



# Cisco Video Surveillance Stream Manager Hybrid Design Guide



## Table of Contents

<b>Chapter 1: Video Surveillance Overview</b> .....	<b>1-1</b>
Video Surveillance Components .....	1-1
Cameras .....	1-2
Transmission Media.....	1-2
Baluns.....	1-4
Matrix Switches.....	1-5
Recording .....	1-7
<b>Chapter 2: Cisco Stream Manager Hybrid Solution</b> .....	<b>2-1</b>
Hybrid Solution Components .....	2-2
Integration Steps .....	2-3
Step 1: Remove legacy recording systems.....	2-4
Step 2: Introduce a Cisco Data Converter .....	2-4
Step 3: Introduce a Cisco Hybrid Decoder.....	2-5
Step 4: Cisco Stream Manager Modules .....	2-6
Viewing Live and Recorded Video.....	2-6
Live Viewing Operation.....	2-6
Recorded Viewing Operation.....	2-7
<b>Chapter 3: Failover and Recovery</b> .....	<b>3-1</b>
Matrix-based N+N Redundancy .....	3-1
How a Failure is Detected .....	3-2
Single Port Failure.....	3-4
Recovering from a Failure .....	3-4
Retrieving Video from a Failover ISP.....	3-4
Failover and Recovery with two Failover ISPs .....	3-5
<b>Chapter 4: Third-Party Equipment Support</b> .....	<b>4-1</b>
<b>Chapter 5: Basic Configuration</b> .....	<b>5-1</b>
Configuring the Integrated Services Platform .....	5-1
Configuring the Cisco Hybrid Decoder .....	5-3
Hybrid Decoder Pools.....	5-5
Time Synchronization .....	5-7
Configuring Failover with a Matrix Switch.....	5-9
Configure the Failover Integrated Services Platform .....	5-9
Configure Video Loss Detection .....	5-12
Configure the Stream Manager Administration and Monitoring Module.....	5-13
<b>Chapter 6: Manufacturer-Specific Configurations</b> .....	<b>6-1</b>
Integration with a Bosch Matrix Switch and Keyboard.....	6-1
Cisco Data Converter .....	6-2
Cisco Hybrid Decoder.....	6-3
Configuring the Bosch LTC 8200 Matrix Switch.....	6-3
Allegiant Master Control Software .....	6-3
Upgrading the Bosch IntuiKey Keyboard .....	6-5
Failover Configuration with a Bosch LTC 8200 Matrix Switch .....	6-9
Integration with an American Dynamics Matrix Switch .....	6-11
Power Supply/Data Converter .....	6-12
Failover Configuration with an American Dynamics Matrix Switch .....	6-13
Integration with a Pelco Matrix Switch and Keyboard.....	6-14
Power Supply/Data Converter .....	6-15
Integrated Services Platform BIOS Setup.....	6-16
Pelco CM9760-KBD Keyboard Setup .....	6-16
Pelco CPU Setup.....	6-17
Failover Configuration with a Pelco Matrix Switch .....	6-19
<b>Appendix A: Network Communications</b> .....	<b>I</b>
TCP/UDP Ports Required for Video Playback .....	I
TCP/UDP Ports Required During a Failover.....	III
<b>Appendix B: Glossary</b> .....	<b>V</b>

## Chapter 1: Video Surveillance Overview

Video surveillance has been a key component of many organizations' safety and security groups for decades. As an application, video surveillance has demonstrated its value and benefits countless times by:

- Providing real-time monitoring of a facility's environment, people, and assets.
- Recording the movements inside and outside a facility's environment for delayed viewing.

Many traditional video surveillance deployments are purely analog and have not yet been able to benefit from a converged network approach. Rather than looking at a massive forklift upgrade, a Cisco hybrid deployment provides an interim solution that allows customers to implement a staged migration to a fully converged IP-based solution.

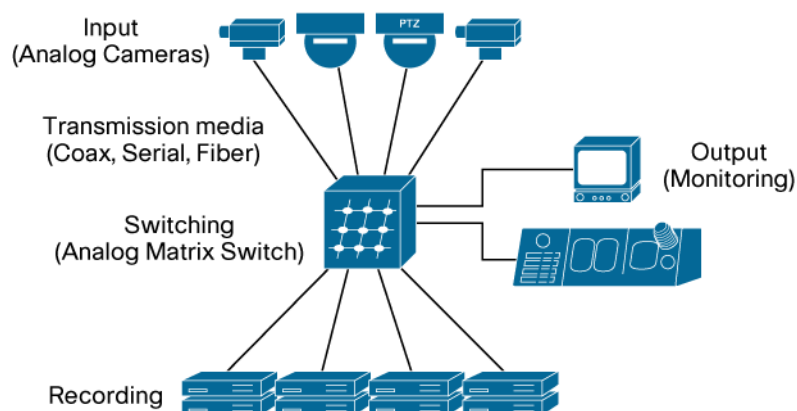
Cisco® video surveillance products can integrate with existing closed-circuit television (CCTV) systems, including matrix switches, keyboard controllers, and displays to enable new digital recording capabilities. A Cisco hybrid solution allows the user interface to remain unchanged and provides an easy migration path to a Cisco Virtual Matrix Switch solution, where the IP network infrastructure provides a dynamic transport of video streams.

Note: The Video Surveillance Solutions Reference Network Guide provides detailed information about the Cisco Virtual Matrix Switch design. This document is available here <http://www.cisco.com/go/srnd>.

### Video Surveillance Components

A typical analog video surveillance system includes the basic system components that are shown in Figure 1. In this system, video streams are monitored concurrently by using a matrix switch as an aggregation device. This approach allows video streams from different cameras to be switched to analog CCTV monitors by using special-purpose keyboard controls. Analog cameras, either fixed or pan-tilt-zoom (PTZ), typically are connected to the matrix switch by using coaxial cables for video transmission and serial cables for PTZ command and control.

**Figure 1.** Typical Analog Video Surveillance System



## Cameras

Analog cameras are a key component of a traditional video surveillance solution. They capture images in the environment and convert them to analog video. Each surveillance environment has unique camera and positioning requirements. Installing a camera in the proper environment (with proper lighting, field of view and power) can be one of the most challenging tasks of implementing the solution.

Selecting the proper camera for the system also is important. A wide variety of cameras are available to meet specific deployment requirements. These devices include cameras with PTZ functionality, day/night capabilities, vandal-resistance, weather-proofing, and many other features.

Serial PTZ data can be transmitted either in a point-to-point fashion or by using a multidrop bus. With a multidrop bus, cameras can be configured with unique system dome IDs and can be daisy-chained by using the same set of electrical wires.

## Transmission Media

To transmit video signals from analog cameras, different media can be used. Coaxial cable is one of the most common cable types, but twisted pair and fiber optic cable have also become popular.

### Coaxial Cable

A coaxial cable consists of a center conductor that is protected by an insulating spacer and a shield, which in most cases consists of a metallic web of conductors. The entire assembly is wrapped with a plastic insulating layer. Proper cable selection and installation is important because cable-related issues are the most common cause of video problems in a CCTV installation.

All coaxial cables have characteristic impedance. CCTV equipment typically uses coaxial cable with impedance of 75 Ohms. Cables are available in different Radio Guide (RG) types. RG specifies how radio frequency signals travel through a 75 Ohm coaxial cable. Table 1 lists the typical RG cables that are used in CCTV environments.

**Table 1.** Coaxial Cable Types

Type	Impedance (Ohms)	Diameter (mm)	Distance (feet)
RG-6/U	75	6	1,000–1,500
RG-11B/U	75	10	2,000–2,500
RG-59B/U	75	6.15	750–1,000

RG-59 is one of the most commonly used cables because it is small in diameter and easy to work with. RG-11 is the largest in diameter and harder to work with, but it supports longer distances.

### Fiber Optic Cable

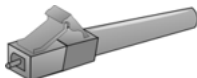
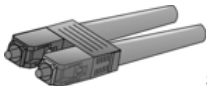

Fiber optic cable is relatively new in CCTV installations, but it has quickly become popular because it can span longer distances and accommodate more bandwidth than coaxial cable. Advantages of fiber optic cable include:

- Wider signal frequency bandwidth than coaxial cable.
- Ability to carry light-modulated signals for longer distances than coaxial cable.
- Immune to nearby signals and electromagnetic interference (EMI), so it provides a lower bit error rate.
- Multiple signals can travel on a single fiber with distances beyond 2,000 feet.

Multi-mode and single-mode are the most common fiber types in use. In multi-mode fiber, light waves are dispersed into numerous rays, called modes, which provide high speeds over medium distances. In single-mode fiber, only one light ray or mode is used to provide a transmission rate that is up to 50 times higher than multi-mode fiber.

The exact distance that can be supported by fiber cable is a function of many factors including the type of cable, signal frequency, bandwidth, and the number of splices and connectors that exist across the entire transmission distance. Multi-mode fiber typically is used in LANs with distances up to 500 meters, but it can be extended up to 5 km. Single-mode fiber is more expensive than multi-mode fiber and is more commonly used in long-haul applications with deployments of up to 60 km. Table 2 describes the more common types of fiber connectors.

**Table 2.** Fiber Connectors

Connector	Insertion Loss	Repeatability	Fiber Type
 LC	<ul style="list-style-type: none"> <li>• 0.15 dB (SM)</li> <li>• 0.10 dB (MM)</li> </ul>	<ul style="list-style-type: none"> <li>• 0.20 dB</li> </ul>	<ul style="list-style-type: none"> <li>• SM, MM</li> </ul>
 SC	<ul style="list-style-type: none"> <li>• 0.20-0.45 dB</li> </ul>	<ul style="list-style-type: none"> <li>• 0.10 dB</li> </ul>	<ul style="list-style-type: none"> <li>• SM, MM</li> </ul>
 ST	<ul style="list-style-type: none"> <li>• 0.40 dB (SM)</li> <li>• 0.50 dB (MM)</li> </ul>	<ul style="list-style-type: none"> <li>• 0.40 dB (SM)</li> <li>• 0.20 dB (MM)</li> </ul>	<ul style="list-style-type: none"> <li>• SM, MM</li> </ul>

#### Unshielded Twisted Pair

Twisted pair cable also is an alternative to coaxial cable installations because it is easier to install and less expensive. Twisted pair cable is used primarily in building or campus telecommunications installations of data and voice networks.

The Electronic Industries Association (EIA) standards define the performance of UTP (unshielded twisted pair) and cable using CATx designations. The typical categories of interest are Cat5, Cat5e, and Cat6 cabling. Most twisted pair cable plants use Cat5 cable or higher, because Cat5 provides better transmission than older UTP cables. For raw analog video, even 1% video loss can be significant. Shielded Twisted Pair (STP) cable is common in the CCTV market. In fact, STP is frequently specified for use by some vendors for their implementations. Be careful with grounding and interference when using STP and avoid mixing STP and UTP in a common cable plant.

Table 3 outlines some of the characteristics of these categories.

Most twisted pair cable plants use Cat5 cable or higher, because Cat5 provides better transmission than older UTP cables. For raw analog video, even 1% video loss can be significant. Shielded Twisted Pair (STP) cable is common in the CCTV market. In fact, STP is frequently specified for use by some vendors for their implementations. Be careful with grounding and interference when using STP and avoid mixing STP and UTP in a common cable plant.

**Table 3.** Twisted Pair Cable

Category	Type	Distance	Bandwidth	Typical Network Use
Cat5	UTP	100 m	100 MHz	100Base-T
Cat5e	UTP	100 m	100 MHz	Gigabit Ethernet
Cat6	UTP	100 m	250 MHz	10 Gigabit Ethernet
Cat7	ScTP	100 m	600 MHz	Up to Gigabit Ethernet

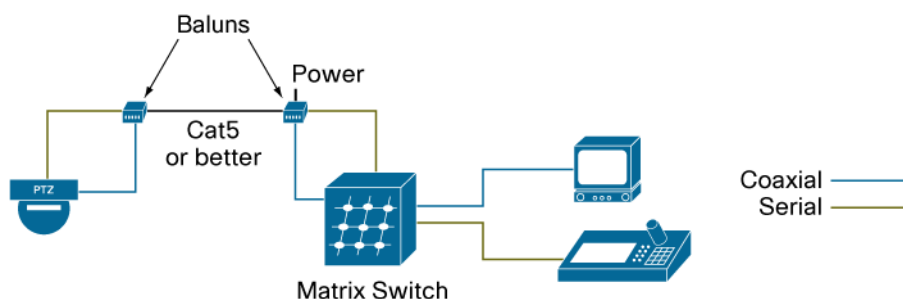
## Baluns

Most existing analog camera deployments have been installed with coaxial cable, but newer installations are introducing twisted pair and fiber optic cables. Because twisted pair is easier to install, a simple solution for new cable deployments is the use of baluns to allow twisted pair cables to transmit video signals, power, and Pan, Tilt, and Zoom (PTZ) data to analog cameras with coaxial connectors.

Baluns interconnect different cables that are not compatible, such as coaxial and twisted pair. Figure 2 shows how a balun can transmit power, video and PTZ data to a camera by using a single twisted pair cable. When using twisted pair cabling, a balun is required at each end of the cable.

By deploying Cat5 or later twisted pair cable, the same cable infrastructure can support future deployment of network devices such as wireless access points and IP cameras.

**Figure 2.** Baluns



A wide variety of baluns are available from third-party manufacturers to support a range of applications. The example in Figure 2 shows a Cat5 cable, but other baluns can be used to convert from Cat5 to coaxial. Be aware that baluns are unmanaged devices that introduce another point of failure and can be difficult to troubleshoot.

### Serial Connectivity

In a CCTV environment, PTZ data is transmitted using serial communications. Table 4 shows the most common serial protocols and some of the relevant characteristics of each:

**Table 4.** Serial Cables

Specification	RS232	RS422	RS485
Maximum Cable Length	20 m	500 m	1,200 m
Maximum Data Rate for RS232	20 kb/s		
Maximum Data Rate for RS422/RS485 (50 m–1,200 m)		10 Mb/s–200 kbps	10 Mb/s–200 kbps
Receiver Input Voltage Range	+/- 15V	-10V to +10V	-7V to +12V
Mode of Operation	Single-ended	Differential	Differential

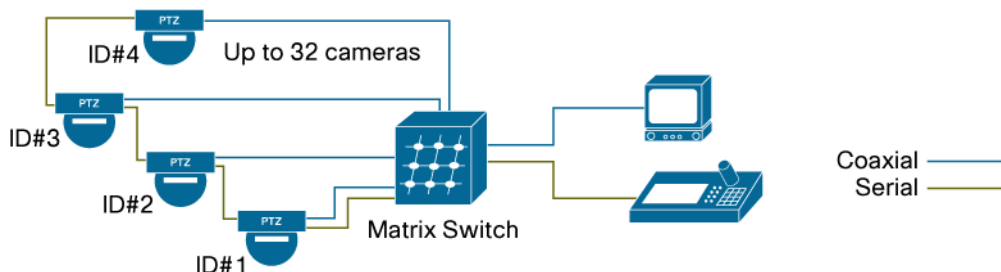
RS-232C is a serial communications standard that is used to interface serial devices over cable lengths of up to 20 meters. RS-232C was originally intended to support modem and printer applications, but it has been expanded to support other applications. RS-422 communications can carry data over longer distances and at higher rates and resist noise interference better than RS-232C.

RS-485 is a variation of the RS-422 standard and is based on a master-slave architecture, in which the master initiates all transactions and the slave only transmits when instructed to do so by the master. RS-485 allows up to 32 devices to communicate at distances up to 500 meters, but the number of devices and distance can be extended using repeaters. A variety of connectors are supported, including RJ11, RJ45, DB9 and DB25.

RS-485 offers a multi-drop capability, in which up to 32 cameras may be configured with unique IDs to receive serial data. Figure 3 shows an example with four cameras that use the same RS-485 bus to transmit PTZ data. A multi-drop configuration typically requires two terminations, one at each end of the network.

Up-the-coax transmission, where electrical signals such as PTZ data communications are transmitted over the same coaxial cable is not supported.

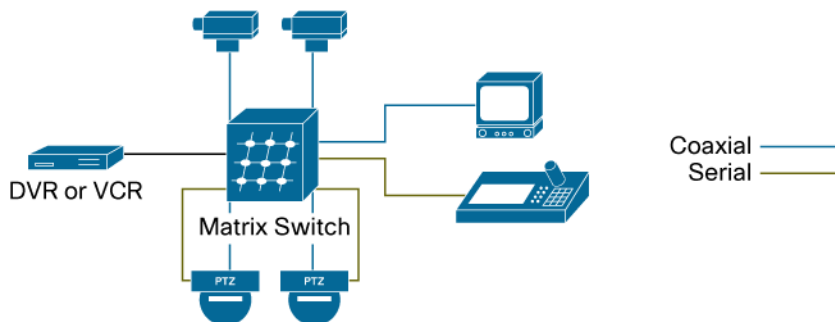
**Figure 3.** Multi-drop Bus Configuration



### Matrix Switches

In a traditional video surveillance environment, a matrix switch is the core element of the solution. A matrix switch acts as an array of video inputs and outputs, allowing users to control the display of different cameras and to switch control of PTZ functions. Figure 4 shows a traditional CCTV system with a matrix switch, where analog video streams are aggregated, controlled, and dispersed to different monitor displays by using analog switching technology.

**Figure 4.** Traditional Matrix Switch



A typical matrix switch can be programmed to display a video stream from any camera on any monitor either manually or by using automatic switching sequences. Some matrix switches include salvo switching capabilities, which allow any number of monitors to be selected to switch as a synchronized group. Also common is the ability to interface with external alarms or contact closures and to display video that is triggered by designated events.

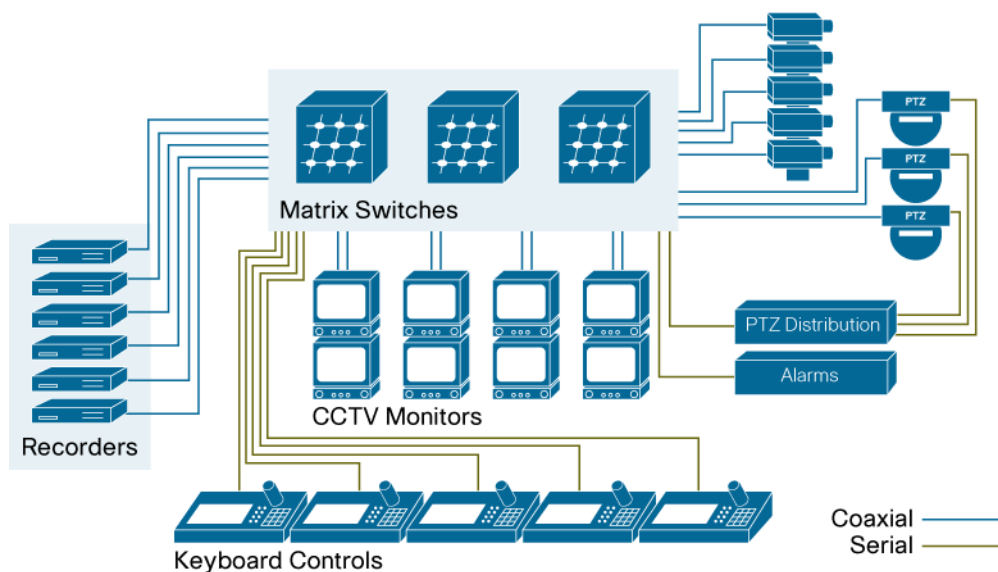
Matrix switches can scale from a small system with a few cameras to an enterprise-class switch that can support thousands of cameras and hundreds of monitors.

In a large matrix switch environment, the system may be configured with many components, including:

- Main CPU bay—A modular system that contains the system processor, power supply, and several video input and output modules.
- Video input module—Accepts input from cameras and other video sources.
- Video output module—Provides outputs to monitors and VCRs.
- Monitor expansion bay—Provides connectivity to several monitors. Typically required in deployments with more than 32 monitors and can also accommodate several keyboards.
- PTZ data distribution unit—Communicates with PTZ cameras typically by using RS-422 data transmission.

The high-level example in Figure 5 shows how a matrix switch system can grow to accommodate many cameras, monitors, and recording devices. In this design, a centralized monitoring facility houses all keyboards and CCTV monitors, which requires the cable infrastructure to be routed to a single location. While this configuration is able to grow to a large number of devices, the cable infrastructure does not allow video to be viewed from other stations at the facility or from remote locations.

