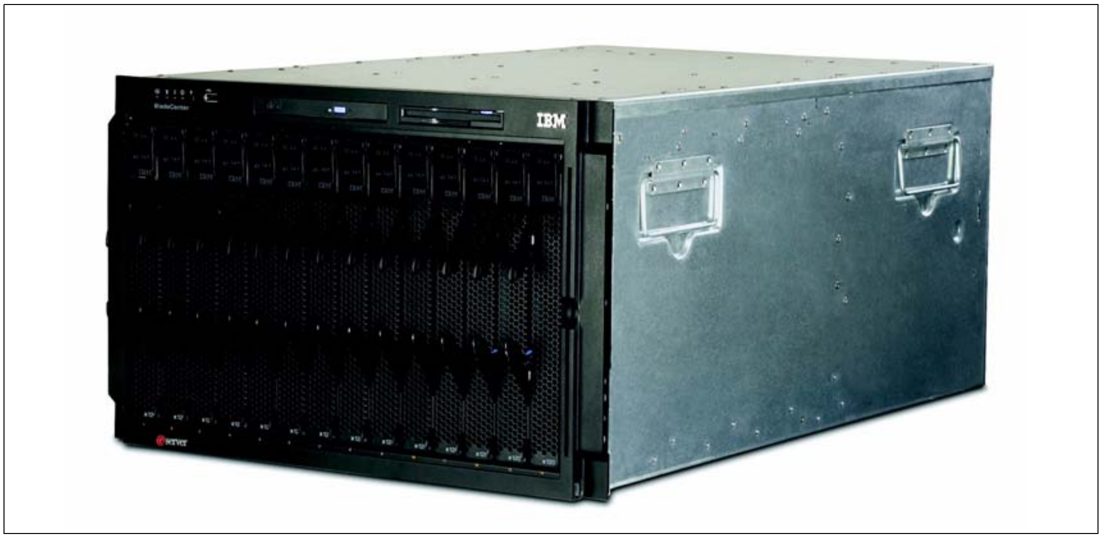


Figure 4-1 IBM BladeCenter E front view

The BladeCenter E chassis ships standard with:

- One Advanced Management Module
- Two hot swap power supply modules
- Two hot swap blower modules
- One USB v1.1 port
- One DVD-ROM drive
- One 1.44 MB diskette drive

This section describes the aspects of the chassis configuration that are required for an HC10 rollout.

4.1.1 Power supply

The BladeCenter E chassis requires the following electrical input:

- Sine-wave input (50-60 Hz single-phase)
- Input voltage:
  - Minimum: 200 V ac
  - Maximum: 240 V ac

The IBM BladeCenter E unit comes with two IEC 320-C19 to C20 power cables. Each power supply has its own IEC 320-C20 power connector.

With four power modules installed (required to support 14 blades), you need four power outlets.

4.1.2 Power modules

There are two power modules standard with the IBM BladeCenter E, which provides power for the first six blade bays. To support all 14 blades, you need to install a second pair of 2000 W Power Supply Modules, part number 39M4675.

The IBM BladeCenter E unit comes with two IEC 320-C19 to C20 power cables. Each power supply has its own IEC 320-C20 power connector. The power supplies in bays 1 and 2 provide power to all the I/O and management modules and to blade bays 1 through 6.

Each pair of power modules is redundant. If either power module fails, the remaining power module continues to supply power, but there is no redundancy. The failed power module must be replaced as soon as possible.

To provide true redundant power, power modules 1 and 3 must connect to a different AC power source than power modules 2 and 4. Connect power modules 1 and 3 to a different PDU than power modules 2 and 4. Then, connect each PDU to an AC power source (building power source or service entrance) that is controlled by a separate circuit breaker.

Note: The IBM BladeCenter E chassis shipped earlier might have different sizes of power supplies: 1200 W, 1400 W, 1800 W, or 2000 W. Only 2000 W power supplies are supported with blades such as the HC10. So, if you plan to install new blades into existing BladeCenter E chassis, you must plan to replace your power modules with 2000 W power modules.

4.1.3 Blower modules

The IBM BladeCenter E chassis comes with two hot-swap blowers for 1+1 cooling redundancy (see Figure 1-4 on page 6).

The blower speeds vary, depending on the ambient air temperature at the front of the BladeCenter E, as follows:

- If the ambient temperature is 72°F or below, the BladeCenter E blowers run at 30% of their maximum rotational speed, increasing their speed as required to control internal BladeCenter temperature.
- If the ambient temperature is above 72°F, the blowers run at 80% of their maximum rotational speed, increasing their speed as required to control internal BladeCenter temperature.

If a blower fails, the remaining blower continues to cool the BladeCenter E unit and blade servers. Replace a failed blower as soon as possible, to restore cooling redundancy.

In noise-sensitive environments, the acoustic attenuation module can be used (see the next section, 4.1.4, “Acoustic Attenuation Module”). The other way of limiting noise level is to use *acoustic mode* setting in the Advanced Management Module. With this mode, the Advanced Management Module throttles the processor speeds of the blades to stay within heat limits.

4.1.4 Acoustic Attenuation Module

The Acoustic Attenuation Module (part number 39M4674), colloquially referred to as the *muffler*, is an option for BladeCenter E that you can install over the blower modules in the rear of the chassis to reduce decibels in sound-sensitive environments. BladeCenter E generates

74 decibels (7.4 bels) at maximum performance levels. The Acoustic Attenuation Module reduces the decibel level down to 69 decibels using a T-shaped baffle (see Figure 4-2).

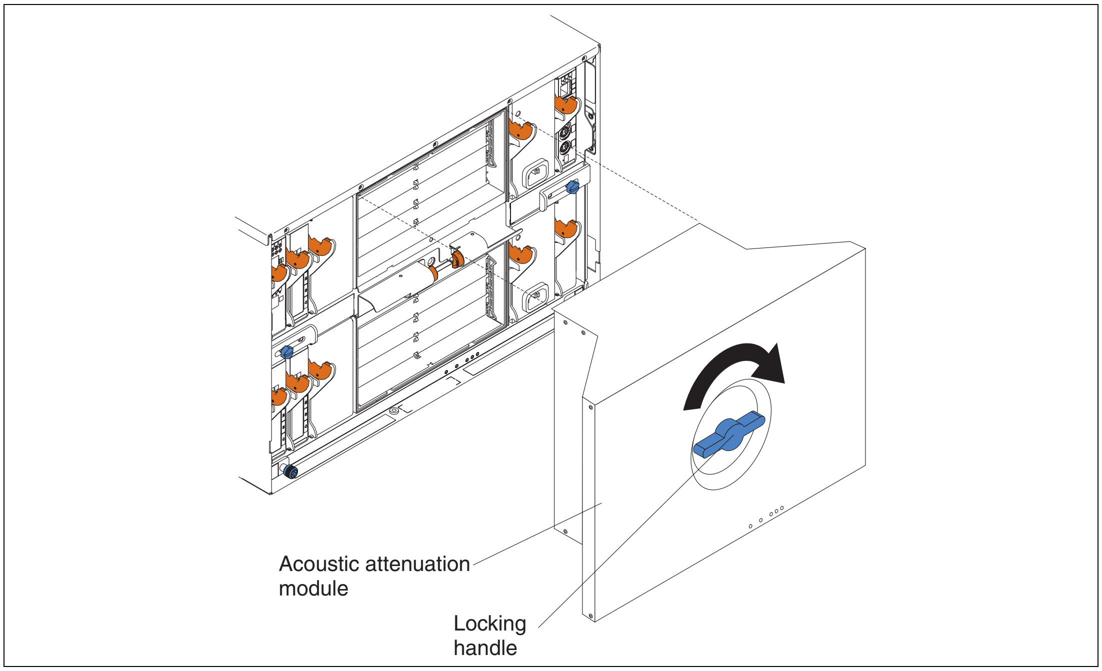


Figure 4-2 IBM BladeCenter E Acoustic Attenuation Module

4.1.5 Cooling considerations

When planning a data center, take the following points into consideration regarding cooling:

- The permissible temperatures and humidity limits for BladeCenter E is:
  - On: 10.0 to 35.0 degrees C (50 to 95 degrees F) at 0 to 914 m (0 to 3000 ft)
  - On: 10.0 to 32.0 degrees C (50 to 90 degrees F) at 914 to 2133 m (3000 to 7000 ft)
  - Off: -40 to 60 degrees C (-40 to 140 degrees F)
  - Relative humidity:
    - On: 8% to 80%
    - Off: 8% to 80%
  - Maximum altitude: 2133 m (7000 ft)
- The amount of heat output of the BladeCenter E chassis in BTU per hour is 8425 BTU/hour (5400 W) with a maximum configuration.

4.1.6 Advanced Management Module

The management module is a hot-swap device that you use to configure and manage all installed BladeCenter components. It provides system management functions and keyboard/video/mouse (KVM) multiplexing for all the blades in the BladeCenter unit. It controls an Ethernet and serial port connections for remote management access.

The BladeCenter E chassis ships standard with one Advanced Management Module. An optional redundant Advanced Management Module, part number 25R5778, provides BladeCenter E with higher levels of resiliency. While in the chassis, the second module is in passive or standby mode. If the active or primary module fails, the second module is automatically enabled with all of the configuration settings of the primary module.

Note: Earlier BladeCenter chassis of type 8677 had the older *Management Module* installed instead of the *Advanced Management Module*. This older device is not supported with the installation of HC10s in the chassis.

The service processor in the management module communicates with the service processor in each blade to support features such as blade power-on requests, error and event reporting, KVM requests, and requests to use the BladeCenter shared media tray (removable-media drives and USB connector).

You configure BladeCenter components by using the management module, setting information such as IP addresses. The management module communicates with all components in the BladeCenter unit, detecting their presence or absence, reporting their status, and sending alerts for error conditions when required.

The Advanced Management Module has different options for local and remote management:

- The 10/100 Mbps Ethernet port can be used for remote management using Web-based, CLI-based, or IBM Director management interfaces.
- The serial port in the front of the Advanced Management Module can be used for local CLI-based management. CLI-based management is useful for unattended remote configurations and batch processing. The Management Module supports only remote management through Ethernet port.
- The Advanced Management Module has two USB ports for a local keyboard and mouse. The Management Module uses PS/2 ports for the same function. You select which blade to control using the appropriate button on the blade.
- The Web interface of both the Advanced Management Module and the Management Module allows remote control of the mouse and keyboard (remote KVM).

In addition to power draw monitoring supported also by the Management Module, the Advanced Management Module will support PowerExecutive™ advancements such as capability to cap power.

The Advanced Management Module requires one IP address used for communications. You should plan to use the same subnet for management module and I/O modules management interfaces. We recommend you use static IP addresses (or at least reservations for DHCP) for the Advanced Management Module.

4.1.7 Ethernet switch modules

The use of HC10 workstation blades requires two Ethernet switch modules be installed in bays 1 and 2 of the chassis. These Ethernet switch modules provide connectivity from all 14 blades to your Ethernet network:

- The switch module in bay 1 provides connectivity to the operating system on each HC10.
- The switch module in bay 2 provides connectivity from the compression card in each HC10 to the CP20 workstation connection devices in your network.

These Ethernet switch modules are not redundant.

Table 4-1 lists the available Ethernet switch modules and common selection considerations that can be useful when selecting an appropriate switch module. For basic Gigabit Ethernet connectivity as you would need with an HC10 solution, we recommend the use of the IBM Server Connectivity Module.

Note: Ensure that the switches that you use are configured to allow the required traffic as described in 4.3.3, “TCP/IP ports” on page 51.

Table 4-1 Switch module selection criteria

Requirement	Suitable switch module
Basic Layer 2 Gigabit Ethernet switching connectivity (VLAN, port aggregation)	► IBM Server Connectivity Module
Advanced Layer 2 Gigabit Ethernet switching: standards-based features (STP, QoS)	► Cisco System Intelligent Gigabit Ethernet Switch Module ► Nortel Networks L2/L3 Copper Gb Ethernet Switch Module
Layer 3 Gigabit Ethernet switching (IP routing, filtering)	► Nortel Networks Layer 2-7 GbE Switch Module for IBM BladeCenter
Layer 4-7 Gigabit Ethernet switching (content-based switching, traffic inspection, server load balancing)	► Nortel Networks Layer 2-7 GbE Switch Module for IBM BladeCenter

4.1.8 IBM Server Connectivity Module

IBM Server Connectivity Module for IBM BladeCenter, part number 39Y9324, is a switch that provides basic Layer 2 functionality. This device is configurable by a non-networking system administrator through a graphical user interface (GUI) or a command-line interface (CLI).

Typical networking concepts—such as spanning tree redundancy, virtual local area networks (VLANs), port filters, link aggregation, port trunks, and remote monitoring (RMON) statistics—are not typically used or understood by this class of administrator.

The default operation is to hide the underlying networking function and configuration from the user. Some functions, such as Spanning Tree Protocol, are eliminated because they are not required. Only a few simple networking parameters are available to the user to configure and control the Server Connectivity Module. See Figure 1-10 on page 16 for a photo of the Server Connectivity Module.

Standard features and functions include:

- Internal ports
  - 14 internal full-duplex Gigabit ports, one connected to each of the blades in the BladeCenter unit
  - Two internal full-duplex 100 Mbps ports connected to the management module in slots 1 and 2
- External copper ports
  - Six external ports are provided using standard Category 5 enhanced (5e) copper cable connectors
  - 10/100/1000 Mbps interfaces: the external ports connect at 10 Mbps Full Duplex, 100 Mbps Full Duplex, or 1 Gbps Full Duplex
  - Auto-negotiation capability
  - Copper connection for making connections to a backbone, end stations, and servers

- Internal Switching
  - Packet switching between the blades and management modules within the chassis to support Serial over LAN (SOL)
- Configuration of the Server Connectivity Module is only through a connection to a management-module port and not through the external switch ports
- Support for tagged VLANs; the administrator can define VLAN identifiers (IDs) to match specific server application requirements
- Cisco EtherChannel compatible static link aggregation
- Management-module control that allows for external ports to be enabled or disabled
- Support for Ethernet jumbo frame formats (up to 9 K bytes per frame)
- Two independent internal 100 Mbps FDX links connected to each of two management modules (jumbo frame support is not required on these links)
- Management-module I2C interface that provides VPD and register access
- Level 2 (L2) switching per current industry standards and practice
- Non-networking device appearance allows administration and installation of this device by the system manager rather than a network administrator
- Port aggregation (only for external ports)
- Port group failover (triggered by external ports)
- IEEE 802.3x Flow Control
- Internet group multicast protocol (IGMP) snooping
- IEEE 802.1Q support for SOL and optional user VLAN tagging of external ports
- RADIUS or TACACS+ user authentication

4.2 IBM BladeCenter S chassis

As we describe in Chapter 1, “Introduction to BladeCenter” on page 1, the BladeCenter S chassis supports up to six blades, including the BladeCenter HC10. You can mix any supported blade servers with the HC10, but we expect that most customers will implement a large number of HC10 workstation blades so that the entire chassis will be full with HC10 blades.

> **Tip:** The primary benefit of the BladeCenter S to HC10 customers is its ability to run off 110V AC power.

Figure 4-3 displays the front view of the IBM BladeCenter S.

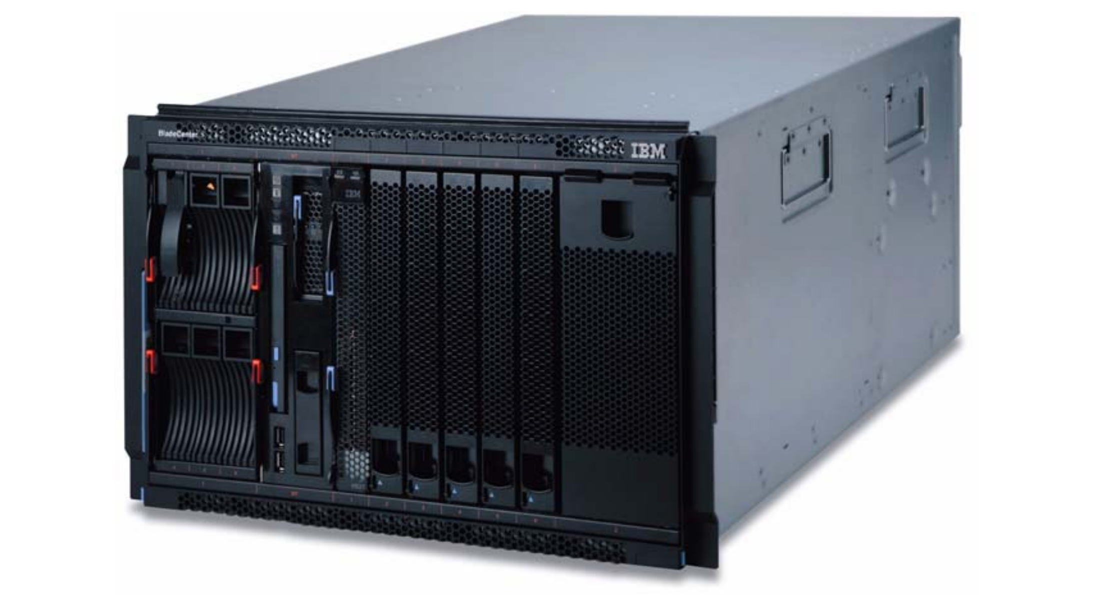


Figure 4-3 IBM BladeCenter S front view

The BladeCenter S chassis ships standard with:

- One six-bay disk storage module
- One Advanced Management Module
- Two hot swap power supply modules
- Four hot swap blower modules
- Two USB v2.0 ports
- One CD-RW / DVD-ROM
- One advanced management module

This section describes the aspects of the chassis configuration required for an HC10 rollout.

4.2.1 Power requirements

One of the unique features of the BladeCenter S chassis compared to the other members of the chassis family is the ability to be powered from a 110V AC power supply.

The BladeCenter S supports up to four auto-sensing power modules that are capable of supporting either 110V or 220V AC power. Two power modules are standard and a maximum of four are supported. The second pair of power modules is part number 43W3582.

The second pair of power modules is required if any of the following instances occur:

- The power requirements of the installed components (servers, I/O modules, disks, and so forth) exceed the capacity of the standard two power modules.
- You install the second storage module, because power modules 3 and 4 also provide the necessary fans to cool this second storage module.
- The power profile that is selected requires more power supplies for redundancy. Power management profiles are configured in the advanced management module user interface, and provide options regarding AC power source redundancy and power module redundancy.

Use the BladeCenter Power Configurator to confirm whether your configuration required the second pair of power supplies:

http://www.ibm.com/systems/bladecenter/powerconfig

You should also review the Power section in Chapter 2 of the *BladeCenter S Planning Guide* for details about power consumption and power management policies.

The power modules are hot swappable components and can be replaced easily during normal BladeCenter operation, assuming a redundant power policy has been selected in the Advanced Management Module. If a power supply fails, the cooling fans inside the power supply continue to operate normally, because the power supply fans are powered from the *common* voltage from the mid-plan. This is important to note as the power supply fans provide the airflow cooling to the Storage Modules.

The power modules are auto-sensing and can support either 110V or 220V AC power. However, you must not mix voltage power sources within the same BladeCenter S chassis.

4.2.2 I/O module bays

The BladeCenter S has four I/O bays as shown in Figure 4-4.

- Bay 1 holds the required Ethernet Switch Module to connect the Ethernet controller of the HC10 and the HC10's compression card to your Ethernet network. Note that unlike the BladeCenter E, the BladeCenter S chassis only uses one bay to route both networks. See Table 4-2 on page 46 for a list of support switch modules.
- Bay 2 is reserved for future use.
- Bay 3 and 4 are for I/O connectivity such as the SAS Connectivity Module or other networking I/O modules. I/O modules in these bays connect to the expansion card installed in the blade servers (either CFFv, small, or standard form factors). Note however, that the HC10 does not have the option to install an expansion card, so if the chassis has only HC10 blades installed in it, then these I/O bays are unused.

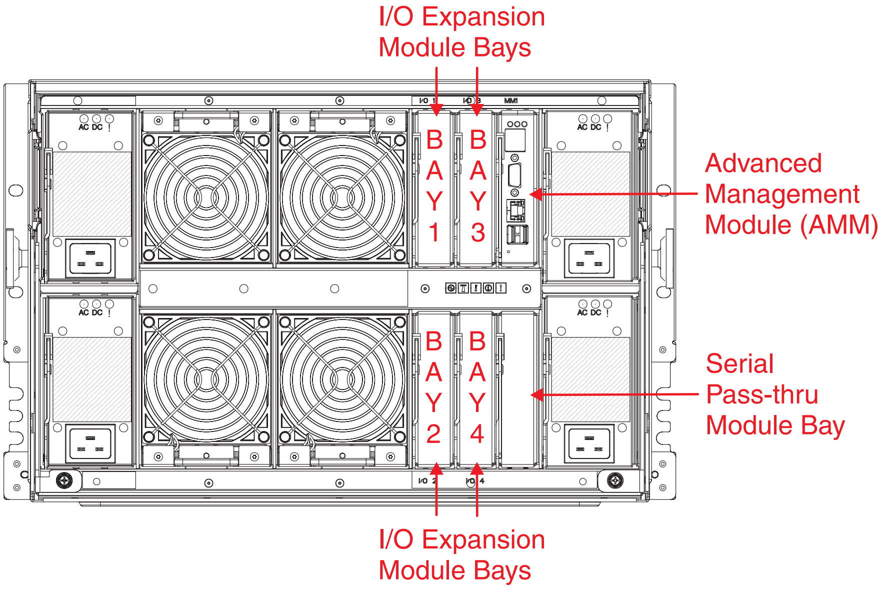

I/O Expansion Module Bays
BAY 1
BAY 3
BAY 2
BAY 4
Advanced Management Module (AMM)
Serial Pass-thru Module Bay
I/O Expansion Module Bays
AC DC
I/O 1
I/O 3
MM1
I/O 2
I/O 4

Figure 4-4 Back of BladeCenter S identifying I/O Module Bay numbers

4.2.3 I/O expansion module options

The following I/O expansion modules are available for the BladeCenter S.

Note: The HC10 does not support expansion cards. To use the onboard storage of the chassis, you will need to have one blade server (for example, an HS21) with a SAS expansion card installed in the chassis, to act as a file server. I/O bays 3 and 4 should then have the SAS Connectivity Module as listed in Table 4-2.

Table 4-2 Supported I/O expansion modules for the BladeCenter S

Part number	Description	Suitable I/O module bays
SAS I/O expansion module		
39Y9195	IBM BladeCenter SAS Connectivity Module	3, 4
Ethernet I/O expansion modules		
32R1860	Nortel Layer 2/3 Copper Gb Ethernet Switch	1, 3, 4[a]
32R1861	Nortel Layer 2/3 Fiber Gb Ethernet Switch	1, 3, 4[a]
39Y9324	Server Connectivity Module	1, 3, 4[a]
32R1783	Nortel 10G Uplink Ethernet Switch	1, 3, 4[a]
Fibre Channel I/O expansion modules		
32R1813	Brocade 10 port - 4 Gb SAN Switch	3, 4[a]
43W6724	QLogic® 10 port - 4 Gb Fibre Channel Switch	3, 4[a]
43W6723	4 Gb Intelligent Pass-thru Module	3, 4[a]
39Y9284	Cisco Systems 4 Gb 10 port Fibre Channel Switch	3, 4[a]
Other I/O expansion modules		
39Y9316	Optical Pass-through Module	1, 3, 4[a]
39Y9320	Copper Pass-Through Module	1, 3, 4[a]

a. Installing this switch module in bays 3 or 4 requires a suitable expansion card installed in the blade servers. Doing so precludes the use of the BladeCenter S internal storage modules.

4.2.4 Storage Modules

The Storage Module is fundamentally a collection of disk drives that are made accessible to blade servers through the SAS expansion card in the blades and the SAS Connectivity Module in bays 3 and 4 of the chassis.

Important: The HC10 workstation blade does not support expansion cards, so it cannot use the storage modules in the BladeCenter S chassis. If you plan to have server blades installed in the chassis as well, then these servers can have the SAS expansion card and access the disks in the storage modules.

You can install a maximum of two Storage Modules in the BladeCenter S chassis, with each Storage Module containing up to six 3.5-inch hot-swap hard drives. Intermixing of SAS and SATA based hard disks within the same Storage Module is supported.

The chassis can accommodate up to six 3.5-inch hard drives in its standard storage module, and six more with an additional storage module. The disks can easily and quickly be assigned directly to blades using built-in predefined configurations or through user definable custom configurations.

Supported disk drives are as follows:

- 73 GB 15 K RPM SAS drive, part number 40K1043
- 146 GB 15 K RPM SAS drive, part number 40K1044
- 300 GB 15 K RPM SAS drive, part number 43X0802
- 500 GB SATA drive, part number 39M4530
- 750 GB SATA drive, part number 43W7576

4.2.5 BladeCenter S Office Enablement Kit

The BladeCenter S Office Enablement Kit, part number 2018-86X, is a new enclosure that is designed specifically for the BladeCenter S chassis for use in offices where the noise requirements are important. Figure 4-5 shows the enclosure.

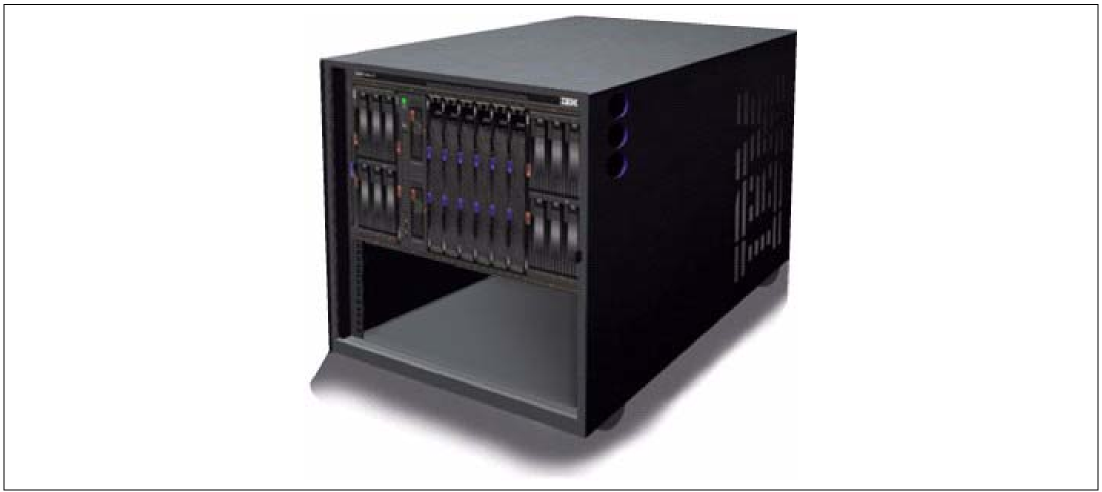


Figure 4-5 BladeCenter S Office Enablement Kit

Based on the NetBAY11, the Office Enablement Kit is an 11U enclosure with security doors and special acoustics and air filtration to suite office environments. With the BladeCenter S chassis installed, this leaves an extra 4U of space to hold other rack devices.

The Office Enablement Kit has the following benefits:

- Acoustical module

  The Office Enablement Kit comes with an acoustical module that helps in making BladeCenter S quiet for the office environment, while allowing easy access to the BladeCenter S components.

- Locking door

  Security is an important consideration in any office environment. The Office Enablement Kit comes with a front locking door that helps ensure that your data will remain safe and secure in any environment.

- 4U of extra space for other devices

  Different businesses use different tools to enable their office IT. The Office Enablement Kit includes 4U of extra space for other types of IT that an office might need. This space can take any IT that fits into a 4U or smaller standard rack space.

- Easily mobile

  The Office Enablement Kit comes with lockable wheels to make your BladeCenter S easily transportable.

- Contaminants Filter

  To help deploy BladeCenter S in any environment, the Office Enablement Kit can include an optional Contaminants Filter. This filter helps protect the BladeCenter S from dust and dirt and can help prolong the life of your IT. Additional filters are available as options, part number 43X0430 or part number 43X0437 for a pack of four filters.

The enclosure has the following approximate dimensions:

- Height: 611 mm (24.1 in)
- Width: 518 mm (20.4 in)
- Depth: 1156 mm (45.5 in)

4.2.6 Using HC10 blades with the BladeCenter S

To take advantage of the internal storage of the BladeCenter S but still have HC10 workstation blades installed in it, we recommend the following configuration:

- Install one server blade, such as the BladeCenter HS21, in one of the six blade bays in the chassis.

  This server blade can have the SAS expansion card installed, which connects to the SAS Connectivity Modules installed in the chassis. The server blade can then access all the internal SAS storage in the chassis and make it available to the HC10 workstation blades as network shares.

- The remaining five blade bays can be filled with HC10 workstation blades.

With this solution, you have a single, portable, chassis that contains five workstation blades and a large amount of near-local storage.

4.3 Network connectivity

The typical HC10 workstation blade solution is based upon three components:

- A number of HC10 workstation blade, installed in a BladeCenter chassis in the data center, typically one per user, although you might consider sharing systems if your company has shift workers.
- A number of CP20 workstation connection devices, placed in each user’s work space.
- Connection management software, from either Devon IT or from Leostream, installed on a server in the data center that manages the initial connection of CP20s to HC10s. We describe this component in more detail in 4.7, “Connection methods” on page 57.

These workstation blades can be connected to your production network along with your other servers and storage as shown in Figure 4-6.

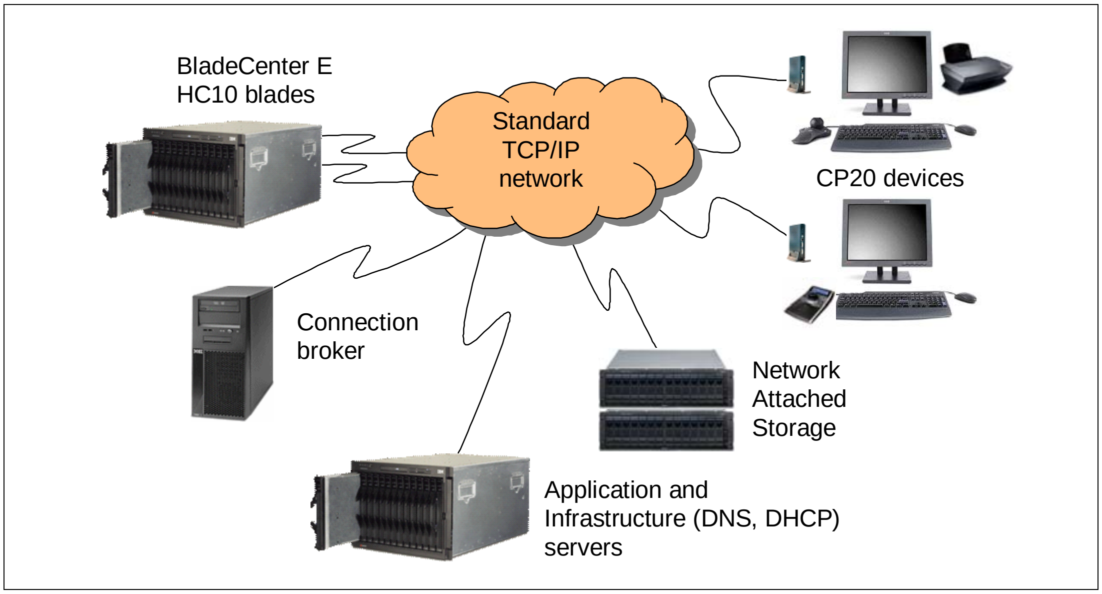


Figure 4-6 Standard HC10 configuration with a connection broker

Figure 4-6 has all systems and devices in your network connected together on the one Ethernet network, which means that the data traffic from the HC10 blades to the CP20 user devices share the same Ethernet network as the production systems. From a security perspective this is not a risk because the CP20 traffic is encrypted.

However, depending on the load of production traffic on the Ethernet network, you might want to consider isolating the devices that communicate using the PC-over-IP protocol, including the compression cards of the HC10 blades, the CP20 workstation connection devices, and the connection broker, as shown in Figure 4-7. Isolating these devices in this way ensures there is sufficient bandwidth to support the PC-over-IP bandwidth requirements.

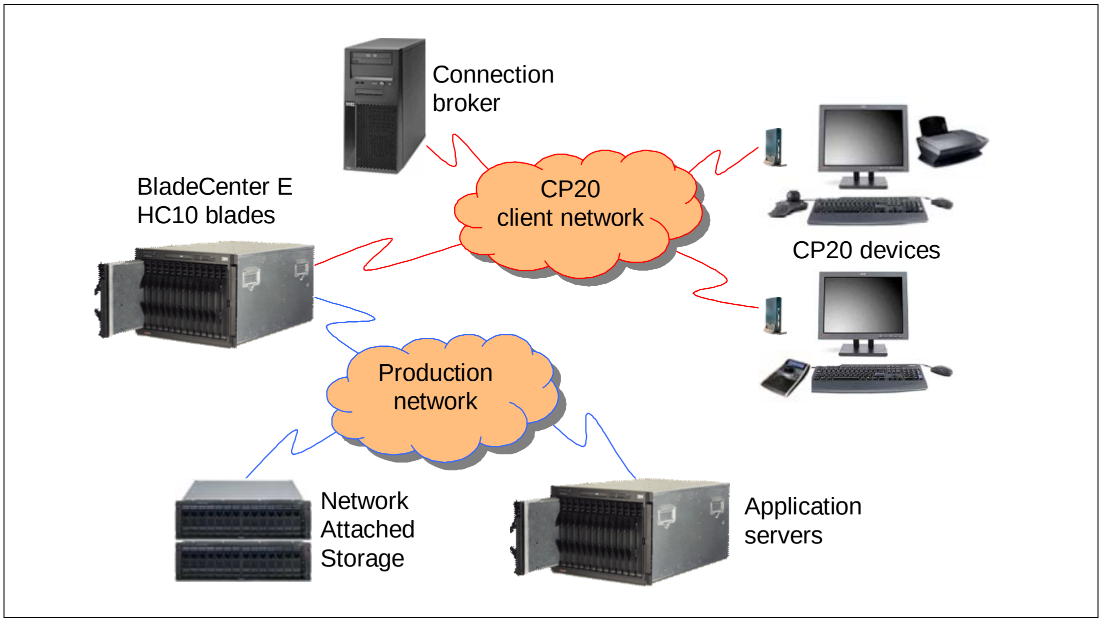


Figure 4-7 Separating the CP20 traffic from the rest of your network

The default configuration for the CP20s and HC10 compression cards is to use DHCP. If you plan to use DHCP (which we recommend), you need to ensure that the DHCP server has the following options set:

- Option 12
- Option 15

Consult the DHCP server documentation on how to configure these options and what value the options should have. In our lab environment, we set Option 12 to the fully-qualified domain name of our name server, which was `itsons.itso.ral.ibm.com`, and we set Option 15 was set to the DNS suffix for our domain, which was `itso.ral.ibm.com`.

4.3.1 I/O modules in the chassis

You need one or two I/O modules installed in the BladeCenter chassis to provide Ethernet connectivity to the HC10 workstation blades and the CP20 workstation connection devices. The supported I/O modules ar:

- A supported Ethernet switch modules as described in 1.4.1, “Ethernet switch modules” on page 15
- The Copper Pass-thru Module as described in 1.4.3, “IBM BladeCenter Copper Pass-thru Module” on page 16
- The Optical Pass-thru Module as described in 1.4.4, “IBM BladeCenter Optical Pass-thru Module” on page 18

Fibre Channel and InfiniBand switch modules are not supported by the HC10 as the HC10 does not have the necessary expansion slot for use by a Fibre Channel or InfiniBand expansion card.

By default, you need two I/O modules: one installed in bay 1 and one installed in bay 2. These I/O modules are used as follows:

- Connectivity to bay 1 of the chassis for use by the HC10 operating system
- Connectivity to the Compression Card and CP20 routing through bay 2 in the chassis

You can change these modules as described in 6.2, “Specifying how the Ethernet switch modules are used” on page 100. For example, If you only have one I/O module installed (for example, in bay 1), then you can configure both network functions to go through bay 1.

4.3.2 Use of the IBM Server Connectivity Module

If you use the IBM Server Connectivity Module for Ethernet connectivity in your BladeCenter chassis (see 1.4.2, “IBM Server Connectivity Module” on page 16), then you need to disable IGMP snooping in the module to allow CP20-HC10 communications.

See the following RETAIN tip H192042 for details on how to do this:

`http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5073011`

4.3.3 TCP/IP ports

Table 4-3 lists the TCP/IP ports that the HC10 and CP20 use. You need to ensure that these ports are opened in firewalls and routers to ensure proper communications between the CP20s and the BladeCenter chassis housing the HC10s.

Table 4-3 Ports used by the HC10 and CP20

Function	Protocol	HC10 & CP20 port number
Dynamic IP	DHCP	UDP 67, 68
Discovery	DNS	TCP/UDP 53
Discovery	SLP	UDP/TCP 427
Web	HTTPS (TLS/SSL)	TCP 443
Web	HTTP	TCP 80 (Redirect to HTTPS)
Management	HTTPS/SOAP/XML	TCP 50000
FW Update	FTP	TCP 21 (Configurable)
Media	IPsec-ESP	N/A (Encrypted)
Media Ctrl	SSL	TCP 8000
Security	HTTPS/SOAP/XML	TCP 50001 (Mutual Auth)
Remote (Brick Only)	RDP (PC-over-IP N/A)	TCP 3389

See RETAIN tip H191730 for related information:

http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072550

4.3.4 VLANs

VLANs are commonly used in the Layer 2 network. You need to consider the number and types of VLANs that are supported, management VLANs, VLAN tagging protocols supported, and specific VLAN configuration protocols implemented (such as Cisco VLAN Trunking Protocol). All switch modules for IBM BladeCenter support 802.10 protocol for VLAN tagging.

4.3.5 Default TCP/IP configurations

The HC10 Workstation Blade contains two IP addresses:

- The IP address on the compression card for communication between the compression card and the workstation connection device.
- The IP address for the workstation blade integrated Ethernet controller, for workstation communication in the network.

The workstation connection device also contains an IP address for communication with the HC10 workstation blade's compression card. See 6.1, "Configuring static IP addresses" on page 96 for more information about changing these IP addresses.

The configuration of the HC10 and CP20 as it ships uses a connection broker with the host name of *ws-broker*. The IP addresses of the CP20 and the HC10 compression card are set to use DHCP.

4.3.6 Latency and bandwidth

There are two parameters: Latency and Bandwidth. IBM testing indicates that a round-trip latency of 60-80 milliseconds or less is needed to produce a good workstation experience with no perceptible lag. With a corporate intranet, this means the HC10 and the workstation device could be separated by as much as 2500 miles. Required bandwidth varies by applications. For textual, 2D data, the required data rate is 1-2 Mbps. 3D applications, such as CAD, require 20-35 Mbps. See Table 4-4 for information about the amount of latency for different distances.

Table 4-4 Measurements of round-trip latency over a test intranet

Distance (miles)	Theoretical fiber latency (msec)	Measured ping (msec)	US distances
0	0	<1	Local
500	7	24	Adjacent States
700	12	36	Adjacent States
1500	25	50	Adjacent States
3000	50	74	Coast to Coast
3000	50	119	Coast to Coast
7000	116	188	Intercontinental

4.3.7 Bandwidth recommendations

Multiple Remote Desktop Devices (CP20s) are connected on a common Ethernet link. This link speed can be at either 100 Mbps or 1000 Mbps. The link speed and the application running in the BladeCenter HC10 Workstation Blade directly affect the user experience at the CP20 remote desktop. If there is not adequate bandwidth allowed for the Ethernet transmission, the user will notice a degradation in the quality of the remote video, which is normally seen as video flicker or screen tearing of the video image.

In video-intensive high resolution environments such as CATIA, limit the number of users to two on a 100 Mbps link and to 15 on a 1000 Mbps link.

Ensure that the BladeCenter HC10 is configured for dynamic bandwidth allocation (this is the default setting). This configuration maximizes the bandwidth that is allocated to each user based on the current network conditions. To set this configuration, set Device Bandwidth Limit to 0 in the HC10 Web interface as described in “Bandwidth option” on page 125.

This configuration allows the I/O Graphics Transmission Adapter to set the transmission bandwidth dynamically. In a worst case scenario, 50 Mbps is allocated for each user in the network.

For the latest bandwidth recommendations, see the following RETAIN tip H191818:

http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072671

4.4 Security

There are many security features built in to the HC10 solution:

- Access to the management interfaces

  The three interfaces are the CP20 local, CP20 Web, and HC10 Web interfaces. Each of these interfaces cannot be accessed without entering a password. This password can be unique for each HC10 and CP20 and can be managed by an administrator.

- Web interface security

  The HC10 and CP20 Web interfaces are secured using SSL and https. All http requests are redirected to https. A CA root certificate is also used to avoid browser certificate warnings.

  Only one user can log into the Web interface at a time. If a user is logged in to the Web interface and a second user attempts to log in, the second user is warned that the target is in use. If the second user decides to log in anyway, the first user is logged out automatically.

- Local data

  There is no local data stored on the CP20. This means that sensitive data is no longer contained on a user's desk and cannot be accessed without a valid connection between the CP20 and HC10.

- Encrypted traffic encrypted between the HC10 and CP20

  A 128-bit SSL tunnel is used for all non-media communications with the CP20. Mutual device authentication that is based on certificates is performed as part of the SSL handshake protocol. Media traffic is encrypted through an 128-bit IPsec ESP tunnel. The keying information for the IPsec tunnel is established securely over the 128-bit SSL tunnel.

- Traffic between the connection broker and the devices secured with SSL

  When a session between an HC10 and a CP20 is disconnected, the connection broker secures the HC10 so that only authorized users can access the Windows desktop. With the Devon IT Connection Broker, the HC10 is put into standby mode so that when the system is accessed, the user is prompted to enter the Windows user ID and password.

