

# Endura™ Network Design Guide



**Endura**

Video Security System

C1640M-B (3/06)



# Contents

---

Welcome to the Endura Network Design Guide .....	5
Audience .....	5
How to Use This Guide .....	5
Endura Overview .....	5
Endura Components .....	6
Endura Product Support .....	6
Network Architecture .....	7
Physical Media .....	7
Network Protocols .....	7
Unicast Routing Protocols .....	7
Multicast Routing Protocols .....	7
Internet Group Management Protocol .....	8
Endura Network Design Considerations .....	8
Understanding the Endura Network Structure .....	9
VLANs .....	9
UPnP .....	9
Endura A Block .....	10
Broadcast Domains and VLANs .....	10
Using TTL to Control Network Traffic in Broadcast Domains .....	11
Endura B Block .....	12
Endura Traffic Summary Details .....	12
Calculating Bandwidth and Storage Requirements .....	13
NTSC Frame Rates .....	14
PAL Frame Rates .....	17
Examples of Worse-Case Bandwidth Calculation in Playback Mode .....	20
Examples of Worse-Case Bandwidth Calculation in Live Video Mode .....	21
Endura Core Block .....	22
Endura C Block .....	23
Examples of Endura Network Designs .....	24
Unmanaged Network Configuration .....	24
Managed Network Configuration .....	25
Connecting the NVR5100 and SEB5000s .....	26
Connecting Multiple NVR5100s and SEB5000s .....	26
Appendix A: Endura Network Configuration Example .....	27
Setting Up Switch A .....	28
Setting Up Switch B .....	29
Example Configuration File for Switch B .....	30
Appendix B: WAN Configuration Example .....	31
Network Configuration Overview .....	31
City A Router (R102) Configuration File .....	32
City B Router (R104) Configuration File .....	33
Verifying the Configuration .....	34
Troubleshooting .....	36
Appendix C: Endura Network Requirements Worksheet .....	37
Index .....	39

## List of Illustrations

---

1	A Block: Encoding, Recording, and Playback	10
2	Using VLANs to Segment the Network into Separate Broadcast Domains for Each Block	10
3	TTL Is Set to 1 in VLAN 2 and Keeps UPnP Traffic Within the A Block	11
4	B Block: Decoding and Viewing Video	12
5	Core Block: Authentication and Security	22
6	Video Traffic Path Through the Core Block	22
7	C Block: Encompasses A, B, and Core Blocks	23
8	Unmanaged Endura Network	24
9	Managed Endura Network	25
10	Using a Patch Cable to Connect the NVR5100 and a Single SEB5000	26
11	Connecting the NVR5100 and Multiple SE5000Bs	26
12	Using VLANs to Connect Multiple NVR5100s and SE5000Bs	26
13	Example Endura Network and HP 5304 Switch Configuration	27
14	Example of a Configuration File	30
15	Sample Endura Network Over a WAN	31

## List of Tables

A	Endura Components	6
B	High Resolution: NTSC Frame Rates with Dual Stream NET5301T Encoder	14
C	Medium Resolution: NTSC Frame Rates with Dual Stream NET5301T Encoder	15
D	Low Resolution: NTSC Frame Rates with Dual Stream NET5301T Encoder	16
E	High Resolution: PAL Frame Rates with Dual Stream NET5301T Encoder	17
F	Medium Resolution: PAL Frame Rates with Dual Stream NET5301T Encoder	18
G	Low Resolution: PAL Frame Rates with Dual Stream NET5301T Encoder	19
H	Endura Network Structures	23

# Welcome to the Endura Network Design Guide

---

Welcome to the Endura™ Network Design Guide. This document is specifically designed as a guide and reference source for designing Endura networks.

This guide is designed to help you with the following:

- Understand the primary building blocks of the Endura network and the role each one plays
- Understand the networking technologies applicable for Endura
- Determine which approach to use for networking and which technologies are best for your security network business requirements

Information in this guide is organized as follows:

- [Network Architecture](#) on page 7
- [Endura Network Design Considerations](#) on page 8
- [Understanding the Endura Network Structure](#) on page 9
- [Appendix A: Endura Network Configuration Example](#) on page 27
- [Appendix B: WAN Configuration Example](#) on page 31
- [Appendix C: Endura Network Requirements Worksheet](#) on page 37

## AUDIENCE

This guide is written for network administrators and engineers who have in-depth networking knowledge and experience.

## HOW TO USE THIS GUIDE

If you are new to Endura, the Endura Network Design Guide serves as a high-level tutorial and network design source. If you are experienced with Endura, this guide serves as a reference source.

- If you are new to Endura, you should read this guide from start to finish to get a good understanding of the Endura system network requirements.
- If you are experienced with Endura, you should always consult this document as a reference source as new information might be available periodically.
- As you read this guide, ensure that you complete the Endura Network Requirements Worksheet. Use this worksheet to validate that your network meets the minimum requirements to support an Endura system. For information on the Endura Network Requirements Worksheet, refer to [Appendix C: Endura Network Requirements Worksheet](#) on page 37.

## ENDURA OVERVIEW

Endura is a high-quality, high-performance network-based video security system, which is based on a powerful distributed system architecture and hardware/software platform for the total utilization of today's Ethernet networks. This noncentralized system allows customers to make use of a facility's network and network infrastructure, representing a significant savings in cabling, hardware, and manpower resources.

No longer limited by traditional, centralized approaches, Endura offers an unconstrained platform for designing and implementing video security systems. There is virtually no end to how a system and its components can interact and share video, audio, and control information.

The Endura hardware platform offers all the components necessary for designing, installing, and utilizing complete networked digital video systems. With encoders, decoders, network video recorders, PC workstations, video console displays, storage expansion boxes, and advanced management technologies, customers now have all the tools necessary for building a high-performance video security system—all delivered over an Ethernet network with total access flexibility.

## ENDURA COMPONENTS

Endura components take full advantage of leading edge technologies such as Universal Plug and Play (UPnP™), allowing for fast, error-proof installations and set up. Essentially, when an Endura device is added to a system, it announces itself and the services it has available. The existing devices acknowledge the new unit and then begin exchanging information as user preferences and profiles dictate.

Table A lists the Endura components. Information in this table is updated periodically and might not describe the latest Endura products.

**Table A.** Endura Components

Endura Component	Description
NET5301T encoder	The NET5301T encoder is a high-performance MPEG4 video encoder. It accepts analog video and audio signals and converts them into digital TCP/IP packets, as well as provides an interface for relays and alarms.
NET5301R decoder	The NET5301R is a high-performance video decoder. It converts digital video and audio streams back into video output for viewing on a composite, S-Video, or VGA monitor.
WS5050 workstation	The WS5050 Endura workstation (WS) is a Windows®-compatible system that is used for viewing video and configuring an Endura system. The WS5050 is supplied with all PC hardware in a stand-alone box.
VCD5000 video console display	The VCD5000 video console display (VCD) is a high-performance, multiple-stream decoding unit. It converts multiple digital MPEG4 streams into video signals to be viewed on either composite, S-Video, or VGA monitors. Up to four decoding cards can be added to this unit. Four models are available that allow users to tailor their viewing systems with up to 64 displays. An unlimited number of video console displays (VCDs) and decoders can be controlled from a single VCD. Using an Endura keyboard or a standard USB-compatible PC mouse and keyboard, users can access the on-screen menus and control an Endura system.
SM5000 system manager	The SM5000 system manager (SM) is an integrated hardware/software component that provides distributed administration of multiple devices. The SM5000 also manages system security, functioning as a key server for user and device authentication.
NVR5100 Series network video recorder	<p>The NVR5100 Series network video recorder (NVR) represents a whole new generation of flexibility and integration for network-based video system recording. It sits at the center of Endura, Pelco's most advanced integrated video security system. The NVR represents the state of the art in scalability, features, and reliability.</p> <p>The NVR5100 is capable of continuous, scheduled, alarm/event, and motion recording. Pre- and post-alarm, event, and motion recording is also available and is fully programmable on a per-channel basis. The unit maximizes storage efficiency using EnduraStor™, a time- and priority-based system that identifies data to be removed when storage reaches capacity.</p>
SEB5000 storage expansion box	The SEB5000 storage expansion box (SEB) is a high-performance storage solution. Each SEB box can add up to 3.9 TB of network storage. Multiple SEBs can be attached to a single NVR unit, providing a very large, very scalable network storage solution.
EnduraStor storage optimization	EnduraStor offers the ability to reduce the frame rate of previously recorded video on an Endura system after a specified period of time. After captured video has reached a user-defined age, EnduraStor goes to work to "prune" the database and reduce the number of recorded frames. By enabling EnduraStor within the system, a user has the unique ability to dramatically extend recording duration at a lower frame rate.

## ENDURA PRODUCT SUPPORT

Pelco provides 24-hour, seven-day-a-week product support designed to assist any customer with a technical problem involving Pelco equipment; just dial (800) 289-9100 or (559) 292-1981 and ask for technical assistance.

# Network Architecture

---

The Endura network topology is based on using current networking technology. Pelco suggests that you recommend or select networking devices and technologies that meet or exceed the features and functionality described in this section.

## PHYSICAL MEDIA

Physical media used in the Endura network is as follows:

- 100baseT minimum.
- 1000baseT (gigabit) is recommended. One gigabit uplinks are required for some components.
- CAT5e cabling (minimum).
- CAT6 is recommended for gigabit links.

## NETWORK PROTOCOLS

This section provides a summary of the networking protocols that are required to implement an Endura network and describes the features/functionality that the protocols must exhibit.

### UNICAST ROUTING PROTOCOLS

Basic unicast connectivity is required to implement an Endura network. At least one of the protocols listed below can be used to meet this requirement:

- **Routing Information Protocol (RIP):** RIP is a simple routing protocol that is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers and is known to waste bandwidth. It also has a limit of 15 hops. If a route is advertised as having 16 hops, it is flagged as unreachable.
- **Open Shortest Path First (OSPF):** OSPF is a routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router-to-router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.
- **Static routing:** This protocol forwards data in a network via a fixed path. Static routing cannot adjust to changing line conditions as can dynamic routing.

### MULTICAST ROUTING PROTOCOLS

Multicast routing is required to allow Endura components to communicate with one another. At least one of the protocols listed below can be used to meet this requirement:

- **Protocol Independent Multicast (PIM):** PIM is a multicast routing protocol that is used in conjunction with an existing unicast routing protocol. PIM comes in two versions: Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).
  - Dense mode is most useful in the following instances:
    - Senders and receivers are in close proximity to one another.
    - There are a few senders and many receivers.
    - The multicast traffic volume is high. Dense mode forwards multicast data everywhere, and lets switches prune out traffic that is not requested.
    - Multicast data is periodically flooded everywhere.
    - The multicast traffic stream is constant.

PIM-DM uses Reverse Path Forwarding and looks a lot like Distance Vector Multicast Routing Protocol (DVMRP). The most significant difference between DVMRP and PIM-DM is that PIM-DM works with whatever unicast protocol is being used. Also, PIM-DM does not require any particular unicast routing protocol.

- Sparse Mode is most useful in the following instances:
  - There are few receivers in a group. Switches send multicast traffic only to the devices that request it.
  - Senders and receivers are separated by Local Area Network (LAN) links.
  - The type of traffic is intermittent.

PIM-SM is optimized for environments where there are many multipoint data streams. Each data stream is sent to a relatively small number of the LANs in the internetwork. For these types of groups, Reverse Path Forwarding techniques waste bandwidth. PIM-SM works by defining a rendezvous point. When a sender wants to send data, it first sends to the rendezvous point. When a receiver wants to receive data, it registers with the rendezvous point. Once the data stream begins to flow from sender to rendezvous point to receiver, the routers in the path will optimize the path automatically to remove any unnecessary hops. PIM-SM assumes that no hosts want the multicast traffic unless they specifically ask for it.