**Figure 5.** Traditional Matrix Switch





## Recording

Most video surveillance environments require recording capability either to meet regulatory requirements or to facilitate the investigation of events that have occurred.

Many traditional installations that relied on video cassette recorders (VCRs) now record events on hard disks instead of VHS tapes. VCR recording systems are cumbersome and can make timely retrieving of video difficult. Other drawbacks include:

- VCRs typically are dedicated to provide only recording or playback. To view video during an investigation, separate record and playback devices are required.
- Device failures can go undetected for a long time. VCR or DVR technology usually does not have device monitoring capabilities that notify an operator when a device fails. In contrast, network-based recording provides management features to immediately send alerts when a failure occurs.
- To review recorded video from a remote location, tapes must be sent to the investigation center or an officer must visit the remote facility. In a network-based environment, video streams can be transmitted immediately to any network location for review.

With the declining availability of VCRs and to address recording limitations, other technologies have emerged to enhance video surveillance recording. For the most part, DVR are stand-alone set-top boxes with video inputs and basic recording software.

Solutions that are based on digital video recorders (DVRs) address some limitations of VCRs, however, they do not provide the scalability and flexibility that an IP-network-based system solution can provide such as integration with other business systems, greater access to video, and the use of video analytics for safety, customer satisfaction, and operator productivity.

While tape-free DVR recording provides an upgrade in functionality over traditional VCRs, the technology still exposes limitations, such as:

- To view recorded events, a PC-based system typically is required, which prevents an operator from using a familiar CCTV keyboard interface.
- The cable infrastructure is centralized and typically relies on the same cable infrastructure that was used to support a VCR installation.
- Only a few channels are recorded per device.

## Chapter 2: Cisco Stream Manager Hybrid Solution

In a Cisco hybrid solution, a matrix switch seamlessly integrates with a Cisco Video Surveillance digital recording system and provides a staged transition to digital video without changing an interface that is familiar to users. This integration also provides a foundation for migrating to a complete IP infrastructure. As part of this integration, operators can view recorded video from analog monitors instead of using a separate viewing station that is dedicated to video review. This integration also allows operators to continue using familiar keyboards and joysticks and improves response time when users investigate events. In a multi-display environment, operators can simultaneously investigate a recorded event and monitor other cameras.

The Cisco hybrid solution offers several benefits to an environment with a traditional matrix switch including:

- Compatibility with a wide range of matrix switches and keyboards. Table 6 and Table 7 on Page 4-1 provide a list of supported matrix switches, cameras, and keyboards.
- Enhanced keyboard functionality that provides immediate video review by using customized key sequences. An operator can also play back video from a specific date and time.
- Recorded video from several cameras may be reviewed at the same time on multiple monitors.
- Simultaneous review and recording of a single video stream.
- Support for redundant recorders for high-availability of recorded video streams.
- Extensive control for review of recorded video, including instant replay, fast forward, rewind, pause, frame advance/reverse, digital zoom, time/date search, still JPEG snapshot image capture, and more.
- System interoperability, which allows operators to use keyboards and joysticks from third-party manufacturers.
- A migration path to a complete Cisco virtual matrix switch design.

Note: The *Video Surveillance Solutions Reference Network Guide* provides more details about the Cisco Virtual Matrix Switch Design. This document is available here:

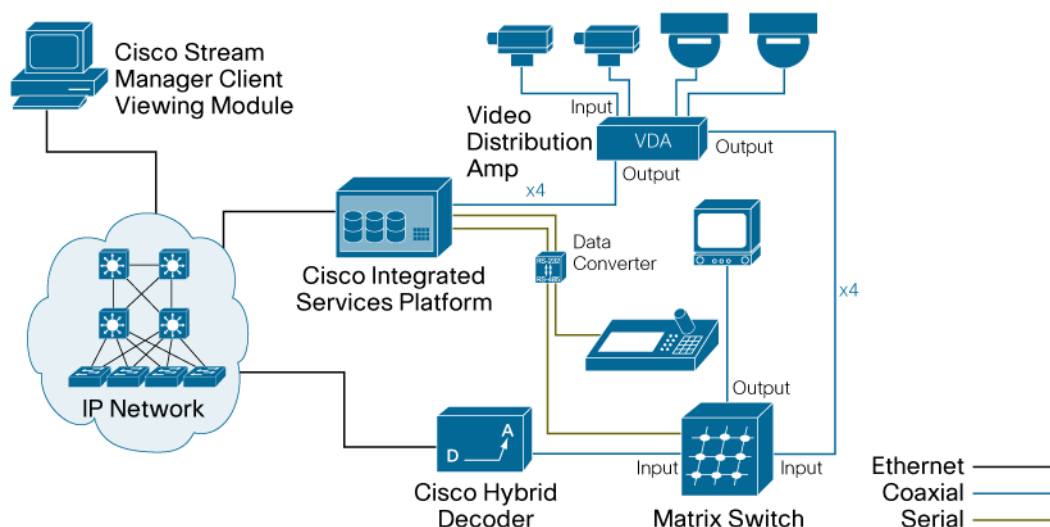
<http://www.cisco.com/go/srnd>

## Hybrid Solution Components

A Cisco hybrid solution is an ideal upgrade for organizations that use video matrix switches. With minimum affect on the existing system, a hybrid solution can add digital recording and instant retrieval features, improving system and operator efficiency. The recording systems are the only components that are replaced. The matrix switch, video cameras, and keyboards remain.

Figure 6 shows a complete hybrid solution that is integrated with a third-party matrix switch.

**Figure 6.** Cisco Hybrid Design



In this design, an Integrated Services Platform (ISP) records video streams and performs digital playback operations that are requested by an operator. The Cisco system integrates with the third-party matrix switches and keyboards that are listed in Table 6 and Table 7 on Page 4-1.

In a hybrid solution, the following Cisco components are introduced to perform digital recording and retrieval:

- Cisco ISP. This device performs digital recording and playback of video streams. The Cisco Video Surveillance Stream Manager Software that runs on the ISP supports a modular deployment and provides features for high-availability and system expansion.
- Cisco data converter. A Cisco data converter is required to integrate some matrix switches with the Cisco hybrid solution. The data converter converts serial signals between RS-232 and RS-485/RS-422. Cisco offers several data converter models to match various third-party matrix switches. A data converter is required for each keyboard that needs access to playback features.
- Cisco hybrid decoders. The hybrid decoder accepts digital recorded video from an ISP and decodes it into analog video, which is passed to the matrix switches. The hybrid decoder connects to a dedicated analog video input port on the matrix switch. The number of hybrid decoders in a solution should match the number of keyboards that require simultaneous playback functionality. Note that the hybrid decoder is a different product than the IP gateway decoder.
- Cisco Stream Manager Client Viewing Module. This PC-based application may be used to display live or recorded video streams from the ISP.

Table 5 lists the Cisco products that are used in a hybrid solution.

**Table 5.** Cisco Part Numbers

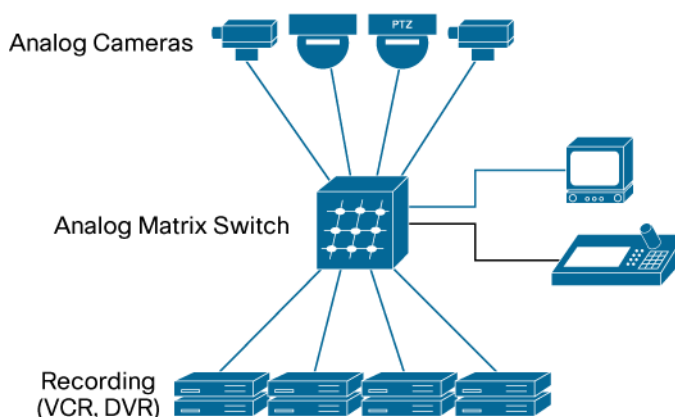
Part Number	Description
<b>Integrated Services Platforms</b>	
CIVS-SP8ECISP-2000	Cisco VS Integrated Services Platform with 8 encoders, 2TB RAID (expandable)–2RU
CIVS-SP8ECISP-6000	Cisco VS Integrated Services Platform, 8 input, 6TBytes (RAID5)
CIVS-SP12-ISP-6000	Cisco VS Integrated Services Platform, 12 input, 6TBytes (RAID5)
<b>Hybrid Decoders</b>	
CIVS-SG1ADISP-C16	Cisco VS 1 port ISP Decoder Card for FE & GE Chassis
CIVS-SG1ADISP-FE	Cisco VS 1 port Standalone ISP Decoder
<b>Data Converters</b>	
CIVS-KYBD2232=	Cisco VS KEYBOARD 232 to RS422/485 ADAPT GENERIC
CIVS-KYBD2232-AD=	Cisco VS KEYBOARD 232 to RS422/485 ADAPT American Dynamics
CIVS-KYBD2232-B=	Cisco VS KEYBOARD 232 to RS422/485 ADAPT FOR BOSCH
CIVS-KYBD2232-P=	Cisco VS KEYBOARD 232 to RS422/485 ADAPT FOR PELCO
CIVS-KYBD2232-U=	Cisco VS KEYBOARD 232 to RS422/485 ADAPT FOR Ultrak
<b>Stream Manager Client Viewing Module</b>	
CIVS-SM-CL30=	Stream Manager Client Viewing Module

## Integration Steps

Integrating the Cisco hybrid solution with an existing video surveillance environment requires only a few steps. A typical environment includes a matrix switch that functions as the central connecting point for all analog cameras, keyboards, monitors, and recording devices.

As shown in Figure 7, each device in the system requires a unique port on the matrix switch, either for input or output. The matrix switch can display video streams from different cameras on different CCTV monitors and direct video streams to recording devices.

**Figure 7.** Existing Matrix Switch



The following sections explain the general steps for integrating the Cisco hybrid solution with an existing video surveillance environment.

### Step 1: Remove legacy recording systems

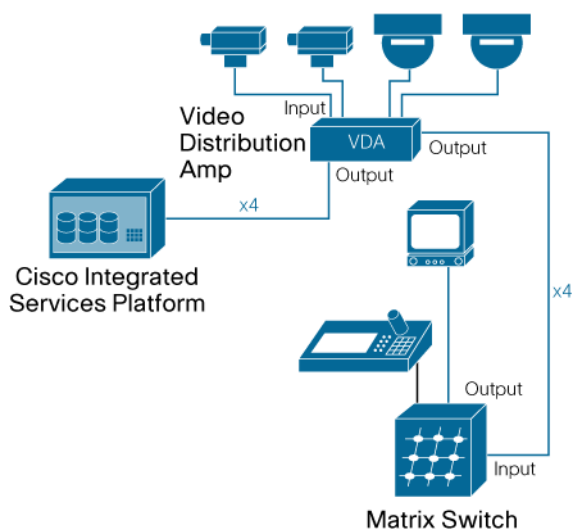
The first integration step is to remove legacy recording systems and introduce a Cisco ISP. The ISP provides 8 or 12 encoding ports (depending on the model) that connect directly to cameras and allow the ISP receive and record video streams simultaneously.

Video streams that are sent to the matrix switch need to be routed through the ISP. A simple way to direct the video streams from the cameras is to use video distribution amplifiers or other looping methods such as looping ports on a matrix switch.

As shown in Figure 8, a video distribution amplifier receives four video streams from analog cameras and splits each signal into two streams. Four coaxial cables connect to input ports on the matrix switch and four coaxial cables connect directly to the encoder ports on the ISP.

Note: The ISP is connected to the IP Network, but this connection is not shown in this figure simplicity.

**Figure 8.** Legacy recording systems

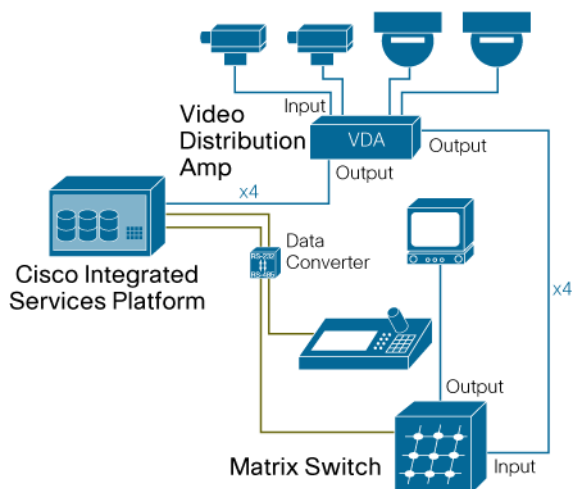


### Step 2: Introduce a Cisco Data Converter

A Cisco data converter is inserted between the matrix switch and the CCTV keyboard to allow the ISP to intercept keyboard commands that identify when an operator wants to switch from live to recorded video. For some systems, the data converter switches serial signals from RS232 to either RS-485 or RS-422 via a dip switch setting. The Stream Manager Software that runs on the ISP interprets the command structure and determines if a command is intended for the matrix switch or intended to display digital playback video.

Figure 9 shows how a Cisco data converter connects to the ISP, the keyboard, and the matrix switch. Note that the keyboard is no longer connected to the matrix switch.

**Figure 9.** RS-232–RS485 Data Converter

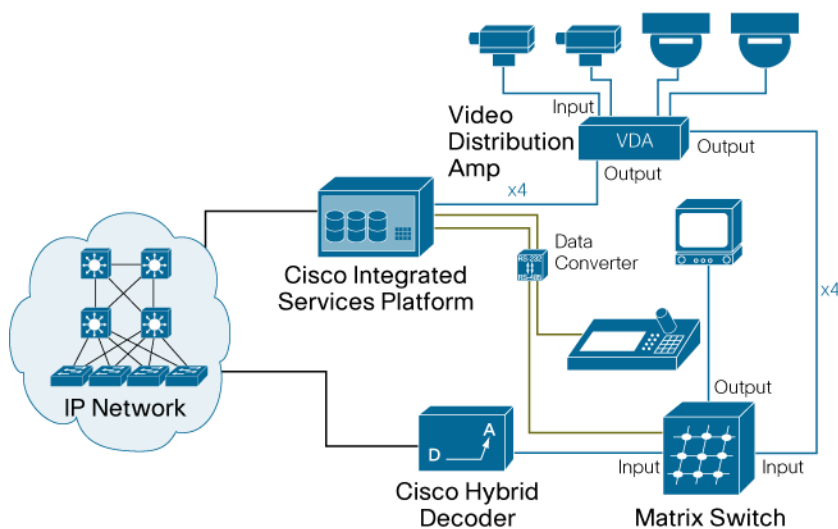


### Step 3: Introduce a Cisco Hybrid Decoder

When a playback feature is requested, the hybrid decoder retrieves the video stream from the proper ISP and delivers it to the proper matrix switch port. The background processing is transparent to operators.

As shown in Figure 10, a hybrid decoder connects via a 10/100BASE-T Ethernet port to the IP network and via a coaxial cable to the matrix switch. An input port from the matrix switch is reserved to act as the input from the hybrid decoder. When an operator requests a playback feature from the keyboard, the matrix switch is instructed to switch video from the reserved input port to the current monitor port.

**Figure 10.** Cisco Hybrid Decoder



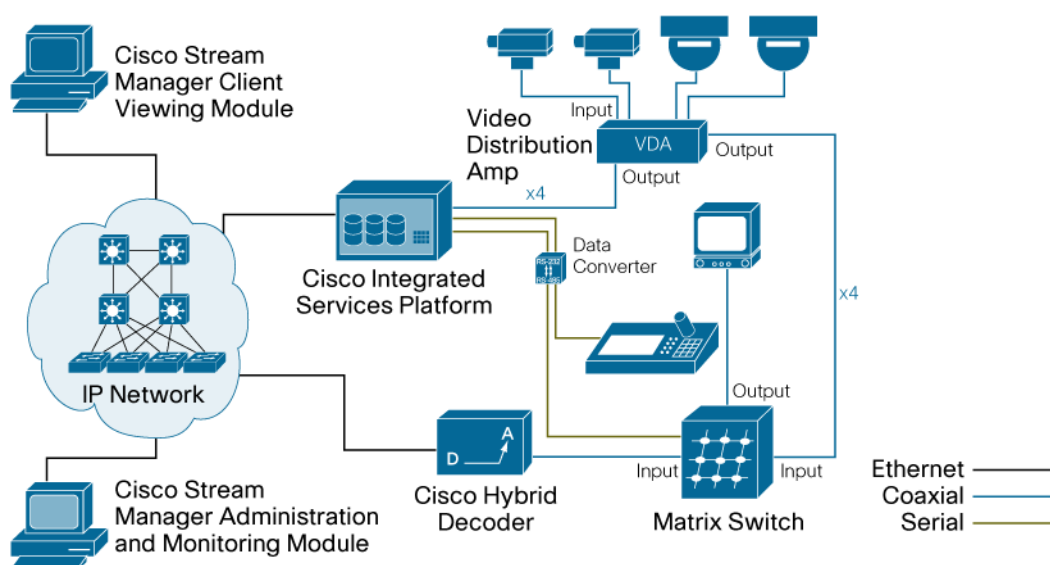
#### Step 4: Cisco Stream Manager Modules

Figure 11 shows a complete hybrid system integrating with a matrix switch to provide playback functionality. The system can easily scale to support thousands of cameras and allows operators to use other Stream Manager utilities for added functionality.

While the hybrid solution can work without the Cisco Stream Manager Client Viewing Module, this Windows-based software provides a flexible way to view streams from any network location. In addition, the software allows exporting video streams to a video file for review.

The Cisco Stream Manager Administration and Monitoring with Failover Module provides system health information and alarm capabilities for all Cisco Video Surveillance devices in the network. This module is required in a failover environment, as explained in the next chapter.

**Figure 11.** Hybrid Design Solution



#### Viewing Live and Recorded Video

When an operator presses a key sequence on the keyboard to retrieve recorded video, the ISP, data converter, and hybrid decoder provide the functionality to identify the request and display the video on the appropriate monitor.

#### Live Viewing Operation

For live viewing operations, the ISP monitors for special key sequences that indicate a request for video playback. If no playback requests are received, the Stream Manager software that is running on the ISP sends the serial commands back to the matrix switch. This step typically takes less than one second and an operator does not notice any delay when switching video streams on the matrix switch.

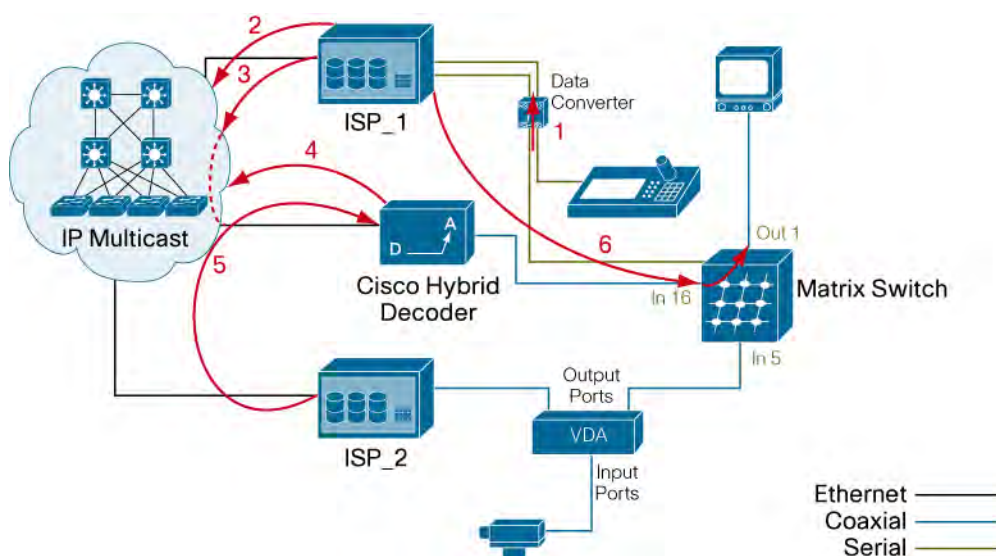
## Recorded Viewing Operation

When an operator requests a playback feature, the ISP detects the request and responds with the proper playback feature. Figure 12 shows the interaction between the ISP, data converter, and hybrid decoder when an operator who is using Monitor 1 requests to view recorded video from Camera 5 by pressing the Instant Replay button.

Note: Appendix A provides additional details about the network communication that takes place during a video playback and describes the TCP/UDP port numbers that are used.

The hybrid decoder is connected to the matrix switch on input port 16 and video for Camera 5 is recorded on the ISP named ISP\_2.