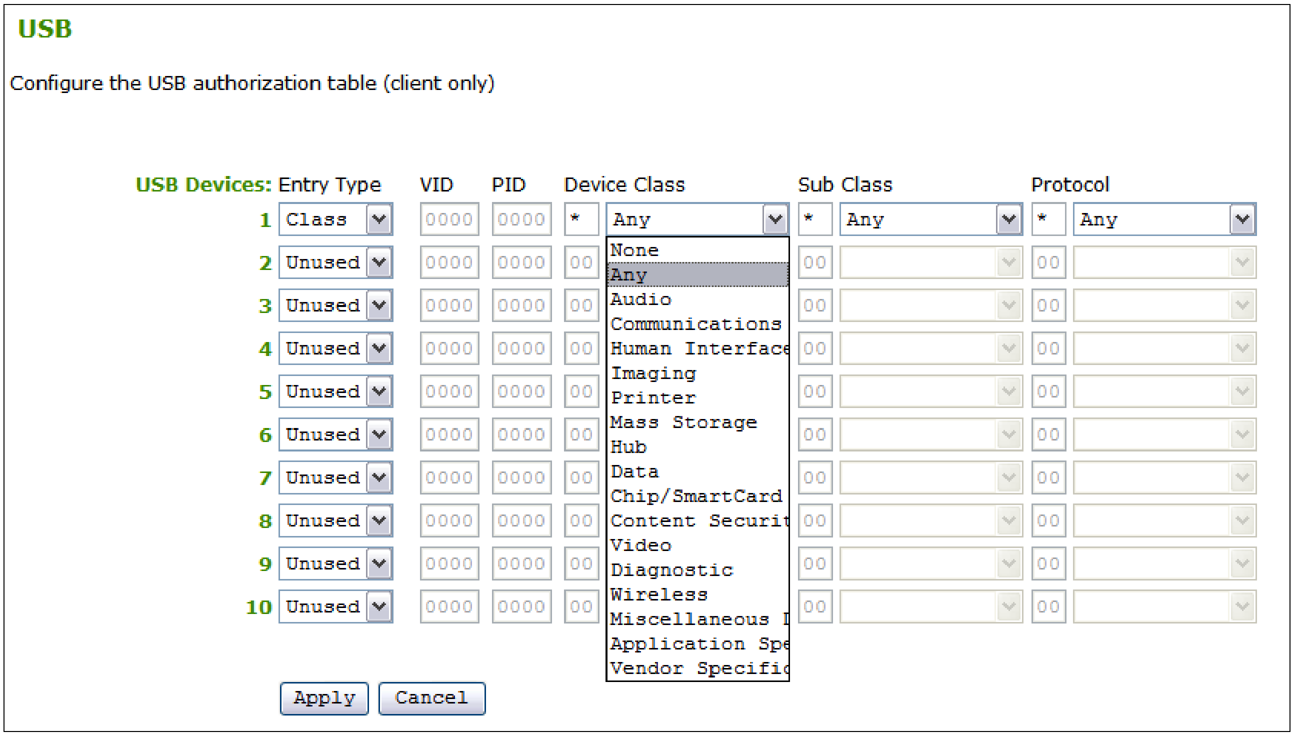
4.5 USB control

A system administrator can limit the USB devices that a user can use.

There is the option to allow all USB devices, no USB devices, or only allow specific USB devices.Thus, if an administrator wants the users to only be able to use human interface devices (mouse, keyboard, and so forth), the USB controls can be set to allow this type of controls. This security feature can be used to ensure that employees do not take sensitive information from the HC10 using a thumb drive.

You configure the USB permissions using the CP20 Web interface, as shown in Figure 4-8. From the drop-down list you can select the type of devices that can be used.

> **Note:** If you plan to restrict the use of certain USB devices, such as thumb drives, it is very important that you also disable the use of USB hubs. Authorization of devices according to user identification, class type, and so forth is done on a per-port basis. Thus, if you allow the use of a hub, then this use allows any type of device to be connected through the hub, regardless of the other USB permissions.



USB

Configure the USB authorization table (client only)

USB Devices:	Entry Type	VID	PID	Device Class		Sub Class		Protocol	
1	Class	0000	0000	*	Any	*	Any	*	Any
2	Unused	0000	0000	00		00		00	
3	Unused	0000	0000	00		00		00	
4	Unused	0000	0000	00		00		00	
5	Unused	0000	0000	00		00		00	
6	Unused	0000	0000	00		00		00	
7	Unused	0000	0000	00		00		00	
8	Unused	0000	0000	00		00		00	
9	Unused	0000	0000	00		00		00	
10	Unused	0000	0000	00		00		00	

Figure 4-8 The USB option showing the different types of devices that can be allowed on the CP20

For more information about this control, see “USB” on page 130.

> **Note:** At the time of writing, there was no way to set USB permissions to multiple devices at one time. You have to set the USB permissions on devices individually.

4.6 Video connectivity

The video cards that are available for the HC10 support one or two monitors. These monitors are connected to the CP20 workstation connection device. Users can choose to have a monitor connected to either the top or the bottom DVI port of the CP20 (see Figure 3-7 on page 36), or both DVI ports.

In addition, because the HC10 is installed in a BladeCenter chassis, the system supports viewing the video from the HC10 through the Advanced Management Module, both locally at the BladeCenter chassis console and remotely using the Advanced Management Module Web browser interface.

Because there are only two ports on the video cards, at most only two of these three video outputs (two digital DVI outputs and the one analog Advanced Management Module output) can be active at the same time. In addition, the video cards impose other restrictions based on what is displayed at the time.

Table 4-5 and Table 4-6 on page 56 list these restrictions. In these tables there are three video sources that can be displayed on either the CP20-attached monitors or the Advanced Management Module console:

- The CP20 interface, where you can configure the CP20 workstation connection device. See 6.3, “CP20 local interface” on page 100.

- The HC10 POST messages.
- The operating system video: Microsoft Windows boot screen and desktop.

The tables show what video sources can be seen out of monitors attached to the three outputs:

- DVI port 1 (the top connector on the rear of the CP20)
- DVI port 2 (the bottom connector on the CP20)
- AMM console (either locally at the BladeCenter chassis or remotely through a browser)

Note: If Monitor Emulation is enabled on a DVI port (as described in “Monitor emulation option” on page 127), then this is the same as a monitor that is attached physically to the port.

We recommend you enable Monitor Emulation.

Table 4-5 shows the video configuration for HC10s with the 2D video card installed. See the table footnotes for explanations.

Table 4-5 NVIDIA NVS 120M 2D video card

	Video to DVI port 1	Video to DVI port 2	AMM console
Video output when only one monitor is connected to DVI port 1 (top port)			
CP20 local interface	Yes	Not connected	Not applicable[a]
HC10 POST messages	Yes	Not connected	No video displayed[b]
Operating system video	Yes	Not connected	No video displayed[b]
Video output when only one monitor is connected to DVI port 2 (bottom port)			
CP20 local interface	Not connected	Yes	Not applicable[a]
HC10 POST messages	Not connected	Yes	Yes
Operating system video	Not connected	Yes	Yes[c]
Video output when two monitors are connected to both DVI ports			
CP20 local interface	Yes	No video displayed	Not applicable[a]
HC10 POST messages	Yes	Yes	No video displayed
Operating system video	Yes	Yes[d]	No video displayed

[a] Not applicable because this is video generated by the CP20 itself. As a result, the AMM console can never be used to view the CP20 local interface.

[b] By design for security reasons, when a single monitor is used and that monitor is connected to DVI port 1, the display cannot be displayed by the AMM console.

[c] To enable operating system video on the AMM console, you must use the NVIDIA Control Panel to mirror the video to both the digital display (DVI port) and the analog display (AMM console).

[d] To enable operating system video across both DVI monitors, you must use the NVIDIA Control Panel to enable Dual view mode.

Table 4-6 shows the video configuration for HC10s with the 2D video card installed. See the table footnotes for explanations.

Table 4-6 NVIDIA FX 1600M 3D video card

	Video to DVI port 1	Video to DVI port 2	AMM console
Video output when only one monitor is connected to DVI port 1 (top port)			
CP20 local interface	Yes	Not connected	Not applicable[a]
HC10 POST messages	Yes	Not connected	No video displayed[b,c]
Operating system video	Yes	Not connected	No video displayed[b]
Video output when only one monitor is connected to DVI port 2 (bottom port)			
CP20 local interface	Not connected	Yes	Not applicable[a]
HC10 POST messages	Not connected	Yes	No video displayed[c]
Operating system video	Not connected	Yes	Yes[d]
Video output when two monitors are connected to both DVI ports			
CP20 local interface	Yes	No video displayed	Not applicable[a]
HC10 POST messages	Yes	No video displayed[c]	No video displayed[c]
Operating system video	Yes	Yes[e]	No video displayed

a. Not applicable because this is video generated by the CP20 itself. As a result, the AMM console can never be used to view the CP20 local interface.

b. By design for security reasons, when a single monitor is used and that monitor is connected to DVI port 1, the display cannot be displayed by the AMM console.

c. The FX 1600M only supports video during POST to one DVI monitor (not the second DVI and not to the AMM).

d. To enable operating system video on the AMM console, you must use the NVIDIA Control Panel to mirror the video to both the digital display (DVI port) and the analog display (AMM console).

e. To enable operating system video across both DVI monitors, you must use the NVIDIA Control Panel to enable Dual view mode.

4.6.1 Limitations with CRT monitors

If a CRT monitor is connected to the CP20 workstation connection device, then under high resolutions or high refresh rates, you might see either corrupted video or no video.

Although the video cards in the HC10s can support resolutions up to 2048x1536, there is a lower limitation by a component in the CP20. This component, called the *Chrontel part*, converts the digital signal coming into the CP20 into an analog signal. The maximum pixel clock on the Chrontel part is 165 MHz. During POST, the video card displays video at the native resolution. For larger CRTs, such as the C220P and P275, the native resolution is 1600x1200 at 75 Hz. This resolution uses a pixel clock higher than 165 MHz and, therefore, no video is displayed.

The same limitation affects resolutions used at the desktop. If a resolution is used that requires a pixel clock higher than 165 MHz, the video driver prunes the higher resolutions and makes the desktop appear larger than the monitor itself by going into pan and scan mode (where the Windows desktop is larger than what is displayed on screen).

For more information, see the following RETAIN tip H191783 at:

http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072597

4.6.2 Other video-related tips

RETAIN tips that are related to video and the Monitor Emulation feature include:

- No video is displayed on the Workstation Connection Device, tip H191777

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072596

- Black screen until Microsoft Windows is reached on the WCD, tip H191763

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072561

- User interaction required at chassis for video on WCD, tip H191777

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072596

- HC10 cannot exit standby mode with mouse or keyboard, tip H191821

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072678

4.7 Connection methods

There are two ways to establish a connection between the HC10 and CP20:

- Connection management software
- Peer-to-peer

4.7.1 Connection management software

The connection manager (also referred to as *the connection broker*) is a software component for creating, maintaining, and removing connections between the HC10s and the CP20s. The software allows for centrally managed connections that can be controlled by a single administrator. As HC10 and CP20 components are added to the environment, their presence, identity, and physical topology are announced to or discovered by one or more instances of a connection manager that executes within the enterprise environment.

When a user attempts to log in to the environment using a CP20, the connection manager recognizes and identifies the particular CP20 unit, identifies an available (or previously assigned) HC10, and creates an association between the two devices.

After this connection is made, the connection manager monitors the state of the connection (*Connected* or *Disconnected*) to provide session management but does intervene in communication between the connected endpoints.

There three ways connections are formed between the HC10 and CP20:

- Fixed seating
- Free seating
- Pooling

Tip: The way devices are connected (free, fixed, and pooling) is controlled by the connection broker.

Fixed seating

Fixed seating is when each CP20 is assigned to a specific HC10 and this connection is the only connection that can be made. In a fixed seating environment, the same CP20 always connects to the same HC10. Figure 4-9 shows a diagram of fixed seating.

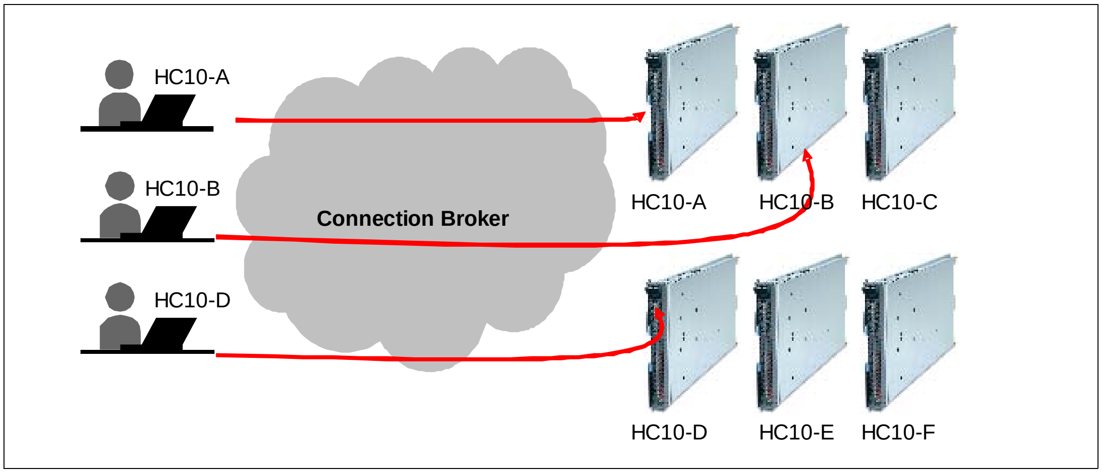


Figure 4-9 Fixed seating connection

In Figure 4-9, when a user sits in front of a CP20 that is assigned to HC10-A, then that CP20 always connects to HC10-A. Logon security is handled by the operating system on the HC10.

Free seating

With *free seating*, it is the user that is associated with a specific HC10, not the CP20 as with fixed seating. Thus, that specified user can sit in front of any CP20 device, enter the user name, and be connected to that user's HC10 workstation blade. Figure 4-10 shows an example of free seating.

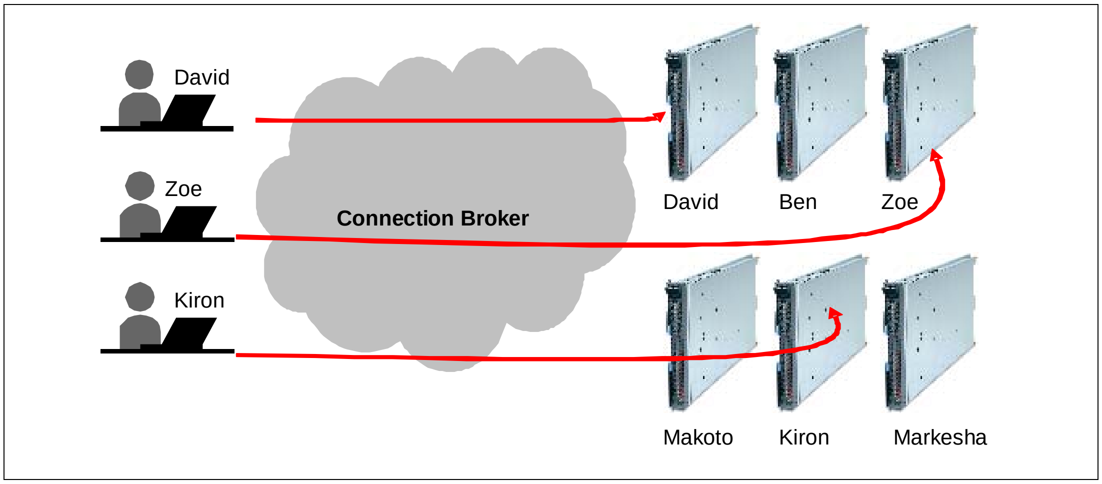


Figure 4-10 Free seating connection

In Figure 4-10, regardless of where the user Zoe sits in the office, when she logs in, she is connected to the same workstation blade every time.

Depending on the connection broker implementation, the user supplies a user name but does not supply a password. As with fixed seating, logon security is handled by the operating system on the HC10.

Pooling

Pooling is a super-set of free seating. Instead of a user being linked to exactly one workstation blade in the case of free seating, with pooling, that user is assigned a workstation from a pool of HC10s.

Refer to Figure 4-11 for an example of pooling. When user Kiron logs in, an authentication database is queried to determine to which pool of workstation blades Kiron is eligible to connect. *Pool B* is returned. The broker then chooses any workstation blade from Pool B and assigns it to Kiron. To ensure user security with pool, Kiron has to enter both a user ID and password before the authentication and assignment process begins.

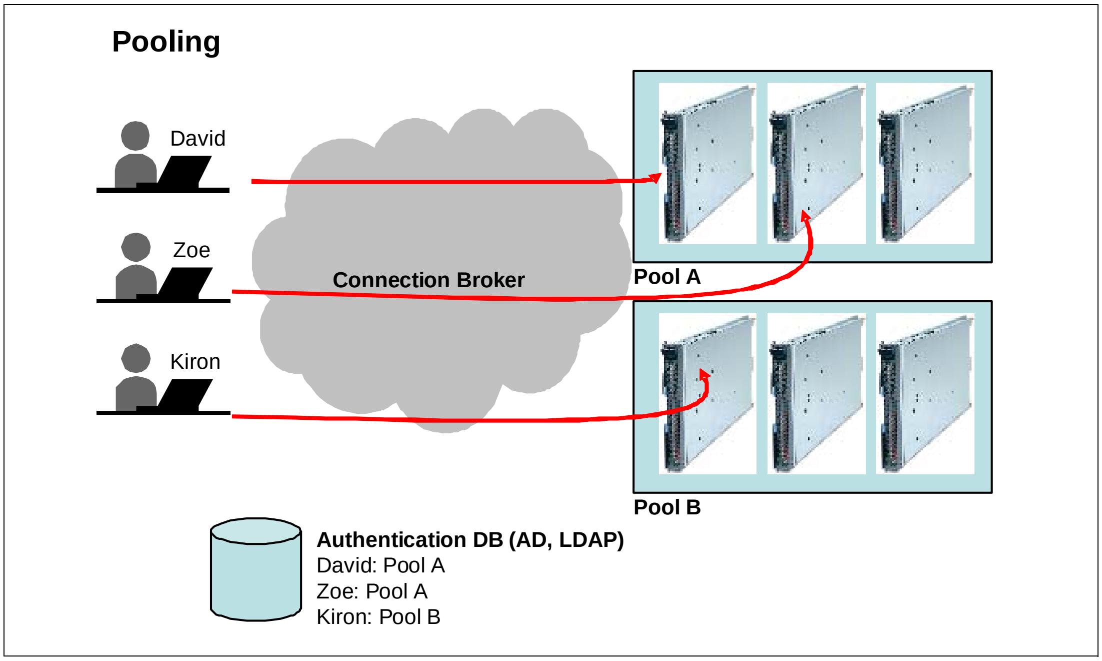


Figure 4-11 Pooling connection example

You can implement pooling in a number of ways, including the following examples:

- Workstations in Pool A can contain highly configured workstations (more memory and faster CPU), whereas Pool B can contain workstations with a standard configuration.
- Pool A systems can have one set of applications installed, whereas Pool B can have another set.
- Pool A can be configured for Spanish speakers, whereas Pool B can be configured for English speakers.

Pooling is a form of free seating, and if you set the pool size to be only one system, then pooling and free seating yield the same result.

4.7.2 Peer-to-peer connections

The alternative to using a Connection Broker is to connect using a peer-to-peer connection. *Peer-to-peer connections* allow for connections between the HC10 and CP20 without any additional software. There are two options for connection:

- Session

  A session connection is when you input the IP address of the HC10 to which you want to connect, which allows you to connect directly to a specific HC10.

- Discovery

  The discovery option presents the user with a list of up to 10 available HC10 blades (that is, not already in session) from which the user can select one to connect to.

Figure 4-12 shows these two options.

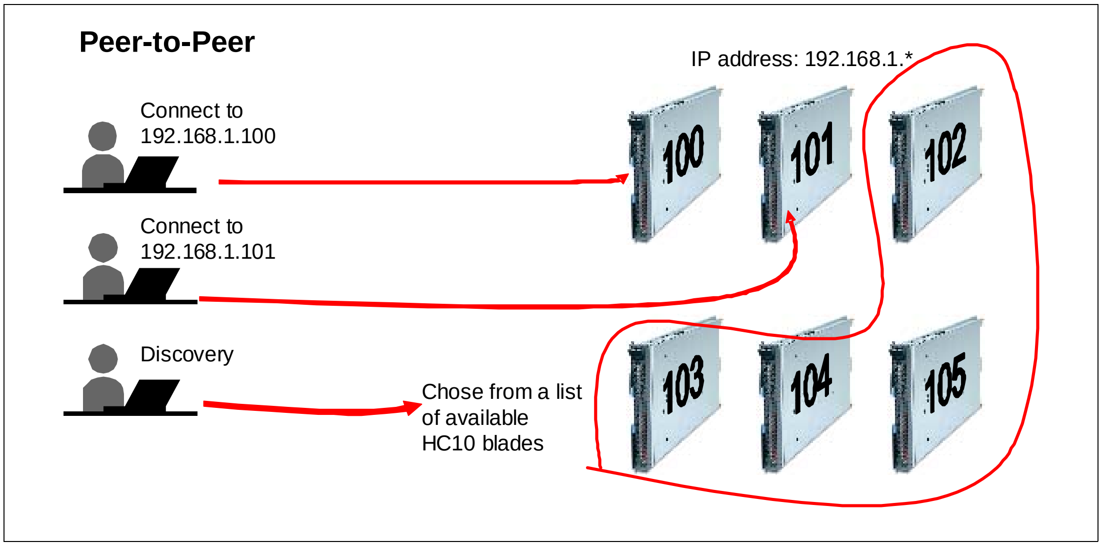


Figure 4-12 Peer-to-peer connections

4.8 Devon IT Connection Manager

Devon IT Connection Manager supports both free seating and fixed seating. The current version does not support pooling or authentication with an LDAP or Active Directory® server.

Devon IT Connection Manager is implemented as an virtual machine-based appliance. You need to download and install either VMware Player or VMware Server prior to running the software. The minimum system requirements for the machine that hosts the VM are:

- VMware Server 1.03 or VMware Player 1.04
- 768 MB RAM
- Pentium® 4 processor at a clock speed of 2 GHz
- 40 GB hard drive space

The broker supports the use of a static IP address or one assigned by DHCP, but we recommend that you use a static IP address. You should ensure that the host name is *ws-broker* because this is the name that the CP20 and HC10 compression cards are configured to look for as they shipped.

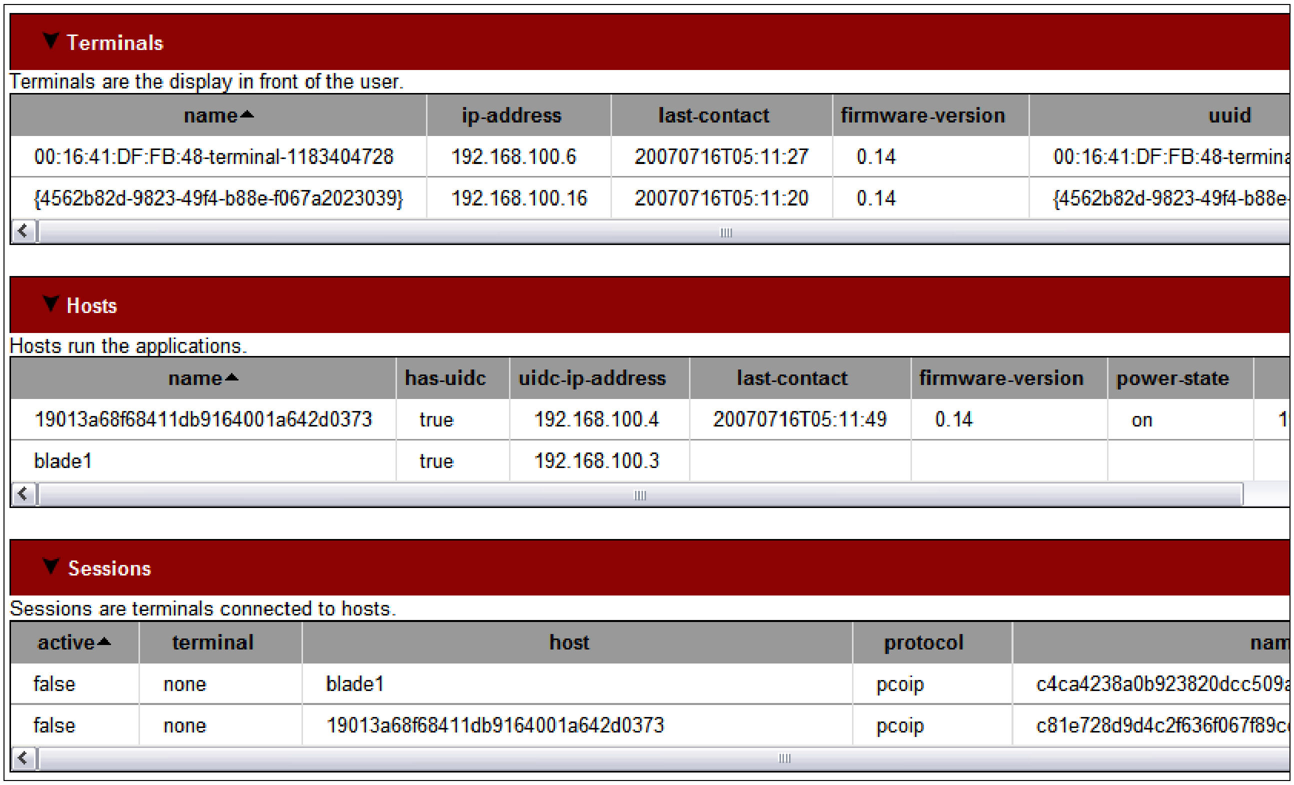
The connection broker has two management interfaces, a Web browser-based graphical user interface (GUI) and a command-line interface (CLI). The Web browsers supported are:

- Firefox 1.5 or later
- Internet Explorer® 7 or later

In the Web-based interface, the devices in the network display as soon as they are powered on and configured to look for a connection broker of host name *ws-broker* (which is the default). The Web interface is split into three tables as shown in Figure 4-13:

- The “Terminals” table lists all CP20 devices that have contacted the broker.
- The “Hosts” table lists all HC10 that contact the broker. The IP address listed is that of the compression card.
- The “Sessions” table lists all active sessions.

You can left click a CP20 or HC10 to get more details about the device in a pane on the right, including an event log that is related to that device. You can also right-click any CP20, HC10, or session to see the available actions.



▼ Terminals

Terminals are the display in front of the user.

name▲	ip-address	last-contact	firmware-version	uuid
00:16:41:DF:FB:48-terminal-1183404728	192.168.100.6	20070716T05:11:27	0.14	00:16:41:DF:FB:48-termina
{4562b82d-9823-49f4-b88e-f067a2023039}	192.168.100.16	20070716T05:11:20	0.14	{4562b82d-9823-49f4-b88e-

▼ Hosts

Hosts run the applications.

name▲	has-uidc	uidc-ip-address	last-contact	firmware-version	power-state	
19013a68f68411db9164001a642d0373	true	192.168.100.4	20070716T05:11:49	0.14	on	1
blade1	true	192.168.100.3				

▼ Sessions

Sessions are terminals connected to hosts.

active▲	terminal	host	protocol	nam
false	none	blade1	pcoip	c4ca4238a0b923820dcc509a
false	none	19013a68f68411db9164001a642d0373	pcoip	c81e728d9d4c2f636f067f89c

Figure 4-13 Browser interface of the Devon IT connection broker

At the time of this writing, Devon IT supported two methods of connection:

- Fixed seating

  This method is used to establish a connection from a specific CP20 to a specific HC10. With this method, the user connects automatically to the HC10 from the CP20.

- Free seating

  This method is used to allow a connection between one CP20 and one HC10 but with more flexibility. When a user attempts to establish a connection (by clicking the **Connect** button on the CP20 screen), a prompt displays so that the user can enter the name to connect as. The HC10 that the user is connected to has the same name as the user name that is entered. Although there can always be only one CP20 connected to one HC10, free seating allows a user to log in to a specific blade from any CP20.

When connections are established, they are shown in the Web-based interface. This interface shows whether the connection exists, which machines (HC10 and CP20) are involved in the connection, and what type of protocol is being used (which will always be PC-over-IP).

There is a search feature within the Connection Management software that allows for ease of management of a large CP20-HC10 environment. The search feature works by filtering out results based on a query. You can apply a search based on of the attributes that are table headings. This search feature allows an administrator to navigate easily through a large number of devices to find information quickly and efficiently. The search feature can also be useful for searching for a group of devices that all begin with the same name (for example, *Floor_1*) or for devices that have the same level of firmware (for example, *0.13*). To view the different search options, see 5.1.4, “Search filter features” on page 79.

Another key component of the Connection Management software is the ability to update the firmware of all the devices in the environment. Firmware can be uploaded to the Connection Management software and then pushed out to all the CP20s and HC10s.

There are two options for firmware updates:

- Immediate

  An immediate update disconnects any connections automatically, installs the new firmware, and resets the compression card. The downside to doing this update during working hours is that it disrupts the user’s connection and take a few minutes to install before the user can re-establish the connection.

- Background

  A background update installs the update the next time there is no connection present. Therefore, if a device is not involved currently in a session when the firmware is pushed out, it is placed automatically in a queue to receive the update. The downside to this method is that if a user never disconnects their CP20 from the HC10, the device is not updated.

As to a firmware update strategy, we recommend that you use background as the primary method to deploy firmware, then use immediate when only a few systems remain (for example, after a week or so).

For details about how to apply the Devon IT Connection Management software in your environment, see 5.1.3, “Updating firmware” on page 74.

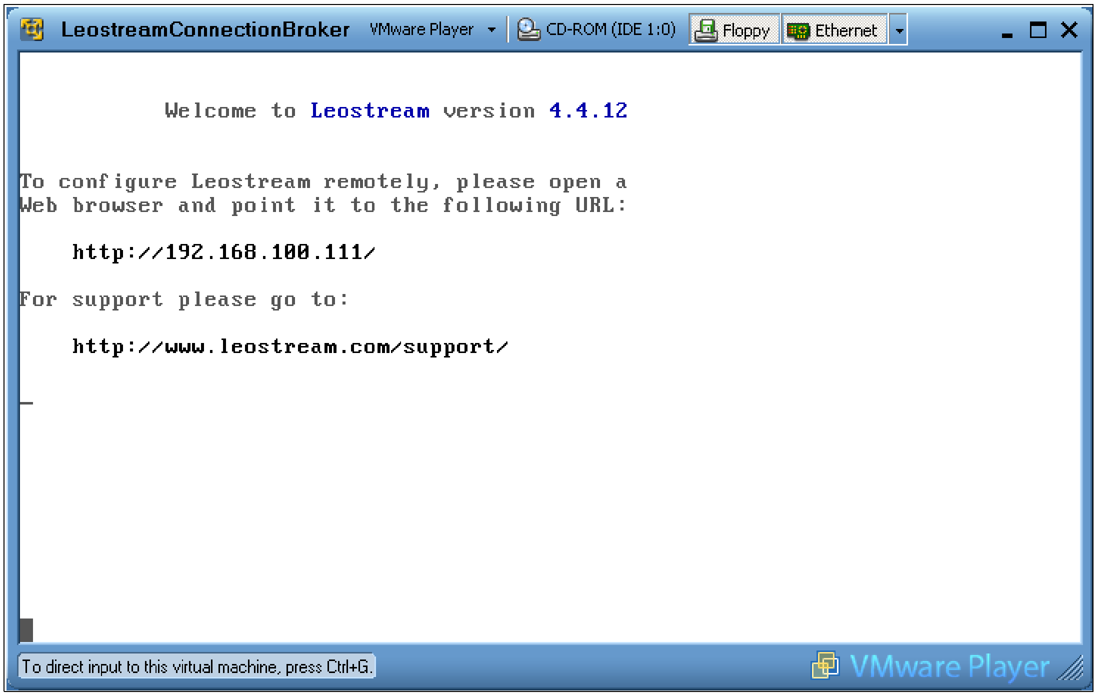
4.9 Leostream Hosted Desktop Connection Broker

The Leostream Hosted Desktop Connection Broker runs as a Virtual Appliance and requires the following minimum hardware:

- Pentium 4™ (or equivalent) 1.5 GHz or faster
- 1.5 GB memory
- 8 GB of hard drive space

You need to use the VMware Converter tool to load the Virtual Appliance image into the virtualization layer.

After you have the software running, you see a panel similar to Figure 4-14, which shows the IP address of the Web-based administrator interface. Go to this IP address using a Web browser. You use this Web interface to perform all administration functions.


LeostreamConnectionBroker
VMware Player
CD-ROM (IDE 1:0)
Floppy
Ethernet
To direct input to this virtual machine, press Ctrl+G.
VMware Player

```
          Welcome to Leostream version 4.4.12


To configure Leostream remotely, please open a
Web browser and point it to the following URL:

    http://192.168.100.111/

For support please go to:

    http://www.leostream.com/support/
```

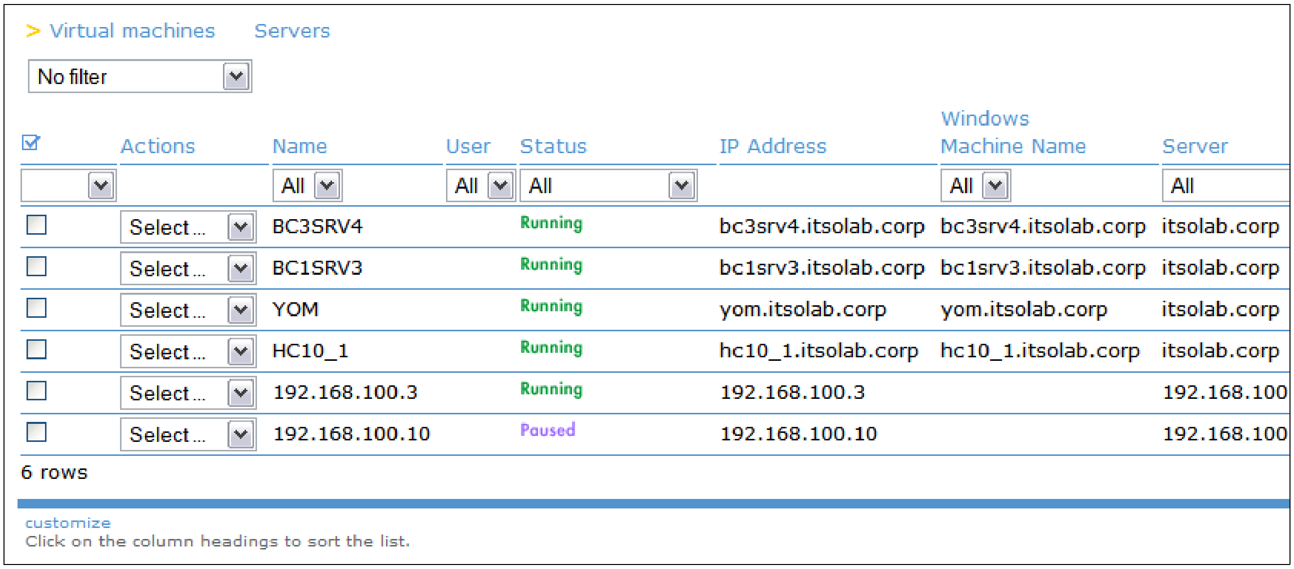
Figure 4-14 The Leostream virtual appliance up and running

> **Note:** If you need to change the IP address of the Connection Broker, then from the console press Alt-F2, and login as user name *admin* with a password of *leo*. You then have the option to change the network settings.

To log in to the Web interface, use the following credentials:

- User name: *admin*
- Password: *leo*

You then have to enter a license key and accept the license terms. The administration interface is accessed using a Web browser, as shown in Figure 4-15.



☑	Actions	Name	User	Status	IP Address	Windows Machine Name	Server
		All	All	All		All	All
□	Select ...	BC3SRV4		Running	bc3srv4.itsolab.corp	bc3srv4.itsolab.corp	itsolab.corp
□	Select ...	BC1SRV3		Running	bc1srv3.itsolab.corp	bc1srv3.itsolab.corp	itsolab.corp
□	Select ...	YOM		Running	yom.itsolab.corp	yom.itsolab.corp	itsolab.corp
□	Select ...	HC10_1		Running	hc10_1.itsolab.corp	hc10_1.itsolab.corp	itsolab.corp
□	Select ...	192.168.100.3		Running	192.168.100.3		192.168.100
□	Select ...	192.168.100.10		Paused	192.168.100.10		192.168.100

6 rows

customize
Click on the column headings to sort the list.

Figure 4-15 Leostream Connection Broker main panel

The Leostream Hosted Desktop Connection Broker provides central management of the HC10-CP20 connections as well as hosted desktop sessions running other remote viewer protocols such as RDP and VNC and using either physical or virtual hardware.

As shipped, the HC10s and CP20s are configured to use a connection broker with the host name *ws-broker*. Because the Leostream broker is configured this way by default, you can establish connectivity from the devices to the connection broker without any further configuration.

There are two additional ways that you can configure the devices to connect to the broker:

- Entering the IP address of the connection broker manually into each HC10 and CP20
- Enabling SLP discovery and having the connection broker discover the HC10-TC10

After the HC10 blades have been discovered, they are displayed in the Connection Broker, alongside any other hosted desktop resource that is available.

Administrators can then divide the blades into a series of resource pools and determine how they are allocated to users, either randomly selected from a Pool or permanently assigned to a particular user.

While it is possible to store user information within the Connection Broker, it is more common to use an external authentication server (Microsoft Active Directory, Novell eDirectory, IBM Tivoli Directory Server, or Open LDAP). The use of an external authentication server lets the hosted desktop assignment be tied to the existing user profiles within the Authentication Server.

For more detailed information about how to apply the Hosted Desktop software to your environment, see 5.2, “Leostream Hosted Desktop software” on page 82.

For product information, see the Leostream Hosted Desktop Connection Broker Web page available at:

`http://www.leostream.com/productVHDC.html`

5

Setup with a connection broker

As we describe in 4.7.1, “Connection management software” on page 57, the connection manager (also referred to as *the connection broker*) is a software component for creating, maintaining, and removing connections between the HC10s (hosts) and the CP20s (terminals). The software allows for centrally managed connections that can all be controlled by a single administrator.

In this chapter, we discuss how to use the BladeCenter HC10 solution with connection broker software. We discuss how to configure the environment with Devon IT Connection Management software and with Leostream Hosted Desktop software and provide information about different security options that can help ensure a secure environment.

It is expected that most customers will implement a connection broker to manage connections. In fact, the HC10 solution is pr-configured and shipped to work this way:

- The CP20 and HC10 compression card use DHCP-assigned IP addresses
- Connection management is enabled in both the HC10s and CP20s
- Devices are configured to connect to a broker with a host name of *ws-broker*

For testing or adhoc connections, the CP20 and HC10 also support peer-to-peer connections as described in Chapter 6, “Configuration options” on page 95.

Topics that we cover in this chapter include:

- 5.1, “Devon IT Connection Broker” on page 66
- 5.2, “Leostream Hosted Desktop software” on page 82
- 5.3, “Security” on page 94

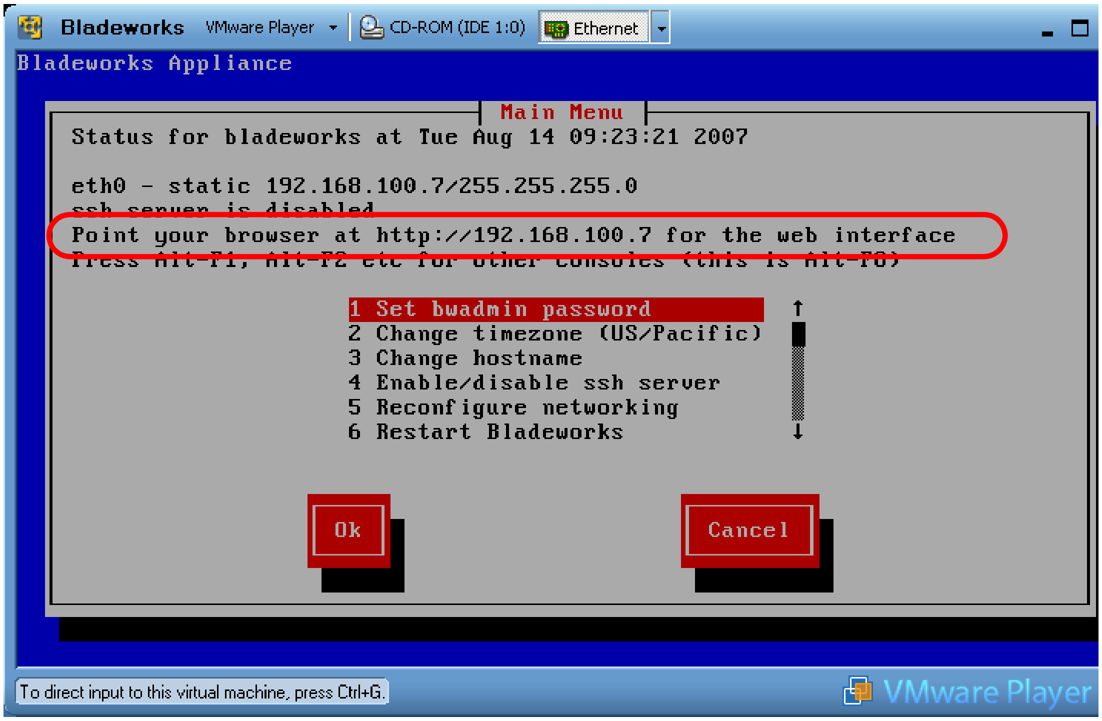
5.1 Devon IT Connection Broker

The HC10 and CP20 devices have a default configuration to use DHCP for their IP addresses and a connection broker for their connections. Both devices use *ws-broker* as the host name of the connection management software and can communicate and create connections as soon as the software is installed on a server. Thus, when the devices are added to the network, they are ready to establish connections.

The Devon IT Connection Management software allows you to connect using either *fixed seating* or *free seating*. The idea of fixed seating is that each CP20 (client or terminal) can always connect to one HC10 (host). With fixed seating, the client and host have the same name in the Connection Management software. The other option to connect is free seating, which allows a user to log in to a specific HC10 from any CP20 in the office.

We do not cover installation of the broker software in this paper, so you need to follow the installation instructions that come with the software. However, at the time of this writing, the installation simply involved decompressing the virtual machine files, running VMware Player or another VMware engine, and following prompts to configure the administrator password, time zone, and network address.

After installing the Connection Management software, enter the virtual machine's IP address (as shown in Figure 5-1) into a Firefox or Internet Explorer 7.0 browser. (IE 7 lists the 250 most recent entries in various logs whereas Firefox will list the most recent 2500 entries.)



```
Status for bladeworks at Tue Aug 14 09:23:21 2007

eth0 - static 192.168.100.7/255.255.255.0
ssh server is disabled
Point your browser at http://192.168.100.7 for the web interface
Press Alt-F1, Alt-F2 etc for other consoles (this is Alt-F8)
```

1 Set bwadmin password
2 Change timezone (US/Pacific)
3 Change hostname
4 Enable/disable ssh server
5 Reconfigure networking
6 Restart Bladeworks
Ok
Cancel
To direct input to this virtual machine, press Ctrl+G.
VMware Player

Figure 5-1 Devon IT Connection Management software VMware virtual image

This action opens the Web interface for the Connection Management software. There are four options on the main panel of this interface as shown in Figure 5-2:

- Quick start

  The quick start option provides instructions on how to use the Connection Management software.