PIM is able to simultaneously support dense mode for some multipoint groups and sparse mode for others.

- **DVMRP:** DVMRP is a routing protocol that supports multicast. Stemming from RIP and used in the Internet's Mbone (multicast backbone), DVMRP allows for tunneling multicast messages within unicast packets. It also supports rate limiting and distribution control based on destination address and is responsible for the following:
  - Routes multicast datagrams
  - Periodically floods multicast traffic (similar to PIM-DM)
  - Allows use of non-multicast aware edge devices

## INTERNET GROUP MANAGEMENT PROTOCOL

Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of multicast groups. IGMP is a required protocol in the Endura network and is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

The specification that defines how to handle “unknown” multicast groups is not definitive. In this case, some vendors block multicast streams that have no members, while other vendors will flood this same traffic. Flooding multicast streams that have no members can present a problem in the Endura network because each video stream can be approximately 2 Mbps. In even a relatively small network, flooding Endura traffic can significantly reduce network performance and the overall performance of the Endura system.

## Endura Network Design Considerations

The Endura network is based on switching and routing technologies. When planning an Endura network, you need to know and understand the difference between the traditional “Core” and “Intelligent Edge” network topology design approach.

- Traditional network design approach
 

The traditional network design topology is based on a central network core, which is responsible for all routing decisions. This approach requires the use of high-performance and high-cost core network equipment. This approach will work if the specified core switch is capable of managing all of the following:

  - Making all of the unicast routing decisions
  - Making all of the multicast routing decisions
  - Handling all Endura network traffic: video, audio, PTZ, and UPnP
  - Handling all other existing network traffic

This approach may meet your network design requirements. However this approach might not be as scalable as the intelligent edge design, because the volume of network traffic can easily consume the capacity of the core switch.

If network expansion is a future goal, then the intelligent edge design offers a scalable networking solution.
- Intelligent edge design approach
 

The alternative to the traditional design is the intelligent edge design. This design is based on placing smart switches at the network edge, which reduces the need for a centralized core to make all routing decisions. Instead of a single core switch managing all of the routing and network traffic decisions, in the intelligent edge design, processing is distributed across all managed switches. The intelligent edge design allows the network to scale because managed switches can be easily added to the network without burdening a single core switch. As compared to the traditional design, the intelligent edge design does not use the concept of a “core switch.”



# Understanding the Endura Network Structure

---

The primary structure of an Endura network topology is organized into functional entities, which are called “blocks.” Grouping the functional entities into individual blocks provide the following benefits:

- Blocks control and isolate traffic.
- Block design can be physical or logical.
- Each block is separated by VLANs.
- Blocks help determine network requirements.

The block concept makes it easy to understand and implement the Endura network design.

- **A Block:** The A Block is functionally responsible for encoding, recording, and storage of the video streams entering the Endura network (both live and playback video).
- **B Block:** The B Block is functionally responsible for decoding and displaying the video streams, as well as providing the control and configuration of all Endura components.
- **Core Block:** The Core Block is functionally responsible for Network layer 3 tasks, authentication and security, and interconnects the A and B blocks.
- **C Block:** The C Block includes the entire block structure: A, B, and Core.

## VLANs

VLANs are an essential network topology requirement in the Endura network.

- Each Endura block is separated by VLANs.
- VLANs are groupings of switch ports creating different network segments for each group.
  - Switches using VLANs create the same division of the network into separate broadcast domains are also a more cost-effective solution.
  - It is necessary to use a router when moving between VLANs.
- VLANs reduce the size of the broadcast domain.
- VLANs are used to managed and restrict Endura traffic.
- VLANs operate at layer 2 of the Open System Interconnection (OSI) model.
- All VLANs should be assigned an IP address to support routing.

## UPnP

Endura uses UPnP to enable easy and dynamic connectivity between devices on a network. Devices may dynamically add themselves to a network without the need for user intervention or configuration. UPnP also allows devices on the network to check in with each other periodically. This means the user can know which devices are available at any one time. If a device goes off line, users can be notified so the problem may be addressed quickly, with minimal down time.

UPnP traffic stays isolated to VLANs because of Time-To-Live (TTL) settings. TTL determines how many network segments a packet can cross into before it is discarded. TTL for UPnP packets is set to 1 so that the UPnP packets do not cross out of their originating block. TTL for video packets is set much higher so that the video packets can traverse the entire network. For more information on TTL is used in the Endura network, refer to [Using TTL to Control Network Traffic in Broadcast Domains](#) on page 11.

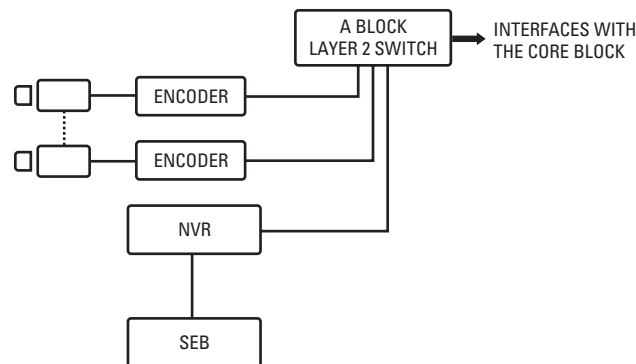
## ENDURA A BLOCK

The A Block is the most important design entity of the network. The A Block is functionally responsible for encoding, recording, and storage of the video streams entering the Endura network (both live and playback video).

The A Block is summarized as follows:

- Each A Block can support up to 48 Encoders and one NVR5100.
- Each A Block is assigned to a specific VLAN.
- The number of A Blocks is unlimited.
- Each A Block has only one NVR5100 for recording of video streams from all Encoders in the A Block. Additional storage is provided by SEB5000 storage expansion boxes.

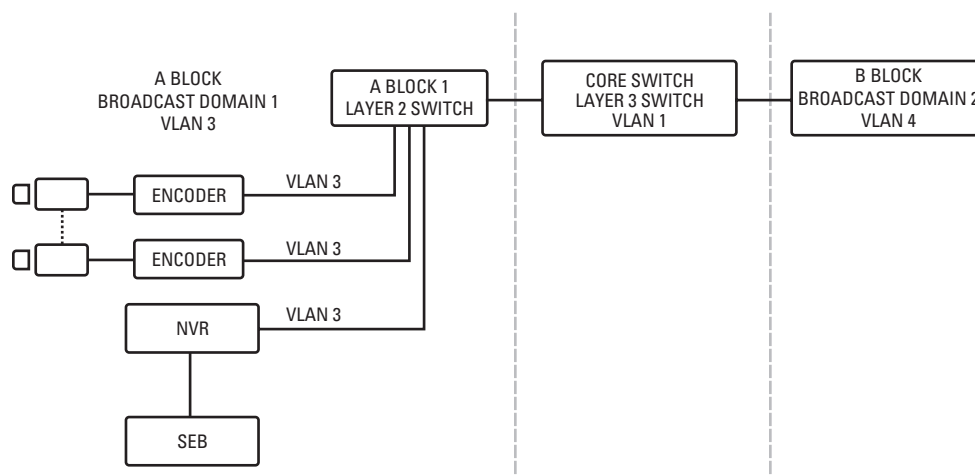
Figure 1 shows the Endura components that comprise the A Block. The SEB5000 is shown directly connected to the NVR5100 using a patch cable. If multiple SEB5000s are required, you can use a dedicated, Pelco-approved gigabit Ethernet switch to expand the video storage of the NVR5100. For more information about connecting SEB5000s to the NVR5100, refer to [Connecting the NVR5100 and SEB5000s](#) on page 26 and [Connecting Multiple NVR5100s and SEB5000s](#) on page 26.



**Figure 1.** A Block: Encoding, Recording, and Playback

## BROADCAST DOMAINS AND VLANS

In a network, the logical area within which all devices can see each other's broadcasts is referred to as a broadcast domain. Endura components generate multicast traffic, which in some cases can be treated like broadcast traffic, depending on the switch. For this reason, it is important to isolate these broadcasts and to create a separate broadcast domain for each Endura block on the network. The most efficient approach is to use VLANs to separate the broadcast domains (refer to Figure 2).



**Figure 2.** Using VLANs to Segment the Network into Separate Broadcast Domains for Each Block

## USING TTL TO CONTROL NETWORK TRAFFIC IN BROADCAST DOMAINS

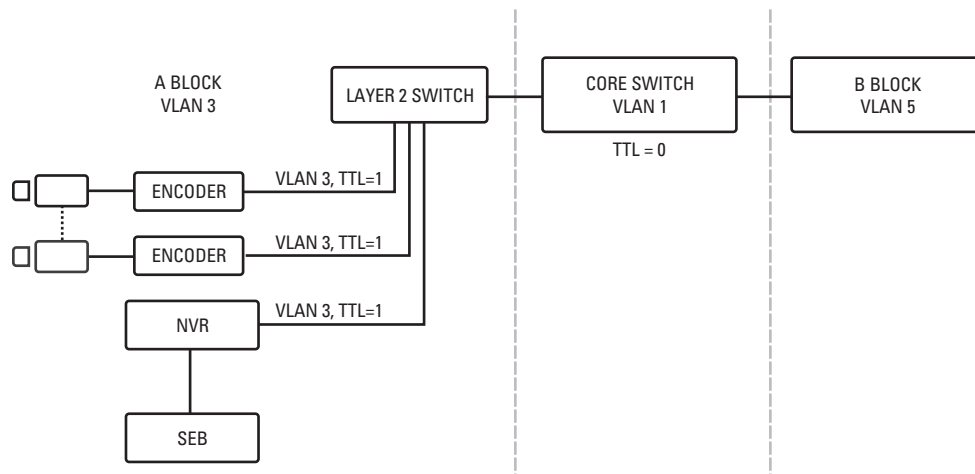
In the Endura network, TTL is used to set the maximum amount of router hops that a packet is allowed to propagate through the network before the packet is discarded. Using TTL provides an effective method to determine how many broadcast domains a given packet can traverse.

- For Endura components (excluding the SM5000), the default TTL settings are as follows:
  - **UPnP traffic:** The TTL is set to 1. In this case, each block is assigned to a specific VLAN, keeping UPnP traffic isolated within that block (refer to Figure 3).
  - **Video packets:** The TTL is set to 3 so that the video packets can traverse the entire network.
- For the SM5000 in the Core Block, the default TTL setting is 4. In this case, the SM5000 Locator broadcasts can traverse across subnetworks to discover Endura components.

This approach ensures that two networking functions be efficiently accomplished:

- Each NVR5100 only records video streams from encoders from which it sees in its block. The NVR5100 sends a query with a TTL of 1, which means it will only discover devices on its VLAN.
- Unnecessary traffic is eliminated from traversing across the Core Block.

Figure 3 illustrates how the broadcast traffic is localized to A Block 1 in broadcast domain 1. In this case, the broadcast traffic from VLAN 1 never traverses the network because TTL is decremented to 0 at the core switch and the packet is dropped.



**Figure 3.** TTL Is Set to 1 in VLAN 2 and Keeps UPnP Traffic Within the A Block

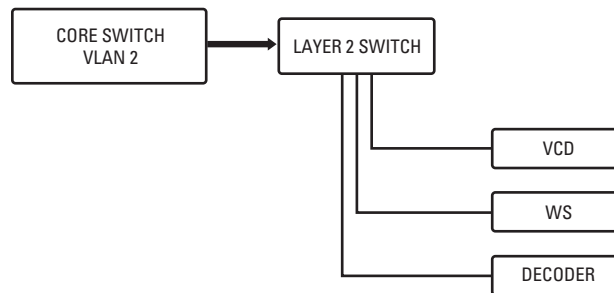
## ENDURA B BLOCK

The Endura B Block generally determines the bandwidth requirements for the network. The B Block is functionally responsible for decoding and displaying the video streams, as well as providing the control and configuration of all Endura components.