**Figure 12.** Example—Playing Recorded Video



In Figure 12, live viewing is taking place and no playback requests have been received. Keyboard control commands are passed through the ISP to the matrix switch transparently until an operator requests the playback of recorded video. Here is an example of the processes that occur when an operator requests playback:

1. While viewing video from Camera #5, an operator presses a key sequence requesting an instant replay of Camera#5. ISP\_1 receives this key sequence and detects that the user wants to play recorded video. The default rewind time is 30 seconds, but this value may be changed as shown on Page 5-12.
2. Through the data converter, ISP\_1 reads the currently selected camera from the matrix switch and sends a device discovery request for an available hybrid decoder.
3. If a hybrid decoder is available, ISP\_1 sends the peripheral ID (Camera#5) and start date/time to the hybrid decoder. If no hybrid decoders are available, the request terminates and no visual changes take place on an operator's monitor.
4. The hybrid decoder sends to all recorders, via multicast, a discovery request for the ISP that has recorded peripheral ID 5 at the specified start date/time.
5. ISP\_2 responds to the hybrid decoder and a new TCP session is established between ISP\_2 and the hybrid decoder.



6. Because the hybrid decoder is configured for input port 16 on the matrix switch, ISP\_1 instructs the matrix switch to switch video from port 16 to the monitor that is selected (switch video input #16 to monitor #1). The monitor displays the recorded video on Monitor 1.

ISP\_1 waits for user input and processes features such as fast-forward and rewind. When an operator presses a key sequence to stop the digital video, ISP\_1 instructs the hybrid decoder to terminate the session with ISP\_2 and instructs the matrix switch to resume live video from camera 5 to monitor 1.

Note: Tests in a lab environment show that the average retrieval time for playback video is approximately 1.5 seconds and that it takes approximately one second to go back to live viewing after an operator stops digital playback.

## Chapter 3: Failover and Recovery

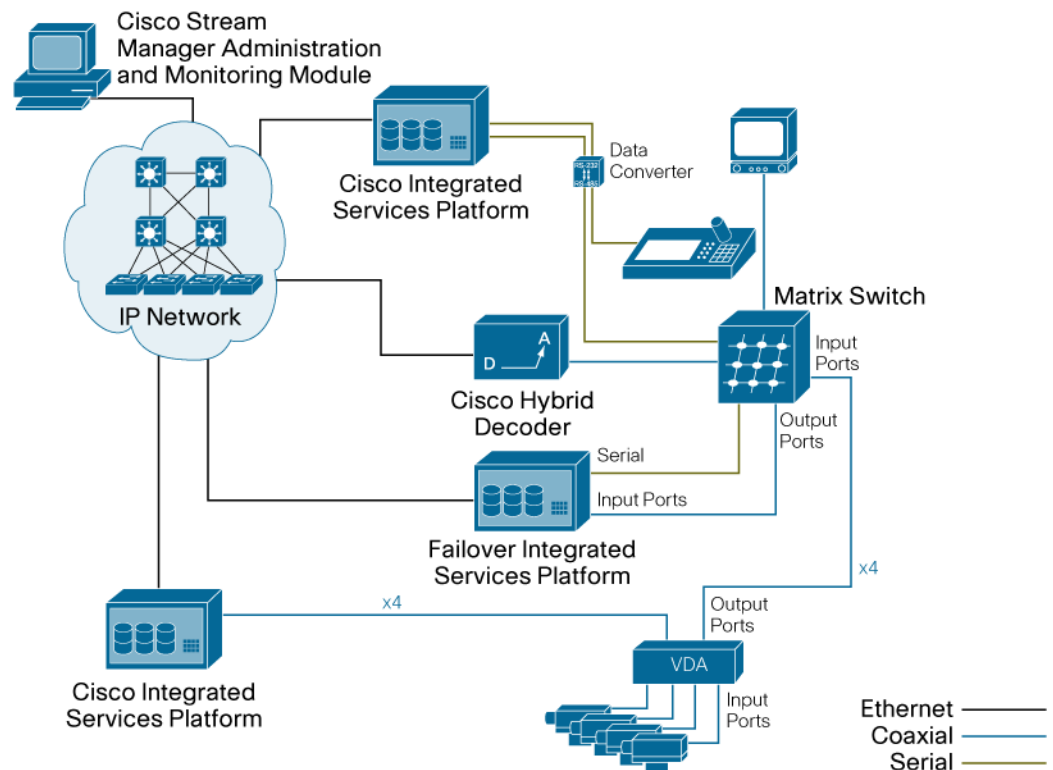
Traditionally, the CCTV industry has considered recorders to be a single point of failure and has avoided recording many video streams on a single device to minimize risk. The Cisco Integrated Services Platform provides recording for many of video cameras and introduces high-availability features that record video streams during failure events.

### Matrix-based N+N Redundancy

To enhance system-level redundancy, Cisco provides a matrix-based N+N redundancy solution, which allows one or more recorders to act as failover recorders for any number of primary recorders.

If a primary ISP fails, the streams that it was recording are recorded by a failover ISP. The failover ISP can also record single encoder ports during a failure. Playback features that were available before the failure, such as time/date search and instant replay, remain available to the operator. Figure 13 shows how an ISP can act as a failover ISP for other ISPs.

**Figure 13.** Matrix-Based N+N Redundancy



The following equipment and software is required to provide redundancy:

- Cisco equipment:
  - At least one dedicated failover ISP. This ISP acts as the failover unit for other ISPs in the environment. It must be configured in failover mode and to record only when a failure is detected. The number of video streams to be backed up depends on the number of

available encoder ports (8 or 12) on the failover ISP. More than one ISP may be configured as a failover ISP for any number of primary ISPs.

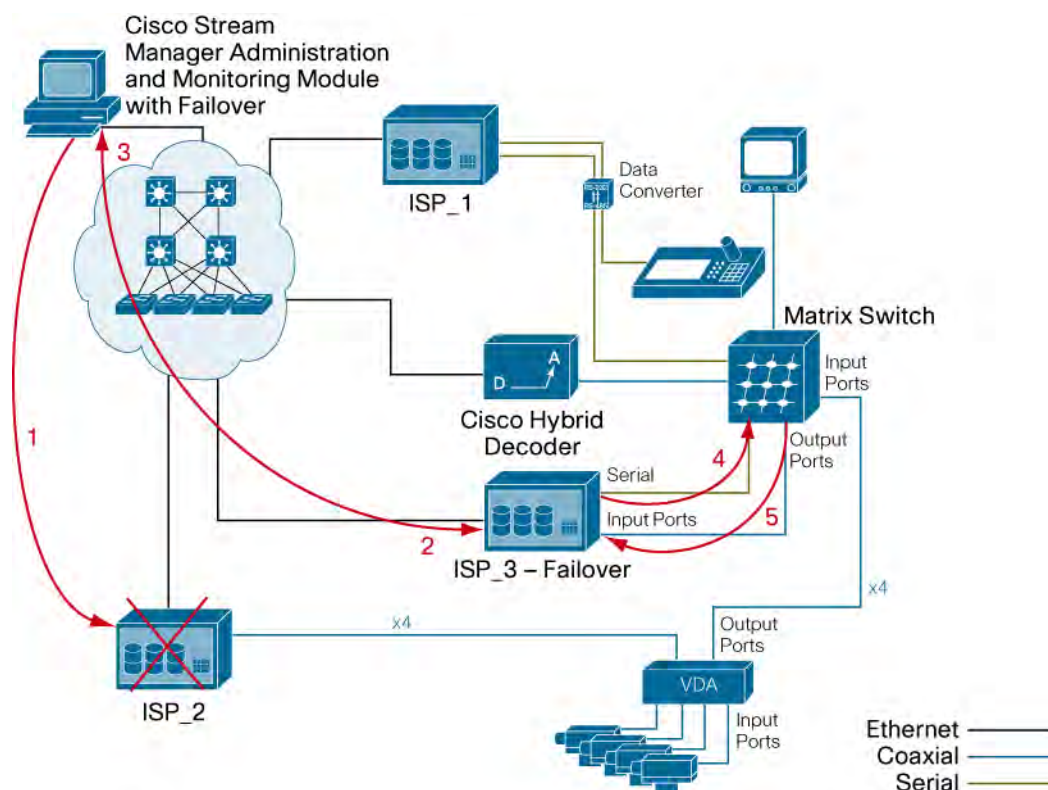
- The Cisco Stream Manager Administration and Monitoring with Failover Module. This Windows-based software provides system health information, including information about server and bandwidth use of all Cisco Video Surveillance devices in a network, and central alarm capabilities. The Administration and Monitoring with Failover Module initiates a failover when either a single encoder port or an entire ISP fails, redirecting video streams to a failover ISP. The module also maintains a history log of failure events.
- Third-party equipment:
  - A supported matrix switch (see Table 6 on Page 4-1) with available monitor output ports. The monitor output ports are connected to the encoder ports of the ISP and become active when a failure is detected. The number of available monitor output ports must be equal to or greater than the number of video streams to be backed up.
  - A serial cable to connect the matrix switch to the failover ISP. For more detailed information about matrix switches, see the “Manufacturer-Specific Configurations” chapter. One serial cable can support failover for more than one failover ISP.
  - A CCTV keyboard that is dedicated to selecting video streams and requesting digital playback features.

To minimize the potential affect of power failures when using redundant devices, follow traditional networking designs and use several electrical circuits.

### **How a Failure is Detected**

The Administration and Monitoring with Failover Module must be active and able to reach all ISPs that are in the environment, including the failover ISP. When the Administration and Monitoring with Failover Module detects a failure on an ISP, it polls the affected device three times, and then redirects the video streams to the failover ISP. The refresh interval for polling is a system-wide configuration option on the Stream Manager Administration and Monitoring with Failover Module, and may be changed from the default value.

Figure 14 shows a deployment in which ISP\_3 is dedicated as a failover ISP and records video streams if a failure occurs.

**Figure 14.** Failover Scenario

The following events take place if ISP\_2 fails:

1. The Administration and Monitoring with Failover Module sends discovery request messages every five seconds to maintain a list of available Cisco Stream Manager video surveillance devices on the network. If a device does not respond to these discovery requests, the Administration and Monitoring with Failover Module waits three times longer than the refresh interval before logging a failure. The default refresh interval is 60 seconds, but this value may be configured as shown on Page 5-17. When the system logs a failure, it displays a notification on the Administration and Monitoring screen and generates an audible alert.
2. The Administration and Monitoring with Failover Module sends a discovery request for available failover ISPs. ISP\_3 responds and specifies the number of free channels that it has available for failover recording.
3. The Administration and Monitoring with Failover Module informs the failover ISP which video streams need to be recorded. A new message is sent every three seconds with details on which port to back up, until the failover ISP reports that there are no longer free channels for recording.
4. Through the serial cable between the matrix switch and the failover ISP\_3, ISP\_3 instructs the matrix switch to redirect video streams to the output ports that are reserved for failover.
5. The redirected video streams are recorded on the failover ISP.
6. If an operator requests video playback during a failure, the retrieval steps are the same as Step 1 through Step 6 that accompany Figure 12 on Page 2-8. These steps explain how video is retrieved from ISP\_3.

Note: If the data converter was connected to ISP\_2, recording on the failover ISP would still take place, but an operator would not be able to request playback video by using that keyboard. An

alternate keyboard that is connected to any ISP on the network could retrieve recorded video. During a failure, the Stream Manager Client Viewing Module cannot retrieve recorded video from the failover ISP.

Note: In a system that is configured with a 20 second refresh rate, typical recovery times are approximately 75–80 seconds. During this time, video streams from the failed device are lost.

### Single Port Failure

The failover solution can also monitor when a single port on an ISP fails or loses video. Such a situation can occur for several reasons, such as a hardware malfunction or a faulty cable.

When a single port loses video, the following steps take place:

1. The ISP is still able to communicate on the network, so it reports the port failure event directly to the Administration and Monitoring with Failover Module, sending a video loss alarm that specifies the peripheral ID of the failed port. Figure 36 on page 5-14 illustrates this configuration.
2. The Administration and Monitoring with Failover Module informs the failover ISP which video stream needs to be recorded.
3. The failover ISP notifies the matrix switch (through the serial cable) to redirect video streams to the first available output port that is reserved for failover.
4. The redirected video stream is recorded on the failover ISP.
5. If an operator requests video playback during a failure, the retrieval steps are the same as Step 1 through Step 6 that accompany Figure 12 on Page 2-8. These steps explain how video is retrieved from the failover ISP.

### Recovering from a Failure

The failover ISP continues to record until the failure is corrected. When a failed device becomes operational, it begins to record video streams and responds to discovery requests from the Administration and Monitoring with Failover Module. After receiving these responses for approximately 10 seconds, the Administration and Monitoring with Failover Module redirects video streams to the primary ISP.

The failover ISP instructs the matrix switch to stop sending video on the output ports and the Administration and Monitoring with Failover Module notifies each failover port to stop recording. It does it in sequence, by notifying one port and waiting for three seconds before notifying the next port. The primary ISP resumes recording video.

Video streams that were recorded on the failover ISP remain on the failover ISP and are not transferred to the primary ISP.

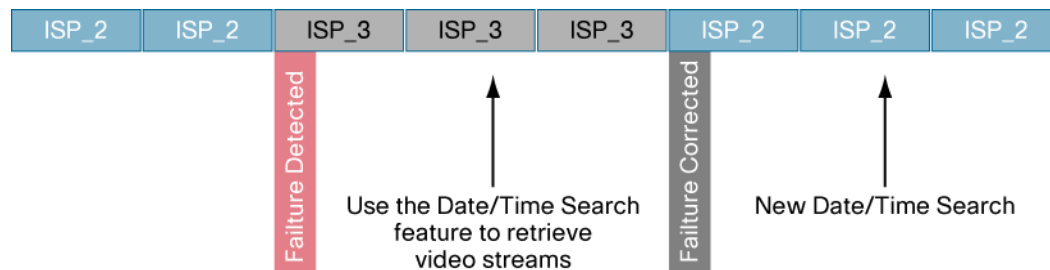
### Retrieving Video from a Failover ISP

After the primary ISP is restored, video playback or exporting is performed on the primary ISP. To retrieve video that was recorded during a failure, an operator performs the steps that accompany Figure 12 on Page 2-8. When doing so, an operator also must specify the start time and date for the desired video.

As shown in Figure 15, if operators requests to review video streams that fall within the time of the failure, video is retrieved from the failover ISP. The video can be played until the point where the

primary ISP was restored. To play recorded video past that point, an operator must perform a new date/time search. This procedure is the same, whether an operator is using the Stream Manager Client Viewing Module or a CCTV keyboard.

**Figure 15.** Failover Timeline



To perform a date/time search from the Stream Manager Client Viewing Module, right-click the appropriate camera, choose View Recorded > Go to Time/Date..., and specify the start date and time, as shown in Figure 16.

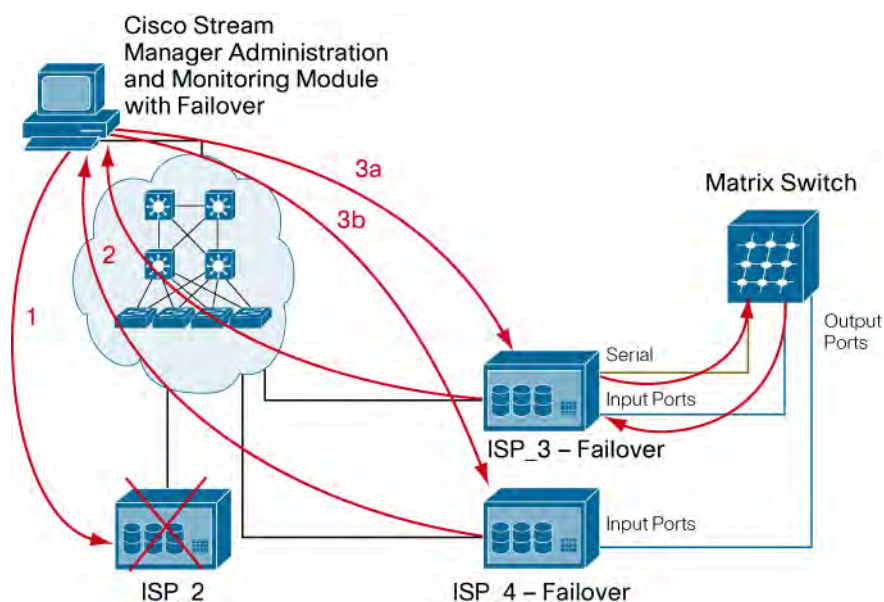
**Figure 16.** Start Date and Time Selection



### Failover and Recovery with two Failover ISPs

The operation on a system with two failover ISPs is similar to the example that is shown on Page 3-3. By sending the periodic discovery requests, the Stream Manager Administration and Monitoring with Failover Module remains aware that more than one ISP is configured in failover mode.

Figure 17 shows an example in which ISP\_3 and ISP\_4 are configured as failover ISPs and record video streams for other video ports or ISPs that fail.

**Figure 17.** Failover with two ISPs

The following events take place if ISP\_2 fails:

1. The Administration and Monitoring with Failover Module determines that ISP\_2 has failed because the module has not received replies after three times the period of the configured refresh interval.
2. The Administration and Monitoring with Failover Module sends a discovery request for available failover ISPs. ISP\_3 and ISP\_4 respond and specify the number of free channels for failover recording.
3. The Administration and Monitoring with Failover Module notifies the first available failover ISP (which could be ISP\_3 or ISP\_4) of the port on which to begin recording. Assuming that ISP\_3 is first:
  - a. The Administration and Monitoring with Failover Module informs ISP\_3 which video stream to begin recording. Through the serial cable between the matrix switch and ISP\_3, ISP\_3 instructs the matrix switch to redirect video streams to the first available output port that is reserved for failover.
  - b. The Administration and Monitoring with Failover Module waits for three seconds, then informs ISP\_4 which port to begin recording. Because ISP\_4 does not have a serial cable that connects to the matrix switch, ISP\_4 requests that ISP\_3 instruct the matrix switch to redirect the next video stream to the next available output port.
1. The Administration and Monitoring with Failover Module continues to assign failover ports in sequence until the failover ISPs report that there are no free channels available.
2. If an operator requests video playback during a failure, the retrieval steps are the same as Step 1 through Step 6 that accompany Figure 12 on Page 2-8. These steps allow video to be retrieved from either ISP\_3 or ISP4.

## Chapter 4: Third-Party Equipment Support

Table 6 provides information about the third-party matrix switches that integrate with the Cisco hybrid solution. Table 7 provides information about the keyboards that integrate with the solution.

**Table 6.** Analog Video Matrix Support

AD Sensormatic	Pelco	Bosch	Honeywell (Ultrak or Maxpro)
Mega Power AD 1024	CM 9760	LTC 8900	Maxpro 1000
Mega Power AD 2000	CM9770	LTC 8800	
AD 168		LTC8600	
		LTC 8500, 8300, 8200	

**Table 7.** Keyboard and System Features

	AD	Bosch	Honeywell* (Ultrak or Maxpro)	Pelco*
<b>Keyboard Functions</b>				
Keyboard Models	AD2088A	IntuiKey-Universal	HEGSA002/KEGS5300	KB-9760
Instant Replay	Yes	Yes	Yes	Yes
Fast Forward	Yes	Yes	Yes	Yes
Rewind	Yes	Yes	Yes	Yes
Pause	Yes	Yes	Yes	Yes
Frame Advance	Yes	Yes	Yes	Yes
Frame Rewind	Yes	Yes	Yes	Yes
Digital Zoom	Yes	Yes	Yes	Yes
Image Position	Yes	Yes	Yes	Yes
Digital Zoom FF	Yes	Yes	Yes	Yes
Digital Zoom RW	Yes	Yes	Yes	Yes
Time/Date Search	Yes	Yes	Yes	Yes
Send JPG Image	Yes	Yes	Yes	Yes
<b>System Functions</b>				
System Clock Sync	NTP or Stream Manager	DB9-Console port RS-232	DB9-Keyboard port RS-232	DB9- MDA port RS-422
Failover Capability	DB9-Keyboard port RS-232	DB9-Console port RS-232	DB9-Keyboard port RS-232	DB9-ASCII port RS-422
Matrix On-Screen display disable during playback	Yes	Yes	Yes	Limited

\* Keyboard has been tested only with a hybrid system and is not supported in a virtual matrix switch environment.