- Web browser-based administration tool

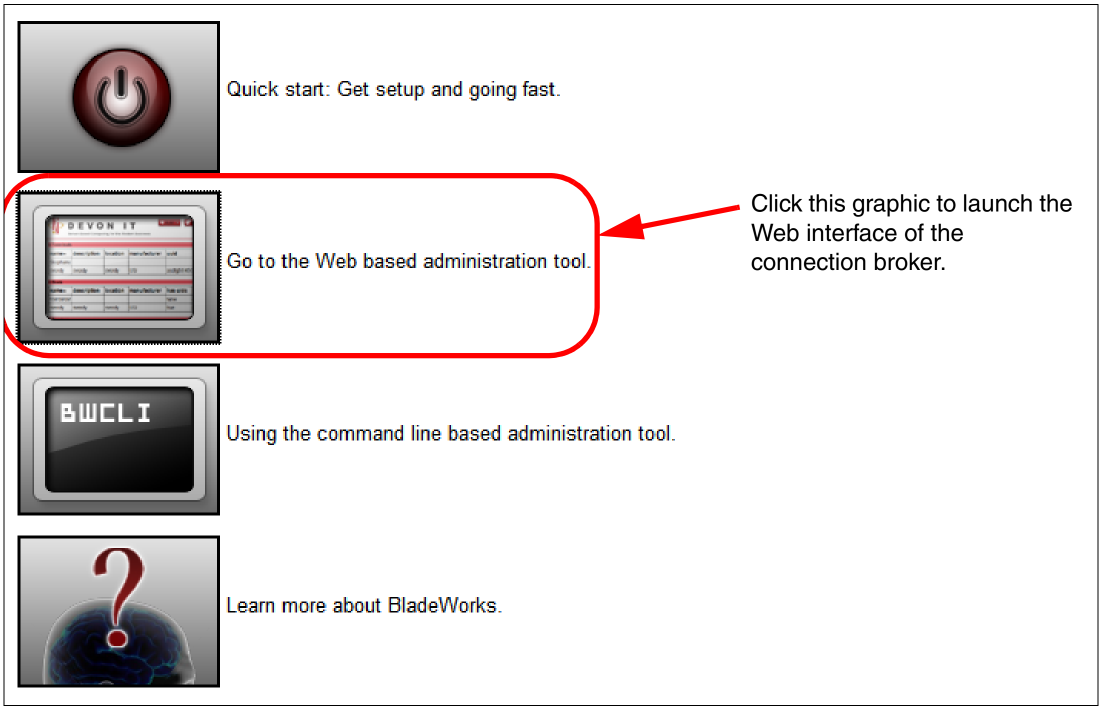
  The Web browser-based interface allows you to manage the HC10 and CP20 environment through a Web interface. (The majority of this section is devoted to describing this interface.)

- Command line based administration tool

  The command-line option provides information about how to use the CLI interface. Managing the CP20 and HC10 environment can be done through the Web interface, but the same tasks can also be achieved with the command-line interface.

- Learn more

  The learn more option allows you to view all of the documentation, including a terminology section, a section on the components and how they react, how to use the management tools, and support information. To begin managing the environment, click the Web based administration tool (see Figure 5-2).



Quick start: Get setup and going fast.

Go to the Web based administration tool.

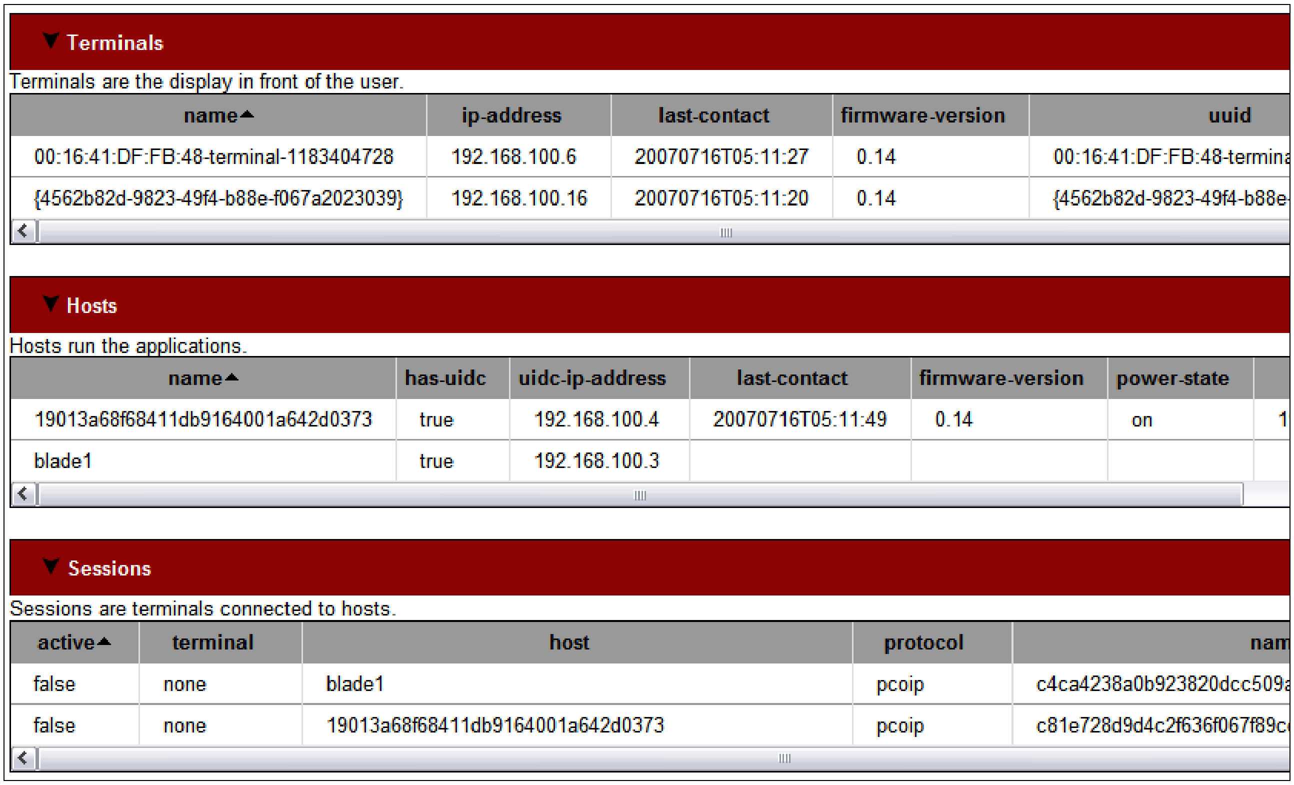
Using the command line based administration tool.

Learn more about BladeWorks.

Click this graphic to launch the Web interface of the connection broker.

Figure 5-2 Main window of the Web-based Connection Management software

The Web based administration tool shows the HC10s (hosts), CP20s (terminals), and connections (sessions) that are present. Figure 5-3 shows an example with active devices and sessions.



▼ Terminals

Terminals are the display in front of the user.

name▲	ip-address	last-contact	firmware-version	uuid
00:16:41:DF:FB:48-terminal-1183404728	192.168.100.6	20070716T05:11:27	0.14	00:16:41:DF:FB:48-termina
{4562b82d-9823-49f4-b88e-f067a2023039}	192.168.100.16	20070716T05:11:20	0.14	{4562b82d-9823-49f4-b88e-

▼ Hosts

Hosts run the applications.

name▲	has-uidc	uidc-ip-address	last-contact	firmware-version	power-state	
19013a68f68411db9164001a642d0373	true	192.168.100.4	20070716T05:11:49	0.14	on	1
blade1	true	192.168.100.3				

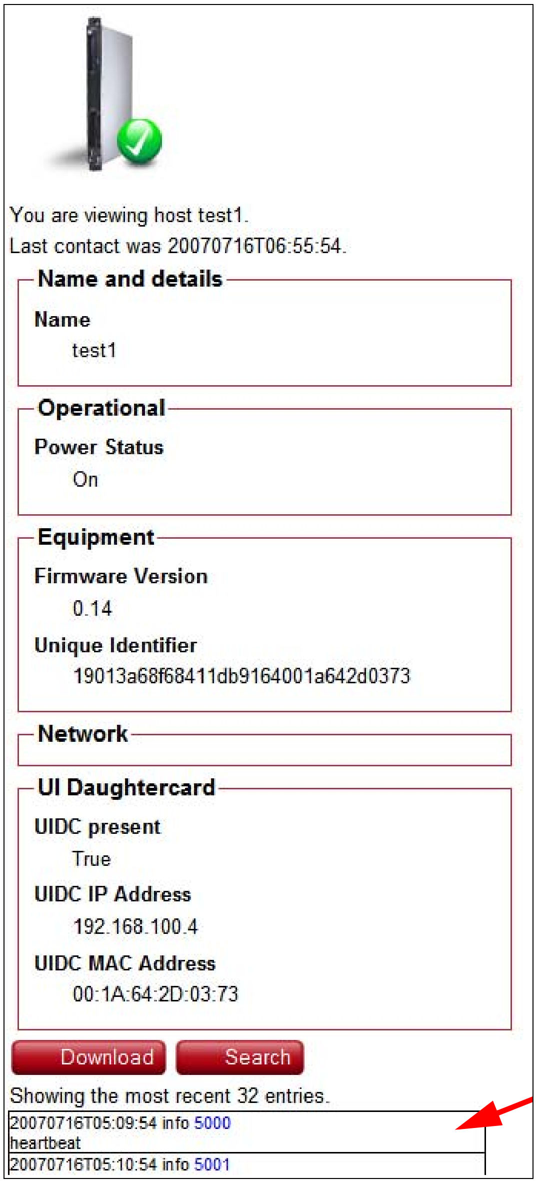
▼ Sessions

Sessions are terminals connected to hosts.

active▲	terminal	host	protocol	nam
false	none	blade1	pcoip	c4ca4238a0b923820dcc509a
false	none	19013a68f68411db9164001a642d0373	pcoip	c81e728d9d4c2f636f067f89c

Figure 5-3 The discovery of devices in the Web administration tool

To view more details about a specific device, click it and a details pane opens on the right side of the window. Figure 5-4 shows an example of this details pane.



You are viewing host test1.

Last contact was 20070716T06:55:54.

Name and details

Name
test1

Operational

Power Status
On

Equipment

Firmware Version
0.14

Unique Identifier
19013a68f68411db9164001a642d0373

Network

UI Daughtercard

UIDC present
True

UIDC IP Address
192.168.100.4

UIDC MAC Address
00:1A:64:2D:03:73

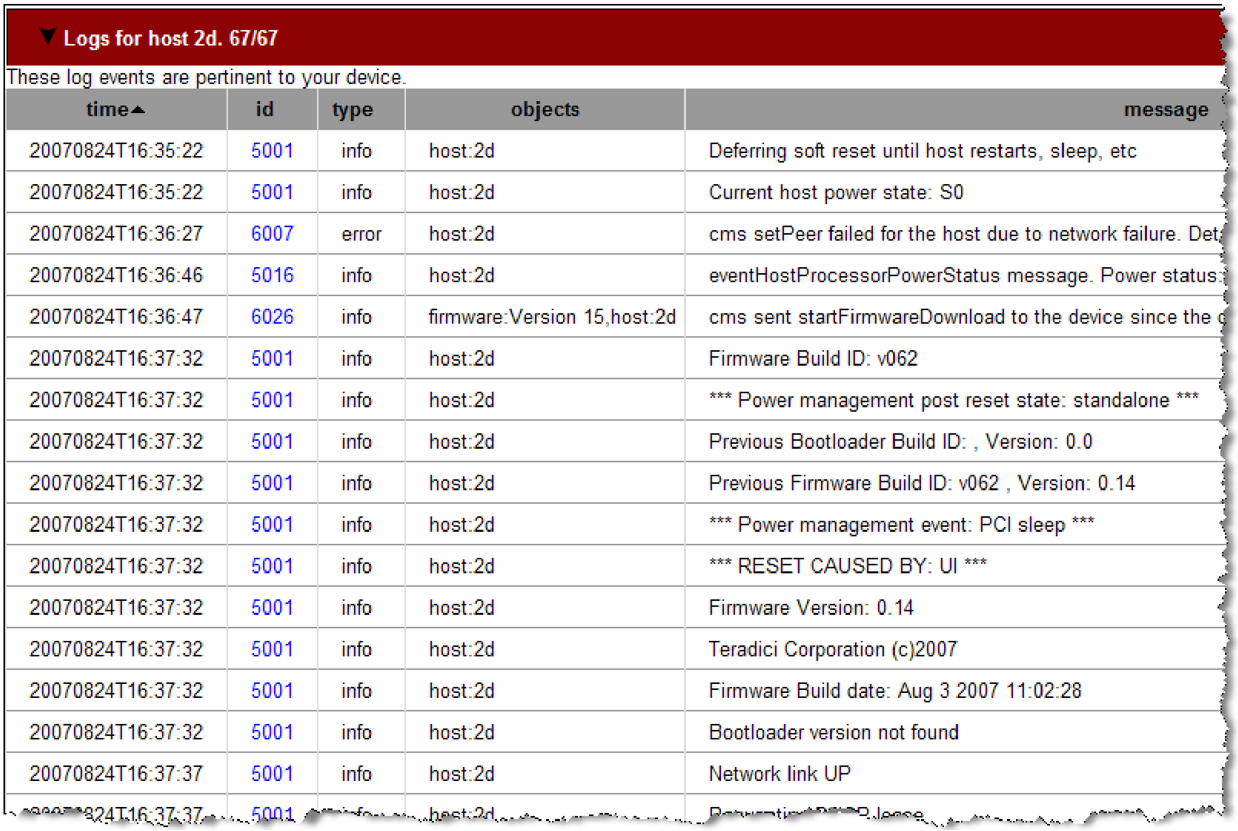
Showing the most recent 32 entries.

```
20070716T05:09:54 info 5000
heartbeat
20070716T05:10:54 info 5001
```

Figure 5-4 Details of a specific device that has been discovered

With an HC10, the Network field is blank by default. You can, if you want, use this field to enter the IP address of the network controller that Windows uses when running on the HC10. The Network field of the CP20 displays the IP address and MAC address of the CP20.

The details pane also includes the most recent log entries as shown in Figure 5-4. An easier way to view them, however, is to click **Search** to shows a larger window of the log messages, similar to that shown in Figure 5-5.



▼ Logs for host 2d. 67/67

These log events are pertinent to your device.

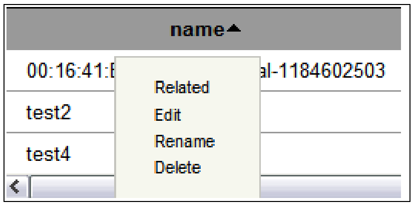
time▲	id	type	objects	message
20070824T16:35:22	5001	info	host:2d	Deferring soft reset until host restarts, sleep, etc
20070824T16:35:22	5001	info	host:2d	Current host power state: S0
20070824T16:36:27	6007	error	host:2d	cms setPeer failed for the host due to network failure. Det
20070824T16:36:46	5016	info	host:2d	eventHostProcessorPowerStatus message. Power status:
20070824T16:36:47	6026	info	firmware:Version 15,host:2d	cms sent startFirmwareDownload to the device since the
20070824T16:37:32	5001	info	host:2d	Firmware Build ID: v062
20070824T16:37:32	5001	info	host:2d	*** Power management post reset state: standalone ***
20070824T16:37:32	5001	info	host:2d	Previous Bootloader Build ID: , Version: 0.0
20070824T16:37:32	5001	info	host:2d	Previous Firmware Build ID: v062 , Version: 0.14
20070824T16:37:32	5001	info	host:2d	*** Power management event: PCI sleep ***
20070824T16:37:32	5001	info	host:2d	*** RESET CAUSED BY: UI ***
20070824T16:37:32	5001	info	host:2d	Firmware Version: 0.14
20070824T16:37:32	5001	info	host:2d	Teradici Corporation (c)2007
20070824T16:37:32	5001	info	host:2d	Firmware Build date: Aug 3 2007 11:02:28
20070824T16:37:32	5001	info	host:2d	Bootloader version not found
20070824T16:37:37	5001	info	host:2d	Network link UP
20070824T16:37:37	5001	info	host:2d	Requesting DHCP lease

Figure 5-5 Log details of the HC10

The log view has a search filter field that lets you search for particular log entries.

You can also click **Download**, as shown in Figure 5-4 on page 69, to save the log entries to a text file.

You can perform certain tasks by right-clicking the device to which you want to make changes. This opens a menu with the options Related, Edit, Rename, and Delete as shown in Figure 5-6.



name▲
00:16:41:[illegible]al-1184602503
test2
test4

Figure 5-6 Options when you right-click a device

When you click **Related**, it shows automatically a device with the same name as the one you clicked. For example, if you have a host called *test2* and a terminal called *test2*, and you right-click the host and click **Related**, the following search query is executed:

```
"+terminal:test2" OR "+name:test2"
```

The results show both the host and the terminal with the name *test2*. To revert back to the original list, simply clear the text from the search field. For more information about searching functions with Connection Management, see 5.1.4, “Search filter features” on page 79.

When you click **Edit**, a menu displays on the right side that allows you to edit the details of the device. Clicking **Rename** allows you to rename a device. You would choose this option, for example, if you want to implement fixed seating, which is achieved by naming both a CP20 and an HC10 the same name.

Clicking **Delete** removes the device from the list, although it displays automatically later. CP20s displays within five minutes without needing to restart them; however, you need to reset the PC-over-IP processor in the HC10 and restart the HC10 before it displays in the list.

You can also add a terminal or host manually by clicking either **Add** → **Terminal** or **Add** → **Host** (see Figure 5-7). This action creates a menu on the right that allows you to complete the details about the device manually. You do not normally need to do this.

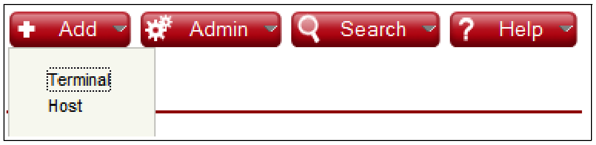
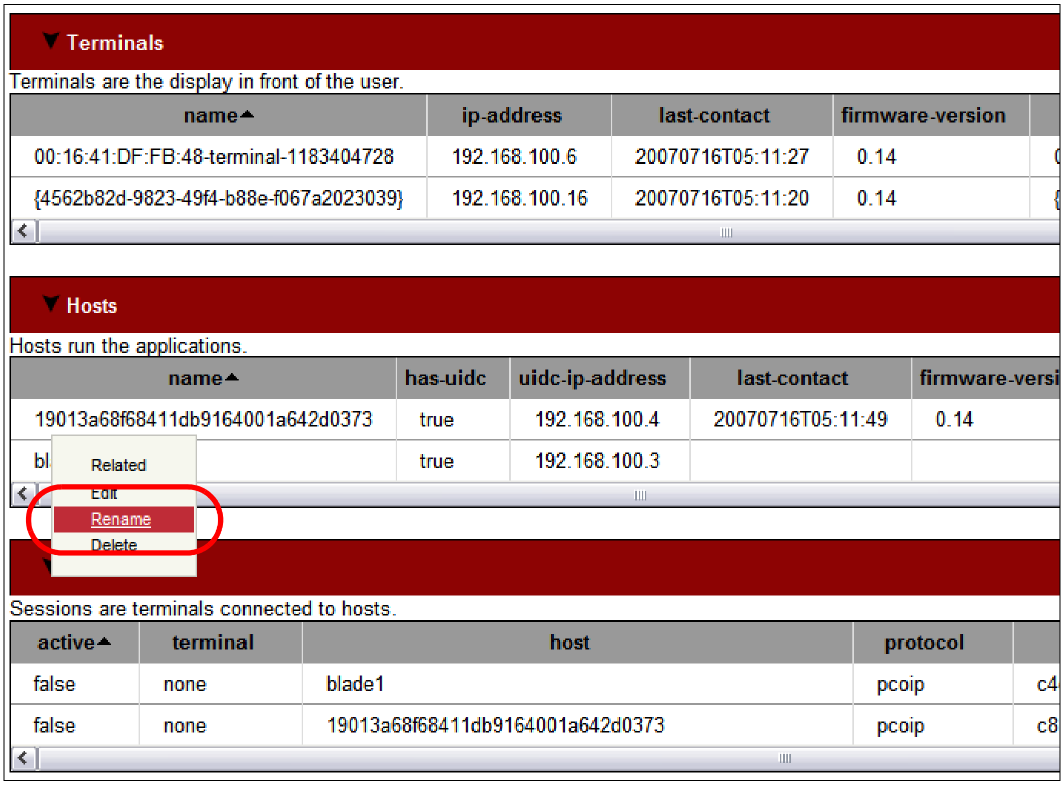


Figure 5-7 Manually adding a terminal or a host

5.1.1 Free seating

A free seating connection allows a user to access a specific HC10 from any location. See “Free seating” on page 58 for a discussion about free seating. To configure this type of connection, follow these steps:

1. Right-click the HC10 that you want to rename and click **Rename** (see Figure 5-8).



Terminals

Terminals are the display in front of the user.

name	ip-address	last-contact	firmware-version	
00:16:41:DF:FB:48-terminal-1183404728	192.168.100.6	20070716T05:11:27	0.14	(
{4562b82d-9823-49f4-b88e-f067a2023039}	192.168.100.16	20070716T05:11:20	0.14	{

Hosts

Hosts run the applications.

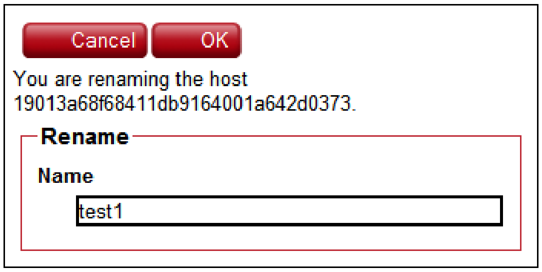
name	has-uidc	uidc-ip-address	last-contact	firmware-versi
19013a68f68411db9164001a642d0373	true	192.168.100.4	20070716T05:11:49	0.14
bl	true	192.168.100.3		

Sessions are terminals connected to hosts.

active	terminal	host	protocol	
false	none	blade1	pcoip	c4
false	none	19013a68f68411db9164001a642d0373	pcoip	c8

Figure 5-8 Renaming a device in Connection Management

2. Enter the name that you want to have in the Name field and click **OK** (see Figure 5-9). Each HC10 must have a unique name.



You are renaming the host 19013a68f68411db9164001a642d0373.

Rename

Name: test1

Figure 5-9 Renaming a device in Connection Management

3. On the CP20, click **Connect**. You are prompted to enter a user name. Enter the name that you just assigned to the HC10 and press **OK** (see Figure 5-10).

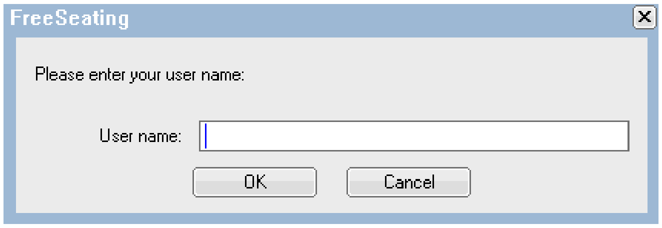


Figure 5-10 Free seating connection with Connection Management

4. The CP20 connects to the HC10 that you entered, and you see the Windows desktop that is running on the HC10 now display on the monitor or monitors that are attached to the CP20. You also see an active session between the host and terminal under the Sessions table in the connection broker. (You might need to refresh the browser window or press the refresh icon on the top-right corner of the session table.)

5.1.2 Fixed seating

To establish a fixed seating connection (each HC10 can be logged in to by one specific CP20), the HC10 (host) and CP20 (terminal) must be renamed to the same name. For example, there can be three CP20s and three HC10s. The three CP20s can be named *User1*, *User2*, and *User3*. The HC10s must also be named *User1*, *User2*, and *User3* in order to create a connection. See "Fixed seating" on page 58 for a discussion about fixed seating.

Tip: You might want to implement a single fixed-seating connection for testing purposes, even if most of your devices use free seating.

To set up a fixed seating connection, follow these steps:

1. Rename all of the HC10s (see "Free seating" on page 72 for an example).
2. Rename the CP20s to the same names as the HC10s, as you did for the HC10s.
3. Click **Connect** at one of the CP20 that you just renamed, and it establishes a session with the HC10 of the same name. Under Sessions, you now see an active session between the host and terminal that you just configured.

5.1.3 Updating firmware

The Devon IT Connection Management software allows you to update the firmware of all of the devices automatically. To do this, follow these steps:

1. At the top of the Web interface of the connection broker, click **Admin** → **Firmware** (see Figure 5-11). This opens a new browser tab or window in which the available firmware versions are shown.

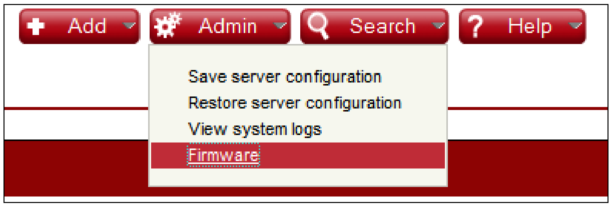


Figure 5-11 Access to the page in which you can update firmware

2. To add a new firmware version, click **Add** → **Firmware** (see Figure 5-12) to open details on the right hand side of the page.

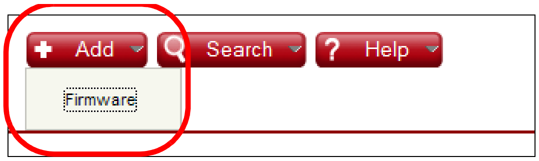
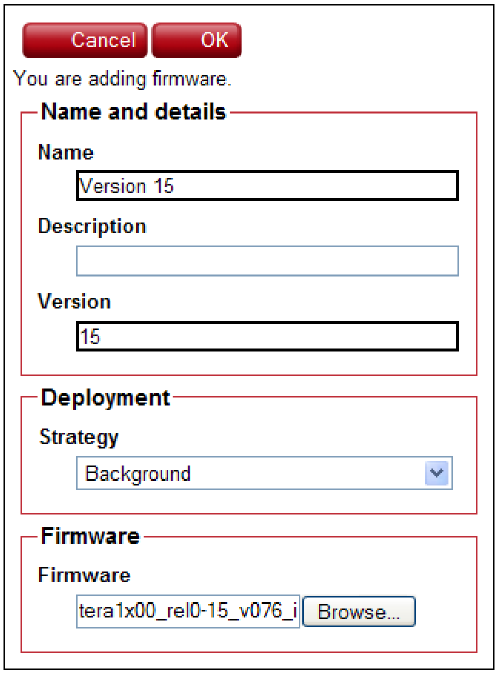


Figure 5-12 Adding firmware in the Connection Management software

3. Fill in the appropriate Name, Description, and Version fields (see Figure 5-13). The name must be unique, otherwise the new firmware overwrites prior firmware with the same name.

   Both the Name and Version fields are required. The contents of version field is used to display to the user what version is being applied; it is not used as the actual version number when compared to the currently installed firmware. The description field is optional.



You are adding firmware.

Name and details

Name: Version 15

Description:

Version: 15

Deployment

Strategy: Background

Firmware

Firmware: tera1x00_rel0-15_v076_i

Figure 5-13 Name and details field when adding firmware

4. Next, you must decide on the deployment strategy. Chose either **Immediate** or **Background** as the strategy (see Figure 5-14):

   – The **Immediate** option updates all the devices automatically, even if there are active connections. It forces all of the connections to end and update the devices.

   – The **Background** option waits until the connection is terminated and then applies the firmware and reset the devices.

   To read more about these options, see 4.8, “Devon IT Connection Manager” on page 60.

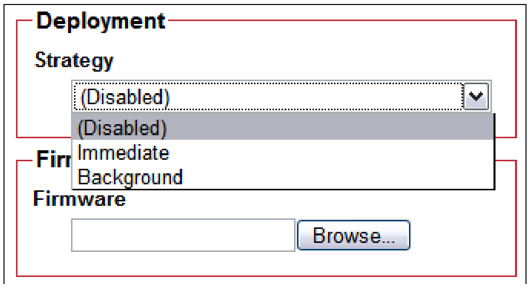
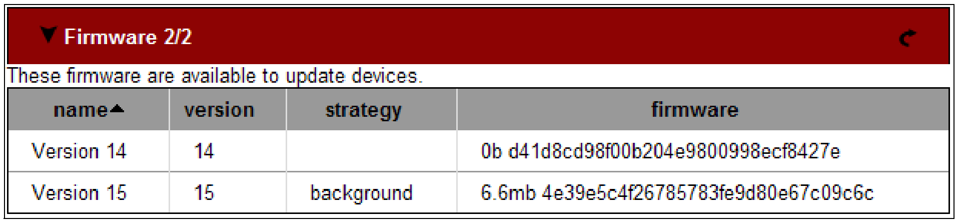


Figure 5-14 Choosing a deployment strategy for the firmware updates

5. Under Firmware, click **Browse**. Then, locate the file that you want to upload (this must be a .app file) and click **Open**.

6. Click **OK** to begin the upload process.
7. The firmware is now uploaded to the broker and is shown in the list of available firmware updates (see Figure 5-15).



These firmware are available to update devices.

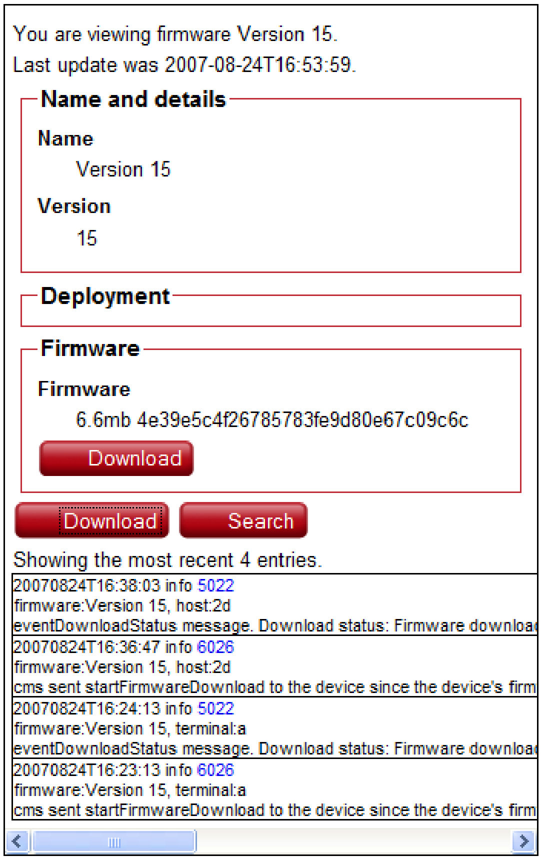
name▲	version	strategy	firmware
Version 14	14		0b d41d8cd98f00b204e9800998ecf8427e
Version 15	15	background	6.6mb 4e39e5c4f26785783fe9d80e67c09c6c

Figure 5-15 The updated list of available firmware

You can see from Figure 5-15 that there are two versions of firmware uploaded. When Version 15 was uploaded, the firmware that was previously uploaded (Version 14) was set automatically to a strategy of (disabled) which appears simply as blank because only one firmware can be active at any one time.

8. Now the firmware is ready to be applied to the HC10 compression cards and to the CP20s. Because you selected *background* as the update strategy, the broker waits until devices are not in session before updating them. Had you selected *immediate*, then the update process would begin right away, terminating sessions if necessary.

When you select a firmware from the list, the right pane displays the logs that are associated with updates, as shown in Figure 5-16.



You are viewing firmware Version 15.
Last update was 2007-08-24T16:53:59.

Name and details

Name
Version 15

Version
15

Deployment

Firmware

Firmware
6.6mb 4e39e5c4f26785783fe9d80e67c09c6c

Showing the most recent 4 entries.

```
20070824T16:38:03 info 5022
firmware:Version 15, host:2d
eventDownloadStatus message. Download status: Firmware downloa
20070824T16:36:47 info 6026
firmware:Version 15, host:2d
cms sent startFirmwareDownload to the device since the device's firm
20070824T16:24:13 info 5022
firmware:Version 15, terminal:a
eventDownloadStatus message. Download status: Firmware downloa
20070824T16:23:13 info 6026
firmware:Version 15, terminal:a
cms sent startFirmwareDownload to the device since the device's firm
```

Figure 5-16 Firmware log that shows which devices have been updated

Tip: You can click **Search** to display the log messages in a full browser window. You can also click **Download** to save the log messages to a text file.

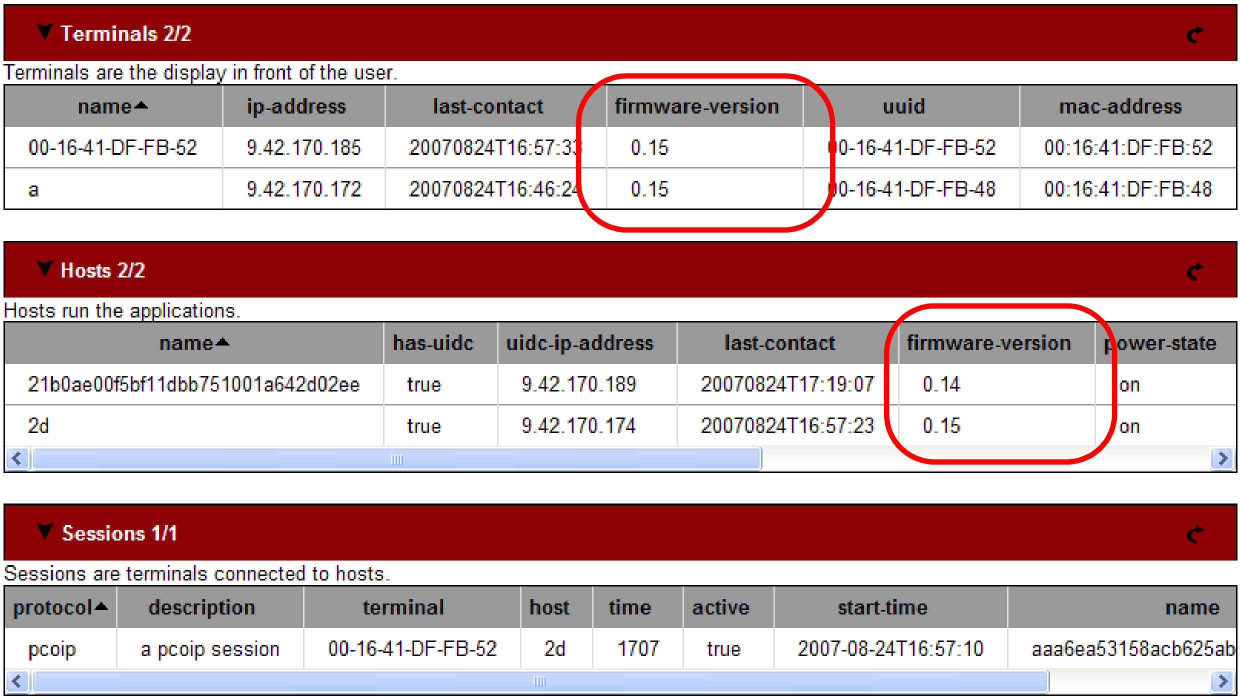
A log entry is made when a device downloads a firmware update from the connection broker. A second message displays in the log when the download to the device is completed. See Example 5-1 for messages from two devices being updated.

Tip: The messages in the log as shown in the Web interface (Figure 5-16) show the newest messages at the top.

Example 5-1 The messages logged in the broker about firmware updates

```
cms sent startFirmwareDownload to the device since the device's firmware version
is outdated. Device's current firmware version is:0.14 while the latest firmware
version is: 15

eventDownloadStatus message. Download status: Firmware download done successfully.

cms sent startFirmwareDownload to the device since the device's firmware version
is outdated. Device's current firmware version is:0.14 while the latest firmware
version is: 15

eventDownloadStatus message. Download status: Firmware download done successfully.
```

You can see on the main page of the Web interface what firmware version each device has as shown in Figure 5-17.



▼ Terminals 2/2

Terminals are the display in front of the user.

name▲	ip-address	last-contact	firmware-version	uuid	mac-address
00-16-41-DF-FB-52	9.42.170.185	20070824T16:57:33	0.15	00-16-41-DF-FB-52	00:16:41:DF:FB:52
a	9.42.170.172	20070824T16:46:24	0.15	00-16-41-DF-FB-48	00:16:41:DF:FB:48

▼ Hosts 2/2

Hosts run the applications.

name▲	has-uidc	uidc-ip-address	last-contact	firmware-version	power-state
21b0ae00f5bf11dbb751001a642d02ee	true	9.42.170.189	20070824T17:19:07	0.14	on
2d	true	9.42.170.174	20070824T16:57:23	0.15	on

▼ Sessions 1/1

Sessions are terminals connected to hosts.

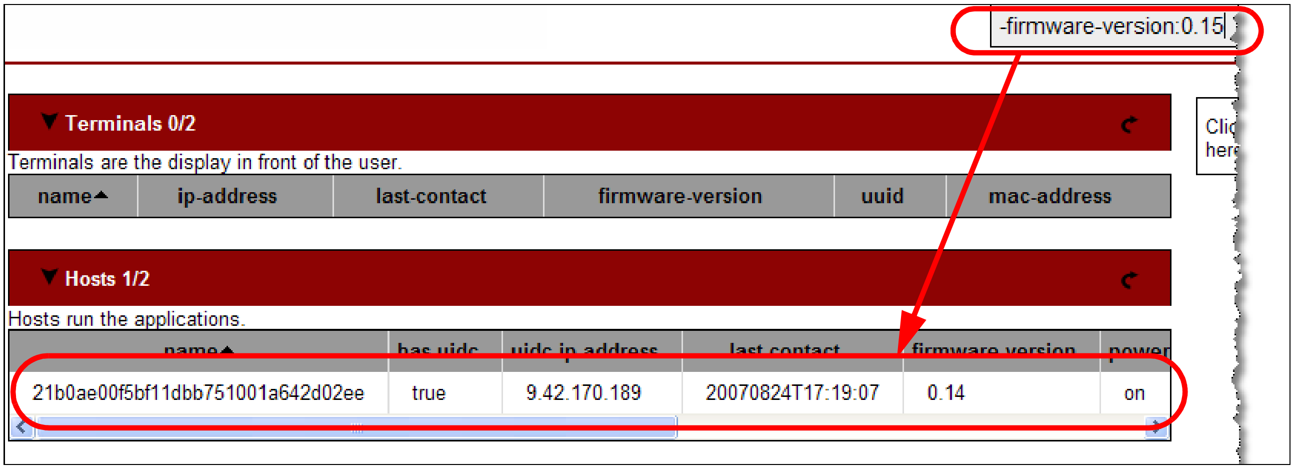
protocol▲	description	terminal	host	time	active	start-time	name
pcoip	a pcoip session	00-16-41-DF-FB-52	2d	1707	true	2007-08-24T16:57:10	aaa6ea53158acb625ab

Figure 5-17 The front page of the broker interface showing the firmware version each device has

If you have a large number of devices, it will be difficult to scan through them to see what devices do not have the latest firmware applied. The solution is to use the search filter capability to display all devices that do not have a specific version (0.15 in our example). The syntax to use is:

```
-firmware-version:0.15
```

Putting this in the search field shows only the devices that do not have version 0.15 installed, as shown in Figure 5-18.



-firmware-version:0.15

Terminals 0/2

Terminals are the display in front of the user.

name▲	ip-address	last-contact	firmware-version	uuid	mac-address

Hosts 1/2

Hosts run the applications.

name▲	has uidc	uidc ip address	last contact	firmware version	power
21b0ae00f5bf11dbb751001a642d02ee	true	9.42.170.189	20070824T17:19:07	0.14	on

Figure 5-18 Displaying only the devices that do not have 0.15 applied.

See 5.1.4, “Search filter features” on page 79 for details about the search filter syntax.

Characteristics of firmware updates

Important points regarding firmware updates include:

- No checks are made on the file that you specify to upload. It does not check that the file you select is in fact a valid firmware file.
- You can upload one firmware file at a time, but you can upload additional firmware files if you desire. However, only one will be active (that is, either *background* or *immediate*). All others are marked automatically as *disabled*. You can edit any previously uploaded firmware files to change their strategy or other fields. If you change a disabled file to an active strategy, then the existing active file is set inactive.
- If you use a firmware name that already exists, then that file is overwritten without warning.
- The version number field is mandatory and is used to display what version is applied in messages that appear during updates. The broker does not use this value to determine the actual version number of the firmware. Instead it reads this directly from the uploaded file.
- The broker decides whether to apply firmware to a specific device by comparing the version of the currently installed firmware to the version it reads from the uploaded file. If these values are different, then the broker attempts to apply the firmware. This method applies to both upgrades and downgrades of firmware.
- If you select *immediate*, then updates begin straight away in small groups of devices. If a user is connected at the time a device is scheduled to be updated, the user is disconnected immediately.
- If you select *background*, then the broker waits for the session to terminate before considering the device eligible for a firmware update. If the user never disconnects the session, then the CP20 and HC10 might never be updated. The administrator should monitor the Firmware Version field to check the status of your devices and, if necessary,

change the strategy to *immediate* to force an update. Use the filter `-firmware-version:x.xx` to show all devices that do not have a specific firmware version.

5.1.4 Search filter features

The Devon IT Connection Broker offers a search filter option to display a subset of HC10s, CP20s, and session. In a large installation with many devices, it might be difficult to find the device that you want to view. The search feature allows you to filter out results by entering text into the search field. As you enter text, the devices shown narrow to only those that match the text.

There are also advanced search options. Other ways to search include:

- *Quoting*: You can put double quotation marks (“ “) around items that contain spaces. You can also use back slashes to escape various characters. For example:

  ```
  "Lab Blade"
  ```

- *Attributes*: To limit a match to particular attributes, use a prefix of the attribute name (column name) followed by a colon (:). For example, you can use the following search option to find all items with IBM as a manufacturer:

  ```
  manufacturer:ibm
  ```

  Every item has a type. For example, to limit the results to just hosts, you can use:

  ```
  type:host
  ```

  If you enter only the attribute name and a colon, then only items with that field and a value for it are shown. For example, enter the following search option shows all items that have an IP address:

  ```
  ip-address:
  ```

- *Exact match*: Normally, any table entry that contains the search string displays in the search results. For example, if you search for *lab*, then it matches *laboratory* and *collaborate*. If you want an exact match, then put a plus sign (+) before the word that you enter. For example, the following search option shows only results that match *lab* exactly:

  ```
  +lab
  ```

  An exact match is also case sensitive. (Matches are normally not case sensitive.) To specify an exact match to a specific attribute, put the plus sign (+) before the attribute:

  ```
  +name:lab
  ```

  If your term needs quoting, then put the entire search string inside double quotation marks:

  ```
  "+name:lab 20"
  ```

- *Not*: Use a minus sign (-) to exclude items. For example, to exclude any reference to *John*, use the following search option:

  ```
  -john
  ```

  Similarly, you can use this syntax to show all devices that do not have a specific firmware. For example, to show devices that do not have version 0.15 installed, use this search filter:

  ```
  -firmware-version:0.15
  ```

- *Or*: If you type multiple words, then all of the words must be found in an entry to result in a match (conceptually there is an `AND` between each word). You can specify that the results must match at least one of the words typed by using OR (which must be in uppercase). For example, the following search option finds items with either *john* or *jane* in them:

```
john OR jane
```

- *Grouping* and *complex queries*: You can put round brackets (parentheses) around words to group them for more complex queries. For example:

  ```
  (a b) OR -(c d) OR e
  ```

  Table 5-1 shows some grouping examples.