The B Block functionality is summarized as follows:

- Based on permissions, can view and control any camera on entire system
- Each B Block is assigned to a specific VLAN
- The B Block can be replicated any number of times (limited only by network capacity)
- Contains all viewing devices
  - NET5301R decoders
  - VCD5000 video console displays
  - WS5050 Endura Workstations (WS)

Figure 4 illustrates the B Block.



**Figure 4.** B Block: Decoding and Viewing Video

## ENDURA TRAFFIC SUMMARY DETAILS

This section provides information that allows you to calculate the bandwidth requirements for the Endura network. The Endura traffic details are summarized as follows:

- Maximum video stream from an NET5301T encoder is 5.0 Mbps plus overhead:
  - Up to 3.0 Mbps total for both multicast live streams
    - Up to 2 Mbps for stream 1 (4CIF)
    - Up to 1 Mbps for stream 2 (CIF)
  - Up to 2.0 Mbps for unicast recording stream

For information on calculating the bandwidth, refer to [Calculating Bandwidth and Storage Requirements](#) on page 13.

- 5.5 Mbps total with audio and data.
- Network utilization should always be figured for the worst-case scenario. For information on calculating the worse-case bandwidth, refer to [Calculating Bandwidth and Storage Requirements](#) on page 13.
- Playback is not a stream, but a “burst” of data.
- Each NVR5100 has a 100 Mbps cap on playback data:
  - The NVR5100 will use as much of 100 Mbps bandwidth as necessary to transmit the requested clip data.
  - The NVR5100 will divide that 100 Mbps up among multiple playback requests if necessary.
- NVR5100 playback is unicast.
- Constant and frequent requests for playback video must be included when determining worse-case bandwidth.

### NOTES:

- Live video traffic is only steamed across the network when requested by a view station.
- Throughput needs to be calculated at various points on the network, depending on how many cameras are going to be viewed and at what size.

## CALCULATING BANDWIDTH AND STORAGE REQUIREMENTS

You must ensure that the B and C blocks are able to handle the worse-case bandwidth ( $B_{WC}$ ) requirements. The following examples describe how to calculate the worse-case bandwidth based on the playback video stream.

**NOTE:** Playback streams are used for calculating worse-case bandwidth requirements because each video stream is played back at the same rate that it was recorded, no matter in what layout mode the video stream is being displayed.

In contrast, when viewing live video, the Endura WS5050, VCD5000, and NET5301R use EnduraView to select the appropriate video stream automatically based on the layout mode.

- **WS5050:** The WS5050 pulls the highest value stream in either the single camera or quad layout mode.
- **VCD5000:** The VCD5000 pulls the lowest stream in quad layout mode.
- **WS5050 or VCD5000:** The WS5050 or VCD5000 pulls the lowest value stream in the 9- or 16-camera layout mode.
- **NET5301R Encoder:**
  - The NET5301R pulls the highest value stream in the single layout mode.
  - The NET5301R pulls the lowest value stream in the quad layout mode.

The following examples demonstrate that the playback video mode requires more bandwidth than does the live video mode. Typical applications do not require displaying the maximum amount of simultaneous playback streams. A more realistic application might require more live video streams are displayed than playback video streams. For this reason both playback and live video calculations are shown to aid in calculating bandwidth.

To ensure that your network resources are more than adequate to support the Endura system, it is recommended that you use the bit rate applicable for the playback video mode when calculating worse-case bandwidth requirements.

- For information on calculating bandwidth for the playback video mode, refer to [Examples of Worse-Case Bandwidth Calculation in Playback Mode](#) on page 20.
- For information on calculating bandwidth for the live video mode, refer to [Examples of Worse-Case Bandwidth Calculation in Live Video Mode](#) on page 21.

The worse-case bandwidth,  $B_{WC}$ , requirements for live and playback video is given by the equation:

$$B_{WC} = B_W + O_H$$

where:

$B_W$  = Bandwidth and is given by the equation:  $B_W = N_S \times B_R$ .

$O_H$  = Overhead and is given by the equation  $O_H = 25\% \times B_W$ .

$N_S$  = Number of streams.

$B_R$  = Bit rate

The above equations are general and assume that all playback streams are of the same quality. For information about  $B_R$  values, refer to [NTSC Frame Rates](#) on page 14 and [PAL Frame Rates](#) on page 17.

## NTSC Frame Rates

This section describes the National Television System Committee (NTSC) frame rates at high, medium, and low resolution with a dual stream NET5301T encoder. You can select 6, 10, 15, and 30 IPS across all resolutions (CIF, 2CIF, and 4CIF) for each camera.

Table B describes the expected performance at high resolution for NTSC frame rates.

**Table B.** High Resolution: NTSC Frame Rates with Dual Stream NET5301T Encoder





Description		High Resolution and Supported Frame Rates			
Layout Mode	Stream/Device	1	2	3	4
	Stream 1	4CIF/30 IPS	4CIF/15 IPS	4CIF/10 IPS	4CIF/6 IPS
	Bitrates	2.0 Mbps	1.5 Mbps	1.0 Mbps	800 Kbps
	Stream 1-I	4CIF/2 IPS	4CIF/2.5 IPS	4CIF/2 IPS	4CIF/2 IPS
	Stream 2	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS
	Bitrates	1.0 Mbps	1.0 Mbps	1.0 Mbps	1.0 Mbps
	Stream 2-I	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS
	WS5050	4CIF/30 IPS	4CIF/15 IPS	4CIF/10 IPS	4CIF/6 IPS
	VCD5000	4CIF/30 IPS	4CIF/15 IPS	4CIF/10 IPS	4CIF/6 IPS
	NET5301R	4CIF/30 IPS	4CIF/15 IPS	4CIF/10 IPS	4CIF/6 IPS
	WS5050	4CIF/30 IPS	4CIF/15 IPS	4CIF/10 IPS	4CIF/6 IPS
	VCD5000	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS
	NET5301R	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS
	WS5050	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS
	VCD5000	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS
	WS5050	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS	CIF/15 IPS
	VCD5000	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS

Table C describes the expected performance at medium resolution for NTSC frame rates.

**Table C.** Medium Resolution: NTSC Frame Rates with Dual Stream NET5301T Encoder









Description		Medium Resolution and Supported Frame Rates			
Layout Mode	Stream/Device	1	2	3	4
	Stream 1 Bitrates Stream 1-I	2CIF/30 IPS 1.5 Mbps 2CIF/2 IPS	2CIF/15 IPS 1.0 Mbps 2CIF/2.5 IPS	2CIF/10 IPS 800 Kbps 2CIF/2 IPS	2CIF/6 IPS 500 Kbps 2CIF/2 IPS
	Stream 2 Birates Stream 2-I	CIF/15 IPS 800 Kbps CIF/2.5 IPS	CIF/15 IPS 800 Kbps CIF/2.5 IPS	CIF/15 IPS 800 Kbps CIF/2.5 IPS	CIF/15 IPS 800 Kbps CIF/2.5 IPS
	WS5050 VCD5000 NET5301R	2CIF/30 IPS 2CIF/30 IPS 2CIF/30 IPS	2CIF/15 IPS 2CIF/15 IPS 2CIF/15 IPS	2CIF/10 IPS 2CIF/10 IPS 2CIF/10 IPS	2CIF/6 IPS 2CIF/6 IPS 2CIF/6 IPS
	WS5050 VCD5000 NET5301R	2CIF/30 IPS CIF/15 IPS CIF/15 IPS	2CIF/15 IPS CIF/15 IPS CIF/15 IPS	2CIF/10 IPS CIF/15 IPS CIF/15 IPS	2CIF/6 IPS CIF/15 IPS CIF/15 IPS
	WS5050 VCD5000	CIF/15 IPS CIF/15 IPS	CIF/15 IPS CIF/15 IPS	CIF/15 IPS CIF/15 IPS	CIF/15 IPS CIF/15 IPS
	WS5050 VCD5000	CIF/15 IPS CIF/2.5 IPS	CIF/15 IPS CIF/2.5 IPS	CIF/15 IPS CIF/2.5 IPS	CIF/15 IPS CIF/2.5 IPS

Table D describes the expected performance at low resolution for NTSC frame rates.

**Table D.** Low Resolution: NTSC Frame Rates with Dual Stream NET5301T Encoder

Description		Low Resolution and Supported Frame Rates			
Layout Mode	Stream/Device	1	2	3	4
	Stream 1 Bitrates Stream 1-I	CIF/30 IPS 1.2 Mbps CIF/2 IPS	CIF/15 IPS 800 Kbps CIF/2.5 IPS	CIF/10 IPS 450 Kbps CIF/2 IPS	CIF/6 IPS 350 Kbps CIF/2 IPS
	Stream 2 Birates Stream 2-I	CIF/15 IPS 800 Kbps CIF/2.5 IPS	CIF/15 IPS 800 Kbps CIF/2.5 IPS	CIF/15 IPS 800 Kbps CIF/2.5 IPS	CIF/15 IPS 800 Kbps CIF/2.5PS
	WS5050 VCD5000 NET5301R	CIF/30 IPS CIF/30 IPS CIF/30 IPS	CIF/15 IPS CIF/15 IPS CIF/15 IPS	CIF/10 IPS CIF/10 IPS CIF/10 IPS	CIF/6 IPS CIF/6 IPS CIF/6 IPS
	WS5050 VCD5000 NET5301R	CIF/30 IPS CIF/15 IPS CIF/15 IPS	CIF/15 IPS CIF/15 IPS CIF/15 IPS	CIF/15 IPS CIF/15 IPS CIF/15 IPS	CIF/15 IPS CIF/15 IPS CIF/15 IPS
	WS5050 VCD5000	CIF/15 IPS CIF/15 IPS	CIF/15 IPS CIF/15 IPS	CIF/15 IPS CIF/15 IPS	CIF/15 IPS CIF/15 IPS
	WS5050 VCD5000	CIF/15 IPS CIF/2.5 IPS	CIF/15 IPS CIF/2.5 IPS	CIF/15 IPS CIF/2.5 IPS	CIF/15 IPS CIF/2.5 IPS



## PAL Frame Rates

This section describes the Phase Alternating Line (PAL) frame rates at high, medium, and low resolution with a dual stream NET5301T encoder. You can select 5, 8.3, 12.5, and 25 IPS across all resolutions (CIF, 2CIF, and 4CIF) for each camera.

Table E describes the expected performance at high resolution for PAL frame rates.

**Table E.** High Resolution: PAL Frame Rates with Dual Stream NET5301T Encoder





Description		High Resolution and Supported Frame Rates			
Layout Mode	Stream/Device	1	2	3	4
	Stream 1	4CIF/25 IPS	4CIF/12.5 IPS	4CIF/8.3 IPS	4CIF/5 IPS
	Bitrates	2.0 Mbps	1.5 Mbps	1.0 Mbps	800 Kbps
	Stream 1-I	4CIF/2 IPS	4CIF/2.5 IPS	4CIF/2 IPS	4CIF/2 IPS
	Stream 2	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	Bitrates	1.0 Mbps	1.0 Mbps	1.0 Mbps	1.0 Mbps
	Stream 2-I	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS
	WS5050	4CIF/25 IPS	4CIF/12.5 IPS	4CIF/8.3 IPS	4CIF/5 IPS
	VCD5000	4CIF/25 IPS	4CIF/12.5 IPS	4CIF/8.3 IPS	4CIF/5 IPS
	NET5301R	4CIF/25 IPS	4CIF/12.5 IPS	4CIF/8.3 IPS	4CIF/5 IPS
	WS5050	4CIF/25 IPS	4CIF/12.5 IPS	4CIF/8.3 IPS	4CIF/5 IPS
	VCD5000	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	NET5301R	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	WS5050	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	VCD5000	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	WS5050	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	VCD5000	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS

Table F describes the expected performance at medium resolution for PAL frame rates.