## Chapter 5: Basic Configuration

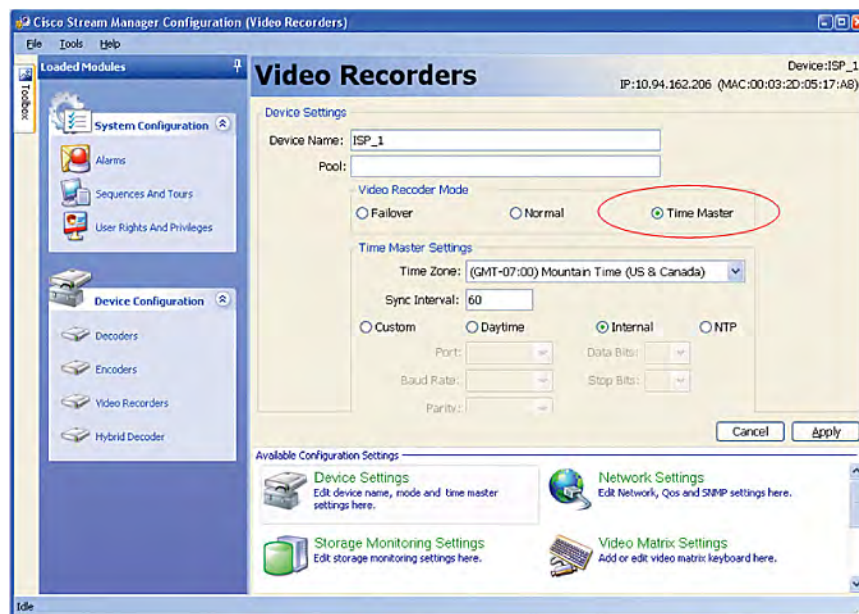
This section describes the general steps that are required to configure a hybrid integration with a matrix switch. Detailed configurations for matrix switches from various manufacturers are provided in Chapter 6.

### Configuring the Integrated Services Platform

To configure an ISP for use in a hybrid environment, it must be configured with the proper mode and IP address and each of the encoder ports must be configured with the proper video resolution and frame rate.

Using the Stream Manager Configuration Module, select the ISP and configure it with the proper device name and mode. In Figure 18, ISP\_1 has been configured as Time Master. For more details about Time configurations, see the “Time Synchronization” section.

**Figure 18.** Device Settings



Click the Network Settings tab and configure the proper IP address, as shown in Figure 19.

Figure 19. Network Settings



The keyboard data converter connects to a selected ISP to allow the ISP to receive playback commands from the keyboard and redirect recorded video to the appropriate monitor. Figure 20 shows that the video switch type has been changed to Phillips to support the Bosch matrix switch. (Bosch acquired the Communications, Security, and Imaging business unit from Philips.)

While playing live video, the monitor displays the on-screen display (OSD) of the matrix switch, but during playback, the OSD displays the date in the format that is configured in the **Time Date Format** field for the ISP. The ISP instructs the matrix switch to alternate between these displays.

Figure 20. Integrated Services Platform Matrix Settings



Each encoder port must be enabled and configured with the proper camera or peripheral ID and video settings. In Figure 21, Port 4 has been configured as Camera ID 4, 4CIF Video Resolution, and 30 fps Frame Rate.

**Figure 21.** Port Video Settings



### Configuring the Cisco Hybrid Decoder

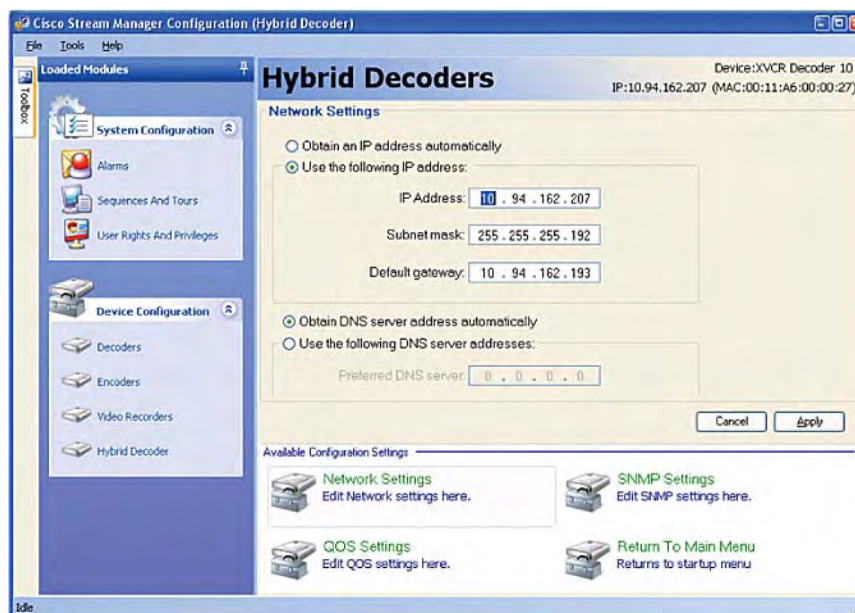
Using the Stream Manager Configuration Module, configure each hybrid decoder in the hybrid environment. To do so, choose the proper hybrid decoder and click **Device Settings**. Figure 22 shows a hybrid decoder configuration that includes a device name and a blank Pool field. For more details about hybrid decoder pools, see the section on "Hybrid Decoder Pools".

**Figure 22.** Device Settings



Click the **Network Settings** tab and configure the proper IP address, as shown in Figure 23.

Figure 23. Network Settings



To specify the Matrix Input port to be used by the hybrid decoder, click **Media Settings**. In Figure 24, port 16 of the matrix switch is selected as the input port to display recorded video from the hybrid decoder.

Figure 24. Media Settings



## Hybrid Decoder Pools

Hybrid decoder pools ensure that the correct hybrid decoder is used in environments with more than one matrix switch or in environments in which specific hybrid decoders are assigned to a group of keyboards. Figure 25 shows an environment with four CCTV keyboards and monitors but only three hybrid decoders. Ideally, a hybrid decoder is available for each keyboard to ensure that all operators can perform playback features simultaneously.

In this example, ISP\_1 is assigned to work exclusively with hybrid decoder 10. Because both devices have been assigned to pool #1, HyDec10 is available exclusively for that keyboard for playback requests.

The two other hybrid decoders in pool #2 are shared among the remaining three operators, making playback features available only to the first two requests. Hybrid decoders that are in use become available to the pool as soon as an operator stops the playback request or the playback timeout occurs. Figure 20 on Page 5-1 shows how to change the default playback timeout of 36000 seconds.

**Figure 25.** Hybrid Decoder Pools

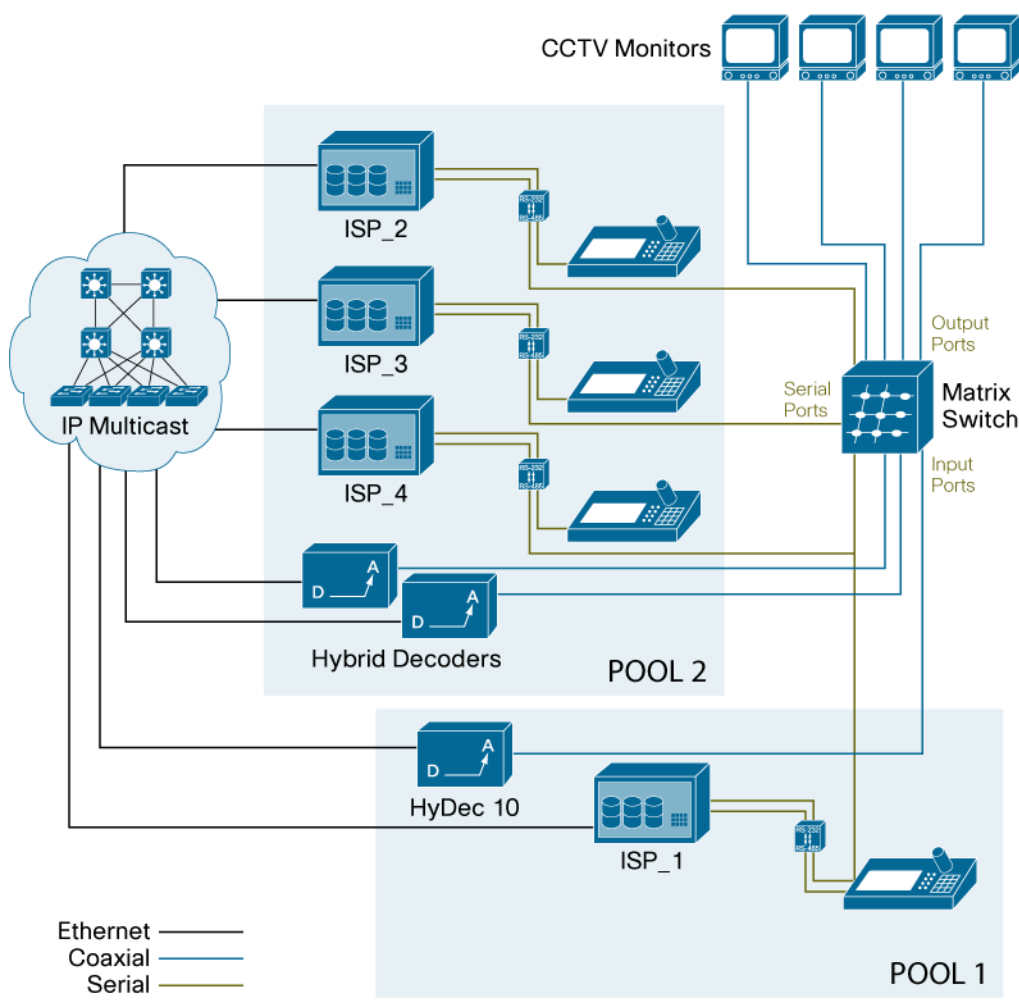


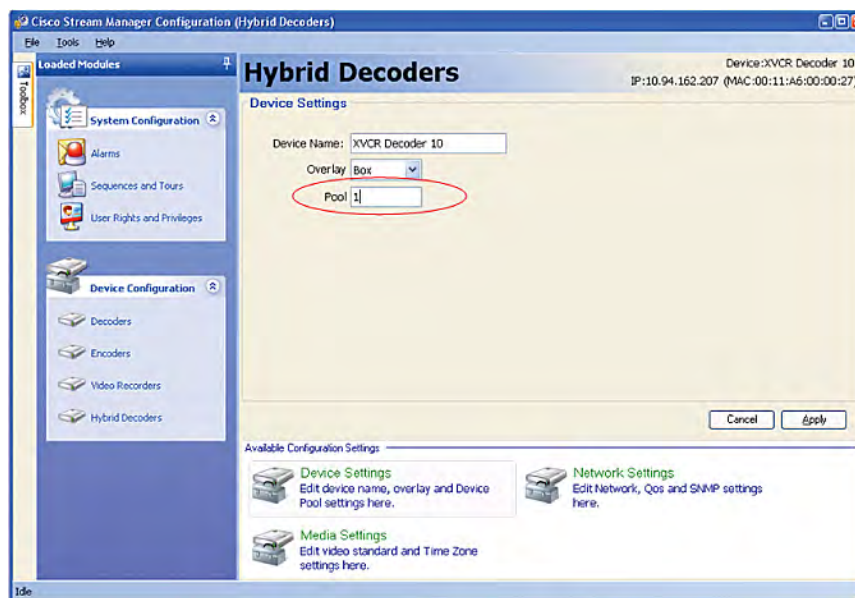
Figure 26 shows an example in which the keyboard data converter is connected to the ISP. In this example, pool #1 is configured to ensure that only hybrid decoders in the same pool respond to playback requests from the keyboard that is connected to this ISP.

**Figure 26.** Hybrid Decoder Pools Settings



As shown in Figure 27, the hybrid decoder is configured with the same pool, pool #1. The overlay setting specifies how the camera information (camera number, date/time, and so on) displays on the monitor.

**Figure 27.** Hybrid Decoder Pool Settings



## Time Synchronization

Maintaining internal clocks that are synchronized to a reliable time source is critical in a surveillance environment, where video streams need to be retrieved from a specific date and time for review. The matrix switch and the ISPs should be synchronized to display the same date and time.

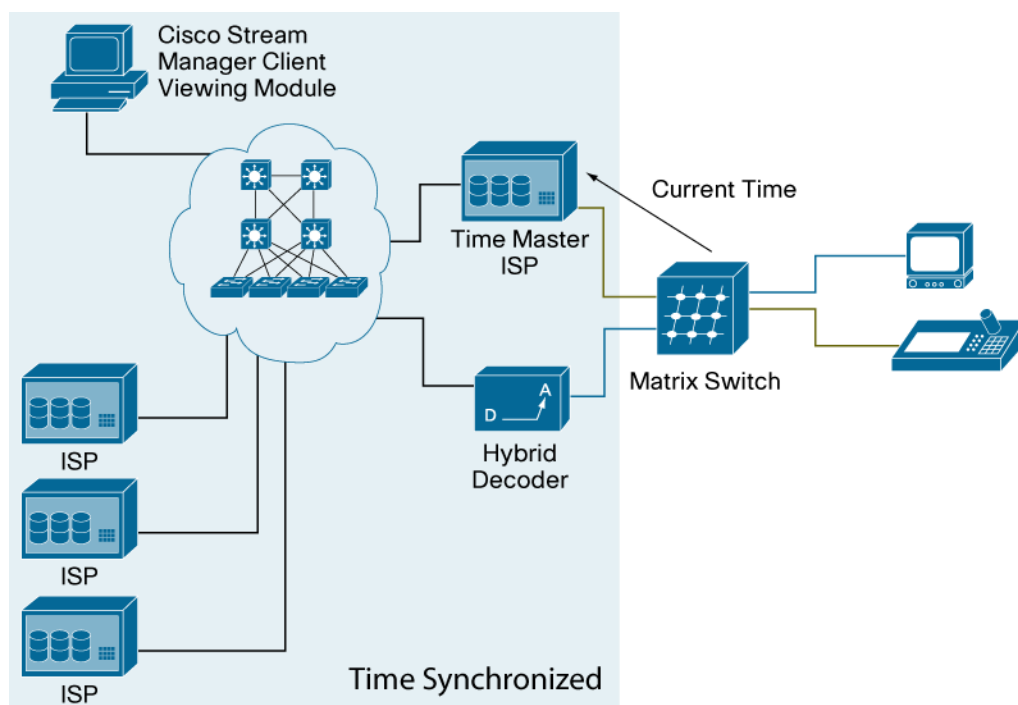
The Stream Manager software that runs on all Cisco Video Surveillance devices can synchronize to the time that is provided by an ISP. In a typical video surveillance solution, one ISP is configured as the time master. This ISP uses multicast updates to synchronize the time on all other devices, including hybrid decoders and the Cisco Stream Manager Client Viewing Module application.

The time master ISP may rely on external devices, such as a matrix switch or devices that run the Network Time Protocol (NTP) to synchronize its clock.

Figure 28 shows a deployment in which a matrix switch is the time source for the time master ISP. The time master ISP receives the current time from the matrix switch and propagates it to other Stream Manager devices. Typically, a serial cable is required to provide clock synchronization.

Note: Only one ISP should be configured as the time master for the environment.

**Figure 28.** Matrix Switch Clock



As shown in Figure 29, ISP\_1 is configured as the time master and by specifying the proper serial communications parameters, the matrix switch acts as the time source for ISP\_1 and the video surveillance environment. In this case, the matrix switch connectivity is configured for a baud rate of 9600 bps, 8 data bits, no parity, and 1 stop bit.

**Figure 29.** Time Synchronization from Matrix Switch



Figure 30 shows how to configure an ISP to act as the time master for the environment. In this example, the Internal ISP clock is used as the reference time.

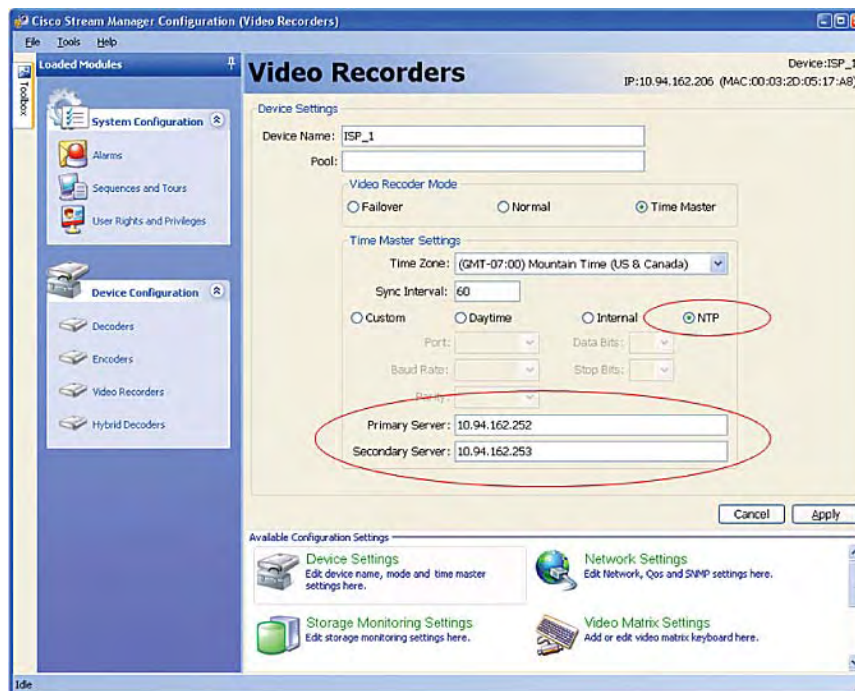
**Figure 30.** Time Synchronization with Internal clock





The ISP also can be configured to receive time from two different NTP sources. To configure NTP time synchronization, choose NTP as the source and specify the NTP servers to provide time to the video surveillance environment, as shown in Figure 31.

**Figure 31.** Time Synchronization—NTP



### Configuring Failover with a Matrix Switch

This section describes the general steps that are required to configure the ISP and the Cisco Stream Manager Administration and Monitoring with Failover Module to support matrix-based N+N redundancy. Detailed hardware requirements for each third-party system are described in Chapter 6.

#### Configure the Failover Integrated Services Platform

To configure an ISP to serve as a failover device for a hybrid system, use the Stream Manager Configuration Module and configure the video recorder mode as failover, as shown in Figure 32. This setting causes this ISP to record video streams only when the Stream Manager Administration and Monitoring with Failover Module detects the failure of another ISP.

Figure 32. Failover Mode



In the window for configuring video matrix settings, change the Video Matrix type to match the appropriate system. In Figure 33, Bosch has been selected to support a Bosch matrix switch.

Figure 33. Matrix Settings



Each port on the failover ISP must be configured to match the port number of the monitor output port from the matrix switch. In Figure 34, the input 1 port of the ISP is configured to receive the video stream from the monitor output 1 port of the matrix switch. The desired storage settings, such as video resolution and frame rate, also are specified for this port.

The video resolution and frame rates that are specified in this screen are used only during a failure. Because the failover ISP can back up different video ports from different ISPs, this setting does not necessarily match the original setting of the primary ISP. Setting all encoder ports to a high video resolution and frame rate guarantees that video quality is maintained during a failure.

**Figure 34.** Port Configuration



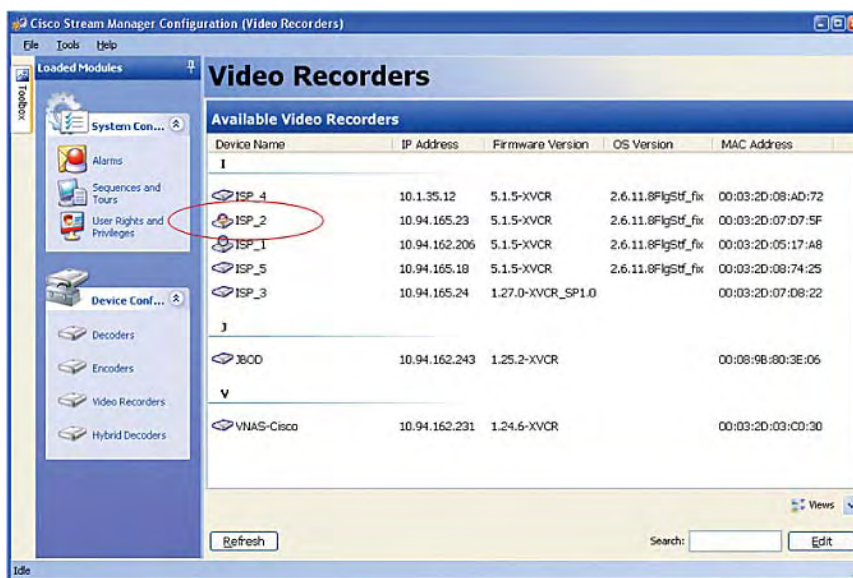
For this example, Table 8 shows how the first eight ISP encoder ports have been assigned to the first eight matrix output ports. All ports are configured with video resolution of 4 CIF and frame rate of 30 fps. A second failover ISP in the network would use different matrix output ports.