Table 5-1 Search filter examples

Example	Meaning
`-description:`	Return items that do not have a description.
`john OR lab`	Return items that have john or lab in them.
`(john OR jane OR tim) lab`	Return items that have lab and at least one of john, jane, or tim.
`-(john OR jane OR tim) lab`	Return items that have lab, but not any of john, jane, or tim.

5.1.5 Security lockup at session disconnect

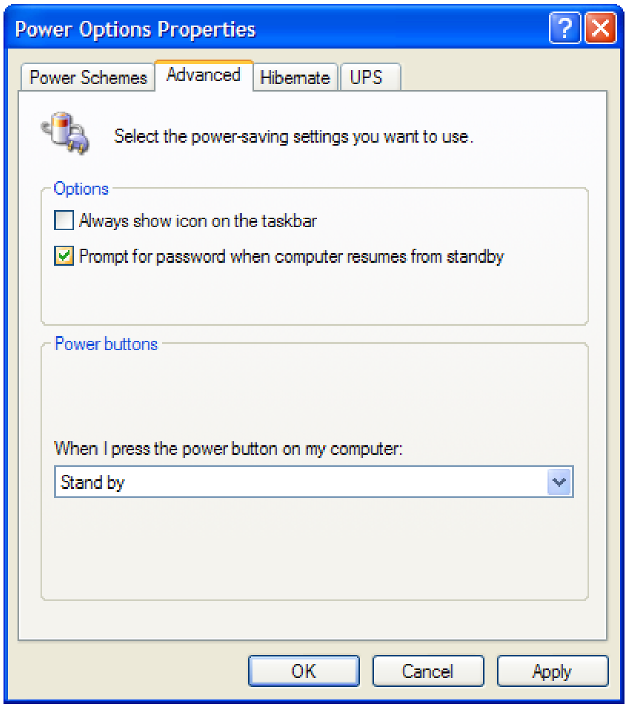
The Devon IT Connection Broker does not authenticate users by prompting for a password. Instead, it relies on the Windows operating system that is running on the HC10 to ensure that only authorized users can log on.

When the user first connects to the HC10, that user is prompted by Windows to enter a user ID and password, assuming a password has been set in the operating system. (Both Windows XP and Vista allow you to start Windows without asking the user for a password. However, we recommend that you change this option to require a user ID and password.)

When a session is terminated, either by simply breaking the connection or by the user pressing the **Session disconnect** button on the CP20 (see Figure 3-7 on page 36), to maintain security, Windows must be rendered secure. The Devon IT Connection Broker renders Windows secure by emulating a “soft power off” command, which is the equivalent of pressing the power off button on a regular PC for less than four seconds. The intent is to put the HC10 into standby mode.

By default, Windows XP reacts to a soft power off event by initiating a shutdown. To ensure that the HC10 is secure when the session is disconnected, we recommend that you reconfigure Windows XP so that the operating system performs a standby instead. To make this change, perform the following steps on the HC10:

1. Open Control Panel and launch the Power Options applet.
2. Click the Advanced tab. The Power Options Properties window opens, as shown in Figure 5-19.



Select the power-saving settings you want to use.

Options

☐ Always show icon on the taskbar

☑ Prompt for password when computer resumes from standby

Power buttons

When I press the power button on my computer:

Stand by

Figure 5-19 Windows XP Power Options

3. Ensure that “Prompt for password when computer resumes from standby” option is selected.
4. Under Power buttons, select **Stand by** for the “When I press the power button on my computer” option. (The default is Shutdown.)
5. Click **OK**.

Now when the user disconnects the session or the CP20 session is lost, the HC10 is placed into standby mode automatically.

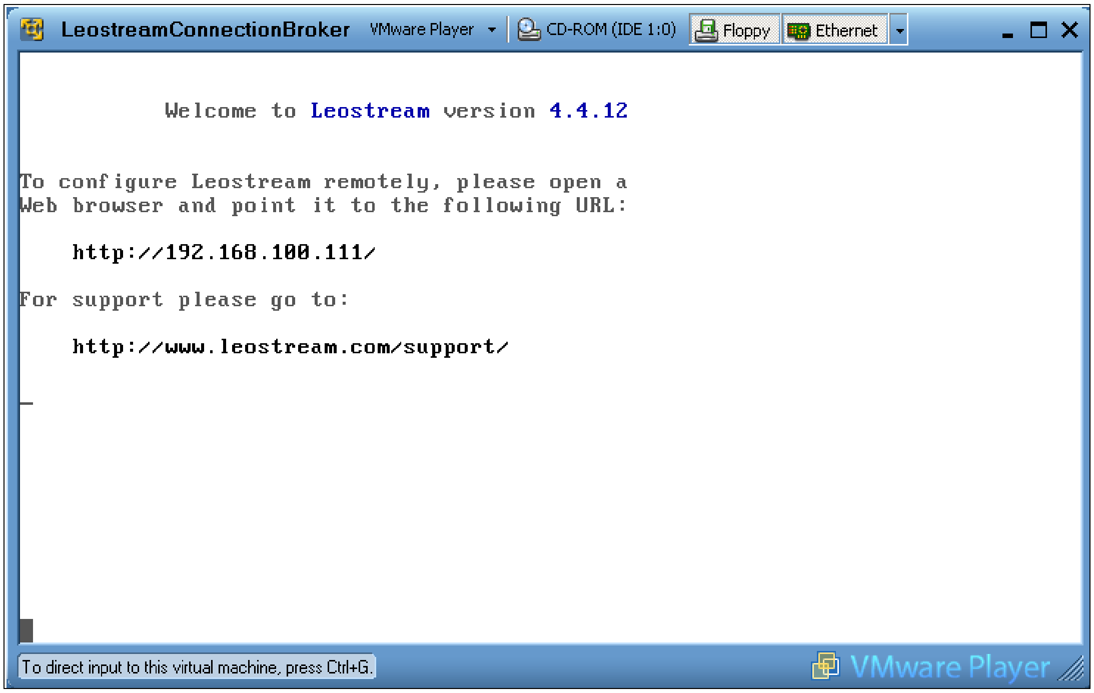
Tip: If you prefer the system to remain running when the session is disconnected, you need to change the power button setting in Figure 5-19 to **Do nothing**. Then, the HC10 remains logged in and accessible to anyone that has access to a CP20, which can be a security exposure.

We recommend that you configure the screen saver option (the Screen Saver tab in the Display applet in Control Panel) to start automatically after 5 or 10 minutes (for example), and select **On resume, password protect**.

5.2 Leostream Hosted Desktop software

As we describe in 4.9, “Leostream Hosted Desktop Connection Broker” on page 62, the Leostream Hosted Desktop software provides central management of the HC10-CP20 connections through authentication and policy management of an LDAP server such as Microsoft Active Directory. This section describes how to configure the Leostream software to provide authenticated connections of CP20s to HC10s. For instructions about how to install the Leostream software, refer to the *Leostream Hosted Client User’s Guide*. The Leostream software runs in a VMware virtual machine.

After you have the software running, you see a panel similar to Figure 5-20 that shows the IP address of the Web-based administrator interface. You use this Web interface to perform all administration functions.


LeostreamConnectionBroker
VMware Player
CD-ROM (IDE 1:0)
Floppy
Ethernet
To direct input to this virtual machine, press Ctrl+G.
VMware Player

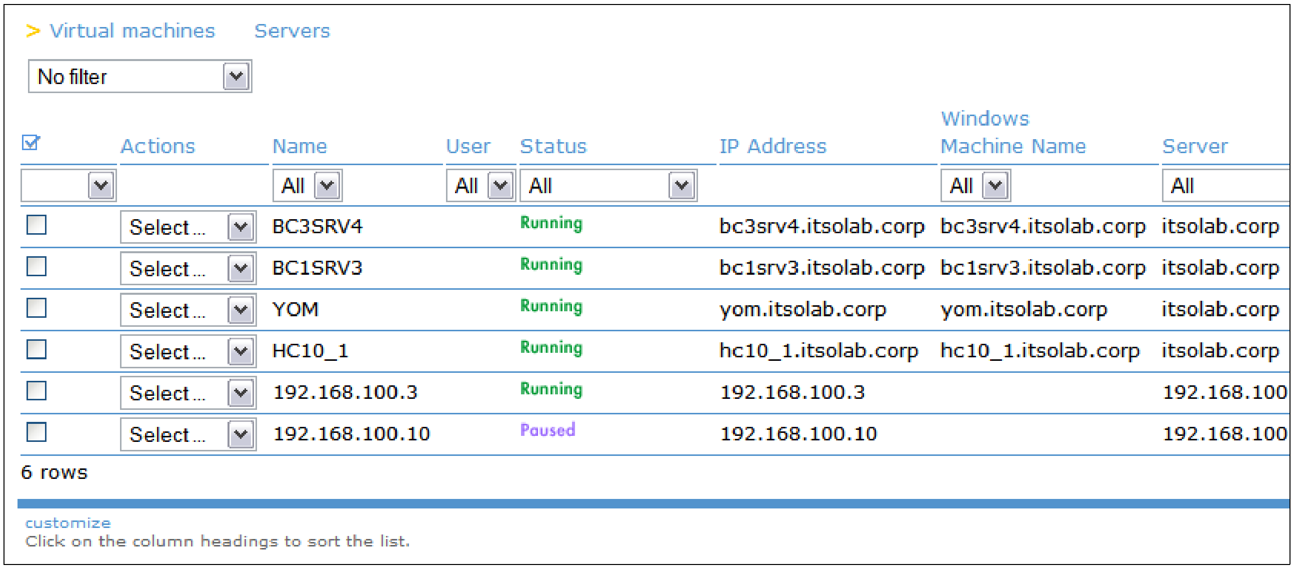
```
          Welcome to Leostream version 4.4.12


To configure Leostream remotely, please open a
Web browser and point it to the following URL:

    http://192.168.100.111/

For support please go to:

    http://www.leostream.com/support/

_
```

Figure 5-20 Obtaining the IP address of the virtual machine

To log in to the Web interface, use the following credentials:

- User name: *admin*
- Password: *leo*

You then have to enter a license key and accept the license terms. The administration interface is accessed using a Web browser and is shown in Figure 5-21.



☑	Actions	Name	User	Status	IP Address	Windows Machine Name	Server
		All	All	All		All	All
□	Select ...	BC3SRV4		Running	bc3srv4.itsolab.corp	bc3srv4.itsolab.corp	itsolab.corp
□	Select ...	BC1SRV3		Running	bc1srv3.itsolab.corp	bc1srv3.itsolab.corp	itsolab.corp
□	Select ...	YOM		Running	yom.itsolab.corp	yom.itsolab.corp	itsolab.corp
□	Select ...	HC10_1		Running	hc10_1.itsolab.corp	hc10_1.itsolab.corp	itsolab.corp
□	Select ...	192.168.100.3		Running	192.168.100.3		192.168.100
□	Select ...	192.168.100.10		Paused	192.168.100.10		192.168.100

6 rows

customize
Click on the column headings to sort the list.

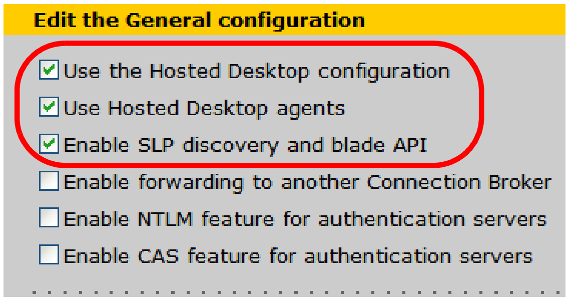
Figure 5-21 Leostream Connection Broker main panel

As shipped, the HC10s and CP20s are configured to use a connection broker with the host name *ws-broker*. Because the Leostream broker is configured this way by default, you can establish connectivity from the devices to the connection broker without any further configuration.

Leostream Hosted Desktop allows a user to connect to a HC10 in a specific group of HC10s (*pooling*) or to hard-assign a HC10. In this software, users are given specific policies. These policies contain specific tags. Each HC10 can be given be given one of these specific tags. Therefore, the tag attribute defines to which machines a user can connect.

Before setting up a connection, you must discover the devices. To do this, follow these steps:

1. Log in to the Hosted Desktop Web interface, and select **System** → **General Configuration**.
2. Select the following options (see Figure 5-22):
   - Use the Hosted Desktop configuration
   - Use Hosted Desktop agents
   - Enable SLP discovery and blade API

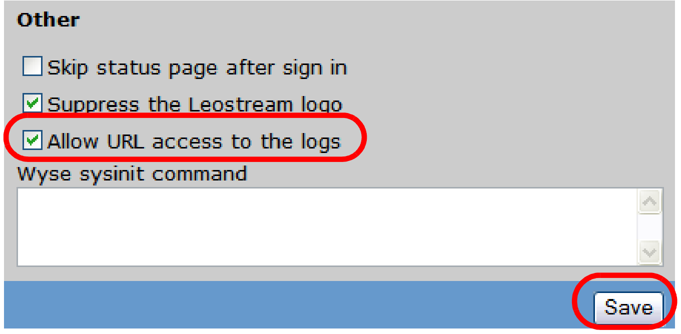


Edit the General configuration

☑ Use the Hosted Desktop configuration
☑ Use Hosted Desktop agents
☑ Enable SLP discovery and blade API
□ Enable forwarding to another Connection Broker
□ Enable NTLM feature for authentication servers
□ Enable CAS feature for authentication servers

Figure 5-22 Enabling SLP discovery and blade API

3. Scroll down to Other and select **Allow URL access to the logs**.
4. Leave all other settings as defaults and click **Save** at the bottom of the panel (see Figure 5-23).



Other

☐ Skip status page after sign in

☑ Suppress the Leostream logo

☑ Allow URL access to the logs

Wyse sysinit command

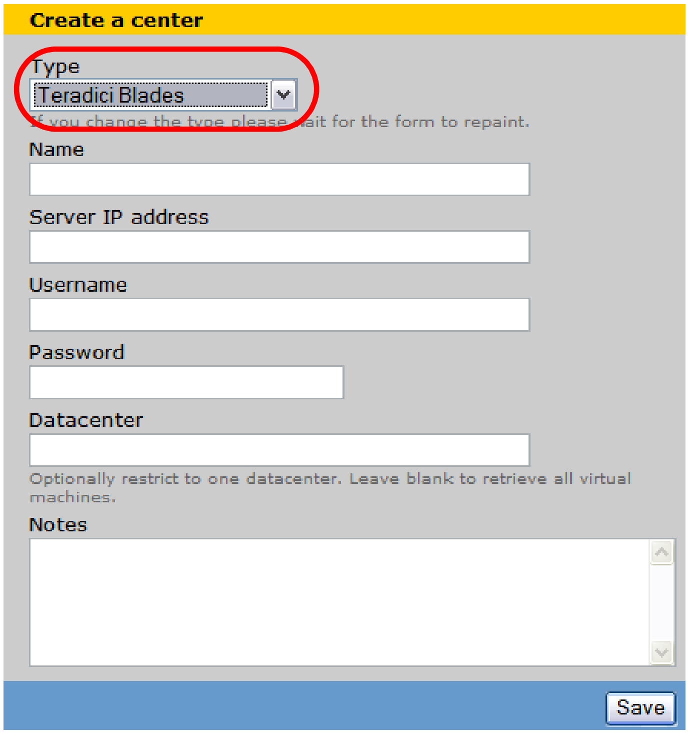
Figure 5-23 Allowing URL access to the logs

5. Reboot the Hosted Desktop software.

5.2.1 Adding a center

It is now important to add a Teradici Center by following these steps:

1. Click **Machines** → **Centers** → **Add a center**.
2. Under Type, select Teradici Blades from the drop-down list if it is not selected already (see Figure 5-24).



Create a center

Type

Teradici Blades

If you change the type please wait for the form to repaint.

Name

Server IP address

Username

Password

Datacenter

Optionally restrict to one datacenter. Leave blank to retrieve all virtual machines.

Notes

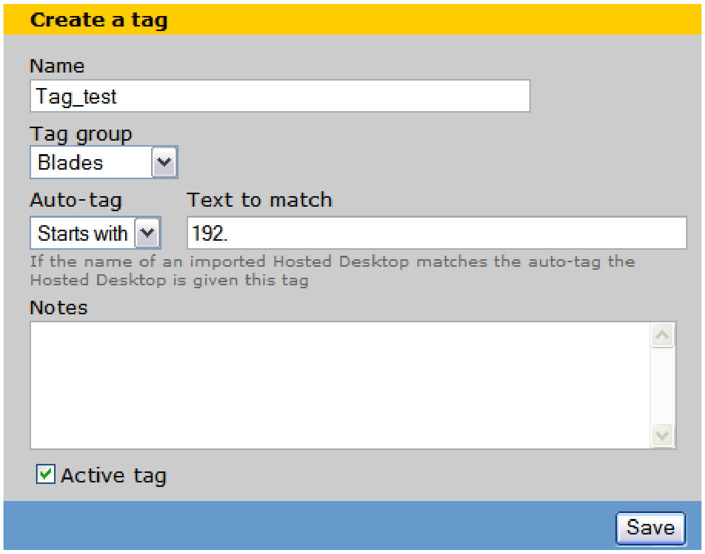
Figure 5-24 Select Teradici Blades as the type when adding a center

3. Leave the other fields blank (they are unused) and click **Save**. The HC10s on your network are now listed under **Machines** → **Hosted Desktops**.

5.2.2 Creating tags

A *tag* is used as a attribute of a machine. A machine can be given a tag and specified a specific tag group by following these steps:

1. Create tag groups by clicking **Users** → **Tags** → **Settings**.
2. Rename the tag groups to anything you desire (for example, Language, Location). These tag groups are used for organizational purposes to contain similar tags (for example, a tag for Spanish, for English, and for French would all be located in the *Language* tag group).
3. Click **Users** → **Tags** → **Create**. In the Create a tag dialog box, create a name for your tag and enter it in the Name field (Figure 5-25).
4. Choose to which tag group you want the tag to belong by selecting it from the drop-down list under Tag group.
5. You can apply this tag automatically to machines by using the Auto-tag field. First select **Starts with**, **Contains**, or **Ends with** from the drop-down list. Then, enter appropriate text in the "Text to match" field. If the name of an imported HC10 matches this auto-tag, the HC10 is given this tag. In our example, we set up an auto-tag to place the tag *Tag_test* on any HC10 with the name that starts with *192* (IP address).



Create a tag

Name: Tag_test

Tag group: Blades

Auto-tag: Starts with

Text to match: 192.

If the name of an imported Hosted Desktop matches the auto-tag the Hosted Desktop is given this tag

Notes

☑ Active tag

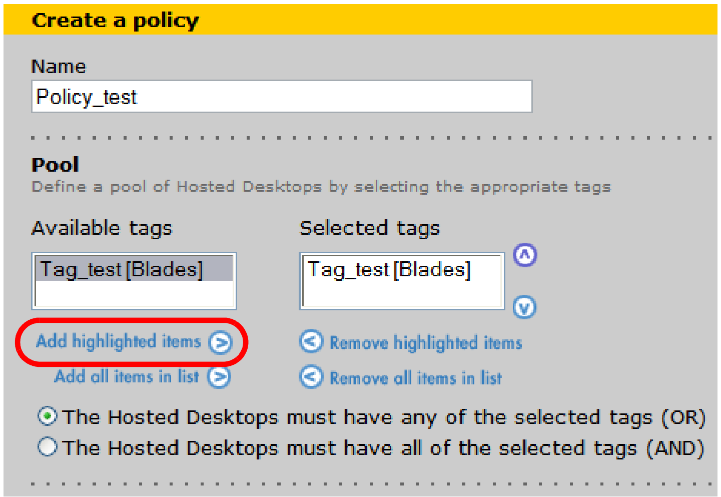
Figure 5-25 Creating a tag with the Leostream Hosted Desktop software

6. Leave the Active tab option selected and click **Save**.

5.2.3 Creating a policy

A policy is used by a user to determine to which machines a user can connect. You can define a select number of HC10s to a pool by selecting an appropriate tag in the policy. Follow these steps:

1. Click **Users** → **Policies** → **Create**. In the Create a policy dialog box, enter the name of the policy in the Name field.
2. To define a pool of HC10s, click a tag that you have created under Available tags and click **Add highlighted items** (Figure 5-26).



Create a policy

Name: Policy_test

Pool

Define a pool of Hosted Desktops by selecting the appropriate tags

Available tags: Tag_test [Blades]

Selected tags: Tag_test [Blades]

● The Hosted Desktops must have any of the selected tags (OR)

○ The Hosted Desktops must have all of the selected tags (AND)

Figure 5-26 Adding a tag to a policy in Leostream's Hosted Desktop software

3. Lead all other settings as the default and click **Save**.

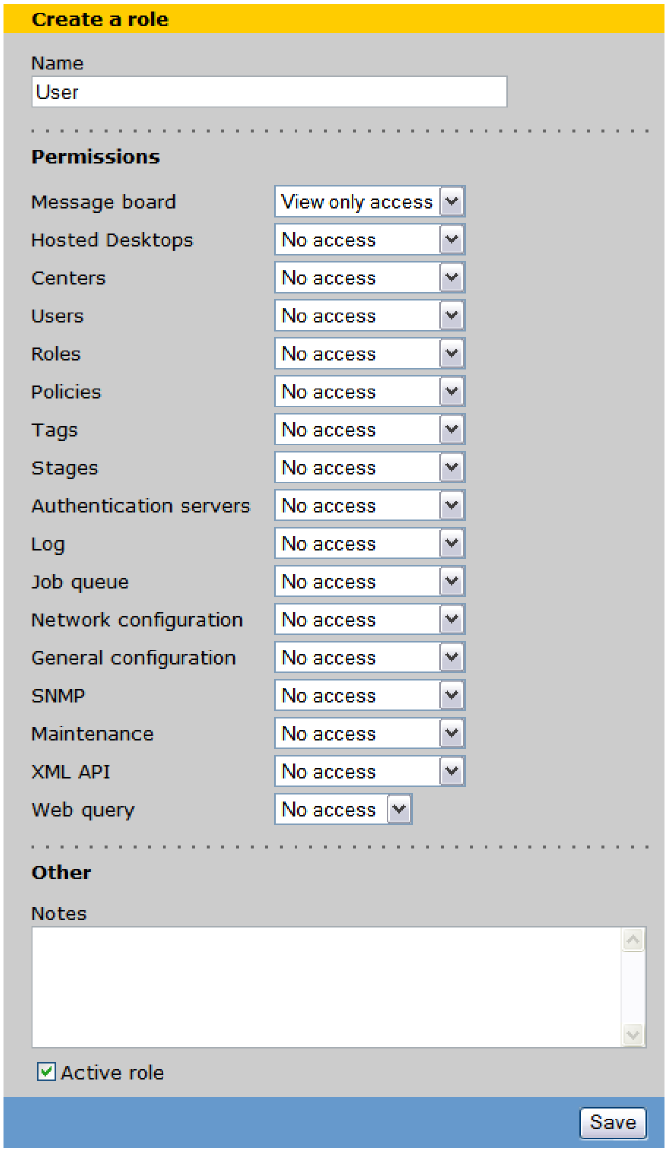
5.2.4 Creating a role

A role defines what a user is able to do. To create a new role, follow these steps:

> **Note:** It is not necessary to perform these steps because roles are created automatically.

1. Click **Users** → **Roles** → **Create**. In the Create a role dialog box, enter the name for the role in the Name field.
2. Under Permissions, select the permissions that you want to set for this role (Figure 5-27).

> **Note:** The administrator role has complete access to everything.



Create a role

Name: User

Permissions

Message board	View only access
Hosted Desktops	No access
Centers	No access
Users	No access
Roles	No access
Policies	No access
Tags	No access
Stages	No access
Authentication servers	No access
Log	No access
Job queue	No access
Network configuration	No access
General configuration	No access
SNMP	No access
Maintenance	No access
XML API	No access
Web query	No access

Other

Notes

☑ Active role

Figure 5-27 Creating a role in Leostream's Hosted Desktop software

3. Click **Save**.

5.2.5 Creating a user

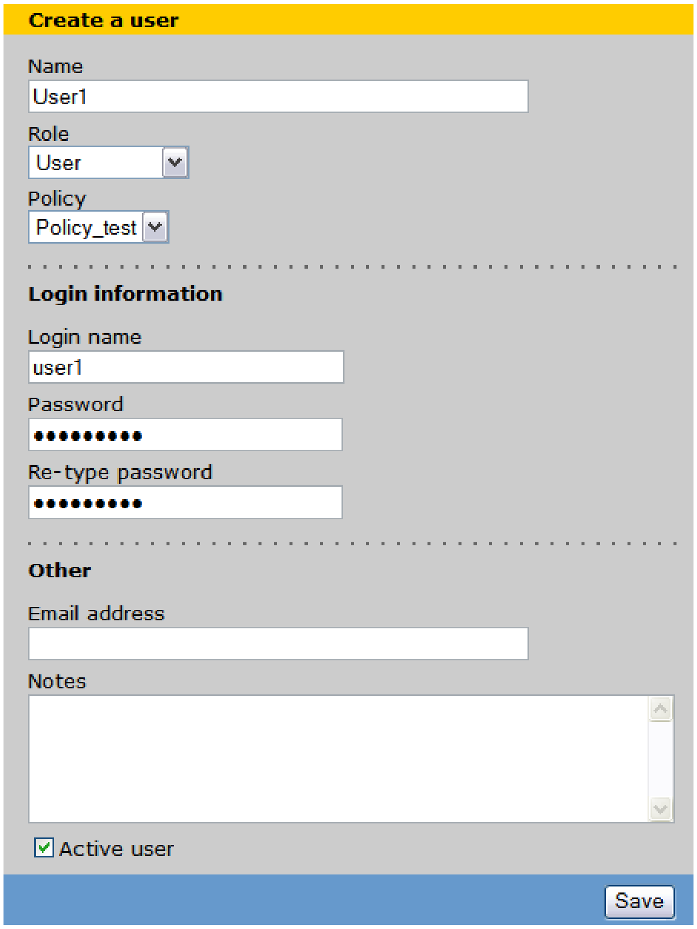
> **Note:** If you use an external authentication server for user accounts, then you do not need to create users in the connection broker. You can skip this section.

A user can be created using a specific policy and given a login name and password. Follow these steps:

1. Click **Users** → **Users** → **Create**. In the Create a user dialog box, enter a name for the user (see Figure 5-28).

   > **Note:** This name is just the name of the user. It is not the login name.

2. Select which role you want the user to have from the Role drop-down list.
3. Select a policy that you have created from the Policy drop-down list. Essentially this policy makes it so a user is assigned a policy, the policy has a tag, and this tag is used to select from machines with the same tag.
4. Enter the name and password that the user logs in with.



Create a user

Name: User1

Role: User

Policy: Policy_test

Login information

Login name: user1

Password: ●●●●●●●●●

Re-type password: ●●●●●●●●●

Other

Email address:

Notes:

☑ Active user

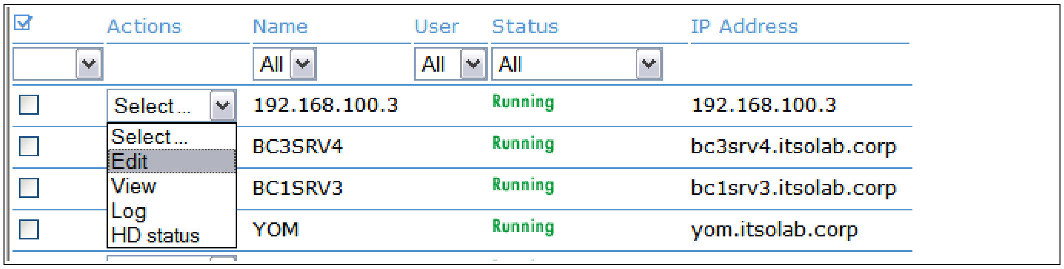
Figure 5-28 Create a user in Leostream's Hosted Desktop software

5. Click **Save**.

5.2.6 Assigning HC10s

It is now time to assign an HC10 to a user. Follow these steps:

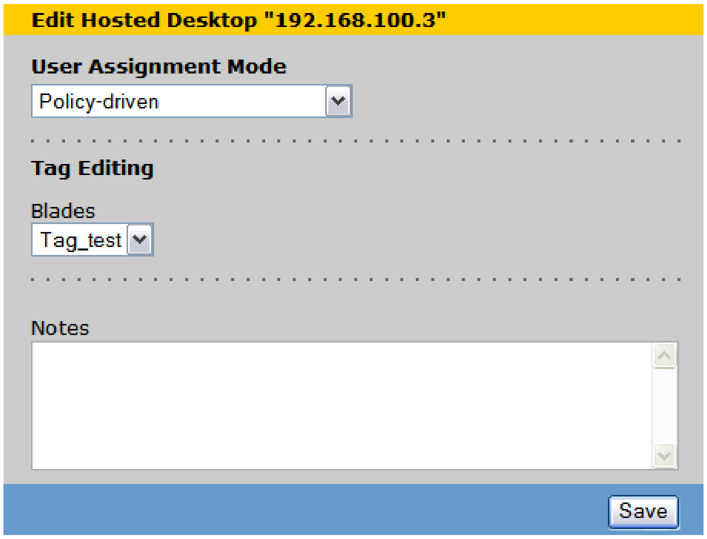
1. Click **Machines** → **Hosted Desktops**.
2. Under the Actions column, select **Edit** from the drop-down list of the HC10 that you want to configure (see Figure 5-29).



☑	Actions	Name	User	Status	IP Address
		All	All	All	
□	Select ...	192.168.100.3		Running	192.168.100.3
□		BC3SRV4		Running	bc3srv4.itsolab.corp
□		BC1SRV3		Running	bc1srv3.itsolab.corp
□		YOM		Running	yom.itsolab.corp

Figure 5-29 Editing a HC10 from the Machines menu of the Hosted Desktop software

3. If you are planning on using a policy to determine to which HC10s a user can connect, select **Policy-driven** from the User Assignment Mode drop-down list. Then, select the policy that you are going to use from the drop-down list under Tag Editing (Figure 5-30).



Edit Hosted Desktop "192.168.100.3"

User Assignment Mode: Policy-driven

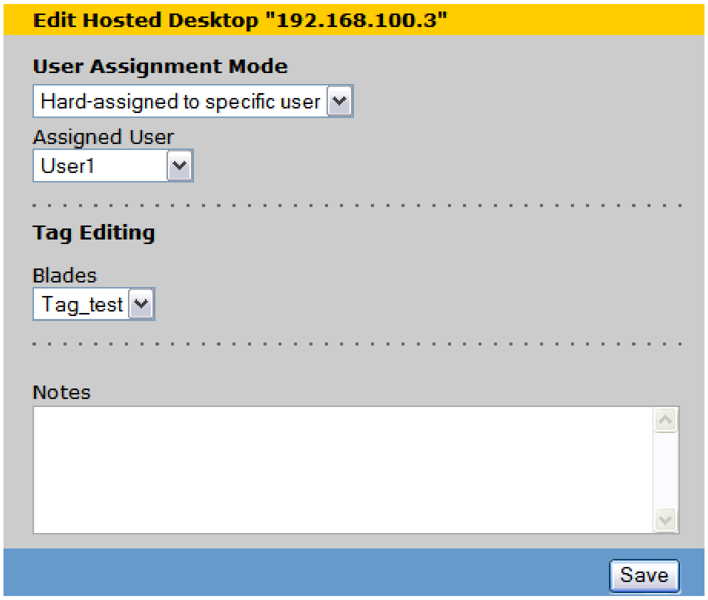
Tag Editing

Blades: Tag_test

Notes

Figure 5-30 Using a policy-driven user assignment mode to connect a user to a HC10

4. If you are planning on hard-coding a user to be able to connect to a specific HC10, select **Hard-assigned to a specific user**. From the Assigned User drop-down list, select the user that you want to be able to connect to this specific HC10 (Figure 5-31).



Edit Hosted Desktop "192.168.100.3"

User Assignment Mode: Hard-assigned to specific user

Assigned User: User1

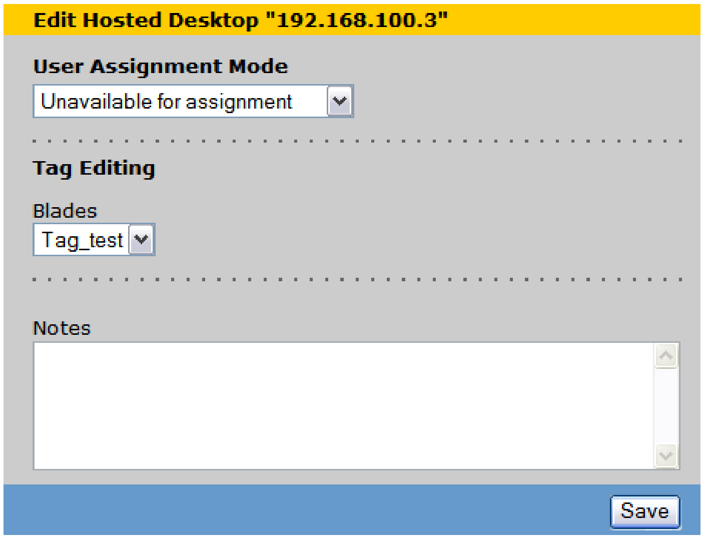
Tag Editing

Blades: Tag_test

Notes

Figure 5-31 Hard-assign a user to a HC10 in the Hosted Desktop software

5. You can also chose to have the HC10 unavailable for assignment by selecting **Unavailable for assignment** from the User Assignment Mode drop-down list (Figure 5-32).



Edit Hosted Desktop "192.168.100.3"

User Assignment Mode: Unavailable for assignment

Tag Editing

Blades: Tag_test

Notes

Figure 5-32 Make the HC10 unavailable for assignment in the Hosted Desktop software

6. Click **Save**.

5.2.7 Connect to the HC10 from the CP20

After following the previous steps, you are now ready to connect to a HC10 with a CP20 using Leostream's Hosted Desktop software. Follow these steps to connect:

1. At the CP20, click **Connect**. You are prompted for a user name and password. Enter the user login information that you created on the Hosted Desktop software earlier (see Figure 5-33). Click **OK**.

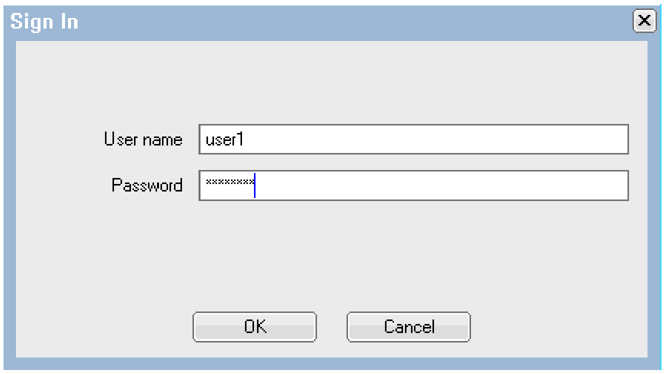


Figure 5-33 Login dialog box on the CP20's local interface when using the Hosted Desktop software

2. A list of available HC10s to which you can connect displays (unless there is only one, in which case it connects automatically). Click the HC10 to which you want to connect and click **OK**. See Figure 5-34.

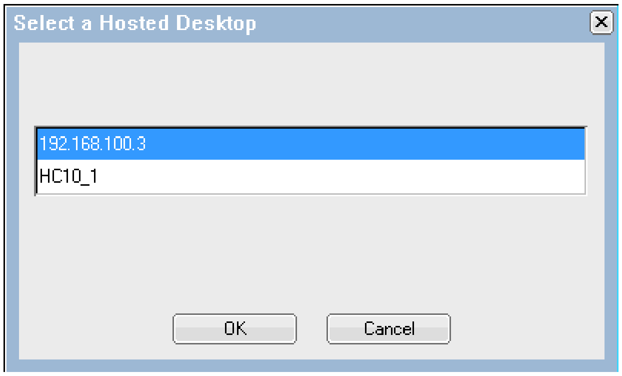
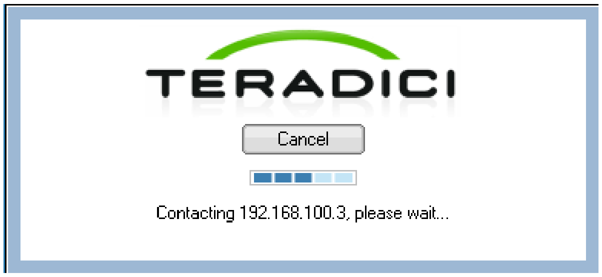


Figure 5-34 Selecting an available HC10 from a list

3. You have now successfully connected to an HC10 (see Figure 5-35).



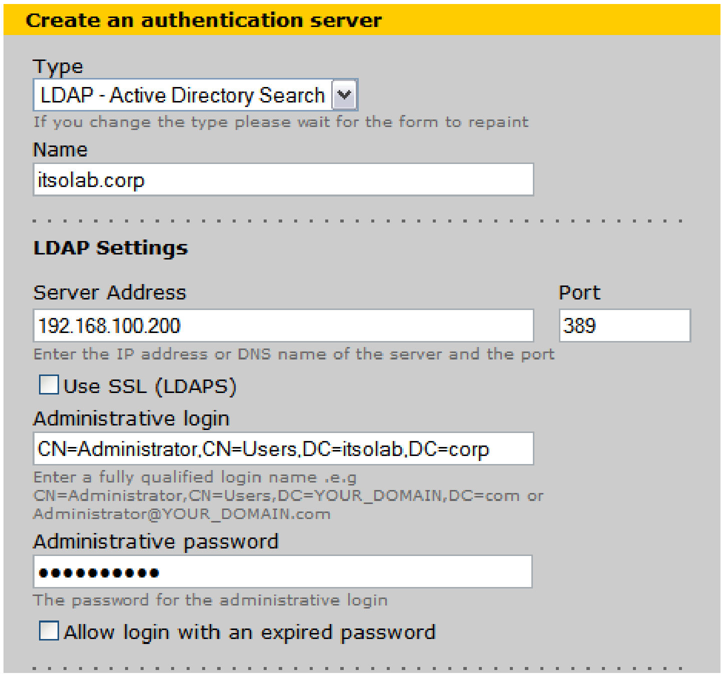
Contacting 192.168.100.3, please wait...

Figure 5-35 The message indicating that the CP20 is connecting to a HC10

5.2.8 Creating an authentication server

Active Directory can be used in conjunction with Leostream Hosted Desktop, which can be useful to load users into the connection broker software. To add an authentication server such as Active Directory, follow these steps:

1. Click **Users** → **Authentication Servers** → **Create**.
2. Complete the form, specifically the Type, Name, and LDAP Settings of your Active Directory, as shown in Figure 5-36.



Create an authentication server

Type
LDAP - Active Directory Search
If you change the type please wait for the form to repaint

Name
itsolab.corp

LDAP Settings

Server Address
192.168.100.200

Port
389

Enter the IP address or DNS name of the server and the port

□ Use SSL (LDAPS)

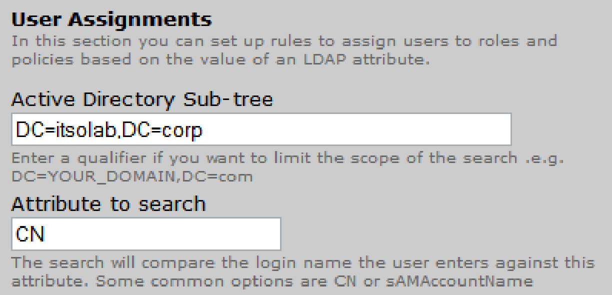
Administrative login
CN=Administrator,CN=Users,DC=itsolab,DC=corp
Enter a fully qualified login name .e.g CN=Administrator,CN=Users,DC=YOUR_DOMAIN,DC=com or Administrator@YOUR_DOMAIN.com

Administrative password
●●●●●●●●●●
The password for the administrative login

□ Allow login with an expired password

Figure 5-36 Initial settings for adding an authentication server

3. Under User Assignments, specify rules that assign policies to users automatically as they are loaded. Complete the Active Directory Sub-tree and Attribute to search, as shown in Figure 5-37.



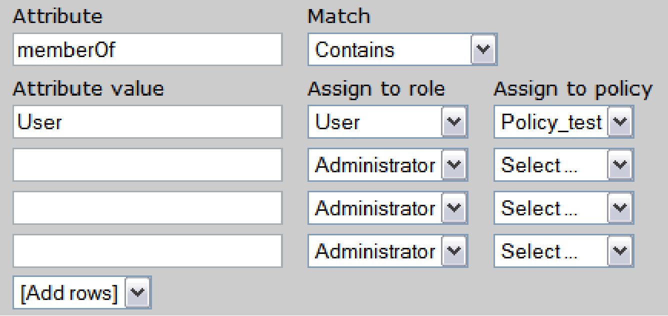
User Assignments
In this section you can set up rules to assign users to roles and policies based on the value of an LDAP attribute.

Active Directory Sub-tree
DC=itsolab,DC=corp
Enter a qualifier if you want to limit the scope of the search .e.g. DC=YOUR_DOMAIN,DC=com

Attribute to search
CN
The search will compare the login name the user enters against this attribute. Some common options are CN or sAMAccountName

Figure 5-37 User Assignments settings when adding an authentication server

4. Determine the Attribute and Attribute value that you want to assign to a specific policy. When that is complete, use the drop-down list to select a policy that you have created (see Figure 5-38). You can do this for many attribute values at the same time.



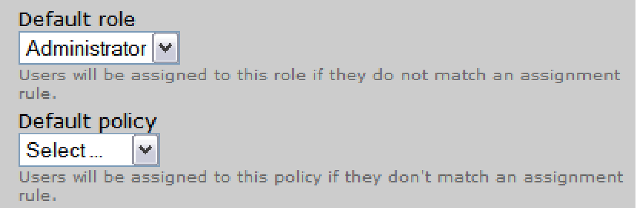
Attribute: memberOf
Match: Contains

Attribute value	Assign to role	Assign to policy
User	User	Policy_test
	Administrator	Select ...
	Administrator	Select ...
	Administrator	Select ...

[Add rows]

Figure 5-38 Automatically assign policies to users

5. It is also possible to set up default roles and default policies in the case that a user does not match any of the prior settings. You can also have all users set to a default role and policy (see Figure 5-39).



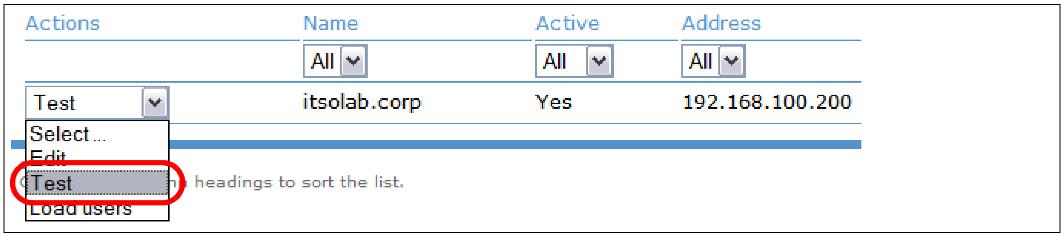
Default role
Administrator
Users will be assigned to this role if they do not match an assignment rule.
Default policy
Select ...
Users will be assigned to this policy if they don't match an assignment rule.