**Table F. Medium Resolution: PAL Frame Rates with Dual Stream NET5301T Encoder**









Description		Medium Resolution and Supported Frame Rates			
Layout Mode	Stream/Device	1	2	3	4
	Stream 1	2CIF/25 IPS	2CIF/12.5 IPS	2CIF/8.3 IPS	2CIF/5 IPS
	Bitrates	1.5 Mbps	1.0 Mbps	800 Kbps	500 Kbps
	Stream 1-I	2CIF/2 IPS	2CIF/2.5 IPS	2CIF/2 IPS	2CIF/2 IPS
	Stream 2	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	Bitrates	800 Kbps	800 Kbps	800 Kbps	800 Kbps
	Stream 2-I	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS
	WS5050	2CIF/25 IPS	2CIF/12.5 IPS	2CIF/8.3 IPS	2CIF/5 IPS
	VCD5000	2CIF/25 IPS	2CIF/12.5 IPS	2CIF/8.3 IPS	2CIF/5 IPS
	NET5301R	2CIF/25 IPS	2CIF/12.5 IPS	2CIF/8.3 IPS	2CIF/5 IPS
	WS5050	2CIF/25 IPS	2CIF/12.5 IPS	2CIF/8.3 IPS	2CIF/5 IPS
	VCD5000	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	NET5301R	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	WS5050	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	VCD5000	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	WS5050	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	VCD5000	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS

Table G describes the expected performance at low resolution for PAL frame rates.

**Table G.** Low Resolution: PAL Frame Rates with Dual Stream NET5301T Encoder

Description		Low Resolution and Supported Frame Rates			
Layout Mode	Stream/Device	1	2	3	4
	Stream 1	CIF/25 IPS	CIF/12.5 IPS	CIF/8.3 IPS	CIF/5 IPS
	Bitrates	1.2 Mbps	800 Kbps	450 Kbps	350 Kbps
	Stream 1-I	CIF/2 IPS	CIF/2.5 IPS	CIF/2 IPS	CIF/2 IPS
	Stream 2	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	Bitrates	800 Kbps	800 Kbps	800 Kbps	800 Kbps
	Stream 2-I	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5 IPS	CIF/2.5IPS
	WS5050	CIF/25 IPS	CIF/12.5 IPS	CIF/8.3 IPS	CIF/5 IPS
	VCD5000	CIF/25 IPS	CIF/12.5 IPS	CIF/8.3 IPS	CIF/5 IPS
	NET5301R	CIF/25 IPS	CIF/12.5 IPS	CIF/8.3 IPS	CIF/5 IPS
	WS5050	CIF/25 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	VCD5000	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	NET5301R	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	WS5050	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	VCD5000	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	WS5050	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS	CIF/12.5 IPS
	VCD5000	CIF/2.5PS	CIF/2.5PS	CIF/2.5PS	CIF/2.5PS

## Examples of Worse-Case Bandwidth Calculation in Playback Mode

**NOTE:** For the examples below, assume that all recorded video is at 4CIF (2 Mbps) at 30 IPS:

- In this case, if playback video is displayed in the single layout mode, then the display rate is at 30 IPS.
- However, if playback video is displayed in 4 x 4 layout mode, the display rate is at 2 IPS. In this case, the bandwidth is still 2 Mbps.

### Example 1: WS5050 Endura Workstation—Playback Video Stream

Each WS5050 can display 16 simultaneous playback streams.

To calculate the worse-case bandwidth for the WS5050:

1. Find the bandwidth.

$$B_W = N_S \times B_R = 16 \times 2 \text{ Mbps} = 32 \text{ Mbps}$$

2. Find the overhead.

$$O_H = 25\% \times B_W = 16 \times 2 \text{ Mbps} \times 25\% = 8 \text{ Mbps}$$

3. Find the worse-case bandwidth.

$$B_{WC} = (N_S \times B_R) + O_H = 32 \text{ Mbps} + 8 \text{ Mbps} = 40 \text{ Mbps}$$

### Example 2: VCD5000 Video Console Display—Playback Video Stream

The Model VCD5001 has one monitor output and can display up to 16 simultaneous playback streams. A Model VCD5004 has four monitor outputs and can display 64 simultaneous playback streams.

To calculate the worse-case bandwidth for the VCD5004:

1. Find the bandwidth.

$$B_W = N_S \times B_R = 64 \times 2 \text{ Mbps} = 128 \text{ Mbps}$$

2. Find the overhead.

$$O_H = 25\% \times B_W = 64 \times 2 \text{ Mbps} \times 25\% = 32 \text{ Mbps}$$

3. Find the worse-case bandwidth.

$$B_{WC} = (N_S \times B_R) + O_H = 128 \text{ Mbps} + 32 \text{ Mbps} = 160 \text{ Mbps}$$

### Example 3: NET5301R Decoder—Playback Video Stream

Each NET5301R decoder can playback 4 simultaneous video streams.

To calculate the worse-case bandwidth for the NET5301R decoder:

1. Find the bandwidth.

$$B_W = N_S \times B_R = 4 \times 2 \text{ Mbps} = 8 \text{ Mbps}$$

2. Find the overhead.

$$O_H = 25\% \times B_W = 4 \times 2 \text{ Mbps} \times 25\% = 2 \text{ Mbps}$$

3. Find the worse-case bandwidth.

$$B_{WC} = (N_S \times B_R) + O_H = 8 \text{ Mbps} + 2 \text{ Mbps} = 10 \text{ Mbps}$$

## **Examples of Worse-Case Bandwidth Calculation in Live Video Mode**

### **Example 1: WS5050 Endura Workstation—Live Video Stream**

Each WS5050 can display 16 simultaneous playback streams.

To calculate the worse-case bandwidth for the WS5050:

1. Find the bandwidth.

$$B_W = N_S \times B_R = 16 \times 1 \text{ Mbps} = 16 \text{ Mbps}$$

2. Find the overhead.

$$O_H = 25\% \times B_W = 16 \times 1 \text{ Mbps} \times 25\% = 4 \text{ Mbps}$$

3. Find the worse-case bandwidth.

$$B_{WC} = (N_S \times B_R) + O_H = 16 \text{ Mbps} + 4 \text{ Mbps} = 20 \text{ Mbps}$$

### **Example 2: VCD5000 Video Console Display—Live Video Stream**

The Model VCD5001 has one monitor output and can display up to 16 simultaneous live video streams. A Model VCD5004 has four monitor outputs and can display 64 simultaneous live video streams.

To calculate the worse-case bandwidth for the VCD5004:

1. Find the bandwidth.

$$B_W = N_S \times B_R = 64 \times 1 \text{ Mbps} = 64 \text{ Mbps}$$

2. Find the overhead.

$$O_H = 25\% \times B_W = 64 \text{ Mbps} \times 25\% = 16 \text{ Mbps}$$

3. Find the worse-case bandwidth.

$$B_{WC} = (N_S \times B_R) + O_H = 64 \text{ Mbps} + 16 \text{ Mbps} = 80 \text{ Mbps}$$

### **Example 3: NET5301R Decoder—Live Video Stream**

Each Encoder can playback 4 simultaneous video streams.

To calculate the worse-case bandwidth for NET5301R Decoder:

1. Find the bandwidth.

$$B_W = N_S \times B_R = 4 \times 1 \text{ Mbps} = 4 \text{ Mbps}$$

2. Find the overhead.

$$O_H = 25\% \times B_W = 4 \text{ Mbps} \times 25\% = 1 \text{ Mbps}$$

3. Find the worse-case bandwidth.

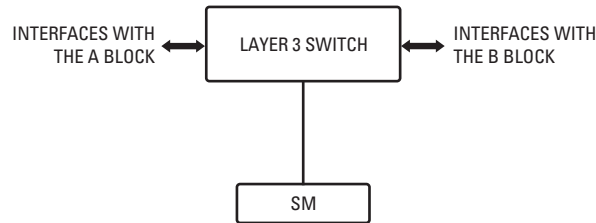
$$B_{WC} = (N_S \times B_R) + O_H = 4 \text{ Mbps} + 1 \text{ Mbps} = 5 \text{ Mbps}$$

## ENDURA CORE BLOCK

The Core Block is functionally responsible for Network layer 3 tasks, discovery, authentication, and security, and interconnects the A and B blocks (refer to Figure 5).

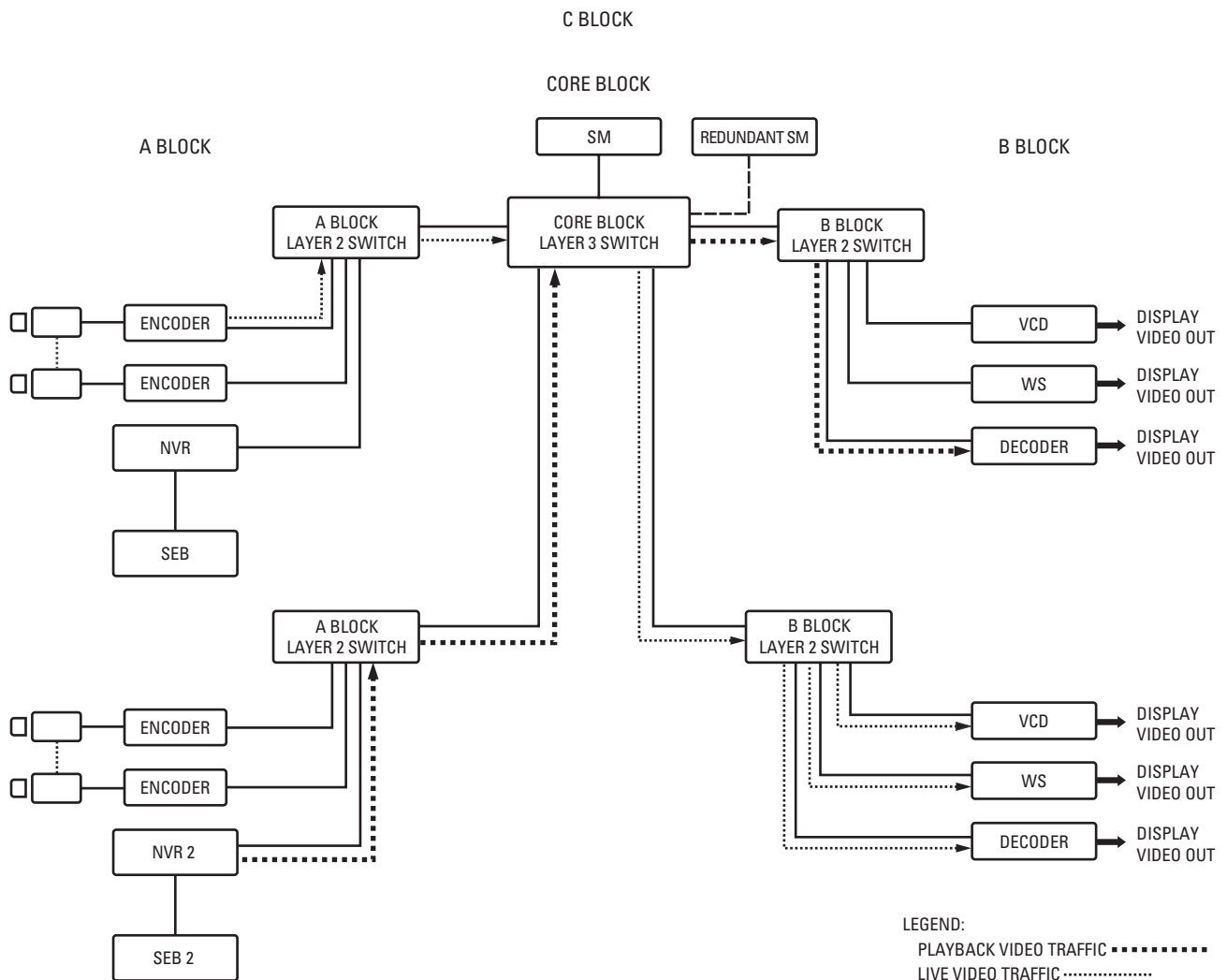
The Core Block is summarized as follows:

- There is only one Core Block for each Endura network.
- The Core Block contains the SM5000 and the redundant SM5000, which provides authentication and security for Endura network.
- The Core Block is on its own VLAN.
- The Core Block includes the core layer 3 switch and any necessary subcore switches.