**Table 8.** Matrix Output Ports

ISP Encoder Port	Matrix Output Port	Video Resolution	Frame Rate
1	1	4CIF	30 fps
2	2	4CIF	30 fps
3	3	4CIF	30 fps
4	4	4CIF	30 fps
5	5	4CIF	30 fps
6	6	4CIF	30 fps
7	7	4CIF	30 fps
8	8	4CIF	30 fps

Figure 35 shows the icon that indicates that ISP\_2 has been configured as a failover device.

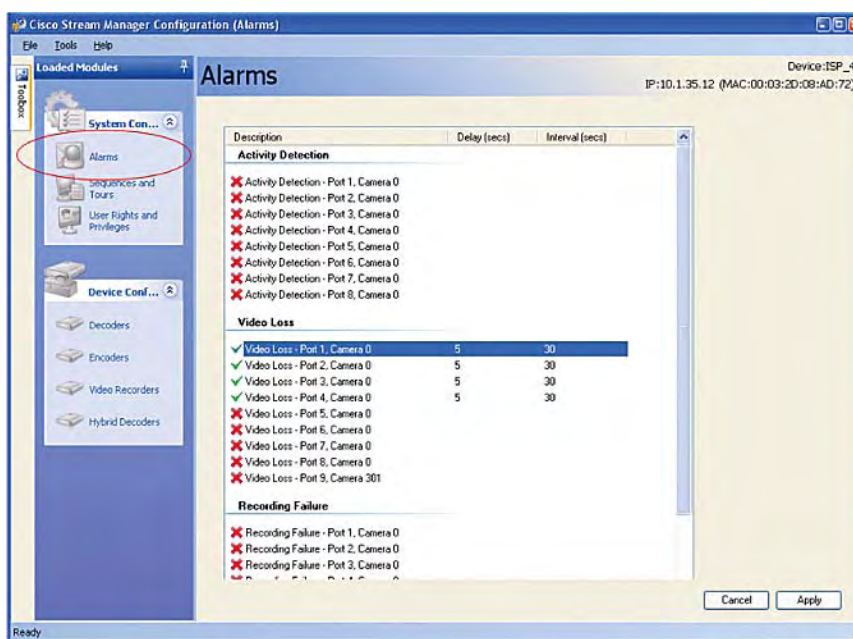
**Figure 35.** Configuration Module



### Configure Video Loss Detection

The previous section describes how to configure an ISP to detect complete ISP failures. To detect when video is lost from individual ports, each port in the environment must be configured to send an alarm to the Stream Manager Administration and Monitoring Module if video loss is detected. Figure 36 shows the configuration that is required for each ISP port.

**Figure 36.** Video Loss Detection



## Configure the Stream Manager Administration and Monitoring Module

The Stream Manager Administration and Monitoring Modules provide system health information and central alarm management capabilities. Its features include:

- Real-time status, including server use and bandwidth use, of all Cisco Video Surveillance devices in the network.
- On-demand status reports that include information about video loss, recording status, raid alarm, and hard disk drive failures.

In addition, the Administration and Monitoring with Failover Module provides failover capabilities that minimize the loss of video recording if a device fails. The Administration and Monitoring with Failover Module transfers video streams from a failed ISP to a failover ISP. If only one video channel fails to record, the system switches only that video stream to the failover ISP.

Figure 37 shows the Main screen of the Administration and Monitoring with Failover Module, with ISP\_2 acting as a failover recorder. Because no failures have been detected, the five ports dedicated for failover are idle.

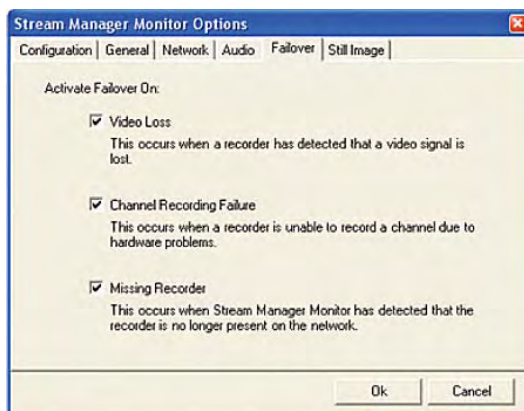
**Figure 37.** Administration and Monitoring with Failover Module

Data Unavailable		Recording Status			
Port	Channel	Type	Rate (Mbps)	Retention	
1					
2	2	Local	2.51	11 days...	
3	3	Local	2.97	11 days...	
4	4	Local	3.03	11 days...	
5	5	Local	2.84	11 days...	
6	6	Local	0.76	11 days...	
7	7	Local	2.97	11 days...	
8	8	Local	2.85	11 days...	
9	34	Network	0.00	11 days...	
10	18	Network	3.45	11 days...	
11	17	Network	1.02	11 days...	
12	33	Network	0.00	01 days...	
13	35	Network	0.00	00 days...	

To configure the Administration and Monitoring with Failover Module to detect failures in specific conditions, choose **Tools > Options > Failover**.

Figure 38 shows the **Failover** tab with configuration settings that cause the Administration and Monitoring with Failover Module to detect single port failures or a missing ISP.

**Figure 38.** Failover Settings



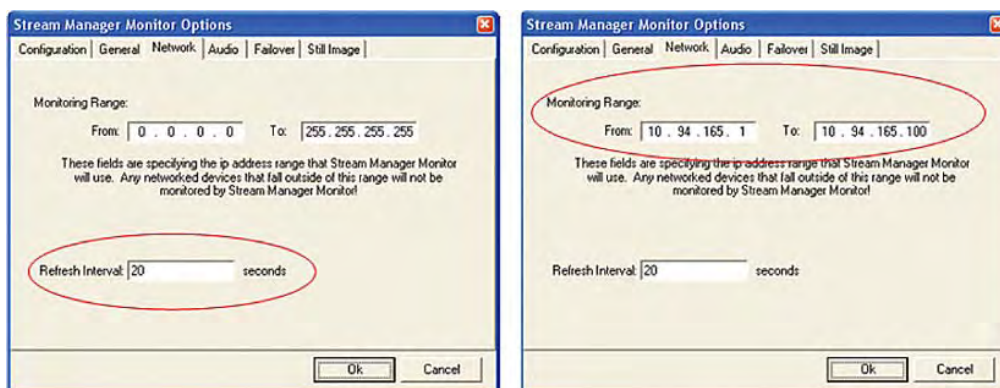
Note: The Video Loss setting is useful for detecting a failure of the cable that connects to the ISP. If a camera fails, the video loss alarm triggers and a failover occurs. Because the camera does not produce video images, no video is recorded.

The refresh interval can be changed in the **Network** tab. The Stream Manager Administration and Monitoring with Failover Module dynamically discovers available devices and continuously monitors for failures. The Administration and Monitoring with Failover Module attempts to reach each device three times before determining that a failure has occurred.

With the default refresh Interval of 60 seconds, it can take up to 180 seconds before the failover ISP begins recording streams. The minimum refresh Interval is 10 seconds, but a setting of 20 seconds is recommended for most environments for efficient use of bandwidth. In Figure 39, the Administration and Monitoring with Failover Module has been configured with a refresh interval of 20 seconds. In this case, approximately 60 seconds of video is lost while the failover process takes place.

The Administration and Monitoring with Failover Module can be configured to monitor only devices with IP addresses within a specific range. In the first example of Figure 39, all devices are monitored. In the second example of Figure 39, only devices with IP addresses in the range of 10.94.165.1 through 10.94.165.100 range are monitored.

**Figure 39.** Network Settings and Monitoring Range



The Administration and Monitoring with Failover Module transfers video streams from a failed ISP to a failover ISP. If only one video channel fails to record, the system switches only that video stream to the failover ISP

Figure 40 shows how, after a failure event, available ports on the failover ISP become active and begin recording traffic that was originally destined to a failed ISP.

**Figure 40.** Failover ISP recording

The screenshot displays the 'Devices 21/22 - 1 System Alerts' window. On the left, a list of devices is shown, including ISP\_1 (Time Master Recorder), various Encoders (10-17, 33-35, 37), ISP\_2 (Failover Recorder), ISP\_5 (Recorder), JBDD (Recorder), and several Monitors (1, 11, 12, 3, 4). ISP\_2 is highlighted, indicating a failure event. The right pane shows 'Device Details' for ISP\_2, including its IP address (10.94.165.23), MAC address (00:03:20:07:07:5F), and running time (0 days 0 hours 13 mins). It also shows storage information: Total Storage: 1.82 TB, Available Storage: 1.25 TB, Total Recording Rate: 14.36 Mbps, and Avg Retention Time: 10 days 22 hrs. A table titled 'Recording Status' shows five channels (1-5) all recording to ISP\_1 at a rate of 2.95 Mbps. Below this is a 'Device Alerts' section.

Data Unavailable		Recording Status				
Port	Monitor	Channel	Original Recorder	Rate (Mbps)	Channel Type	
1	1	1	ISP_1	2.95		
2	2	2	ISP_1	2.79		
3	3	3	ISP_1	2.95		
4	4	4	ISP_1	2.79		
5	5	5	ISP_1	2.95		

If a failure occurs, the Administration and Monitoring with Failover Module updates the history log with event details. To view the log, choose **History > View Log...** or press F5. Figure 41 shows an example in which five cameras have been successfully redirected to the failover ISP.

**Figure 41.** History Log

```

2/26/2007 1:39:43 PM | History log cleared
2/26/2007 1:42:52 PM | Missing Device: Time Master Recorder ISP_1
2/26/2007 1:42:55 PM | Failover: Successfully failed over camera 1
2/26/2007 1:42:58 PM | Failover: Successfully failed over camera 2
2/26/2007 1:43:02 PM | Failover: Successfully failed over camera 3
2/26/2007 1:43:06 PM | Failover: Successfully failed over camera 4
2/26/2007 1:43:10 PM | Failover: Successfully failed over camera 5

```

A simple way to verify that video streams are being recorded to the failover ISP is to select playback keyboard functions, such as instant replay or time/date search, while in failover mode.

The failover ISP continues to record until the failed ISP recovers. At that time, the Stream Manager Administration and Monitoring with Failover Module polls the recovered ISP three times before switching back to the primary ISP and returning the failover ISP to standby mode. Figure 42 shows a history log that indicates that the failover ISP has stopped recording the failed video streams.

**Figure 42.** History Log

```
2/26/2007 1:39:43 PM | History log cleared
2/26/2007 1:42:52 PM | Missing Device: Time Master Recorder ISP_1
2/26/2007 1:42:55 PM | Failover: Successfully failed over camera 1
2/26/2007 1:42:58 PM | Failover: Successfully failed over camera 2
2/26/2007 1:43:02 PM | Failover: Successfully failed over camera 3
2/26/2007 1:43:06 PM | Failover: Successfully failed over camera 4
2/26/2007 1:43:10 PM | Failover: Successfully failed over camera 5
2/26/2007 1:47:07 PM | Failover: Stopping unwanted failover of camera 1
2/26/2007 1:47:09 PM | Failover: Stopping unwanted failover of camera 2
2/26/2007 1:47:13 PM | Failover: Stopping unwanted failover of camera 3
2/26/2007 1:47:16 PM | Failover: Stopping unwanted failover of camera 4
2/26/2007 1:47:19 PM | Failover: Stopping unwanted failover of camera 5
```



## Chapter 6: Manufacturer-Specific Configurations

This section describes the configuration required to integrate with third-party matrix switches and keyboards to add digital recording and instant retrieval features.

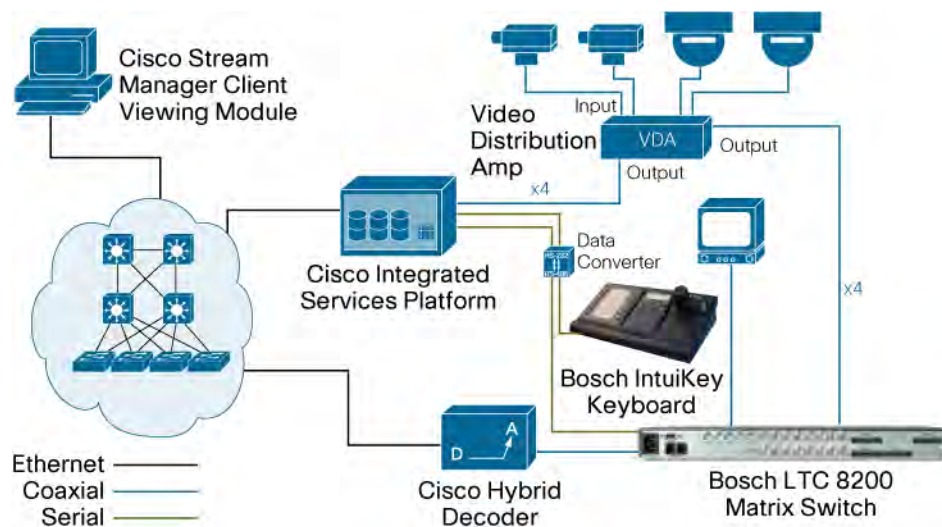
### Integration with a Bosch Matrix Switch and Keyboard

As shown in Table 6 on Page 4-1 Cisco Video Surveillance devices integrate with several third-party matrix switches and keyboards. The examples in this section focus on the Bosch LTC 8200 matrix switch and Bosch IntuiKey keyboard, but similar steps apply to other Bosch systems.

The following equipment is required to integrate with a Bosch matrix switch and keyboard:

- A Bosch matrix switch with an available input port.
- A Cisco Integrated Services Platform to perform digital recording of video streams.
- Cisco data converter. A data converter is connected between the matrix switch, keyboard, and ISP to convert serial signals between RS-232 and RS-485. This deployment allows the ISP to intercept keyboard commands that identify when an operator wants to switch from live to recorded video. A data converter is needed for each keyboard that requires access to playback features.
- Cisco hybrid decoders. The hybrid decoder requests video from the ISP and decodes it into analog video, which is passed to the matrix switch. The hybrid decoder connects to a dedicated input port on the matrix switch. The number of hybrid decoders in a solution should match the number of keyboards that require simultaneous playback functionality.

**Figure 43.** Bosch Hybrid Integration



### Cisco Data Converter

A Cisco data converter is required to integrate a matrix switch with the Cisco hybrid solution. Figure 44 shows the proper way to interconnect the data converter to the ISP, the Bosch keyboard, and the matrix switch:

**Figure 44.** Cisco Data Converter

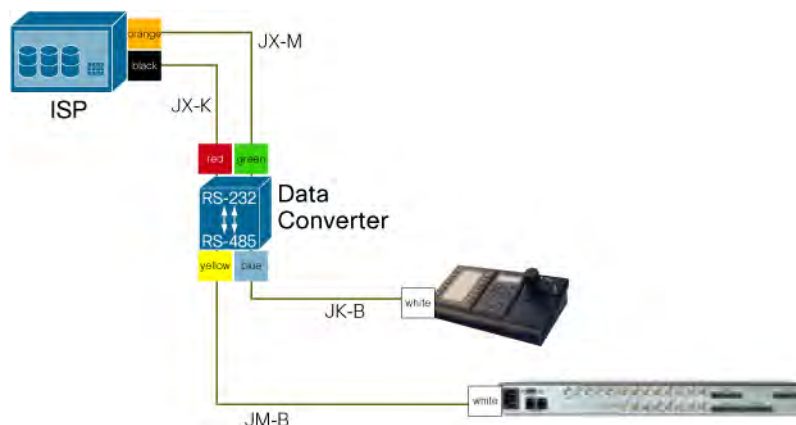
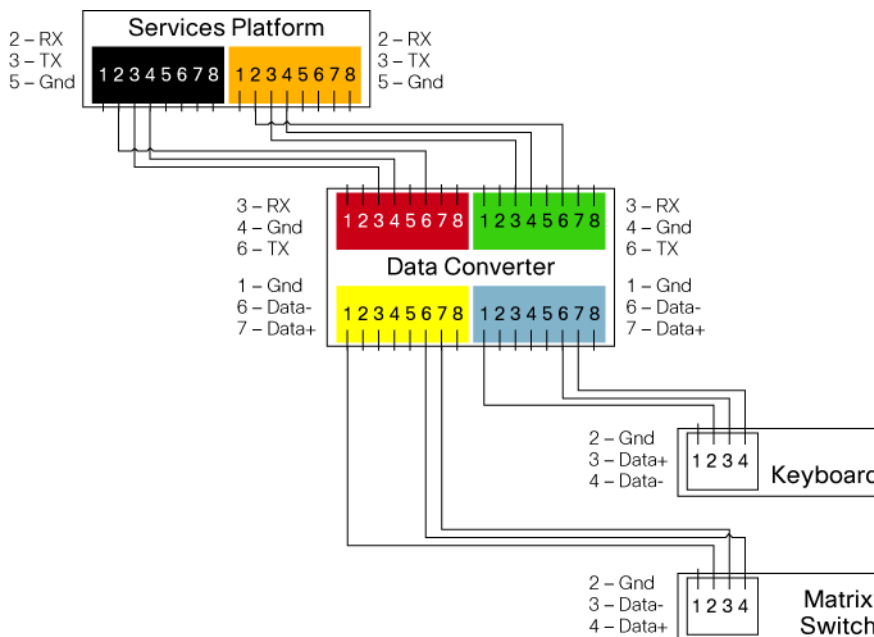


Figure 45 shows the cable pinouts of the Cisco data converter for a Bosch IntuiKey keyboard.

**Figure 45.** Cisco Data Converter Pinouts



### Cisco Hybrid Decoder

When a playback feature is requested, the hybrid decoder retrieves the video stream from the proper ISP and displays it on the proper matrix switch port. This process is transparent to operators.

The hybrid decoder is connected via Ethernet to the IP network and via a coaxial cable to the matrix switch. A port from the matrix switch is reserved to be the input port from the hybrid decoder. When an operator requests a playback feature from the keyboard, the ISP instructs the matrix switch to redirect the reserved input port to the monitor output port that is associated with the requesting keyboard.

### Configuring the Bosch LTC 8200 Matrix Switch

The Cisco hybrid solution supports integration with the Bosch matrix switches that are listed in Table 6 on Page 4-1.

The examples in this section are based on the LTC 8200 matrix switch and IntuiKey keyboard, but most of the concepts apply to other Bosch models.

By default, the 16 input ports of the LTC 8200 are configured as Camera 1 through Camera 16. These port numbers must match the camera number or peripheral ID of a Cisco IP gateway encoder. In an environment with more than 16 cameras or with camera numbers that are greater than 16, the camera numbers on the matrix switch must be changed to match the camera number of the corresponding encoders.

### Allegiant Master Control Software

Bosch provides configuration software for the LTC 8200 that allows changing camera numbers and making other configuration changes. The Allegiant Master Control Software may be obtained from Bosch.

Note: This software requires a license from Bosch. A parallel port hardware key also may be required.

To change camera numbers, launch the Master Control Software from a Windows workstation. Figure 45 shows the user login screen.

**Figure 46.** Master Control Software



Note: The default password for User "Installer" is "1" (the number one).

Choose **File > New** and select the proper matrix switch model as shown in Figure 47.