Figure 5-39 Setting default roles and default policies

6. Click **Save**. You have added an authentication server successfully.

You can also test the authentication of users from the authentication server. Follow these steps:

1. Click **Users** → **Authentication Servers.**
2. From the Actions column, select **Test** from the drop-down list (see Figure 5-40).



Actions	Name	Active	Address
	All	All	All
Test	itsolab.corp	Yes	192.168.100.200

Figure 5-40 Testing a user from the authentication server

3. At the resulting menu enter the user name and password and click **Authenticate**.

5.3 Security

An important feature of the HC10 and CP20 devices is the ability to secure important data. Each HC10 and CP20 is password protected on both Web interfaces, as well as on the CP20's local interface. The default password is set as PASSW0RD (with a zero not the letter *O*), and we highly suggest that you change the default password to a unique password. For more information about how to change a password, see 6.3.1, "Changing a password" on page 101. This added protection disables users from being able to change configuration options.

You can also configure which USB devices are allowed for use with the CP20 and HC10. For example, you might want to disable the use of USB thumb drives. There is always the threat that someone can insert a thumb drive into a machine and take extremely sensitive data within minutes. However, with the ability to disallow the use of thumb drives, this security threat is no longer an issue. There are many other options too, depending on your requirements. An administrator can have the environment set up so that only a keyboard and mouse (Human Interface Devices) work. You can also allow printers, imaging, and so forth. For more information about configuring access to USB devices, see "USB" on page 130.

6

Configuration options

Most customers will use a connection broker to manage the connections between CP20s and HC10s. In fact, the HC10 solution is preconfigured to work this way:

- DHCP-assigned IP addresses
- Connection management enabled in both the HC10s and CP20s
- Both device types are configured to connect to a broker with a host name of *ws-broker*

If you do not want to use a connection broker, you can use a peer-to-peer connection. In this chapter, we describe how to use a peer-to-peer connection.

You might also have a need to perform additional configuration steps. This chapter describes the available interfaces that the HC10 and CP20 provide, including:

- CP20 local firmware-based interface
- CP20 Web browser interface
- HC10 Web browser interface

We describe each of the configuration options and also address firmware updates using these interfaces (as opposed to using the Devon IT Connection Broker as described in 5.1.3, “Updating firmware” on page 74).

Topics that we cover in this chapter include:

- 6.1, “Configuring static IP addresses” on page 96
- 6.2, “Specifying how the Ethernet switch modules are used” on page 100
- 6.3, “CP20 local interface” on page 100
- 6.4, “HC10 and CP20 Web interfaces” on page 118
- 6.5, “Setting up a peer-to-peer connection” on page 139
- 6.6, “Firmware updates” on page 145

Note: The figures and text in this chapter are based on Version 17 of the CP20 and HC10 compression card firmware.

6.1 Configuring static IP addresses

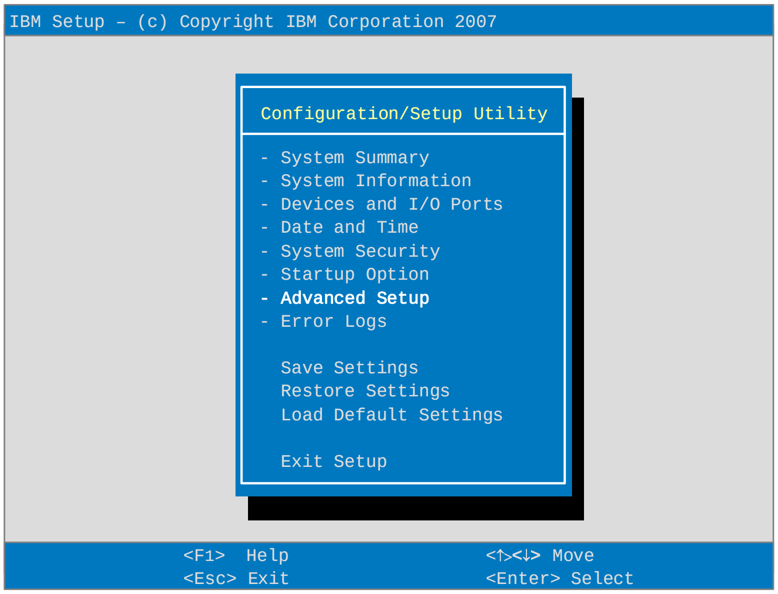
The default configuration of the HC10 and CP20 is to use DHCP. However, if you cannot use DHCP or want to use static addresses, it is important to configure the IP address of the blade workstation compression card and the workstation connection device so that they can communicate with each other.

To access the Web interfaces of these devices, the IP address of the compression cards must be determined. For the HC10, the IP address of the compression card is found in the BIOS. The IP address of the CP20 is found using the CP20's local interface. After these addresses are found, you can access and change them from the Web interface.

6.1.1 IP configuration in the HC10 BIOS

The configurations of the compression card on the HC10 are viewed and set through the BIOS or the HC10's Web interface. To determine and set the IP configurations through the BIOS, follow these steps:

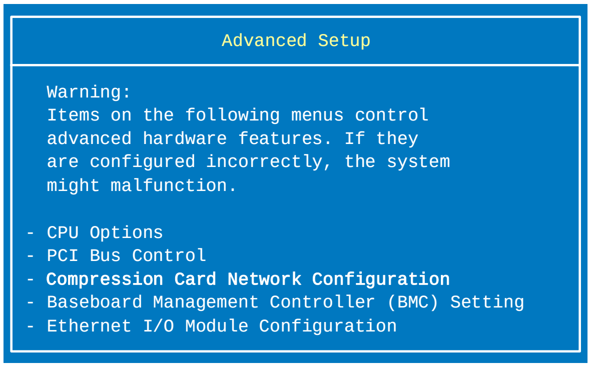
1. When the HC10 is booting, press F1 to enter the Configuration/Setup Utility. Select **Advanced Setup** and press Enter (Figure 6-1).



```
IBM Setup – (c) Copyright IBM Corporation 2007

Configuration/Setup Utility

- System Summary
- System Information
- Devices and I/O Ports
- Date and Time
- System Security
- Startup Option
- Advanced Setup
- Error Logs

  Save Settings
  Restore Settings
  Load Default Settings

  Exit Setup

<F1>  Help                    <↑><↓> Move
<Esc> Exit                    <Enter> Select
```

Figure 6-1 Main menu of the Configuration/Setup utility

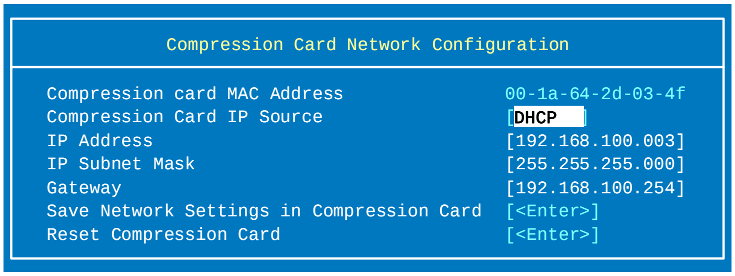
2. Select **Compression Card Network Configuration** and press Enter (Figure 6-2).



```
                    Advanced Setup

   Warning:
   Items on the following menus control
   advanced hardware features. If they
   are configured incorrectly, the system
   might malfunction.

 - CPU Options
 - PCI Bus Control
 - Compression Card Network Configuration
 - Baseboard Management Controller (BMC) Setting
 - Ethernet I/O Module Configuration
```

Figure 6-2 Advanced setup menu in the HC10s BIOS

3. The menu shows that the device is using DHCP and gives you the IP address (Figure 6-3). This IP address is the IP address of the HC10's compression card and can be used to access the Web interface.



```
                 Compression Card Network Configuration

   Compression card MAC Address                 00-1a-64-2d-03-4f
   Compression Card IP Source                   [DHCP   ]
   IP Address                                   [192.168.100.003]
   IP Subnet Mask                               [255.255.255.000]
   Gateway                                      [192.168.100.254]
   Save Network Settings in Compression Card    [<Enter>]
   Reset Compression Card                       [<Enter>]
```

Figure 6-3 IP address of the HC10's compression card

4. If you are planning on using static IP addresses, highlight `DHCP` and press the right arrow key. It now shows `Static` and allows you to change the address fields. Enter the IP address that you want to use. Make sure the address is unique to avoid any network conflicts.
5. Enter the subnet mask and gateway of your network.
6. Move down to `Save Network Settings in Compression Card` and press Enter.
7. Press Enter again to confirm that the settings have been saved.
8. Press Esc until you return to the main Configuration/Setup Utility menu.
9. Exit the Setup panels.

The IP settings have been configured on the HC10.

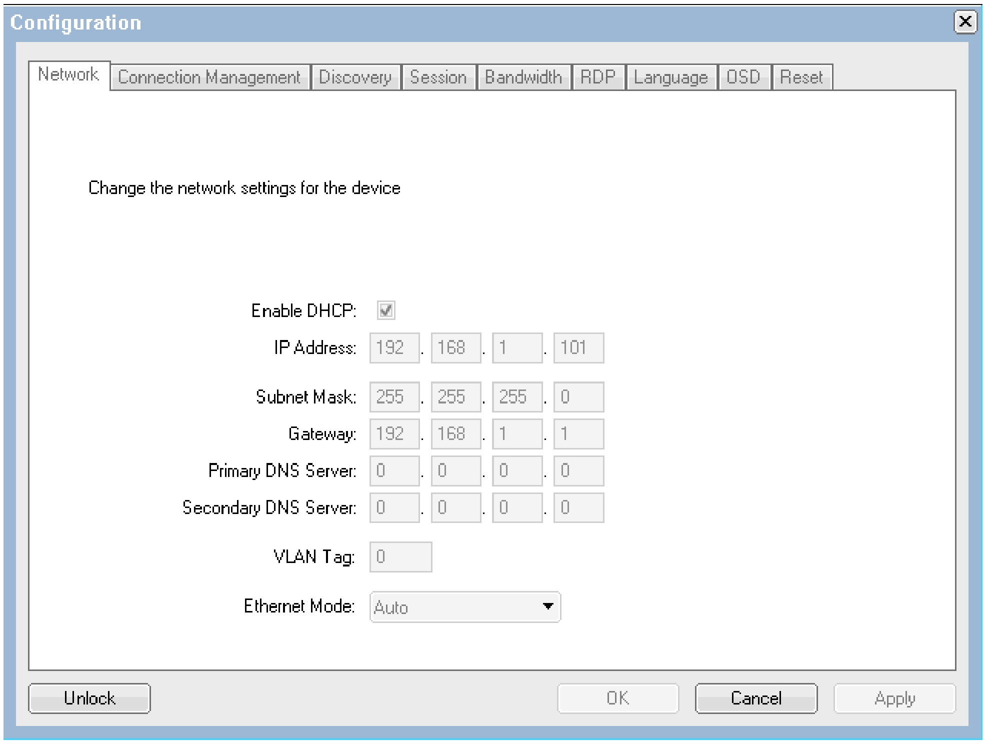
6.1.2 IP configuration of the CP20 using the local interface

The IP configuration of the CP20 are viewed and set through the CP20's local interface or the CP20's Web interface. To determine and set the IP configuration through the local interface, follow these steps:

1. Turn on the CP20 and click **Options** → **Configuration**.
2. Select **Unlock**, enter your password, and press **OK** to unlock the settings.

> **Note:** The default password is PASSW0RD (with a zero not the letter *O*). See 6.3.1, "Changing a password" on page 101 for information about how to set a password.

3. Under the Network tab, it says that DHCP is used and all of the configuration boxes are disabled. You can determine the dynamic IP address here, as shown in Figure 6-4.



Change the network settings for the device

Enable DHCP: ☑
IP Address: 192 . 168 . 1 . 101
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 1 . 1
Primary DNS Server: 0 . 0 . 0 . 0
Secondary DNS Server: 0 . 0 . 0 . 0
VLAN Tag: 0
Ethernet Mode: Auto

Figure 6-4 How to determine the dynamic address of the CP20

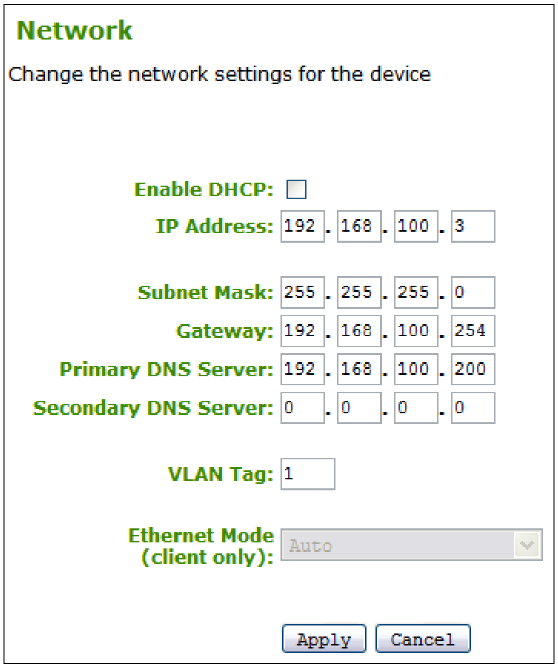
4. If you plan on using static addresses, clear the box labeled Enable DHCP, and enter the IP address that you want to assign to the CP20.
5. Enter the subnet mask and gateway of your network. This mask must be the same as the HC10 for the CP20 and HC10 to communicate (see Figure 6-10 on page 103).
6. Click **Apply** → **OK** to apply the settings.
7. The CP20 must be turned off and back on to have the settings take effect.

The IP settings have been configured on the CP20.

6.1.3 Configuring the HC10 IP address via the Web interface

If you already know the IP address of the HC10 compression card and want to change it, you can also use the Web interface to the compression card using a Web browser running on another system. Follow these steps:

1. Turn on the HC10.
2. Connect a computer to the network to which I/O module 2 is connected.
3. Open a Web browser on the computer and enter the blade workstation IP in the browser address field. Use the BIOS to determine the IP address of the HC10 (6.1.1, “IP configuration in the HC10 BIOS” on page 96) and press Enter.
4. In the browser window, click **Configuration** → **Network** from the menus. The panel shown in Figure 6-5 displays.



Network

Change the network settings for the device

Enable DHCP: □

IP Address: 192 . 168 . 100 . 3

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 100 . 254

Primary DNS Server: 192 . 168 . 100 . 200

Secondary DNS Server: 0 . 0 . 0 . 0

VLAN Tag: 1

Ethernet Mode (client only): Auto

Figure 6-5 The network configuration settings of the HC10

5. Change the IP Address, Subnet Mask, and Gateway of the HC10 to the desired configuration.
6. Click **Apply** and close the Web browser.
7. Shut down the HC10 and turn it on to allow the changes to take effect.

6.1.4 Configuring the CP20 IP address using the Web interface

You can also configure the IP settings of the CP20 with another computer that is on the same network as the blade workstation. Follow these steps:

1. Turn on the CP20.
2. Connect a computer to the network to which I/O module 2 is connected.
3. Open a Web browser on the computer and enter the CP20 IP address in the browser address field. Use the CP20’s local interface to determine the IP address of the devices

(see 6.1.2, “IP configuration of the CP20 using the local interface” on page 98) and press Enter.

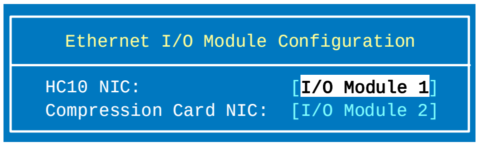
4. In the resulting dialog box, select **Configuration** → **Network**. See Figure 6-10 on page 103.
5. Change the IP Address, Subnet Mask, and Gateway of the CP20 to the desired configuration.
6. Click **Apply** and close the Web browser.
7. Shut down the CP20 and turn it on to allow the changes to take effect.

6.2 Specifying how the Ethernet switch modules are used

The HC10 workstation blades communicate through Ethernet using Ethernet switch modules (ESMs) installed in the BladeCenter chassis. By default, the HC10 requires two ESMs to be installed:

- The ESM in bay 1 of the BladeCenter chassis is used for Windows networking traffic
- The ESM in bay 2 of the chassis is used to connect the compression card in the HC10 (also known as the I/O Graphics Transmission Adapter) to the CP20

You can change these defaults in the HC10 BIOS. In the Advanced Setup panel in BIOS, select **Ethernet I/O Module Configuration**. The panel shown in Figure 6-6 displays.



```
Ethernet I/O Module Configuration

HC10 NIC:               [I/O Module 1]
Compression Card NIC:   [I/O Module 2]
```

Figure 6-6 Selecting which Ethernet switch modules are used

Here, you select which switch modules that you want to use for Windows networking (`HC10 NIC` in Figure 6-6) and the HC10-CP20 connection (`Compression Card NIC`). The choices in each case are:

- I/O Module 1
- I/O Module 2

Thus, if you prefer, you can configure both to use I/O Module 1 and install only one ESM in your BladeCenter chassis. In this configuration, the Windows traffic and the CP20 traffic are on the one production network. HC10-CP20 traffic is still secure, because it is encrypted.

6.3 CP20 local interface

The CP20 local interface allows you to:

- Configure the IP settings.
- Establish a connection with Connection Broker software.
- Connect to a HC10 by entering IP and MAC addresses of the HC10 manually or by using the discovery option.
- Set bandwidth limitations.
- Change the RDP-specific configuration.

- Choose a language.
- Set the on-screen display text.
- View an event log, session statistics, or ping an IP address.
- View the information about the CP20 and apply a password to protect the settings.

Under **Options** on the main menu of the CP20, there are five choices (see Figure 6-7).

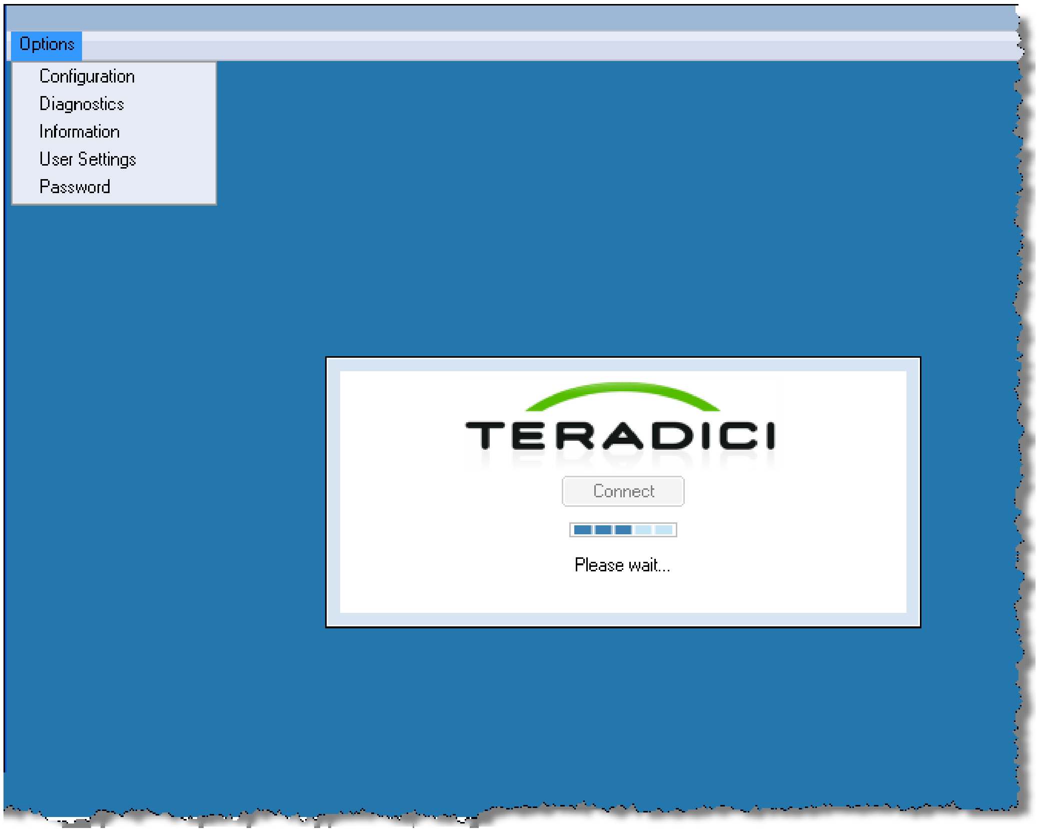


Figure 6-7 Options menu of the CP20 interface

We discuss these menu options in the following sections:

- 6.3.2, “Configuration panel” on page 102
- 6.3.3, “Diagnostics panel” on page 112
- 6.3.4, “Information panel” on page 116
- 6.3.5, “User Settings panel” on page 117
- 6.3.6, “Password panel” on page 118

6.3.1 Changing a password

To make any changes to the CP20s configuration, you must unlock the menus. To set a password and unlock the configuration settings, do the following:

1. Click **Options** → **Password**.
2. In the Change Password dialog box, enter the old password.

> **Note:** The default password is PASSW0RD (with a zero not the letter *O*).

3. Enter a new password and confirm this new password. Click **OK**. See Figure 6-8.

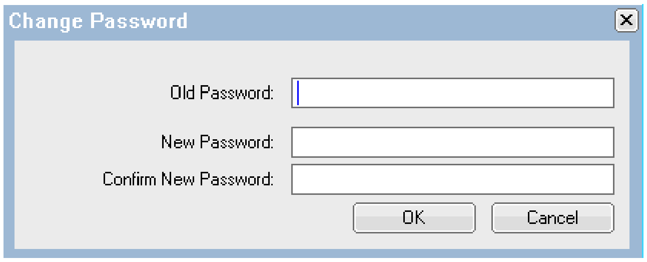
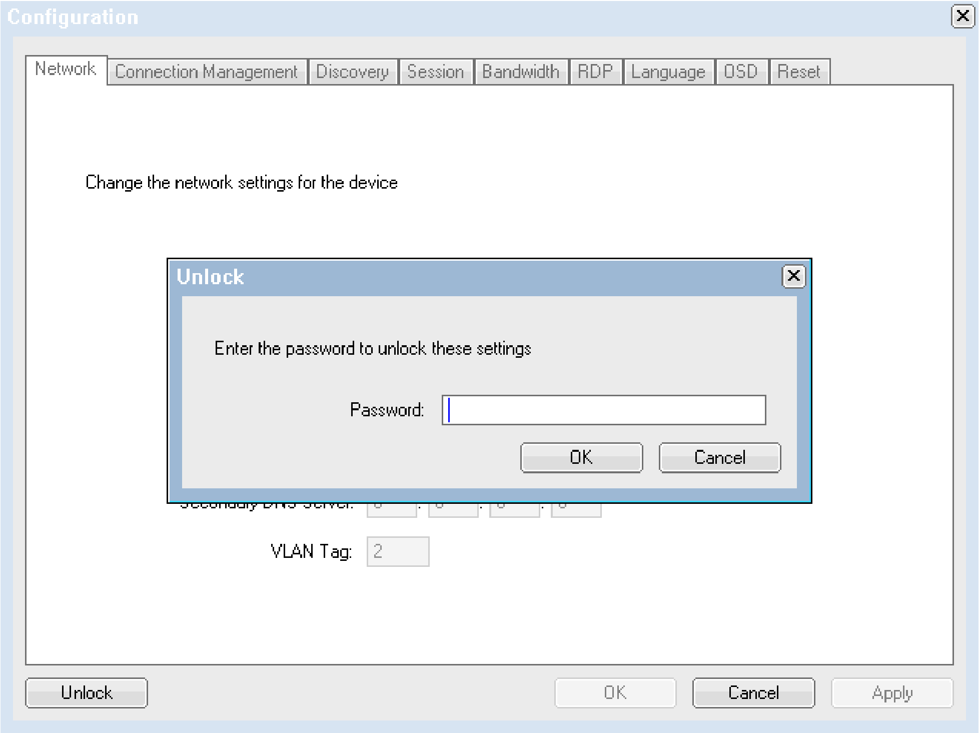


Figure 6-8 Change password menu of the CP20 interface

4. Click **Options** → **Configuration** → **Unlock**.
5. Enter the password that you just created. If you did not create a new password, enter the default: PASSW0RD (with a zero not the letter *O*). See Figure 6-9. Click **OK**.


Change the network settings for the device

Enter the password to unlock these settings

VLAN Tag: 2

Figure 6-9 Unlock the settings on the CP20 interface

6.3.2 Configuration panel

The Configuration panel shows a window with a series of tabs, which we describe in the following sections.

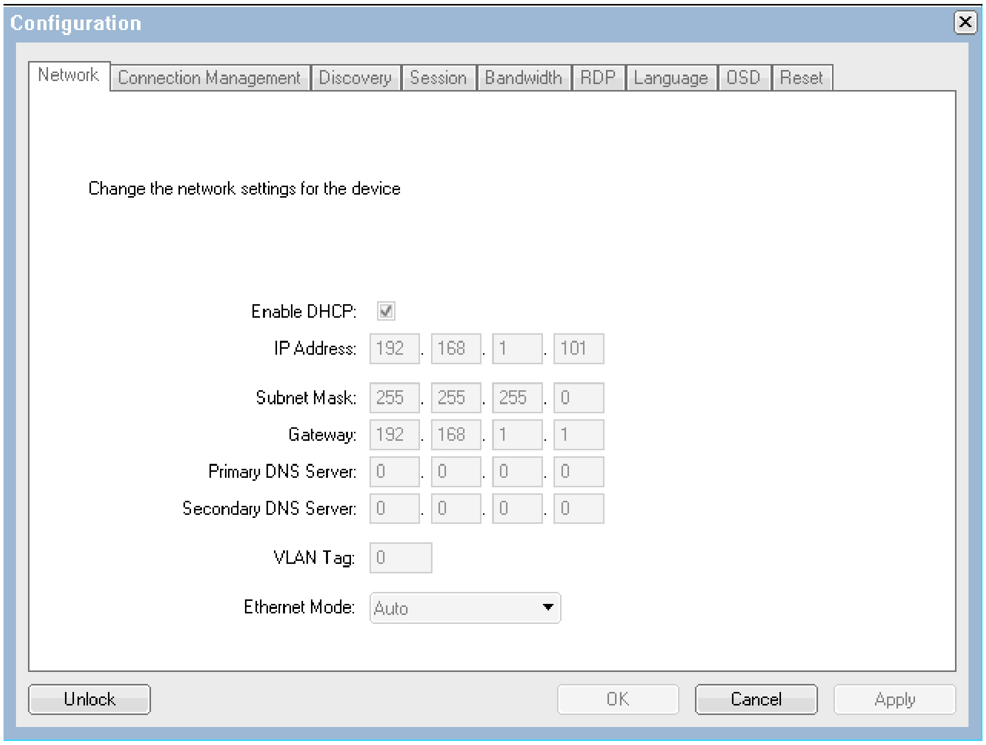
> **Note:** Before changing any parameters, you have to enter a password by clicking the **Unlock** button. The default password is PASSW0RD (with a zero not the letter *O*).

A key aspect to the settings in the Configuration panel is that some of the settings are ignored under certain circumstances, as follows:

- If you enable the use of a connection broker (that is, if you select **Enable Connection Management** in the Connection Management tab), then all fields in both the Discovery tab and Session tab are ignored.
- If you enable discovery (that is, you do not have **Enable Connection Management** selected in the Connection Management tab, but you do select **Enable Discovery** in the Discovery tab), then all fields in the Session are ignored.
- If you enable the use of a connection broker, or enable discovery, or you select **PCoIP** as the session type in the Session tab, then the contents of the RDP tab ignored.

Network tab

To establish a connection, the network settings must be configured through the Network tab as shown in Figure 6-10. See also 6.2, “Specifying how the Ethernet switch modules are used” on page 100.



Change the network settings for the device

Enable DHCP: ☑

IP Address: 192 . 168 . 1 . 101

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 1

Primary DNS Server: 0 . 0 . 0 . 0

Secondary DNS Server: 0 . 0 . 0 . 0

VLAN Tag: 0

Ethernet Mode: Auto

Figure 6-10 The network tab of the CP20 interface

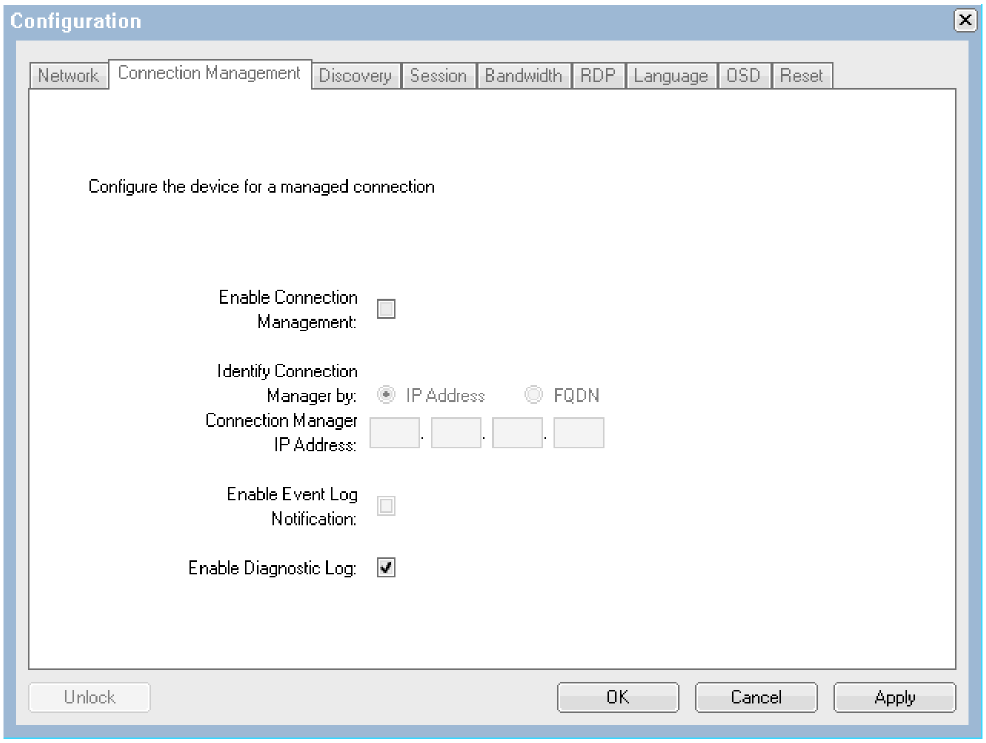
The Network tab allows you to chose between using DHCP or a static address. The default is set to DHCP, and the boxes are all disabled. The address currently assigned by DHCP is shown in the disabled fields.

You can change the IP address to static by clearing the Enable DHCP check box and entering the IP Address, Subnet Mask, Gateway, and Primary and Secondary DNS servers.

If you have configured a VLAN for your HC10 CP20 connections, enter the VLAN tag under the VLAN Tag field.

Connection Management tab

The Connection Management tab allows you to configure the CP20 for a managed connection (see Figure 6-11). This tab allows you to configure the devices to use connection broker software for a managed connection.



Configure the device for a managed connection

Enable Connection Management: □

Identify Connection Manager by: ● IP Address ○ FQDN

Connection Manager IP Address: . . .

Enable Event Log Notification: □

Enable Diagnostic Log: ☑

Figure 6-11 Connection management tab of the CP20 interface

If you select **Enable Connection Management**, the CP20 attempts to connect to the Connection Broker software to establish a connection to an HC10. If you are configuring the connection broker software manually, you must then chose whether you are going to connect through the connection broker's IP address or fully qualified domain name (FQDN).

To use IP address, select **IP Address** and enter the IP address in the appropriate field. For FQDN, select **FQDN** and enter the domain name.

There are also two options for event logs:

- You can select **Enable Event Log Notification**. When this option is selected, the device sends event log messages to the connection broker, approximately once a minute and up to 10 messages at a time until all received messages have been sent. The event log is cleared between power cycles and resets of the device.
- The use of **Enable Diagnostic Log** is used for diagnostic purposes only. This option does not send messages to the connection broker.

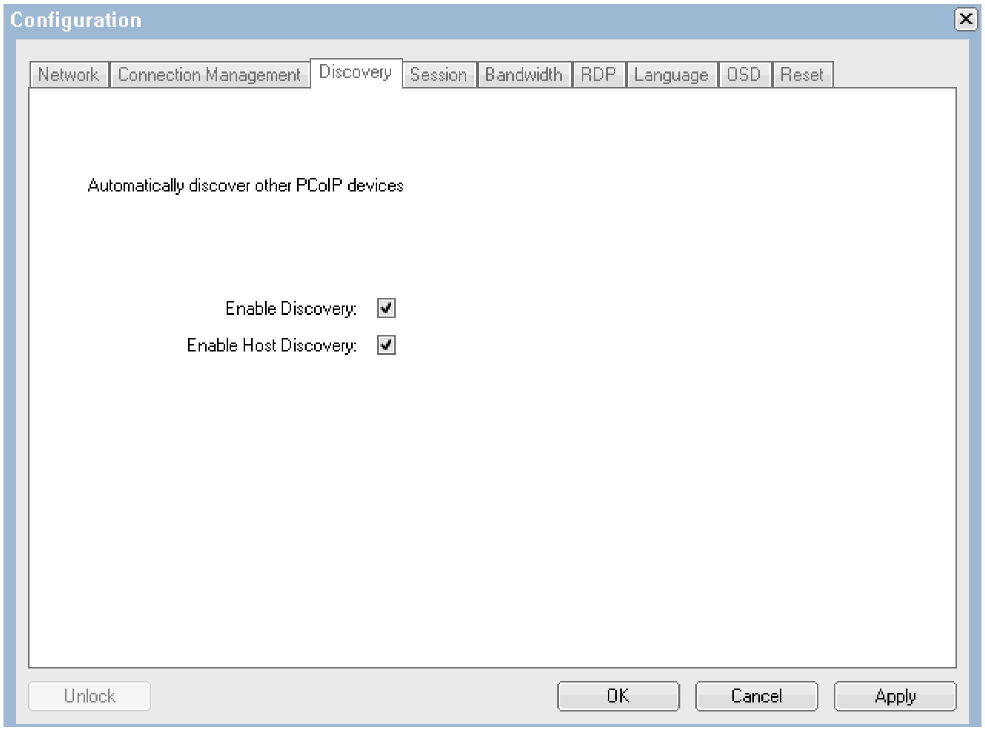
Tip: When **Enable Connection Management** is selected in the Connection tab, the contents of the Discovery tab, Session tab, and RDP tab are all *ignored*. These three tabs are for peer-to-peer configurations only. These parameters are not used because the use of a connection broker and peer-to-peer connectivity are mutually exclusive options.

Discovery tab

The Discovery tab (see Figure 6-12) enables a peer-to-peer connection and, when you connect, searches automatically for all available HC10s to which you can connect. This tab and the session tab allow you to connect directly from a CP20 to an HC10 without the use of a connection broker.

> **Tip:** Both the Discovery tab and the Session tab relate to peer-to-peer connections. The parameters in the Session tab let you specify an exact HC10 to connect to, whereas the Discovery tab lets you pick an HC10 from a list of all available HC10s (that is, HC10s that are online but not already in session). You could consider Discovery to be a rudimentary connection broker.

For more information about how to use a peer-to-peer connection, see 6.5, “Setting up a peer-to-peer connection” on page 139.



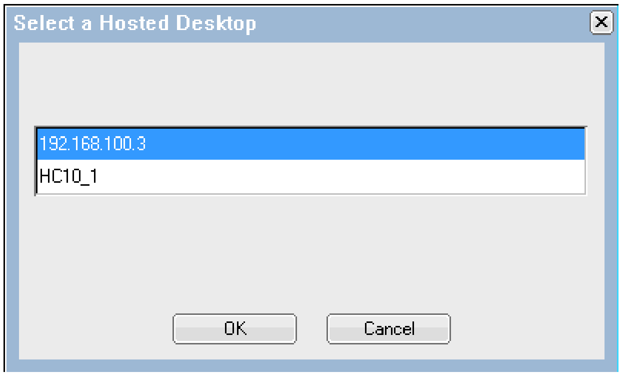
Automatically discover other PCoIP devices

Enable Discovery: ☑

Enable Host Discovery: ☑

Figure 6-12 The Discovery tab of the CP20 interface

The purpose of discovery is for the CP20 to find an available HC10 to connect to. There are two options that can be configured on this tab. To use the discovery option, you must select both **Enable Discovery** and **Enable Host Discovery**. Selecting both of these options gives you the option of which HC10 you can to connect to. With this option, the CP20 discovers available HC10s and creates a list of available HC10s, such as the one shown in Figure 6-13. You can select from the HC10 to which you want to connect from this list.



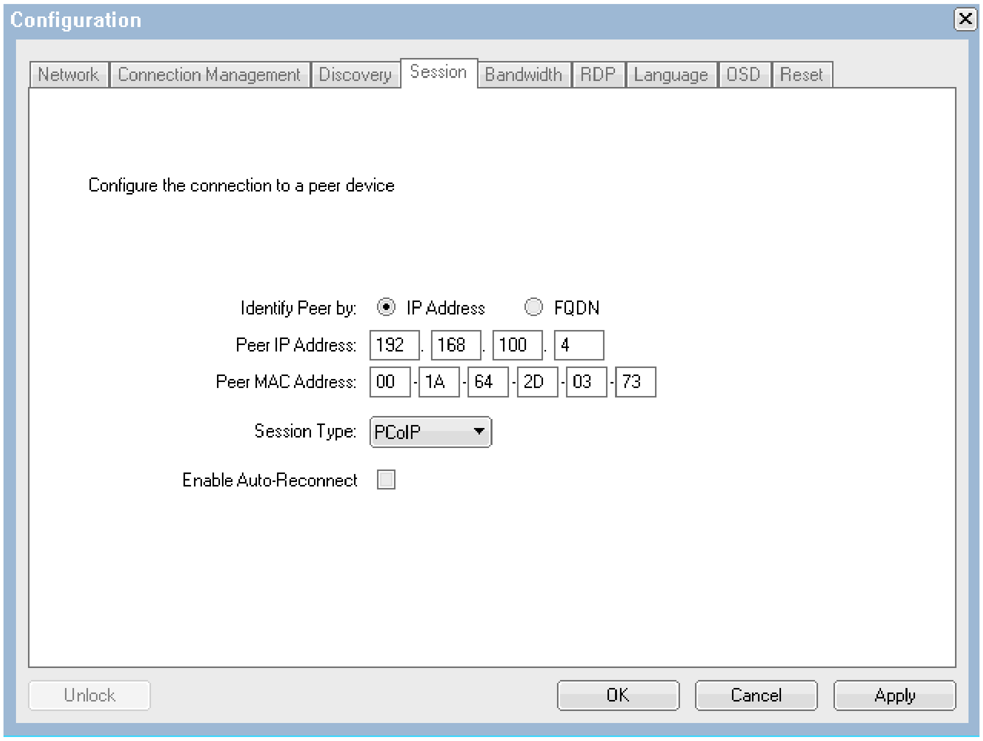
192.168.100.3
HC10_1

Figure 6-13 List of available HC10s to connect to

> **Note:** If **Enable Connection Management** is selected in the Connection tab as shown in Figure 6-11 on page 104, the Discovery feature is not used and settings on this tab are ignored.

Session tab

The Session tab, as shown in Figure 6-14, allows you to configure a peer-to-peer session by specifying the IP address and MAC address manually of the exact HC10 to which you want this CP20 to connect. For more information about how to use a peer-to-peer connection, see 6.5, “Setting up a peer-to-peer connection” on page 139.



Configure the connection to a peer device

Identify Peer by: ● IP Address ○ FQDN

Peer IP Address: 192 . 168 . 100 . 4

Peer MAC Address: 00 - 1A - 64 - 2D - 03 - 73

Session Type: PCoIP

Enable Auto-Reconnect □

Figure 6-14 The Sessions tab of the CP20 interface

Note: For the fields in the tab to be active, you must ensure that **Enable Discovery** is *not* selected in the Discovery tab and that **Enable Connection Management** is *not* select in the Connection Management tab. With either of these options selected, all fields in the Session tab are ignored.

You can establish a peer-to-peer connection by either knowing the HC10s IP address or fully qualified domain name (FQDN). To use the IP address, select **IP Address** and enter the HC10 compression card's IP address in the appropriate fields. To use FQDN, select **FQDN** and enter the domain name.

You also need to enter the MAC address of the compression card of the HC10. Two ways to determine the MAC address are:

- Boot the HC10 and press F1 to go into BIOS, then select **Advanced Settings → Compression Card Network Configuration**. The MAC address displays on the panel that displays.
- Leave an incorrect value for the MAC address as shown in Figure 6-14 on page 106 and try to connect to the HC10. The connection fails with the message "`Session Refused!`". Then, **click Options → Diagnostics**. In the Event Log, you see two entries: one that lists the incorrect MAC address and one that lists the MAC address that was expected. Simply copy that expected address into the fields as shown in Figure 6-14 on page 106. For example, if you specified a fake MAC address of all zeros (`00-00-00-00-00-00`), then the messages that you see in the event log would be similar to that shown in Example 6-1.

  Example 6-1 Error log messages showing the correct MAC address of the compression card

  ```
  Connecting with host (9.42.170.185, 00-00-00-00-00-00)
  Peer MAC mismatch: (00-1A-64-2D-02-EE, 00-00-00-00-00-00)
  ```

  The correct MAC address is this example is `00-1A-64-2D-02-EE`.

Note: Future firmware updates can remove the need to enter the MAC address.

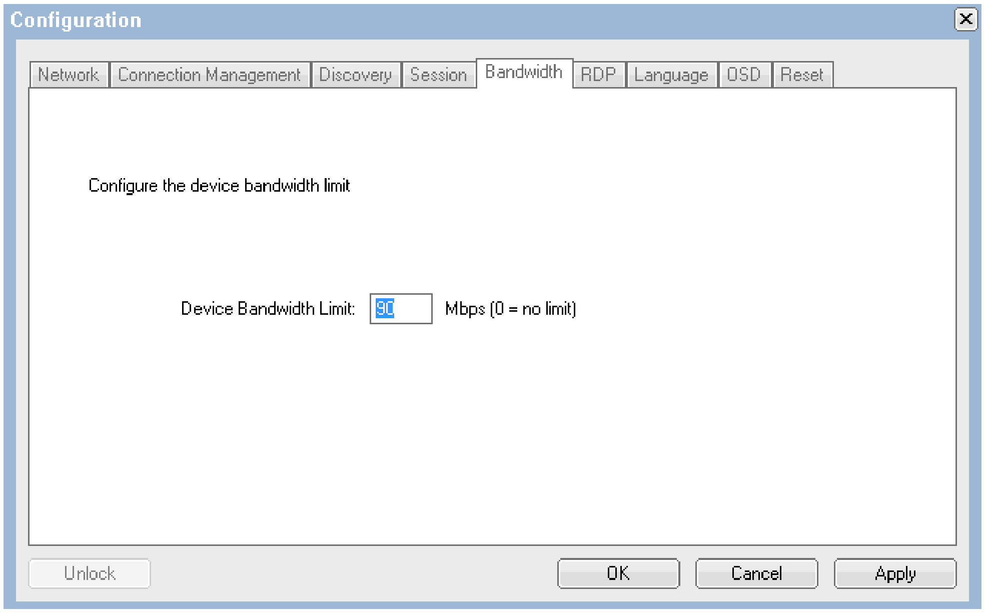
The Session Type can be either PCoIP or RDP; however, to connect to an HC10, the Session Type needs to be set to PCoIP.