**Figure 5.** Core Block: Authentication and Security

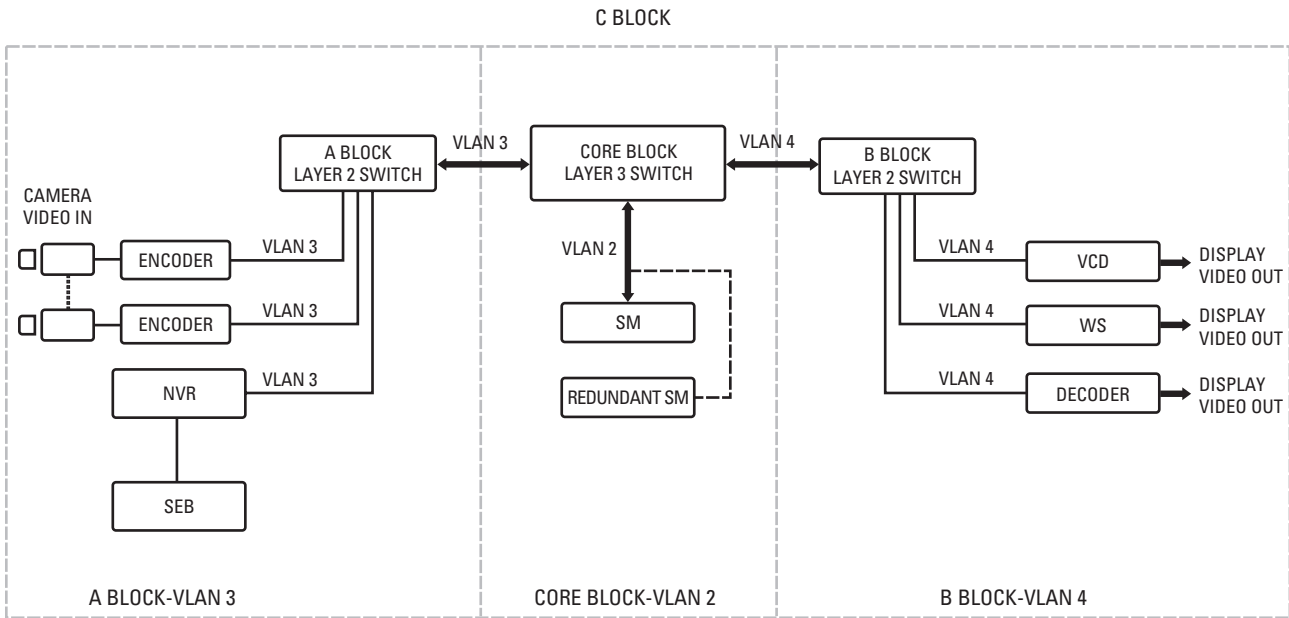
Live video streams flow from the encoder, and playback video streams flow from the NVR5100. Both streams flow through the Core Block to the B Block (refer to Figure 6). The Core Block must be able to handle maximum anticipated system usage.



**Figure 6.** Video Traffic Path Through the Core Block

# ENDURA C BLOCK

Figure 7 illustrates how the A, B, Core, and C Blocks concept is implemented to form a complete Endura network. The Endura network is scaled by replicating the A and B Blocks to accommodate the video input and performance requirements for the network application.



**Figure 7.** C Block: Encompasses A, B, and Core Blocks

Table H lists the Endura network blocks and summarizes the functionality for which each block is responsible.

**Table H.** Endura Network Structures

Entity	Function	Network Devices
A Block	<p>The A Block is functionally responsible for encoding, recording, and storage of the video streams entering the Endura network (both live and playback video).</p> <p>The A Block is summarized as follows:</p> <ul style="list-style-type: none"> <li>Each A Block can support up to 48 NET5301T encoders and one NVR5100.</li> <li>Each A Block is assigned to a specific VLAN.</li> <li>The number of A Blocks is unlimited.</li> <li>Each A Block has only one NVR5100 for recording all NET5301T video streams: video is recorded on the NVR5100 and stored on the SEB5000.</li> </ul>	NET5301T encoders, NVR5100, SEB5000 storage expansion box, and a layer 2 switch
B Block	<p>The B Block is functionally responsible for decoding and displaying the video streams, as well as providing the control and configuration of the Endura networking components.</p> <p>The B Block is summarized as follows:</p> <ul style="list-style-type: none"> <li>Based on permissions, operators can view and control any camera on entire system.</li> <li>Each Block is assigned to a specific VLAN.</li> <li>The B Block can be replicated any number of times (limited only by network capacity).</li> </ul>	NET5301R decoders, VCD5000 video console display, WS5050 Endura Workstation, and a layer 2 switch

**Table H. Endura Network Structures** *(Continued)*

Entity	Function	Network Devices
Core Block	<p>The Core Block is functionally responsible for Network layer 3 tasks, authentication and security, and interconnects the A and B blocks.</p> <p>The Core Block is summarized as follows:</p> <ul style="list-style-type: none"> <li>• There is only one Core Block for each Endura network.</li> <li>• The Core Block provides authentication and security for Endura network.</li> <li>• The Core Block is on its own VLAN.</li> <li>• The Core Block includes the core layer 3 switch and any necessary subcore switches.</li> </ul>	SM5000, redundant SM5000s, and a layer 3 switch
C Block	The C Block includes the entire block structure: A, B, and Core.	Includes all networking equipment

## EXAMPLES OF ENDURA NETWORK DESIGNS

This section describes various Endura network configurations that are scalable and allow you to structure the network for the current as well as future application requirements. Since Endura is a system comprised of high bandwidth IP products, there are specific networking approaches that must be observed.

- If Endura is going to be integrated into an existing network, the existing network must meet the requirements as listed in [Endura Network Design Considerations](#) on page 8.
- The Endura Block design approach must be implemented to manage Endura network traffic efficiently.

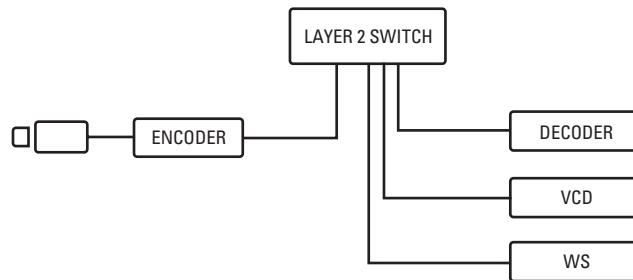
There are two types of Endura network designs:

- Unmanaged
- Managed

### UNMANAGED NETWORK CONFIGURATION

The unmanaged Endura network only supports viewing of live video. As shown in Figure 8, an unmanaged Endura network can include NET5301T encoders and NET5301R decoders, a WS5050 Endura Workstation, VCD5000 video console display, and a switch. The unmanaged network can support up to 16 cameras.

A unmanaged Endura network does not include the SM5000 system manager or NVR5100. In this case, there is no recording or security functionality. The WS5050 provides limited system manager functionality and can only handle up to 16 cameras on a system. If the security network application requires more than 16 cameras or an NVR5100, then the network must be designed as a managed network requiring a SM5000 system manager.

**Figure 8. Unmanaged Endura Network**



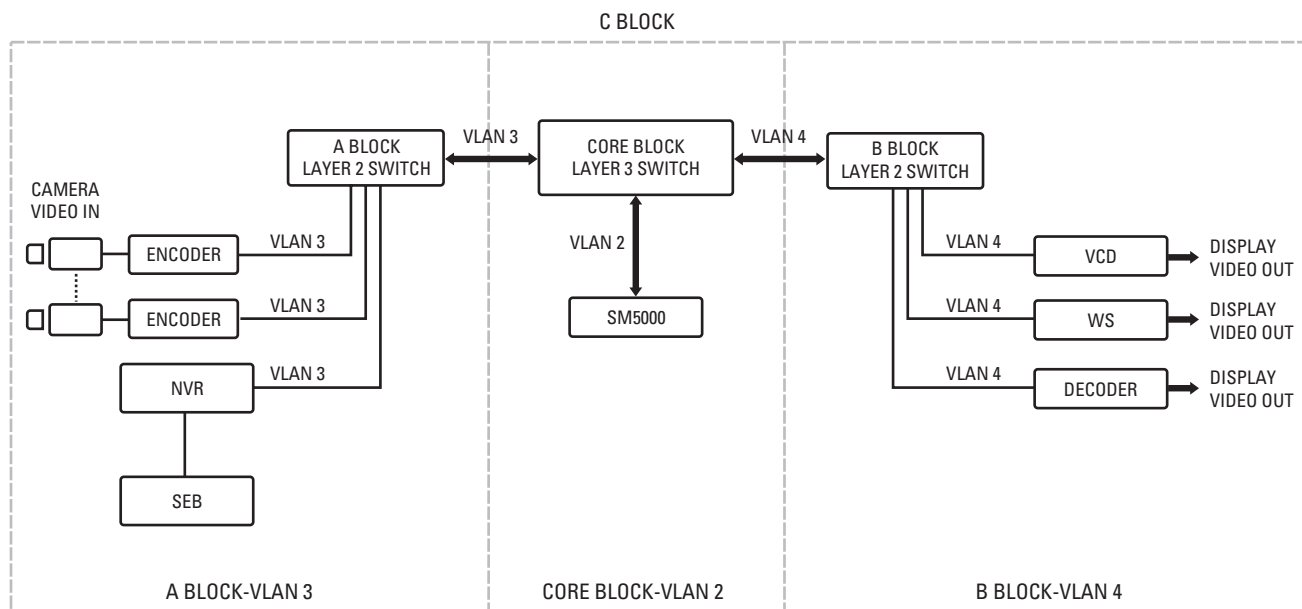
## MANAGED NETWORK CONFIGURATION

The managed Endura network supports viewing of live and playback video, recording, and security. As shown in Figure 9, a managed Endura network includes the full assortment of Endura components: NET5301Ts, NET5301Rs, WS5050s, VCD5000s, NVR5100s, the SM5000, and switches.

The managed Endura network is designed in a four-part block structure (A Block, B Block, C Block, and Core Block). For more information about the block design concept, refer to [Endura C Block](#) on page 23.