**Figure 47.** Matrix Switch Model

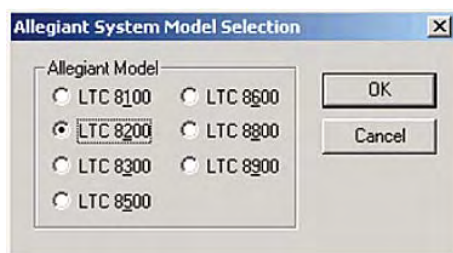
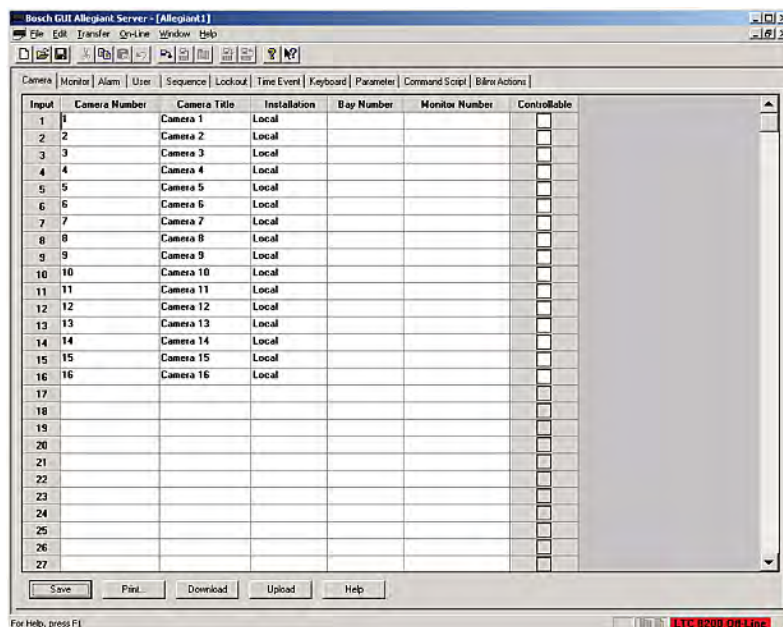


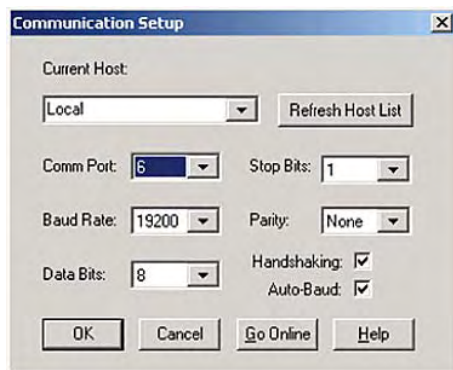
Figure 48 shows the main window, which lists available cameras and their respective camera numbers.

**Figure 48.** Available Cameras



Connect the serial cable from the IntuiKey keyboard to the Windows PC and specify the proper serial port under **Transfer > Communication Setup**. Figure 49 shows Comm Port 6 used to connect from the PC to the console port on the LTC 8200.

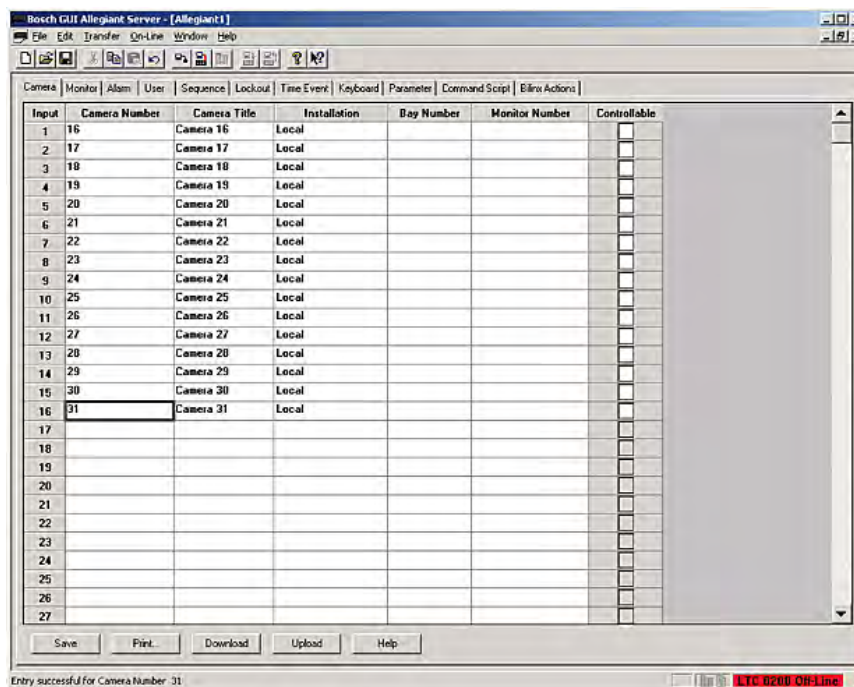
**Figure 49.** Serial Port Settings



Choose **On-Line > Go On-Line** to initiate communication with the LTC 8200. A green status bar should appear at the bottom of the screen.

The following example changes camera numbers to Camera 16 through Camera 31.

**Figure 50.** Camera Number Change



Make any necessary changes to the camera ports and click Download to update the LTC 8200 with these changes.

### Upgrading the Bosch IntuiKey Keyboard

The IntuiKey series has two distinct software images: the operating system firmware and a language table image. Cisco provides a language table image that can be downloaded to the keyboard to enhance the keyboard functionality and interaction with the ISP. This same image is used in a virtual matrix switch solution.

To download the latest firmware and to obtain more information upgrade procedures, visit the Bosch website.

Requirements:

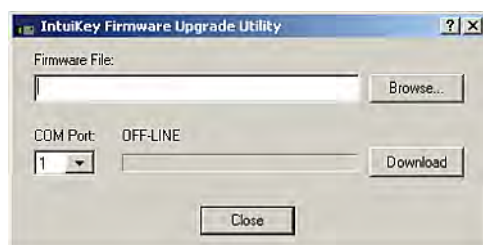
- The keyboard must be running firmware release 1.7x. The version is displayed on the keyboard when it boots up.
- Windows PC with a serial port.
- Industry-standard 9-pin female to 9-pin female RS-232 null modem cable.
- IntuiKey downloader program.
- IntuiKey configuration software.
- The current hybrid language table file, which may be obtained from the Software Download page at <http://www.cisco.com>. A valid ID CCO is required to download this file.

### Uploading a New Firmware Image

If the keyboard is not running release 1.7x, follow these steps to upgrade the firmware:

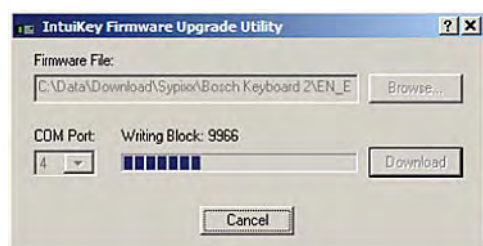
- Step 1. Download and install the IntuiKey downloader program.
- Step 2. Download the firmware image from the Bosch website. The filename should be similar to IntuiKey\_firmware\_1.73.s20.
- Step 3. Connect the serial cable to the PC and the keyboard.
- Step 4. Place the keyboard in Bootloader mode. To do so, while powering up the keyboard, press and hold the 1 and 0 buttons simultaneously.
- Step 5. Launch the IntuiKey Firmware Upgrade Utility (filename: IntuiFUU.exe) as shown in Figure 51.

**Figure 51.** Firmware Upgrade Utility



- Step 6. Specify the location of the firmware file and the proper Windows COM port and click **Download**. The download process begins as shown in Figure 52.

**Figure 52.** Firmware Upgrade Utility



- Step 7. Press the **[Clr]** button on the keyboard when finished. The keyboard should boot up with the new firmware image.

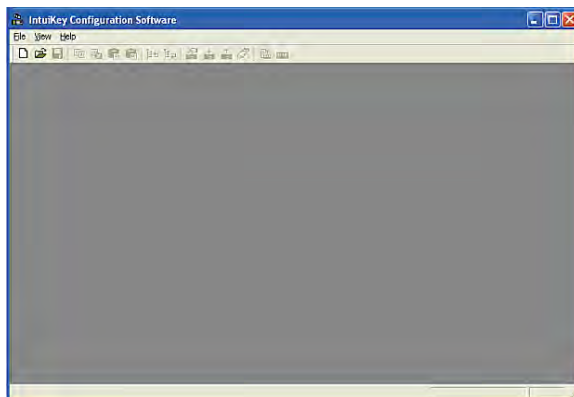
### Uploading a New Language File

Cisco provides an updated language file that enhances the keyboard functionality and communication with the ISP. To upload language file to the keyboard, follow these steps:

- Step 1. Download and install the IntuiKey configuration software.
- Step 2. Download the language file from the Software Download page at <http://www.cisco.com>. The filename should be similar to: IntuiKey\_ciscoIPS\_v2.int. This version should be compatible with the proper keyboard firmware image.
- Step 3. Connect the serial cable to the PC and the keyboard.
- Step 4. Place keyboard in Bootloader mode. To do so, while powering up the keyboard, press and hold the **1** and **0** buttons simultaneously.

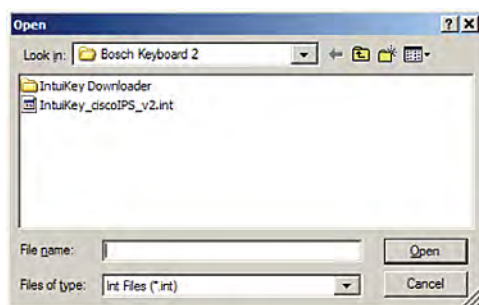
Step 5. Launch the IntuiKey Configuration Software (filename: IntuiKey.exe). The IntuiKey Configuration screen appears, as shown in Figure 53.

**Figure 53.** IntuiKey Configuration Software



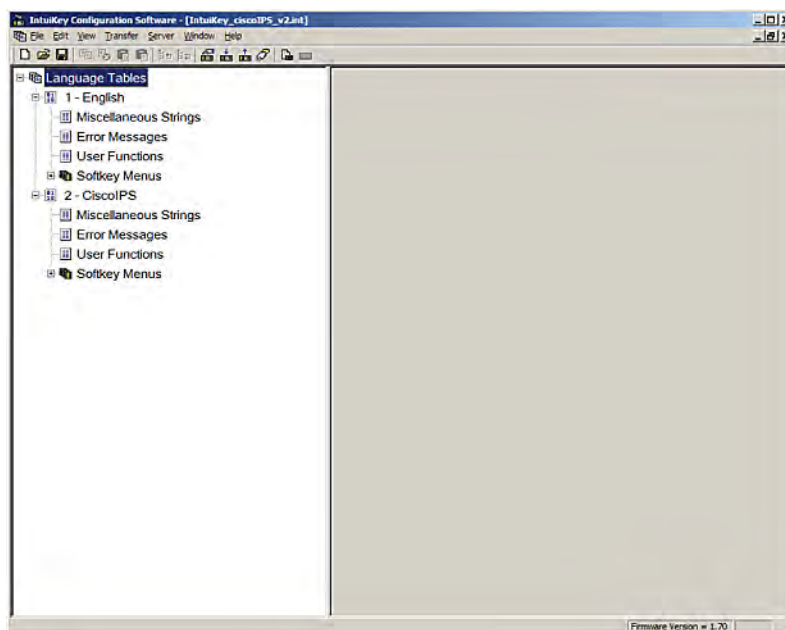
Step 6. Choose **File > Open** and specify the location of the language file, as shown in Figure 54.

**Figure 54.** Language File Location



The main screen appears as shown in Figure 55.

**Figure 55.** IntuiKey Configuration Software



Step 7. Choose **Transfer > Configure COM Port...** and specify the Windows COM port that is used by your PC for serial communications, as shown in Figure 56.

**Figure 56.** Serial Port Settings



Step 8. Choose **Transfer**, specify the CiscoIPS image in the second field, and then click **Download**, as shown in Figure 57.

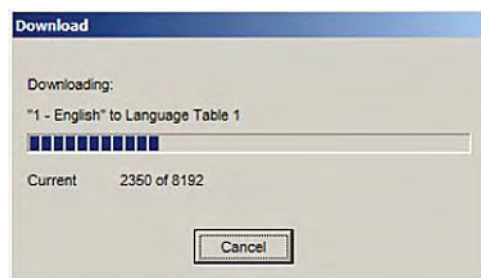
**Figure 57.** Image Location



Note: Make sure to not overwrite the language file in slot #1.

The downloading process begins, as shown in Figure 58.

**Figure 58.** Image Download



Step 9. Press the [Clr] button on the keyboard when finished. The keyboard should boot up with the new language file.



Step 10. To verify that the new language file has been loaded, press the **Allegiant** key. Figure 59 shows the new hybrid features that are available when you press the **Command Script/Playback** key.

**Figure 59.** Language File Features

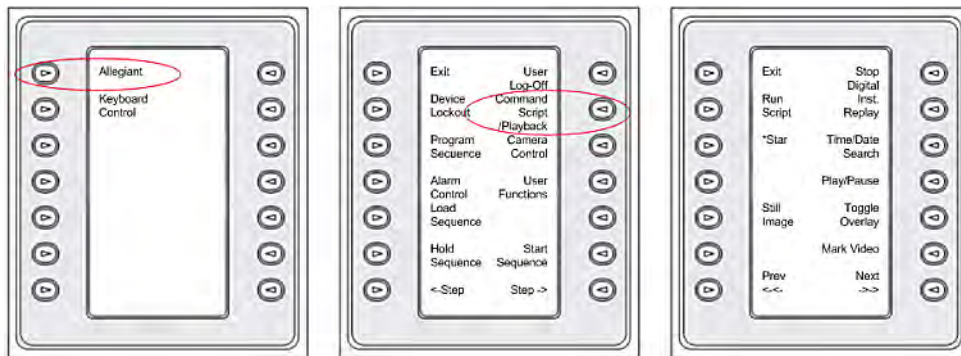


Figure 60 shows some of the features that are added by the Cisco ISP language file and how they map on the IntuiKey keyboard.

**Figure 60.** Bosch IntuiKey Integration

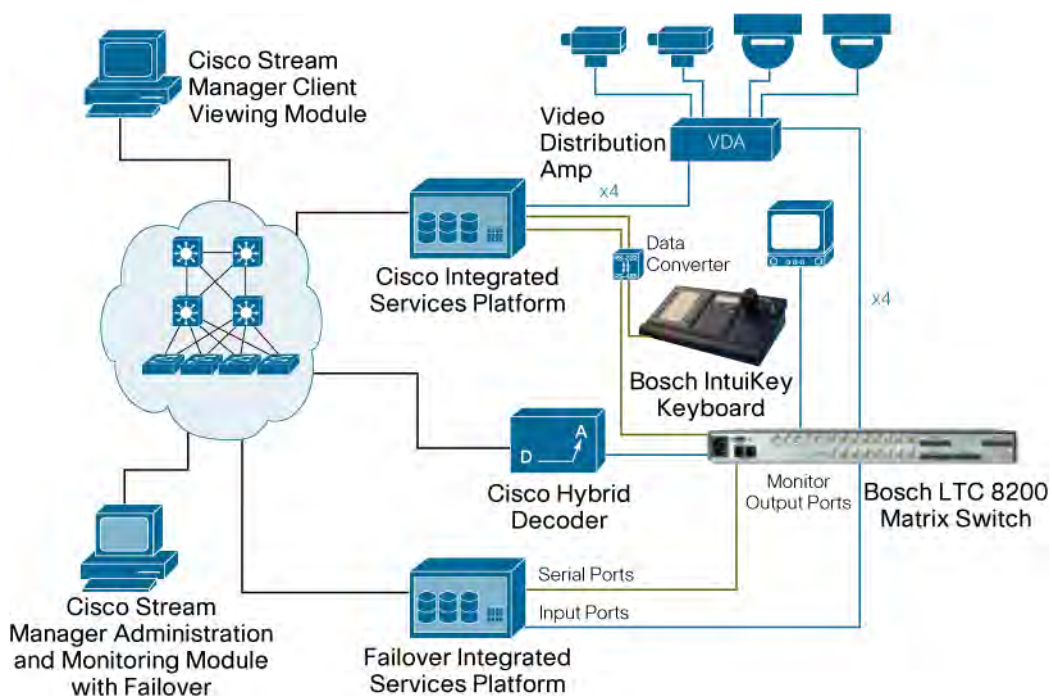


### Failover Configuration with a Bosch LTC 8200 Matrix Switch

This section describes how a hybrid solution that includes a Bosch Matrix Switch can be configured for a matrix-based N+N redundancy.

Note: The example in this section focuses on the LTC 8200 Matrix Switch, but similar steps apply to other Bosch systems.

Figure 61 shows how an ISP can act as a failover recorder for other ISPs by using a Bosch LTC 8200 Matrix switch.

**Figure 61.** Bosch Hybrid Failover Solution

The following equipment and software is required for this solution:

- A dedicated ISP for failover.
- The Cisco Stream Manager Administration and Monitoring with Failover Module.
- A Bosch matrix switch with available output ports.
- RS-232 console cable to connect from the matrix switch to the failover ISP. This cable carries instructions for the matrix switch to redirect video streams to the failover ISP. This cable may be purchased directly from Bosch or built by using the pinouts that are shown in Table 9.

**Table 9.** RS-232 Serial Cable Pinout

Pin Number	Allegiant Designation	9-Pin Female (ISP Side)
1	CHASSIS GND	None
2	Receive	Data 3
3	Transmit	Data 2
4	CTS	1
5	RTS	8
6	NO CONNECTION	None
7	DATA GND	5
8	NO CONNECTION	None
9	NO CONNECTION	None
		(pins 4 & 6 jumpered)
		(pins 1 & 7 jumpered)

By default, the 16 input ports of the LTC 8200 are configured as Camera 1 through Camera 16. These ports numbers must match the camera number or peripheral ID of the encoder port on the ISP. In an environment with more than 16 cameras or with camera numbers that are greater than

16, the camera numbers must be changed to match the camera number of the corresponding encoder.

Bosch provides configuration software for the LTC 8200 that allows changing camera numbers and other matrix settings. See the “Configuring the Bosch LTC 8200 Matrix Switch” in Chapter 6: for more information about the Master Control Software.

Note: The current Stream Manager Software release requires monitor output ports to be numbered starting with Port 1. This limitation does not exist for input ports.

Chapter 5: provides detailed configuration steps for failover integrations.

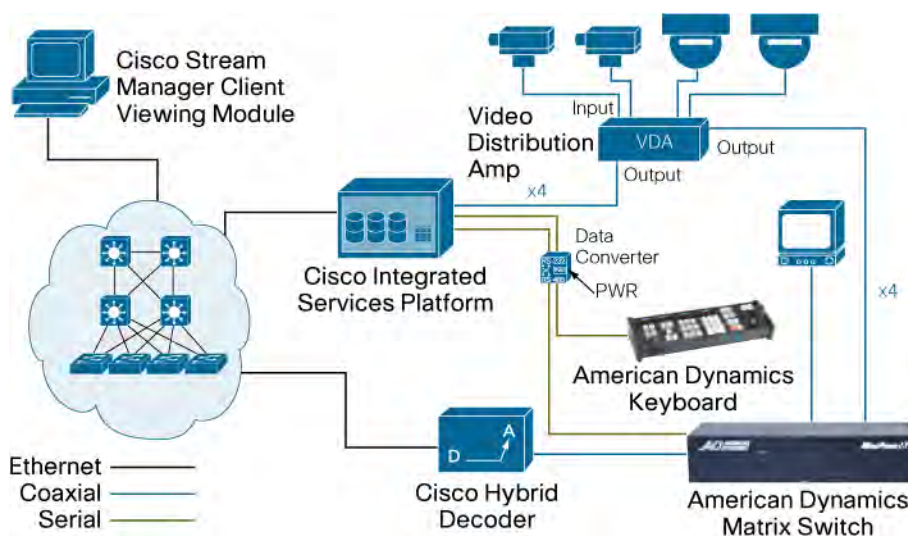
### Integration with an American Dynamics Matrix Switch

As shown in Table 6 on Page 4-1, Cisco integrates with several third-party matrix switches and keyboards. The examples in this section focus on the American Dynamics MegaPower matrix switch and the American Dynamics 2088 keyboard, but similar steps apply to other American Dynamics systems.

The following equipment is required to integrate with an American Dynamics matrix switch and keyboard:

- An American Dynamics matrix switch with an available input port.
- A Cisco ISP to perform digital recording of video streams.
- A Cisco data converter. A Cisco data converter is connected between the matrix switch, keyboard, and ISP to convert serial signals between RS-232 and RS-422. This deployment allows the ISP to intercept keyboard commands that identify when an operator wants to switch from live to recorded video. A data converter is needed for each keyboard that requires access to playback features.
- Cisco hybrid decoders. A hybrid decoder accepts recorded video from the ISP and decodes it into analog video, which is passed to the matrix switch. The hybrid decoder connects to a dedicated input port on the matrix switch. The number of hybrid decoders in a solution should match the number of keyboards that require simultaneous playback functionality.

**Figure 62.** American Dynamics Hybrid Integration



### Power Supply/Data Converter

A power supply/data converter is required to integrate a matrix switch with the Cisco hybrid solution. This device also provides power to the keyboard. Figure 63 shows the proper way to interconnect the data converter to the ISP, the American Dynamics keyboard, and the matrix switch.