The **Enable Auto-Reconnect** configures the CP20 to try to connect to the last HC10 to which it connected automatically when the CP20 is turned on. The CP20 only tries to reconnect on a boot and not after a session disconnect.

The Session tab is not considered if Connection Management or Discovery are enabled. Although you still can configure the settings, this tab is ignored if either of these options are enabled.

Bandwidth tab

The Bandwidth tab, shown in Figure 6-15, allows a user to set the device bandwidth limit in Mbps. To set this as unlimited, simply enter zero (0) or enter any maximum amount.



Configure the device bandwidth limit

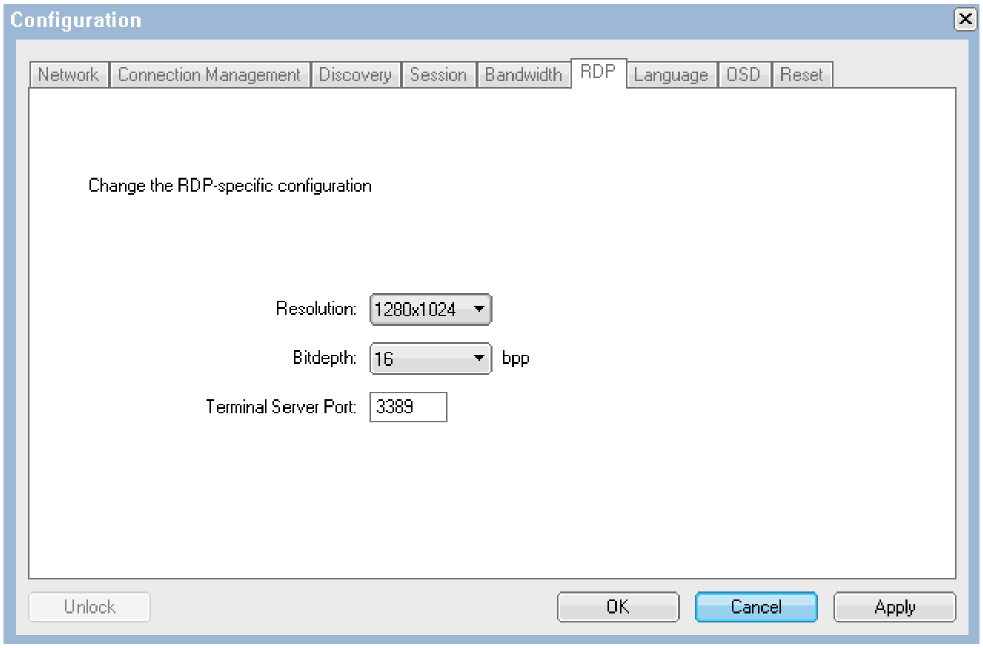
Device Bandwidth Limit: 90 Mbps (0 = no limit)

Figure 6-15 The Bandwidth tab of the CP20 interface

RDP tab

The RDP tab, shown in Figure 6-16, allows a user to configure the resolution, bit depth, and terminal server port for a RDP connection. The fields in this tab are used only if you have specified RDP as a Session Type under the Session tab. Otherwise, these fields are ignored.

For a CP20 to HC10 configuration, the RDP tab is not used, because the session type is always PCoIP.



Change the RDP-specific configuration

Resolution: 1280x1024

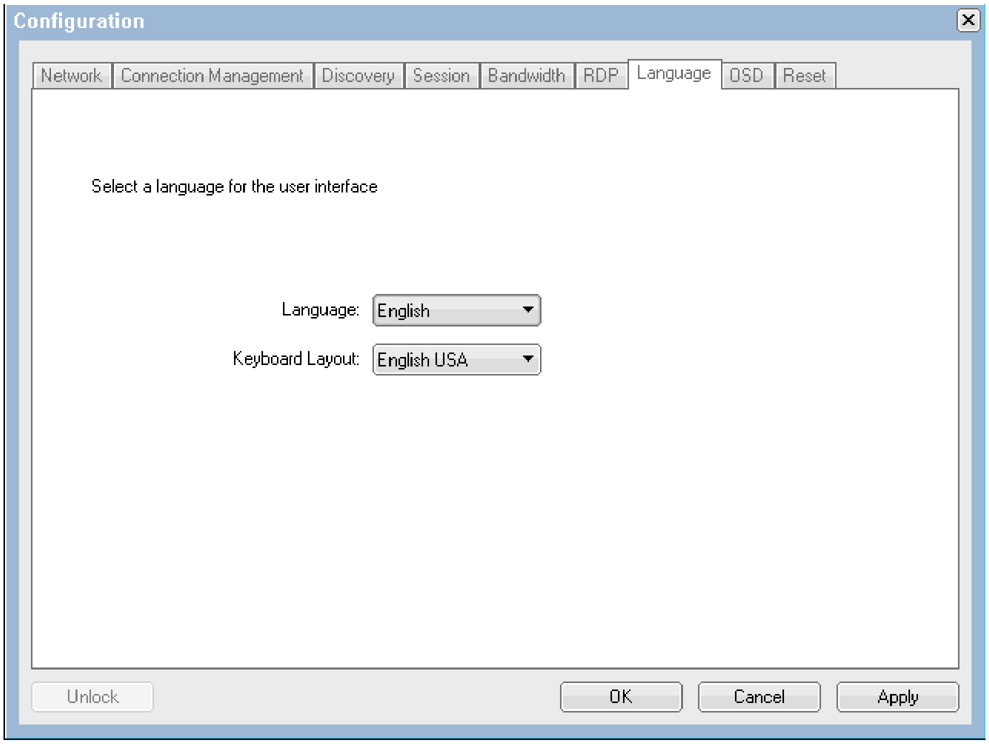
Bitdepth: 16 bpp

Terminal Server Port: 3389

Figure 6-16 The RDP tab of the CP20 interface

Language tab

The Language tab allows you to change the language settings and keyboard layout of the CP20 (see Figure 6-17).



Select a language for the user interface

Language: English

Keyboard Layout: English USA

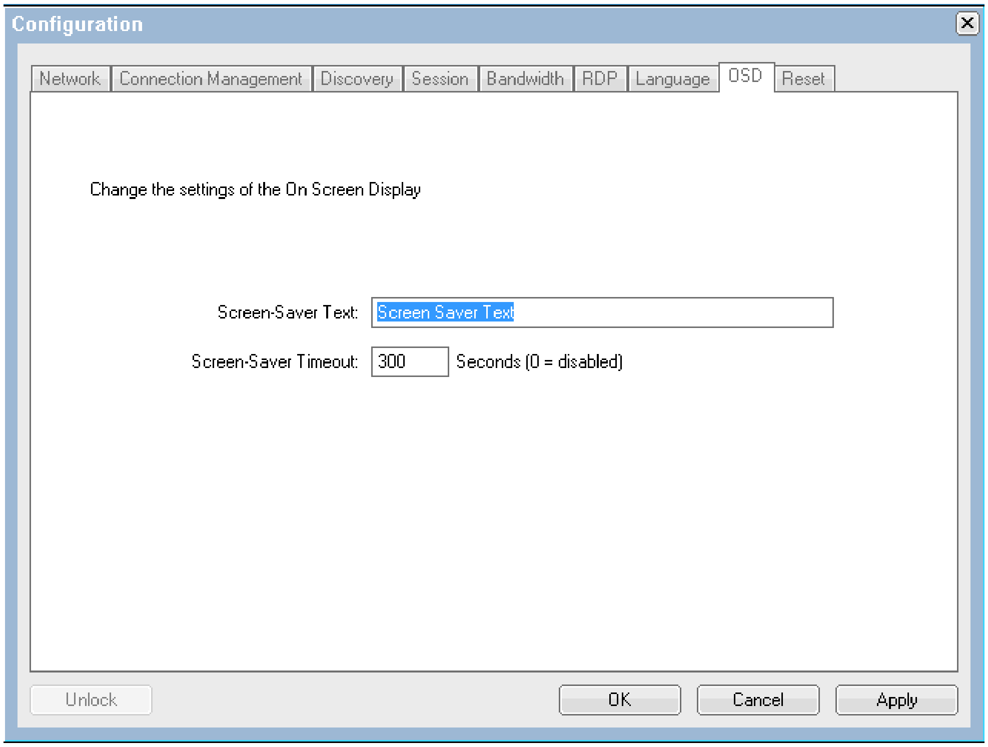
Figure 6-17 The Language tab of the CP20 interface

At the time of this writing, there is only one language option for the CP20: English. For keyboard layout, you can chose between English U. S. and French Canada.

Note: The settings on the Language tab do not affect any language settings that you have defined in Windows on the HC10. These settings are just for the local and Web interfaces of the CP20.

OSD tab

The OSD tab allows you to set screen saver text for when the CP20 is not in session (Figure 6-18). The default screen saver text is `Screen Saver Text`, and the default timeout is set to 300 seconds (5 minutes).



Change the settings of the On Screen Display

Screen-Saver Text: Screen Saver Text

Screen-Saver Timeout: 300 Seconds (0 = disabled)

Figure 6-18 The OSD tab of the CP20 interface

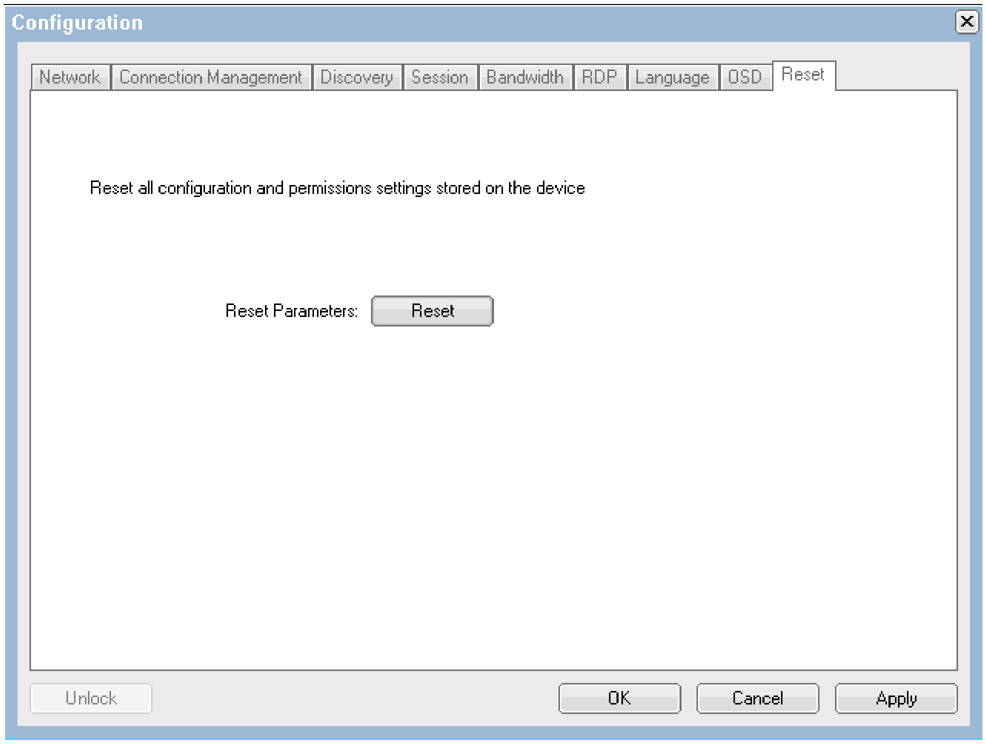
To change the text, enter new text in the Screen-Saver Text field. You can enter in excess of 200 characters, but the text does not wrap.

You can also change the amount of time that it takes before the screen saver is used by entering a new number in the Screen-Saver Timeout field. This timeout value is entered in number of seconds. Entering zero (0) disables the screen saver.

The actual screen saver is a black background with rudimentary, white text that is placed on the screen randomly. The screen saver is used only when there is no active session to an HC10.

Reset tab

The Reset tab enables you to reset the CP20 configuration back to the default settings (Figure 6-19).



Reset all configuration and permissions settings stored on the device

Reset Parameters: Reset

Figure 6-19 The Reset tab of the CP20 interface

To reset all of the configurations, click **Reset**, which changes all of the configurations to the default and makes the device use DHCP and a Connection Broker.

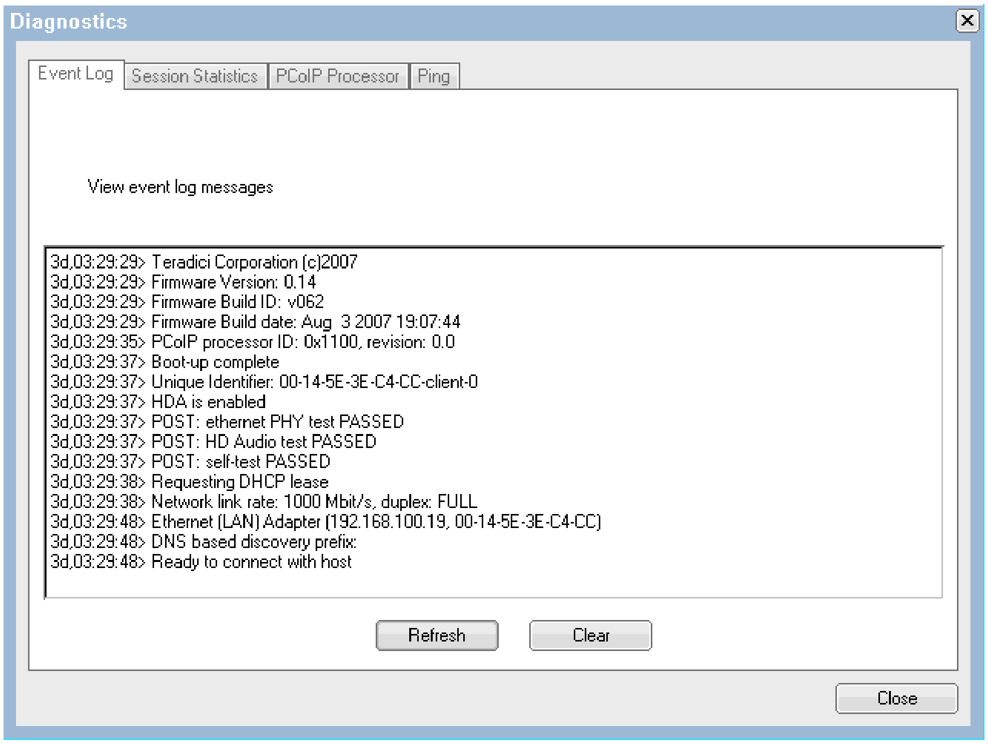
> **Note:** This reset action also resets the login password to PASSW0RD (with a zero not the letter *O*).

6.3.3 Diagnostics panel

The diagnostic panel is useful when you are having connection problems.

Event Log tab

The Event Log tab, as shown in Figure 6-20, can be helpful in troubleshooting a connection problem.



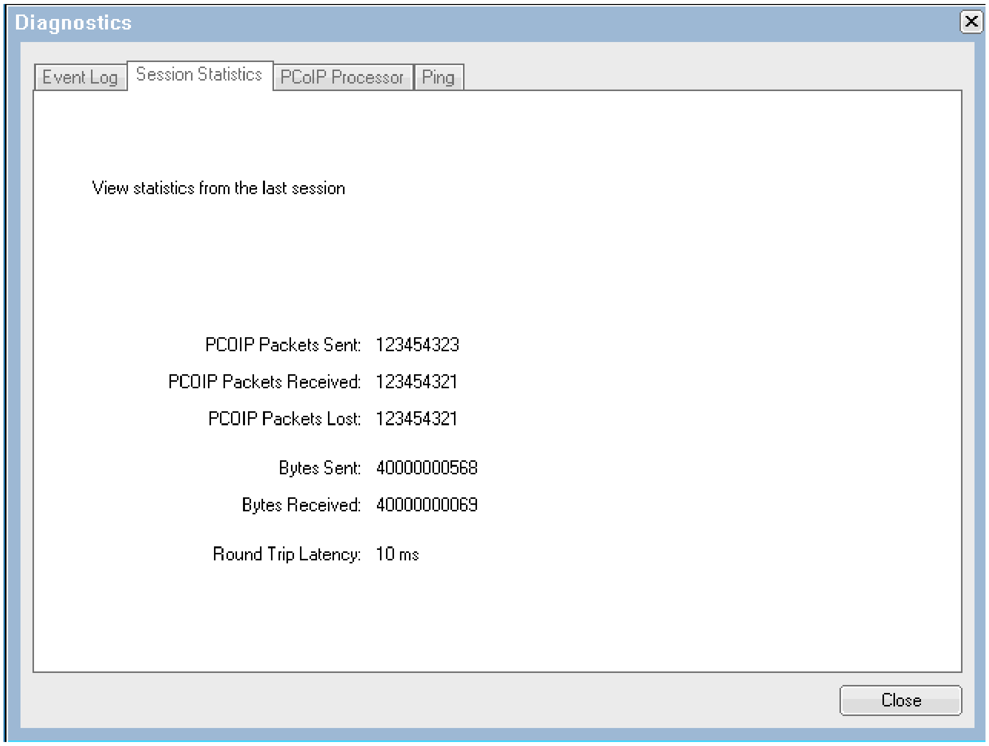
```
3d,03:29:29> Teradici Corporation (c)2007
3d,03:29:29> Firmware Version: 0.14
3d,03:29:29> Firmware Build ID: v062
3d,03:29:29> Firmware Build date: Aug  3 2007 19:07:44
3d,03:29:35> PCoIP processor ID: 0x1100, revision: 0.0
3d,03:29:37> Boot-up complete
3d,03:29:37> Unique Identifier: 00-14-5E-3E-C4-CC-client-0
3d,03:29:37> HDA is enabled
3d,03:29:37> POST: ethernet PHY test PASSED
3d,03:29:37> POST: HD Audio test PASSED
3d,03:29:37> POST: self-test PASSED
3d,03:29:38> Requesting DHCP lease
3d,03:29:38> Network link rate: 1000 Mbit/s, duplex: FULL
3d,03:29:48> Ethernet (LAN) Adapter (192.168.100.19, 00-14-5E-3E-C4-CC)
3d,03:29:48> DNS based discovery prefix:
3d,03:29:48> Ready to connect with host
```

Figure 6-20 The Diagnostics menu showing the event log

The Event Log tab shows any events that have happened along with a time stamp of when each event occurred. The Even Log tab includes a Refresh button to make sure the logs contain the most recent events and also a Clear button to remove all logs.

Session Statistics tab

The Sessions Statistics tab allows you to view information about a current session (Figure 6-21).



View statistics from the last session

PCOIP Packets Sent: 123454323
PCOIP Packets Received: 123454321
PCOIP Packets Lost: 123454321

Bytes Sent: 40000000568
Bytes Received: 40000000069

Round Trip Latency: 10 ms

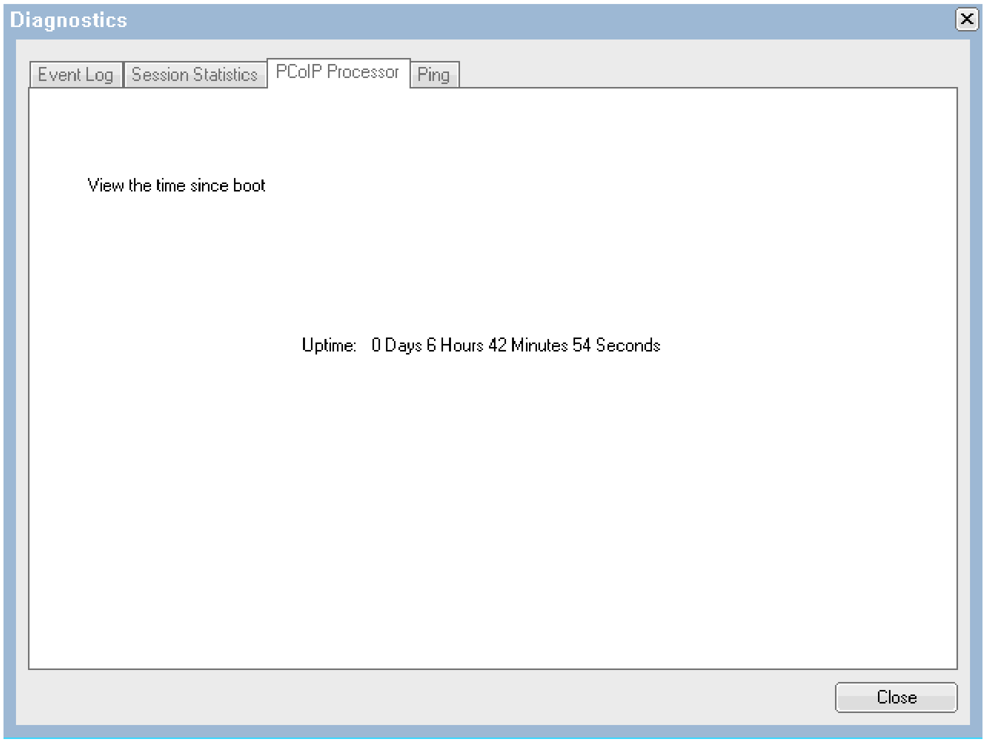
Figure 6-21 The Sessions Statistics tab of the CP20 local interface

This tab allows you to view the number of PC-over-IP packets that have been sent, received, and lost and shows the number of bytes sent and received.

It also shows a value of round trip latency in ms. This displays the round trip latency from the PC-over-IP processor in the CP20 to the PC-over-IP processor in the compression card of the HC10 and back again. The value is accurate within +/- 1 ms. This value is useful in determining whether your distance between the CP20 and HC10 and your network design is sufficient for reasonable use.

PCoIP Processor tab

The PCoIP Processor tab allows you to view the amount of time that has elapsed since the last boot (Figure 6-22).



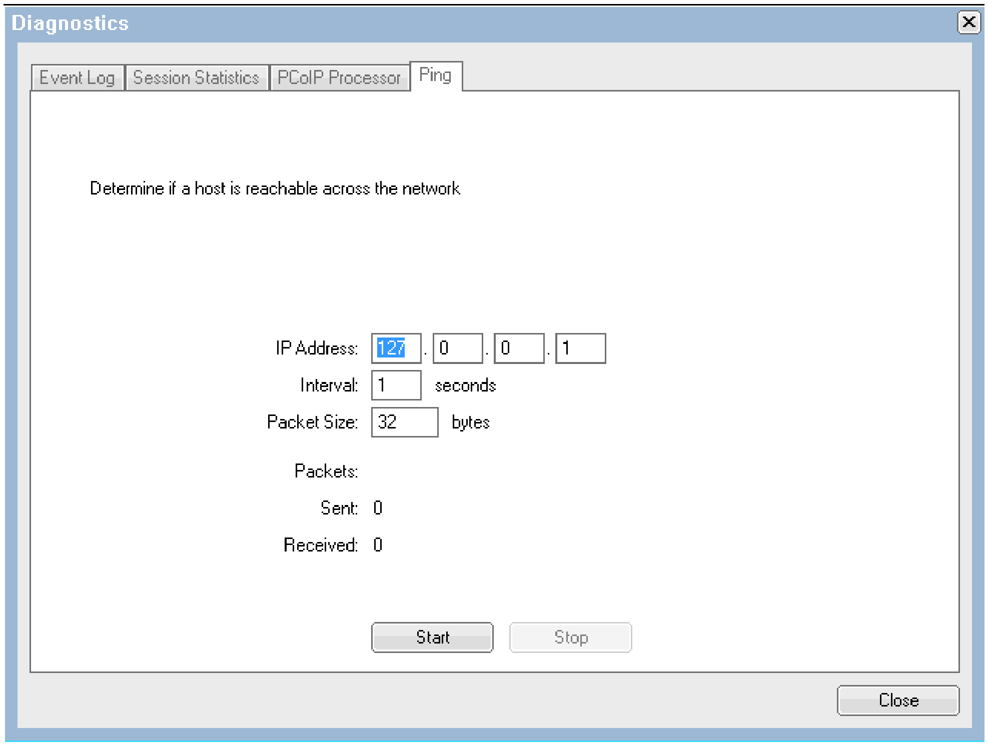
View the time since boot

Uptime: 0 Days 6 Hours 42 Minutes 54 Seconds

Figure 6-22 The PCoIP Processor tab of the T C10 local interface

Ping tab

The Ping tab allows you to ping an IP address (Figure 6-23).



Determine if a host is reachable across the network

IP Address: 127 . 0 . 0 . 1
Interval: 1 seconds
Packet Size: 32 bytes

Packets:
Sent: 0
Received: 0

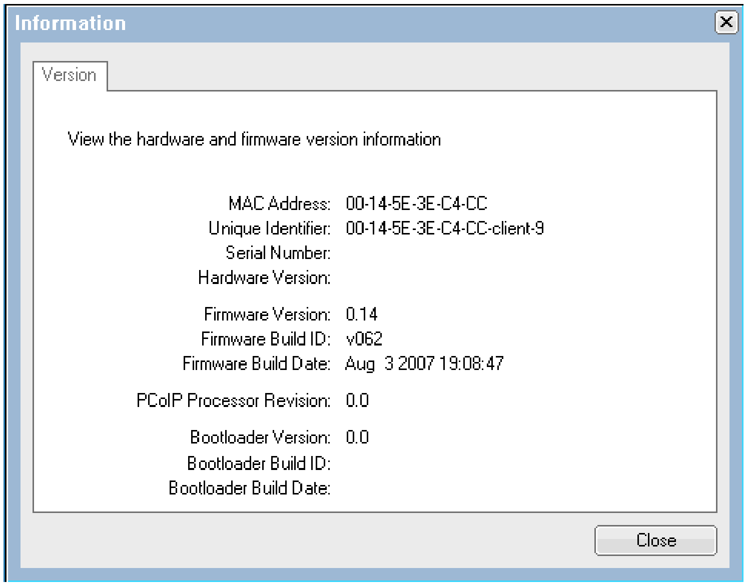
Figure 6-23 The Diagnostics menu showing the ping option

To ping an IP address, enter the IP address that you want to ping, along with the interval seconds and the size of the packet. Click **Start**, and it says how many packets were sent and received.

If the number sent equals the number received, you are pinging the IP address successfully. However, if it says that none are received, that means you cannot ping the IP address. This feature is a good feature to use if you are having trouble connecting to a specific address.

6.3.4 Information panel

The Information panel only has one tab, Version. The Version tab lists much of the hardware and firmware information of the CP20 (Figure 6-24).



View the hardware and firmware version information

MAC Address: 00-14-5E-3E-C4-CC
Unique Identifier: 00-14-5E-3E-C4-CC-client-9
Serial Number:
Hardware Version:

Firmware Version: 0.14
Firmware Build ID: v062
Firmware Build Date: Aug 3 2007 19:08:47

PCoIP Processor Revision: 0.0

Bootloader Version: 0.0
Bootloader Build ID:
Bootloader Build Date:

Figure 6-24 The Version tab on the CP20 interface

This tab allows you to obtain the MAC address, serial number, and hardware version of the CP20. It is also helpful to see which firmware version the CP20 is currently using.

It is important to keep the firmware as the most recent version. You can use the Devon IT Connection Broker software to deploy firmware as described in 5.1.3, “Updating firmware” on page 74.

6.3.5 User Settings panel

In the User Setting panel, you can adjust the mouse and keyboard responsiveness while in the CP20 local interface.

The Mouse tab, as shown in Figure 6-25, lets you specify how fast or slow the mouse pointer moves in relation to moving the mouse.

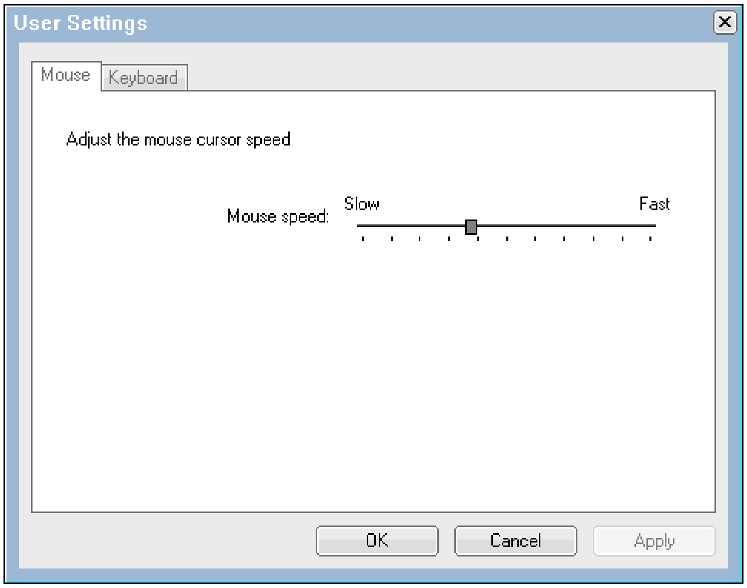


Figure 6-25 Mouse user settings tab in the CP20 local interface

The Keyboard tab, as shown in Figure 6-26, lets you control how the keyboard reacts to key presses.

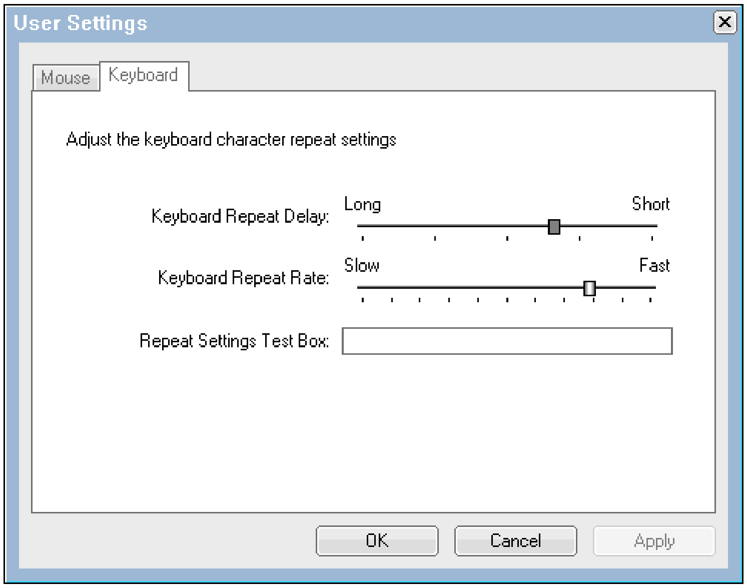


Figure 6-26 Keyboard user settings tab in the CP20 local interface

6.3.6 Password panel

The Password panel (Figure 6-27) allows you to set a password for the HC10 or the CP20. The default password is PASSW0RD (with a zero not the letter *O*). We recommend that you change the password for all the devices as a security measure.

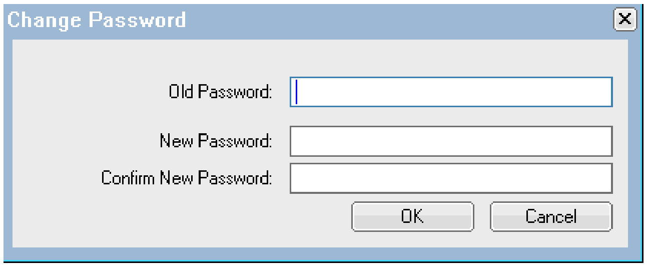


Figure 6-27 Changing the password to the CP20 configuration panels

Note: Changing the password using the local CP20 also changes the password used to connect through the Web interface.

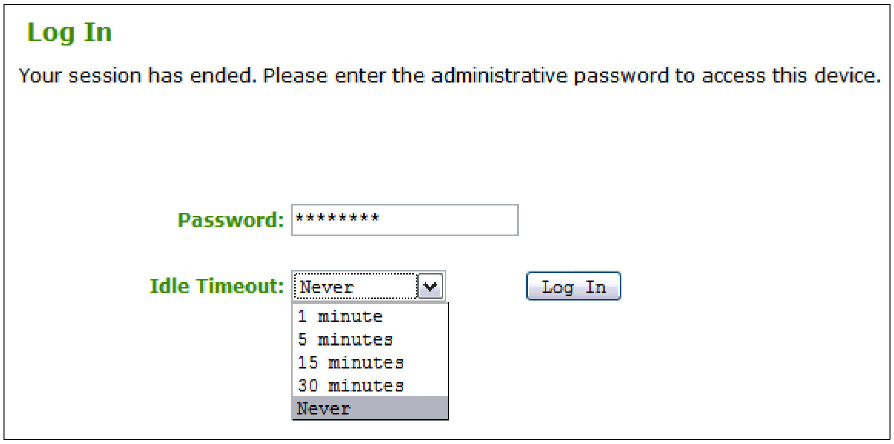
6.4 HC10 and CP20 Web interfaces

The HC10 and CP20 have very similar Web interfaces. They have the same layout and contain the same options; however, some options apply to only the HC10 or CP20. In the figures in this section, we typically show the same dialog box in both HC10 and CP20 interfaces to highlight the differences. In cases where the dialog box is identical, we only display one version.

The following steps explain how to access the Web interfaces:

1. Turn on the HC10 or CP20 (the device that you want to access).
2. Connect a computer to the network to which I/O module 2 is connected (or the Ethernet switch module that you have configured to route the HC10-CP20 traffic, if you have changed the defaults).
3. Open a Web browser on the computer, and enter the IP address of the device in the browser address field.

4. Enter the password (default is PASSW0RD, with a zero not the letter *O*), choose the idle time, and click **Log in**. See Figure 6-28.



Log In

Your session has ended. Please enter the administrative password to access this device.

Password: ********

Idle Timeout: Never

Figure 6-28 Web interface password panel

Only one user at a time can log in to the Web interface. If a user is logged in to the Web interface, a second user who attempts to log in is warned that the target is in use. If the second user decides to log in anyway, the first user is logged out automatically. To log out, click **Log out** in the upper left of the window (see Figure 6-29).

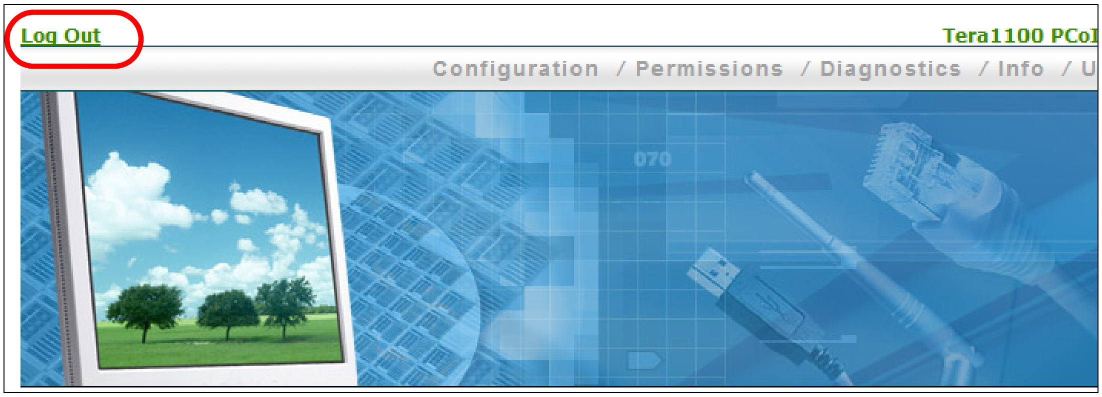


Figure 6-29 Logging out of the Web interface

When logged in, there are five menu options that provide a sublist of options. We discuss these options in the following sections:

- 6.4.1, “Configuration menu” on page 120
- 6.4.2, “Permissions menu” on page 130
- 6.4.3, “Diagnostics menu” on page 132
- 6.4.4, “Info menu” on page 136
- 6.4.5, “Upload menu” on page 138

6.4.1 Configuration menu

The Configuration menu allows you to configure the device and prepare it for a connection (Figure 6-30). The Configuration menu, except for the additional Password and User Settings options, is identical to the local interface of the CP20.

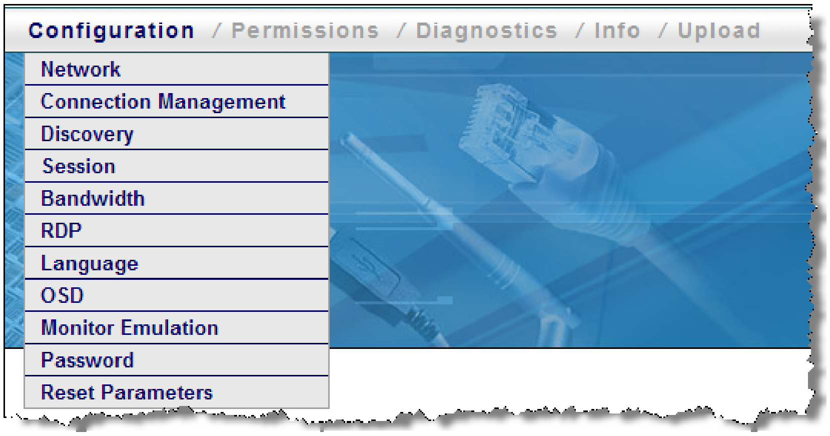


Figure 6-30 Configuration menu

Like the CP20 local interface, A key aspect to the settings in the Configuration menu is that fields in some submenu items are ignored under certain circumstances, as follows:

- If you enable the use of a connection broker (that is, if you select **Enable Connection Management** in the Connection Management window), then all fields in both the Discovery window and Session window are ignored.
- If you enable discovery (that is, you do not have **Enable Connection Management** selected in the Connection Management window, but you do select **Enable Discovery** in the Discovery window), then all fields in the Session window are ignored.
- If you enable the use of a connection broker, or enable discovery, or you select **PCoIP** as the session type in the Session window, then the contents of the RDP window are ignored.

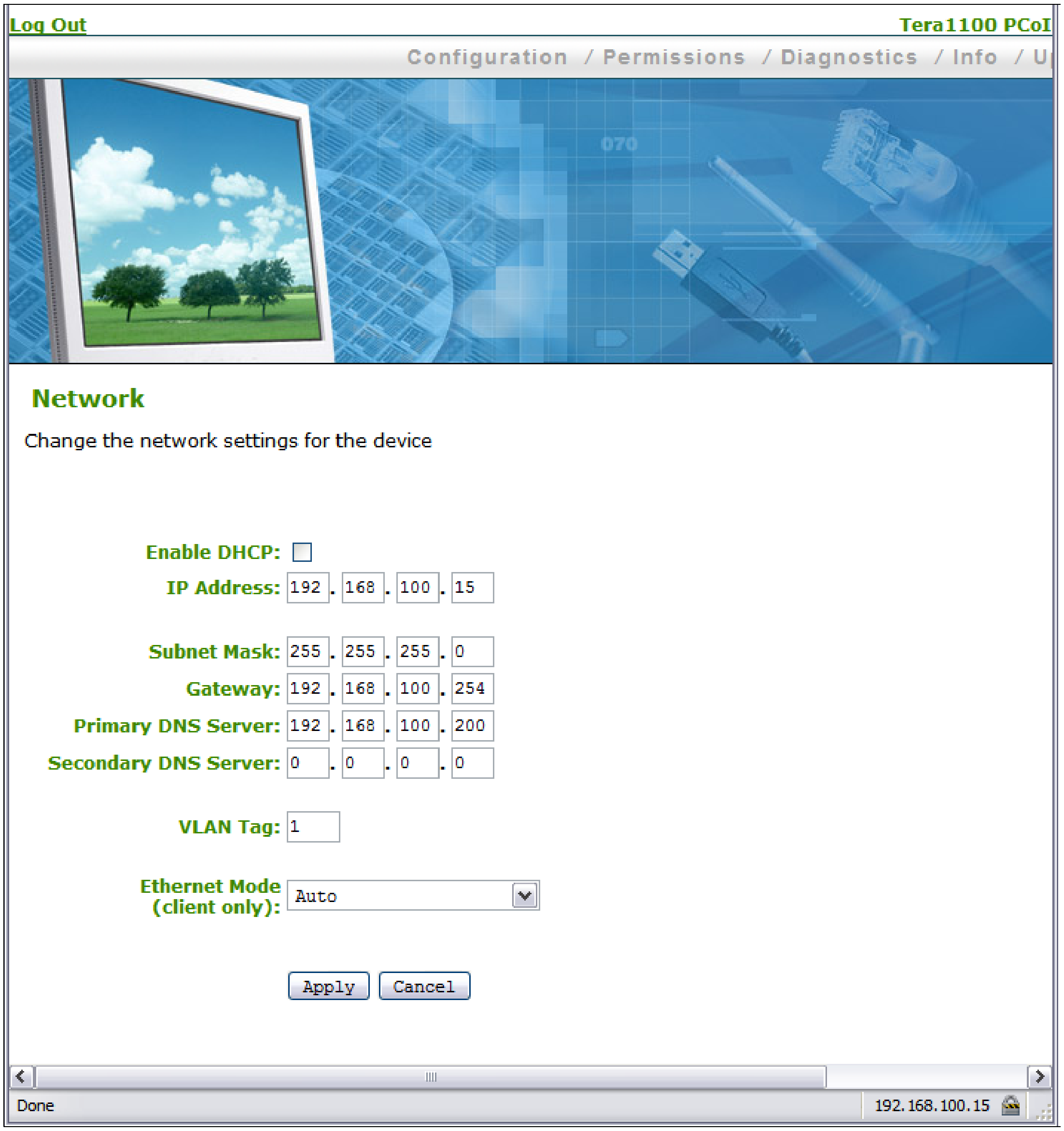
We discuss each of the configuration menu items in detail in the following sections:

- "Network option" on page 121
- "Connection Management option" on page 122
- "Discovery option" on page 123
- "Session option" on page 124
- "Bandwidth option" on page 125
- "RDP option" on page 126
- "Language option" on page 126
- "OSD option" on page 127
- "Monitor emulation option" on page 127
- "Password option" on page 129
- "Reset Parameters option" on page 129

Network option

The Network option (Figure 6-31) allows you to configure the IP settings of the device. This option is the same for both the CP20 and HC10, except that you can chose the Ethernet Mode for the CP20, which allows you to choose either Auto or 100 Mbps Full-Duplex.

> **Tip:** Even those the Web interfaces of the CP20 and HC10 are the same layout, they are still separate interfaces. So, for example, to configure both devices to use DHCP to get an IP address, you must configure this separately in *both* Web interfaces.