- **A Block (VLAN 2):** This is where all video streams enter the network (both live and playback) and where video is recorded by the NVR5100s and stored in SEB5000s. Each A Block can contain no more than 48 NET5301Ts and one NVR5100. The NVR5100 in each respective A Block records video streams from the Encoders in the same A Block.
- **B Block (VLAN 4):** This is where all video viewing takes place, and VCD5000s, NET5301Rs, and WS5050s are connected to the Endura network.
- **Core Block (VLAN 3):** This is where the SM5000 resides. The Endura Core Block interconnects the A and B Blocks.
- **C Block:** The entire structure including A Blocks, B Blocks and the Core Block is referred to as the C Block.

For more information about the block design concept, refer to [Endura Network Design Considerations](#) on page 8.



**Figure 9. Managed Endura Network**

You can have multiple A Blocks in an Endura network.

- The number of cameras and amount of storage needed for the video security network determines how many SEB5000s are needed in an A Block.
- As with A Blocks, there can be multiple B Blocks in the network, but as many as the network can support. Generally, the B Block uses the most bandwidth across the network.
- The SM5000 is connected to the core switch and resides in the Core Block.
- The Core Block implements network connectivity between all Endura components to comprise the basic Endura network.

## Connecting the NVR5100 and SEB5000s

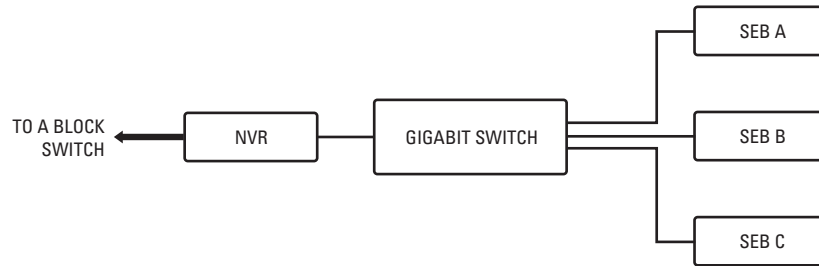
The SEB5000 storage expansion box can be connected to the NVR5100 in one of two ways:

- A patch cable is used to connect a single SEB5000 directly to an NVR5100 (refer to Figure 10). The NVR5100 and SEB5000 Ethernet port is autosensing.



**Figure 10.** Using a Patch Cable to Connect the NVR5100 and a Single SEB5000

- A dedicated, gigabit Ethernet switch can be used to expand the video storage of the NVR5100. In this case, no more than eight SEB5000s can be interface to a single NVR (refer to Figure 11).



**Figure 11.** Connecting the NVR5100 and Multiple SE5000Bs

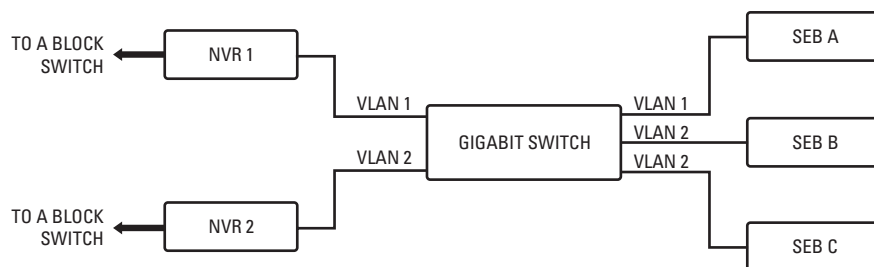
## Connecting Multiple NVR5100s and SEB5000s

In a large system it is possible to use one storage switch to network multiple NVR5100 and SEB5000 combinations. If multiple NVR5100s are used in the network, Pelco requires that VLANs be configured on the storage switches because it is important to segment communication so that each NVR5100 only communicates with the SEB5000s to which the NVR5100 is assigned.

Figure 12 shows an example of how to segment the network using VLANs.

- NVR5100 #1 resides in VLAN 1 and NVR5100 #2 resides in VLAN 2.
- SEB5000 #1 resides in VLAN 1 and SEB5000 #2 and SEB5000 #3 reside in VLAN 2.

In this case, NVR5100 #1 stores video streams on SEB5000 #1 and NVR5100 #2 stores video streams on SEB5000 #2 and SEB5000 #3. The segmenting of devices by VLANs prevents NVR5100 #1 from communicating with SEB5000 #2 or #3. Likewise, NVR5100 #2 is prevented from communicating with SEB5000 #1.

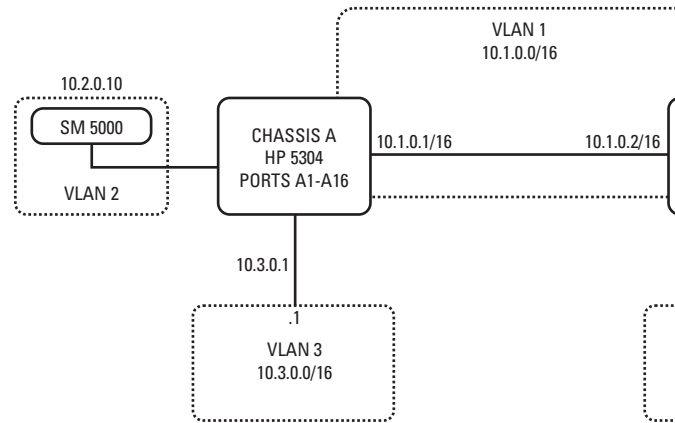


**Figure 12.** Using VLANs to Connect Multiple NVR5100s and SE5000Bs

## Appendix A: Endura Network Configuration Example

This section provides an example of how to configure an HP 5300 series chassis switch for an Endura Network. The information in this section is only an example of how to configure an HP 5300 series chassis switch. Although this example is typical, other network configurations can support Endura. For more information about advanced configurations, refer to HP Advanced Traffic Management Guide at [www.hp.com/go/procurve](http://www.hp.com/go/procurve).

Figure 13 illustrates a high-level Endura network topology using the HP 5300 series switch.



**Figure 13.** Example Endura Network and HP 5304 Switch Configuration

The network diagram above will be used throughout this document to demonstrate how to set up a basic Endura system.

The HP 5300 series chassis switches have multiple slots available to insert a variety of modules as follows:

- ProCurve Switch xl 16-port 10/100/1000 Module (J4907A)
- ProCurve Switch xl 10/100-TX PoE Module (J8161A)
- ProCurve Switch xl 10/100-TX Module (J4820A)
- ProCurve Switch xl 100/1000-T Module (J4821A)
- ProCurve Switch xl Mini-GBIC Module (J4878A)
- ProCurve Switch xl 100-FX MTRJ Module (J4852A)

For the purposes of discussion in this section, assume the following:

- Switch A has one 16-Port 10/100/1000 Module in slot A (Ports A1-A16).
- Switch B has one 16-Port 10/100/1000 Module in slot B (Ports B1-B16).
- The switches are in their default state.
- The command 'erase startup-config' was issued before any configuration.
- Ports A16 and B16 are used to link the two switches together.

**NOTE:** Use the serial cable that is supplied during all configurations. While this is not necessary, it allows you to view messages during the bootstrap process on the switch, which might be helpful if you have to perform troubleshooting.

The following sections provide a procedure configuring switch A and B using RIPv2 as a routing protocol because RIPv2 is easier to configure. However, static routes or OSPF are alternative methods. Also, IP helper addresses are setup on VLAN 1, which is only required if a DHCP client resides on this VLAN. No device other than a switch should reside on VLAN 1 because there are multiple gateways on VLAN 1.

## SETTING UP SWITCH A

The following procedure is an example shows how to configure switch A from the HP 5300 series command line interface (CLI).

To set up switch A:

1. Access the HP ProCurve switch command line interface (CLI), and log into the switch.  
The HP ProCurve Switch 5304XL# prompt is displayed.
2. Enter **config** to access the configuration mode.  
The HP ProCurve Switch 5304XL(config)# prompt is displayed.
  - a. Enter **ip routing** to enable IP routing.
  - b. Enter **ip multicast-routing** to enable multicast routing.
  - c. Enter **router rip** to enable RIP routing.  
The HP ProCurve Switch 5304XL(rip)# prompt is displayed.
  - d. Enter **exit** to exit the RIP configuration mode.  
The HP ProCurve Switch 5304XL(config)# prompt is displayed.
3. Do the following:
  - a. Enter **router pim** to access the PIM configuration mode and enable PIM-DM routing.
  - b. Enter **exit** to exit the PIM configuration mode.  
The HP ProCurve Switch 5304XL(config)# prompt is displayed.
4. Enter **vlan 1** to access the VLAN 1 configuration mode.  
The HP ProCurve Switch 5304XL(vlan-1)# prompt is displayed.
  - a. Enter **ip address 10.1.0.1/16** to assign an IP address with a 16-bit network prefix to VLAN 1.
  - b. Enter **ip igmp** to enable IGMP on VLAN 1.
  - c. Enter **ip rip** to enable RIPv2 on VLAN 1.
  - d. Enter **ip pim** to enable PIM on VLAN 1.
  - e. Enter **ip helper-address 10.2.0.10** to specify where to forward DHCP requests. (In this example, the SM5000 is providing DHCP service for the Endura network.)
5. Enter **vlan 2** to access the VLAN 2 configuration mode.  
The HP ProCurve Switch 5304XL(vlan-2)# prompt is displayed.
  - a. Enter **untagged A1** to assign ports A1 to A15 to VLAN 2. (This type of assignment is not necessary for VLAN 1 because all of VLAN 1's ports by default are in VLAN 1.)
  - b. Enter **ip address 10.2.0.1/16** to assign an IP address with a 16-bit network prefix to VLAN 2.
  - c. Enter **ip igmp** to enable IGMP on VLAN 2.
  - d. Enter **ip rip** to enable RIPv2 on VLAN 2.
  - e. Enter **ip pim** to enable PIM on VLAN 2.
  - f. Enter **ip helper-address 10.3.0.10** to specify where to forward DHCP requests. (In this example, the SM5000 is providing DHCP service for the Endura network.)
6. Enter **vlan3** to access the VLAN 3 configuration mode.  
The HP ProCurve Switch 5304XL(vlan-3)# prompt is displayed.
  - a. Enter **untagged A2** to assign ports A2 to A15 to VLAN 3. (This type of assignment is not necessary for VLAN 1 because all of VLAN 1's ports by default are in VLAN 1.)
  - b. Enter **ip address 10.3.0.1/16** to assign an IP address with a 16-bit network prefix to VLAN 3.
  - c. Enter **ip igmp** to enable IGMP on VLAN 3.
  - d. Enter **ip rip** to enable RIPv2 on VLAN 3.

- e. Enter **ip pim** to enable PIM on VLAN 3.
- f. Enter **ip helper-address 10.3.0.10** to specify where to forward DHCP requests. (In this example, the SM5000 is providing DHCP service for the Endura network.)
7. Enter **exit** to exit the VLAN configuration mode.
8. Enter **write memory** to save your configuration.

**NOTE:** The helper address in step 5f is not necessary since the system manager/DHCP server is on the same network.

## SETTING UP SWITCH B

The following procedure is an example shows how to configure switch B from the HP 53XX command line interface (CLI).