**Figure 63.** Data Converter

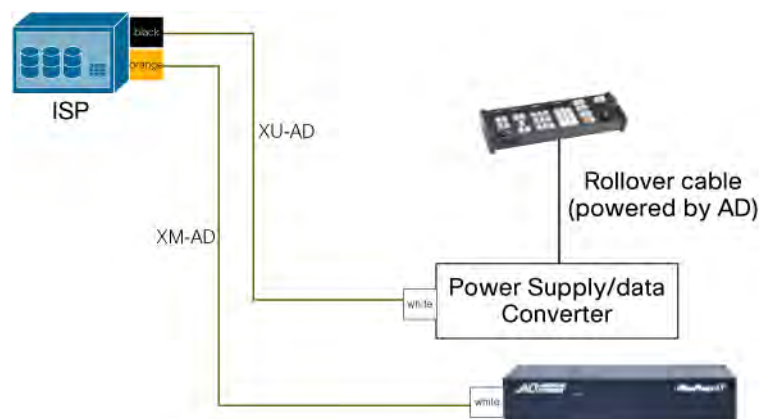
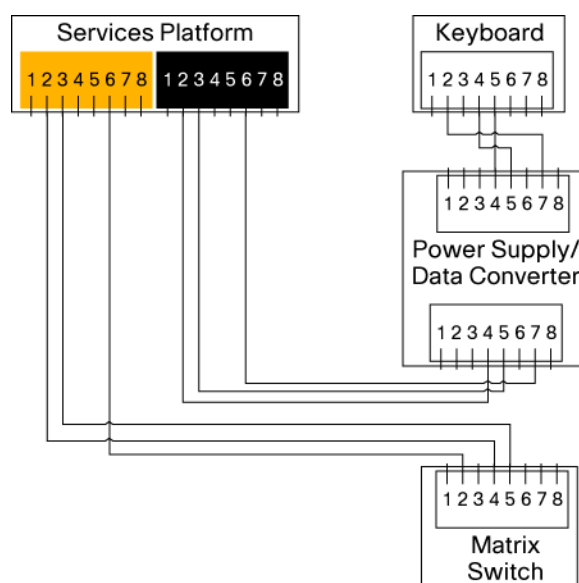


Figure 64 shows the cable pinouts of the data converter for an American Dynamics keyboard.

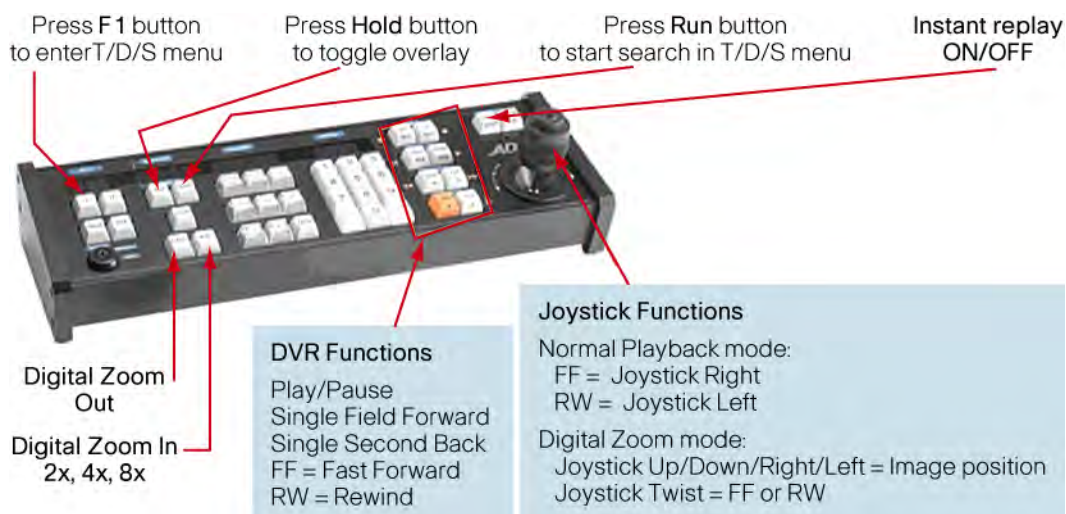
**Figure 64.** Data Converter Pinout



Note: For other configurations and related documentation, visit the American Dynamic support page [Configuring the American Dynamics 2088 keyboard](#).

No specific keyboard programming is required for the American Dynamics 2088 keyboard. Figure 65 shows how the American Dynamic keys interface with the ISP to provide playback functions.

**Figure 65.** American Dynamics Keyboard Integration



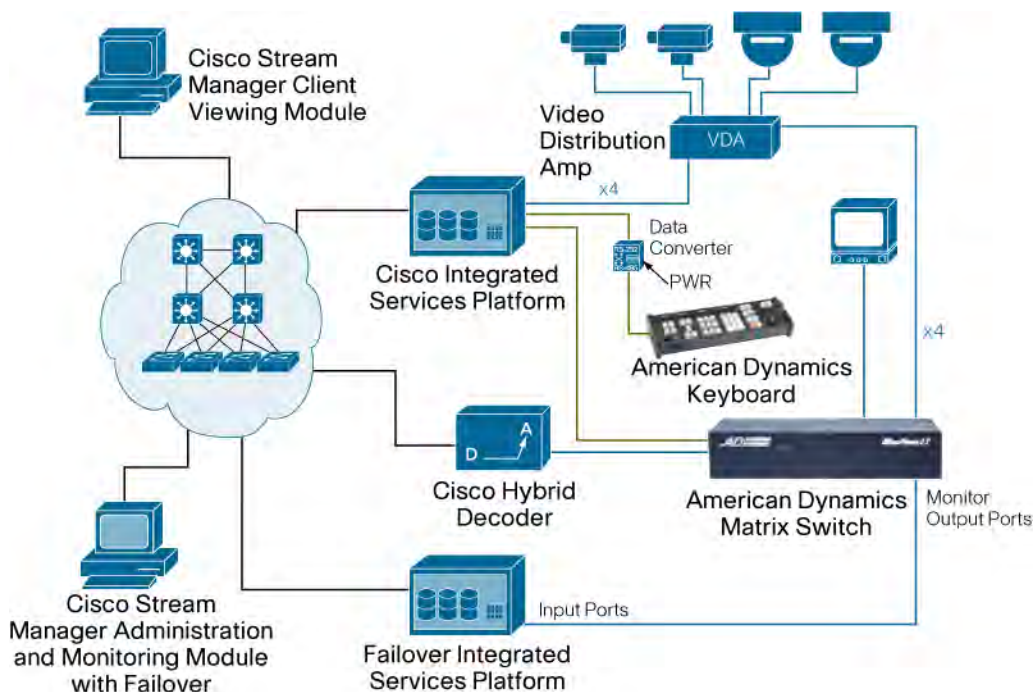
**Failover Configuration with an American Dynamics Matrix Switch**

This section describes how to configure a hybrid solution with an American Dynamics matrix switch for a matrix-based N+N redundancy.

Note: The example in this section focuses on the MegaPower LT matrix switch, but similar steps apply to other American Dynamics systems.

Figure 66 shows how an ISP can act as a failover recorder for other ISPs by using an American Dynamics matrix switch.

**Figure 66.** Hybrid Failover Solution



The following equipment and software is required:

- A dedicated ISP for failover.
- Cisco Stream Manager Administration and Monitoring with Failover Module.
- An American Dynamics matrix switch with available output ports.

Chapter 5: provides detailed configuration steps for failover integrations.

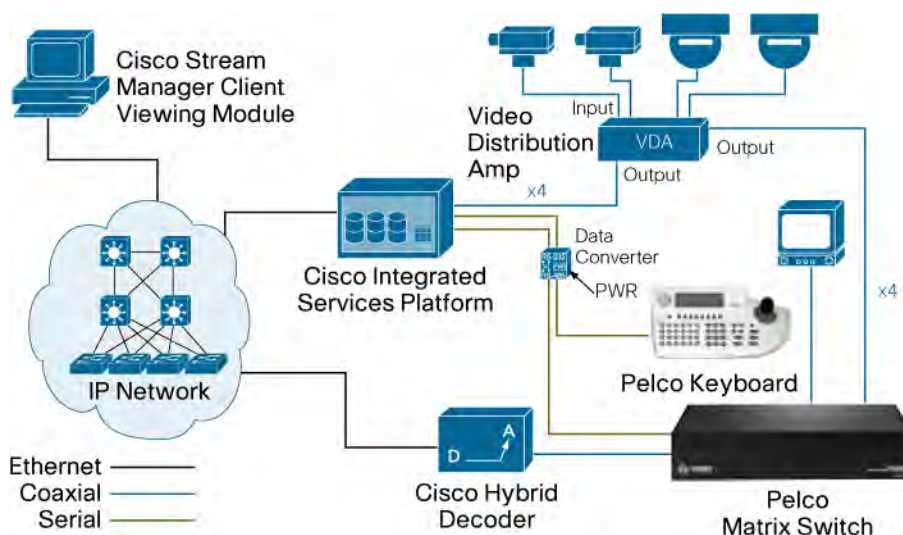
### Integration with a Pelco Matrix Switch and Keyboard

As shown in Table 6 on Page 4-1, Cisco integrates with several third-party matrix switches and keyboards. The examples in this section focus on the Pelco 9760 matrix switch and the Pelco CM9760-KBD keyboard, but similar steps apply to other Pelco systems.

The following equipment is required to integrate with a Pelco matrix switch and keyboard:

- A Pelco matrix switch with an available Input port.
- A Cisco ISP to perform digital recording of video streams.
- Cisco data converter. A Cisco data converter is connected between the matrix switch, keyboard, and ISP to convert serial signals between RS-232 and RS-422. This deployment allows the ISP to intercept keyboard commands that identify when an operator wants to switch from live to recorded video. A data converter is needed for each keyboard that requires access to playback features.
- Cisco hybrid decoders. A hybrid decoder accepts recorded video from the ISP and decodes it into analog video, which is passed to the matrix switch. The hybrid decoder connects to a dedicated input port on the matrix switch. The number of hybrid decoders in a solution should match the number of keyboards that require simultaneous playback functionality.

**Figure 67.** Pelco Hybrid Integration



### Power Supply/Data Converter

A power supply/data converter is required to integrate a matrix switch with the Cisco hybrid solution. Figure 68 shows the proper way to connect the data converter to the ISP, the Pelco keyboard, and the matrix switch.

**Figure 68.** Data Converter

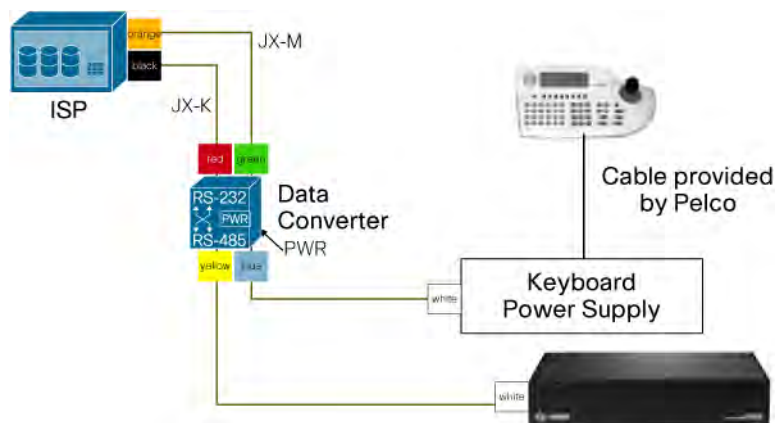
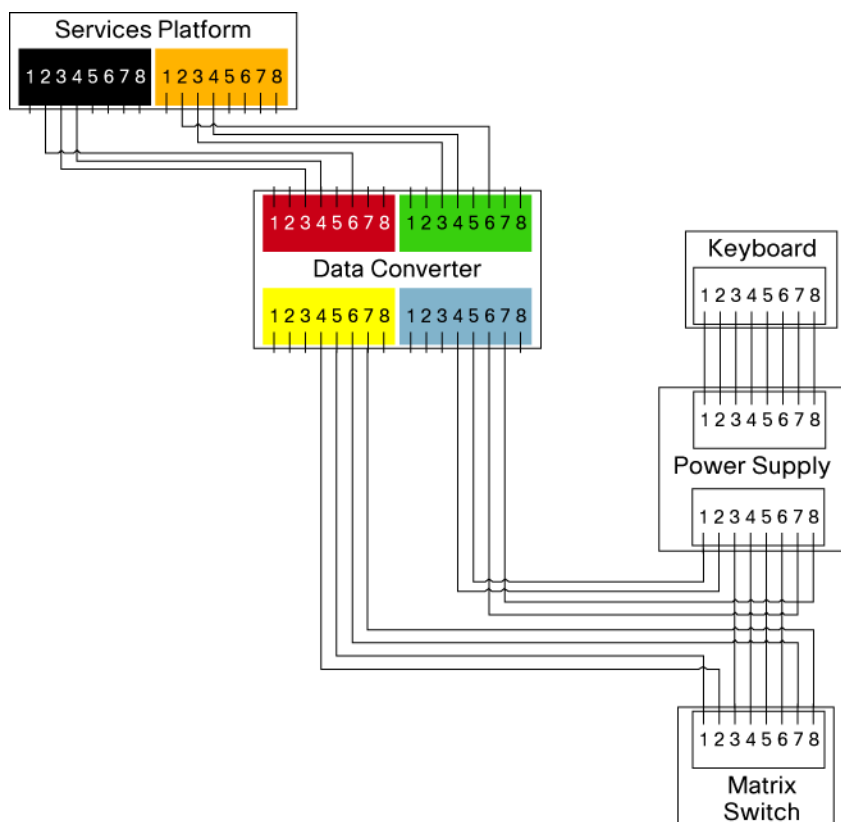


Figure 69 shows the cable pinouts of the data converter for a Pelco keyboard.

**Figure 69.** Data Converter Pinouts



### Integrated Services Platform BIOS Setup

The serial ports on the ISP must be configured with the proper Interrupt Request (IRQ) settings.

Note: To change the IRQ settings, the ISP must be rebooted

Follow these steps to configure the IRQ settings on the ISP:

- Step 1. Reboot the ISP that is connected to the Pelco keyboard and access the BIOS setup screen.
- Step 2. Select the **Integrated Peripherals** settings and make these settings:
  - Serial Port 3—use IRQ 10
  - Serial Port 4—use IRQ 11
- Step 3. Choose **Save then Exit** to apply these changes.

### Pelco CM9760-KBD Keyboard Setup

To program the keys on a Pelco CM9760 keyboard, make sure that the keyboard is connected directly to the matrix switch (not to the ISP).

Make sure the keyboard is in Setup Mode by following these steps:

- Step 1. Flip Dip Switch 2, which is located underneath the keyboard.
- Step 2. Log in to the keyboard (the default password is 1234).
- Step 3. Press the leftmost key (not the Esc key) in the row of blue keys.
- Step 4. Continue to press this key until the cursor is next to FNC70.

Figure 70 shows the key mappings for the integration with the Pelco keyboard

**Figure 70.** Pelco CM9760 Keyboard Integration





### Programming the keys

For each of the keys that are listed in Table 10 follow this procedure to program each key:

- Step 1. Press the desired program key.
- Step 2. Press the blue key (third key from the left in the top row).
- Step 3. Press the blue key that is directly under the **Def Num** on-screen label.
- Step 4. Using the numeric keypad, enter the desired ISP command from Table 10.
- Step 5. Press the blue key that is directly under the **Def Num** label.

**Table 10.** Key Programming

Function	ISP Command
Instant Replay	99
Time/Date Search	98
Next field (Time/Date search )	97
Previous field (Time/Date search )	96
Play / Pause	95
Toggle GUI	94
Single Frame Fast Forward	93
Single Frame Rewind	92
Mark Video	91
Still Image Capture	90

After all keys are programmed, press the blue key that is directly under the **Save** label. Then press the rightmost blue key repeatedly until you are prompted to flip dip switch 2. Flip this switch, and log back in to the keyboard.

### Pelco CPU Setup

To integrate with the ISP, the Pelco matrix switch must be configured with the proper ports and macros.

#### Configure the Ports

Using the Pelco Management software, configure the two spare ports as described in Table 11.

**Table 11.** Spare Ports

Setting	Datetime Port	ASCII Port
Equipment number	10	48
Baud Rate	4800	4800
Parity	Even	Even
Data Bits	8	8
Stop Bits	1	1

For Keyboard Number (KBD NUM), use the lowest unused keyboard number.

Choose the **Open Comms** tab and locate two free ports. The ports are numbered starting with 5 from the bottom right of the rear panel of the CPU, as shown in Figure 71.

**Figure 71.** Matrix Switch Physical Ports

28	20	12
27	19	11
26	18	10
25	17	9
24	16	8
23	15	7
22	14	6
21	13	5

#### Configure Macros

Two macros must be configured for each monitor that requests playback video.

Use the Pelco management software to create two macros for each monitor, starting at 100. For example:

```

100  MID  20, 1  (Enable overlays on Monitor 20)
101  MID  20, 2  (Disable overlays on Mon 20)
102  MID  21, 1  (Enable overlays on Monitor 21)
103  MID  21, 2  (Disable overlays on Mon 21)

```

To assign monitor bank numbers for video playback, a BASE number is required. This BASE number is used by the `xvcr.xml` file in the ISP. The following formula is used to allocate macro numbers:

$$\text{Macro} = \text{BASE} + 2 * \text{Mon}$$

For example, using 60 as the BASE number:

```

60 + 2*20 = 100, making 100 the first macro number:
100  MID  20, 1  (Enable overlays on Monitor 20)
101  MID  20, 2  (Disable overlays on Monitor 20)

```

For monitor 27:

```

60 + 2*27 = 114, making 114 the macro number:
114  MID  27, 1  (Enable overlays on Monitor 27)
115  MID  27, 2  (Disable overlays on Monitor 27)

```

The `xvcr.xml` file must be updated with the matching BASE number. This file is located on the ISP in the `/usr/config/running` folder. The following example shows a portion of the `xvcr.xml` file that focuses on the Pelco keyboard definition:

```

<Keyboard>
  <Model>Pelco</Model>
  <KeyboardPort>2</KeyboardPort>

```

```

<MatrixPort>1</MatrixPort>
<IdleTimeout>0</IdleTimeout>
<InstantReplay>0</InstantReplay>
<TimeDateFormat>0</TimeDateFormat>
<MacroBase>60</MacroBase>
</Keyboard>

```

Note: Make sure to allow access to all users when creating a new macro.

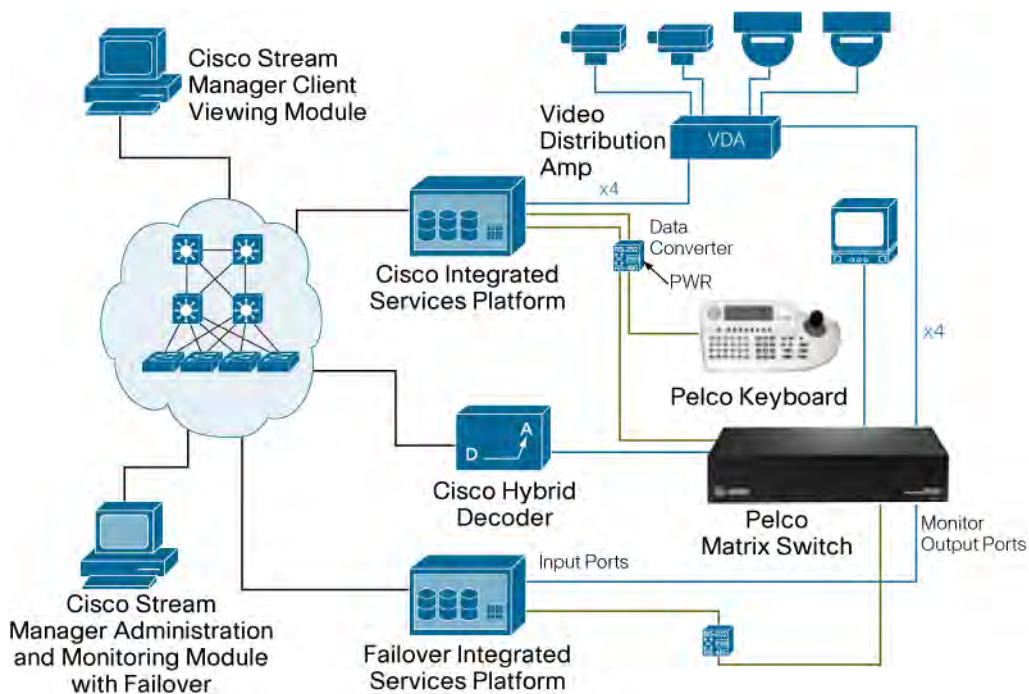
### Failover Configuration with a Pelco Matrix Switch

This section describes how to configure a hybrid solution with a Pelco matrix switch for a matrix-based N+N redundancy.