Network

Change the network settings for the device

Enable DHCP: □

IP Address: 192 . 168 . 100 . 15

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 100 . 254

Primary DNS Server: 192 . 168 . 100 . 200

Secondary DNS Server: 0 . 0 . 0 . 0

VLAN Tag: 1

Ethernet Mode (client only): Auto

Figure 6-31 The Network option (both the HC10 and CP20)

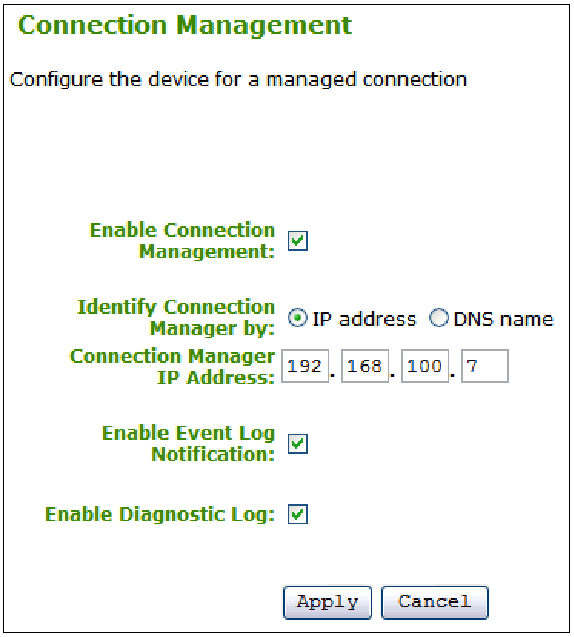
The Network option allows you to chose between using DHCP or a static address. The default is set to DHCP, and the boxes are all disabled. The disabled boxes indicate the IP address that has been assigned by DHCP.

To configure the device to use a static address, clear the Enable DHCP check box. Then, you can enter the IP Address, Subnet Mask, Gateway, and Primary and Secondary DNS servers.

If you have configured a VLAN for your HC10-CP20 connections, enter the VLAN tag under the VLAN Tag field. You can also chose either auto or 100 mbps Full-Duplex as the Ethernet mode (this option is only available on the CP20).

Connection Management option

The Connection Management option (Figure 6-32) allows a user to configure the device with a connection management software.



Connection Management

Configure the device for a managed connection

Enable Connection Management: ☑

Identify Connection Manager by: ● IP address ○ DNS name

Connection Manager IP Address: 192 . 168 . 100 . 7

Enable Event Log Notification: ☑

Enable Diagnostic Log: ☑

Figure 6-32 The Connection Management option (appears in both the HC10 and CP20)

If you select **Enable Connection Management**, the CP20 attempts to connect to the Connection Broker software to establish a connection to an HC10. If you are configuring the connection broker software manually, you must then chose whether you are going to connect through the connection broker's IP address or fully qualified domain name (FQDN).

To use IP address, select **IP Address** and enter the IP address in the appropriate field. For FQDN, select **DNS name** and enter the domain name.

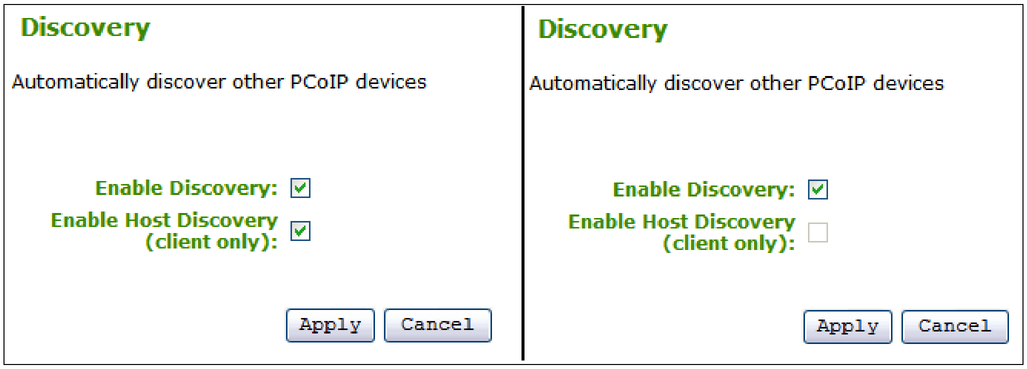
There are also two options for event logs:

- You can select **Enable Event Log Notification**. When this option is selected, the device sends event log messages to the connection broker, approximately once a minute and up to 10 messages at a time until all received messages have been sent. The event log is cleared between power cycles and resets of the device.
- The use of **Enable Diagnostic Log** is used for diagnostic purposes only. This does not send messages to the connection broker.

> **Tip:** When **Enable Connection Management** is selected in the Connection window, the contents of the Discovery window, Session window, and RDP window are all *ignored*. These three window are for peer-to-peer configurations only. These parameters are not used because the use of a connection broker and peer-to-peer connectivity are mutually exclusive options.

Discovery option

The Discovery option enables a peer-to-peer connection and, when you connect, searches automatically for all available HC10s to which you can connect (Figure 6-33). This option and the Session option allow you to connect directly from a CP20 to an HC10 without the use of a connection broker.



Discovery

Automatically discover other PCoIP devices

Enable Discovery: ☑
Enable Host Discovery (client only): ☑

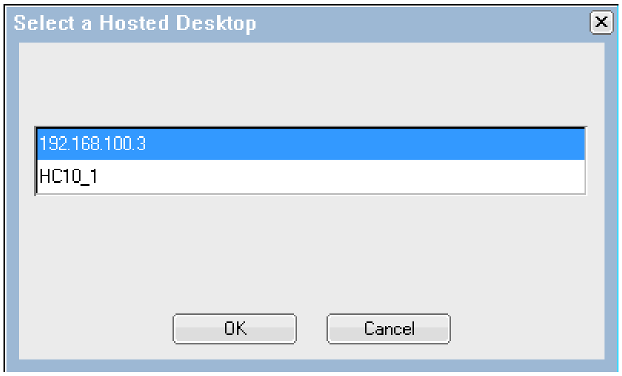
Discovery

Automatically discover other PCoIP devices

Enable Discovery: ☑
Enable Host Discovery (client only): □

Figure 6-33 The Discovery Option on the Web interface of the CP20 (left) and the HC10 (right)

There are two options that can be configured on this option. To use the discovery option, you must select both **Enable Discovery** and **Enable Host Discovery** on the CP20, and you must select **Enable Discovery** on the HC10. Selecting these options gives you the option of which HC10 that you want to connect to. With this option, the CP20 discovers available HC10s and creates a list of available HC10s such as the one shown in Figure 6-34. You can select from the HC10 to which you want to connect from this list.



Select a Hosted Desktop

192.168.100.3
HC10_1

Figure 6-34 List of available HC10s to connect to <<STOP>>

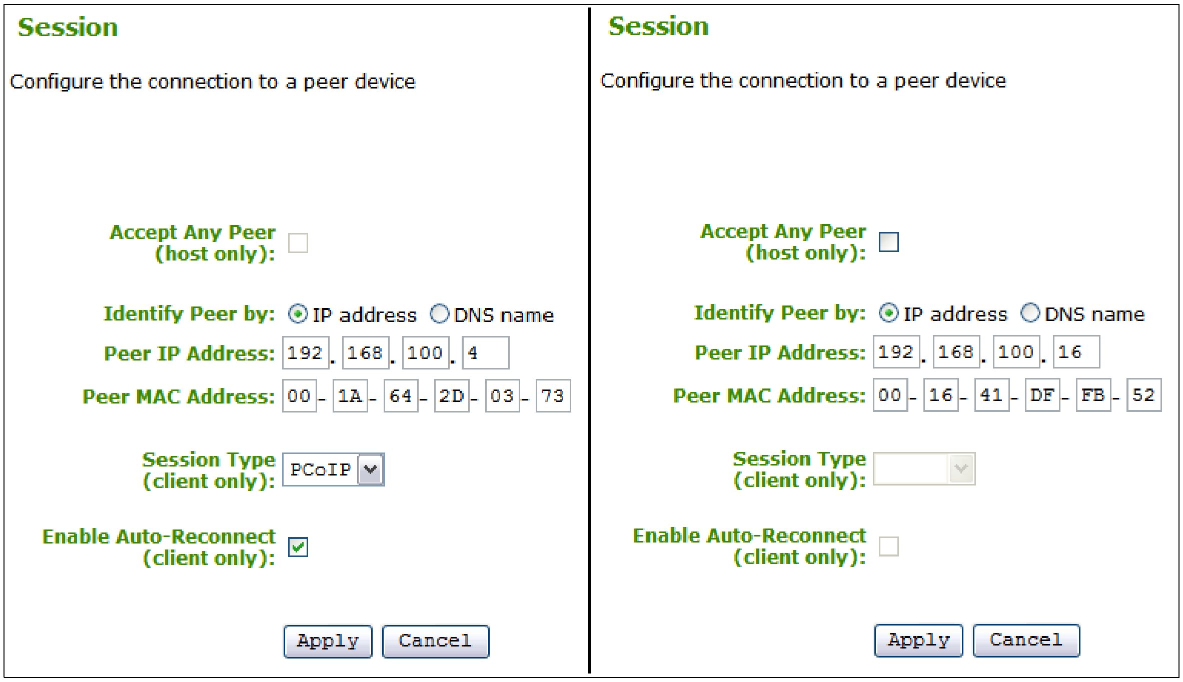
Note: If **Enable Connection Management** is selected in the Connection tab shown in Figure 6-11 on page 104, the Discovery feature is not used and settings on this tab are *ignored*.

For more on the Discovery option, see 6.5.3, “Connect to a HC10 with discovery options” on page 143.

Session option

The Session option, as shown in Figure 6-35, allows you to configure a peer-to-peer session by specifying the IP address and MAC address manually of the exact HC10 to which you want this CP20 to connect. For more information about how to use a peer-to-peer connection, see 6.5, “Setting up a peer-to-peer connection” on page 139.

> **Note:** For the fields in the option to be active, you must ensure that **Enable Discovery** is *not* enabled in the Discovery option and that **Enable Connection Management** is *not* enabled in the Connection Management option. With either of these options enabled, all fields in the Session option are *ignored*.



Session

Configure the connection to a peer device

Accept Any Peer (host only): □

Identify Peer by: ● IP address ○ DNS name

Peer IP Address: 192 . 168 . 100 . 4

Peer MAC Address: 00 - 1A - 64 - 2D - 03 - 73

Session Type (client only): PCoIP

Enable Auto-Reconnect (client only): ☑

Session

Configure the connection to a peer device

Accept Any Peer (host only): □

Identify Peer by: ● IP address ○ DNS name

Peer IP Address: 192 . 168 . 100 . 16

Peer MAC Address: 00 - 16 - 41 - DF - FB - 52

Session Type (client only):

Enable Auto-Reconnect (client only): □

Figure 6-35 The Sessions option for the Web interface of the CP20 (left) and the HC10 (right)

As shown in Figure 6-35, fields that apply only to the HC10 (host) are disabled in the CP20 (client) and vice versa.

On the CP20 (left side of the figure), you can establish a peer-to-peer connection by either knowing the HC10s IP address or the fully qualified domain name (FQDN). To use the IP address, select **IP Address** and enter the HC10 compression card’s IP address in the appropriate fields. To use FQDN, select **FQDN** and enter the domain name.

You also need to enter the MAC address of the compression card of the HC10. Two ways to determine the compression card MAC address are:

- Boot the HC10 and press F1 to go into BIOS. Then, select **Advanced Settings** → **Compression Card Network Configuration**. The MAC address displays on the dialog box that opens.
- Leave an incorrect value for the MAC address in Figure 6-35 and try to connect to the HC10. The connection fails with the message “`Session Refused!`”. Then, click **Options** → **Diagnostics**. In the Event Log, you see two entries: one that lists the incorrect MAC address and one that lists the MAC address that was expected. Simply copy that expected address into the fields in Figure 6-35. For example, if you specified a fake MAC address of

all zeros (`00-00-00-00-00-00`), then the messages you see in the event log would be similar to that shown in Example 6-2.

Example 6-2 Error log messages showing the correct MAC address of the compression card

```
Connecting with host (9.42.170.185, 00-00-00-00-00-00)
Peer MAC mismatch: (00-1A-64-2D-02-EE, 00-00-00-00-00-00)
```

The correct MAC address is this example is `00-1A-64-2D-02-EE`.

On the HC10, you can elect to either allow any CP20s to connect to this HC10 by selecting **Accept any Peer**, or if you want to allow only one specific CP20 to connect, then leave **Accept any Peer** clear and fill in the fields as described previously. You can obtain the MAC address of the CP20 from the Information panel (see Figure 6-24 on page 116).

Note: Future firmware updates might remove the need to enter the MAC address.

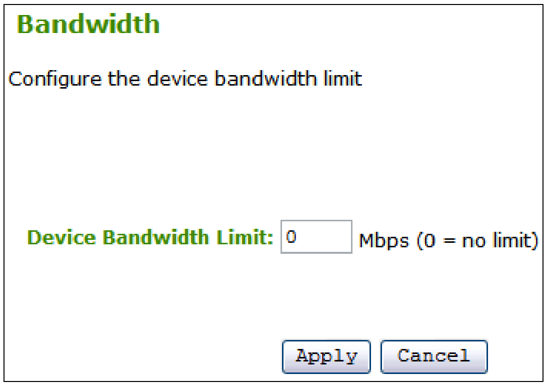
The Session Type can be either PCoIP or RDP; however, to connect to an HC10, you need to set this option to PCoIP. This field is only valid on the CP20.

The Enable Auto-Reconnect option configures the CP20 to try to connect automatically to the last HC10 to which it connected when the CP20 is turned on. The CP20 tries to reconnect only on a boot and not after a session disconnect.

The fields in this window are not used if connection management or discovery are enabled. Although you will still be able to configure the settings, this tab will be ignored if either of those are enabled.

Bandwidth option

The Bandwidth option allows you to set the bandwidth limits for the device (Figure 6-36). To change the bandwidth limit, either enter a number for the maximum Mbps or enter zero (0) for no limit.



Bandwidth

Configure the device bandwidth limit

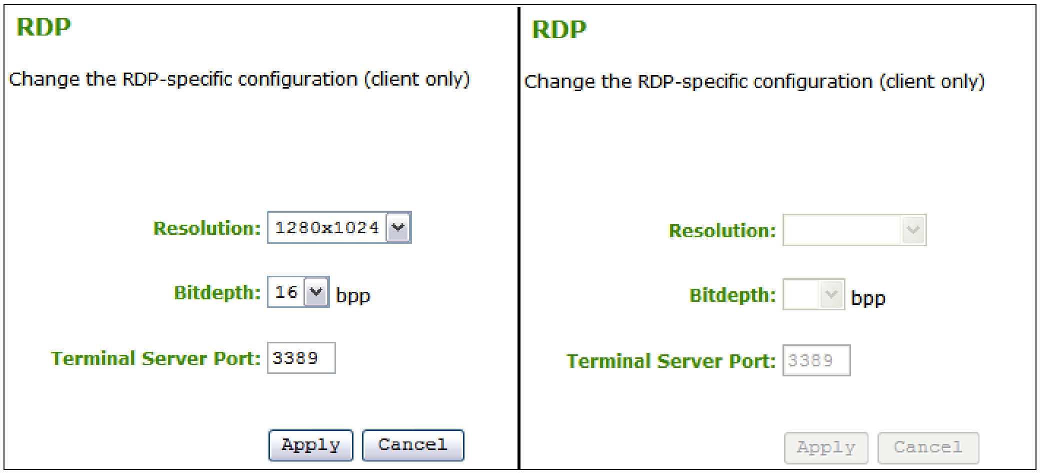
Device Bandwidth Limit: 0 Mbps (0 = no limit)

Figure 6-36 The Bandwidth option on the Web interface of the HC10 and CP20

The setting in the HC10 controls the downstream bandwidth which is mostly video traffic. The setting in the CP20 controls the upstream bandwidth which is mostly USB traffic. We recommend you leave this value at 0, as this will allow the devices to dynamically allocate bandwidth as needed.

RDP option

The RDP option, as shown in Figure 6-37, allows a user to configure the resolution, bit depth, and terminal server port for a RDP connection. These changes can only be done on the client side.



RDP

Change the RDP-specific configuration (client only)

Resolution: 1280x1024

Bitdepth: 16 bpp

Terminal Server Port: 3389

RDP

Change the RDP-specific configuration (client only)

Resolution:

Bitdepth: bpp

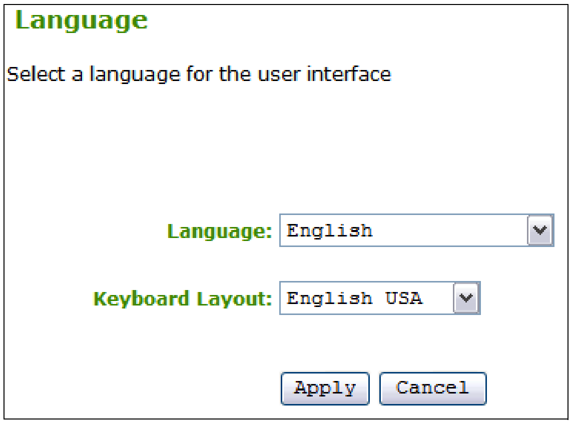
Terminal Server Port: 3389

Figure 6-37 The RDP option on the Web interface of the CP20 (left) and the HC10 (right)

The fields in this window are ignored unless you have specified RDP as a Session Type under the Sessions option. For a CP20 to HC10 configuration, this tab is not used, because the session type will always be PCoIP.

Language option

The Language option allows you to set a desired language for the CP20 and set the keyboard layout (Figure 6-38). To set a language or keyboard layout, simply select the appropriate option from the drop-down menu.



Language

Select a language for the user interface

Language: English

Keyboard Layout: English USA

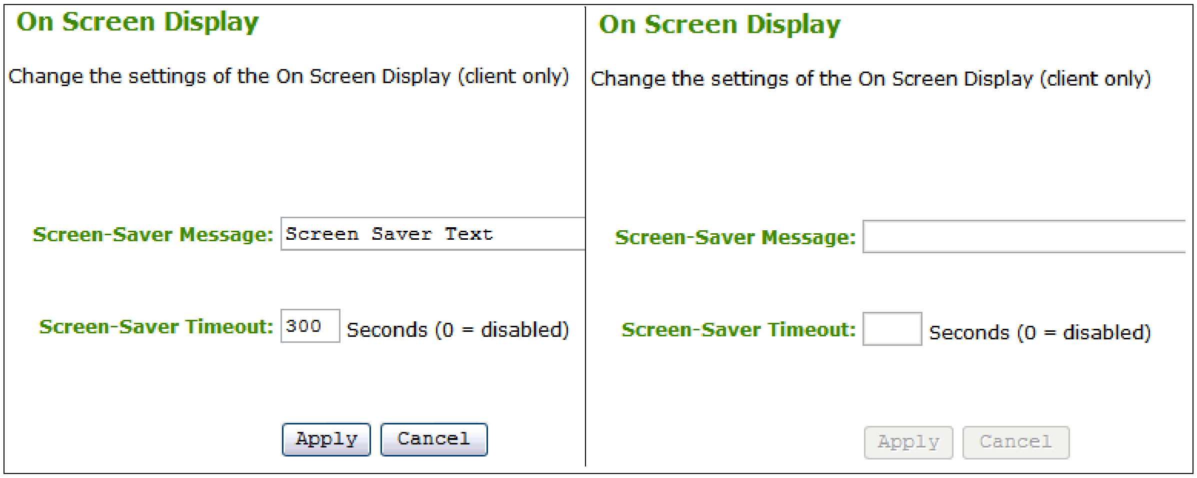
Figure 6-38 The Language option (both the HC10 and CP20)

This option is only available for the CP20. At the time of this writing, there was only one language option for the CP20: English. For keyboard layout, you can chose between English U. S. and French Canada.

Note: The settings on the Language tab do not affect any language settings that you have defined in Windows on the HC10. These settings are just for the local and Web interfaces of the CP20.

OSD option

The OSD option allows you to enter a message to appear as a screen saver and to set a screen saver timeout. This option is only available on the CP20. The buttons and text boxes are disabled on the HC10 interface. See Figure 6-39.



On Screen Display

Change the settings of the On Screen Display (client only)

Screen-Saver Message: Screen Saver Text

Screen-Saver Timeout: 300 Seconds (0 = disabled)

On Screen Display

Change the settings of the On Screen Display (client only)

Screen-Saver Message:

Screen-Saver Timeout: Seconds (0 = disabled)

Figure 6-39 The OSD option on the Web interface of the CP20 (left) and the HC10 (right)

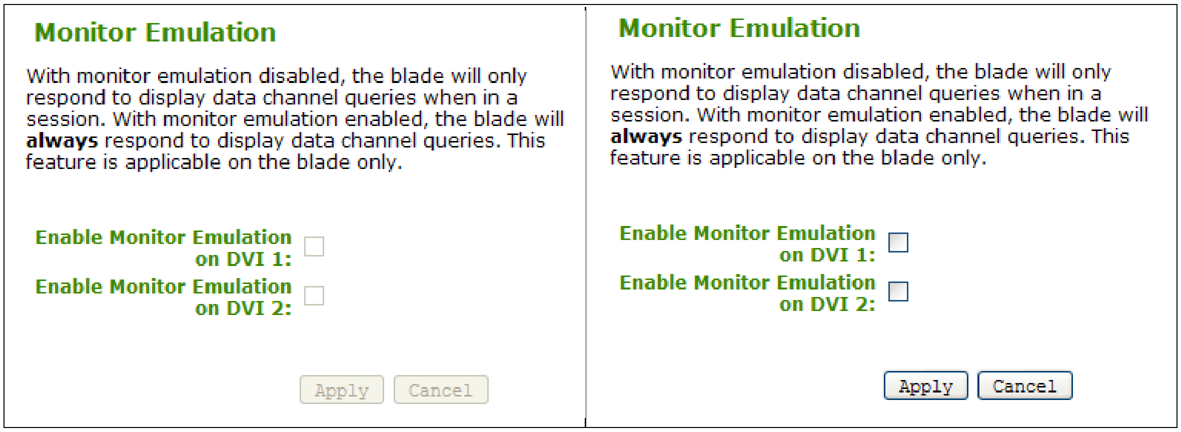
The default screen saver text is `Screen Saver Text`, and the default timeout is set to 300 seconds (5 minutes).

To change the text, enter new text in the **Screen-Saver Text** field. You can also change the amount of time that it takes before the screen saver is used by entering a new number in the **Screen-Saver Timeout** field. This timeout is entered in number of seconds, and entering zero (0) disables the screen saver.

The actual screen saver is a black background with simple, white text that is placed randomly on the screen. This screen saver is used only when there is no active session to an HC10.

Monitor emulation option

Monitor emulation option is a function that you enable on the HC10s (see Figure 6-40). When enabled, the compression card on the HC10 presents to the video card that a monitor is connected even when a CP20 workstation connection device isn't in session.



Monitor Emulation

With monitor emulation disabled, the blade will only respond to display data channel queries when in a session. With monitor emulation enabled, the blade will **always** respond to display data channel queries. This feature is applicable on the blade only.

Enable Monitor Emulation on DVI 1: □

Enable Monitor Emulation on DVI 2: □

Monitor Emulation

With monitor emulation disabled, the blade will only respond to display data channel queries when in a session. With monitor emulation enabled, the blade will **always** respond to display data channel queries. This feature is applicable on the blade only.

Enable Monitor Emulation on DVI 1: □

Enable Monitor Emulation on DVI 2: □

Figure 6-40 The Monitor Emulation option on the Web interface of the CP20 (left) and the HC10 (right)

We recommend that you enable this option. If the CP20 device or devices that are to connect to this HC10 have two monitors attached, you need to select both boxes in Figure 6-40. If you have only one monitor attached to each CP20, then only select that box.

This feature emulates a monitor by presenting digital extended display identification data (EDID) to the video card when the compression card gets power. This feature allows EDID to be available before you are in session with the CP20, which helps with the timing of the video card receiving EDID and displaying video on the monitors connected to the CP20. It allows video to be seen when a session is connected after the desktop has been reached and when the session is disconnected and reconnected without turning off the blade.

Note: After monitor emulation is enabled, you must restart the HC10 before it is activated.

Configuration notes:

- On the back of the CP20, the upper DVI port is *DVI 1* and the lower port is *DVI 2*. See Figure 3-7 on page 36.
- If you enable Monitor Emulation on both DVI 1 and DVI 2, you also need to enable the second monitor in the NVIDIA driver before you will see video on DVI 2.
- If you plan to connect to multiple HC10 workstation blades using the same CP20, you must enable Monitor Emulation the same way.

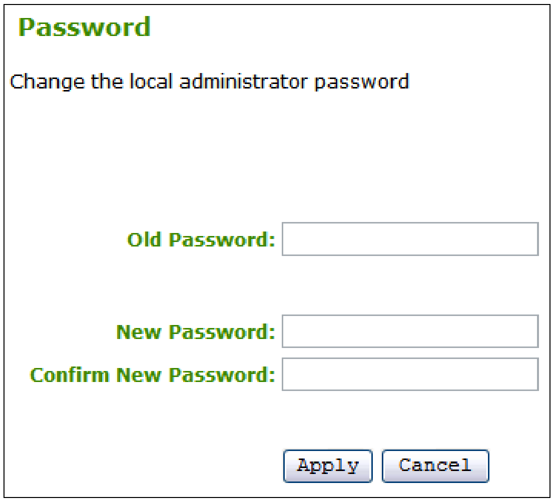
Notes:

- If you enable Monitor Emulation on both DVI ports, you will not be able to use the BladeCenter Advanced Management Module local console or browser-based remote console to view HC10 video because the video card only supports two monitors and the DVI connections have priority.
- If you have a monitor connected to DVI port 1 and enable Monitor Emulation, you will also not be able to view the HC10 video using the BladeCenter Advanced Management Module local console or browser-based remote console. This feature is by design for security reasons. If you want to be able to use the AMM console (local or remote), then connect the monitor to DVI 2.
- If you only have Monitor Emulation enabled on one port but connect monitors to both ports, then you will need to manually enable the second monitor in the operating system using the NVIDIA Control Panel.
- On HC10 blades with the NVIDIA FX 1600M 3D video card installed, if you enable Monitor Emulation on one DVI port, then you will not be to see POST messages, because the FX 1600M only supports one monitor during POST.

See 4.6.2, “Other video-related tips” on page 57 for a list of RETAIN tips that are related to video and the Monitor Emulation feature.

Password option

The Password option allows you to set a password for the HC10 or the CP20 (Figure 6-41). The default password is PASSW0RD (with a zero not the letter *O*). We recommend that you change the password for all the devices as a security measure.



Password

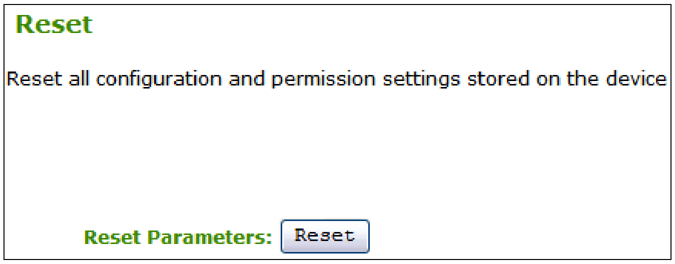
Change the local administrator password

Figure 6-41 The Password option (both the HC10 and CP20)

> **Note:** Changing the password here also changes the password that is used to connect to the local CP20 interface.

Reset Parameters option

The final option under the Configuration menu is Reset Parameters (Figure 6-42). This option allows you to reset all of the configurations and permissions to the default, which means that the devices go back to using DHCP and are enabled for use with a Connection Broker. To reset the parameters, simply click **Reset**.



Reset

Reset all configuration and permission settings stored on the device

Figure 6-42 The Reset Parameters option (both the HC10 and CP20)

> **Note:** This reset option also resets the login password to PASSW0RD (with a zero not the letter *O*).

6.4.2 Permissions menu

The Permissions menu, shown in Figure 6-43 allows you to set various permissions:

- Which USB devices can be connected to the USB ports of the CP20
- Whether audio from the HC10 is routed to the CP20
- What the HC10 remote power button does on the CP20

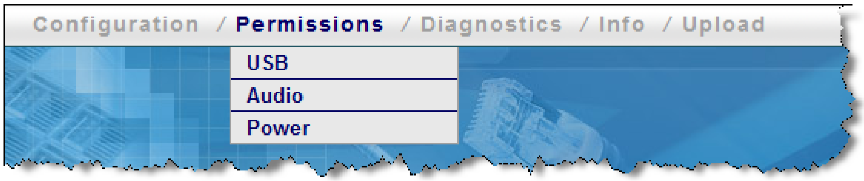
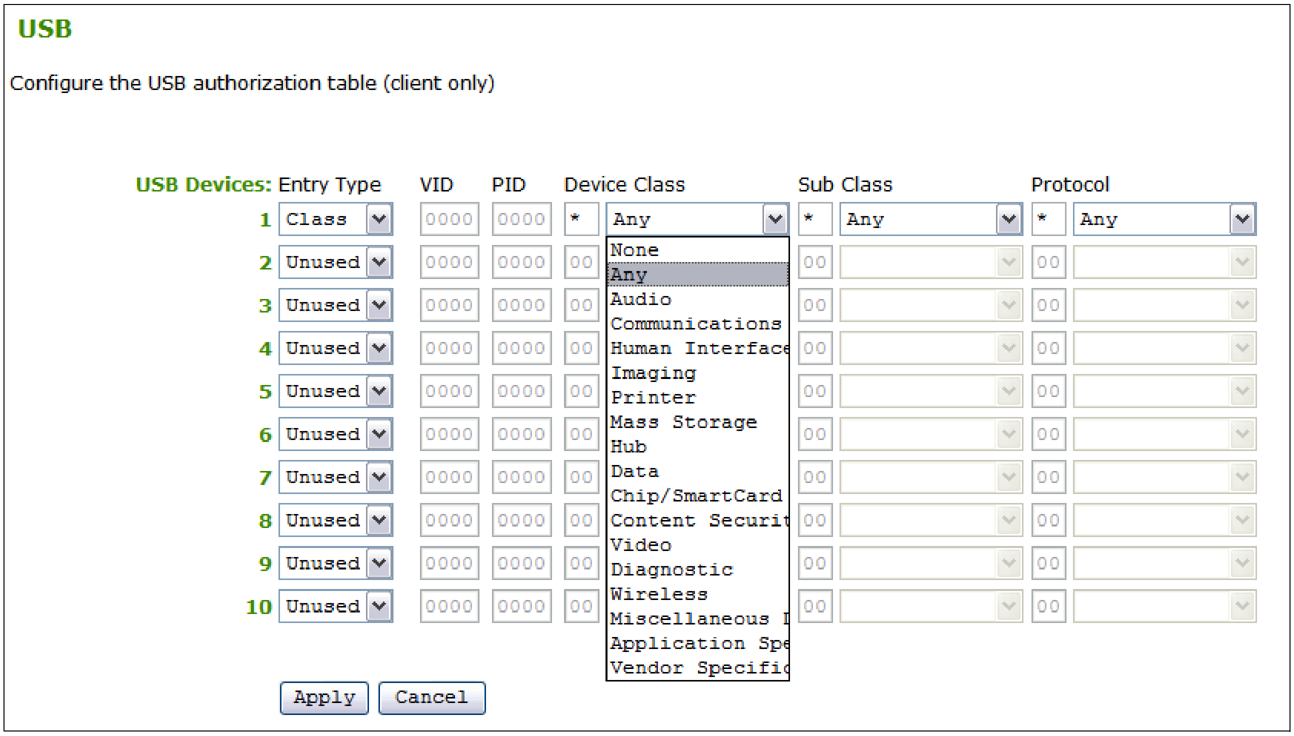


Figure 6-43 The Permissions menu on the Web interface of the HC10 and CP20

USB

The USB window allows you to configure which USB devices are permitted for use with the CP20 (Figure 6-44). This configuration option is only accessible from the CP20 Web interface. From the drop-down list, you can select which type of devices you will allow to be used.



USB

Configure the USB authorization table (client only)

USB Devices:	Entry Type	VID	PID	Device Class		Sub Class		Protocol	
1	Class	0000	0000	*	Any	*	Any	*	Any
2	Unused	0000	0000	00		00		00	
3	Unused	0000	0000	00		00		00	
4	Unused	0000	0000	00		00		00	
5	Unused	0000	0000	00		00		00	
6	Unused	0000	0000	00		00		00	
7	Unused	0000	0000	00		00		00	
8	Unused	0000	0000	00		00		00	
9	Unused	0000	0000	00		00		00	
10	Unused	0000	0000	00		00		00	

Figure 6-44 The USB option showing the different types of devices that can be allowed on the CP20

The USB authorization table is provided as an addition security or control feature. By default, all USB device types are allowed but for security purposes you can specify exactly which devices are allowed. All other USB devices you have not authorized are simply ignored when inserted.

As shown in Figure 6-44, you specify the types of USB devices allowed in the Device Class column. For example, if you only want the user to be able to plug in a keyboard and mouse, select **Human Interface Devices** from the Device Class drop-down list and leave Class and Protocol as **Any**. There are 10 rows that allow you to give permissions to multiple devices.

There are three Entry Types from the first column of drop-down lists:

- The **Unused** option should be chosen for the rows that are not needed.
- The **ID** option allows you to enter the VID and PID of a particular device that you want to authorize. You can find these values by authorizing all USB devices, attaching the particular device, and viewing the Attached Devices option (see “Attached Devices option” on page 137). Then, choose ID as the entry type and enter the VID and PID numbers of the device in the appropriate fields.
- The **Class** entry type allows you to select from a list of device classes for the devices you want to authorize (see Figure 6-44 on page 130). If a device is not authorized, there will be no impact when that USB device is plugged into the CP20. It will not be considered inserted.

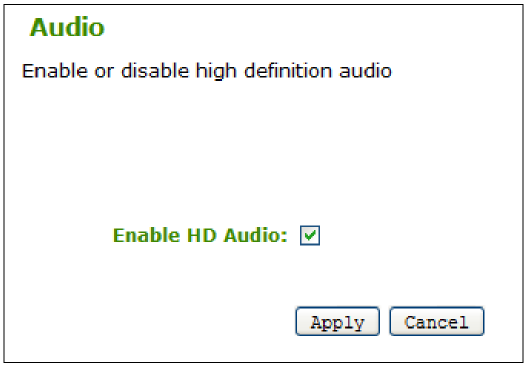
If you plan to restrict the use of certain USB devices such as thumb drives, it is very important that you also disable the use of USB hubs. Authorization of devices according to user identification, class type, and so forth is done on a per-port basis. Thus, if you allow the use of a hub, then you allow any type of device to be subsequently connected through the hub, regardless of the other USB permissions.

Audio option

For a user to use speakers and microphone, audio must be enabled both on the HC10 and the CP20.

Note: Audio is disabled by default.

The Audio option provides an option for enabling HD audio, as shown in Figure 6-45.



Audio

Enable or disable high definition audio

Enable HD Audio: ☑

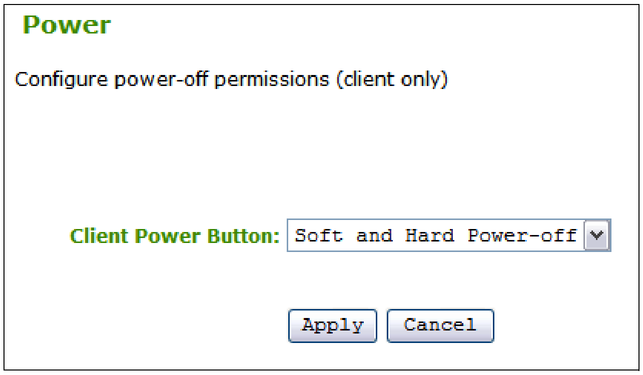
Figure 6-45 The Audio option (both the CP20 and HC10)

To enable audio for the user, this parameter must be enabled on both the CP20 and the HC10. Clearing either prevents audio. If you clear this option in the HC10, then the audio device is not visible to Windows.

Changing this setting on the HC10 (either enabling or disabling) requires that you reboot the HC10 before the change takes affect.

Power option

The Power option, as shown in Figure 6-46, controls what action the HC10 remote power button on the front of the CP20 performs when pressed (see Figure 3-7 on page 36).



Power

Configure power-off permissions (client only)

Client Power Button: Soft and Hard Power-off

Figure 6-46 The Power option (CP20 only)

The Power options are:

- *Power-off not permitted*: The button on the CP20 does nothing.
- *Soft power-off only*: The button performs and the operating system shuts down, then turns off the HC10.
- *Hard power-off only*: Pressing the button for four seconds or longer turns off the HC10 immediately, not allowing it to end its processes or shut down first. Pressing the button for less than four seconds does nothing.
- *Soft and hard power-off*: Allows you to do either a soft or hard power off. For a soft power off, you must hold the button for less than four seconds. For a hard power off, you must hold the button for longer than four seconds.

6.4.3 Diagnostics menu

In this section, we discuss the options under the Diagnostics menu (Figure 6-47).

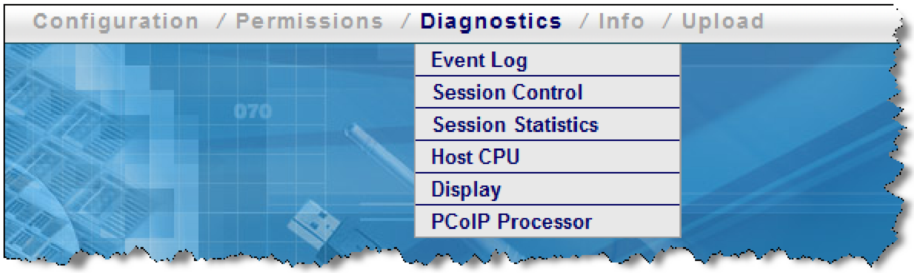
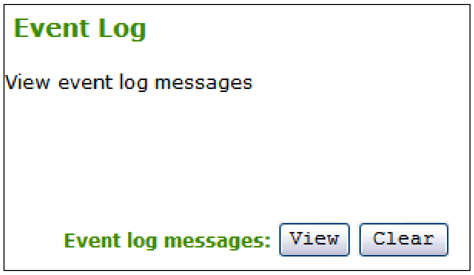


Figure 6-47 The Diagnostics menu on the Web interface HC10 and CP20

Event Log option

The Event Log option provides two buttons to either view the event log or to clear it (Figure 6-48).



Event Log

View event log messages

Event log messages:

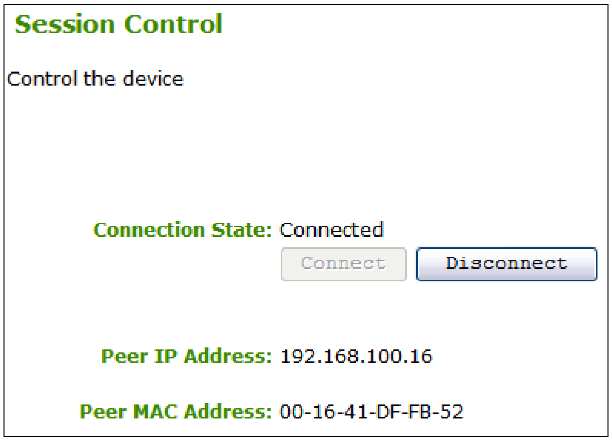
Figure 6-48 The Event Log option of the Web interface of the HC10 and CP20

To view the event log, click **View** to open a new browser window with the log information.

To clear the even log, click **Clear**.

Session Control option

The Sessions Control option states whether there is an active connection and allows you to connect or disconnect the device (Figure 6-49).



Session Control

Control the device

Connection State: Connected

Peer IP Address: 192.168.100.16

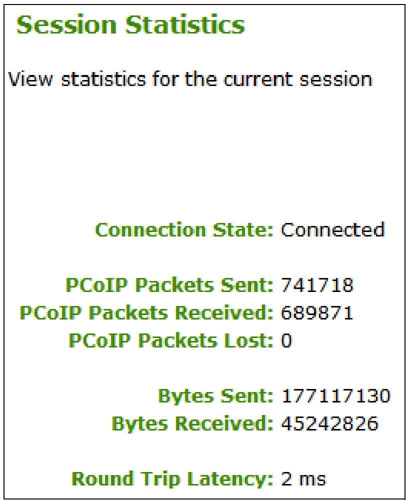
Peer MAC Address: 00-16-41-DF-FB-52

Figure 6-49 The Session Control option on the Web interface of the HC10 and CP20

If the device is connected, you are able to disconnect the session by clicking **Disconnect**. This is the same as pressing the Session Disconnect button on the front of the CP20 (see Figure 3-7 on page 36). If the connection is listed as disconnected, you are able to click the **Connect** button, and it connect using the method that you configured previously.

Session Statistics option

The Session Statistics option gives the statistics for the current session or states that it is disconnected if there is no active session (Figure 6-50).



Session Statistics

View statistics for the current session

Connection State: Connected

PCoIP Packets Sent: 741718
PCoIP Packets Received: 689871
PCoIP Packets Lost: 0

Bytes Sent: 177117130
Bytes Received: 45242826

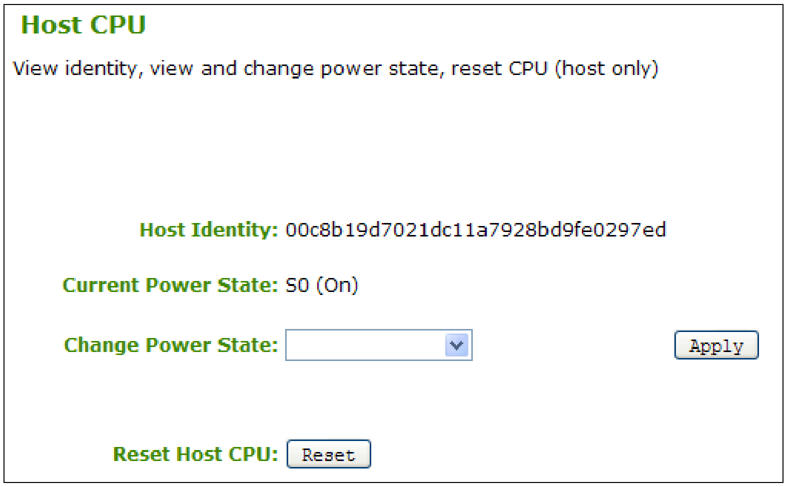
Round Trip Latency: 2 ms

Figure 6-50 The Session Statistics option on the Web interface of the HC10 and CP20

This option allows you to view the number of PC-over-IP packets that have been sent, received, and lost. It also shows the number of bytes sent and received. Finally, it shows the round trip latency in ms. This is the latency time that it takes for a packet to get from the compression card of the HC10 to the compression card of the CP20 and back.

Host CPU option

The Host CPU option allows you to view the host identity, view and change the current power state, and reset the host CPU. These options are only available on the HC10. See Figure 6-51.