To set up switch B:

1. Access the HP ProCurve switch command line interface (CLI), and log into the switch.  
The HP ProCurve Switch 5304XL# prompt is displayed.
2. Enter **config** to access the configuration mode.  
The HP ProCurve Switch 5304XL(config)# prompt is displayed.
  - a. Enter **ip routing** to enable IP routing.
  - b. Enter **ip multicast-routing** to enable multicast routing.
  - c. Enter **router rip** to enable RIP routing.  
The HP ProCurve Switch 5304XL(rip)# prompt is displayed.
  - d. Enter **exit** to exit the RIP configuration mode.  
The HP ProCurve Switch 5304XL(config)# prompt is displayed.
3. Do the following:
  - a. Enter **router pim** to access the PIM configuration mode and enable PIM-DM routing.
  - b. Enter **exit** to exit the PIM configuration mode.  
The HP ProCurve Switch 5304XL(config)# prompt is displayed.
4. Enter **vlan 1** to access the VLAN 1 configuration mode.  
The HP ProCurve Switch 5304XL(vlan-1)# prompt is displayed.
  - a. Enter **ip address 10.1.0.2/16** to assign an IP address with a 16-bit network prefix to VLAN 1.
  - b. Enter **ip igmp** to enable IGMP on VLAN 1.
  - c. Enter **ip rip** to enable RIPV2 on VLAN 1.
  - d. Enter **ip pim** to enable PIM on VLAN 1.
  - e. Enter **ip helper-address 10.3.0.10** to specify where to forward DHCP requests. (In this example, the SM5000 is providing DHCP service for the Endura network.)
5. Enter **vlan 3** to access the VLAN 3 configuration mode.  
The HP ProCurve Switch 5304XL(vlan-3)# prompt is displayed.
  - a. Enter **untagged B1-B15** to assign ports B1 to B15 to VLAN 3. (This type of assignment is not necessary for VLAN 1 because all of VLAN 1's ports by default are in VLAN 1.)
  - b. Enter **ip address 10.3.0.1/16** to assign an IP address with a 16-bit network prefix to VLAN 3.
  - c. Enter **ip igmp** to enable IGMP on VLAN 3.
  - d. Enter **ip rip** to enable RIPV2 on VLAN 3.
  - e. Enter **ip pim** to enable PIM on VLAN 3.

- f. Enter **ip helper-address 10.3.0.10** to specify where to forward DHCP requests. (In this example, the SM5000 is providing DHCP service for the Endura network.
6. Enter **exit** to exit the VLAN configuration mode.
7. Enter **write memory** to save your configuration.

## EXAMPLE CONFIGURATION FILE FOR SWITCH B

Figure 14 shows an example of the configuration file for switch B.

```
; J4850A Configuration Editor; Created on release #E.08.44

hostname "HP ProCurve Switch 5304XL"

module 2 type J4907A

ip routing

snmp-server community "public" Unrestricted

vlan 1
    name "DEFAULT_VLAN"
    untagged B16
    ip address 10.1.0.2 255.255.0.0
    no untagged B1-B15
    exit

vlan 3
    name "VLAN3"
    untagged B1-B15
    ip address 10.3.0.1 255.255.0.0
    ip helper-address 10.3.0.10
    ip igmp
    exit

ip multicast-routing

router rip
    exit

router pim
    exit

vlan 1
    ip rip
    ip pim all
    exit

vlan 3
    ip rip
    ip pim all
    exit
```

**Figure 14.** Example of a Configuration File

## Appendix B: WAN Configuration Example

This appendix provides a sample configuration for multicasting over a generic routing encapsulation (GRE) tunnel as an example of how to configure an Endura network using WAN connectivity. Much of the information in this appendix is derived from the online document titled *Multicasting Over a GRE Tunnel*, published by Cisco Systems®. To view this document, go to or click [http://www.cisco.com/en/US/tech/tk828/technologies\\_configuration\\_example09186a00801a5aa2.shtml](http://www.cisco.com/en/US/tech/tk828/technologies_configuration_example09186a00801a5aa2.shtml).

In an Endura application scenario, where you want to extend an existing Endura network across a network that does not support multicast, it is recommended that you configure a GRE tunnel to send multicast traffic between routers. In this case, the GRE tunnel is required because the multicast source and receiver are separated by an IP cloud that is not configured to support IP multicast traffic. In such network scenarios, configuring a tunnel across an IP cloud with PIM will allow multicast packets to be exchanged between the source and receiver.

This appendix describes the configuration, verification, and related issues pertaining to multicasting over a GRE tunnel. The information presented in this appendix was created from devices in a specific lab environment. All of the devices used in this appendix started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

### NETWORK CONFIGURATION OVERVIEW

As shown in Figure 15, the multicast source (10.1.1.1) is connected to R102 and is configured for multicast group 239.1.1.20. The multicast receiver (10.2.2.3) is connected to R104 and is configured to receive multicast packets for group 239.1.1.20. Separating R102 and R104 is an IP cloud, which is not configured for multicast routing.

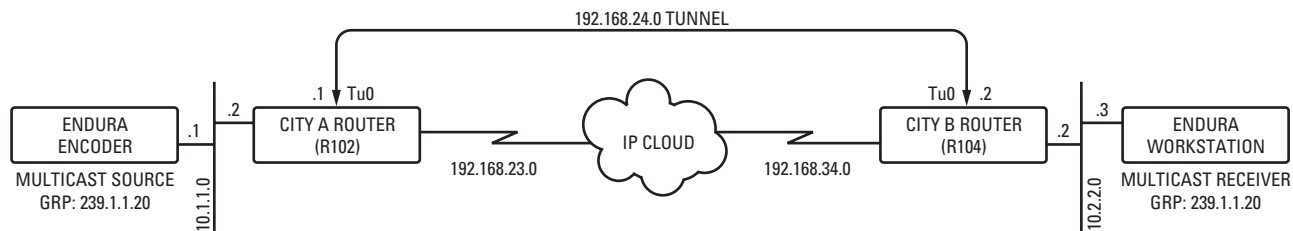


Figure 15. Sample Endura Network Over a WAN

A tunnel is configured between R102 to R104 sourced with their loopback interfaces. The `ip pim sparse-dense mode` command is configured on tunnel interfaces and multicast-routing is enabled on R102 and R104. Sparse-dense mode configuration on the tunnel interfaces allows sparse-mode or dense-mode packets to be forwarded over the tunnel depending on rendezvous point (RP) configuration for the group.

- **For dense mode:** With PIM dense mode configured over the tunnel, an `ip mroute 10.1.1.0 255.255.255.0 tunnel 0` command is configured on R104 to ensure a successful RPF for multicast source address 10.1.1.1. Incoming (10.1.1.1, 239.1.1.20) multicast packets over Tunnel0 (Tu0) are checked for Reverse Path Forwarding (RPF) using this mroute statement. After a successful check, the multicast packets are forwarded to outgoing interface list (OIL) interfaces.

- **For sparse mode:** With PIM sparse mode configured over the tunnel, ensure that the following points are addressed:

- For a successful RPF verification of multicast traffic flowing over the shared tree (\*,G) from RP, an `ip mroute rp-address nexthop` command needs to be configured for the RP address, pointing to the tunnel interface.

Assuming R102 to be the RP (RP address 2.2.2.2) in this case, the mroute would be the `ip mroute 2.2.2.2 255.255.255.255 tunnel 0` command, which ensures a successful RPF check for traffic flowing over the shared tree.

- For a successful RPF verification of multicast (S,G) traffic flowing over the Shortest Path Tree (SPT), an `ip mroute source-address nexthop` command needs to be configured for the multicast source, pointing to the tunnel interface.

In this case, when SPT traffic is flowing over tunnel interface an `ip mroute 10.1.1.0 255.255.255.0 tunnel 0` command is configured on R104 to ensure a successful RPF verification for incoming (10.1.1.1, 239.1.1.20) multicast packets over the Tu0 interface.

The sample configuration files for R102 and R104 are described in the following sections:

- [City A Router \(R102\) Configuration File](#) on page 32
- [City B Router \(R104\) Configuration File](#) on page 33

## CITY A ROUTER (R102) CONFIGURATION FILE

```
r102#
version 12.2
!
hostname r102
!
ip subnet-zero
no ip domain-lookup
!--- It stops IP domain lookup, which improves the show command response time.
!
ip multicast-routing
!--- Enables IP multicast routing.
!
interface Loopback0
ip address 2.2.2.2 255.255.255.255
!--- Tunnel Source interface.
!
interface Tunnel0
!--- Tunnel interface configured for PIM and carrying multicast packets to R104.
!
ip address 192.168.24.1 255.255.255.252
ip pim sparse-dense-mode
tunnel source Loopback0
tunnel destination 4.4.4.4
!
interface Ethernet0/0
!
!--- Interface connected to Source.
!
ip address 10.1.1.2 255.255.255.0
ip pim sparse-dense-mode
!
interface Serial8/0
ip address 192.168.23.1 255.255.255.252
!
!--- Note IP PIM sparse-dense mode is not configured on serial interface.
!
router ospf 1
log-adjacency-changes
network 2.2.2.2 0.0.0.0 area 0
network 10.1.1.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
!
ip classless
ip pim bidir-enable
!
line con 0
line aux 0
line vty 0 4
login
!
end
```



## CITY B ROUTER (R104) CONFIGURATION FILE

```
r104#
version 12.2
!
hostname r104
!
ip subnet-zero
no ip domain-lookup
!
!--- It stops IP domain lookup, which improves the show command response time.
!
ip multicast-routing
!
!--- Enables IP multicast routing.
!
interface Loopback0
ip address 4.4.4.4 255.255.255.255
!
!--- Tunnel Source interface.
!
interface Tunnel0
ip address 192.168.24.2 255.255.255.252
!
!--- Tunnel interface configured for PIM and carrying multicast packets.
!
ip pim sparse-dense-mode
tunnel source Loopback0
tunnel destination 2.2.2.2
!
interface Ethernet0/0
ip address 10.2.2.2 255.255.255.0
ip pim sparse-dense-mode
!
interface Serial9/0
ip address 192.168.34.1 255.255.255.252
!
!--- Note IP PIM sparse-dense mode is not configured on serial interface.
!
router ospf 1
log-adjacency-changes
network 4.4.4.4 0.0.0.0 area 0
network 10.2.2.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 0
!
ip classless
no ip http server
ip pim bidir-enable
ip mroute 10.1.1.0 255.255.255.0 Tunnel0
!
!--- This Mroute ensures a successful RPF check for packets flowing from the source.
!--- 10.1.1.1 over Shared tree in case of dense mode and SPT in case of sparse mode.
!
(Continued on next page)
```

```

ip mroute 2.2.2.2 255.255.255.255 tunnel 0
!
!--- This Mroute is required for RPF check when sparse mode multicast traffic is
!--- flowing from RP (assuming R102 with 2.2.2.2 as RP) towards receiver via tunnel
!--- before the SPT switchover.
!
line con 0
line aux 0
line vty 0 4
login
!
end

```

## VERIFYING THE CONFIGURATION

Complete the following steps to verify your configuration:

1. Use the show ip igmp groups command to verify that the receiver has sent its IGMP join membership request for group 239.1.1.20 to R104.

```
r104# show ip igmp groups
```

```

IGMP Connected Group Membership
Group Address      Interface          Uptime    Expires    Last Reporter
239.1.1.20         Ethernet0/0        00:00:04  00:02:55   10.2.2.3

```

2. Use the show ip mroute *group-address* command to display that when the source 10.1.1.1 starts multicasting packets for the group 239.1.1.20, R102 installs the (\*,239.1.1.20) and (10.1.1.1, 239.1.1.20) entries in the R102 mroute table, as shown below.

```
r102# show ip mroute 239.1.1.20
```

```

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

```

```

(*, 239.1.1.20), 00:00:09/00:02:59, RP 0.0.0.0, flags: D
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:00:09/00:00:00
    Ethernet0/0, Forward/Sparse-Dense, 00:00:09/00:00:00

```

```

(10.1.1.1, 239.1.1.20), 00:00:09/00:02:58, flags: T
  Incoming interface: Ethernet0/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:00:09/00:00:00

```

**NOTE:** In the (10.1.1.1, 239.1.1.20) entry, the OIL is Tunnel0.

3. Use the `show ip mroute group-address` command to verify that R104 has the (\*,239.1.1.20) and (10.1.1.1, 239.1.1.20) entries while it is forwarding multicast packets for group 239.1.1.20 sourced from 10.1.1.1, as shown below.