Note: The example in this section focuses on the CM9700 matrix switch, but similar steps apply to other Pelco systems.

Figure 72 shows how an ISP can act as a failover recorder for other ISPs by using a Pelco 9700 matrix switch.

**Figure 72.** Pelco Hybrid Failover Solution

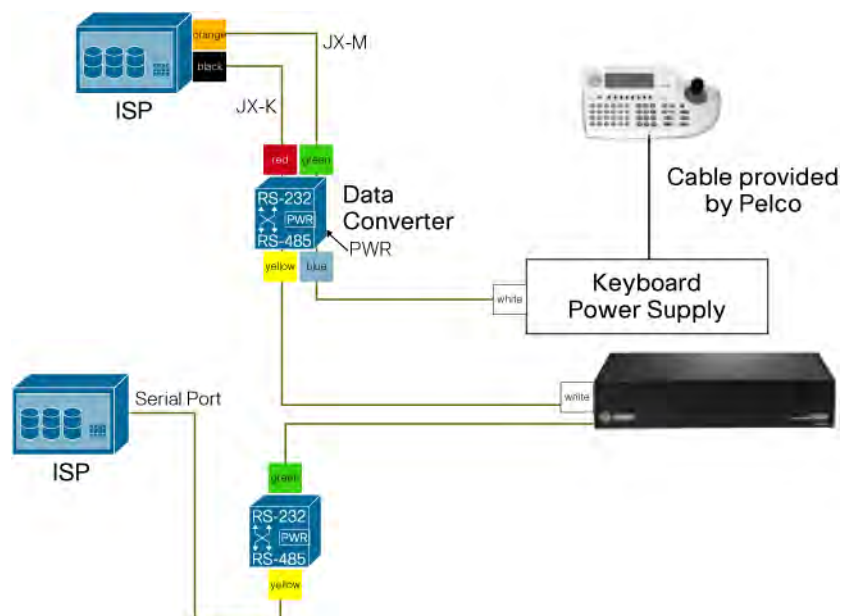


The following equipment and software is required to configure failover with a Pelco matrix switch:

- A dedicated ISP for failover
- The Cisco Stream Manager Administration and Monitoring with Failover Module
- A Pelco matrix switch with available output ports
- An additional data converter between the failover ISP and the Pelco matrix switch

Figure 73 shows the detailed serial cable connections to support the failover integration with a Pelco matrix switch.

**Figure 73.** Pelco Failover Serial Connectivity



Chapter 5 provides detailed configuration steps for failover integrations.

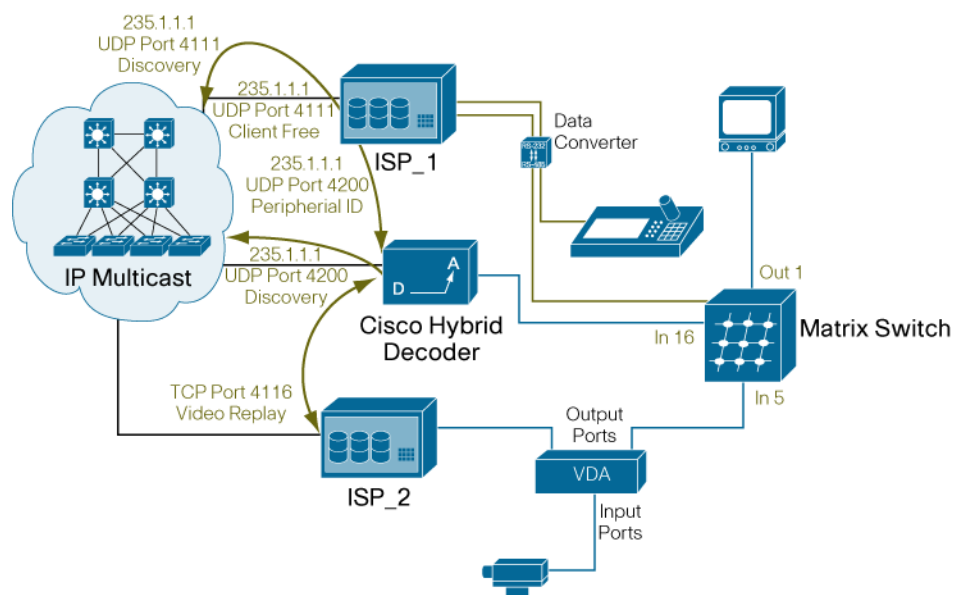
## Appendix A: Network Communications

### TCP/UDP Ports Required for Video Playback

Communication between Stream Manager devices requires a network that is enabled for IP multicast. The “Viewing Live and Recorded Video” section on Page 2-8 explains the steps that take place when video playback is requested. This section describes the network communication and the TCP/UDP ports that are used during a video playback request.

Figure 74 shows the different TCP/UDP ports used during video playback from an ISP.

**Figure 74.** Example—Playing Recorded Video



ISP\_1 sends a Discovery Request (target UDP port 4111) on multicast group 235.1.1.1 at approximately every 5 seconds. This request includes a new Target UDP port (range 4300–4500) in which devices must respond. Active Stream Manager devices respond with information about their capabilities, such as device type, name, and configuration details of each camera. This request allows the ISP to become familiar with the current environment.

When video playback is requested, the following communication takes place:

1. ISP\_1 receives the key sequence and detects that the user wants to play recorded video.
2. ISP\_1 reads the selected camera from the matrix switch and sends a device discovery request for an available hybrid decoder.

ISP\_1 must send a new Discovery Request to ensure that a hybrid decoder is free. The request also takes place on UDP port 4111, but includes a type of XVCRClient and state of Free. The return target is set in the range of UDP port 4300–4500.

1. If a hybrid decoder is available, ISP\_1 sends the peripheral ID and the start date/time to the hybrid decoder.
  - If a hybrid decoder is free, it responds (on the specified UDP port 4300–4500) to ISP\_1 with its capabilities, including the Matrix Input Port, overlay and timezone configurations.

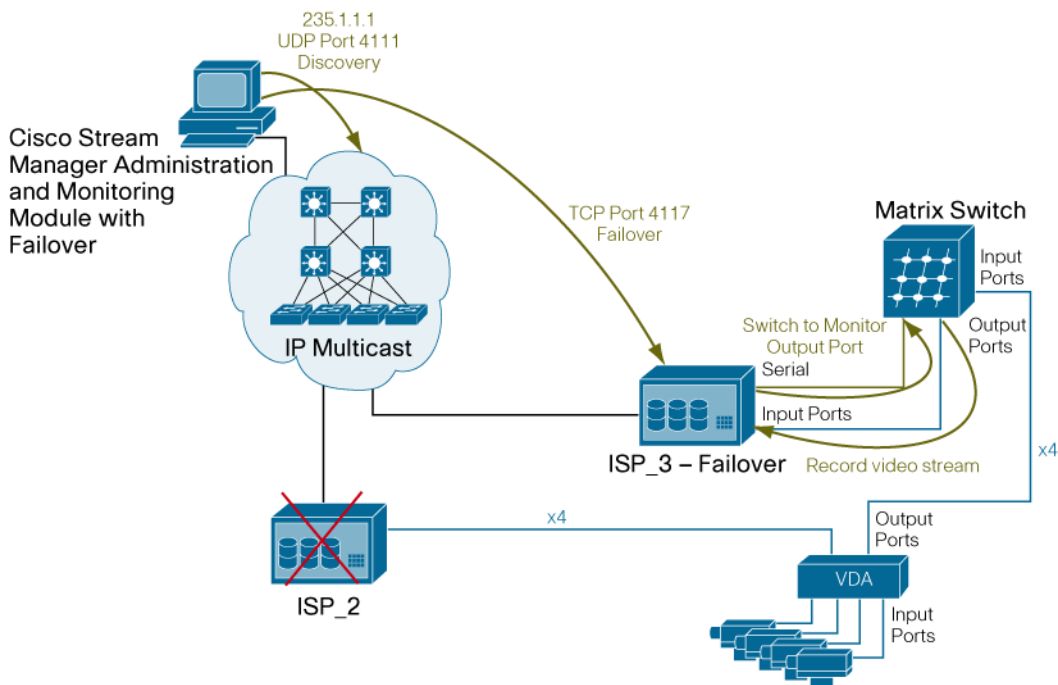
- ISP\_1 responds by using the subscription port (UDP port 4200) with the peripheral ID and start date/time to playback.
1. The hybrid decoder sends a discovery request for the ISP that has recorded peripheral ID 5 at the specified start date/time.  
The hybrid decoder sends this request by using the Device Discovery port (UDP port 4111) to the multicast address 235.1.1.1. This request includes the PeripheralID and StartDateTime and a new target UDP port in the 4300–4500 range.
  1. ISP\_2 responds to the hybrid decoder and a new TCP session is established between ISP\_2 and the hybrid decoder. This session allows recorded video to flow between ISP\_2 and the hybrid decoder.
    - ISP\_2 responds with an announcement that video is recorded on this ISP.
    - The hybrid decoder initiates a new TCP session with ISP\_2 by using the Replay port (TCP port 4116).
    - Using TCP port 4116, recorded video packets flow between ISP\_2 and the hybrid decoder.
  1. ISP\_1 instructs the matrix switch to switch video input #16 to monitor #1. The monitor displays the recorded video on monitor 1.
  2. When an operator presses a key sequence to stop the digital video, ISP\_1 instructs the hybrid decoder to terminate the session with ISP\_2 and instructs the matrix switch to resume live video from camera 5 to monitor 1.
    - ISP\_1 receives the request to terminate playback video via the data converter and notifies the hybrid decoder by using the subscription port (UDP port 4200).
    - The hybrid decoder tears down the TCP session (port 4116) with ISP\_2.

## TCP/UDP Ports Required During a Failover

Communication between Stream Manager devices requires a network that is enabled for IP multicast. The “Matrix-based N+N Redundancy” section on Page 3-1 explains the steps that occur when a failure is detected. This section describes the network communication and the TCP/UDP ports that are used during a failover.

Figure 75 shows the different TCP/UDP ports used during a failover event.

**Figure 75.** Example—Failover ISP



The Stream Manager Administration and Monitoring with Failover Module must be able to communicate with all Stream Manager devices in the environment. This module polls a device three times before logging a failure. In this example, ISP\_3 backs up video streams that are recorded by ISP\_2.

1. The Administration and Monitoring with Failover Module is configured to poll devices every 20 seconds, sending Discovery Requests and Failover Discover Requests (target UDP port 4111) on multicast group 235.1.1.1. These requests include a new target UDP port (range 4300–4500) in which devices must respond. Active Stream Manager devices respond with information such as device type, name, and configuration of each camera. The Administration and Monitoring with Failover Module reviews the responses of all active devices and determines what ISPs are configured as failover ISP.
2. When ISP\_2 fails to respond three times, the Administration and Monitoring with Failover Module initiates a new TCP session with ISP\_3 using the failover port (TCP port 4117) and communicates the camera ID (or peripheral ID) of the first port to back up.
3. Via the serial cable, ISP\_3 instructs the matrix switch to switch video from the failed port to the first configured monitor output port (Camera ID# to monitor Output#). ISP\_3 begins to record on its input port.

4. The TCP session closes and the Administration and Monitoring with Failover Module waits for three seconds.
5. After three seconds, the Administration and Monitoring with Failover Module opens a new session with ISP\_3 using the failover port (TCP port 4117) and transmits the camera ID of the next camera to be backed up. This step is repeated until all failed ports are backed up or until the available failover ISP ports are exhausted. If a second ISP is configured in failover mode, the Administration and Monitoring with Failover Module assigns ports in a round-robin fashion to all available failover ISPs.

While the video streams are backed up, video playback or export requests operate as explained in the “TCP/UDP Ports Required for Video Playback” section.

When the failure is restored, the following steps occur:

1. During its normal device discovery steps, the Administration and Monitoring with Failover Module receives a response from ISP\_2 and recognizes that ISP\_2 has been restored.
2. The Administration and Monitoring with Failover Module starts a new TCP session (TCP port 4117) with ISP\_3 to communicate that the first port is now operational and to stop recording on the first monitor output port.
3. The failover ISP, ISP\_3, instructs the matrix switch to stop sending video on the monitor output port and stops recording on that port.
4. The Administration and Monitoring with Failover Module waits for three seconds and repeats Step 2 and Step 3 until all ports are recovered.



## Appendix B: Glossary

A	
<b>Alert</b>	A message sent to security personnel indicating the location and nature of an emergency or threat.
<b>Attenuation</b>	A decrease or loss of signal. Within a fiber or coaxial-cabled surveillance system, this causes degradation in the video image (e.g. jitter, noise, loss of signal).
C	
<b>Camera</b>	An optical device capable of viewing a given area and translating that view into an electronic signal.
<b>Central Station</b>	A remote location that is designed to monitor signals from physical security systems.
<b>Channel</b>	A single video signal.
<b>Closed-Circuit Television (CCTV)</b>	A television system in which signals are distributed via cables to a closed network of monitors. This system is most often used for security surveillance in small, closed areas like buildings or parking garages.
<b>Coaxial Cable</b>	(aka, Coax). A type of cable that is capable of passing a range of frequencies with low loss. It consists of a hollow metallic shield in which one or more center conductors are put in place and isolated from one another and from the shield.
<b>Common Intermediate Format (CIF)</b>	The term CIF is used to mean specific video resolution: 352x288 in PAL 352x240 in NTSC. CIF is 1/4th of "full resolution" TV, also called D1
<b>Console (CCTV)</b>	The part of a monitoring station an operator uses to control surveillance cameras. Usually consists of a joystick for PTZ control and a set of numbered buttons allowing the operator to switch cameras displayed on an attached monitor. It may also refer to the entire structure at a monitoring station that houses the keyboards, joysticks, monitors, phones, etc. for controlling the physical security system.
<b>Contrast</b>	The ratio of light to dark portions of a video image.
D	
<b>Day and Night</b>	Refers to a video camera's ability to provide images in both lighted and dark conditions by changing the imaging format from color to black-and-white, respectively.
<b>Decoder</b>	A hardware or software device that employs a codec to translate a signal from its digital form into an analog output for display on a monitor.
<b>Depth of Field</b>	The distance between two objects, front to back, which is in focus in a televised scene. With a greater depth of field, more of the scene, near to far, is in focus.
<b>Digital PTZ</b>	(aka, ePTZ). The capability to virtually pan-tilt-zoom within a digital image. The feature does not require the ability to mechanically move a camera or its focus. Currently an emerging feature of megapixel cameras.
<b>Digital Video Recorder (DVR)</b>	Digital Video Recorder is the industry standard term applied to PC-based or embedded systems that encode and record video images to a computer hard drive. DVRs provide a quicker method of retrieving the recorded information unlike media such as VHS tapes and other equipment that stores information in a sequential manner. DVRs are often integrated into enterprise networks through a single Ethernet interface yet they terminate multiple analog cameras, typically four, eight or sixteen. (See also <b>Network Video Recorder</b> .)
<b>Dome Camera</b>	A video imaging device contained within a demisphere. Generally supports the ability to change its focus (i.e. camera PTZ inside the dome) within the field-of-view allowable by the dome itself.
E	
<b>Encoder</b>	A hardware or software device that employs a codec to translate an analog video signal into a digital form.
F	
<b>Field of View (FOV)</b>	A camera's area of focus (i.e. what it can see).
<b>Frame</b>	The total area of the picture that is scanned. With interlaced video, the frame is comprised of two fields.
<b>Frame Rate</b>	See <b>Frames Per Second</b> .
<b>Frames Per Second (FPS)</b>	A measure of a camera's rate of output of single snapshots. Also known as images per second and frame rate.

H	
<b>Horizontal Resolution</b>	The maximum number of individual picture elements that can be distinguished in a single scanning line.
I	
<b>Image Size (Lenses)</b>	Reference to the size of an image formed by the lens onto the camera pickup device. The current standards are: 1", 2/3", 1/2", 1/3" and 1/4" measured diagonally.
<b>IP or Network Camera</b>	A video imaging device that natively attaches to an Ethernet network and delivers its images in IP packets. It differs from its analog equivalents in that it does not require an external encoder to translate the video into a digital signal nor to attach to the IP network.
<b>IP Video Surveillance (IPVS)</b>	Refers to the system or process of monitoring an area by using an IP network as the transport for remote video signals. The components of an IPVS system include edge devices such as IP cameras, IP encoders, or DVRs; an IP network for transport; recording devices such as NVRs; monitoring stations including monitors and consoles served through decoders or PCs running monitoring software; and management software for configuration and maintenance.
<b>Iris</b>	A camera's eye. An adjustable opening that controls the amount of light entering a camera from its lens projected onto the camera's imager.
J	
<b>Joystick</b>	The part of a surveillance system console that allows an operator to steer a camera into different positions.
K	
<b>Keypad</b>	A device that provides a user interface to control a security system or subsystem. Typically includes a numerical 10-key touchpad to allow entering of passcodes and commands. See also <b>Console</b> .
L	
<b>Level Control</b>	Main iris control. Used to set the auto-iris circuit to a video level desired by the user. After setup, the circuit will adjust the iris to maintain this video level in changing lighting conditions. Turning the control toward High will open the iris; toward Low will close the iris.
M	
<b>Manual Iris Lens</b>	A lens with a manual adjustment to set the iris opening (F stop) in a fixed position. Generally used for fixed lighting applications. (See also <b>Fixed Iris Lens</b> .)
<b>Matrix Switch</b>	A video signal device able to route any of its inputs (i.e. cameras) to any of its outputs (i.e. Monitors and recorders). Through a matrix switch, the relation of inputs to outputs is a one-to-one connection unless a looping device is introduced. The actual number of inputs to outputs is generally not one-to-one. Inputs usually exceed the number of outputs available. Matrix switches are usually located at a security operations center, where all video concentrates and displays on multiple monitors. Users control the matrix via a joystick and keyboard that allows switching and the remote control of pan-tilt-zoom cameras.
<b>Mega-Pixel Camera</b>	An IP camera capable of providing extremely detailed image resolution (on the order of HDTV quality). Mega-pixel loosely refers to a single image as containing multi-million pixels.
<b>Monitor</b>	A CRT used to display live and recorded analog video.
<b>Monitoring</b>	The sending of alarm, trouble, and other signals to a remote location such as a security operations center.
<b>Motion Detection (Video)</b>	The process of analyzing a camera's video signal to determine if there is any movement (pixel changes) in the picture and then subsequently trigger an alarm.
N	
<b>Network Video Recorder (NVR)</b>	A PC or network appliance running special software used to capture and store images emanating from IP cameras and encoders. An NVR differs from a DVR in that it provides no encoding of analog video signals; in other words, it has no video inputs. Typically the NVR acquires video by attaching to the source over an IP network. (See also <b>Digital Video Recorder</b> .)
<b>NTSC (National Television Systems Committee)</b>	A committee that worked with the FCC in formulating the standards for the United States color television system. NTSC specifies a resolution of 480 lines at 30 frames per second. (See also <b>PAL</b> .)
P	
<b>Physical Security</b>	The use of personnel, equipment, and procedures to control the access to a facility and its assets.

<b>PTZ (Pan-tilt-zoom)</b>	Describes the capability to change a camera's field of view through three planes of reference. Panning refers to physically sweeping a camera from side-to-side (xy-plane) whereas tilting is the ability to move it up-and-down (azimuth). Zooming changes a camera's lens magnification giving the visual effect that the point-of-focus is closer or further away.
<b>R</b>	
<b>Resolution</b>	A measure of the ability of a camera, encoder or video system to reproduce detail. In analog systems, resolution usually refers to the number of lines that make up an image. Whereas with digital systems, resolution gives a measure of the number of pixels used to generate the image.
<b>S</b>	
<b>Security Operations Center (SOC)</b>	The command center where security personnel monitor and respond to security and safety related incidents.
<b>U</b>	
<b>UTP</b>	Unshielded twisted pair. A cable medium with one or more pairs of twisted insulated copper conductors bound in a single
<b>Z</b>	
<b>Zoom (Digital)</b>	The process of magnifying a video image by using computational algorithms on the digital signal.
<b>Zoom (Optical)</b>	The process of magnifying a video image by changing a lens' focal length.
<b>Zoom Lens</b>	A lens that may be effectively used as a standard or telephoto lens by varying its focal length.
<b>Zoom Ratio</b>	The ratio of the starting focal length (wide position) to the ending focal length (telephoto position) of a zoom lens. A lens with a 10X zoom ratio will magnify the image at the wide-angle end by 10 times.



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)