Host CPU

View identity, view and change power state, reset CPU (host only)

Host Identity: 00c8b19d7021dc11a7928bd9fe0297ed

Current Power State: S0 (On)

Change Power State:

Reset Host CPU:

Figure 6-51 The Host CPU option on the Web interface of the HC10 (HC10 only)

The Host Identity uniquely identifies the HC10 attached to the CP20.

The Current Power State field lists the current state of the HC10. The possible states are:

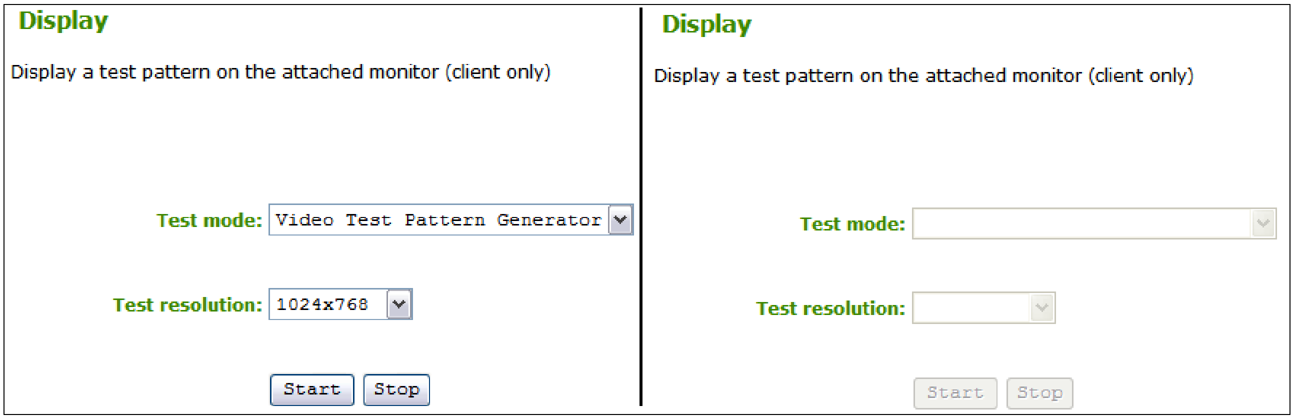
- S0 (Power On)
- S1 (Sleep)
- S2 (Sleep)
- S3 (Standby)
- S4 (Hibernate)
- S5 (Power Off)

The Change Power State field allows changing the power status of the Host computer. The available states to change to are:

- S0 (On): Turn the HC10 on
- S3 (Soft Off): Performs a soft power-off of the HC10 with a controlled OS shutdown
- S3 (Hard Off): Performs a hard shut down of the HC10 without OS involvement

Display option

The Display option is used to display a test pattern on the screen of the CP20. This option is disabled on the HC10 and available only for the CP20. See Figure 6-52.



Display

Display a test pattern on the attached monitor (client only)

Test mode: Video Test Pattern Generator

Test resolution: 1024x768

Display

Display a test pattern on the attached monitor (client only)

Test mode:

Test resolution:

Figure 6-52 The Display option on the Web interface of the CP20 (left) and the HC10 (right)

There are two options for test mode which each generate a pattern on the CP20:

- Video Test Pattern Generator
- Pseudo Random Bitstream

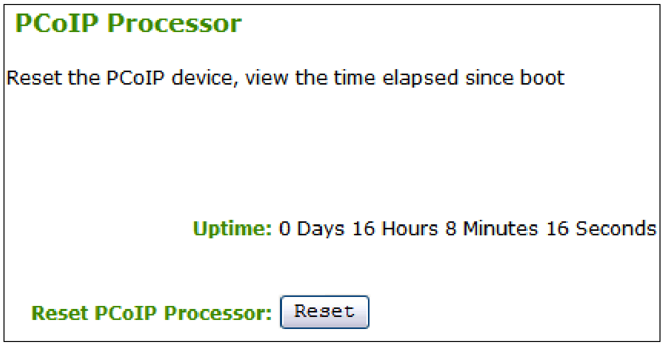
There is also a drop-down list of test resolutions that includes:

- 1024x768
- 1280x1024
- 1600x1200
- 1920x1200

After you have selected the appropriate test mode and resolution, click **Start**. You will the test on the CP20’s display. To stop the test, click **Stop**.

PCoIP Processor option

The PCoIP Processor option is used to see the time elapsed since the last boot and to reset the PC-over-IP processor. Certain configurations prompt you to reset the PC-over-IP processor, and this is where you can do that. To reset the processor, click **Reset**. See Figure 6-53.



PCoIP Processor

Reset the PCoIP device, view the time elapsed since boot

Uptime: 0 Days 16 Hours 8 Minutes 16 Seconds

Figure 6-53 The PCoIP option of the Web interface of the HC10 and the CP20

If the device you are resetting is a CP20, then it resets (restarts) the PC-over-IP processor immediately. If you are resetting the PC-over-IP processor on the HC10 compression card, then the reset occurs the next time the HC10 is shutdown, rebooted, or goes into standby or hibernation.

6.4.4 Info menu

In this section we discuss the options in the Info menu (Figure 6-54).

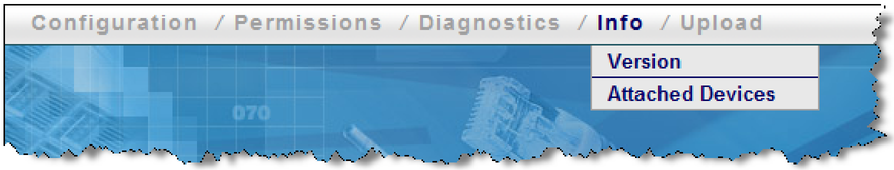
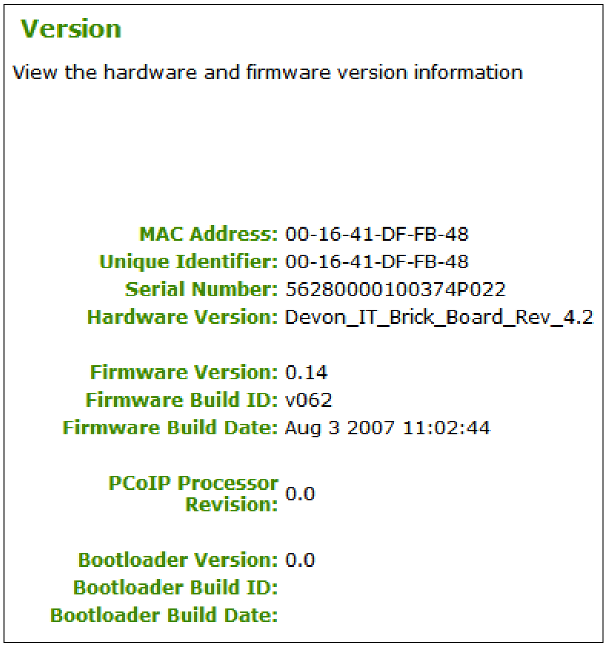


Figure 6-54 The Info menu on the Web interface of the HC10 and the CP20

Version option

The Version option allows you to see the information about your device (Figure 6-55).



Version

View the hardware and firmware version information

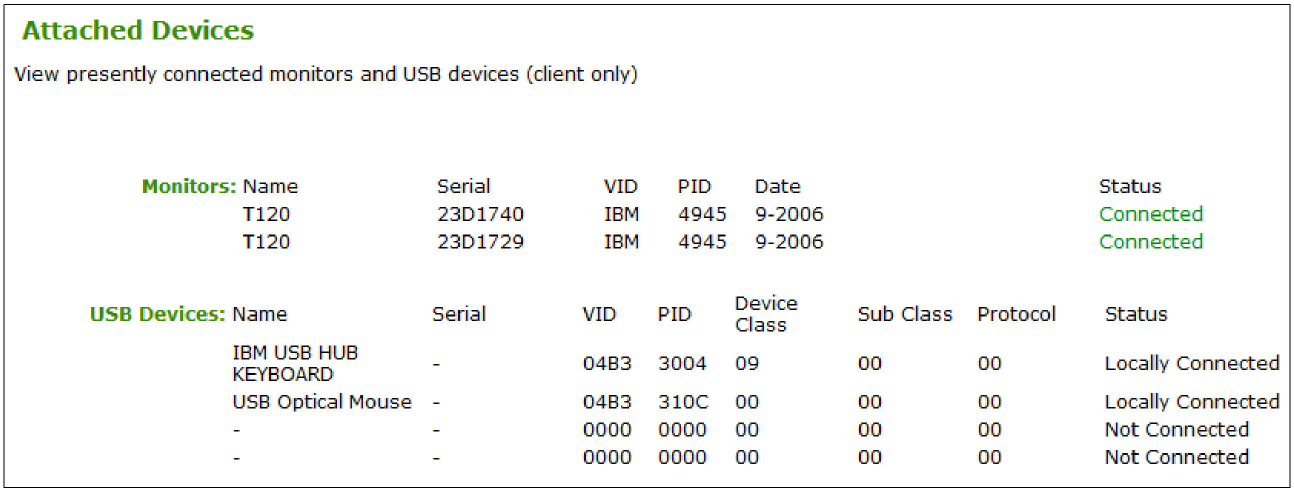
MAC Address:	00-16-41-DF-FB-48
Unique Identifier:	00-16-41-DF-FB-48
Serial Number:	56280000100374P022
Hardware Version:	Devon_IT_Brick_Board_Rev_4.2
Firmware Version:	0.14
Firmware Build ID:	v062
Firmware Build Date:	Aug 3 2007 11:02:44
PCoIP Processor Revision:	0.0
Bootloader Version:	0.0
Bootloader Build ID:	
Bootloader Build Date:	

Figure 6-55 The Version option on the Web interface of the HC10 and the CP20

This option allows you to obtain the MAC address, serial number, and hardware version of the HC10 and CP20. It is also helpful to see which firmware version and build the HC10 or CP20 is currently using. It is extremely important to keep the firmware as the most recent version. There is also information about the PC-over-IP processor and bootloader version that is being used.

Attached Devices option

The Attached Devices option allows you to view the monitors and USB devices that are connected. This option is only available on the CP20's Web interface. See Figure 6-56.



Attached Devices

View presently connected monitors and USB devices (client only)

Monitors:	Name	Serial	VID	PID	Date	Status
	T120	23D1740	IBM	4945	9-2006	Connected
	T120	23D1729	IBM	4945	9-2006	Connected

USB Devices:	Name	Serial	VID	PID	Device Class	Sub Class	Protocol	Status
	IBM USB HUB KEYBOARD	-	04B3	3004	09	00	00	Locally Connected
	USB Optical Mouse	-	04B3	310C	00	00	00	Locally Connected
	-	-	0000	0000	00	00	00	Not Connected
	-	-	0000	0000	00	00	00	Not Connected

Figure 6-56 The Attached Devices option on the Web interface of the CP20

This option shows all the monitors and USB devices that are currently attached to the CP20. This can be very useful to find the VID and PID numbers to use in conjunction with the USB security features (see “USB” on page 130).

6.4.5 Upload menu

In this section, we discuss the options in the Upload menu (Figure 6-57).

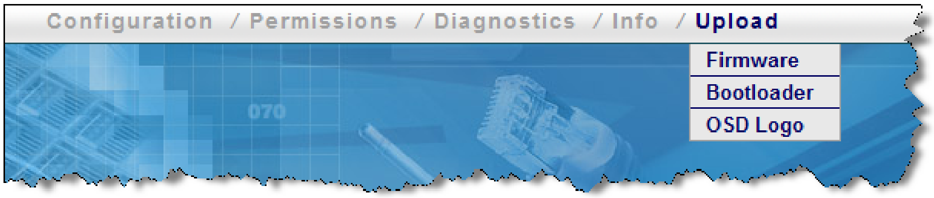
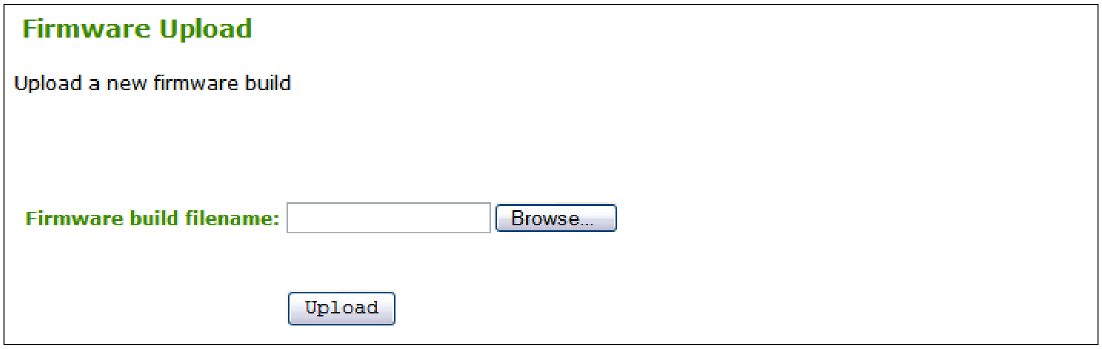


Figure 6-57 The Upload menu on the Web interface of the HC10 and the CP20

Firmware option

The Firmware option allows you to upload new firmware to the CP20 or HC10 (Figure 6-58). Browse for the appropriate file and click **Upload**. For more information about firmware updates see 6.6, “Firmware updates” on page 145.



Firmware Upload

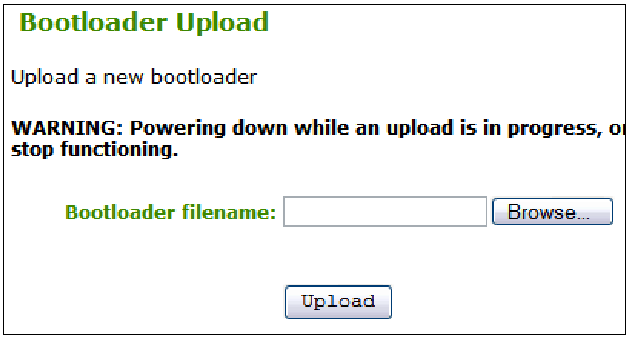
Upload a new firmware build

Firmware build filename:

Figure 6-58 The Firmware option on the Web interface of the HC10 and the CP20

Bootloader option

The Bootloader option allows you to upload a new bootloader file, which is special firmware. Browse for the appropriate file and click **Upload**. See Figure 6-59.



Bootloader Upload

Upload a new bootloader

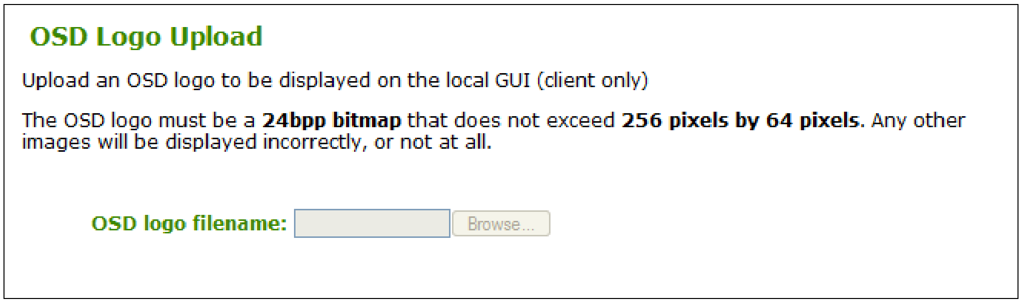
**WARNING: Powering down while an upload is in progress, o
stop functioning.**

Bootloader filename:

Figure 6-59 The Bootloader option on the Web interface of the HC10 and the CP20

OSD Logo option

The OSD Logo option allows you to upload a logo that can be seen on the CP20 local interface (see Figure 6-60).



OSD Logo Upload

Upload an OSD logo to be displayed on the local GUI (client only)

The OSD logo must be a **24bpp bitmap** that does not exceed **256 pixels by 64 pixels**. Any other images will be displayed incorrectly, or not at all.

Figure 6-60 The OSD Logo option of the Web interface of the HC10 and the CP20

The logo displays similar to the IBM logo shown in Figure 6-1 on page 96. The requirements of the picture are:

- No larger that 256 pixels wide by 64 pixels high
- BMP format (uncompressed)
- No greater that 24 bits per pixel

6.5 Setting up a peer-to-peer connection

Users can use peer-to-peer configuration when they want to connect CP20s to HC10s without the use of a connection broker. There are two ways to connect to the HC10 peer to peer:

- Session

  Connect using the host name or IP address and the MAC address of a specific HC10 compression card. For more information about the session method, see 4.7.2, “Peer-to-peer connections” on page 60.

- Discovery

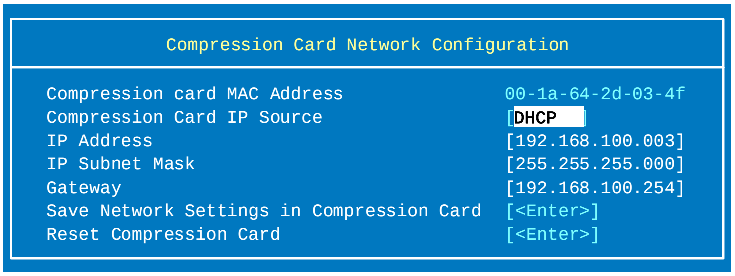
  Search for available HC10s and select one from a list to connect to it. For more information about the Discovery method, see 4.7.2, “Peer-to-peer connections” on page 60.

In most situations, we expect a connection broker software to be used. However, if the number of HC10s implemented is small (for example, a chassis of 14 or less), it is reasonable to use a peer-to-peer connection.

6.5.1 Determining the IP and MAC addresses of the devices

Depending on the connection method that you choose, before you can connect, you might need to know the IP address of the HC10 or CP20. To determine the IP address and MAC address of the HC10 compression card, do the following:

1. Boot the HC10 into BIOS.
2. Select **Advanced Setup** → **Compression Card Network Configuration**.
3. The IP address and MAC address are listed as shown in Figure 6-61.

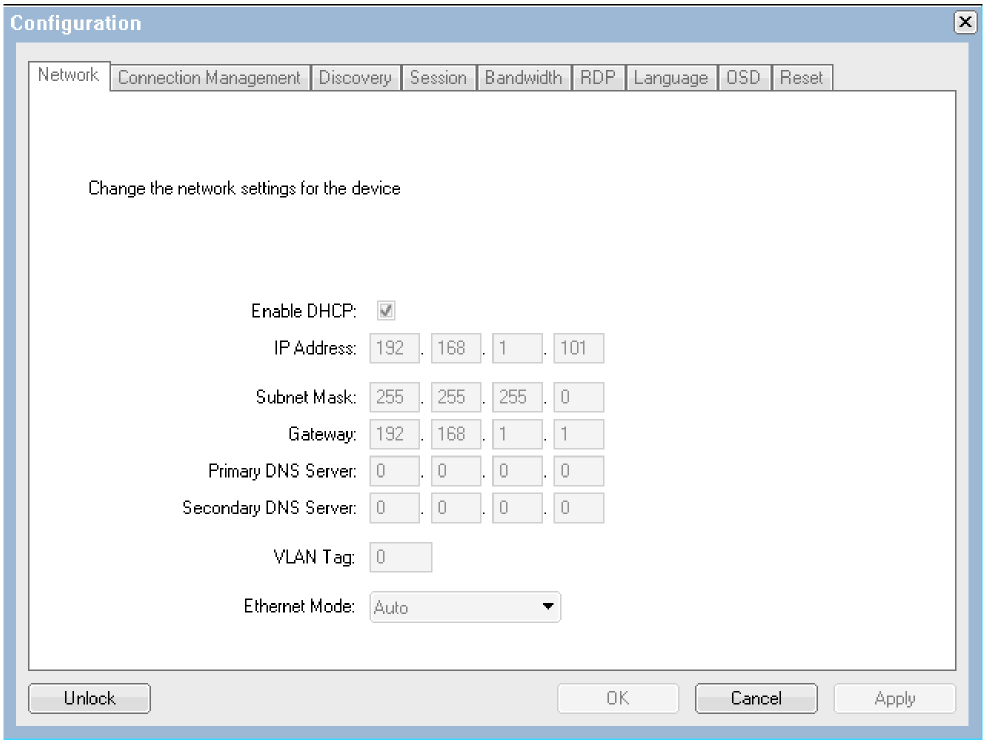


```
                 Compression Card Network Configuration

   Compression card MAC Address                      00-1a-64-2d-03-4f
   Compression Card IP Source                        [DHCP    ]
   IP Address                                        [192.168.100.003]
   IP Subnet Mask                                    [255.255.255.000]
   Gateway                                           [192.168.100.254]
   Save Network Settings in Compression Card         [<Enter>]
   Reset Compression Card                            [<Enter>]
```

Figure 6-61 IP address of the HC10's compression card

To determine the IP address and MAC address of the CP20, do the following

1. Turn on the CP20.
2. At the CP20 connect panel, click **Options** → **Configuration**.
3. The IP address that the CP20 is using (static or DHCP-assigned) is shown in the Network tab, similar to Figure 6-62.



Change the network settings for the device

Enable DHCP: ☑

IP Address: 192 . 168 . 1 . 101

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 1

Primary DNS Server: 0 . 0 . 0 . 0

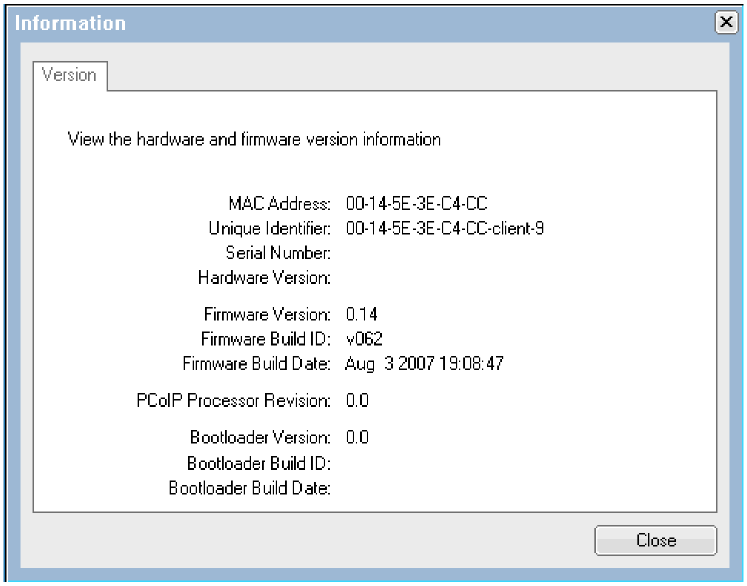
Secondary DNS Server: 0 . 0 . 0 . 0

VLAN Tag: 0

Ethernet Mode: Auto

Figure 6-62 The Network tab showing the CP20 IP address

4. To determine the MAC address of the CP20, click **Cancel** to close the Configuration window. Then, click **Options** → **Information**.
5. The window that opens shows the MAC address, similar to Figure 6-63.



View the hardware and firmware version information

MAC Address: 00-14-5E-3E-C4-CC
Unique Identifier: 00-14-5E-3E-C4-CC-client-9
Serial Number:
Hardware Version:

Firmware Version: 0.14
Firmware Build ID: v062
Firmware Build Date: Aug 3 2007 19:08:47

PCoIP Processor Revision: 0.0

Bootloader Version: 0.0
Bootloader Build ID:
Bootloader Build Date:

Figure 6-63 The Information window showing the CP20 MAC address

6.5.2 Directly connect to a HC10

This section describes how to configure the CP20 and HC10 to enable a direct connection between the two without the use of a connection broker. You need to know the IP address and MAC address of the HC10 compression card and the CP20. Follow the instructions in 6.5.1, “Determining the IP and MAC addresses of the devices” on page 140 to get this information.

To configure the CP20, do the following:

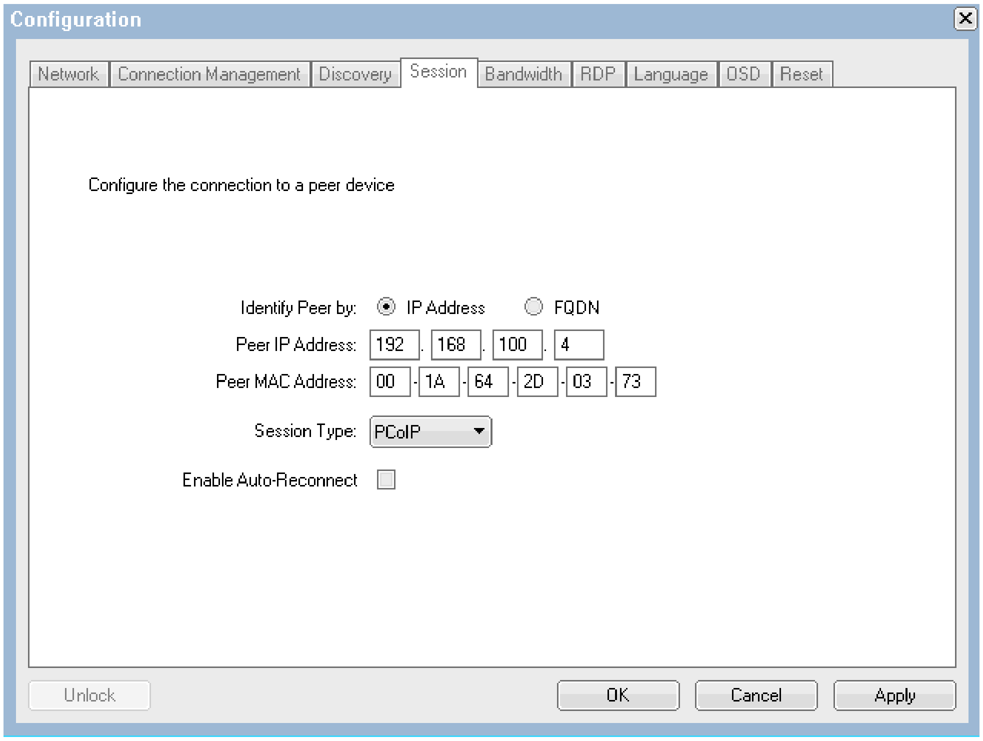
1. Turn on the CP20.
2. At the CP20 connect panel, click **Options** → **Configuration**.
3. Click **Unlock** and enter the password (the default password is PASSW0RD, with a zero not the letter *O*) and click **OK**.
4. In the Connection Management tab, ensure that **Enable Connection Management** is *not* selected.
5. In the Discovery tab, ensure that **Enable Discovery** is *not* selected.

6. Click the Session tab (see Figure 6-64).

   a. If you are going to connect by IP address, select **IP Address** and enter the IP and MAC addresses of the HC10 that were determined earlier.

   b. If you are going to connect by fully-qualified domain name, select **FQDN** and enter the peer FQDN that you have set up.

   c. Leave the default Session Type at **PCoIP**.



Configure the connection to a peer device

Identify Peer by: ● IP Address ○ FQDN

Peer IP Address: 192 . 168 . 100 . 4

Peer MAC Address: 00 - 1A - 64 - 2D - 03 - 73

Session Type: PCoIP

Enable Auto-Reconnect □

Figure 6-64 Session tab of the local interface

7. Click **OK** to save your changes. If you are prompted to restart the client processor, turn off the CP20 using the rocker switch at the back of the unit and turn it back on again.

To configure the HC10 compression card to accept a peer-to-peer connection request, do the following:

1. Open a Web browser. Enter the HC10 compression card's IP address in the browser address field and press Enter.
2. Enter the device's password (the default is PASSW0RD, with a zero not the letter *O*).
3. Click **Configuration** → **Connection Management** and ensure that **Enable Connection Management** is *not* selected. Click **Apply** if you made changes.
4. Click **Configuration** → **Discovery** and ensure that Enable Discovery is *not* select. Click **Apply** if you made changes.
5. Click **Configuration** → **Session**. If you want the HC10 to accept a connection from any CP20, select **Accept Any Peer**. Otherwise, specify the CP20 by IP address and MAC address or by DNS host name. Click **Apply** if you made changes.

Now that the CP20 and HC10 are configured, at the CP20 connect window, click **Connect** to connect to the HC10. If the HC10 is turned off, the blade is turned on automatically.

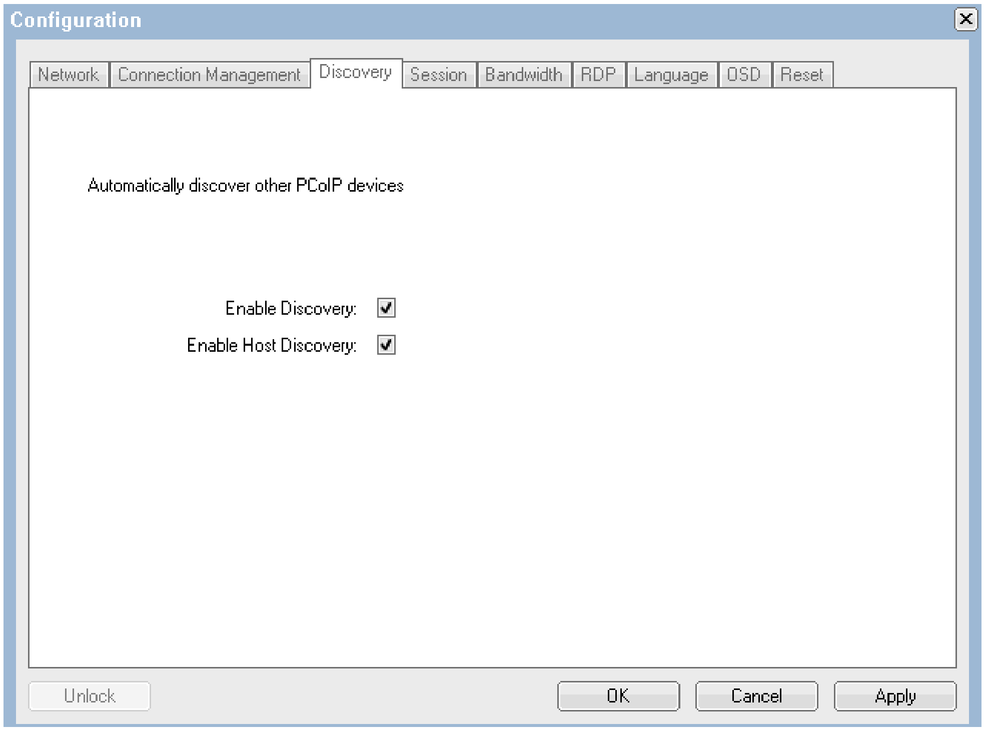
Tip: If you get the error message `Connection Refused!` when you try to connect, then the most likely causes are either that you still have Connection Management enabled on the HC10 or that you have entered the MAC address of either the HC10 (in the CP20 configuration) or the CP20 (in the HC10 configurations) incorrectly. Review the Event Log in the Diagnostics menu for information about why the connection was not established.

6.5.3 Connect to a HC10 with discovery options

With discovery, you do not need to specify any IP addresses, host names, or MAC addresses to connect. Instead, the CP20 sends a broadcast to the subnet to all online HC10s, and a list is presented of available HC10s from which you can choose to connect.

Before you can connect, you need to configure the devices to be in discovery mode. First configure the CP20:

1. Turn on the CP20.
2. At the CP20 connect window, click **Options** → **Configuration**.
3. Click **Unlock** and enter the password (the default password is PASSW0RD, with a zero not the letter *O*) and click **OK**.
4. In the Connection Management tab, ensure that **Enable Connection Management** is *not* selected.
5. In the Discovery tab, select **Enable Discovery** and **Enable Host Discovery** as shown in Figure 6-65.



Automatically discover other PCoIP devices

Enable Discovery: ☑

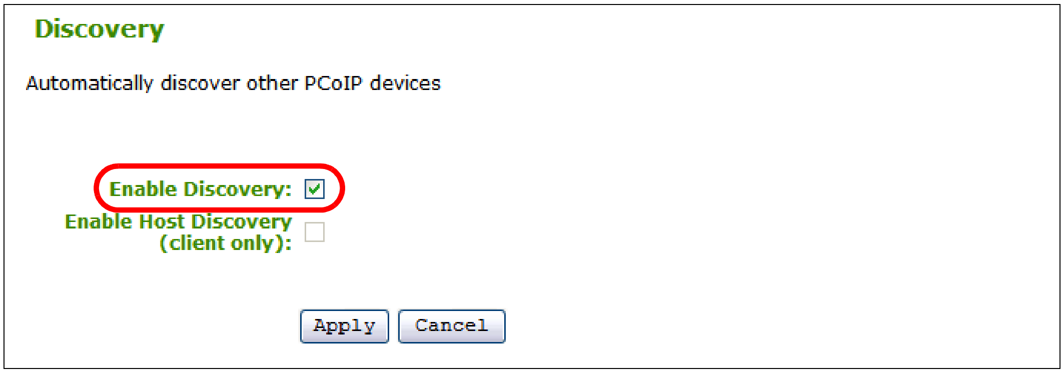
Enable Host Discovery: ☑

Figure 6-65 Discovery configuration in the CP20

6. Click **OK** to save your changes. If you are prompted to restart the client processor, turn off the CP20 using the rocker switch at the back of the unit and turn it back on again.

The next step is to enable discovery on the compression card of each HC10, as follows:

1. Connect a computer to the network to which the compression card and CP20s are connected.
2. If you know the compression card's IP address, continue to the next step. Otherwise follow the instructions in 6.5.1, "Determining the IP and MAC addresses of the devices" on page 140 to get this information.
3. Open a Web browser and enter the HC10 compression card's IP address in the browser address field and press Enter.
4. When prompted, enter the device's password (the default is PASSW0RD, with a zero not the letter *O*).
5. Click **Configuration** → **Discovery**.
6. Select **Enable Discovery**, as shown in Figure 6-66. Then, click **Apply** to save the change.


Discovery

Automatically discover other PCoIP devices

Enable Discovery: ☑

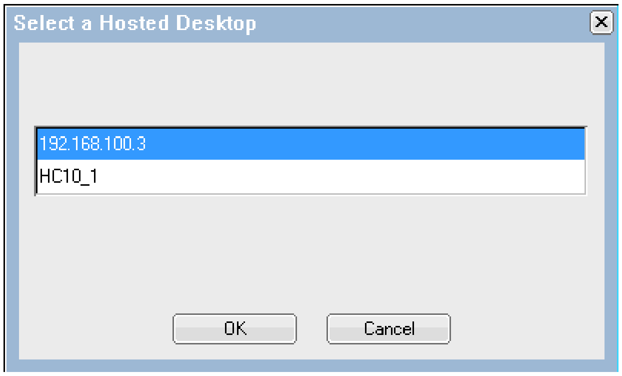
Enable Host Discovery (client only): □

Figure 6-66 The Discovery menu allows you to enable discovery

7. Click **Configuration** → **Connection Management** and ensure that **Enable Connection Management** is *not* selected. Click **Apply** if you made changes.

Now that the CP20s and HC10s are configured for discovery, on the CP20 connect window, click **Connect**. After a short delay, a list of available HC10s displays, similar to Figure 6-67. Select the HC10 to which you want to connect and click **OK**.

Note: Up to ten HC10s can be displayed.


Select a Hosted Desktop

192.168.100.3

HC10_1

Figure 6-67 List of available HC10s to connect to

Tip: If you attempt to connect to an HC10 that is listed in the window shown in Figure 6-67, but you get the error `Connection Refused`, check the settings of that HC10 to ensure that **Enable Connection Management** is not selected.

6.6 Firmware updates

It is important to have the latest firmware applied to the PC-over-IP processors in both the HC10 compression card and the CP20. If you are using Devon IT Connection Broker, we recommend that you use it to deploy firmware. See 5.1.3, “Updating firmware” on page 74 for information about how to do this.

If you are not using the Devon IT Connection Broker, you can update a device manually, as follows:

1. Download the latest firmware from:

   `http://www.ibm.com/support`
2. Decompress the file to a temporary directory. The firmware file that you upload to the device has a .app extension.
3. Connect your computer to the same network as the HC10 compression card and CP20.
4. Turn on the HC10 or CP20 (the device that you want to update).
5. Open a Web browser and enter the IP address of the device that you want to update (that is, either the HC10 compression card or CP20). If you do not know the IP address of the device, follow the instructions in 6.5.1, “Determining the IP and MAC addresses of the devices” on page 140 to get this information.
6. Click **Upload** → **Firmware**.
7. Click **Browse** and browse for the .app firmware file that you downloaded. Select this file and click **OK**.
8. Click **Upload** to upload the firmware. This process can take a few minutes.
9. Repeat steps 5 through 8 for any other devices that you want to update.

There are many ways to verify that the firmware of the HC10 and CP20 are up to date. The following locations state the firmware version:

- The Information menu on the HC10 or CP20 Web interface (see 6.4.4, “Info menu” on page 136).
- The Information menu on the CP20 local interface (see 6.3, “CP20 local interface” on page 100).
- The main panel of the Devon IT Connection Management software (see Figure 5-3 on page 68).

Abbreviations and acronyms

AC	alternating current
AMM	Advanced Management Module
API	application programming interface
ASF	Alert Standard Format
BIOS	basic input output system
BMC	baseboard management controller
BMP	bitmap
BS	Bachelor of Science
BTU	British thermal unit
CA	Certification Authority
CAD	computer aided design
CAE	computer aided engineering
CD	compact disk
CLI	command-line interface
CPU	central processing unit
CRT	Cathode Ray Tube
DDC	Display Data Channel
DHCP	Dynamic Host Configuration Protocol
DIMM	dual inline memory module
DNS	Domain Name System
DVI	Digital Video Interface
EDID	Extended Display Identification Data
ESM	Ethernet switch modules
ESP	Encapsulating Security Payload
FDX	full duplex
FQDN	fully qualified domain name
FTP	File Transfer Protocol
GB	gigabyte
GIS	geographic information systems
GUI	graphical user interface
HD	high definition
HT	Hyper-Threading
HTTP	Hypertext Transfer Protocol
I/O	input/output
IBM	International Business Machines
ID	identifier
IE	Internet Explorer
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGTA	I/O Graphics and Transmission Adapter
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IT	information technology
ITSO	International Technical Support Organization
KVM	keyboard video mouse
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LED	light emitting diode
MAC	media access control
MB	megabyte
NIC	network interface card
OS	operating system
OSD	on no display
PC	personal computer
PCI	Peripheral Component Interconnect
PDU	power distribution unit
PFA	Predictive Failure Analysis®
PID	Product ID
POST	power on self test
PXE	Preboot Execution Environment
RADIUS	Remote Authentication Dial In User Service
RAM	random access memory
RDM	Remote Deployment Manager
RDP	Remote Desktop Protocol
RETAIN	Remote Electronic Technical Assistance Information Network
RMON	Remote Monitoring
RPM	revolutions per minute
SAN	storage area network
SAS	Serial Attached SCSI
SATA	Serial ATA
SDRAM	static dynamic RAM

SFF	Small Form Factor
SLP	Service Location Protocol
SNMP	Simple Network Management Protocol
SOL	Serial over LAN
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control System
TCO	total cost of ownership
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	TCP offload engine
URL	Uniform Resource Locator
USB	universal serial bus
VGA	video graphics array
VID	Vendor ID
VLAN	virtual LAN
VM	virtual machine
VNC	Virtual Network Computing
VPD	vital product data
VRM	voltage regulator module
WCD	Workstation Connection Device
WHQL	Windows Hardware Quality Labs
WOL	wake on LAN

Related publications

We consider the publications that we list in this section particularly suitable for a more detailed discussion of the topics that we cover in this paper.

IBM Redbooks publications

You can search for, view, or download books, papers, Technotes, draft publications, and additional materials, as well as order hardcopy IBM Redbooks publications, at the IBM Redbooks publications Web site:

ibm.com/redbooks

Related IBM Redbooks and Redpaper publications:

- *IBM eServer xSeries and BladeCenter Server Management*, SG24-6495
- *IBM BladeCenter Products and Technology*, SG24-7523

Other publications

These publications are also relevant as further information sources. The can be downloaded as follows:

1. Go to http://ibm.com/support.
2. Select **BladeCenter** from the Choose support type pull-down and click ➔.
3. Under Popular links, click **Publication lookup**.
4. Select **BladeCenter HC10** from the Product family pull-down and click **Continue**.

A direct link is the following:

http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/resourceselect?familyind=5353629&typeind=0&osind=0&continue.x=37&continue.y=13&brandind=5000020&oldfamily=5353629&taskind=2&pubs=Y

Relevant publications are as follows:

- *IBM BladeCenter HC10 Installation and User's Guide*
- *IBM BladeCenter HC10 Problem Determination and Service Guide*
- *IBM CP20 Installation, Use and Troubleshooting Guide*
- *Installing Microsoft Windows Vista on the HC10*

Online resources

These Web sites are also relevant as further information sources.

Product information pages

- BladeCenter HC10 and CP20 product page

  http://www.ibm.com/systems/bladecenter/workstation/

- IBM BladeCenter home

  http://www.ibm.com/bladecenter

- IBM BladeCenter HC10 product announcement

  http://www.ibm.com/isource/cgi-bin/goto?it=usa_annred&on=107-336

- IBM CP20 Workstation Connection Device product announcement

  http://www.ibm.com/isource/cgi-bin/goto?it=usa_annred&on=107-580

- IBM BladeCenter S product announcement

  http://www.ibm.com/isource/cgi-bin/goto?it=usa_annred&on=107-576

- Devon IT Connection Broker

  http://devonit.com/gateway/gateway_bladeworks.php

- Leostream Hosted Desktop Connection Broker

  http://www.leostream.com/productVHDC.html

- IBM BladeCenter Power Configurator

  http://www.ibm.com/systems/bladecenter/powerconfig

- SAS Connectivity Module and Expansion Card product announcement

  http://www.ibm.com/isource/cgi-bin/goto?it=usa_annred&on=107-575

- IBM ServerProven compatibility information for BladeCenter

  http://www.ibm.com/servers/eserver/serverproven/compat/us/eserver.html

Support pages

- IBM Support home

  http://ibm.com/support

- IBM BladeCenter support home

  http://www.ibm.com/systems/bladecenter/support/

- IBM BladeCenter support forum

  http://www.ibm.com/developerworks/forums/dw_forum.jsp?forum=819&cat=53

- RETAIN tip H191783: CRT monitors corrupted or no video

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072597

- RETAIN tip H191730: Blade does not authenticate through a firewall

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072550

- RETAIN tip H192042: IBM CP20 Workstation Connection Device cannot connect to HC10 with server connectivity module

  http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5073011

- RETAIN tip H191818: Bandwidth recommendation

  `http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072671`

- RETAIN tip H191777: No video is displayed on the Workstation Connection Device

  `http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072596`

- RETAIN tip H191763: Black screen until Microsoft Windows is reached on the Workstation Connection Device
- `http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072561`
- RETAIN tip H191821: Cannot exit standby mode with mouse or keyboard

  `http://www.ibm.com/support/docview.wss?uid=psg1MIGR-5072678`

- IBM Director downloads

  `http://www.ibm.com/systems/management/director/downloads.html`

- Windows Audio Device Technologies

  `http://www.microsoft.com/whdc/device/audio`

- Intel High Definition Audio

  `http://www.intel.com/design/chipsets/hdaudio.htm`
  `http://www.intel.com/standards/hdaudio/`

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services