**r104# show ip mroute 239.1.1.20**

```
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.1.1.20), 00:07:10/00:00:00, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel0, Forward/Sparse-Dense, 00:07:10/00:00:00
    Ethernet0/0, Forward/Sparse-Dense, 00:07:10/00:00:00

(10.1.1.1, 239.1.1.20), 00:01:13/00:02:24, flags: CLT
  Incoming interface: Tunnel0, RPF nbr 192.168.24.1, Mroute
  Outgoing interface list:
    Ethernet0/0, Forward/Sparse-Dense, 00:01:13/00:00:00
```

**NOTE:** In (10.1.1.1, 239.1.1.20), the incoming interface is Tunnel0 and the RPF neighbor is 192.168.24.1—the Tunnel head end on R102. The RPF verification is done based on the Mroute configured on R104, and the multicast packets are pushed out to the OIL to the receiver connected on the Ethernet 0/0 interface.

4. Use the `show ip rpf ip-address` command to perform an RPF verification for packets sourced from 10.1.1.1. The following example confirms that RPF for 10.1.1.1 is via Tunnel 0, on which we are receiving the multicast (S,G) packets.

**r104> show ip rpf 10.1.1.1**

```
RPF information for ? (10.1.1.1)
  RPF interface: Tunnel0
  RPF neighbor: ? (192.168.24.1)
  RPF route/mask: 10.1.1.1/24
  RPF type: static
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

Certain show commands are supported by the Output Interpreter tool, which allows you to view an analysis of show command output.

## TROUBLESHOOTING

If your multicast over GRE tunnel is not working, one of the following could be the cause:

- **Tunnel not UP/UP:** The tunnel source and destination do not match on each end of the tunnel. For example, if the tunnel destination on R102 was changed to the IP address 10.2.2.2 instead of 2.2.2.2 while the configuration on R104 remained the same, the tunnel would not come up. To verify the status of the tunnel, use the show interface tunnel 0 command.
- **RPF Failure:** Use the show ip mroute count command to verify that the multicast packets are dropped because of RPF failure. A sample output of the show ip mroute count command and its increasing counters for RPF failure is shown in bold below:

```
r104# show ip mroute count
```

```
IP Multicast Statistics
3 routes using 1642 bytes of memory
2 groups, 0.50 average sources per group
```

- **Forwarding Counts:** Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second  
Other counts: Total/**RPF failed**/Other drops(OIF-null, rate-limit etc)

```
Group: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0
```

```
Group: 239.1.1.20, Source count: 1, Packets forwarded: 11, Packets received: 45
Source: 10.1.1.1/32, Forwarding: 11/0/100/0, Other: 25/14/0
```

!-- After some time, the show ip mroute count command is issued again.

!-- You can see the RPF failed counter increasing:

```
r104# show ip mroute count
```

```
IP Multicast Statistics
3 routes using 1642 bytes of memory
2 groups, 0.50 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)
```

```
Group: 224.0.1.40, Source count: 0, Packets forwarded: 0, Packets received: 0
```

```
Group: 239.1.1.20, Source count: 1, Packets forwarded: 11, Packets received: 50
Source: 10.1.1.1/32, Forwarding: 11/0/100/0, Other: 30/19/0
```

```
r104#
```

Use the show ip rpf *source* command to ensure that the RPF interface is the same as that on which the source multicast packets are received—Tunnel 0 in this example. For more information on RPF failures, go to or click <http://www.cisco.com/warp/public/105/mcastguide0.html> to access the IP Multicast Troubleshooting Guide.

- **PIM Neighbors:** Router R102 is not forwarding over the Tunnel0 interface because it is not seeing a PM neighbor R104. You can use the show ip pim neighbor command on R102 to show the neighbor R104 over the tunnel. You can also use the show ip pim int command to show that there is a neighbor. Verify that the interface level ip pim sparse-dense-mode command is configured on both ends of the tunnel and that IP multicast-routing is enabled.

## Appendix C: Endura Network Requirements Worksheet

The Endura Network Requirements Worksheet allows you to identify essential network resources that must be available to support the Endura system. It is recommended that you complete this worksheet before integrating the Endura system into a new or existing network.

Please check all that apply.

### ☐ Unicast Routing

The network supports one of the following unicast routing protocols:

☐ RIP      ☐ OSPF      ☐ Static      ☐ Other: \_\_\_\_\_

Comment/question: \_\_\_\_\_

### ☐ Multicast Routing

The network supports one of the following multicast routing protocols:

☐ PIM-SM      ☐ PIM-DM      ☐ DVMRP      ☐ Other: \_\_\_\_\_

Comment/question: \_\_\_\_\_

### ☐ IGMP

The network supports one of the following versions of IGMP:

☐ IGMP v1      ☐ IGMP v2

Comment/question: \_\_\_\_\_

### ☐ Multicast Traffic

Does the network device flood multicast traffic?

☐ Yes      ☐ No

Comment/question: \_\_\_\_\_

### ☐ Bandwidth

Does the network provide enough bandwidth to support the current Endura system and allow for future network growth?

☐ Yes      ☐ No

Comment/question: \_\_\_\_\_

### ☐ Network Design

Do you have an Endura network design in place?

☐ Yes      ☐ No

Comment/question: \_\_\_\_\_



# Index

---

## Numerics

1000baseT 7  
100baseT 7  
4CIF 12

## A

authentication 22

## B

bandwidth, calculating  
  for live video stream 21  
  for playback video stream 20  
  quad layout 13  
  worse-case 13  
blocks  
  as a design requirement 10  
  broadcast domains 10  
  description of  
    A Block 10  
    B Block 12  
    C Block 23  
    Core Block 22  
    responsibility of each block 23  
  provides network structure 5  
  separated by VLANs 9  
  TTL, how used 11  
broadcast domains 9

## C

CAT5e 7  
CAT6 7  
CIF 12  
core  
  block 22

## D

dense mode (PIM-DM) 7  
devices, network  
  Endura components 6  
  HP5300 series configuration 27  
digital video 6  
Distance Vector Multicast Routing Protocol. See DVMRP  
distance vector protocol. See DVMR  
domains, broadcast 9  
DVMRP 7, 8

## E

Endura components  
  description of products 6  
  network devices 5  
Endura networks  
  broadcast domains, how used 10  
  design approaches 24  
  integrating with existing network 24  
  managing Endura traffic 24  
  scalability of 24  
  structure of

  A Block 10  
  B Block 12  
  C Block 23  
  Core Block 22  
  TTL, how used 11  
EnduraStor 6  
EnduraView 13

## G

GRE  
  tunnels 31  
  tunnels, troubleshooting 36

## H

hop count 7

## I

IGP  
  OSPF  
Intelligent edge network design 8  
interface, tunnel 31  
Interior Gateway Protocol  
  See IGP

## L

layout mode 13

## M

managed Endura network  
  configuration of 25  
  Endura devices 25  
  functionality of 25  
  NVRs and SEBs, connection of 26  
  NVRs and SEBs, segmenting network using VLANs 26  
modes, viewing 13  
MPEG4 video encoder 6  
multicast  
  group 31  
  group memberships 8  
  source 31  
  traffic 7  
multicast protocols  
  DVMRP 7, 8  
  PIM-DM 7  
  PIM-SM 8  
multicast streams  
  blocking of 8  
  flooding 8  
multiple-stream decoding 6

## N

network devices  
  Endura components 6  
  HP5300 series switch 27  
network topology 7  
  based on blocks 5, 9  
  core, traditional 8

- Endura network structure 9
- intelligent edge 8
- network designs, examples of 24
- protocols 7
- VLANs 9
- NVR (network video recorder) 6

## O

- Open Shortest Path. See OSPF
- OSPF 7
- overhead, for bandwidth 13

## P

- packets, multicast 36
- packets, video 9, 11
- physical media
  - Ethernet cabling 7
- PIM
  - dense mode 7, 36
  - neighbors 36
  - sparse mode 7, 8, 36
- PIM-DM 7
- PIM-SM 8
- product support 6
- protocols 7
  - DVMRP 7
  - OSPF 7
  - PIM-DM 7
  - PIM-SM 7
  - RIP 7

## R

- redundant SM5000 22
- rendezvous point 8
- Reverse Path Forwarding
  - See RPF
- RIP (Routing Information Protocol) 7
- routing
  - multicast 31
  - unicast 7
- RPF
  - failure 36
  - mroute statement
  - verification of multicast traffic 31
- RPF (Reverse Path Forwarding) 7

## S

- scaling Endura network, using
  - A Block 10
  - B Block 12
- security 22
- SM5000 system manager 6
- sparse mode (PIM-SM) 7
- Storage Expansion Box. See SEB
- storage requirements 12
- S-Video 6
- switches
  - layer 3 22
  - subcore 22
  - used to connect multiple NVRs and SEBs 26
  - VLAN-aware 8
- system manager 6

## T

- TCP/IP protocol suite 7
- Time to Live. See TTL
- traditional design 8
- traditional network design 8
- traffic, network
  - Endura (performance summary) 12
  - UPnP 9
  - VLANs, helps manage 9
- troubleshooting
  - GRE tunnels 36
- TTL
  - default setting for Endura components 11
  - setting 9
- tunnel
  - destination 36
  - GRE 36
  - source 36
  - status of, verifying 36

## U

- unicast protocols
  - OSPF 7
  - RIP 7
- unknown multicast groups 8
- unmanaged Endura network
  - configuration of 24
  - Endura devices in 24
  - functionality of 24
- UPnP
  - traffic, isolation of 9
- UPnP (Universal Plug and Play) 6

## V

- VGA 6
- video security systems 5
- video stream
  - B Block 13
  - highest 13
  - lowest 13
  - playback 13
  - viewing, live 13
- video, viewing of
  - B Block 12, 25
  - live and playback video 12, 25
- VLANs
  - how created 9
  - separate Endura blocks 9
  - traffic management 9

## W

- WANs
  - generic routing encapsulation (GRE) tunnel 31
  - how to configure 31



REVISION HISTORY

Manual #	Date	Comments
C1640M	7/05	Original version.
C1640M-A	12/05	The PC Workstation was renamed to WS5050 Endura Workstation. The VLAN references and descriptions in text and graphics on pages 10, 11, 17, and 19-24 were revised to clarify technical content.
C1640M-B	3/06	Updates the <i>Calculating Bandwidth and Storage Requirements</i> section to add new NTSC and PAL frame rates supported in Version 1.3 across all resolutions (CIF, 2CIF, and 4CIF).

Pelco, the Pelco logo, Camclosure, Esprit, Genex, Legacy, and Spectra are registered trademarks of Pelco.  
Endura, EnduraStor, and ExSite are trademarks of Pelco.  
DLP is a registered trademark of Texas Instruments, Inc.  
Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries.  
UPnP is a trademark of UPnP Implementers Corporation.  
Cisco Systems is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and/or other countries.

©Copyright 2006, Pelco. All rights reserved.



Worldwide Headquarters  
3500 Pelco Way  
Clovis, California 93612 USA

USA & Canada  
Tel: 800/289-9100  
Fax: 800/289-9150

International  
Tel: 1-559/292-1981  
Fax: 1-559/348-1120

**[www.pelco.com](http://www.pelco.com)**

**ISO9001**

United States | Canada | United Kingdom | The Netherlands | Singapore | Spain | Scandinavia | France | Middle East